

E-Commerce

The Cutting Edge of Business

Second Edition

Authors' Profiles



Kamlesh K Bajaj is Deputy Controller in the office of Controller of Certifying Authorities (CCA) and Director, CERT-In, in the Department of Information Technology under the Ministry of Communications and Information Technology. His experience of three decades in the field of Information Technology spans a wide range: information systems planning and implementation, EDI and e-commerce, information security, and artificial intelligence and Expert Systems. Dr Bajaj holds a doctoral degree from McMaster University, Canada. He is a Fellow of the Institution of Electronics and Telecommunication Engineers, and a Fellow of the National Academy of Sciences. He has worked with CAE Electronics Ltd, Montreal, Canada, and Air India. Before moving to the DIT, he was Deputy Director General in the National Informatics Centre. As Deputy Controller in the office of CCA, he is responsible for implementing the technical and legal provisions of the Information Technology Act, 2000. As Director, CERT-In, Dr Bajaj heads the Computer Emergency Response Team for providing proactive and reactive services to the cyber community in India. Promotion of cyber security awareness and early warning system are his major responsibilities.

He has published and lectured extensively on the IT Act 2000, e-commerce, digital signatures, cyber security and cyber crimes. Dr Bajaj is the author of *Office Automation*, and *Fundamentals of Computers* for senior secondary students.



Debjani Nag is Assistant Controller in the office of Controller of Certifying Authorities, Department of Information Technology Ministry of Communications and Information Technology. She holds an M.Tech in Computer Science from IIT Delhi. With the CCA since 2001, her current responsibilities include the implementation of the technology related provisions of the Information Technology Act, 2000 for establishing trust in e-commerce and e-governance in the country. Earlier, she worked with the National Informatics Centre on the development of e-commerce and security solutions and the development of messaging systems under the ERNET project of the erstwhile Department of Electronics, Government of India. Prior to joining NIC, she worked with Tata Consultancy Services and Telecommunications Consultants India Ltd.

E-Commerce

The Cutting Edge of Business

Second Edition

KAMLESH K BAJAJ

*Deputy Controller (Technology)
Controller of Certifying Authorities, and
Director, CERT-In
Department of Information Technology
Ministry of Communications & Information Technology*

DEBIANI NAG

*Assistant Controller (Technology)
Controller of Certifying Authorities
Department of Information Technology
Ministry of Communications & Information Technology*



Tata McGraw-Hill Publishing Company Limited

NEW DELHI

McGraw-Hill Offices

New Delhi New York St Louis San Francisco Auckland Bogotá
Caracas Kuala Lumpur Lisbon London Madrid Mexico City Milan
Montreal San Juan Santiago Singapore Sydney Tokyo Toronto

Information contained in this work has been obtained by Tata McGraw-Hill, from sources believed to be reliable. However, neither Tata McGraw-Hill nor its authors guarantee the accuracy or completeness of any information published herein, and neither Tata McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that Tata McGraw-Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.



Tata McGraw-Hill

Copyright © 2005, by Tata McGraw-Hill Publishing Company Limited.

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

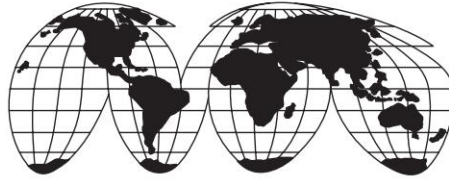
This edition can be exported from India only by the publishers,
Tata McGraw-Hill Publishing Company Limited.

ISBN 0-07-058556-3

Published by the Tata McGraw-Hill Publishing Company Limited,
7 West Patel Nagar, New Delhi 110 008, typeset in Palatino at
The Composers, 260, C.A. Apt., Paschim Vihar, New Delhi 110 063 and
text and cover printed at Rashtriya Printers, M-135, Panchsheel Garden,
Naveen Shahdara, Delhi 110 032

RZZCRRBBDLYXC

*Dedicated to all those in the country
who will help discover
the
lifestyles
value systems
institutions
policies
economics
and
other social entities
of the Information Age
through the use of EC technologies*



Preface to the Second Edition

The second edition of this book is appearing after a gap of six years. In the Internet era, this is more like a couple of decades. Much has happened during these years. The Internet has indeed created a global digital economy with new opportunities. It has graduated from being a new technology to a medium going through the process of consolidation, leading to the transition to a mature Internet economy. From 'Emerging Digital Economy' in 1999, the 'Digital Economy' actually arrived by 2002. The Internet has brought about revolutionary transformation in the way people live and work, in the way commerce is conducted, and in the way governments provide services to their citizens.

The first year of this period, i.e. period 1999–2000, was like a different age in which a big hype was created about a 'new economy' around the dotcom, in what came to be known as the dotcom boom of 2000. Any business built around dotcom, or with the remotest dotcom linkage attracted the best minds, the best venture capitalists and the attendant huge funding. Companies were priced on the ways in which dotcoms would attract the attention of consumers and citizens, instead of actual volume of business that might be conducted. The boom period saw exponential growth, with valuations which were linked to "eyeballs" seeing a website as opposed to any business models that were backing that website. The inevitable happened. The dotcom bust of 2001 saw valuations crash exponentially and

rightly so. There was gloom all around Internet business or e-business. The venture capitalists started running away from dotcom industry back to the so called 'old economy'. The second half of these six years saw the re-emergence of the network economy with the old economy companies, and the brick-and-mortar stores embracing the Internet as an additional channel for reaching out to customers and other businesses. A new form of e-business, backed by solid business models, started emerging. It was interesting to see that the e-commerce forecasts made by companies such as IDC, Gartner in the time of dotcom boom, i.e. in the year 2000 for the year 2004 actually turned out to be nearly true in 2004 notwithstanding the dotcom bust in the intervening years. This was made possible by the dogged efforts of pure-play dotcoms such as Amazon. The innovative efforts of a pure-play dotcom such as eBay in the field of auctions, and the existing old economy companies such as Intel in using Internet as a new channel for better and faster delivery of services to its customers. Travel and ticketing emerged as a major growth area that could naturally benefit from the Internet since no goods required to be distributed—the attendant logistics had, therefore, not to be organized. Retail online also continued to increase substantially. Interesting studies on consumer behaviour revealed that they saw no difference between online and offline shopping. People began resorting to both. Some of them would see goods online and go and shop for them in traditional stores, while in many other situations they would see the goods in real world stores and go back and shop for them online.

E-Commerce is here to stay, without the hype that was created by the dotcom. The industry and consumers alike have accepted the Internet as an additional channel for reaching out to each other. New ways of exploiting the Internet continue to be discovered and new business models keep emerging to make the right companies survive in the highly competitive e-marketplace. In this revised edition, we have tried to capture the spirit of what has happened during these six years. This has led us to delete several chapters and rewrite some others in entirety. Yet another major development that has been addressed

is the widespread adoption of e-governance. International e-governance case studies have been included in Chapter 2, though the title of the chapter does not explicitly reflect the same; those from India are presented in an entirely new chapter.

The new chapters that have been added are:

- Chapter 15 Cyber Crimes
- Chapter 16 Information Technology Act, 2000
- Chapter 17 Public Key Infrastructure
- Chapter 18 Electronic Payment Systems and Internet Banking
- Chapter 19 E-Commerce (Case Studies)
- Chapter 20 E-Governance (Case Studies)

The appendices find their place in the book only to reinforce the contents of the chapters. To supplement the changes in the second edition, the appendices too have been revised. Many of the appendices have been removed completely and the following new appendices have been added.

- Information Technology Act, 2000
- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
- Public Key Infrastructure (PKI) Standards
- European Union Directive on a Community Framework for electronic signatures
- OECD Guidelines for Cryptography Policy issued by Organisation for Economic Co-operation and Development
- European Union Convention on Cyber Crimes
- Indian Computer Emergency Response Team (CERT-In)—profile of objectives, functions, role and activities (public brochure released on inauguration of CERT-In).
- E-Commerce sites of interest (revised)
- E-Governance sites of interest

The thrust of the book is once again on presenting the technology behind e-commerce, and the processes that enable e-commerce to happen. We have also tried to underscore the

importance of security aspects of e-commerce, since it is the trust in electronic environment that will make more and more businesses and consumers venture into the Internet jungle that has come to be haunted more and more by cyber criminals. The technology and processes that help make e-commerce secure from such attackers; and the legal framework together provide the necessary deterrent, and generate confidence for the growth of e-commerce. All these topics have been covered in detail.

Our focus in the second edition continues to be on Business Managers, e-commerce Managers, developers of e-commerce applications and students of MBA and MCA programs. We hope that the book will meet the expectations of all these groups of users. We welcome constructive criticism and feedback at the following email addresses:

kkbajaj@gmail.com

debjani.nag@gmail.com

Kamlesh K Bajaj
Debjani Nag



Preface to the First Edition

Albert Einstein had defined time and space into a single variable at the turn of the century. The resulting energy mass equivalence led to profound changes in physics, which in turn gave mankind a better understanding of sub-atomic phenomena, as well as those on the cosmological scale. The technology arising out of this science has been largely used for the benefit of society.

As we get ready to enter the next century, yet another fundamental redefinition of time and space called the Internet promises to bring about unprecedented changes in society. Commonly known as the Net, it is an interconnection of computer communication networks spanning the entire globe, crossing all geographical boundaries. Touching lifestyles in every sphere, the Net has redefined methods of communication, work, study, education, interaction, leisure, entertainment, health, trade and commerce. There now is a telecommuting global work force in redefined time and space. The Net is changing everything. From the way we conduct commerce, to the way we distribute information. Being an interactive two-way medium, the Net, through innumerable websites, enables participation by individuals in business-to-business, and business-to-consumer commerce, visits to shopping malls, bookstores, entertainment sites, and so on, in cyberspace. One can visit websites not only to download the desired information, but also to fill out forms and lodge them again with the same sites.

In this emerging networked global society, where barriers and tariffs are being dismantled, and where time is of the essence, nations are building their information infrastructures. These National Information Infrastructures are being linked to the Global Information Infrastructure, predominantly for conducting commerce. While Electronic Commerce is becoming a part of day-to-day life and businesses are refusing to deal with any paper in the near future, a whole range of issues, which are matters ripe enough to be dealt with by the governments have surfaced. These include laws for Electronic Commerce, taxation on goods and services sold over the Internet, policing the boundaries, if at all possible, etc. Several international organizations including the UN are seized of these matters, and a number of working groups and committees are addressing these issues through reports and documents. In November 1998, UNCTAD organized a conference on 'Global Electronic Trading' in Lyons, France to create further awareness on these issues.

The Net is also about a new model of governance, a reinvention of the government which fits in with the information age. The computer-based information systems implemented by the governments the world over have been primarily based on the existing rules and procedures. The Internet now enables whole new ways of delivering government services to its citizens in their homes and offices at various levels: local, state and central. It allows services and governance to be anytime, anywhere processes, round the clock. Distribution of printed forms is no longer required, since the web with forms can be connected to the citizens. This calls for radically changing government processes. In applications such as government procurement, processes have been innovated to completely alter the way the government makes purchases. The procurement process has become electronic. The processes associated with taxation, customs, municipal and civil services, legal information, and other ways of interacting with government for filing documents, or receiving information from it, are undergoing radical changes through the technology of the Web and the Internet.

It is time for us to reflect on this technology in our context. We have to harness it for our betterment. We have to find our own solutions to the problems facing our country, especially since, even at the turn of this century and the millennium, we are not an industrial society, in the way the western countries are. In fact, India is unique by virtue of the co-existence of three forms of society. We still have a predominantly rural population based on an agricultural society, while the urban centres are substantially industrial, and are witnessing the dawn of the Information Age. We have to understand the tools of Electronic Commerce and the Internet in order to apply them effectively to find solutions for our society.

The last two years have seen a spurt in the growth of the use of electronic mail (e-mail) and the Internet within India. While e-mail has been mainly used for interpersonal messaging, the need to use information and communication technologies for business communication is increasingly being felt by organizations. With the announcement of the Internet Service Providers (ISP) policy, and the recommendations of the National IT Task Force set up by the Prime Minister, this segment of business communications using e-commerce is poised for a quantum leap.

In this book, the authors have attempted to cover both the 'technology' and the 'non-technology' aspects of Electronic Commerce, and present it in a manner suitable for awareness generation among management, as well as to provide the basic building blocks for e-commerce implementation.

Through 18 chapters and 9 appendices, the 'technology' sections of the book cover the components of Electronic Commerce, different e-mail systems, Directory Services, EDI and UN/EDIFACT standards, the Internet and its technologies, Security mechanisms for EC, and Identification and Tracking Tools. The 'non-technology' sections discuss various methods for streamlining business processes through BPR techniques, and for managing the resultant change and the legal environment in which e-commerce systems can be sustained. The existing

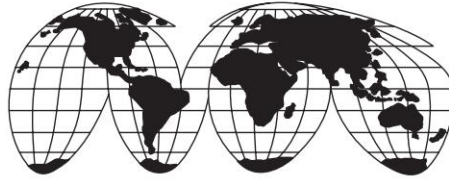
infrastructure in India for conducting e-commerce, how to get started and some case studies are also discussed.

The book is aimed at people involved in trade and commerce. Businesses which are trying to understand Internet and Internet Commerce for expanding their activities through newer and cost-effective methods of reaching their customers would also benefit from this volume. The content of *E-Commerce* would be of immense value to government officials, financial institutions, public sector and private industry wanting to learn about 'The Cutting Edge of Business'.

We invite your suggestions, ideas and feedback on the book at our website: members.rediff.com/ec_book/book.htm

You can also communicate with us through k kb@hub.nic.in or deb@hub.nic.in.

Kamlesh K Bajaj
Debjani Nag



Acknowledgements (From the First Edition)

The book took nearly two years to complete. During this period, there were different types of pressures at work and at home when my mother was seriously ill. Lalita, my wife, was always there to share my burden, and to provide the much needed support, encouragement, and affection. She has been a source of strength and practical wisdom for me. Sameer and Mansi, my children, were very understanding and supportive by being less demanding on my time. They are big enough to have keenly followed the progress of the book. In fact they are part of the youth to whom e-Commerce over the Internet will be as natural as the existing methods of working have been to us. This book is for my mother, who is no more, but memories of her love and affection shall forever be cherished by me.

KAMLESH K BAJAJ

I am indebted to my parents for getting me where I am today, for always being there for me and for always believing in me. Thank you, Ma and Baba. Throughout the period during which this book was written, my husband, Rajiv, was highly supportive, understanding, and encouraging. At times, when the task seemed daunting he kept me focussed on the importance of this book. The future belongs to today's children. This book is for my son, Rajeshwar, who, I hope, will grow up to find e-Commerce a part of the way of life in our country.

DEBJANI NAG



Contents



PART I

THEME OF THE BOOK

- 1. Information Technology and Business 3
- 2. E-Commerce 14



PART II

ELECTRONIC COMMUNICATION

- 3. PCs and Networking 59
- 4. E-mail 73
- 5. The Internet 103
- 6. Intranets 129



PART III

BUILDING BLOCKS FOR E-COMMERCE

- 7. Electronic Data Interchange 141
- 8. The UN/ EDIFACT Standard 157
- 9. The Internet and Extranets 173
- 10. Identification and Tracking Tools 187



PART IV

REENGINEERING FOR CHANGE

- 11. Business Process Reengineering201
- 12. Management of Change223



PART V

CONCERNS FOR E-COMMERCE GROWTH

- 13. Legal Issues233
- 14. Cyber Security250
- 15. Cyber Crimes281



PART VI

CREATING TRUST IN THE ELECTRONIC ENVIRONMENT

- 16. Information Technology Act, 2000.....301
- 17. Public Key Infrastructure316
- 18. Electronic Payment Systems and Internet Banking324



PART VII

CASE STUDIES IN INDIA

- 19. E-Commerce—Case Studies343
- 20. E-Governance—Case Studies358



PART VIII

APPENDICES

- 1. *UN/EDIFACT Message Directory*381
- 2. *Sample UN/EDIFACT Mapping*387
- 3. *United Nations Commission on International Trade Law (UNCITRAL)*399
- 4. *The Information Technology Act, 2000*415
- 5. *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*498
- 6. *PKI Standards*508

7. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures	511
8. OECD Guidelines for Cryptography Policy issued by Organisation for Economic Cooperation and Development	533
9. European Union Convention on Cybercrime	542
10. Indian Computer Emergency Response Team	579
11. E-Commerce Sites of Interest	589
12. E-Governance Sites of Interest	590
Index	593

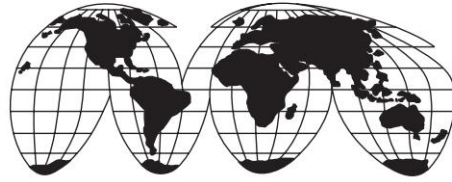
PART

I

Theme of the Book

- Information Technology and Business
- E-Commerce

Information and Information Technology are the key drivers of the Information Age, which is also referred to as the post industrial society. The Information Age has ushered in a knowledge-based industrial revolution. The businesses in this era are networked and use IT to survive in a highly competitive environment. The relationship between IT and business is discussed in Information Technology and Business, while E-Commerce provides glimpses of the worldwide developments that have made e-commerce what it is today.



Chapter 1

Information Technology and Business

A new industrial revolution is in the making, similar to the one that took place at the turn of the nineteenth century. Many economists, management experts and organisation theorists agree that the world is leaving the (old) industrial age and entering a new age; the “*Third Wave*” of Toffler, or Drucker’s post-industrial society. It is being increasingly referred to as the **Information Age**. What are the drivers of the new industrial revolution, or the Information Age? The primary drivers of technology and markets are well known. Marketing, enterprise, entrepreneurship are some of the other drivers. According to Professor Tom Cannon¹, “the new industrial revolution which surrounds us requires profound change; profound change in the way we consider enterprise, develop our businesses, the way we manage and the structures within which we manage”. He foresees not just a change in the market but a fundamental change in the economic relationships between people, between economies, and between societies. Information, and Information Technology (IT) are the key drivers of this Age.

Productivity and efficiency of businesses to reduce costs of products and services, and to use technology to continually innovate and to capture markets is nothing new except that the competition is much more fierce than ever before. Technology

is an enabler of change and a catalyst, but change has to be driven by business drivers that take advantage of the technology. Globalisation of the marketplace, and means of accessing the same, through national and global information superhighways have given a new dimension to the concept of information. In fact, information and knowledge are critical to manage **change**, which is a distinguishing feature of the Information Age. If there is one thing which is permanent during the foreseeable future for businesses, it is change. Businesses do not have sufficient time to consolidate. They are characterised by constant and continuing change. There are continuous changes in the market, changes in customer needs and requirements, changes in technology, changes in resources, changes in system environs, and also changes in rules, regulations and legislations of governments. The challenge in the twenty-first century is not only to survive international competition, and use new technologies, but also to manage change in technology, and in markets.

Manufacturing organisations have already embedded Just-In-Time technologies with full automation of factories to improve productivity and reduce costs. When most organisations have adopted similar technologies, where does the competitive edge come from? Products have to ultimately reach customers in the marketplace. These involve movement from manufacturers to warehouses, to wholesalers, to distributors, and to retailers, in the form of a complex supply chain. Warehousing, and transportation involving sea ports, airports, sea and air transportation, along with national check posts, and international customs barriers, are activities that create major bottlenecks for the efficiency and cost-effective movement of goods. The competitive edge today comes from the efficient management of supply chains.

The competitive advantage for a business comes from its knowledge base, and its ability to mobilise and integrate knowledge. It is knowledge that plays the dominant role in an Information Age business. Labour and capital, which were the

paramount assets of an industrial age business, today stand replaced by knowledge as the most important asset to be managed by businesses. Gary S. Tjaden² compares the key business characteristics of the industrial age and the Information Age businesses through Table 1.1.

Table 1.1 *Comparison of Industrial Age and Information Age*

<i>Industrial Age</i>	<i>Information Age</i>
1. Mass production	Mass customisation
2. Labour serves tools	Tools serve labour
3. Labour performs repetitive tasks	Labour applies knowledge
4. Command and control structure	Common control structure
5. Capital-intensive	Knowledge-intensive
6. Capitalists own production means	Labour owns production means
7. Capital is the primary driver	Knowledge is the primary driver

Information Age is thus **knowledge-based, post industrial revolution**. Such a business is bound to be networked and uses information technology to survive in a highly time-competitive environment. Its other major characteristic is that it is a learning organisation. Senge³ defines learning organisations as, “organisations where people continually expand their capacity to create the results they truly desire, where new and expansive patterns of thinking are nurtured, where collective inspiration is set free and where people are continually learning how to learn together”.

Economist Paul Romer believed technology to be an integral driver of growth. Discovery and innovation are perceived to be more important to competitiveness than manufacturing. This, in turn, depends upon knowledge generation, which has become a high priority for organisations. According to Nonaka and Takeuchi⁴, knowledge creation is essential to innovation in

companies. The latter must be organised with three super-imposed structures. These include a traditional hierarchy for handling routine business activities and creating explicit knowledge, a nebulous structure comprising teams to generate new ideas and solve problems, and a knowledge base that includes explicit and tacit knowledge. The requirements of the new industrial revolution, or the Information Age, are thus the efficient creation and use of information and knowledge. Information Technology becomes a transforming resource for the organisation of the twenty-first century. Since technology diffuses rapidly as a consequence of continuing scientific advancement, and since it is available to organisations and their competition alike, it is knowledge which is the differentiator. It is the effective and innovative use of Information Technology to create the right kind of information from its knowledge base that is associated with technology which can create significant value in the competitive age. Electronic Commerce is an outstanding example of this kind of value addition for businesses in the marketplace. Technologies that are associated with Electronic Commerce have brought about a veritable revolution in the way businesses are conducted. Managers are thus required to use technology to shape their organisations. The existing structures and processes are required to be changed, including people who would be more empowered as team members to deliver goods and services, and not be controlled by their managers⁵.

The Information Age is characterised by extensive use of global communication networks. The networked organisation is the new paradigm. It is the Internet and the information superhighways that have ignited the imaginations of people. The Internet, which was the exclusive preserve of the academic and research community ever since its creation in the 1960s, was allowed for commercial use in the 1990s. Suddenly a large pool of information became available on the World Wide Web at no charge. Information on various subjects had been created in a number of universities and scientific laboratories and it

could be instantly searched from anywhere using the Web technology. The very same tools which were in use in these institutions became available for commercial exploitation. There has been no end to the creative imaginations of those who have put to use the Internet for business and commerce already. New methods have been developed for distributing data, and delivering entertainment over telephone, while at the same time connecting cable TV and satellite networks to the Internet. The merging of data, information, and entertainment electronics has opened up new vistas for businesses. While new businesses are getting created around the convergence of computer, communication, and consumer electronics, existing businesses, companies, corporates and organisations are restructuring and re-organising themselves to take advantage of the Internet into their scheme of things. Intranets and extranets have spawned to improve productivity across all sectors of the economy. The technology and tools of Internet commerce have begun to transform industries in many fundamental ways. These include developing new ways to sell on the Internet, managing costs, purchasing, production planning, supply chain management, organising work processes, and so on. All these are becoming increasingly important for providing companies a competitive edge to their businesses. What is of great importance in the globalisation of markets is its seamless realisation through the Internet. A business connected to the Internet is immediately global in reach and connectivity with no additional expenditure whatsoever.

The organisation of the twenty-first century is expected to be a learning organisation, a networked organisation with completely decentralised methods of working and an empowered workforce with totally new re-engineered work processes. Change, cost, competition and customer are the drivers of this Information Age. The Internet, intranets and extranets through the tools of Electronic Commerce are beginning to make this happen. Information technology and business were never so closely related. Together they are defining new organisations, new products and services, new ways of

delivering them, and new ways of satisfying the needs of customers. The virtual corporation paradigm is becoming a reality. A small biomedical company in Washington, USA, has only six employees with research, toxicology studies, and production contracted out.

The free flow of information, which is enabled by the Internet without any geographic and national barriers, does present security and privacy problems. Similarly, there are legal issues with respect to patents, trademarks, copyrights, responsibility of ownership of data, contracts, and so on. This calls for fundamental changes in the legal, commercial and economic paradigm for the post-industrial society or Information Age. This is once again similar to changes which were brought about by the first industrial revolution at the end of the nineteenth century.

Electronic commerce tools are also being used to change methods of governance. Electronic governance, as it has come to be known, uses the Internet and other proprietary networks to deliver services to citizens, and to bring in transparency between governments and citizens. Information can be retrieved, forms can be submitted, and returns can be filed electronically. The procurement of goods and services by governments is becoming electronic. New methods and procedures are re-engineered from the existing processes to reduce time, cut red tape and present an efficient government to citizens. After all, government is all about transacting business with the public in areas such as taxation; the issuance of documents such as passports, and driving licences; processing documents to issue import licences, other type of permits, etc.

This book is all about Electronic Commerce (e-commerce) technology and the tools that make e-commerce the cutting edge of business. It attempts to cover both the “technology” and the “non-technology” aspects of Electronic Commerce and the Internet, and to present it in a manner suitable for awareness generation among management as well as for providing basic building blocks for e-commerce implementation. It is divided

into 8 parts which comprise 20 chapters. These parts cover the following broad areas:

- Part I : Theme of the Book
- Part II : Electronic Communication
- Part III : Building Blocks for E-Commerce
- Part IV : Re-engineering for Change
- Part V : Concerns for E-Commerce Growth
- Part VI : Creating Trust in the Electronic Environment
- Part VII : Case Studies in India
- Part VIII : Appendices

Broad topics covered in the chapters are as follows:

Chapter 2, E-Commerce—Provides a glimpse of worldwide developments that have made e-commerce what it is today. The status of e-commerce in some countries is also presented. Some of the prominent e-commerce case studies that have contributed to the creation of the Internet economy are discussed. Likewise, e-governance case studies from some of the advanced countries are discussed.

Chapter 3, PCs and Networking—introduces the basics of the tools and technologies. This can be skipped by those who are familiar with PCs and networking.

Chapter 4, E-Mail—talks about the concepts of computer communications and electronic mail based on the OSI Reference Model of the ISO. Both X.400 and Internet mail are covered along with an overview of X.500 Directory Services. Although Internet e-mail is ubiquitous, X.400 is retained to give a glimpse of the bygone era.

Chapter 5, The Internet—gives a brief history of the evolution of the Internet and the kind of services on the Internet today. Internet technologies, including Internet-2 are included.

Chapter 6, Intranets—briefly describes the concept of intranets and the methods of implementing the same in an organisation.

Chapter 7, Electronic Data Interchange—covers the benefits of the EDI system and its various components. The X.435 series of recommendations for EDI Messaging is also included.

Chapter 8, UN/EDIFACT—contains the structure and syntax of the UN/ EDIFACT standard. The interchange structure is explained in detail to bring out all components such as Messages, Segments, Data Elements and Codes.

Chapter 9, The Internet and Extranets—describes how these tools and networks are being used for e-commerce.

Chapter 10, Identification and Tracking Tools—contains the methods for automatic identification of products and trade units—a vital link in supply-chain management.

Chapter 11, Business Process Re-engineering—discusses the need and methodologies available for looking afresh at the processes within an organisation prior to the introduction of new technology tools.

Chapter 12, Management of Change—describes how to manage change as a result of the introduction of new ways of working.

Chapter 13, Legal Issues—covers the issues that need to be addressed to ensure a predictable legal environment which protects the rights of traders, consumers and citizens without impinging on the growth of e-commerce and e-governance.

Chapter 14, Cyber Security—covers the myriad risks that organisations and individuals are exposed to as a result of the implementation of new tools and technologies, and the measures that can be taken to counter these risks. Different cryptographic systems are also discussed and the Public Key Certification method based on the X.509 standard is included.

Chapter 15, Cyber Crimes—addresses the different types of cyber crimes, associated forensics for investigation of these crimes and the current provisions in the IT Act, 2000, for dealing with them.

Chapter 16, Information Technology Act, 2000—introduces the Indian IT Act, 2000, which provides legal recognition to electronic records and digital signatures. The Act, which covers computer misuse and crimes, also encompasses several aspects relevant to the growth of e-commerce, and e-governance.

Chapter 17, Public Key Infrastructure—covers the PKI framework which forms the basis for electronic authentication made legally valid by the IT Act, 2000.

Chapter 18, Electronic Payment Systems and Internet Banking—discusses the methods for electronic payments without which e-commerce and e-governance transactions cannot be completed.

Chapter 19, E-Commerce (Case Studies)—includes six success stories across B2B, B2C and C2C e-commerce in India.

Chapter 20, E-Governance (Case Studies)—focuses on some of the successful projects in the country-at the national level in the Indian Customs and the Railway Reservation System, and at the State Government level in the Land Records and e-Seva Government portal projects.

The Appendices attempt to reinforce the contents of the chapters and are organised as follows:

Appendix 1—The UN/EDIFACT Message Directory, contains the list of messages as contained in the UN/ EDIFACT directory D.97B along with UN/ EDIFACT Control Segments.

Appendix 2—Sample UN/EDIFACT Mapping, in which a sample document is taken and the process of mapping to an UN/ EDIFACT message is presented.

Appendix 3—UNCITRAL Model Law on E-Commerce, on the legal aspects of Electronic Data Interchange (EDI) and related means of communication.

Appendix 4—Information Technology Act, 2000, contains the Act enacted by the Indian Government in June 2000, for legal recognition of electronic transactions, and digital signatures.

Appendix 5—UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, provides additional legal certainty regarding the use of electronic signatures. This model law follows a technology-neutral approach.

Appendix 6—Public Key Infrastructure (PKI) Standards, which are to be followed by Certifying Authorities and users for the use of Digital signatures.

Appendix 7—European Union Directive on a Community Framework for Electronic signatures, which proposes to facilitate the use of electronic signatures and to contribute to their legal recognition.

Appendix 8—Organisation for Economic Co-operation and Development (OECD)—Guidelines for cryptography policy, which looks at the development of cryptographic methods and related standards, implementing privacy and data protection using these methods and the legal and liability issues related to encryption.

Appendix 9—European Union Convention on Cyber Crimes, which seeks to control cyber crimes by requiring participating nations to create a specific, uniform body of laws to deal with these crimes.

Appendix 10—Indian Computer Emergency Response Team (CERT-In), contains the profile of objectives, functions, role and activities as outlined in the public brochure released on the inauguration of CERT-In.

Appendix 11—E-Commerce Sites of interest

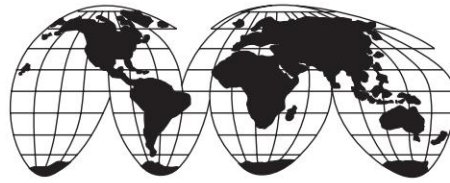
Appendix 12—E-Governance Sites of interest



References

1. Cannon, Tom, 'Management 2000—The Vision', *The British Journal of Administration Management*, July/ August, 1996, pp. 8–10.

2. Tjaden, Gary S., *Measuring the Information Age Business*, The Information Revolution, edited by Alan L. Porter and William H. Read, Ablex Publishing Corporation, USA, 1998.
3. Senge, Peter, *The Fifth Discipline: The Art and Practice of the Learning Organization*, Doubleday, New York, 1990.
4. Nonaka, I., and H. Takeuchi, *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, Oxford University Press, Oxford, 1995.
5. White, Robert M., and Richard H. White, *Technology, Jobs, and Society: The New Challenge of Change*, The Information Revolution, Edited by Alan L. Porter and William H. Read, Ablex Publishing Corporation, USA, 1998.



Chapter 2

E-Commerce



2.1 Electronic Commerce

Information Technology has transformed the way people work. Electronic Commerce (e-commerce) has unleashed yet another revolution, which is changing the way businesses buy and sell products and services. Associated with buying and selling of information, products and services over computer communication networks, e-commerce helps conduct traditional commerce through new ways of transferring and processing information, since it is information which is at the heart of any commercial activity. Information is electronically transferred from computer to computer, in an automated way.

E-Commerce refers to the paperless exchange of business information using electronic data interchange, electronic mail, electronic bulletin boards, electronic funds transfer, World Wide Web, and other network-based technologies. E-Commerce not only automates manual processes and paper transactions, but also helps organisations move to a fully electronic environment and change the way they operate. After the e-commerce Framework was announced by the US Government in 1997—at the time when the Internet was allowed to be used by commercial organisations—it was the US Government's announcement that all federal purchases would be made

paperless that gave an impetus to this new way of conducting trade and commerce. Surprisingly, it is an application that is today associated with e-governance, namely e-procurement. The European Union followed with a similar directive to its member states to make government procurement paperless through e-procurement. In fact, e-procurement using e-commerce tools turned out to be one of the major drivers in the growth of e-commerce. In the last decade, organisations have started conducting e-commerce over the Internet, the network of networks. The Internet gave yet another boost to e-commerce because it is a low cost alternative to proprietary networks. E-Commerce standards are, however, under development. The more well known Electronic Data Interchange (EDI), the inter-organisational exchange of business documentation in structured, machine-processable form over computer communication networks, is still the dominant part of e-commerce.

Information gathering, processing, manipulating and distributing is common to trade and commerce, no matter what the commodity or service that is being exchanged. Today, it is the velocity of information processing and dissemination, which determines the speed of real commerce. Computers and networks, by virtue of their sheer speeds, are creating electronic marketing with the potential to be more efficient in finding and interacting with customers, communicating with trading partners, and developing new products and markets. While on the one hand, Local Area Networks (LANs), and enterprise wide intra-networks have resulted in rising expectations for data access, communications and productivity throughout the business world, on the other, low cost high speed open networks interconnected as a network, commonly known as the **Internet**, have kept pace with the requirements through the establishment of national information infrastructures, with high speed national information highways being their main backbones. Widespread access to network communication tools including electronic mail (e-mail), online services, and Web browsers have created a new

awareness of the commercial potential of the Internet. While the Internet has already been successfully used for marketing, advertising and some commerce, much of its technical potential remains to be commercially harnessed. EDI is still the proven application of e-commerce, especially for business-to-business commerce.

Organisations and countries worldwide are seized of the impact e-commerce will have on the world economy, globalisation of markets, international trade, financial markets, etc. The world is at the threshold of a new industrial revolution that is being shaped by the Internet in general, and e-commerce in particular. E-Commerce implies not just using network-based technologies to conduct business. It is about moving organisations to a fully electronic environment through a change in their work procedures, re-engineering their business processes, and integrating them with their business partners beyond their traditional boundaries. E-Commerce has brought about a veritable revolution in the way business is conducted. There is a paradigm shift from paper-based transactions to fully electronic organisations, and as observed earlier, IT, in general, and tools of Internet commerce have begun to transform industries in many fundamental ways.



2.2 Electronic Data Interchange (EDI)

EDI can be used to electronically transmit documents such as purchase orders, invoices, shipping notices, receiving advices, and other standard business correspondence between trading partners. EDI can also be used to transmit financial information and payments in electronic form. When used for effecting payments, EDI is usually referred to as Financial EDI and Electronic Funds Transfer (EFT).

EDI is a way of substituting electronic transactions for paper ones. However, it is much more than mere substitution. It is a means to streamline procedures, and improve efficiency and

productivity. EDI allows a new look at the 'processes' within an organisation, with a view to re-engineer them in what has come to be known as Business Process Re-engineering (BPR).

2.2.1 Benefits of EDI

Computers have speeded up the production of invoices, purchase orders, etc. When these documents are produced by high-speed printers, however, they must still be detached, inserted, and mailed; copies must also be filed by the originating organisation. Originals must be physically transported to the addressee, opened, carried to the appropriate individual within the addressee organisation, and processed, which usually entails keying of the data into an MIS system, manually.

The use of EDI eliminates many of the problems associated with traditional information flow, which are delineated below.

- The delay associated with making documents is eliminated.
- Since data is not repeatedly keyed, the chances of error are reduced.
- The time required to re-enter data is saved.
- As data is not re-entered at each step in the process, labour costs can be reduced.
- Since time delays are reduced, there is more certainty in information flow.

Another advantage in the use of EDI is that it generates a functional acknowledgment whenever an EDI message is received, and it is electronically transmitted to the sender. This acknowledgment states that the message is received.

Therefore, the core concept of EDI is that data are transferred electronically in machine-processable form, i.e. the EDI message can be immediately processed by the receiving computer without any human intervention, or interpretation or re-keying. Hence it is most suited in areas where any of the following characteristics exists:

- A large volume of repetitive standard actions.

- Very tight operating margins.
- Strong competition requiring significant productivity improvements.
- Operational time constraints.
- Trading partners' request for paperless exchange of documents.

The benefits are so compelling that companies must soon adhere to EDI standards if they expect to sell to large US organisations such as Fortune 1000 companies, wherein the volume of these documents is always burdensome. Likewise, in order to minimise production costs, the manufacturing industry has started using EDI. For example, at Levi Strauss, retailers must order jeans a month in advance, unless they use EDI, in which case they can order two weeks ahead. This reduces inventory costs. Retail companies such as Wal-Mart have their own proprietary EDI networks to connect with suppliers and logistics handlers. Wal-Mart, the retail king with a turnover in excess of US\$ 250 billion, does not conduct business with any supplier who does not adopt its EDI system for paperless transactions.



2.3 E-Commerce Types

A business organisation can organise itself to conduct e-commerce with its trading partners, which are businesses, and/or with its customers. The resulting modes of doing business are referred to as Business-to-Business (B2B), and Business-to-Consumer (B2C) e-commerce. There is yet another category of e-commerce, referred to as Consumer-to-Consumer (C2C). The auction or sale of goods by one person to another through special auction sites run by business organisations falls under this definition. The formal definitions of these categories are given below.

B2B: This is e-commerce between businesses. The exchange of products, services or information between businesses on the

Internet is B2B e-commerce. Some examples of B2B websites include company websites, product supply and procurement exchanges, specialised or vertical industry portals, brokering sites, information sites, and banking and financial sites that provide information for its business customers and employees. For example, Seekandsource.com is a very large Indian cross-industry marketplace that is ideal for businesses buying and selling to a wide cross-section of industries. B2B needs to have inbuilt processes to integrate sellers' and buyers' systems for delivering maximum benefits to trading partners.

B2C: This is business-to-consumer e-commerce. It may be defined as any business selling its products or services to consumers over the Internet for their own use. Amazon.com, the online bookseller that launched its site in 1995 to sell books and other products directly to consumers, is a prime example of B2C e-commerce. In addition to online retailers, B2C has grown to include services such as online banking, travel services, online auctions, real estate, health services, insurance and other services. Retailers do not have to integrate with their customers' systems, though they need to track their preferences to keep their loyalty to their (retailers') sites so as to ensure their repeat visits.

C2C: This is consumer-to-consumer e-commerce. A virtual marketplace on the Internet in the form of a website enables sellers and buyers to meet and exchange goods, including used goods, at a negotiated price in C2C. Such a site is known as an auction site, and it started out like a garage sale. The most famous site is eBay.com, which started the C2C revolution. Many similar companies in other countries have been acquired by eBay. For example, in India, the auction site Bazee.com has recently been taken over by eBay.

E-Business

A business organisation may establish itself as an electronic business, known as e-Business or e-Biz, by suitably re-engineering its processes so as to be a fully electronic business in terms of its interface with its trading partners, as also with its

customers. Today's business processes are intricate and complex. A simple transaction may involve several trading partners spread across the globe, and it may trigger actions in many other business processes. These complexities and interdependencies of business processes are often handled through business systems, which seamlessly knit seemingly different organisations by virtue of their embracing of the electronic environment through the use of e-commerce to become electronic organisations. The result is e-Business, which, though focused on e-commerce, goes well beyond it.

The Aberdeen Consulting Group defines e-Business as 'the automation of the entire spectrum of interactions between enterprises and their distributed employees, trading partners, suppliers, and customers'.

The Giga Group simply defines e-Business as 'the application of electronic network technologies to transform business processes'.

Although evolution began with early e-Business initiatives such as browser-based applications, e-Business transcended well beyond web-enabled product sales. A business would develop web applications that were 'focused, functional, and frequently fixed (4Fs)'—referred to as 4F e-Business applications.

In the realm of e-governance, the services are similarly categorised as being delivered by one government organisation to another government agency, or to a citizen. These are known as government-to-government (G2G), or government-to-citizen (G2C) e-governance applications. There is yet another application in which a government interacts with its employee electronically, government-to-employee (G2E) interface. The formal definitions of these categories are given below.

G2G: The interaction of back-end government systems of different departments or organisations through a G2G portal, akin to B2B e-commerce, integrates their functions for presenting a unified image of the government to citizens. G2G interactions take place without citizens' knowledge. Data may be exchanged

through such portals at pre-fixed times, say in batch mode, or it may be triggered by an action in the computer systems of one government organisation. For example, the Customs department and DGFT (Directorate General of Foreign Trade) systems may integrate through a customs portal to present a single image to citizens.

G2C: A government website or a portal delivering services to a citizen is a G2C transaction, akin to B2C e-commerce. The website is designed to publish and deliver services to a citizen, and to enable him to trigger a transaction, with the citizen paying for the service delivered to him through the B2C site. For example, the issuing of a birth certificate, or a driving licence by the concerned G2C site to a citizen would fall under this definition.

G2E: Through such a website a government may disseminate information to an employee concerning him, and may allow him to interact with it for a transaction.



2.4 E-Commerce and the World at Large

The Internet is creating a global digital economy with new opportunities. It has graduated from being a new technology to a medium going through the process of consolidation, leading to the transition to a mature Internet economy. Its most distinguishing feature is that Internet connectivity is ubiquitous—access to the Internet is sought to be made as universal as the telephone. The development of infrastructure, therefore, is a key area of growth in countries around the world. Various forecasts had estimated that more money would be spent in building technology and business infrastructures in the years leading up to 2004 than the actual amount of e-commerce transacted. One such forecast by IDC in the year 2000 put infrastructure spending in the year 2004 at US\$ 1.98 trillion, while e-commerce spending in the same year would be US\$ 2.5 trillion. At the time of writing in the middle of 2004, these forecasts are believed to be correct, though at the time of the

'Internet bubble burst' around 2000–01, e-commerce was at an all-time low, and forecasts had become gloomier.

The information infrastructure for e-commerce and e-governance applications comprises the following: a robust, widespread telecommunications infrastructure spanning the entire country to make telephone and Internet connections available at an affordable price; PC proliferation at an affordable price; and a legal and administrative framework to create a predictable environment for e-transactions. The former are best represented by indicators such as teledensity, PC penetration, and Internet connectivity. These are briefly described in section 2.5. We will examine the impact that Internet commerce is having internationally.

It was in 1999 that the Internet frenzy was at its peak. Ideas were dominating valuations of companies. It was thought that an idea for a new service, or the sales of existing products through websites would result in huge profits. The handling of logistics, such as supply chain issues, in the physical world was not considered necessary. There was no need for physical presence, or brick-and-mortar offices to back a website in cyberspace. Such companies were known as pure-play dotcoms. Crazy ideas could get support from venture capitalists. The market capitalisation of pure-play dotcoms, even without any sales or other revenues, rose to dizzy heights of several billions of dollars. Wild figures were being projected for Internet commerce. The cyberspace bookstore, amazon.com led this group of pure-play dotcoms. Amazon learnt the hard way that books had to be delivered to customers from warehouses—either their own or those of publishers—thus requiring the building of necessary supply chains in the physical world. It took several years to reach a profitability level. Most other pure-play dotcom companies did not survive. Exceptions are the leading auctions company, eBay, and travel and ticketing companies such as expedia.com. The positive fallout of dotcom failures, however, has been the decision of traditional companies to embrace dotcom approach to sell their products and services as an

additional channel to reach out to customers. They have discovered that if they do not adopt e-commerce technology, there will be a permanent erosion of their competitive position in the marketplace. So, the traditional economy has moved to adopt e-commerce. Retailing online has come to be known as e-tailing.

E-Commerce was perceived as B2C, with thousands of websites mushrooming all over the place catering to consumers. With millions of Internet users browsing cyberspace, there was hope that they would all be shopping on the Net. It was realised, rather painfully, by entrepreneurs that consumer trust in an electronic environment would not come by easily. People started using websites more for window shopping, and collecting of information about products, rather than actually for ordering. Consumer behaviour did not turn out to be along expected lines. consumers would use the Internet to search the right product at the right price, and then go to buy it from a store in the real world, i.e. for shopping offline. Today, in the US, three out of four customers walking into a car showroom have already researched their choice online. They would also know how much they need to pay for it. It is the same story with other products and services. However, this trend is changing as we shall see in the Amazon.com case study.

Consumers see no difference between online and offline shopping. They seem to do both. They perceive the Internet as just another sales channel, and a convenient tool for browsing and research. Thereafter they make their purchase in whatever way happens to suit them best. It is for this reason, i.e. for reaching out to customers, that most traditional companies opened shop in cyberspace. They also had to find ways of advertising and marketing online. Sponsored links on search sites such as Google and Yahoo! have thus become effective marketing tools for online companies. In the US alone, retail e-commerce touched US\$ 106 billion in 2003, and was expected to be of the order of US\$ 120–150 billion in the year 2004. This, however, is still the tip of the iceberg, constituting a mere 2–3

percent of retail sales in that country. Similar trends are visible in European and other countries.

For consumers there is lot more to online shopping than merely buying products and merchandise. Services such as travel and banking are moving online very rapidly. In travel, airlines are reaching out to their customers directly, or through online websites. Travel is estimated to account for about one-third of online consumer spending. According to PhoCusWright Consumer Travel Trends Survey, over 35 million Americans bought travel services online in the year 2003 (a 17 percent increase over the previous year). Nearly 20 percent of bookings in America are now done online. People feel that they have control over their travel plans, their bookings are safe, their money is secure and that their problems are dealt with promptly if they make online deals. They have the convenience of buying everything in one place. The satisfaction of getting a bargain, and above all, value for money is what lures them to websites for browsing and actually buying their tickets. Technology helps lower transaction costs for online travel agents. They offer cheaper business travel than many offline agents. The top online travel agency sites include Expedia, Travelocity, Orbitz and Cheaptickets in the United States; Ebookers, Opodo, Lastminute, Travelocity and Bridge the World in Britain; and Wideroe in Norway. Expedia.com alone sold \$ 10 billion dollar worth of travel in the year 2003. Similarly, the top performing airline sites in terms of selling online tickets include Continental, Northwest, America West, and American Airlines in the United States; Virgin Atlantic, British Airways, EasyJet, and British Midland in Britain; and Air France¹.

E-Commerce has spawned a new line of online business that was hitherto buried in the 'classified' sections of newspapers. Today, billions of dollars of used goods are sold on Internet auction sites, with the most successful site being eBay. Second-hand cars now constitute eBay's biggest category. People not only buy and sell used goods, they post their experiences on the website which helps generate further trust in auctions on the

eBay site. Even settlement of transactions by way of payments, however small, has been facilitated by easy-to-use 'paypal', that incorporates traditional methods such as credit card, and existing bank accounts for debit and credit. An astounding \$ 24 billion worth of trade was done on eBay in the year 2003. In India, 'baazee' is an auction site that is doing extremely well. It has recently been acquired by eBay. In China too, eBay's service is the biggest e-commerce site.

As regards other services on the Internet, pornography ranks in a category by itself. In fact, it is one service that helped e-commerce grow, since while browsing for pornographic websites, users would visit other sites too. In the year 2004, Americans spent an estimated \$ 2 billion on pornographic sites according to the trade magazine, 'Adult Video Magazine'. Gambling online, on the other hand, is estimated to be worth around \$ 6 billion worldwide.

Then there are online music, games and video services, constituting e-entertainment, that are a rage among consumers, especially youngsters. Today millions of music files are downloaded across the world. Many of these are stored on portable players. As a result, in many cities, traditional record shops are closing down. Apple's iPod is the most successful portable music player. A combination of its beautiful slim player incorporating fashionable technology, and its online music store iTunes, has enabled Apple to sell 2.5 million songs a week. In order to expand its sales worldwide, Apple needs to establish a music-downloading service outside the US, and to comply with local copyright laws. Many other music and software companies are trying their own brands in online music. The movie business is waiting in the wings to re-invent itself on the web—it is watching closely how music is sold online.

Advertising and marketing on the web is picking up in new and unique ways. In early days of e-commerce, it was perceived that all online content would be free, since it would be paid for by advertisers on websites. Initially, online newspapers, magazines, music, video, gaming sites were free. Most of them

wound up in the absence of proper business models, since advertising revenues did not measure up to the requisite levels. More recently, popular search engines like Google and Yahoo!, incorporating powerful software programs known as crawlers, are being used by Internet users throughout the world to reach their desired destinations on the basis of search keywords. When search results are returned, sites which have paid for sponsorship appear prominently as sponsored links. While pages are returned ranked in their likely order of usefulness, sponsored links appear in one corner. Google lists its sponsored links on the right side of its page while Yahoo! puts them on a box at the top. Since search engines have become an essential link between buyers and sellers, huge marketing and advertisement budgets are being allocated by most online companies to get high rankings in sponsored links. A study by the New York-based Interactive Advertising Bureau in partnership with PricewaterhouseCoopers found that online ad spending grew to US\$ 7.3 billion in the year 2003.

There is yet another way for starters to get noticed online. They can offer goods and services through one of the websites that already get a lot of traffic. Amazon, eBay, and Yahoo! are becoming huge trading platforms for other companies. The products and services offered have to stand up to intense price competition, since consumers check for prices not only against other online sites, but also in physical stores. Consumer behaviour online has a marked property of no permanent loyalty to any online store or shop, unlike in the physical world. Consumers will go to another shop because the next site is just a click away. The link between the online and offline world is having a direct impact on traditional shops. It is projected that many shops will actually turn into showrooms. Customers will research their products online, see them in showrooms to 'feel' the actual products, and then go back online to order from their preferred websites.

Other online services that are part of e-commerce include financial services, ticket sales agencies, hotel and car reservations,

online dating and matchmaking, tracing of ancestors, and illegal buying of drugs online. The list is endless. The imagination of the people is the limit to applications on the Internet. For example, people are using eBay auction site to operate 'virtual stores'. Thousands of people around the world make a full-time living to earn a second income from buying and selling things on web-sites. In a recent survey, eBay found that some 4,30,000 people in America alone make full-time or substantial living from trading on websites.

All this constitutes B2C and C2C e-commerce. B2B e-commerce, on the other hand, is, according to some estimates, well in excess of US\$ 1 trillion. This is touched upon briefly in the next section.

2.4.1 US Digital Economy

The economic growth of nations is now directly related to growth in the IT industry and the use of IT in trade, commerce, governance and other activities of human life. Studies have shown that sustained economic growth in the US during the past decade could primarily be attributed to growth in the IT sector. Figures published by the US Department of Commerce² suggest that during the years, 1995–1998, the IT industries—key enablers of e-commerce—were responsible for 35 percent of the US' real economic growth, whilst representing only 8 percent of the US GDP. In 1996 and 1997, the same industries are believed to have lowered US inflation by 0.7 percent. It was estimated that by the year 2001, nearly 40 percent of the US population would be online, as compared to only 13 percent in Europe. It was further estimated that in direct proportion, the e-commerce market would be three times more significant to the economy in the US than in Europe. This, in turn, would have a direct relation to the income gaps between the US and Europe. It is projected that the already wide income gaps between the information-rich and information-poor countries will further widen if the Internet and e-commerce are not integrated into businesses by the latter.

The US Digital Economy Report 2002, published in June 2003, signified that the digital economy had already arrived, since the word 'emerging' was dropped. Notwithstanding the failure of a large number of e-commerce companies—more commonly known as dotcom companies, during 2000–2001, the Internet business was not considered to be in danger of disappearing. Over 10 percent of the dotcom companies closed down in 2001. The failure of many online dotcom companies led to the realisation that they had to be backed by solid business models for generating revenues. The euphoria at the closure of the last century, that dotcom companies would replace real world physical companies came a cropper. Merely providing access to products and services by online companies through their websites was not enough. This had to be integrated with actual services in the physical world such as supply chain management, which was slow to develop. However, the lessons have now been learned and migration to the e-commerce world continues.

Before we look at a couple of interesting case studies that have given an impetus to e-commerce, it might be instructive to examine the phenomenal growth of the Internet, which is the driver for e-commerce.



2.5 Internet Connectivity

The Internet reached 150 million users in a span of just four years. This may be compared with radio that took 59 years to reach out to 50 million users and TV that took 33 years to reach out to 100 million users. By the end of the year 2003, there were 687.6 million Internet users. Internet connectivity is being enabled through broadband devices including mobile phones.

The developed world, in particular the US and some of the OECD countries, has had a very long lead over developing countries in telecommunication infrastructure and the use of the Internet as well as Internet commerce. The private sector is highly developed there and has reached the present stage wherein

government funding has given them vast experience in the fields of commerce, business, governance, etc. The developing countries are, however, struggling to come to grips with the fundamental growth indicators of the Internet.

It is common to compare developments in any country with those in the US. This is primarily because the Internet, e-commerce, and e-governance were largely developed in that country. Internet users in the US crossed 150 million in January 2004. E-Commerce figures for the year 2003 in the US were: B2B at \$ 1331 billion, and B2C at \$ 106 billion³. The US Government official figures for the digital economy, published by the Department of Commerce, also place B2C transactions at nearly \$ 100 billion for the year 2003.

In contrast, Internet subscribers in India at the end of March 2004 were only 4.2 million. Other than home subscribers, all Internet connections taken by organisations, and businesses are used by multiple users. Hence, with an average of 5 users per subscriber account, this translates to approximately 20 million users. This is a reasonably large number for the Internet economy to thrive. One can compare this favourably with, say Australia, which has 3.6 million Internet users.

Yet another indicator of Internet economy activity is the number of Internet servers in a country. It has been pointed out in Chapter 4 in the section on Domain Names, that the country top level domains (ccTLDs) are operated by each individual country. There are also the generic level TLDs, known as com, org, net, edu, gov, mil, int, biz, arpa and others. At the time of writing, as per the DNS Survey of July 2004, conducted⁴ by [http:// www.isc.org/](http://www.isc.org/), there are 285.1 million servers connected to the Internet. Servers are those that have a unique IP address, with a domain name, and are connected to the Internet. Out of these, nearly 192.9 million are in the category of gTLDs, while the remaining 92.2 million are in the country domains. North America and Europe account for 5.9 and 44.5 million ccTLD servers, respectively. This does not include servers in gTLD such as .com which are mostly located in the US. Asian countries

have the following numbers: Japan has 16.5 million servers, Korea, 0.3 million, Taiwan, 3.2 million, Singapore, 0.5 million, Malaysia, 0.11 million, India, 0.14 million, and China, 0.16 million. Australia accounts for some 4 million servers. Latin America has about 6.6 million servers (including Brazil—3.5 million, Argentina—0.9 million, and Mexico—1.5 million). South Africa has 0.4 million servers. The rest of the world with 110 odd countries accounts for approximately 10 million servers. Clearly, Internet activity is very low in most of the countries. Of the 285.1 million Internet hosts worldwide, 263.7 million are in the developed world. Asia, excluding Japan, Taiwan and Korea, has 3.1 million hosts only, which accounts for about one percent of the total number of hosts. India has only 1,43,654, while China has 1,62,821 servers.

However, there is one category of gTLD, namely .com that is used by all countries. There are 53.4 million .com servers that are used for e-commerce. Although these are largely located in the US, businesses in most other countries also use the same. Similarly, there are 127.3 million .net, and 8.2 million .edu servers with 1.5 million .org servers. Again, all these are used by organisations in all the countries. It would not be incorrect to assume that these are apportioned among the countries in a manner that reflects the above distribution of ccTLD servers. These contribute significantly to e-commerce transactions for these smaller countries too (smaller in terms of Internet use).

The worldwide population of Internet users is 687.6 million. Their distribution is highly skewed: USA—159m and Canada—16m; Europe—190m; Japan—62m; China—80m; India—19m, Australia—11m. The number of Internet users in India and China is clearly not as low as the number of Internet hosts⁵.

It has been observed that e-commerce volumes are in direct proportion to some of the above indicators. The developing countries are rightly concerned that if there are increasing returns to scale in the globalised networked economy, characterised by Internet commerce, there could be risk of further polarisation. The point is not whether to use the Internet and be a part of the

global electronic commerce. No country has that option. The scenario of the Internet economy has already arrived. Countries have to make use of the opportunity and overcome the dangers of isolation and polarisation.



2.6 E-Commerce—Case Studies Leading the Transformation

B2B comprises about 80–90 percent of all e-commerce by value. Businesses are transforming themselves into e-Businesses by incorporating e-commerce tools, re-engineering their business processes and integrating them with those of their partners. In this section, we will present three case studies that are leading this transformation in different areas. Intel is an existing company that started using the Internet as a distribution channel in the mid-1990s. It transformed itself into an e-Business. Amazon is a pure-play dotcom company that rediscovered itself, after initial emphasis of sales through website only, in the physical world by incorporating a supply chain, warehousing, and customer relationship to become a profitable business. eBay is yet another pure-play dotcom company that pioneered C2C e-commerce and became a profitable company from the very beginning.

2.6.1 Intel

In the mid-1990s, Intel adopted e-commerce technologies to reach out to its customers and trading partners. Within a few years, Intel was handling over 3 million page hits per day with an online revenue of \$ 2 billion per month. Intel's websites deliver online information and support to a complex network of customers, employees, channel resellers, suppliers and OEMs. Over 6000 users in more than 50 locations around the world use the customised, personalised and secure B2B functionality. By the year 2002, over 85 percent of Intel's sales orders were

transacted electronically, and many online ordering applications were linked with back-end ERP systems. As a result, Intel's efficiency rose to new levels, and enabled it to respond more quickly to changes in the marketplace.

Intel defined e-business in terms of what they called 100 percent e-corporation concept: a corporate strategy to re-engineer and automate business processes, using business systems and Internet technologies, aimed at significantly improving customer, employee and supplier business interactions. Their concept was thus consistent with the other two definitions of e-Business given earlier in Section 2.3. All these definitions encompass a broad range of business processes, including:

- Multi-entity product design collaboration
- Simple electronic product marketing and information sharing
- E-Commerce sales of product to consumers or between businesses
- Internal business process re-engineering
- Multi-entity supply chain collaboration
- Customer relationship management

It was clear that business processes and interactions needed as much focus as the systems and automation.⁶⁻⁹ Real value comes from significant changes in the business processes in an e-business implementation. System implementations alone carry little value. Moreover, e-Business capabilities can apply to a broad range of business processes and their interactions. Some examples of business process transformations and associated systems are given in Table 2.1.

Intel identified the following key areas for e-Business enhancement:

- Substituting information for inventory: Businesses are improving their bottom lines by streamlining supply chains and basing business decisions on faster, more reliable information.

Table 2.1 *Business Processes and their Interactions*

<i>Business process transformation</i>	<i>Associated systems</i>
Change from centralised warehousing to geography-based local warehousing.	Inventory management system Local warehouse replenishment system.
Transition from manually received orders over phone and fax to automatically received orders over the Internet.	Order management system or web-based order management system.
Transition from employee benefits administrators entering and tracking information in a telephone help-desk environment to employees logging on to view and modify their own benefits selections.	Web-based employee self-help benefits selection tool.
Purchasing raw materials through Internet-based 'reverse auctions' instead of face-to-face, multi-round, contract-based negotiations.	Internet auction site.

- Secure online collaboration: Internet links between trusted business partners enable the creation of 'value chains' that speed the entire process of developing and delivering products and services.
- Enhanced customer relationships: Online services help businesses respond more quickly and effectively to customer needs. By using data warehousing and business intelligence technologies, they can also understand their customers better, thereby improving their ability to deliver targeted products, services and support.

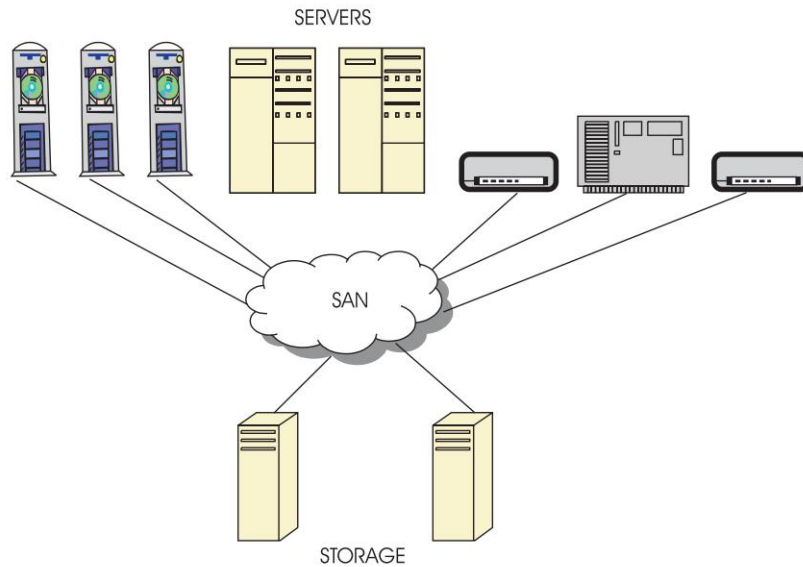
Each of these businesses relies on one or more complex technology-based solutions as given in Table 2.2.

Table 2.2 *Improving Business through Technology*

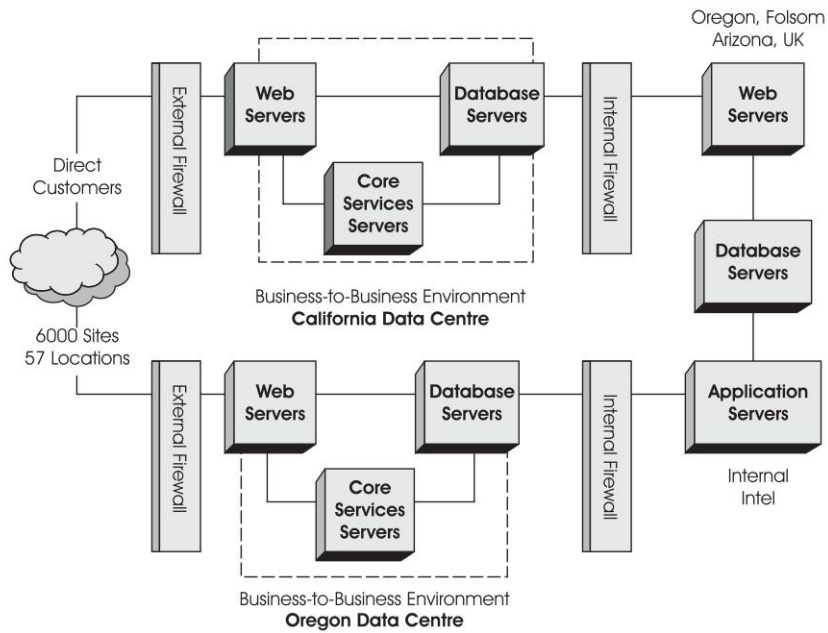
<i>Process improvement</i>	<i>Technology solution</i>
Substituting information for inventory	Enterprise Resource Planning (ERP) databases, data warehouses, business intelligence, supply chain management
Secure collaboration with business partners	SSL web servers, directory services, secure e-mail, virtual, private, networks (VPNs), B2B e-commerce
Enhanced customer service via quicker response and new services	Customer relationship management (CRM), e-commerce, online sales and support

It was in 1997 that Intel deployed its own Pentium Pro systems as servers on which the first B2B applications were launched. From a mere 5-server data centre, Intel's e-Business set-up grew to over 850 servers in the year 2000. It comprised a complex environment supporting customer-side B2B, supplier-side business-to-channel (B2B), and other special business programs. These environments continue to grow. New types of applications are constantly being developed and deployed. These new applications and capabilities require new features and infrastructure that, in turn, increase the complexity of the environment. Intel is constantly looking for ways to increase scalability and flexibility—in fact, reliability, availability and scalability (RAS) of platforms is the running theme in keeping e-business on track. It implemented networked storage solutions in the form of Storage Area Networks (SANs) to provide scalable alternatives by consolidating storage for many servers into a storage utility. Networked storage allows processing and storage resources to scale independently.

Intel operates two data centres in Oregon and California to run its e-Business. These centres support the high levels of performance and availability that are essential for online business.



➤ **Fig. 2.1** *SAN model for storage where processing and storage scale independently*



➤ **Fig. 2.2** *Intel's e-business environment*

The key elements of Intel's e-Business infrastructure are:

- A multi-tier server architecture
- A scalable storage infrastructure
- Flexible integration with core business systems
- Proactive management
- A scalable, redundant and response network infrastructure
- A comprehensive e-Business roadmap

In 2001, Intel announced the first e-marketplace for its 10,000-odd product dealers to enable them to offer more cost-efficient and complete PC and server solutions. The Intel Business Advantage Portal, a B2B e-marketplace, brought together Intel's dealers with third party suppliers, providing dealers the opportunity to earn rebates and commissions on PC products and e-business related services. This was done with a view to address the changing demands on dealers such as declining margins and lack of resources to offer total solutions to their customers. This initiative resulted in product dealers becoming more profitable and gave them greater flexibility on pricing through rebates and commission on third party products, such as software, hardware and e-commerce services. Suppliers had the opportunity to increase their customer base by working with Intel product dealers through this portal. The Intel e-Business network expanded to include thousands of computer companies, resellers, service providers, web consultants, and software vendors. Through such alliances, Intel continues to help companies take advantage of the new business opportunities emerging in e-Business.

2.6.2 Amazon

Amazon.com, a pure-play B2C dotcom website, opened as an online bookstore in July 1995.¹¹ Its mission was 'to use the Internet to transform book buying into the fastest, easiest, and most enjoyable shopping experience possible.' Jeff Bezos, CEO of Amazon.com, argued that retail stores required lot of real estate in prime locations to sell products to customers, and that the

cost of real estate was always going up. Technology, on the other hand, was always getting cheaper. He wanted to trade technology for real estate in his virtual bookstore. He chose books as the first product in his virtual store, because it is easier to offer a 'selection' to customers. Computers can be used to sort, search and organise them. While the largest physical bookstore stores under 200,000 titles, Amazon offers more than 3 million. As a product it was easier to ship since it is not a bulky item; it is of low value and hence carries very little risk. Trading technology for real estate made it possible for Amazon to sell books cheaper to customers. Moreover, it worked closely with publishers to help reduce the percentage of unsold/returned books from as high as 30 percent in physical bookstores to less than 3 percent. This enabled it to further reduce the sale price to its customers. Today, it can sell bestsellers at discounts as high as 30 percent.

Jeff Bezos' vision was to build the most customer-centric company, and to establish a virtual shop wherein a customer could buy anything. He characterised his customer-centric vision as consisting of three things: "The first is that customer-centric means figuring out what your customers want by asking them, then figuring out how to give it to them, and then giving it to them. That's the traditional meaning of customer-centric, and we're focused on it. The second is innovating on behalf of customers, figuring out what they don't know they want, and giving it to them. The third, meaning unique to the Internet, is the idea of personalization: re-decorating the store for each and every individual customer."

Amazon did translate this vision into reality by launching a 'Your Store' service in 2001. Today, the biggest bookstore is rapidly becoming the biggest anything store. The Amazon.com main website offers millions of books, CDs, DVDs, free electronic greeting cards, online auctions, games, videos, toys, tools, electronics, home furnishings, apparel, kitchenware, computers, health and beauty goods, prescription drugs, gourmet foods, and services including film processing. Expansion continues with

Amazon moving into uncharted territories in its quest to become the world's biggest store. The website, however, renews its customer commitment: "While our customer base and product offerings have grown considerably since our early days, we still maintain our founding commitment to customer satisfaction and the delivery of an educational and inspiring shopping experience."

The website offers an extensive catalogue of products, and a wide variety of other shopping services and partnership opportunities. The facilities it offers are as follows:

- Search for books, music, videos.
- Browse virtual aisles in hundreds of product categories.
- Get personalised recommendations based on prior purchases.
- Explore the world and additional items on Amazon's international sites.
- Become an Amazon.com Associate and earn money by selling products on one's own site.

Amazon was a pioneer in improving the shopping experience. Its innovations included one-click shopping, product review information, purchase circles (information on what is being read by other areas or groups), e-mail alerts, recommendations, wish list, and the page you made (recently viewed portions of the site).

Amazon found that it was very easy to leverage the trust of existing customers with any new product it launched. Technology enabled it to include new products on its website by using the same software that it uses for selling books. In the words of its CEO Bezos:

"On the Internet, companies are scale businesses, characterized by high fixed costs and relatively low variable costs. You can be two sizes: you can be big, or you can be small. It's very hard to be medium. A lot of medium-sized companies had the financing rug pulled out from under them before they could get big ... When we open a new category, it's basically the same software. We get to leverage the same customer base, our brand name, and

the infrastructure. It's very low-cost for us to open a new category, whereas to have a pure-play single-line store is very expensive. They'll end up spending much more on technology and other fixed costs than we will just because our earlier stores are already covering those costs.”¹⁰

As a result, Amazon is now the largest store on earth. And it is profitable. There was a time during 2000–01 when the Internet bubble had burst. The hype of Internet stores, and of pure-play dotcoms replacing brick-and-mortar stores was appearing as a bluff. Experts were talking about lack of appropriate business models for e-commerce. Logistics were being overlooked in the hype of pure-plays. Most dotcoms were going bust. In fact, statistics showed that 80–90 percent of Internet companies in the B2C segment disappeared in the US. But the Internet as an additional channel to reach out to customers was recognised by existing retail stores and other businesses. For example, Barnes & Noble, the largest bookstore, opened its website to sell to its customers on the Internet. It did quite well for some time. However, by the end of 2003, Amazon.com had successfully overtaken Barnes & Noble. The key was its successful expansion into many forms of retail, though it faced competition in every new product or service segment. For example, CDnow.com was there to sell CDs; and JC Penney and Circuit City—traditional retailers—moved online. However, leveraging on its customer base and its infrastructure, Amazon.com proved that the ideas created by the Internet bubble had a lot more substance, though many financial models certainly needed a major correction. Proper business models indeed had to be invented. It moved beyond retailing into partnering, auctions and services. It announced key partnerships with Target in September, 2001 for order fulfilment and customer care services. Several other partnerships included the Mervyns.com, MarshallFields.com, Giftcatalog.com websites. The idea of a big store—the biggest store on earth—on the Internet for customers to shop for all their needs was indeed workable.

Amazon also expanded in parallel into international markets. Even in July 1995, it had customers from 45 countries. By the

year 2000, 13.8 percent of its revenues came from over 150 countries. It opened distinct websites for its customers in Britain, Germany, France and Japan with content in local languages for customers. The company also became sensitive to local cultures. It also opened local offices in these countries to serve customers.

According to Nielsen's Net Ratings, Amazon.com had 31 million unique visitors in the month of November 2001, as compared to 27 million for Yahoo! and 26 million for eBay websites. It was ranked among the top ten fastest growing e-tailers. It posted its first quarterly profit of US\$ 5.8 million in the fourth quarter of 2001—the total sales in the year were US\$ 3.1 billion. With sales of US\$ 1.46 billion in the third quarter of 2004, it was expected to have total sales of US\$ 6.9 billion in the year 2004, with an operating income of about US\$ 500 million. This is expected to grow. In the year 2005, the sales is expected to go to US\$ 8 billion, and the operating income to about US \$ 600 million.

There have been other success stories too in the B2C segment of e-commerce. Today, Google and Yahoo services dominate online advertising business. Both of them are positioning themselves as powerful e-commerce platforms and important providers of general purpose technology services. They are not just search engine market leaders anymore. (Very soon in that segment, they may have reasonable competition from others like Microsoft.) Expedia maintains a healthy lead over the airline industry joint venture Orbitz. Kazaa.com and Apple's iTunes have nearly eliminated the offerings of many music industry giants. PayPal and eBay control the Internet funds transfer business. In other industries such as news, banking, investing and travel, several pre-Internet firms are also online leaders. For example, Dell (computers), Cisco (networking products), and Wal-Mart (retail) are also very successful. Intel has been discussed as a case here.

In more and more sectors, the dotcoms are emerging as profitable businesses. No longer are any questions being asked about their survival. Perhaps the right business models for B2C

have been discovered, and continue to be found. Pure-play dotcoms as well as existing companies with the web as another channel to reach out to customers are turning the corner. Do we see the future? Well, Amazon, Google, and Yahoo! have made great progress towards becoming broad-based Internet-wide resources. Like operating systems and databases before them, can they be used in a manner that creates new forms of value in ever expanding ways? The idea of web services is on the right course, and will perhaps reach its destination the way pure IT companies like Microsoft, Oracle and IBM have done in delivering IT services to customers.

2.6.3 eBay

The eBay website proclaims that “eBay is the world’s Online marketplace, enabling trade on a local, national and international basis. With a diverse and passionate community of individual and small businesses, eBay offers an online platform where millions of items are traded each day.”¹² eBay enables a visitor to the site to find, buy, and pay for an item by bidding as if he were participating in an auction. In order to find an item, a visitor can either enter the desired name, or browse through the categories of items provided under the first step ‘Find’. Thirty two categories, from Antiques to Video Games are listed alphabetically much like alphabetic listings in the classifieds sections of newspapers. For example, when he clicks on the category of ‘Books’, a visitor is taken to a page with further classifications running into several hundreds with special attributes like hard cover or paperback, first or later editions, publication year, used or new, quality of book, textbook, children or teenage use, subject matter and so on. Users have access to lively discussions on booksellers; they can join the Book Readers Discussion Board. The online marketplace thus provides a unique shopping experience. Consumers are bidding for items put on sale by other consumers in this most frequently used C2C website ebay.com. It has made auctions, bidding and

shopping fun-filled activities. Small businesses also use this e-marketplace to sell their items.

By the middle of 2001, Nielsen Net Ratings found that about 28 percent of North American online consumers had participated in online auctions. These participants spent an average of more than two hours a week at auction sites. eBay was launched in September 1995¹³ by an entrepreneur, Pierre Omidyar who was looking for a way to create a fair and efficient market on the Internet in the form of an auction. It was launched as AuctionWeb, and rechristened eBay in September 1997. People were initially trading almost exclusively in collectibles like Beanie Babies and coins. eBay charged a fee for transactions completed through C2C auctions. It was profitable from day one. People closed deals, and arranged for shipping of items to one another. eBay had no logistics to arrange for. The site offered people the opportunity to meet other people. They enjoyed that more than selling and buying things.

Eight years after its initial launch, eBay had 95 million registered users and listed almost a billion items a year in over 45,000 product categories. Of those, ten product categories delivered worldwide trading volumes in excess of a billion dollar each. Today, auctions account for nearly 18–20 percent of online retail. In the year 2003, a total of US\$ 24 billion worth goods were traded on eBay.

Organising data into categories, and enabling users to select what they need, just like what Amazon offered in the case of books, was an important element of eBay's strategy. It offered newspaper classifieds with the added advantage of non-linear search. Prospective buyers were presented a platform to interact with sellers, bid for items they were interested in, close the auction deals, arrange person-to-person meetings for exchange of goods traded, settle payments. The cycle of interface underwent improvements. For example, payments were enabled through PayPal.

eBay turned out to be a direct competitor of newspapers. For releasing a newspaper advertisement, a seller has to compose it,

go to an office to deliver it, pay for it, and after publishing, he has to be available at his home to answer telephone calls of prospective buyers. He has to provide detailed description of the product to callers each time. A small fraction would turn up for inspection of the item at the seller's home. All advertisement are prepaid with prices varying on the basis of reach and product category. Newspapers were the de facto C2C marketplace due to their brand name and local presence before the advent of the Internet. A study in the US showed that in 1998–99, classified advertising revenues of all newspapers were of the order of US\$ 16.6 billion in 2001. This figure declined to US\$ 15.8 billion in the year 2003. This was attributed to the growth in online auctions. This was fuelled by the replacement of offline activities as well as by new transactions. eBay enabled sellers to post attributes of items on sale, the expected price, and their choice of how potential buyers could contact them. The medium of e-mail as a response meant that a seller did not have to be glued to his telephone as was the case after placing an advertisement in the classified sections of newspapers.

Users can search specific categories, sub-categories or the entire eBay database of listings by using keywords to describe their areas of interest. Detailed descriptions and images of items offered for sale, payment and shipping terms are invariably included in the listings. eBay encourages buyers and sellers to communicate directly by e-mail, and they have to close the transaction independently between themselves. eBay does not directly participate in the physical transaction nor in the payment. Sellers can choose English or Dutch auctions lasting three, five, seven or ten days. eBay charges sellers a listing fee and transaction fee. For example, in the year 2004, the listing fee payable by sellers varied from US\$ 0.30 to \$ 4.80. Special rates were applicable in some categories, for example, vehicles \$ 40, motor cycles \$ 30, and real estate, \$ 100–150. Transaction fee ranged as follows: 5.25 percent, of first \$25, 2.75 percent of \$ 25–\$ 1,000. eBay charged extra for some options, including reserve selling price for auction 1 to 2 dollars. The Home Page featured items charged at \$ 39.95 each, Featured Plus at \$ 19.95

each, Highlight at \$ 5, Bold at \$ 2, while the Buy-It-Now option was at \$ 1.

eBay opened a feedback forum from the very beginning. Following a successful auction, buyers and sellers were encouraged to leave feedback for one another. This was in the form of a 'positive', 'neutral', or 'negative' rating and a one-line summary to help prospective traders know the credentials of people they were dealing with. Transaction-related feedback could be left only by the buyer and the seller. It helped establish a degree of 'virtual trust'. eBay gradually became a trading channel for both new and established businesses. This included individuals for garage sales, hobbyists, small businesses, and even established companies like Sun Microsystems and IBM that used eBay as a clearance channel. Professional sellers were concerned about their feedback ratings. eBay created a PowerSeller program to encourage small businesses to use its trading platform: sellers with 98 percent positive feedback rating and monthly sales of \$ 2,000, \$ 10,000, or \$ 25,000 respectively were recognized as Bronze, Silver, or Gold PowerSellers, respectively, with the attendant benefits decided by eBay.

Starting as a marketplace for collectors of low-priced items like Beanie Babies and PEZ dispensers, eBay expanded into mainstream product categories such as computers, consumer electronics, jewellery and sports equipment. eBay's view of growth in a product category was based on the fact that products are listed by its members, which are split into multiple sub-categories as they become popular. As the number of transactions in a category grows, it evolves into a separate community of buyers and sellers with like interests. eBay has special marketing and business development activities to accelerate the development of the most active categories. Category managers are designated for introducing category-specific bulletin boards and chat rooms, and for integrating category-specific content to a liaison role with eBay's IT staff. As a result from a collectibles trading site, eBay has migrated to a mainstream retail platform. By 2003, there were ten categories that reached over US \$ 1

billion each in trading. The growth of eBay's automobile category is very striking. In 1999, eBay had about 18,000 vehicles listed each quarter including mostly collector and vintage cars that were hard to find in used car relationships. It decided to build this category, and acquired Kruse International, a respected brand in the auto collector market. By the end of 1999, it launched a specialised automobile site called 'eBay Automotive' that targeted both collectors and the used car buyer segment. The site grew rapidly, and by the year 2000, it became the dominant online automobile marketplace. It formed a strategic alliance with AutoTrader.com, which helped bring over five million monthly visitors to eBay searching over 1.5 million car listings, automotive-specific content, and access to AutoTrader's extensive dealer relationships. eBay Motors thus became the fastest growing category. It not only helped collectors buy vintage cars, but also assisted ordinary buyers looking for used cars at a reasonable price.

A similar direction was also taken by eBay in its main arena, namely auctions. It acquired Butterfield & Butterfield (B&B), the world's fourth largest bricks-and-mortar auction house in 1999. eBay was thus able to have access to high ticket items like fine art and high-end collectibles. It also had access to a network of 50 experts and authentication services for art and collectibles. B&B also supplied the inventory for eBay's newly created Great Collections site. It is worth noting that within a couple of months of this acquisition, Sotheby's Holdings, Inc.—one of the two biggest auction houses—forged a US\$ 45 million alliance with Amazon.com. Even the elitist auction thus went online. However, eBay failed to market high-end art online. It could not attract upscale buyers in large numbers. In January 2001, the Great Collections site was re-launched as eBay Premier, with eBay trying to address buyers' insecurities and fears by adding a system of online appraisals and an improved authenticity guarantee. eBay also rolled out Live Auctions technology, enabling online buyers to submit bids to auctions that took place offline. However, even this high-end market proved elusive. It was becoming clear that with high-end art, people like to see it

and touch it and basically get a look-and-feel, which they can't do online. In August 2002, eBay sold B&B back to a traditional auction house. It may be mentioned here that Sotheby's had a similar experience. It annulled its alliance with Amazon.com as early as October 2000.

In 1999, eBay had taken several other initiatives. It launched its 'Go Local' initiative with its first regional auction site—eBay Los Angeles. By the end of the year, it had launched 53 regional sites covering the 53 largest metropolitan areas in the US. It wanted to encourage the sale of items that were too bulky or expensive to ship, items that people preferred to inspect before purchasing, and items of local interest.

In the same year, eBay made a foray into international markets. It acquired Alando.de in Germany and launched sites in the UK and Australia. By January 2004, eBay was present in 28 international markets, and its international revenues accounted for a quarter of the total revenues. It employed different strategies to enter different countries. These included building a user community through internal efforts, leveraging an existing platform to expand a new, same language market, acquiring a company already present in the local market, or partnering with strong local companies. For example, in India, eBay acquired a successful online auction site, baazee.com.

Sellers and buyers meet through the eBay marketplace, and interact through it as also directly. They follow the auction or fixed price formats facilitated by the website. Payments are made by buyers and goods are received by them from sellers. Most items require small payments to be exchanged. Both buyers and sellers found it inconvenient to deal with money orders or cheques. PayPal, a micro-payment gateway for effecting such payments, became very popular with the trading community. It made C2C payments as easy as sending an e-mail. The service was offered free to the buyer, but sellers were required to pay a small fee to PayPal, that was comparable to credit card charge. PayPal spread rapidly. It linked the service to the bank accounts of buyers and sellers. eBay's own payment service, Billpoint,

with a similar fee structure did not succeed. Rather than being account-based, Billpoint operated as a master merchant, aggregating payments from small eBay sellers. Of the eBay auctions that offered electronic payments in the first quarter of 2002, 47 percent accepted PayPal only, 7 percent accepted Billpoint only, and 19 percent accepted both. In July 2002, eBay acquired PayPal for US\$ 1.5 billion in stock, integrated it with the eBay platform and offered it as the official mode of online payments on eBay.

There are other auction sites such as Yahoo! Auctions, Half.com, and Amazon.com. But eBay is the world's largest auctions C2C marketplace, just as Amazon.com is the world's biggest store.



2.7 E-Governance—Case Studies Leading the Transformation

Governments, with their procedures and processes that were created in response to the needs of governance of the society that was in the process of industrialisation over a century ago, are trying to re-invent themselves in tune with the needs of the information age. Old procedures have continued beyond their period of utility and have become a hindrance to the effective and timely delivery of services. They also contribute to the continuation and spread of corrupt practices. The “re-inventing government” goals include the following:

- Empower communities to solve their own problems by pushing ownership and control of public services out of the bureaucracy, into the community
- Open government services to competition among potential providers, public agencies, private firms, and NGOs
- Make service providers more responsive to their customers, particularly by giving customers a choice of competing providers

- Find ways, including IT tools by which government can communicate more effectively with their customers
- Give service providers the freedom to carry out their responsibilities as they see fit, but then hold them strictly accountable for the results
- Deregulate government internally, creating personnel, budget and procurement systems that are less rigid and rule-bound, in order to free employees from red tape and to unleash their initiatives
- Remove unnecessary bureaucratic levels and flatten hierarchies
- Use market rather than administrative mechanisms to solve societal problems.

The result of this movement has been the emergence of electronic government, as it is called in the USA, Government online as known in Australia, and Information Age Government under the modernising government programme of the British government. The modern age government considers people not only as citizens but also as consumers. Their right to information is considered fundamental. Transparency in governance and the delivery of services electronically to citizens are at the heart of electronic government or government online. Electronic government subsumes all the activities such as citizen services, re-engineering with IT, electronic procurement, electronic filing of returns, payment of fees for services to the government, and so on. It is, in fact, a fundamental transformation of government and governance at an unprecedented scale. An important element of e-governance is a citizen's view of the government. He does not care which department or multiple departments are involved in servicing his request. To him, it is one government. Integrated services that break down the barriers of government structure and jurisdiction, cut across multiple departments and meet the real needs of consumers, be they individuals or businesses. A seamless national approach in integrating the governments at the federal, state and local levels characterises the electronic government in delivering one-stop government services.

The term e-Government was invented in 1995. In a survey carried out by Andersen Consulting, the electronic availability of 157 government services was tested, and countries were ranked according to the ratio of services available interactively online. The results published on May 18, 2000 ranked the US, Singapore and Australia as the top three, in this order, e-governments in action. Canada and France were ranked fourth and fifth respectively in this international survey¹⁴. The survey ranks online services in three orders of sophistication:

- Publish
- Interact
- Transact

At the first level, i.e. publish, the e-government simply provides online information. At the next level of sophistication, websites allow interaction, i.e. citizens can download forms, fill them up and lodge them back with the websites for further action. In the transaction phase, a citizen can pay appropriate fees for services through an electronic payment gateway, thereby completing the transaction electronically.

The typical first-generation government websites of each agency for providing information have been superseded by the portal concept, such as the 'firstgov.gov'. A portal is a window to an array of web-based content. They are typically multi-functional, as they offer a variety of capabilities aggregated in one place. As regards e-government, portal refers to the main government website. So, the first step in building a portal approach is to inventory services across departments, and select the ones that are online candidates.

In an attempt to present best practices, we will describe the experiences of the following three countries: the US, the UK and Australia, as case studies.

2.7.1 The US Government

On June 24, 2000, the US President, in his first ever Internet address webcast to the nation unveiled new e-government

initiatives that build on the already successful e-governance programmes launched over the last few years.¹⁵ These include the following:

- Citizens will be able to search all online resources offered by the federal government from a single website called “firstgov.gov”.
- Citizens, small businesses and community groups will have one-stop access to grants and procurement opportunities.
- Citizens will be encouraged to suggest new ideas for advancing e-government.

There were over 20,000 government websites at that time which provided access to government services. Some of the popular ones include the following:

- Department of Health and Human Service’s Healthfinder service provides tips on choosing a health plan, a doctor, a course of treatment, information on different illnesses, medical resources, health research, etc.
- Department of Education’s new Gateway to Educational Materials enables students, teachers and parents to access lessons and educational material on any topic.
- Small Business Administration has a website that counsels and advises people interested in starting their own businesses.
- The FedStats website provides government statistics on all 40 federal government statistical programmes.
- The Social Security Administration website helps citizens plan retirement benefits by calculating the estimated social security benefits for an individual.
- Agencies from across the Federal Government have joined hands to provide federal resources for academic excellence.
- Online trading advice for investing wisely and avoiding fraud is provided by the Securities and Exchange Commission.
- One can find a fuel-efficient car with help from the Department of Energy and the Environmental Protection Agency.

- Learn how one can pay back student loans and volunteer in one's community through the Corporation for National Service.

Studies in the US have established the business case for moving citizen services from 'standing in line' to online. Depending on the service, the population required to use that service, and other variables, governments are saving up to 70 percent by moving services online as compared to the cost of providing the same services over the counter¹⁶.

The process of delivering services has revealed that not all government operations consist of one simple form and one payment. Many government services require non-linear, complex collaboration among employees across departments. These operations can be performed by the employees on the same technology infrastructure built for citizen services through an intranet. Through intranet technologies, employees as well as external authorised members can share information and collaborate across the boundaries of their work communities. E-Government boils down to developing 'killer capabilities' and integrating strategies to leverage the power of the Internet.

The US government is also encouraging the creation of communities to bring the people together on local issues. This is based on the realisation that people are not just citizens; they are also parents, volunteers, neighbours, business owners, employees, consumers, students, sport enthusiasts, and so on. The same infrastructure as for e-government can be used for this too.

Finally, the government is leading the movement to build the confidence of citizens in electronic governance. The US has in position a government-wide public key infrastructure (PKI). It already has 30 production uses of PKI, uses that have moved into full production after a pilot period. These include the PKI systems at NASA, the Department of Commerce, the Federal Aviation Administration and the Federal Deposit Insurance Corporation. The overall US Federal Government approach is

set out in a document called 'Access With Trust'. It outlines a plan to issue free digital certificates to the public through the Access Certificates for Electronic Services (ACES) initiative. These certificates will allow them to do business transactions with the government.

2.7.2 The UK Government

The British Prime Minister views modernising government as a vital part of his programme of the renewal of Britain. In his presentation of the Modernising Government Programme to the Parliament in March 1999, the Prime Minister said in his Foreword, "... in line with the Government's overall modernisation programme, in line with our policy of investment for reform, it is modernisation for a purpose: modernising government to get better government—for a better Britain". The document recognises that modernising government is a long-term programme, and it sets a road map for the future.¹⁷ It sets a challenge to modernise government, and to create better government to improve the lives of people. The British Government has established a target of all dealings with government being deliverable electronically by 2008.

The government has committed the following:

- Policy making for delivering meaningful outcomes, incorporating best practices
- Responsive public services delivered to citizens to fulfil their needs, and not as per the convenience of service providers
- Quality public services—efficient, high quality delivery of services
- Information Age Government: use the latest technology; and, develop an IT strategy for government which will establish a cross-government co-ordination machinery and frameworks on such issues as the use of digital signatures, and websites and call centres
- Effective use of public service.

The central government is planning services that reflect business needs, and services that reflect real lives. These include national, citizen-focused programmes, group-focused programmes, as also area-based programmes designed to tackle the problems of a particular locality. One-stop shop services are planned in areas such as veterans' advice, advice to lone parents on income support, social support to low income units, and so on.

There is a plan to devise a corporate IT strategy for the Government. Electronic services offered to citizens and businesses include filing of income tax returns, health services, access to educational resources through the National Grid for learning, social security services, establishment of a University for industry to provide lifelong learning, services to post office customers, electronic public records, and so on.

As per the intermediate milestone, citizens are electronically able to:

- Book driving and theory tests
- Look for work and be matched to jobs
- Submit self-assessment tax returns
- Get information advice about benefits
- Use the National Grid for Learning
- Apply for training loans and student support.

Likewise, businesses are electronically able to:

- Complete VAT registration and make VAT returns
- File returns at Companies House
- Apply for regional support grants
- Receive payments from government for the supply of goods and services.

The government regularly publishes a range of new frameworks across government to cover data standards, digital signatures, call centres, smartcards, digital TV, and websites.

2.7.3 The Australian Government

The Australian government released its strategy paper titled *Government Online* in April 2000. It believes that the Government has a role in providing people with confidence in, and understanding of, the online environment, and that this would be reflected in how well it makes the online transition. The government resolved to adopt online technologies to provide better services and improve its own business practices.¹⁸ It made the following specific commitments:

- Deliver all appropriate services electronically on the Internet by 2001
- Establish a Government Information Centre through the Office for Government Online as a main point of access to information about government services
- Establish electronic payment as the normal means for government payments by 2000
- Establish a government-wide intranet for secure online communication.

More than 400 online service delivery initiatives have been planned by various government agencies. Services delivered through the Internet include:

- Client-service information and support
- Procurement
- Payment to suppliers
- Receipt of revenue
- Public relations
- Advertising.

Initiatives such as these require a common set of ‘enablers’ to be in place in order to facilitate their development and their use. Citizens have to be assured that online information and transactions are private and secure and, where necessary, the identity of the counter-party is authenticated. It turns out that the infrastructure required for authentication, privacy and security is the same as that for electronic commerce. Digital

signatures, certification authorities, and Public Key Infrastructure are all the required enablers for Government Online.



References

1. Special Supplement on E-Commerce, *The Economist*, May 15, 2004—A Perfect Market by Paul Markillie.
2. *Emerging Digital Economy II*, Department of Commerce, US Government, June 1999.
3. Forrester Research, Ipos-Reid, 2003 quoted in ‘E-Commerce Growth Statistics’ at http://www.seotechnologies.com/Internet_statistics/ecommerce.
4. <http://www.isc.org>.
5. Data for December, 2003 published on September 16, 2004 at URL www.itu.int.
6. Intel’s e-Business Center White Paper, on the Intel website www.intel.com.
7. Intel Information Technology White Paper on e-business, value, business process transformation, on the Intel website www.intel.com.
8. Intel Itanium Architecture Accelerates e-Business, on the Intel website www.intel.com.
9. Evolution of Intel’s e-Business Data Centre Architecture from Yesterday to Tomorrow, *Intel Technology Journal* Q4, 2000, on the Intel Website www.intel.com.
10. *Amazon.com*—A Business History by Sandeep Krishnamurthy, University of Washington, September 27, 2002 (was to appear in *E-Commerce Management: Text and Cases*)
11. Amazon URL <http://www.amazon.com>.
12. ebay URL <http://www.ebay.com>.
13. ebay Case Study—”Going, Going, Gone!—Consumer Auctions” by Haim Mendelson, Graduate School of Business, Stanford University, March 2004.
14. Electronic Government International, May 26, 2000.

15. 'The Quest for Electronic Government: A Defining Vision' by Janet Caldw, Institute for Electronic Government, IBM Corporation, July 1999.
16. FirstGov URL *<http://www.firstgov.gov>*.
17. Directgov URL *<http://www.direct.gov.uk>*.
18. Australia Government Online Report, 2004.

PART

II

Electronic Communication

- PCs and Networking
- E-mail
- The Internet
- Intranets

PCs and Networking introduces basics of the tools and technologies required for Electronic Commerce. E-mail talks about the concepts of computer communications and electronic mail based on the OSI Reference Model of the ISO. Both X.400 and Internet mail are covered along with an overview of X.500 Directory Services. The Internet gives a brief history of the evolution of the Internet and the kind of services on the Internet today, along with the different connectivity options that are available. Internet technologies and Internet-2 are also briefly described. Intranets describes the concepts of intranets and the methods of implementing the same in an organisation.



Chapter 3

PCs and Networking



3.1 Computers

The basic tools essential for e-Commerce are computers and networks. The computers are either workstations of individual office workers, or servers wherein large databases and other information reside. It is the network that connects both categories of computers. According to Andrew S. Tanenbaum, a computer network is an *interconnected* collection of *autonomous* computers.¹ These computers, in the early days of their existence, were single machines housed centrally and were used to carry out all the data processing needs of an organisation. The terminals connected to them over communication links were simple dumb terminals, i.e. with no intelligence. It is the advent of the Personal Computer (PC) which has given a new meaning to the network, as well as to the concept of a server computer and a client computer. The clients and servers are connected as a network. With an increase in processing power and a decrease in costs, more and more powerful machines have moved to the desktops of users as PCs, and a new scenario has emerged in which the work in an organisation gets done with the help of a large number of separated but interconnected computers, i.e. a computer network.

The Operating System or OS is the most basic program within a computer. An OS manages the resources of the computer

system in a fair, efficient and secure way. Resources include memory (main as well as secondary), peripherals such as printers, Input-Output devices and the Central Processing Unit (CPU). The objective is to provide a suitable interface with the hardware, relieving the application programmers of low level control functions.

In the days of mainframe computers, each machine would have its own OS which would have come from the manufacturer. Some of the most common OS, that we have today are DOS (which has been phased away in most parts of the world), Windows (3.1/ 95/ 98/ 2000/ NT) and many flavours of Unix. The development of Unix originally began in AT&T Bell Labs in the late 1960s/ early 1970s. Their System Five, Release 4, popularly known as SVR4 was extensively used in the late 1980s. Meanwhile Sun Microsystems developed SunOS, which later came to be known as Solaris. UnixWare evolved from Novell, which bought Unix from AT&T. Apple has its own OS for its Macintosh series of computers.

The Disk Operating System or DOS was first released by IBM in August 1981 as PC-DOS. Microsoft's MS-DOS was also developed around the same time and soon MS-DOS became the standard OS shipped with IBM Personal Computers.

Development of the Windows OS was started by Microsoft in the early 1980s. The objective was to develop an easy-to-use graphical interface with drop-down menus, mouse support and multi-tasking. The versions moved from 1.0 to 2.0 until Windows 3.11, which appeared in April 1994, corrected some existing problems, mostly network-related, and was widely used. Windows 95 has also been in use, and in June 1998, Windows 98 was launched by Microsoft with the promise of ease of use through Internet integration, enhanced performance and reliability, and new entertainment capabilities.

Windows 98, Second Edition, incorporated Internet-related features with the Internet Explorer browser and the NetMeeting

Software which was designed for home computer users, Windows Me (Millennium Edition), was launched in 2000. Windows Me was the last Microsoft operating system to be based on the Windows 95 code base. All subsequent operating system products were to be based on the Windows NT and Windows 2000 kernel.

Windows 2000 Professional was designed to replace Windows 95, Windows 98, and Windows NT Workstation, with added major improvements in reliability, ease of use, Internet compatibility, and support for mobile computing.

Windows XP (experience) was launched in October 2000. While Windows XP Professional built on the foundation of Windows 2000 to improve reliability, security and performance, Windows XP Home Edition made frequently used features more accessible and was designed for home users.

The 64-bit edition of Windows XP was built for workstations using the Intel Itanium 64-bit processor for users who require large amounts of memory and high performance. The Windows XP Media Center Edition operating system was released in October 2002 for specialised media centre PCs while the Windows XP Tablet PC Edition was unveiled in November 2002.

The Windows 2000 server family was launched in February 2000. Windows 2000 Server was offered as an entry level application server, while Windows 2000 Advanced Server was designed to support business-critical applications. The Windows 2000 Datacenter Server was intended to deliver a high level of scalability and availability for highly demanding server applications.

Launched in April 2003, Windows Server 2003 promises to deliver significantly greater dependability, security, and scalability as compared to the earlier versions. Four versions are tailored to the varying needs of organisations: Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition, for mission-critical server workloads, and Windows Server 2003, Datacenter Edition, to support high levels of

scalability and reliability. For dedicated web serving and hosting applications, the Windows Server 2003, Web edition, is a single-purpose operating system for rapidly developing and deploying Web services and applications. The 64-bit versions of the Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, operating systems have been designed specifically for 64-bit Intel Itanium hardware, to support memory-intensive applications.

Although the desktop PC has become more and more powerful over the years, there are classes of databases that are best maintained in a central repository, due to requirements for sharing and protecting that information. Most PCs, which are placed on virtually all desktops of organisations, are used primarily for e-Mail, word processing, browsing and querying/ updating of databases.

The processing power of PCs has been progressing rapidly. Currently, PCs based on Intel's Pentium 4 processor, operates on clock speeds ranging from 2.6 GHz to 3.6 GHz, while the Intel Celeron processor delivers clock speeds upto 2.4 GHz. Mobile technology is being supported through Intels Centrino based on Pentium M processor delivering clock speeds ranging from 1.4 GHz to 1.7 GHz. The server segment is being addressed through Itanium 2 and Xeon Processor with clock speeds of 1.5 GHz and 2.8 GHz respectively.

However, with an increase in processing power, users are demanding and using advanced PC applications with features supporting image processing and digital video editing. These kinds of applications, in turn, demand larger and faster storage capacity. Removable drives are also used to provide for 'unlimited' storage capacity.



3.2 Networking

Business enterprises now have a number of computer systems dispersed in organisational units both within and outside

countries, depending on the business scenario. With the vast amount of information that is stored in these machines, decision making in today's fiercely competitive world depends entirely on access to the right kind of information at the right time. This entails the interconnection of computing resources, both at the intraorganisation and interorganisation levels.

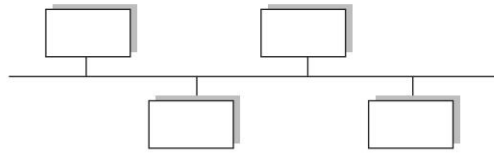
With increase in resources and processing power, the need for optimum network performance to deliver enough throughput is crucial. Local Area Networks or LANs are computer networks which are owned by organisations or institutions and cover areas upto a few square kilometers. A Wide Area Network or WAN, on the other hand, covers a large geographical area, which could extend throughout a country or even the world. The intermediate network, which normally covers an area within city limits, is called a Metropolitan Area Network or MAN. LANs, WANs and MANs are differentiated from each other on the basis of their size, data transmission technology and their network topology. In this section, we cover the common network topologies and media for data transmission. The communication protocols are discussed in subsequent chapters. The satellite communication network is considered a little more in detail in view of its importance in developing countries such as India. Each organisation has to decide for itself the topology and media that should be used depending on circumstances and cost/performance criteria.

3.2.1 Network Topologies

There are different topologies in which computers can be connected to one another over networks. The various topologies that networks can be built around are discussed below.

Bus

The topology of the bus network is shown in Fig. 3.1. This topology is commonly used to build LANs. Every node connected on a bus network is allowed to receive every

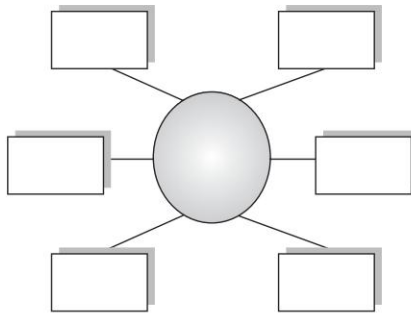


➞ **Fig. 3.1** *Example of a bus topology*

transmission on that network. The main problem faced in implementing this topology is the fact that only one communication channel exists to serve the entire network. As a result, if this channel fails, then the whole network will go out of operation.

Ring

The ring topology is another popular topology used for configuring networks. As shown in the Fig. 3.2, the data in a ring network flows in a circular fashion.



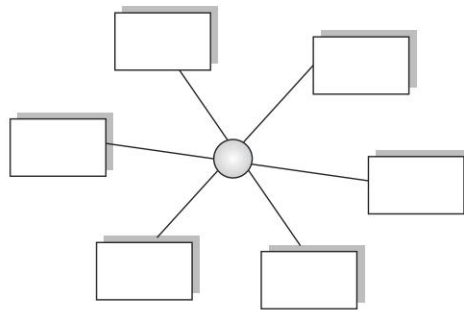
➞ **Fig. 3.2** *Ring network topology*

Mostly data flows in one direction, with one node receiving the transmission and relaying it to the next node in the ring. Here too, there is a single channel to connect the nodes. In the event of a channel failure between two nodes, the entire network goes down. Network suppliers sometimes develop ring networks with two rings so that in case of a single channel failure, the

network continues to function. This topology too is more commonly deployed in LANs.

Star

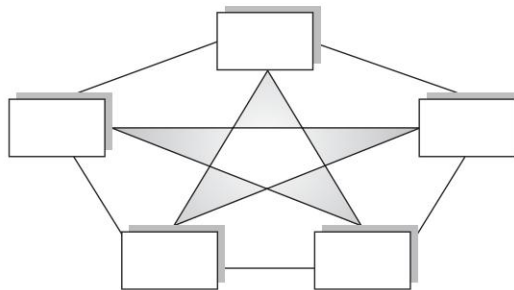
The topology of the star network normally used in WANs, is depicted in Fig. 3.3. At the centre of a star network is the hub through which all traffic is routed. As a result, in the event of the failure of the hub computer, the network too will fail!



➞ **Fig. 3.3** *Star topology*

Mesh

The mesh topology, which is shown in Fig. 3.4, has been used more frequently in recent years.

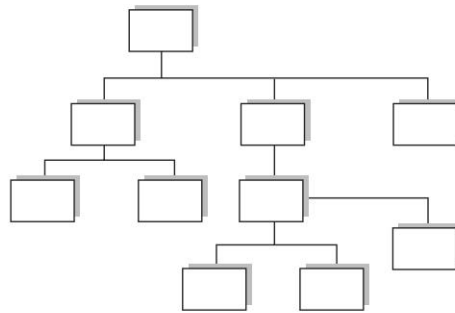


➞ **Fig. 3.4** *Mesh network topology*

Due to the multiple number of paths between nodes, the reliability of the network is improved. However, this improvement comes for a price, and mesh networks are much more expensive as compared to networks based on other topologies.

Tree

The tree, or a hierarchical network topology is one of the simpler and more common topologies found today. Figure 3.5 shows an example of a tree network.



➡ Fig. 3.5 Hierarchical network topology

Reliability problems can arise in this configuration due to the control exercised by the topmost node in the 'tree'. This topology too is used to set up WANs.

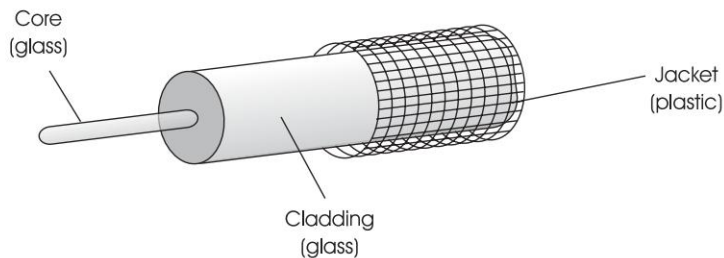


3.3 Communication Media

There are a large variety of communication media that are used to interconnect computers. One of the most common transmission media used is the *twisted pair* cable which consists of two insulated copper wires twisted around each other. The telephone network has been a major user of this kind of cable.

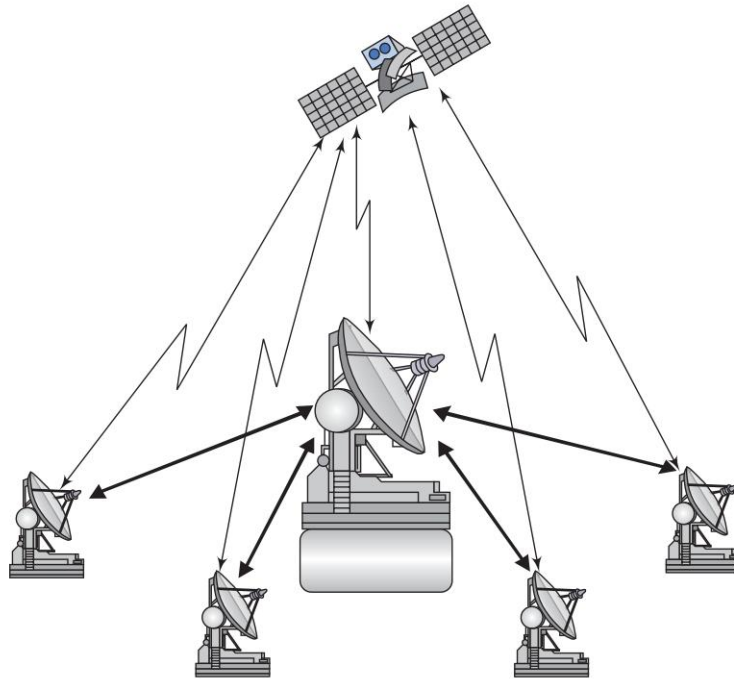
Another very commonly used transmission media is the *co-axial* cable. Co-axial cables contain a very thick copper wire at the centre. This wire is surrounded by insulating material, which, in turn, is encased in a cylindrical conductor. The conductor is again wrapped in protective plastic. These cables are therefore able to provide higher bandwidth (1–2 Gbps on short distances) with superior noise immunity.

Optical Fibres are made from ultra-thin fibres of glass. Information is sent on optical fibres in the form of light pulses, which when detected, generate electric pulses. Fibre optics can be used for LANs as well as for long distance transmissions. While supporting much higher bandwidths than copper, it is also much more reliable, has relatively lower attenuation and is much more difficult to tap.



➞ **Fig. 3.6** *Optical fibre*

Satellite communication provides reliable data transmission over a network of a large number of geographically distributed sites. Not only textual data, but images, voice and video are also transmitted over satellite networks. An essentially broadcast medium, communication can be achieved in two ways—either directly between end-users, or via a central or master station, which relays the contents of the communication to the destination. Satellite communication has been used in sectors such as television broadcasting and public telecommunications. Transmission costs depend on the network capacity and bandwidth—the distance between sending and receiving centres



➡ Fig. 3.7 *A model of satellite communication*

is immaterial in satellite communications. The reliability of satellite communications is reflected in reported network availability rates above 99.5 percent and Bit Error Rates of 10^{-7} , i.e. only one bit is expected to be in error in every 1,00,00,000 bits transmitted.

Satellites used for communications are almost exclusively in the geostationary orbit, located at 36,000 km above the equator. Satellites are launched and operated by organisations like Intelsat, which offer data communication speeds ranging from 1200 bps (bits per second) to several Mbps. The former are in the C-band which operates at lower frequencies, while high data rates are possible at very high frequencies in the gigahertz (GHz) range in what is known as the Ku-band. In between, the extended C-band offers data communication at 64 Kbps or higher rates. Regional and national satellites have also been launched.

The Indian satellites are known as INSAT. They enable communication in C-band, extended C-band and the Ku-band.

3.3.1 VSAT or Very Small Aperture Terminal

This is an end-user equipment used to receive and send data, images, voice and video over the satellite network. With a typical antenna size of 1.2 to 2.4 metres, a VSAT gives full access to a network which may comprise hundreds or even thousands of nodes. Such a network would be extremely expensive to use if dedicated lines, whether terrestrial or satellite, were to be used. The interactive nature of a VSAT allows two-way communication from remote locations in the same manner as the terrestrial telephone network. VSATs are more reliable than normal leased lines as there is no question of digging or damage to the cables.

There are frequency bands for all forms of radio spectrum usage in satellite communications. In general, fixed, commercial VSAT systems use satellite transponders operating at C-band (uplink 6 GHz and downlink 4 GHz) or Ku-band (uplink 14 GHz and downlink 11 or 12 GHz). The reliability of C-band used for low speed communications is well established. Signals on the high-speed Ku-band are susceptible to rain attenuation. However, equipment is available to automatically make adjustments by using stronger signals and/ or larger dishes.

VSATs can be used by financial institutions such as banks to consolidate branch transactions, process loans, conduct banking through Automated Teller Machines (ATMs) and operate Electronic Funds Transfer. VSATs have evolved from being a low-speed data communications medium to handling multimedia requirements for transmission of voice, image and video.

VSAT networks are generally set up in one of the following three configurations:

- **Point-to-point** networks provide two-way communications between two VSATs located at remote sites.

- **Star** networks provide multi-point communications between a Master Earth Station (MES) or 'hub' and VSATs located at multiple remote sites.
- **Mesh** networks provide direct communications between multiple VSATs located at different sites on the network.

In the Star configuration, communication is 'double-hop', i.e. all communications are routed through the MES or hub whereas, in the case of point-to-point and mesh networks 'single-hop' communications is achieved without the need for going via the hub station. These communication channels are not permanent and are established only for the duration of the call.

Antennas in mesh networks tend to be larger and more expensive, but higher data transmission speeds (1.5 Mbps and higher) can be achieved. On the other hand, star networks use very powerful master earth stations (MES) and smaller and relatively inexpensive VSAT stations. The low power signals generated by these VSATs are picked up by the MES and their strength is boosted for further transmission to the destination VSAT. Star networks have the advantage of maintaining effective control of the network from the hub.

3.3.2 Access Schemes

The network protocol employed by the VSAT facilitates efficient transfer of data over the satellite link, while the multiple access scheme allows many users to share the satellite transponder resource. The various access schemes in use are as follows:

- *Frequency Division Multiple Access* (FDMA)—users share the transponder by prior allocation of individual channels. Single Channel Per Carrier (SCPC) is an FDMA scheme in which the input data stream is used to modulate an RF (radio frequency) carrier and assign dedicated carrier frequency to each client.
- *Time Division Multiple Access* (TDMA)—each user is assigned the full bandwidth of the channel for a short period, which is then made available to another user for

the next period and so on. TDMA techniques are used by mesh networks.

- *Code Division Multiple Access (CDMA)*—transmitted signals are ‘spread’ over a bandwidth in excess of the data signal by combining with a code signal. The codes allow individual codes to be distinguished from each other and thereby allow sharing of a common frequency band.
- *Frequency Time Division Multiple Access (FTDMA)*—allows maximum utilisation of available bandwidth through a combination of FDMA and TDMA.

3.3.3 VSAT Network Components

A VSAT network comprises a Master Earth Station (MES), a number of remote VSAT earth stations and a host computer site.

The MES in a star network not only provides the communications link for the rest of the network but also performs address coding, transponder monitoring, monitoring and controlling of the traffic flow through the network and controlling access to the satellite. In addition to the dish of the antenna (normally between 5 to 9 metres in diameter), the necessary RF electronics, network switching system and a network control computer at the MES are present.

In order to set up a VSAT earth station, both indoor and outdoor equipment are required. Among the outdoor equipment, the RF terminal is very compact and is quite often attached to the antenna itself. The RF equipment is composed of an LNB (Low-Noise Block Converter) for receiving and an upconverter and SSPA (Solid-State Power Amplifier) for transmission.

Indoor VSAT equipment consists of one or more compact boxes of the size of a personal computer. It incorporates a modulator/ demodulator, a microprocessor for data communications and a microprocessor for providing protocol handling for interfacing to the terminal equipment.

VSAT systems have developed rapidly to support the introduction of new communication services which have become indispensable to the efficient operation of many corporations and businesses. VSATs also have a major role to play in Third World countries with virtually no terrestrial telecommunication infrastructure.

Two-way VSAT networks offering voice and data services, or even two-way video conferencing, to satisfy domestic and international requirements, are being widely used. Other typical VSAT applications include point-of-sale, credit authorisation, electronic payment systems, Electronic Data Interchange (EDI) and inventory control.



References

1. Tanenbaum, Andrew S., '*Computer Networks*' Fourth edition, 2003.



Chapter 4

E-Mail



4.1 Computer Communication Systems

In order to understand the issues that need to be addressed before getting two computer systems to ‘talk’ to one another, we look at a parallel in voice communication during a telephone conversation between two persons. For carrying out a telephone conversation, each of these persons should be able to access this service from a telephone. The originator of the call should know the telephone number of the person with whom the conversation is to be carried out. The connection has to be established by dialling the telephone number and a meaningful session will start only when the intended person becomes available at the telephone on the other end. For these persons to be able to understand each other, they should either speak the same language or employ the services of a translator who understands both languages. There is also an unwritten understanding between the two that, if any part of the conversation is missed, it would be repeated for the benefit of the listener. With the help of standardisation, the underlying telephone network assumes the responsibility of all the electrical and physical requirements for transporting the conversation being carried out over it.

Similar issues exist in getting computers to communicate with one another. The objective is to allow computers to communi-

cate with each other as 'open' systems, irrespective of their make, location or operating system. This requires the communicating entities to agree on the format of the data being exchanged as well as to lay down the procedures for controlling and regulating information flow and detecting and correcting errors that may creep in. Similarly, some standards have to be established for the physical/ electrical characteristics that enable information flow across communication networks. These are the 'protocols' that govern communication between computer systems connected in a computer network.



4.2 ISO's Open System Interconnection Model

The diverse requirements of users connected to networks range from supercomputer access to simple chat sessions across the network. This has necessitated the development of protocol specifications. Protocols take into account the different devices and communication media that could comprise a computer network.

The concept of providing protocol functions in layers within each communicating system was formalised by the International Standards Organisation(ISO) in the late 1970s. ISO's Open Systems Interconnection(OSI) Reference Model defined the protocols and interfaces needed to support an open system. The OSI Reference Model was developed to devise standards so that the concept of global communication across heterogeneous computer platforms could be achieved.

This model comprises seven layers in which each layer is supported by the layer below and provides support to the layer above. The number of layers was arrived at by optimising on the complexity of functions provided by each layer while ensuring ease of layer management. The seven layers are:

Layer 7

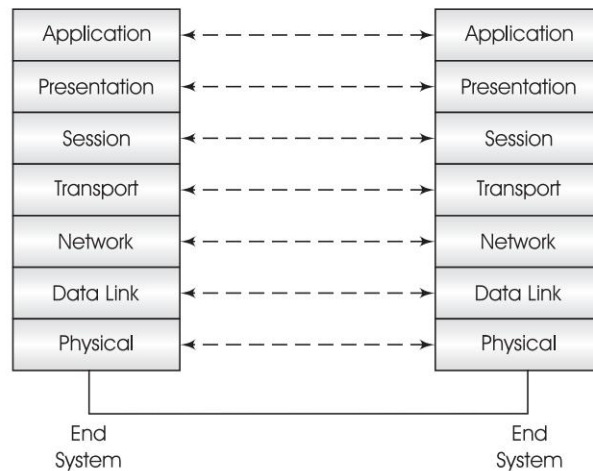
Application

Layer 6

Presentation

<i>Layer 5</i>	<i>Session</i>
<i>Layer 4</i>	<i>Transport</i>
<i>Layer 3</i>	<i>Network</i>
<i>Layer 2</i>	<i>Data Link</i>
<i>Layer 1</i>	<i>Physical</i>

Layers 1 through 3 are known as the lower layers and govern communication across a segment (from one system to the directly connected system or network node) of a communication network, whereas layers 4 through 7 are the higher layers which govern end-to-end (across all intermediate systems and network nodes) communication between the originating and destination systems (see Fig. 4.1). All seven layers must be implemented on originating and destination systems. The higher layers need not be implemented on systems which are intermediate network nodes.



➡ **Fig. 4.1** *The OSI reference model*

Services at each layer are provided through 'entities'. Similar entities in corresponding layers across systems are called 'peer entities'. These peer entities co-operate to provide network services across communicating systems. Layers also have

associated control messages which convey instructions between peer entities to facilitate this co-operation. A control message is known as a Protocol Data Unit (PDU). While logical communication is between peer layers/ entities, physically information passes through all the layers on each system. Requests for services from a higher layer to a lower layer are passed in Service Data Units (SDU). SDUs may contain the PDU that the requesting layer wants to convey to the corresponding layer at the other end. At each subsequent layer the PDUs are generated on the basis of the SDUs received and passed on to the layer below as an SDU again. The reverse process follows at the receiving end and each layer is presented with the PDU as intended by the corresponding layer on the sending system. The functions of each of these layers are described below.

Physical Layer

The interface between the computer system and the actual physical transmission medium is defined in this layer. This includes aspects such as physical connectors, voltage levels, etc. Some of the most common sources of interface standards are the Electronic Industries Association's RS-232 and Telecommunication Standardisation sectors V.24 and V.35.

Data Link Layer

Detection and correction of errors that may have crept in during data transmission across a single span/ segment of the communication network are performed in this layer. It includes procedures for establishing identities of communicating parties, data exchange and retransmission in case of errors. Early data link protocols included IBM's Binary Synchronous Communication and Synchronous Data Link Control (SDLC) and ISO's High-level Data Link Control (HDLC).

With the advent of LANs, this layer was split into two sub-layers—Media Access Control (MAC) for information flow and Logical Link Control (LLC) for error detection and correction.

IEEE's 804.3 defines the MAC standard and IEEE 804.2 defines the LLC standard for the widely popular Ethernet LAN.

Network Layer

This layer routes information between computer systems which may or may not be connected to the same network. The services at this layer are of two types:

- *Connectionless*—The packets of information traverse across different routes and may be delivered out of order at the destination in a datagram service.
- *Connection-oriented*—A specific route is always established before communication starts and all data flows on this pre-established route. This is also called a 'virtual circuit'.

One of the most widely known network layer protocols is the X.25 protocol for packet switching. In packet switching, the information is broken up into packets of fixed length and sent, along with addressing and other control information, maybe along separate routes. Re-assembling of the information is done at the destination.

Transport Layer

End-to-end reliable data transmission is provided by this layer, irrespective of the reliability of the underlying network. When a message is being relayed across several nodes before reaching its destination, the message could have been received and acknowledged by an intermediate node but lost before reaching the next node. This layer ensures delivery in such situations. ISO defines five classes of the Transport Protocol—Classes 0 through 4 depending on the grade of service provided by the underlying layers. The most commonly used Transport Protocol is Class 4 which operates over unreliable networks.

Session Layer

When information is being exchanged between two computer systems, the flow of information is managed by this layer.

Activities can be started, halted or re-started from previously established synchronisation points.

Presentation Layer

Internal representation of information differs widely among computer systems. This layer provides a common representation of information while it is being exchanged between two computer systems. However, this layer tends to be 'null' in many protocol implementations.

Application Layer

This layer provides OSI services such as File Transfer, Electronic Mail, Remote Log-in, Directory Access and Remote Job Entry to users, and is, therefore, different from other layers which do not directly interact with end-users.

Some of the services provided at the Application layer are Electronic Mail, File Transfer, Directory Services and Remote Login. While the File Transfer Protocol allows movement of computer files back and forth between the source and destination systems, Remote Login enables a user to use a remote computer system just as one would on a terminal which is placed and connected on the premises itself. However, both these assume the availability of the remote computer system, i.e. the remote system should be online for either of these services to be run.

The TCP/IP Stack

The Advanced Research Projects Agency (ARPA) of the US Government's Department of Defence set up the ARPANET in the late 1960s while exploring new communication technologies. The experimental version that was then established between four nodes blossomed by the mid-seventies into a network that stretched coast-to-coast in the United States.

As a result of continued research and development, the communication protocols used in the ARPANET formed the

basis of the development of the now widely known TCP/ IP (Transmission Control Protocol/ Internet Protocol) suite of protocols. The evolution and working of the Internet is covered in more detail in Chapter 5 on the Internet.

TCP/ IP is a protocol suite that consists of the Internet Protocol (IP) and the Transmission Control Protocol (TCP). The IP defines a unique address for each computer on the Internet, much like an address in the postal service. The TCP part of the Internet Protocol suite takes the information sent by a user, and divides it into smaller packets. The TCP numbers each packet so that the receipt can be verified and data can be put back in the proper order.

TCP/ IP allows the Internet to provide a reliable full duplex data and graphics transfer, and lately multimedia transfer too. It also offers the following networking functions to the Internet:

- Addressing
- Connection establishment
- Connection release
- Data flow control
- Routing and management
- Name control and translation
- Status translation and communication
- Fragmentation and reassembly
- Delivery

Co-ordinated by the Internet Architecture Board (IAB), the Internet utilises multiple alternate pathways to achieve an extremely high degree of resilience. The InterNIC, supported by the NSF, provides network information services to the networking community. Network Information Centre (NIC) provides Internet registration services including IP address allocation, domain name registration, and Autonomous System Number assignment. It also provides answers to questions related to IP-address and domain name registration. InterNIC's directory services include the Directory of directories, Directory

Services, and Database Services which store data and make it available to all Internet users.

The most important “traditional” services offered over TCP/IP are:

- *File Transfer* The file transfer protocol (FTP) allows a user on any computer to get files from another computer, or to send files to another computer. Security is handled by requiring the user to specify a user name and password for the other computer. The target system may only allow access to certain directories of files. Provisions are made for handling file transfer between machines with different character set, end of line conventions, etc. FTP can be run any time a file is to be accessed on another system. The file can then be downloaded to the requesting system or copied onto the target computer system.
- *Remote Login* The network terminal protocol (TELNET) allows a user to log in to any other computer on the network by specifying the computer to connect to. Once connected, all inputs are meant for the destination computer. When the telnet program exits, the user is back on the local computer.
- *Electronic Mail* Using the Simple Mail Transfer Protocol (SMTP), messages can be sent to users on other computers on the network.

FTP, Telnet and SMTP are the equivalent of OSI services of File Transfer, Remote Login, and e-mail respectively in the Application layer. There are no specific Presentation and Session layers.

Data to be sent on TCP/IP is split up into packets, each containing addressing information. These packets are then sent from one node of the network to another until the final destination is reached. At each node, routers decide the next node that a data packet has to be switched to. However, packets corresponding to the same data need not traverse the same route to the destination. At the destination, these are all sequenced

and collated together before being delivered. These and other Internet services are covered additionally in Chapter 5 on Internet.



4.3 Electronic Mail

Electronic mail is the means by which we can electronically get our messages across to one another as against the conventional mode of paper-based messaging. Messages can be prepared and sent reliably over communication networks from the desktop computer of the sender to be received at the desktop computer of the recipient. In addition to savings in time caused by not having to handle paper, the advantage of being able to send and receive mail as and when convenient is retained. E-mail has not only emerged as a reliable and convenient method of inter-personal messaging, but has also been deployed in changing work processes within organisations.

The main components of electronic mail systems are:

- *User Agent (UA)*, which allows the user to prepare an electronic mail
- *Message Transfer Agent (MTA)*, which is responsible for routing electronic messages to their destinations
- *Message Store (MS)*, where electronic mail can be stored until it is picked up by the recipient.

Early electronic mail systems were built around the first two; the concept of a Message Store was added later on. MTAs are interconnected to each other to collectively form a message transfer system. In order to send electronic mail, the sender does not have to ensure that the recipient's computer system is on. It can be sent and received at the convenience of the user.

The Consultative Committee on International Telephony and Telegraphy (CCITT) developed the X.400 series of standards recommendations for supporting cross-platform messaging. This was done on the basis of the OSI Reference Model developed by the International Standards Organisation.

Internet electronic mail based on the TCP/ IP protocol suite is the messaging standard SMTP that has been widely deployed. The specifications for TCP/ IP are developed by the Internet Engineering Task Force (IETF), which produces a set of documents, each called an RFC (Request for Comments). A number of these go through the standardisation process to emerge as Internet Standards. Like the IETF other bodies are also involved with protocols and technical policy. However, none of these bodies has anything to do with the running of the Internet.



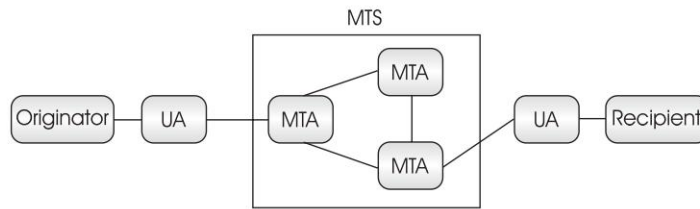
4.4 The X.400 Message Handling System

The formal development of the X.400 series of recommendations for Message Handling Systems (MHS) was done by the CCITT, an international standardisation body in the area of telecommunications. The purpose of the MHS is to enable users to exchange messages on a store-and-forward basis with the objective of enabling a standard message format so that the contents can be interpreted correctly in any environment. Messaging networks should be such that messages do not get lost or modified during transmission. In addition to these basic requirements, a set of service elements are also included which allow the configuration of different grades of service for end users.

Work on the development of such a messaging system had started in 1982 but it was only in 1984 that the first X.400 series of recommendations was published by the CCITT. Commercial implementations based on the 1984 X.400 standard began appearing in 1986. The 1988 version improved reliability and security and also introduced the message store.

4.4.1 X.400 MHS Functional Model

As depicted in Fig. 4.2, Message Transfer Agents (MTA), Message Stores (MS), User Agents (UA) and Access Units (AU)



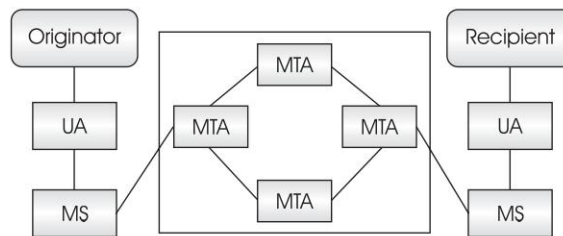
➤ **Fig. 4.2** X.400 (1984) message handling system

comprise the X.400 Message Handling System. The Message Transfer System (MTS) is formed by a collection of interconnected MTAs. A message submitted on behalf of one user, the originator, is conveyed by the MTS and subsequently delivered to the agents of one or more additional users, the recipients. Optionally, it is assisted in the storage of messages by the MS. The MTS comprises a number of MTAs which collectively perform the store-and-forward message transfer function.

Each X.400 user interfaces with the MTS through an UA. A user is assisted in the preparation, storage, and display of messages by the UA. UAs are used by message originators to prepare X.400 messages for submission to the MTA as well as for receiving X.400 messages from the MTA. The MTA, in turn, is responsible for ensuring message delivery to the recipient.

If the UA of the recipient is registered with the same MTA as that of the originator, then the message is delivered and a delivery notification is generated for being sent to the message originator. If, however, the recipient UA is not served by this MTA, then the MTA forwards the message to another MTA. The MTA to which the message has to be forwarded is decided on the basis of the routing tables that have already been incorporated into the forwarding MTA. This process of message relay from one MTA to another continues till the MTA on which the recipient's UA is registered has been reached. If, however, for whatever reason, the message cannot be delivered, a non-delivery notification is generated at the current MTA and the same is transmitted back to the originator of the message.

The concept of an MS was added in 1988. Figure 4.3 shows the linkages. This was done to alleviate the problem faced by an MTA in delivering a message if the UA was not online. With the introduction of the MS, UAs submit and receive messages to/ from the MS. The MTA also picks up messages from and delivers to the MS. The UA can then access the MS at any convenient time, and at the same time not hold up the MTA's delivery process.



➞ **Fig. 4.3** X.400 (1988) message handling system

Access Units (AU) were introduced to ensure that it was possible to interface existing messaging technologies. Access units link the MTS to communication systems of other kinds (e.g., postal systems). The teletex AU was defined in the 1984 X.400 series, while the AUs for telex and postal delivery were defined in 1988.

4.4.2 X.400 Protocols

A number of protocols are defined to support X.400 messaging across computers connected over communication networks. These are:

- *Message Transfer Protocol (P1)* is used by MTAs for switching and forwarding messages between interconnected MTAs.
- *Inter-personal Messaging Protocol (P2)* defines the standard for the format of X.400 messages between the originator and the recipient. A P2 message comprises a heading and

a body which could be made up of many parts. The heading contains details of the originator and recipient(s), message identification, and other elements which are listed in the service elements below. The actual information to be transmitted is sent in the body of the message.

- *Submission and Delivery Protocol (P3)* is used to interconnect the UA with the MTA.
- *Message Store Access Protocol (P7)* was not contained in 1984 X.400 (standards). P7 supports operations to access the Message Store and also allows submission of messages by the UA. P3 is then used in the interaction between MS and MTA.

4.4.3 X.400 MHS Service Elements

The service elements available in X.400 Message Handling Systems include the following:

- Delivery Notification Services, which are used to indicate the delivery or non-delivery of a message.
- Receipt Notification Services, which are used to indicate to the originator of a message whether or not a message has been read by the intended recipient(s).
- Specification of Recipients, as messages can be sent to single or multiple recipients.
- Miscellaneous Message Transfer Services such as submission and/ or delivery time stamp indication, Deferred Delivery after a specified date and time and its cancellation.
- Miscellaneous Inter-personal Messaging (IPM) Service Elements. These include, but are not limited to, provision for:
 - Primary, copy and blind copy recipients
 - Handling body parts such as text, fax, images, voice, teletex, videotex, etc.
 - Message forwarding
 - Importance indication
 - Expiry date indication

- Cross-referencing with other messages
 - Obsoleting indication
 - Sensitivity indication
 - Reply request indication (personal, private and company confidential)
 - Body part encryption indication
- Conversion-related Services, which allow for conversion of the contents of a message from one type to another.
 - Distribution List Services, which allow the originator to address a message to a distribution list. The first expansion of the list takes place at the MTA which serves one or more recipient UA(s).
 - Alternate Recipient Services. If a message cannot be delivered to the recipient, it can be delivered to the alternate recipient, if specified.
 - Physical Delivery Services, which allow the delivery of messages by physical means such as postal delivery, express mail, fax, etc.
 - Message Store Related Services such as auto-forwarding and listing, summarising, fetching and deleting of stored messages.
 - Security Services including secure access management, message content integrity, message/report origin authentication, confidentiality, message sequence integrity, proof and non-repudiation of submission, proof and non-repudiation of delivery and non-repudiation of origin.

4.4.4 X.400 Management Domains

Two different domains are defined for managing X.400 MHS. These are the *Private Management Domain (PRMD)* of organisations which operate private X.400 networks for their in-house communication requirements, and the *Administrative Management Domain (ADMD)* of organisations which are service providers providing communication services to clients. PRMDs and ADMDs operate independently. Two PRMDs can be directly

connected to one another or they may be connected through ADMDs. However, in either of these cases, agreements have to be reached and signed before message exchange can begin.

4.4.5 X.400 Addressing

An address in the X.400 scheme is referred to as an ORAddress (Originator-Recipient Address). The attributes of an X.400 ORAddress which are most visible to an user are:

- Country Name
- ADMD Name
- PRMD Name
- Organisation Name
- Organisation Unit 1
- Organisation Unit 2
- Organisation Unit 3
- Organisation Unit 4
- Personal Name
- Common Name
- Domain Defined Attribute (DDA)

If the recipient uses an AU, then the AU-related address can be included in the ORAddress.

The X.400 address of a user named Ram Kumar could therefore, for example, be specified as

C=IN;A=XYZMAIL400;O=XYZ;OU1=EDI;S=KUMAR;G=RAM,

where C stands for Country, A for ADMD, O for Organisation and OU1 for Organisation Unit 1. The personal name has been broken up into S for Surname and G for Given name.

The Domain Defined Attribute (DDA) is the only attribute of the ORAddress which is case-sensitive. This is used for specifying a non-X.400 recipient's address using a DDA type and a DDA value. For example, if mail is to be sent to an Internet user *ram@hub.nic.in*, the ORAddress could be

C=IN;A=XYZMAIL400;P=XYZGW;O=SMTP,

where the organisation is used to represent the SMTP gateway for sending RFC-822 Internet mail. (RFC-822 format is covered later in this chapter.) The additional attribute for defining the Internet domain would be

RFC-822=ram@hub.nic.in



4.5 Internet Addresses

The addressing scheme on the Internet uses the Internet Protocol Version 4 based on 32-bit address, consisting of four 8-bit groups (octets) joined by a period, each with a value of less than 256. For example, the address 194.80.1.4, 211.144.100.198, and 124.100.98.14 are typical IP addresses. The first two or three pieces of the address represent the network a system is on, called its subnet.

The right end of the address specifies the host on which the addressee would receive his e-mail. The Internet mail, like the postal envelope gets dispatched from an address such as 124.100.98.14 to an addressee, say 194.80.1.4.

There are three different types of addresses—classes A, B and C, specifying both the network and the host within the network.

Class A addresses begin with 1 to 126 and use only the first octet for the network number. The other three octets are available for the host number. Thus 24 bits are available for hosts. These numbers are used for large networks. However, there can therefore only be 126 of these very big networks.

Class B addresses use the first two octets for the network number. Thus network numbers are 128.1 through 191.254. The numbers 0 and 255 are not used, for reasons given below. Addresses beginning with 127 are also not used, because these are used by some systems for special purposes. The last two octets are available for host addresses, giving 16 bits of host address. This allows for 64516 computers, which should be enough for most organisations.

Class C addresses use three octets, in the range 194.1.1 to 223.254.254. These allow only 254 hosts on each network, but there can be a large number of these networks. Addresses above 223 were reserved for future use.

Many large organisations find it convenient to divide their network number into 'sub-nets'. This sub-net strategy requires special provisions in the network software.

In Internet addresses, 0 and 255 have special meanings. 0 is reserved for machines that don't know their addresses. In certain circumstances, it is possible for a machine not to know the number of the network it is on, or even its own host address. For example, 0.0.0.23 would be a machine that knew it was host number 23, but didn't know on what network. 255 is used for 'broadcast'. A broadcast is a message that every system on the network must see.

4.5.1 Internet Protocol Version 6

IP version 4, which has been around for twenty years, has been facing problems with the rapidly shrinking IP address space available. Since IP v4 comprises 32-bit addresses, there can be about 4,300,000,000 addresses. With the Internet expanding its reach to a plethora of devices, this is no longer sufficient for a world whose population is larger. Estimates indicate that the address space created by IP v4 will be exhausted by the year 2008, give or take three years!

The Internet Engineering Task Force (IETF) started work on the development of the next generation IP (IP ng) around 1992. A basic specification for IP v6 was developed in 1995.

The most significant contribution of the new IP v6 protocol was the availability of a much larger address space— 3.4×10^{38} —by virtue of the fact that the new addresses are 128 bits long.

With IP v4 widely implemented, one of the key design objectives in specifying IP v6 was to facilitate smooth transition

from IPv4 to IP v6 through support of embedded IP v4 addresses, pseudo-checksum rules, etc.

The other major changes effected as a result of the implementation of IP v6 relate to the following:

- Optimisation of header fields either by dropping some of them or making them optional
- Improved support for header options and extensions to provide more flexibility for introduction of new options in the future
- Labelling of packets to enable flow control requests of sender
- Support for authentication, data integrity and optionally, confidentiality.

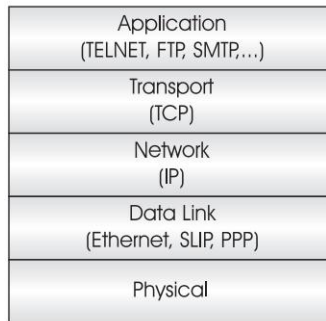
In order to ensure a seamless transition, the following three methods have been employed:

- Tunnelling—IP v6 packets are tunnelled through an IP v4 network.
- Dual stack—Both IP v4 and IP v6 stacks are run on hosts and routers.
- Translation—gateways translate packets between IP v4 and IP v6 and vice versa.

4.5.2 The Simple Mail Transfer Protocol

This protocol is used in TCP/ IP networks for transferring electronic mail messages between end-user computers and mail servers. SMTP is used only when both the mail sender and receiver are ready at the same time. If the destination PC is not connected (it dials in periodically to an ISP), then a post office must be used to temporarily store the mail. A post office protocol (POP) must then be used to retrieve the mail.

SMTP provides mechanisms for the transmission of mail, directly from the sending user's host to the receiving user's host when the two hosts are connected to the same transport service, or via one or more relay SMTP-servers when the source



➞ **Fig. 4.4** *The TCP/IP stack*

and destination hosts are not connected to the same transport service. They are equivalent to MTAs in the X.400 world.

In order to be able to provide this relay capability, the SMTP-server must be supplied with the name of the ultimate destination host as well as the destination mailbox name.

The main body of a mail message cannot contain control characters. For including them; they must first be converted into ASCII, often using *uuencode*—a separate program. The corresponding program at the other end is then *uudecode*, which restores the control characters.

4.5.3 Multipurpose Internet Mail Extension

Since binary data are not supported by Internet e-mail, the Multipurpose Internet Mail Extension (MIME) standard was developed to enable such data to be sent as attachments to e-mail messages. These attachments include files such as spreadsheets, word processing documents, images, etc. The file name containing multimedia information can be specified so that it is picked up. The extension in the file name indicates the type of the file. When the MIME message reaches the destination, which must support MIME, an icon is displayed to indicate the type of the MIME attachment. The corresponding application

on which the MIME attachment can be viewed can then be run for viewing the document/ attachment.

4.5.4 The Post Office Protocol

On certain types of smaller nodes on the Internet, it is often impractical to have an SMTP server and associated local mail delivery system kept resident and continuously running. It may also be difficult to keep a computer connected to an SMTP server for a long duration of time. Yet users want to be able to store and manage their mail on their own system, no matter how small the system is. This is made possible by using an User Agent (UA) to manage e-mail messaging on a client system.

The Post Office Protocol (POP) allows UAs to access hosts so that e-mail messages that have been received can be retrieved and outbound messages can be uploaded to the server for onward transmission. Extensive manipulation of mail is not allowed at the server and once the mail has been downloaded on the UA system, it is deleted from the SMTP server.

4.5.5 Internet Mail Access Protocol

This type of Internet mail server is an enhancement of services as obtained using POP. It allows connected stations to first view message headers and choose the mail messages they wish to receive. The others remain stored on the mail server.

The Internet Message Access Protocol (IMAP), allows a client to access and manipulate electronic mail messages on a server. It permits the manipulation of remote message folders, called 'mailboxes', in a way that is functionally equivalent to local mailboxes.

IMAP includes operations for creating, deleting and renaming mailboxes; checking for new messages; permanently removing messages; setting and clearing flags; searching; and selective fetching of message attributes, text, and portions thereof.

Messages are accessed by the use of numbers. These numbers are either message sequence numbers or unique identifiers.

4.5.6 Domain Name System

Internet addresses, as numbers, are difficult to remember. Humans are good at remembering names or mnemonics. The IP address has, therefore, been mapped into a name, which consists of the user's name and a domain, the group that the computer belongs to. The structure of computer address looks as follows:

User's e-mail address on a computer : *user@somewhere.domain*
Computer's name : *somewhere.domain*

The 'user' is generally the person's account name on the system. Computer's name *somewhere.domain* signifies name of the system or location, and the kind of the organisation. User also signifies that the person has only a partial access and can receive e-mail, and is not directly connected to the Internet. This kind of address is known as a Fully Qualified Domain Name (FQDN). Some of the geographic and organisational domains on the Internet are as follows:

gov	Government Agencies
mil	Military Site
edu	Educational Institutions
com	Commercial organisations
net	Sites that perform some administrative function for the Net
org	Organisation, Non-profit
us	United States
in	India
au	Australia

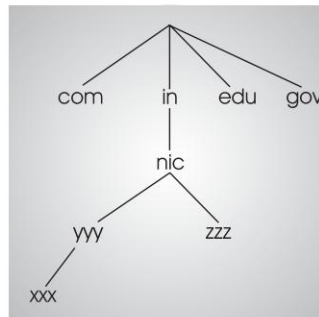
The computers on the Internet know one another through the **Domain Name Server (DNS)** database. While sending out an e-mail, the mail system resolves the address of the addressee

from the DNS, and sends it to the appropriate domain; the system that accepts the incoming mail routes it to the destination with the help of a router.

The DNS is the distributed hierarchical naming system for resources within the Internet community. A node on the DNS tree can be named by traversing the tree from itself to the root. At each node, the name is added and a period (‘.’) appended to it until the root is reached

In the Fig. 4.5, the domain name of the node xxx is, therefore, as given below:

xxx.yyy.nic.in



➡ **Fig. 4.5** *Part of a DNS tree*

Each node can have any number of child nodes but only one parent node. Child nodes must have different names to ensure an unique naming system.

In the 1980s, seven Generic Top Level Domains (gTLDs) (.com, .edu, .gov, .int, .mil, .net, and .org) were created. Domain names could be registered in three of these (.com, .net, and .org) without restriction; the other four were for limited purposes. Various discussions concerning additional gTLDs, led to the introduction of seven new gTLDs in 2001 and 2002. These are .biz, .info, .name, .pro, .aero, .coop, and .museum. Domains are registered for these domains as presented.

.com	Unrestricted (but intended for commercial registrants)
.edu	United States educational institutions
.gov	United States government
.int	Organisations established by international treaties between governments
.mil	United States military
.net	Unrestricted (but intended for network providers, etc.)
.org	Unrestricted (but intended for organisations that do not fit elsewhere)
.info	Unrestricted use
.pro	Accountants, lawyers, physicians, and other professionals
.biz	Businesses
.name	For registration by individuals
.aero	Air-transport industry
.coop	Co-operatives
.museum	Museums

4.5.7 RFC-822 Addressing

RFC-822 is the format of a user address when messages are addressed in the SMTP world. It follows the convention of being specified in two parts—local and domain—and is represented as

local@domain

For example, a user address could be

user_name@domain_name

The *user_name* could be an actual user ID on the system or it could be provided as *GivenName.Surname*, which would be suitably aliased to the actual destination of the message. The domain name, as described above, enables the determination of

the mail server in the organisation where the message is to be delivered.

Root Servers

Name servers accept requests from other name servers to convert domain names into IP addresses.

When a web browser is provided with a URL to be contacted, the browser contacts a name server to convert the domain name provided in the URL into its IP address. This name server is specified at the time of setting up the connections to the Internet.

The name server contacted may already have the corresponding IP address from an earlier interaction. Otherwise, it would locate the IP address by contacting one of the Root Name Servers. The root servers, in turn, know the IP addresses of all the name servers, which handle the top level domains such as .com, etc. A list of all root servers is available with all name servers. The name server contacts these root servers.

The root server returns the IP address of the name server handling the requested domain to the requesting name server. This process continues between name servers until the IP address is located and returned to the browser. Reliability is built into this system through redundancy of name servers at every level, so that if one fails, another can take over and handle the request or by name servers caching, for a limited time period, the IP addresses resolved so that they do not have to contact the root servers again for the same information. There are thirteen root servers located in different parts of the world.



4.6 E-mail Security

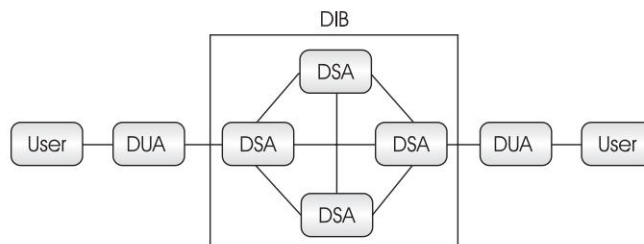
The security of e-mail messages essentially revolves around providing capability for encrypting and signing messages. Secure MIME(S/ MIME), integrates MIME with the Public Key Crypto System (PKCS) standard. The different types of cryptosystems are dealt with in Chapter 14, on Cyber Security.



4.7 X.500 Directory Services

The need for a common directory to keep track of all messaging addresses resulted in the development of the X.500 series of recommendations on Directory Services by the ISO/ CCITT. The first publication of these recommendations in 1988, was later re-published with modifications in 1993.

CCITT's X.500 recommendations specify the architecture and protocols to set up a distributed database system, which can be accessed by open systems over computer communication networks. The Functional Model of the Directory Service as laid down by the X.500 series of recommendations, comprises a series of Directory Systems Agents (DSAs) which are interconnected to form a Directory Information Base (DIB). DIB Services are provided to other DSAs or to users through Directory User Agents (DUAs).



➞ **Fig. 4.6** X.500 directory system

The Directory is implemented as a distributed database. The DSA is the core directory server. A single DSA will typically hold only a part of the data available in the total directory. The DUA is the client process that accesses information in the directory either as an user interface or embedded in another application. The protocol through which a DUA accesses one or more DSAs is the Directory Access Protocol (DAP), whereas the protocol that DSAs use to talk to each other is the Directory System Protocol (DSP).

The organisational model of a Directory Service provider comprises of Private Directory Management Domains (PRDMD) and Administrative Directory Management Domains (ADDMD), much in the same manner as in the case of X.400 Message Handling Services.

The DIB consists of a collection of objects which in turn consist of a collection of attributes. These objects are structured hierarchically in a Directory Information Tree(DIT). Each of these objects belong to one or more classes.

X.500 follows a hierarchical naming structure. An example name is as follows:

CN=Debjani Nag; O=CCA; C=IN.

This name represents the person with Common Name (CN) “Debjani Nag”, within the organisation (O) “CCA”, within country “IN”. The name components are typed (Common Name, Organisation, and Country in the example above). This is in contrast to other systems such as the domain naming scheme. Objects are represented as entries in an X.500 directory. These entries are given a type (or types), known as the object class, by use of an object class attribute. Typical object classes are people, organisations, and computers. Information within objects is held as a set of typed attributes. For example, there may be a ‘telephone number’ attribute with one or more values.

The operations to access and manage data in the X.500 directory are:

- read
- compare
- search
- add
- delete
- modify

X.500 evolved significantly since the original X.500(1988) version. This led to significant updates in the 1993 specification to include:

- Replication using Directory Information Shadowing Protocol (DISP).
- Access Control in view of data replication.
- Changes to the internal operations and management features.

4.7.1 Lightweight Directory Access Protocol (LDAP)

The goal of the original Lightweight Directory Access Protocol (LDAP) was to give simple lightweight access to an X.500 directory, to facilitate the development of X.500 DUAs and use of X.500 for a wide variety of applications.

Elements of the X.500 protocols were modified to produce the simpler protocol LDAP. In X.500, names and attributes have a complex encoding, whereas in LDAP, they are given a simple text string encoding. LDAP maps directly onto TCP/ IP and removes the need for a heavy amount of OSI protocol. Since LDAP has been designed to run over TCP/ IP, it is especially suited for the development of the Internet and intranet directory-based applications. Of course, these gains cost some functionality. LDAP's lack of security and signature features posed a problem for electronic commerce implementations. However, the newer versions hold the promise of authentication, encryption, integrity and replication. Its simple Application Programming Interface (API) facilitates easy implementation of directory enabled applications.

LDAP relies on X.500 for service definition and distributed operations. Because LDAP was defined as an access protocol to X.500 and not as a complete directory service, it was possible to specify LDAP very concisely. Also known as X.500 Lite, LDAP allows directory entries to be arranged in a hierarchical structure comprising the 'root' node at the top, followed by country information, entries for companies, states or national organisations. Under these come the entries for organisational units, such as branch offices and departments and finally individuals.



4.8 E-mail User Agent (UA)

E-mail user agents help the user in sending and receiving electronic mail. Some e-mail softwares continuously check for newly received e-mail in the background, automatically downloading it in case of new arrivals. Others need explicit instruction to check with the e-mail server for new messages. While this is being done and new messages, if any, are being downloaded, the user has to wait to perform other tasks.

Normally, on the main screen of any e-mail User Agent, there will be a column which displays all the folders belonging to the user. Folders are, like their manual equivalents, used to file copies of electronic mail sent/ received by the user. Some folders come pre-built within the e-mail client such as *In* where mail is received, *Out* where copies of e-mail messages that have been sent are stored and *Trash* for housing discarded messages. Other folders can be created for storing messages based on the personal preferences of the user.

On selecting a folder, the headers of all the messages that are stored in that folder are displayed in a split window. (Headers contain a line of information on each message such as the subject, sender identification, time of receipt and priority attached to the message.) The bottom half displays the contents of the particular message that has been selected in this folder. This is the standard three-pane-in-a-box window in which the folders, contents of a folder and the selected message can be viewed simultaneously.

The Tool Bars on the top of the screen are used for mailbox management. New folders can be created while other folders such as Trash can be emptied. When a message has been selected, the following buttons can be used:

- **Reply**—Automatically, the address of the sender from whom the mail has been received is picked up and presented in the *To* component of the new message preparation window that pops up. The subject is also picked

up from the received message and prefixed with *Re:* to generate the subject for the reply message.

- **Forward**—The user is presented a message window in which the *To* component has to be filled up to identify the recipient of the forwarded message. Any copy recipients can be included as well. An option is also provided for adding comments on the forwarded message. The original contents of the message being forwarded are preserved while the subject is re-generated by prefixing the subject of the received message with *Fwd:*
- **File in Folder**—This option is used for filing away e-mail messages into the desired folders.
- **Print**—The contents of the currently selected e-mail message can be printed using this option.
- **Security**—If messages are to be made more secure by incorporating confidentiality and authentication, this option is used. The use of digital signatures for authentication is covered in Chapter 14. However, use of this option requires prior configuration of the security parameters.
- **Delete**—This option can be used to delete the currently selected message in the open folder.

Most e-mail clients support the above capabilities. They may be named differently, but their functions essentially remain the same.

Following are some of the features to look out for when selecting an e-mail client (this is only an indicative list and not an exhaustive one).

General

- SMTP/ POP3/ IMAP4 protocols for submission and receipt of mail
- LDAP protocol for Directory Access
- Security features such as S/ MIME or PGP/ MIME
- Address Books.

E-mail Preparation

- Integrated Editor for message composition
- View HTML mail and preserve live URLs
- Display of message attachments
- Multiple attachments in single message.

E-mail Management

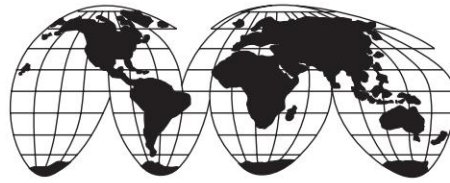
- Display headers and message text
- Display number of new or unread messages
- Icon for messages with attachments
- Support for aliases
- Message filtering based on subject, sender, message text.

Although all e-mail clients generally support combinations of the above features, only a few support all the important ones. Selecting the right e-mail client depends on the proposed use of the e-mail account. Business users would feel that security features are critical as well as the inclusion of Address Books and Directory Access. When used in the home, the more important features may be the ability to handle HTML documents with live URLs as well as to personalise e-mail messages.

Some of the most popular and widely used e-mail clients are:

- America Online
- CompuServe
- Eudora
- Lotus Mail
- Microsoft Outlook Express
- Netscape Messenger

Along with their commercial offers, many of these also offer freeware wherein somewhat stripped down versions of these e-mail clients are available in the public domain.



Chapter 5

The Internet



5.1 The Internet: A Brief Introduction

The Internet, a group of worldwide information highway and resources, is enabling the world to become truly an information society. Viewed as a prototype for the National Information Infrastructure (NII), its origins can be traced to an experimental network established with funding from the Advanced Research Project Agency (ARPA) of the US Department of Defence (DoD), to enable the scientists engaged on DoD projects to communicate with one another. Starting in 1965 with four sites in the US, it soon grew to ten widely dispersed sites including those in the UK and Norway. Electronic mail over the ARPAnet, as it was called, was a great success. The National Science Foundation (NSF) took over the academic community network project in the mid-1980s, after the defence traffic was moved away from the ARPAnet to MILNET. In 1987, the NSF created NSFnet.

Regional and corporate networks were permitted to connect to the NSFnet. Geographically contiguous chains were created by connecting networks to their nearest neighbours. Each chain was connected to a supercomputer centre. This enabled any computer on any network to communicate with any other network computer by using the store and forward techniques. It is the NSFnet which was later christened as the Internet.

The Internet has continued to grow ever since. The traffic growth, following the popular Internet mail service, led to the upgradation of the NSFnet backbone by IBM and MCI, and later they took over its management too. With this upgradation, the Internet moved to modern computers and faster links, such as T1 (1.544 Mbps) and T3 (44.7 Mbps). Today, the Internet has two types of backbones: NSFnet and Commercial Internet. The US Federal Government which owns the NSFnet forbids its commercial use. The commercial Internet, on the other hand, comprises several private backbones run by a number of Internet Service Providers (ISPs). The users have to pay for Internet services for access through these routes. One such private backbone is operated by Advanced Network and Services Inc. (ANS), owned by IBM, MCI, and Merit Inc.

It was only in 1991 that a set of small commercial networks created the Commercial Internet Exchange (CIX) for commercial use. Commercial collaboration, technical support by e-mail, pay-for-use databases which were forbidden on the NSFnet became possible on CIX. CIX gave a big boost to the growth of the Internet.

The Internet is neither run nor owned by anyone. Every organisation that is plugged into the Internet is responsible for its own computers. It is more or less self-regulated. Among its advantages are: no membership fees, no censorship, no government control. The prominent disadvantage is that when something goes wrong, there is no central control to ask for help. However, a number of Internet Technical Groups co-ordinate the Internet's basic workings. These are:

The Internet Engineering Task Force (IETF): The *IETF* co-ordinates the operation, management, and evolution of the Internet. It has a major role in the development of the Internet's communication protocols.

The Internet Research Task Force (IRTF): The *IRTF* is concerned with the long-term research problems and technical issues confronting the Internet.

The Internet Architecture Board (IAB): The IAB concerns itself with technical and policy issues involving the evolution of the Internet's architecture. IAB oversees the IETF and IRTF and ratifies major changes proposed by them. It performs the following functions:

- Reviewing Internet standards
- Managing the publication process of Request for comment documents
- Performing strategic planning for the Internet, identifying long-range problems and opportunities
- Acting as an international technical policy liaison and representative for the Internet community
- Resolving technical issues that cannot be treated within the IETF and IRTF framework.

There is yet another organisation, called The Internet Society which is considered as the 'Parent' of the IAB. It also does not run the Internet. But its members do work to keep it running smoothly. The charter of the Internet Society has the following goals:

- To facilitate and support the technical evolution of the Internet as a research and education infrastructure, and to stimulate the involvement of the scientific community, industry, government and others in the evolution of the Internet.
- To promote educational applications of Internet technology for the benefit of government, college and universities, industry, and the public at large.
- To provide a forum for exploration of new Internet applications, and to stimulate collaboration among organisations in their operational use of the global Internet.

The Internet Corporation for Assigned Names and Numbers (ICANN) was established in October 1998 for technical coordination on the Internet. A coalition of the technical, business, academic and user communities got together as ICANN for technical functions which were earlier being handled

by the Internet Assigned Numbers Authority (IANA) under contract to the Government of the United States. These functions include the assignment of:

- Internet domain names
- IP address numbers
- protocol parameter and port numbers

The operation of the Root Server system is also co-ordinated by ICANN.

Internet Service Providers have Network Entry Points (NEP) or Point-of-Presence (POP) through which users can get connected to the Internet. The user may be an individual wishing to connect only a PC, a small company with a system and a few terminals, an organisation or a campus with a LAN and several PCs and servers on it, or a corporate entity having its own network comprising a LAN and/ or a WAN. The ISPs are thus required to provide connections of various types and speeds. The Internet connection may thus be any of those depicted in Fig. 5.1.

The connections to the Internet fall in the following categories.

Dedicated Connection

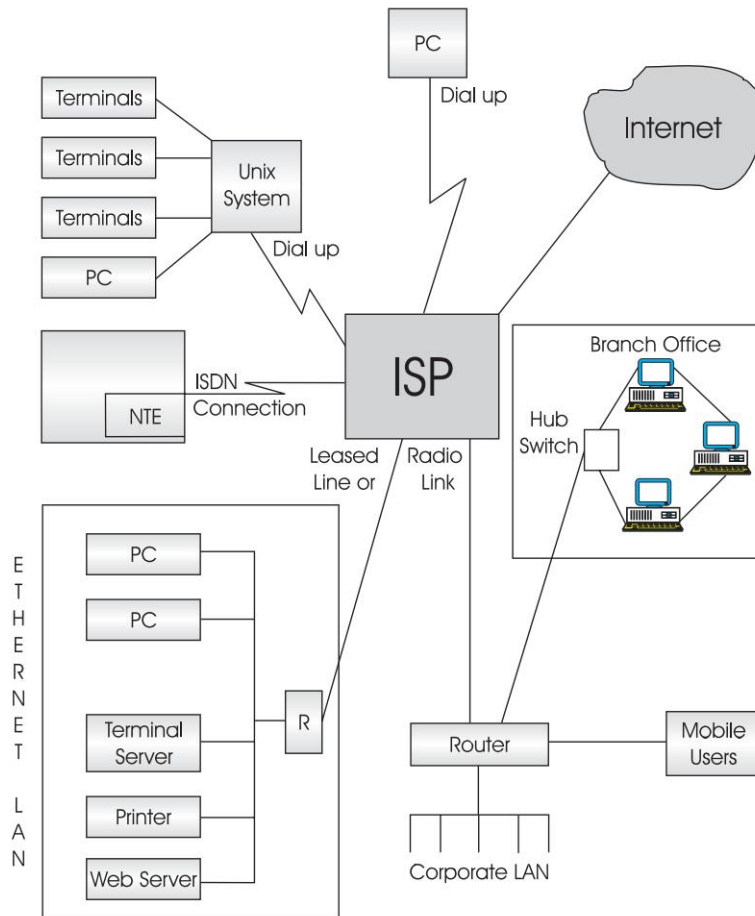
A leased telephone line at 56 Kbps or 64 Kbps (frame relay) or a T1 link at 1.544 Mbps connects a gateway computer or router/ bridge of a corporate LAN/ WAN to the router of an ISP. At the high end, even a T3 line may be possible for a dedicated connection.

On-demand Connection

This is more like a dedicated connection except that the user has to dial-up the ISP using a modem or ISDN.

Dial-up Shell Account

In this type of connection, a single user with a PC connects to the ISP's computer. The user has to manually download his



➞ **Fig. 5.1** *The Internet connectivity options*

data from the ISP's computer using a protocol such as X-Modem, Z-Modem (not widely used) or Kermit. ISP generally provides a direct Internet connection to the dial-up user, though it is not uncommon for very low cost service providers to give only a UUCP connection to the Internet.

Serial Line Internet Protocol (SLIP) or Point-to-Point (PPP) Account

The SLIP/PPP account is more like an on-demand type of a

connection for a single user PC. All the client applications can be run directly from the PC. The difference lies essentially in the inability of the user to run a server through this account; a facility which is available to an on-demand connection. This type of connection, therefore, cannot be used as a gateway to a LAN.

Part-time Polled Connection

This connection is based on the Unix-to-Unix Copy (UUCP) Protocol. A user organisation may dial an ISP at periodic intervals, and transfer its mail, etc. A single UUCP connection enables an organisation to serve several mail users, since it can, in turn, route messages to other systems on the organisation's network using store-and-forward messaging. However, interactive Internet client-server applications are not possible through UUCP.



5.2 Internet Communication Protocols

A communication protocol allows different kinds of computers using different operating systems to communicate with one another. It is essential for the Internet, since it is not made up of any single type of computer system; in fact, the greatest possible diversity of computer systems is to be found on the Internet. When ARPAnet grew large by the end of 1970s, its original set of standards and communication protocols could not support the further growth of the network. It switched to a new protocol called the TCP/ IP, and by 1983, all computers on the ARPAnet were using this protocol. A user connected on any network on the Internet can communicate with people or software located on any other network connected to the Internet using this common set of protocols, the TCP/ IP. Thus any computer that 'speaks' the language TCP/ IP can talk to any Internet machine. TCP/ IP is the protocol that underlies the Internet.

Historically, UNIX systems developed the UUCP protocol to network themselves into a network called UUCPNET, around the same time the TCP/ IP was evolving. UNIX systems were later equipped to communicate using either TCP/ IP or UUCP, and to transfer data from one protocol to another. A system could receive data by TCP/ IP and transmit it out by UUCP, or vice versa. In this role, this system acted as a gateway or a bridge between networks.

Files and electronic mail can be exchanged with other systems via UUCP. UUCP is a point-to-point protocol designed for communicating over telephone and serial lines. UUCP is still widely used for transporting electronic mail between computers that do not have TCP/ IP, and is especially useful for isolated systems that obtain their e-mail feed over serial lines.

The UUCP program allows the transfer of files between remote computers and the execution of commands on remote computers. Since these computers may be connected by telephone lines, UUCP transfers can take place over thousands of miles. Technically, therefore, a UUCP site in New Delhi can transfer a file to, or execute a command on, a connected UUCP system anywhere in the world. The UUCP commands, however, do not allow interactive sessions with the remote site.



5.3 Internet Services and Resources

There are innumerable information resources located on any number of servers on the Internet. It is a veritable source of knowledge, an inexhaustible source. Services on the Internet which can be broadly categorised into two groups:

- Communicating in cyber space
- Locating and retrieving information

are briefly described in the following sections:



5.4 Internet Mail

Electronic mail is the oldest service on the Internet and still the most dominant. It enables one to send information in the form of letters, messages, advertisements, spreadsheets, game programs, binary files, multimedia data files across the Net to one or more Internet addressees. Most messages reach their destination across the globe in minutes. E-mail on the Internet is inexpensive, volume-independent and distance-independent. The user normally pays a flat rate for connectivity to the ISP.

E-mail software comprises of Mail Servers on the Internet, and Mail User Agent or Mail Reader at the user-end. The mail servers are based on various protocols including Simple Mail Transfer Protocol (SMTP) Servers, and Post Office Protocol (POP) Servers. All these and the ISO standards-based X.400 Message Transfer Agents for storing and forwarding messages, have already been described in Chapter 4.

The Mail User Agent software running on a PC or a terminal is used to compose and send mail via a server, retrieve mail from a server and display the same on the user's screen. It can perform a variety of functions to make mail management easier for the user: submit/ retrieve messages, retain/ remove after fetch, resend, spell check, alarm for informing arrival of new messages, folder facility, attach/ detach, system address book, sort, delete, filter, print, etc. Internet Mail UAs may use POP or some proprietary Protocol such as Microsoft-Mail or CC:Mail.

The Mail UA can also process attached files using proprietary formats, within a message, or the Multipurpose Internet Mail Extension (MIME) Protocol which has developed into an Internet standard. MIME message can hold EDI body parts, since the concatenation of various message parts is allowed in MIME. Likewise, pictures, graphics, audio, and video files can be attached as MIME files in the message. A message formatted according to the MIME-EDI specifications can travel over the Internet using SMTP, and get automatically transferred to an

EDI processing program. This enables EDI messages to be transferred over the Internet. In this case, the Mail UA would function more as an automated e-mail message processing program, unlike the typical UA which is interactive in nature.

There are other ways of communicating on the Internet too. They are briefly discussed below.

5.4.1 Usenet News

The Usenet news is similar to an electronic bulletin board. There are countless boards, each dedicated to a specific topic and shared by thousands of users. These bulletin boards are referred to as newsgroups. Messages are organised into newsgroups, which are, in turn, classified into various classes such as business, science, magazines, health, computers, etc. There are over 10,000 newsgroups carried by major ISPs. Newsgroups may be 'free form', i.e. anyone can post a message on it, or 'moderated' in which case someone running the newsgroup is required to approve a message before posting on the electronic bulletin board.

Starting with the first experimental Usenet group in 1979 by the University of North Carolina, and the Duke University, USA, there has been a virtual explosion in the sites that carry Usenet. There are over 100,000 sites that carry Usenet, and several million users participate in them. There is no central administration of Usenet; it is run by people who use it.

There are several uses of Usenet News. One can post one's question, say on a new software package, on a newsgroup. Someone will respond with solutions. An organisation connected to the Internet may choose to carry only a particular set of newsgroups to promote its interests. Usenet news could be used to broadcast EDI messages to target community.

5.4.2 Mailing Lists

The Usenet group is open to all, but if the interest is confined to a smaller domain, a mailing list may be used. Discussion groups or announcements of a specific nature generally use mailing lists. Usually servers allow more and more users to enlist themselves in the mailing lists by sending an e-mail message. A discussion group's members, restricted to only subscribers as per the mailing list, receive messages from the server as soon as someone has sent one. Normally there is no charge for the use of a mailing list. However, the sender can charge for the content, e.g. e-magazines. An organisation could use a mailing list to broadcast EDI messages such as RFQs (Request For Quote) to its potential vendors. The vendors may subscribe to different mailing lists depending upon the products or services they sell. This enables them to receive inquiries from buyers.

5.4.3 Internet Relay Chat

The IRC service on the Internet differs from Usenet in that the chat or discussion takes place in real-time. It is a very popular service, being a multi-user implementation of the Unix "talk" program. Developed in 1988 by J. Oikarinen in Finland, the IRC, offering a unique type of talking experience on the Net, has been used extensively for the live coverage of world events, news and sports commentary. The IRC network on the Internet consists of multiple interconnected servers. The IRC service comprises a number of channels: public, private, secret or invisible. A user can choose a channel of his choice and be part of a particular conference on the Internet. The user's interaction with his conference mates is through a software program running on his system, known as the IRC client. IRCIIWIN, WS-IRC and WINIRC are some of the well known IRC clients.

The IRC allows a user to change from one chat group to another, join any conversation or only listen. The user can eavesdrop on other people's conversation just like in normal

talk mode. IRC can also permit a user to invite some of his confidants into a corner for a secretive talk on the Internet.

5.4.4 Internet Talking

This Internet 'Live' audio/ video service allow a user's computer to connect to other users computers on the Internet. The messages are exchanged in real-time by these users as soon as they are typed by any of them. A program executing in the background, called the 'talk daemon' handles the actual communication service. This program should be compatible between users desiring to engage in Internet talking. Once the connection is made, the talk daemon divides each user's screen into two halves by drawing a horizontal line in the middle. The local user's keyboard strokes are captured in the upper half, while the typed text of the remote user is displayed on the lower half of the screen. If there are more than two users in the talk mode, the "ytalk" program divides each user's screen into as many partitions as the number of users. Netscape's cool-talk is one of the better known packages for this service.

Similarly, video exchange can also be conducted in real-time over the Internet. Software packages include Cinecom and VDO Phone.



5.5 Internet Search

The Internet is an enormous resource of information: computer software, newspapers, magazines, graphics, library books, articles and literature on philosophy, religion, history, science, art, health, and so on. How can one search the Internet for the information or data one is looking for? How can one locate the right server on the Net, and retrieve the right kind of information without getting lost in the sea of information ? Locating and retrieving information are the key problems. While part of this requirement can be fulfilled through e-mail, other types of search

tools are required to carry out this task. The major tools of the Internet can be divided into the following groupings:

- Telnet, rlogin, and rsh
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- WHOIS
- World Wide Web (WWW).

These are briefly described in the following sub-sections.

5.5.1 Telnet

This is a very popular Internet service which enables a user to log into another computer to run software there. Telnet is a program which allows a computer to establish a session with a remote host on the Internet. One can login either to access a shell such as the Unix operating system on the remote computer, or a utility like a database, or weather service. Many public services can be accessed by using Telnet, such as library card catalogues, and databases on servers. Once a user has logged into the remote server, he can execute various commands to operate the host system. rlogin, and rsh are also remote login Internet services.

5.5.2 File Transfer Protocol (FTP)

FTP is a tool that is used to transfer data/ files among computers on the Internet. FTP is a set of specifications, a program which enables one to log into an account on a remote computer in order to send files to it, or receive files from it. FTP differs from Telnet in that it is not used to run programs on remote computers. It is a very useful tool for sharing information by moving files between computers. The files may be of any type: text, graphics, multimedia, binary files.

FTP is a collection of programs which includes both the client and the server software. The server provides a specific resource,

and the client makes use of it. A client sends a request message to a computer running as an FTP server, which sends the requested document to the former. The interaction is thus between an FTP client program on a local computer with the FTP server program on a remote host on the Internet. In Internet parlance, this is referred to as the FTP client downloading files from a remote FTP server on the Net. There is also a provision to upload files to a remote Internet host.

Telnet requires a user to have an account on the remote system. For undertaking file transfer, one needs permission to use FTP to access a computer. There is, however, another facility that enables an Internet user to access files without being registered on the FTP server. This is called Anonymous FTP. The user signs in as Anonymous, and accesses directories which are open to the public. The public domain software, and information on the Internet are huge, and continue to grow. It is the largest library of information. Anonymous FTP allows anyone plugged into the Internet to download innumerable files from thousands of FTP servers providing the Anonymous user facility. The world of Anonymous FTP includes free software, books, magazines, weather pictures, space research, literature, and so on.

5.5.3 WHOIS

WHOIS is a program that can be used to find information on users and sites on the Internet. A client WHOIS program on a computer can initiate search on a WHOIS server and present the result. One can also Telnet to a public WHOIS server to get content information about the desired users/ Internet sites.

5.5.4 World Wide Web

The World Wide Web (WWW) or the Web is a system for organising, linking and providing point-and-click access among related Internet files, resources and services. The point-and-click

access is due to the underlying hypertext or hypermedia approach of the Web search engine. The Web is an Internet-based navigational system, an information distribution and management system with tremendous potential for commerce. It has become an integral part of the Internet.

The computer-based information programs that enable web navigation are hypertext or hypermedia. Hypertext refers to computer-based documents in which cross-references are embedded within documents and other entries. Each cross-reference is a pointer to another document or to other actions, lists or menus. This approach enables a user to move from one place in a document to another in a non-sequential manner. Unlike a book in which one moves from chapter to chapter, one moves randomly throughout a hypertext document. Words, phrases and icons in the document become links that allow one to jump to a new location or another on the Web.

Documents today include not just text, but graphics, photographs, audio and video in the form of multimedia documents. The concept of hypertext has, therefore been extended to what is known as hypermedia. The hypermedia links connect to visuals such as graphics, audio, etc., in addition to text. The hypermedia documents thus get presented on a PC with excellent visuals, supported by audio commentary and video clippings. The Web supports hypermedia navigation, which allows a multimedia document to be stored in a Web server, and to be downloaded by Web client software for display on the user's PC plugged into the Internet. Like other Internet services, the Web service also uses the client-server model. The client is known as the Web Browser. It is a tool that enables an Internet user to access many services and resources on the Internet. The Web browser offers an easy-to-use, graphical point-and-click interface to the Internet; it can initiate Telnet and FTP sessions, read Usenet news, access Gopher items, set WAIS search, etc. This enables a user to travel through the Web, to surf the Web.

The Web facility on the Internet is made up of a collection of servers and clients that can exchange information. According to InterNIC's Internet Domain Survey, more than 317 million (as of January 2005) Web host computers support interactive hypermedia information. These are the websites on the Internet. The Web is a distributed system, since pieces of information are stored on different Web servers worldwide in the HyperText Markup Language (HTML). These are communicated to one another or to a Web client in the HyperText Transmission Protocol (HTTP). The prominent Web browsers are Mozilla Fire Fox, Opera, Netscape, and Internet Explorer.

Web technology differs significantly from other Internet services. With FTP, for example, when a user connects to a remote computer, the connection is continuous, i.e. the line is occupied till he is finished with the task. The web browser, on the other hand, opens a connection to a remote computer, the website, and retrieves the initial information, and quickly closes the link. The connection is re-opened briefly, as soon as the user requests more information from the server through a click. Since the connection with a remote host occurs only for a fraction of a second, the limited resources of the Internet in the form of lines and bandwidth, are more effectively utilised with the Web approach. The first information that one gets from a remote website is known as a Home Page. This, in turn, leads a user to a series of other documents, files, and resources that reside on that computer or on other web servers around the world.

The links or hyperlinks, which define the hypertext or hypermedia documents, are actual live links. One can activate the link, and cause what if references, to appear on the user's computer. Web documents are all hypertext documents. The highlighted words or pictures in a document are links that actually store hidden addresses to connect with the resources to which they point. A click on this portion produces the desired information. These hidden addresses are called Uniform Resource Locators (URLs). URLs represent links to documents, files and resources on the Internet.

The World Wide Web has grown in an anarchic manner, like the Internet itself. No person, company, or organisation owns the Web. It is a distributed system with millions of users, and perhaps an equal number of web authors, who contribute to this electronic warehouse. The applications of this global database range from education and entertainment to government and commerce. Websites are hosted by educational, commercial, and government institutions. According to the statistics available by Anonymous FTP from nic.merit.edu, the web traffic comprises the following: US educational—49 percent, US commercial—20 percent, US Government—9 percent, other countries—22 percent.

The Web has indeed graduated into an enabling mechanism for electronic commerce.



5.6 Issues of Concern

Concerns about the Internet emanate from issues such as integrity, confidentiality, non-repudiation, and authentication. In addition, ease-of-use, reliability, support, and rapid delivery are of concern. Essentially, these reduce to the following major issues with the Internet:

- Robustness
- Reliability
- Bandwidth
- Security

5.6.1 Robustness

Business and trade demand that the delivery of transaction should be guaranteed, i.e. the Internet must be robust. In the commercial world, a message cannot bounce back undelivered. A document reported missing by a trading partner is unacceptable. The Internet was created as a robust infrastructure since its design was based on the stringent requirements of the military. It is indeed robust, since the TCP/ IP suite of protocols

and the underlying architecture of the Internet are stable and mature, and product implementations based on the TCP/ IP suite are also stable and mature. Dynamic routing on the Internet ensures that packets do reach their destinations even if there are network outages along the way. Moreover, commercial ISPs administer their portions of the Internet at high levels of reliability and availability.

5.6.2 Reliability

The commercial world demands that the Internet should guarantee the time of delivery. The IETF is continuously working on issues related to this to evolve standards so that the Internet should provide essential value-added services. Some of the existing characteristics of the Internet and proposed initiatives for reliable transmission of messages over the Internet include the following:

- Special authentication/ non-repudiation programs would fetch delivery and receipt reports.
- Protocols and tools exist for diagnosing problems across the interconnected systems. A trace route or ping *command* can diagnose the source of problems.
- For assured delivery, use of dedicated Internet connection is recommended to transmit information via SMTP, instead of a store and forward connection
- For high reliability applications, redundant ISPs with separate backbones and redundant mail servers at separate locations are recommended.
- An IETF initiative is working on the Reservation Setup Protocol (RSVP) with the objective of allowing Internet applications to obtain special quality of service for their data flows by reserving resources along the data path. The integrated services envisioned on the Internet have RSVP as a key component.

5.6.3 Bandwidth

The Internet has caught the imagination of the young and the old, in the developed world as also in the developing countries. The number of connections to the Internet continues to grow everyday. Servers of all types, websites including those for business and conveyance are growing on the Internet. More and more people are getting hooked to surfing the Net. New ways of information delivery on the Net are seeking to redefine not only information, but also entertainment. New boxes are under development for video, audio and graphics downloading as infotainment. The Internet has also been promoted for commercial transactions. Secure, reliable, and cheap e-commerce transactions on the Internet promise to radically alter the business scenario. The result with all this hype is exponentially increasing traffic. The Internet is already getting choked. The Internet bandwidth needs to be augmented substantially to assure commercial users of its availability when they need it.

Nations are moving in the direction of setting up National Information Infrastructures (NII), high bandwidth information highways, to link with the Global Information Infrastructure (GII). This is the subject of Chapter 11.

5.6.4 Security

Security of transactions is of paramount concern to the commercial world. The Internet, being an open network, can be invaded by hackers and criminals from all quarters. The intermediate nodes through which the message packets get routed, are extremely vulnerable to security breaches. Secure Electronic Transaction (SET) protocol has been designed to make credit card transactions on the Internet fully secure. There are already products available from a number of companies which guarantee security on the Internet. E-Commerce security issues are discussed in Chapter 14.



5.7 Browsers

Web browsers, as their name suggests, are used for browsing through web pages on the Internet websites. Early browsers displayed web pages containing text and links to other web pages. The pages were stored as HTML files. The ability to display forms to be filled, along with buttons and pull-down menus was introduced in Mosaic2.0, the browser developed by the National Centre for Supercomputing Applications. Other browsers that were introduced in the mid-1990s include Cello, Internet Chameleon for Windows 3.1 and 95, Internetworks, Netcruiser and winWeb.

When Netscape launched its browser, it had a great impact as image files which could be downloaded could also be displayed even before the entire page had been downloaded. This was followed by the capability to include animated images, so that moving pictures could also be included in web pages.

Finally, it is Netscape's Navigator and Microsoft's Internet Explorer that have emerged as the top ranking web browsers. Both of these offer a core set of features conforming to HTML so that text, images and links can be handled. Helper applications are used by both browsers.

The inclusion of frames, plug-ins and Java by Netscape further enhanced browser capabilities. Frames allowed the development of multiple, independently scrollable panes on websites. Plug-in applications and Java allowed the inclusion of third party programs and development of web-embedded applications. Not to be left behind, the facilities provided by Java have been built by Microsoft in its ActiveX model.

While Netscape's Navigator is available on all platforms, Internet Explorer is tailored for the Windows environment.



5.8 HyperText Markup Language

The HyperText Markup Language (HTML) is the language used to prepare documents which are accessible over the World Wide Web. Web browsers display these documents in a pre-determined format.

Traditionally, document preparation on computers has been handled by word processing programs such as Word Perfect and Word. These programs normally insert binary codes for specifying the format of a document's contents. HTML, however, operates in a different mode. ASCII codes are used to identify both the content and its presentation format. As such, any text editor can be used to create HTML documents. This makes the document size much smaller and also removes the problems faced because of different binary codes used by different word processing programs to represent the same format characteristic.

In HTML, markup tags, bracketed between “<” and “>” symbols, are used to decide on the presentation of documents. The markup tags are usually paired, with an ending tag starting with a slash (< / [tag] >). For example, any text between the tags and </ b> will be displayed in bold by the browser. If the text contains a < a href> tag, the browser knows that what follows describes a hyperlink to another document. Depending on the version of HTML being used, there are specific components that must be included in any HTML document.

One of the powerful features of HTML is its ability to link to documents on other computers. These documents are identified on the basis of the Uniform Resource Locator (URL). The URL can be thought of as a networked extension of the standard filename concept, except that in this case the file and its directory can exist on any computer on the network. The object being accessed could be a file, a document stored in a database or the result of network search. The URL contains three parts: access protocol, machine name and path information of the document in the format:

protocol:// machine.name/ directory/ document

A document called `urlfile.doc` available on an anonymous ftp server called `ftp.anon.com` is the directory `pub/ files`. (An anonymous ftp server allows any user to log on with the user ID `anonymous`. The user's e-mail address is normally provided as the password.) This file could be accessed by the URL:

`file://ftp.anon.com/pub/files/urlfile.doc`

The most common URLs are those for anonymous FTP, gopher or HTTP servers, for pointing to Usenet news groups, remote login with Telnet or sending e-mail. The URL used for sending e-mail is in the format:

`mailto:<login@host>`

5.8.1 HyperText Transport Protocol

HyperText Transport Protocol (HTTP) is used to transfer HTML documents across the Internet. HTTP provides a means of transparently moving from document to document and indexing within a document. As a client/ server architecture, the background actions that occur when a user clicks a link on an HTML page, causing that page to be replaced by a new page, are somewhat complex. These are:

- The client browser (ex. Netscape Navigator or Microsoft Internet Explorer) uses HTTP commands to communicate with the HTTP server through a reference provided by the URL.
- A TCP/ IP connection is established from the client to the server.
- A request message is sent by the browser client to the server computer, typically for a file containing either text, images, audio clips, animation clips, video clips, or another hypertext document.
- The server sends a response message with the requested data to the client. Messages are passed in a format similar to that used by Internet mail and MIME.
- The connection is terminated.

A status message is returned by the server and includes the message's protocol version, a success or error code, and a message.

WWW Servers or HTTP servers are commonly used for serving hypertext documents. For example an HTTP file called `urlfile.html` in the directory `/pub/` files on the HTTP server "`www.httpserv.com`" can be accessed through the URL

`http://www.httpserv.com/pub/files/urlfile.html`



5.9 Java

Java evolved around a Sun Microsystems research project started in the early 1990s for looking into the distributed control of consumer electronic devices. At that point of time, the project had nothing to do with studying programming languages. However, as work on the project progressed, it was realised that a new programming language was needed. This was because programming languages like C++ that were being used were emphasising speed. In consumer electronics, however, reliability is a much more important factor. This resulted in the creation of a new language called Oak in August 1991.

However, the technology that developed out of this project did not take off. Sun then saw an opportunity for Oak to survive in the rapidly emerging World Wide Web. The product was made available for non-commercial use in the hope of making it a standard. Oak was renamed Java in January 1995.

Java is an object-oriented network capable programming language. All variables and methods (the Java name for functions and procedures) are defined within objects or classes. Java programs can run as stand-alone applications or as 'applets' running under a Java capable browser. An applet is written in the Java language, compiled and called from an HTML web page. An application is written in the Java language, compiled and called from the command line or from another program.

Platform independence means that a program can run on a wide variety of computers. Java is compiled into bytecode which runs on a virtual machine available on many platforms. Both applets and applications run on this interpreter—the Java virtual machine.

The Java Development Kit (JDK) runs under Solaris, Windows and Linux. The JDK has been ported to many other environments including IBM AIX and Linux. The number of operating systems supporting Java continues to grow rapidly.

With Java, Sun Microsystems established the first programming language that was not tied to any particular operating system or microprocessor. Applications written in Java will run anywhere, eliminating one of the biggest headaches for computer users: incompatibility between operating systems and versions of operating systems. Additionally, Java programs cannot cause system crashes since it carefully checks each and every memory access to ensure that it is valid.



5.10 Internet 2

In order to ensure that the academic world on the Internet continues to get fast access, a group of universities started work on a joint project called Internet2². Internet2 is more of a test bed, wherein new applications, protocols, and high-speed networks will lay the groundwork for tomorrow's global Internet. Internet2 was the result of a 1995 meeting of higher education CIOs and government and industry network leaders which concluded that Internet then, could not meet the remote collaboration and distance education needs of the future. Since then, the group has grown to include 205 universities, as well as virtually every major research institution. A new company, the University Corporation for Advanced Internet Development (UCAID), was formed to serve as a support umbrella for Internet2.

Internet2 plans to connect universities at rates up to a gigabit per second (1,000 Mbps). Internet2 links are being built on top of existing Internet links including the vBNS (very high speed Backbone Network Service). The vBNS is an existing backbone originally designed to connect a few supercomputing sites. The goal is to allow applications to exchange data at 100 Mbps from end to end. At these data rates, the network requires very fast switches—thus the “gigapop”, a point of presence (POP) that can route a gigabit per second.

A big goal of the project is transferring the technology to industry for general deployment. The IETF will continue to be the standards body for ratifying any new protocols and technologies from Internet2.

In April 1998, the then US Vice President, Al Gore formally announced an IP network, code-named Abilene, to provide the native backbone for the Internet2 project intended to give a faster route through cyberspace to research universities. From 2.5 gigabits per second, the cross-country backbone for the regional aggregation model provided by Abilene is being upgraded to 10 gigabits per second, with the goal of offering 100 megabits per second of connectivity between every Abilene connected desktop. By April 2003, Abilene had 221 participants including both universities and research laboratories. Expanded access was also provided to 70 sponsored participants and 25 state education networks.

The Internet2 project is expected to bring focus, energy and resources to the development of a new family of advanced applications to meet emerging academic requirements in research, teaching and learning.

Internet2 addresses major challenges facing the next generation of university networks by:

- Creating and sustaining a leading edge network capability for the national research community.
- Directing network development efforts to enable a new generation of applications to fully exploit the capabilities

of broadband networks media integration, interactivity, real time collaboration to name a few.

- Integrating the work of Internet2 with ongoing efforts to improve production Internet services for all members of the academic community.

The Mission of the Internet2 project is to facilitate and co-ordinate the development, deployment, operation and technology transfer of advanced, network-based applications and network services to further US leadership in research and higher education, and accelerate the availability of new services and applications on the Internet.

Its goals are to:

- Demonstrate new applications that can dramatically enhance researchers' ability to collaborate and conduct experiments
- Demonstrate enhanced delivery of education and other services (e.g., healthcare, environmental monitoring) by taking advantage of 'virtual proximity' created by an advanced communications infrastructure
- Support development and adoption of advanced applications by providing middleware and development tools
- Facilitate development, deployment, and operation of an affordable communications infrastructure, capable of supporting differentiated Quality of Service (QoS) based on applications requirements of the research and education community
- Promote experimentation with the next generation of communications technologies
- Co-ordinate adoption of agreed working standards and common practices among participating institutions to ensure end-to-end quality of service and interoperability
- Catalyse partnerships with governmental and private sector organisations
- Encourage transfer of technology from Internet2 to the rest of the Internet

- Study impact of new infrastructure, services and applications on higher education and the Internet community in general.



References

1. Anderson, Christopher, 'Electronic Commerce: In Search of the Perfect Market', *The Economist*, May 10, 1997 p. 13.
2. Internet2 Home Page at www.internet2.edu/html.



Chapter 6

Intranets



6.1 Intranet

With the introduction of the World Wide Web, a whole new way of looking at the Internet emerged. Coupled with its ease of use, the Web opened up vast storehouses of information, all available through mouse-clicks on the Web browser. E-mail, File Transfer and Remote Login had already been around for quite some time. Harnessing this technology to fulfil the internal information flow requirements of organisations, gave birth to the ‘intranet’.

What is an intranet? Intranets use Internet technology to deliver an organisation’s internal information. This includes integration of e-mail, FTP, Mail Server(s) and Web server(s) with the internal applications; the user interface is provided by Web browsers. Of these, Web servers are the most visible part of the intranet since this is where the organisation’s Web pages would be hosted and accessed by the client machines.

The objective of an intranet is to organise each individual’s desktop with minimal cost, time and effort to be more productive, cost-efficient, timely and competitive. With an intranet, access to all information, applications and data can be made available through the same browser. Intranets connect people together with Internet technology, using web servers,

web browsers, and data warehouses in a single view. Of course, all clients and servers must support the TCP/ IP protocol. Though it uses Internet technology, an intranet does not have to be connected to the Internet. However, moving mail and other information across the Internet to clients and partners might be needed, so an Internet connection may be desirable. The differences between the Internet and intranets need to be appreciated in order to handle applications properly. Whereas the Internet is always starved of bandwidth, intranets, even on the slowest LANs with bandwidth of 10 Mbps, have no bandwidth issues. Therefore, an application designed for the intranet may be choked on the Internet, while those for the Internet may run in a flash on an intranet. Since the Internet is an open environment, security is a major issue. Intranets, on the other hand, are secured and confined to organizations.

Intranets provide a lot of choice and flexibility by virtue of being developed on open standards and protocols. Existing applications do not have to be rewritten to the new client-server environments. New versions of word processors, spreadsheets and database programs have built-in Internet capabilities. A Web page can be automatically produced from an existing word-processed document by simply saving it as an HTML document. However, policies for using the technology within the organisations are extremely important. Who decides the content and processing/ routing rules? What is the approval process for getting content out on the website? Who maintains the content?

The open nature of the Internet cannot be replicated in an intranet since company data would be available on it and would need to be handled very cautiously. Security is provided in the intranet environment through the deployment of protocols such as Secure Sockets Layer (SSL), Secure Electronic Transactions (SET), and Secure MIME (S/ MIME) to provide confidentiality, data integrity, authentication and digital signatures. Access to internal information systems from outside can be regulated through the installation of Firewalls. These are explained in Chapter 14.

The departments in an organisation which could benefit by implementing an intranet include Finance, Sales and Marketing, Manufacturing, R&D, Personnel and Customer Support. The IDC reported a case study of Silicon Graphics which invested \$1,324,421 in implementing an intranet. About three-fourths of this amount was invested in software. The Return on Investment was calculated at 1,427%!

Closer home, *The Times of India* implemented the first intranet in the country in the year 1996. Their large network of computers was integrated through a Web server for sharing information and applications from terminals at geographically dispersed locations. In addition to smoother functioning, the company reported huge direct savings in telephone and photocopying costs.



6.2 Intranet Services

An intranet provides Internet services within an organization. The intranet client is a universal browser using TCP/ IP protocol. There may be any number of servers in the organization; they may support any services on any operating system. As long as they support TCP/ IP protocol stack, they are part of the intranet. Figure 6.1 shows an intranet.

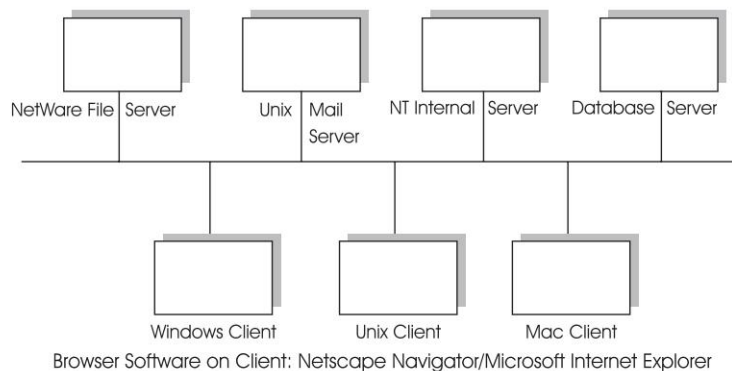


Fig. 6.1 A multiclient, multiserver intranet

An intranet has to be designed for the specific functionality requirements of an organization. The requirements or services may include the following:

- Mail Services
- File Transfers
- Web Services
- Audio Services
- Video Services

The enhanced intranets are characterised as Full Service Intranets. This term is defined by Forester Research as: 'A Corporate TCP/ IP network which delivers reliable, feature-rich applications that share five core, standards-based services—directory, e-mail, file, print, and network management'.

The key is to set up an intranet which incorporates in its design the concept of the universal browser as the touchstone for a vendor-independent implementation based on non-proprietary networking standards. The easiest way to start is by providing e-mail services from a standards-based server, i.e. SMTP mail server with client using Netscape Navigator or the Microsoft Internet Explorer browser to retrieve mail, using POP3 protocol, from the mail server. The simplest way for setting up a server is by installing a Unix system which has built-in free SMTP mail server software. No expensive gateways are required. In fact Unix is available for free as Linux which comes complete with SMTP mail server. This is the easiest way to get started and demonstrate the usefulness of an intranet, and thus enlist the support of the top management.

The essential components of an intranet include the following:

- A network
- TCP/ IP on servers and clients
- Hardware for hosting intranet services
- Software— Mail server as the minimum
 - Web server for hosting Web pages
- Mail servers
- Browsers

The optionals include:

- HTML editors
- Productivity tools which are Web-aware
- E-mail Remote User Agents
- Proxy servers
- CGI
- Java
- ActiveX

While the essential components will make an intranet operational, it is the optional elements that make it truly useful by delivering all, or most of the intended intranet services. The Web services, database linkages, applications requiring users to fill forms, graphics and beautification of sites, etc. are enabled by the tools mentioned above.

While mail and Web-enabled applications on an intranet help in cost savings realised from reductions in printing and distribution costs, one of the largest benefits is the increased access to information. An intranet achieves the following in an organization:

- reduced costs
 - printing, paper, software distribution, mailing, order processing
- reduced telephone expenses
- easier, faster access to technical and marketing information
- easier, faster access to remote locations
- increased access to competitive information
- latest, up-to-date research base
- easier access to customers and partners
- collaborative, group working
- increased accuracy and timeliness of information
- just-in-time information

According to James Cimino, the challenge is to realise the following from focused intranet implementations.

- easily accessible information

- reduced information searching time
- sharing and reuse of tools and information
- reduced set-up and update time
- simplified, reduced corporate licensing
- reduced documentation costs
- reduced support costs
- reduced redundant page creation and maintenance
- faster, cheaper creation
- one-time archive development costs
- sharing of scarce resources and skills.

This requires that the management analyse the business problems or the issues that are being addressed through an intranet. The focus should, therefore, be not on technology, but on business. It is the business needs that should drive an intranet. All or some of the above benefits will make a business case for an intranet. Requirements must, therefore, be studied carefully, and the intranet tailored towards realising them to provide the organization with the much-needed tools for operational efficiency, better turn-around time, better knowledge base, more productivity, and competitiveness to survive in the marketplace.



6.3 Intranet Implementation

The intranet is best implemented in a phased manner. Assuming that a network is already in place, the steps essentially revolve around selecting servers and software, the operating system and special tools for content creation. The emphasis should be on creating a system that is amenable to constant change and updation rather than on static documents, because if it is the latter, the users would soon lose interest in accessing information from the corporate intranet. The existing databases, and software applications should also be integrated into the intranet. This calls for a proper plan to be prepared. The important steps to implementation are the following:

- **Planning** The scope of services and facilities; mail, websites, homepages, administration of the site, layout of pages, connecting with existing databases and applications, dial up access to intranet and connecting with the Internet.
- **Subnets** The detailed planning of the intranet, with all its subnets. If the number of servers and clients is large, there may be many subnets. IP addressing plan should be worked out in detail.
- **Servers and Software** Server hardware platforms and the software that will be used on them for hosting mail and Web services need to be finalised. Similarly, for intranet users, browsers and mail clients have to be standardised. The best way to start is to take any existing Intel desktop system and convert it into a server platform, which may host both mail and Web services. As the intranet load grows, this could be split into multiple-servers without the users feeling any difference. Web server, mail server, print server, Domain Name Server (DNS), workflow applications, etc. could be implemented on different hardware systems.
- **Operating System** Choose an operating system from among the following popular server operating systems—Unix, Linux, Windows NT, NetWare, Mac OS, OS/ 2, AS/ 400. The choice of operating system will determine the software requirements of the Web server, mail server, etc. It will have a direct bearing on the total cost of intranet software. Today PC class servers have broken into the erstwhile exclusive domain of RISC servers for Web services, by their increased performance, robustness and reliability. While Unix was the operating system on RISC systems, non-Unix platforms are equally aggressive solutions now.

It should be installed on the server, complete with the TCP/ IP suite of protocols. Web server and mail server have to be configured as the very minimum as intranet software. DNS services should preferably be implemented from the

very beginning. IP addresses and subnet masks must be allocated and all nodes and servers tested for communication. It is better to plan for, and use TCP/IP addresses duly registered with InterNIC so that connection to the Internet at a future date avoids address conflicts.

- **Proxy Servers** If the intranet requires the users connected on it to share a single Internet dial-up connection on the network, a proxy server is essential. It is the proxy server that dials into the Internet connection and all the nodes access the Internet through it.
- **Content Creation Software** HTML editors, Web-enabled office productivity tools would be essential on client machines which have already been equipped with browsers and E-mail software.
- **Training** Train the users on mail and Web applications. Show them how to use a discussion group, mailing list server, FTP server. Show them how to convert their existing documents and reports for the intranet, and make the same available to all. Show them how to create new content using the office-suites, productivity tools, HTML editors, etc.
- **Existing Databases** Set up a group of programmers to study the existing database, and to Web-enable them for intranet.
- **Web Publishing** The Web is like a magazine, and content creation is like Web publishing. The magazine is on the Web server, and is meant for employees of an organization who are on the intranet. The contents have to be catchy, enticing, easy to access, and uptodate. Web design and maintenance thus becomes a major issue on an intranet.



6.4 The Webmaster

Intranets have generally come to be managed in organizations

by managers who have been christened as Webmasters. In the Internet world, the Webmaster is responsible for the setting up and maintenance of a company's internal or external website. This term and the role borrowed from there, has been given a wider meaning in the Intranet. The Webmaster is responsible for the creation and maintenance of Intranet servers and services. He or she maintains the functionality of the intranet services provided, and is responsible for updating the content of the websites, mail directories, integrating with databases, connection with the Internet, and so on.

The Webmaster has to know the organization's business very well, besides being familiar with the Internet and being thorough with programming languages and network technology. Intranet planning requires that the Webmaster visualise the present and future goals of websites, on a wider canvas. Emerging technologies and business models must fascinate him or her. Above all, he or she must be able to work with the organization's Intranet committee, since the Intranet is expected to change methods of working. And change management is not easy. We will discuss this separately in Chapter 12. The committee must include representatives from all corporate departments who should articulate their requirements. Since the Webmaster is required to have many types of skills, and since no one person may have them, the greatest ability that one is looking for is that of a desire to learn and acquire new skills. In short, the Webmaster must clearly understand the organisation's problems and challenges, develop a cross-organisational plan for the Intranet, translate it into a technical plan to support the plan, and deploy effective support tools on servers and clients to initially provide the desired complement of intranet services, with an eye to the future for full intranet services. The Webmaster must be alive equally to the concerns of the management and those of the users, providers and developers.

As the intranet grows, the Webmaster may cease to be just one person. In larger organizations, several people collectively may act as the Webmaster or as an intranet team. Distribution

of responsibilities can ensure up-to-date content including websites, directories, database links etc. The least that may be essential is the generation of Web page content by respective users or departments in HTML format, so that the Webmaster can publish them faster on the Intranet. However, central control is necessary for logical server administration, which involves the security of the intranet, website creation and content.

The Webmaster can enable intranet application to be ready for e-commerce through the Internet gateway. It is in this role that an intranet becomes an extranet. Chapter 9 takes a look at this.

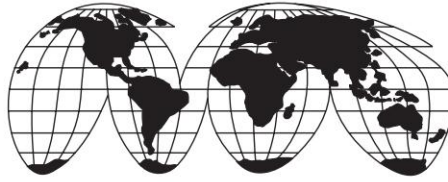
PART

III

Building Blocks for E-Commerce

- Electronic Data Interchange
- The UN/ EDIFACT Standard
- The Internet and Extranets
- Identification and Tracking Tools

Electronic Data Interchange covers the costs and benefits of an EDI system and its various components. The X.435 series of recommendations for EDI Messaging is also included. The UN/ EDIFACT Standard contains the structure and syntax of the UN/EDIFACT standard. The interchange structure is explained in detail to bring out all components such as Messages, Segments, Data Elements and Codes. The Internet and Extranets describes how these tools and networks are being used for Electronic Commerce. Identification and Tracking Tools shows the methods for automatic identification of products and trade units—a vital link in supply-chain management.



Chapter 7

Electronic Data Interchange



7.1 Electronic Data Interchange

Electronic Data Interchange (EDI) is the electronic exchange of business documents in a standard, computer-processable, universally accepted format between trading partners. EDI is quite different from sending electronic mail messages or sharing files through a network, or a bulletin board. In EDI, the computer applications of both the sender and the receiver, referred to as Trading Partners (TPs) have to agree upon the format of the business document which is sent as a data file over an electronic messaging service. Figure 7.1 illustrates the traditional methods of business documents handling versus sending these documents over EDI.

Since data is exchanged in standard pre-defined formats, it becomes possible to exchange business documents, irrespective of the computerised business application at either end of communication. For example, the Supplier's Accounts Receivable application for raising an Invoice for payment could still be implemented on a file system using COBOL while the customer's Accounts Payable may be based on an RDBMS such as ORACLE.

Figure 7.2 illustrates how EDI messages can be used to totally automate the procurement process between two trading partners.

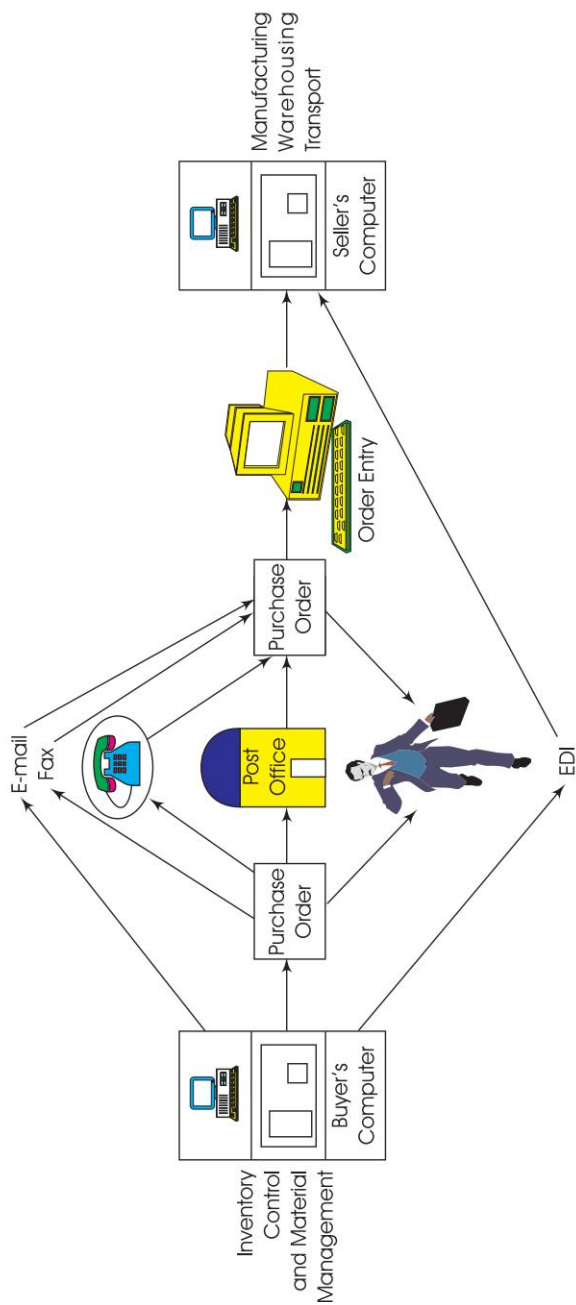
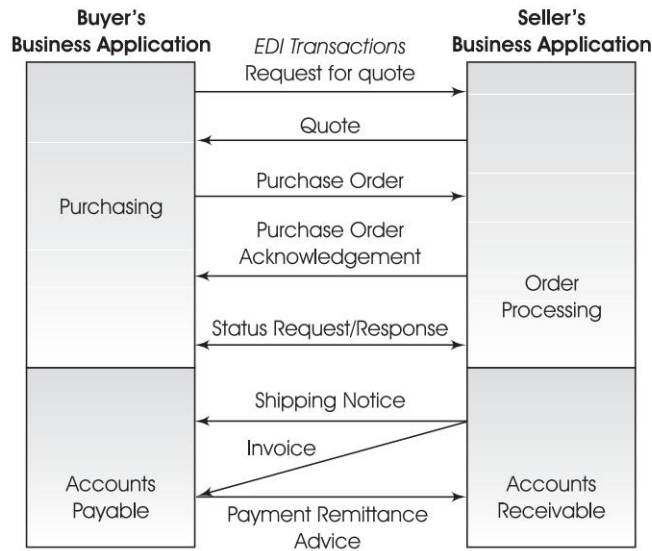


Fig. 7.1 EDI vs traditional methods



➡ **Fig. 7.2** *EDI-enabled procurement process*

Once data are entered into the buyer's computer system and transmitted electronically, the same data get entered into the seller's computer, without the need for re-keying or re-entry. This is normally referred to as application-to-application EDI. EDI can be fully integrated with application programs. This allows data to flow electronically between trading partners without the need for re-keying, and between internal applications of each of the trading partners.

The repeated keying of identical information in the traditional paper-based business communication creates a number of problems that can be significantly reduced through the usage of EDI. These problems include:

- Increased time
- Low accuracy
- High labour charges
- Increased uncertainty

EDI consists of standardised electronic message formats for common business documents such as Request for Quotation,

Purchase Order, Purchase Order Change, Bill of Lading, Receiving Advice, Invoice, and similar documents. These electronic transaction sets enable the computer in an organisation to communicate with a computer in another organisation without actually producing paper documents. It thus eliminates the human effort required to read, sort, and physically transport such documents. The documents for which standard EDI formats are either in existence or under development, constitute about 85 percent of the official communications associated with commercial transactions among business, government, and educational institutions, and non-profit establishments in most of the industrialised world. It is estimated that in the developing countries also, the preponderance of these documents is in similar proportion.

In order to take full advantage of EDI's benefits, a company must computerise its basic business applications. Trading partners are individual organisations that agree to exchange EDI transactions. EDI cannot be undertaken unilaterally but requires the co-operation and active participation of trading partners. Trading partners normally consist of an organisation's principal suppliers and wholesale customers. Since large retail stores transact business with a large number of suppliers, they were among the early supporters of EDI. In the manufacturing sector, EDI has enabled the concept of Just-In-Time (JIT) inventory to be implemented. JIT reduces inventory and operating capital requirements.



7.2 Costs and Benefits

Where EDI has been implemented, computers electronically exchange business documents with each other, ideally without human intervention. This reduces operating costs, administrative errors, and delivery delays. The benefits accruing from EDI implementations can be classified into direct benefits and long-term strategic benefits.

7.2.1 Direct Benefits of EDI

- Since the transfer of information from computer to computer is automatic, there is no need to re-key information. Data is only entered at the source.
- The cost of processing EDI documents is much smaller than that of processing paper documents.
- Customer service is improved. The quick transfer of business documents and marked decrease in errors allow orders to be met faster.
- Information is managed more effectively.

7.2.2 Strategic Benefits

- Customer relations are improved through better quality and speed of service.
- Competitive edge is maintained and enhanced.
- Reduction in product costs can be achieved.
- Business relations with trading partners get improved.
- More accurate sales forecasting and business planning is possible due to availability of information at the right place at the right time.
- There is improved job satisfaction among data entry operators, clerks, etc. when they are re-deployed in more creative activities.

Most organisations with mature EDI programs find that they order more frequently, more orders of smaller quantities. This is consistent with the principles of JIT manufacturing and Quick response (QR) retailing, and requires greater flexibility in the supply chain. Reliance on fax technology limits flexibility and makes it necessary to carry out time-intensive error-prone re-keying of data. If only one order is received per week, then there are up to five working days to process that order. However, if orders are received daily or even hourly via EDI, the processing time is dramatically reduced. This is where EDI is clearly superior.

Even if a trading partner is planning to send only purchase orders electronically at this time and perhaps infrequently, at that, there still may not be a choice about implementing EDI. Most organisations, even the largest and most prestigious ones, find that implementing EDI involves a phased approach; consequently, some functions may not be in place from the start. It is quite common for a large organisation to convert order processing from paper-based to EDI first and bring in other processes later.

Implementing purchase orders on EDI is typically the first step. It is easy to cost-justify and involves the fewest interruptions to the overall environment. Other transactions such as invoices, delivery notices and functional acknowledgments are usually implemented soon thereafter.



7.3 Components of EDI Systems

The three main components required to be able to send or receive EDI messages are:

- EDI standards
- EDI software
- Communication networks

7.3.1 EDI Standards

While using EDI, it becomes possible for a business application on the computer of one organisation to communicate directly with the business application on the computer of another organisation. This exchange of information should be independent of hardware, software or the nature of implementation at either of these two organisations.

In order to achieve this, it is required to extract data from the business application and to transform it into a standard format which is widely, if not universally, acceptable. This standard

data, when received at the destination, is interpreted and automatically delivered to the recipient application in an acceptable form.

The exchange of business documents in a commonly agreed structured format necessitated the development of EDI standards. EDI standards are basically data standards in that they lay down the syntax and semantics of the data being exchanged. In the US, the transportation industry was one of the first to develop EDI standards. Certain large segments of the retail industry also saw the advantages of EDI and proceeded to develop unique standards. They developed their own standards because the earlier standards of the transportation industry were not adequate to accommodate some of the retailers' requirements. The Uniform Communication Standard (UCS) was devised by the grocery segment and adopted by them and several other retail sectors. Meanwhile, in Europe, other sets of standards were developing. These were Trade Data Interchange (TDI) for warehousing, Organisation for Data Exchange by Tele Transmission in Europe (ODETTE) for the automobile industry, and Data Interchange for Shipping (DISH).

Independent efforts resulted in standards for participants in specific industries in the US. It soon became evident, however, that all businesses could benefit from the use of EDI. Some groups promoted the idea of an industry-wide EDI standard. This led to the formation of the Accredited Standards Committee (ASC) X12. The X12 Committee of the American National Standards Institute (ANSI) has, therefore, developed standards for use by all US businesses. These are commonly known as ANSI X12 Standards. Today, EDI standards are firm but not static because the development of EDI is a continuing effort. Specific industry groups are continuing to evolve new transaction sets that may be candidates for standardisation.

UN/ EDIFACT (EDI for Administration, Commerce and Transport) standard was announced in 1987 by the United Nations. The EDIFACT Standard has since been promoted by

the UN for international trade. Electronic documents are replacing paper documents. EDIFACT activity is undertaken by two international organisations. The ISO is responsible for developing syntax rules and the data dictionary. The United Nations Economic Commission is the other agency concerned with the use, promotion and standardisation of EDIFACT messages.

The basic unit of communication among EDI trading partners defined by EDIFACT is an interchange. An interchange consists of functional groups of messages. Each functional group may contain many messages of the same type. Every message consists of a collection of segments with each segment comprising data elements, both composite and otherwise. Special delimiters are specified in the service segment to be used as separators for segments, component data elements and (composite) data elements. UN/ EDIFACT is the subject matter of a separate chapter.

Transmission of EDI messages in standard formats over data networks is enabled using separate standards defined by ITU and other international organisations.

7.3.2 EDI Software

EDI software consists of computer instructions that translate the information from unstructured, company-specific format to the structured EDI format, and then communicate the EDI message. EDI software also receives the message and translates from standard format to company specific format. Thus the major functions of the EDI software are data conversion, data formatting and message communication.

Although any file transfer protocol can be used to transport standard EDI messages, the benefits of using X.400 Message Handling Systems (MHS) to do this were recognised early on. These include the store-and-forward nature of X.400 MHS as well as the generation of delivery reports. A special upgrade to

X.400 MHS was brought out in 1990 through the X.435 standard—a protocol specially designed for handling EDI messages. X.435 standards are discussed later in this chapter.

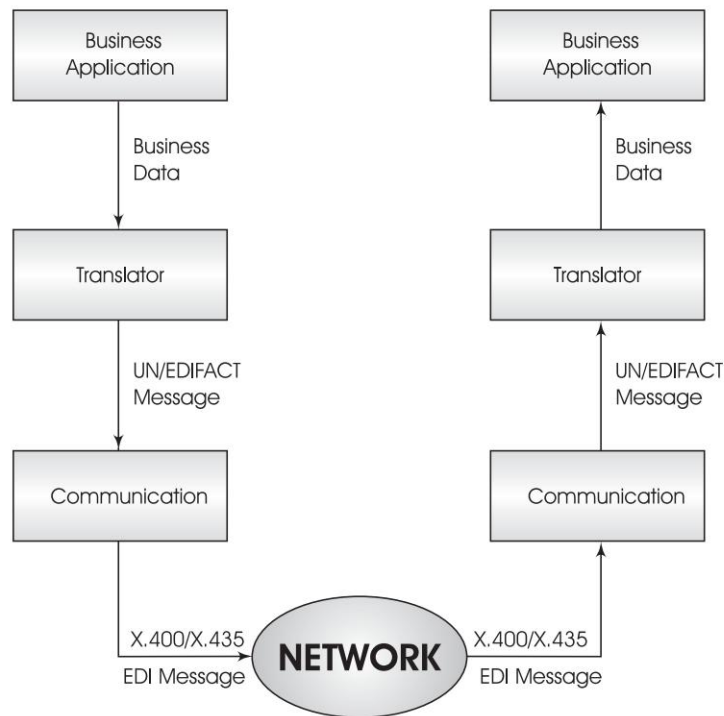
EDI translators perform the important function of translating business data from company-specific formats to standard formats and vice versa. When a document is received, the EDI translation software automatically changes the standard format into the proprietary format of the document processing software.

The most important concern when buying EDI translation software is flexibility. A good EDI translation software product can handle multiple standards and version/ release upgrades.

EDI users in different parts of the world began electronic trading before UN/ EDIFACT was established. Therefore, a number of national standards (e.g., ANSI ASC X12 in North America and TRADACOMS in the UK) are well entrenched in certain user communities. There are also industry-specific and even company-specific standards in effect. It is, therefore, essential that EDI translation software be able to handle more than one standard.

Another issue is that of version/ release upgrades. EDI software, like any other computer software, undergoes regular updates to provide new features and capabilities as well as to make using it easier. EDI translation software should be able to easily accommodate such upgrades or modifications, otherwise EDI communication with partners whose software has been upgraded may suffer. For organisations using inflexible software products, each upgrade creates monumental problems, resulting in substantial costs.

The issue of a single file structure relates to the previous two concerns. EDI uses flat files, that is, data files that use fixed fields (e.g., P.O. number, buyer name, etc.) in a defined order, with the transaction information contained in a continuous string of text characters. Regardless of the standard and the version/ release of that standard, it should be possible to maintain the same flat file structure.



➡ **Fig. 7.3** *The components of EDI systems*

This is critical for EDI to be integrated with existing business processes. The flat file becomes the mechanism for transferring information to and from business applications (e.g., order entry, order processing, accounts, inventory). This helps prevent the problems associated with dealing with some files in one way and other files another way. The goal is to simplify the process, not complicate it.

7.3.3 Communication of EDI Messages

EDI documents are electronically exchanged over communication networks which connect trading partners to one another. These documents are stored in user mailboxes on the network's EDI server from where they can be downloaded/

uploaded at the user's convenience. These networks provide users with a single point interface to the trading community, thereby freeing the user from the worries of handling different communication protocols, time zones and availability of the computer system at the other end—problems in cases where direct links have to be maintained with each Trading Partner.

Some of the features to look out for, when selecting a network service provider are the following:

- The level of customer service
- The degree to which their systems can handle inevitable changes in standards and provide a wider range of functions anticipated in the coming years
- costs.

For the exchange of EDI messages over the Internet, issues relating to message delivery acknowledgement and security of business documents are being addressed by the Internet Engineering Task Force.

The reliability of message transmission along with the generation of delivery notifications provided by X.400 Message Handling Systems resulted in a number of EDI server products being developed over X.400-based communications. In 1990, CCITT (now ITU) released the X.435 series of recommendations which attempted to define features that would be needed in an environment where business documents are being exchanged and would not necessarily be available in an Inter Personal Managing (IPM) environment. (The X.435 recommendations have been included here only for the sake of completeness—they are not being widely used).

Recommendation X.435 is one of a set of recommendations for message handling. The entire set provides a comprehensive blueprint for an MHS realised by any number of co-operating open systems. It defines the message handling application called EDI messaging (EDIMG), a form of message handling tailored for exchange of EDI information, a new message content type and associated procedures known as P_{edi} (Protocol for EDI). It is

designed to meet the requirements of users of ISO 9735 (EDIFACT), and other commonly used EDI systems.

Within the series of recommendations on message handling, recommendation X.402 constitutes the introduction to the series and identifies the other documents in it. The architectural basis and foundation for message handling are defined in still other recommendations. Recommendation X.402 identifies those documents as well.

The P_{edi} protocol available within the X.435 series of recommendations of ITU(CCITT), is specifically designed for EDI messages. It includes many features not available in the protocol solutions for inter-personal messaging.

X.435 defines EDI-specific User Agents (EDI-UA) and Message Stores (EDI-MS). The message transfer service used is the same as that used by the IPMS.

An EDI Message (EDIM) consists of (Figs 7.4 and 7.5):

- Heading—a set of heading field(s), each an information item giving a characteristic to the EDI message
- Body—a sequence of one or more body parts.

The primary body part contains the EDI interchange itself or a forwarded EDI message. The circumstances under which an EDI message is forwarded are discussed further in this chapter. Only one EDI interchange per EDIM is specified. Other body parts that can be included in the EDIM are related to the Primary body part and can be used to carry data, such as voice, text or a drawing related to the interchange.

The EDI heading contains information required to provide services such as selective retrieval that more fully satisfies EDI requirements. The header contains both X.400-specific fields and EDI interchange-specific fields. The EDI-specific fields are copied from the data elements contained in the EDI interchange header segment.

The reason for copying data is to allow the EDI user agent to make decisions on the basis of the data without having to parse

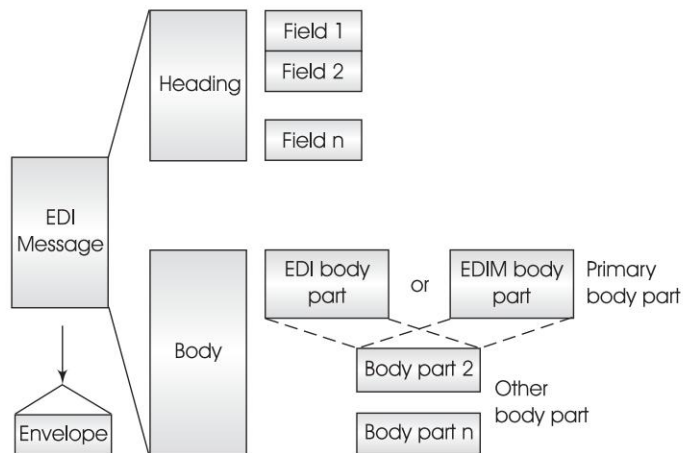


Fig. 7.4 X.435 EDI message structure

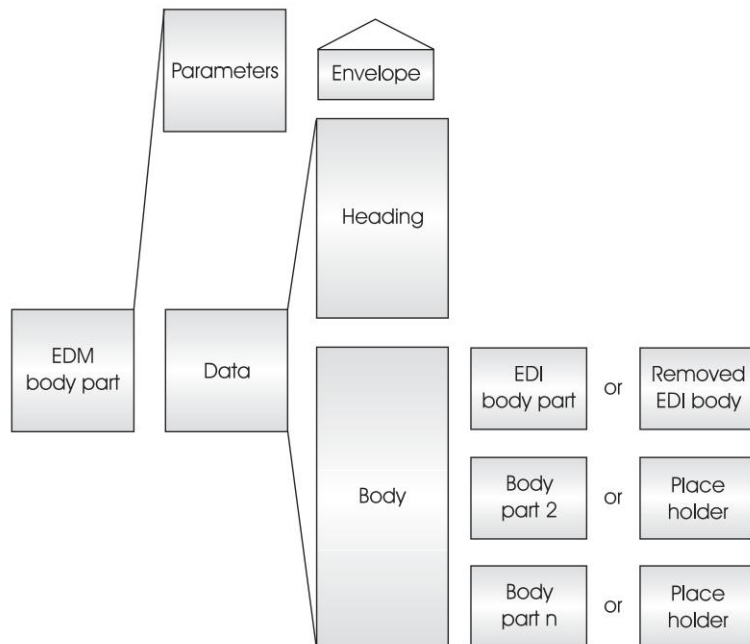
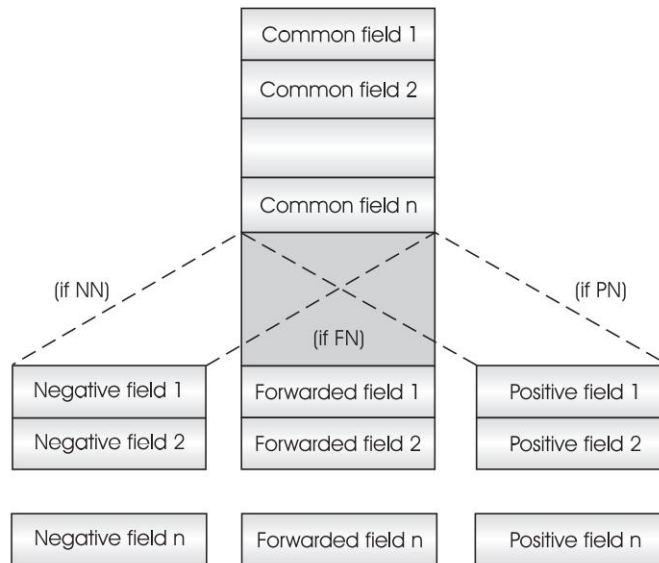


Fig. 7.5 X.435 EDIM body part structure

the EDI interchange syntax. For convenience, X.435 refers to data elements defined in the EDIFACT-UNB segment. No loss of generality is implied, since other EDI standards have comparable header segments and data elements.

X.400 message handling systems provide for generation of delivery/ non-delivery reports. A delivery report, as the name suggests, only informs the sender that the message has been delivered to the recipient's mailbox. No information is received by the sender as to whether the recipient has retrieved the message and taken responsibility or not. These delivery reports are, therefore, not of much use when the messages that are being sent over X.400 are business documents being exchanged between business applications of different organisations.

In order to counter this problem, the X.435 recommendations introduced the concept of EDI notifications. Three types of notifications are defined (Fig. 7.6). They include:



➡ **Fig. 7.6** X.435 EDI notification structure

- Positive Notification (PN)—A PN is sent by the recipient User Agent (UA) when it has accepted responsibility for the EDI message received.
- Negative Notification (NN)—An NN is sent when the recipient UA determines that it can neither accept responsibility, nor forward the EDI message, along with the EDI notification request contained in it, to another UA.
- Forwarded Notification (FN)—An FN is sent when the recipient UA determines that it cannot accept responsibility for the EDI message and decides to forward the message, along with the EDI notification request contained in it, to another UA.

The common fields contained in each of these notifications include.

- Identification of the original EDIM to which this notification pertains
- ORName of the UA which is generating this notification
- ORName of the first recipient in a forwarding chain
- Time of notification generation.

These notifications are sent by the recipient UA if and only if requested for by the originating UA.



7.4 EDI Implementation Issues

At an entry level implementation of EDI, paper forms could be replaced by electronic forms. These forms are filled within the organisation and sent over a communication network to the recipient. However, in this approach, data is not directly picked up from the computerised in-house business application. The consequent re-entry of data negates the realisation of a major benefit of EDI.

For a solution in which all benefits of EDI are achieved, EDI should be integrated with the business applications. Or, there could be a Front-end processor (FEP) taking care of translation

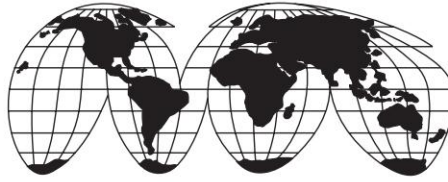
and communication. This FEP could be connected over a LAN to the computer system on which the organisation's business application is running. Information could then be downloaded and uploaded between the FEP and the computer. This approach ensures the smooth flow of data between business processes and the EDI module. Full-blown, integrated EDI is a hands-off process that relies on computers to do the work. Preparing and processing purchase orders is a very routine matter in any company. Computers handle these mundane tasks, thereby freeing the staff to take on more creative and profitable tasks, such as strategically managing operations and promoting new business opportunities. This is what EDI was meant to do. With an integrated approach, for every purchase order received, the appropriate functional areas are automatically updated. This updating might include sales figures, inventory management, accounts receivable, general ledger accounting, and so on. Integration allows you to reap the full benefits of EDI implementation facilitating not only cost savings, but also improved work processes, easily accessible and better quality information, and improved customer responsiveness.



7.5 Legal Aspects

In case of paper documents, certain legal terms and conditions are printed on the back of each form. In case of EDI, the same information is accounted for in what is known as a trading partner agreement. The laws of the land also have to be suitably modified to cater to this new electronic environment for conducting business transactions.

These and related issues concerning the legal aspects of electronic commerce have been dealt with in Chapter 13.



Chapter 8

The UN/EDIFACT Standard



8.1 Introduction

As has been defined in Chapter 7, EDI is the electronic exchange of business documents in a standard, computer-processable, universally accepted format between trading partners. These documents are generated by the computerised business application of one trading partner, transmitted over a computer network and when received by the intended recipient, the document is directly handled by the corresponding computerised business application at that end thus eliminating the need for manual intervention.

In a manual document-processing environment, invoices are received by a customer from a number of suppliers. Each supplier's invoice might be presented in a totally different format, yet the accountant is able to decipher the content from all these varied presentations. In an EDI environment however, when the documents are being received by a computer and not a person, the computer has to be informed well in advance about the type of information and the format in which it is being presented. This is where EDI standards come in, to provide the structured information that is one of the key components of an EDI system.

The history of EDI standards has already been covered in Chapter 7. In this chapter we focus on what has come to be

recognised as the international standard for EDI messages—the United Nations Standards for EDI for Administration Commerce and Transport (UN/ EDIFACT). They comprise a set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data, and in particular that related to trade in goods and services between independent, computerised information systems.

By 1985, two data standards for EDI that had been extensively used were the American National Standards Institute's ANSI X12 and the Guidelines for Trade Data Interchange—GTDI—in Europe. However, since these two standards were not meeting the requirements of international trade, a committee was set up by the United Nations to formulate an international standard for EDI.

UN/ EDIFACT sets out a new 'language' for document interchange, and as with any other language, this too has a syntax or grammar. This syntax is specified by the International Standard Organization's ISO 9735 standard. The vocabulary of 'words' for UN/ EDIFACT is contained in the UNTDED—the UN Trade Data Elements Dictionary. These data elements are logically grouped into 'sentences' and 'paragraphs' to build up standard formats for different business documents.

An UN/ EDIFACT message is a collection of data values relating to business documents. About 150 standard message formats have been developed within UN/ EDIFACT covering all three areas:

Administration: messages such as Customs Declarations, Legal Administration request/ response, job applications, etc.

Commerce: Tender, Purchase Order, Invoice, Payment Order, Remittance Advice, etc.

Transport: Transport Booking, Multimodal Status Report, Arrival Notice, etc.



8.2 An EDIFACT Message

An EDIFACT *message* is a collection of information that is exchanged to convey information related to a specific transaction between the partners engaged in EDI. Messages are composed of logically-grouped segments required for the type of message transaction covered. The term *message* is also known in other standards as a Transaction Set. A list of these messages as in Directory D.97B is appended at Appendix 1.

A *segment* is the intermediate unit of information in a message. A segment consists of a predefined set of functionally-related data elements which are identified by their sequential positions within the set. A segment begins with a segment identifier, a unique 3-alphabetic upper-case code which uniquely identifies each segment, and ends with a segment terminator. For example, the BGM tag identifies the segment as 'Beginning of Message' and the NAD tag identifies a 'Name And Address' segment (Table 8.1).

The status of a segment in a specific message type may be:

- *Mandatory (M)*—this segment must be used in the message.
- *Conditional (C)*—this segment will be used in the message depending on certain conditions.

Segments have specific places in a message and the same segment type may occur more than once in a message. Segments may occur in any of the following three sections of the message:

- *Header Section*—a segment occurring in this section relates to the entire message.
- *Detail Section*—a segment occurring in this section relates to the detail information only and will override any similar specification in the header section.
- *Summary Section*—only segments containing totals or control information may occur in the summary section, e.g. invoice totals, overall discount, etc.

Table 8.1 The NAD Segment

NAD	M	I			Name and address
3035	PARTY QUALIFIER		AN..3	M	[D] Code giving specific meaning to a party.
C082	PARTY IDENTIFICATION DETAILS				[D] Identification of a transaction party by code.
3039	Party id. identification		AN..35	M	[D] Code identifying a party involved in a transaction. User or association defined code. May be used in combination with 1131/3055.
1131	Code list qualifier		AN..3	C	[D] Identification of a code list.
3055	Code list responsible agency, coded		AN..3	C	[D] Code identifying the agency responsible for a code list.
C058	NAME AND ADDRESS			C	[D] Unstructured name and address: one to five lines.
3124	Name and address line		AN..35	M	[D] Free form name and address description.
3124	Name and address line		AN..35	C	[D] Free form name and address description.
3124	Name and address line		AN..35	C	[D] Free form name and address description.
3124	Name and address line		AN..35	C	[D] Free form name and address description.
3124	Name and address line		AN..35	C	[D] Free form name and address description.
C080	PARTY NAME			C	[D] Identification of a transaction party by name, one to five lines. Party name may be formatted.
3036	Party name		AN..35	M	[D] Name of a party involved in a transaction.
3036	Party name		AN..35	C	[D] Name of a party involved in a transaction.
3036	Party name		AN..35	C	[D] Name of a party involved in a transaction.

(Contd)

Table 8.1 (Contd)

NAD	M	I			Name and address
3036	Party name		AN..35	C	[D] Name of a party involved in a transaction.
3036	Party name		AN..35	C	[D] Name of a party involved in a transaction.
3045	Party name format, coded		AN..3	C	[D] Specification of the representation of a party name.
C059	STREET			C	[D] Street address and/or PO Box number in a structured address: one to three lines.
3042	Street and number/ p.o box		AN..35	M	[D] Street and number in plain language, or Post Office Box No.
3042	Street and number/ p.o box		AN..35	C	[D] Street and number in plain language, or Post Office Box No.
3042	Street and number/ p.o box		AN..35	C	[D] Street and number in plain language, or Post Office Box No.
3042	Street and number/ p.o box		AN..35	C	[D] Street and number in plain language, or Post Office Box No.
3164	CITY NAME		AN..35	C	[D] Name of a city (a town, a village) for addressing purposes.
3229	COUNTRY SUB-ENTITY IDENTIFICATION		AN..9	C	[D] Identification of the name of sub-entities (state, province) defined by appropriate governmental agencies. Use code defined by appropriate national authority.
3251	POSTCODE IDENTIFICATION		AN..9	C	[D] Code defining postal zones or addresses. Use code defined by appropriate national authority.
3207	COUNTRY, CODED		AN..3	C	[D] Identification of the name of a country or other geographical entity as specified in ISO 3166. Use ISO 3166 two alpha country code.

Some segments may be repeated a number of times at their specific locations in the message structure. Examples of the status and maximum number of repetitions of some segments are indicated in the Segment Table under the headings for the Purchase Order message contained in Appendix 2 (Fig. A2.3).

Within a message, specific groups of functionally-related segments may be repeated; these segment groups are referred to as loops. The maximum number of repetitions of a particular loop at a specific location is indicated in the message Segment Table.

A group of repeating segments (a loop) may be nested within other loops, provided that the inner loop terminates before any outer loop terminates.

A *data element* is the smallest unit of information in a segment. Its description and usage are defined in the UN/ EDIFACT Data Element Directory (EDED). Two or more data elements may be grouped together to form a *composite data element*. The data elements forming a composite data element are data elements in their own right and are included in UN Trade Data Elements Directory (UNTDDED). They are referred to as components in the Composite Data Elements Directory (CDED). The use of data elements in a segment is defined in the UN/ EDIFACT Data Segment Directory.

The status of a data element in a segment may be:

- *Mandatory*—this data element must be used in the segment.
- *Conditional*—this data element will be used in the segment depending on certain conditions.

The segments in the Segment Directory are designed for use in a wide range of message types. This means that in some message types one or more conditional data elements or composite data elements in a segment may not be used.

A data element whose function is to give a more precise meaning to another data element is referred to as a *qualifier*. The data value of a qualifier is a code taken from its associated code set. The code sets are part of the UN/ EDIFACT Code Lists.

The following UNTDED notation is used to indicate the data type and length of each data element (Table 8.2):

Table 8.2

a3	3 alphabetic characters, fixed length
n6	6 numeric characters (numbers), fixed length
an5	5 alphanumeric characters, fixed length
a..6	upto 6 alphabetic characters
an..35	upto 35 alphanumeric characters
n..9	upto 9 numeric characters (number)

In addition, the following notation (Table 8.3) is used:

Table 8.3**Datatype**

a	alphabetic
n	numeric
an	alphanumeric
id	alphabetic, numeric or alphanumeric identifier

Segments are functionally defined to be applicable over a wide range of messages. However, restrictions may apply according to the function of the segment within the structure.

A United Nations Standard Message (UNSM) is designed to be used in, and across different industries and applications for both national and international exchange. To meet these requirements, several segments and segment groups are defined as conditional. It is important, therefore, that users intending to use the message, first study each conditional segment and segment group to decide which are necessary for their particular application. Each UNSM is identified by a 6-character code,

such as INVOIC for Invoice document, ORDERS for Purchase Orders and REMADV for Remittance Advice.

To illustrate message structure there will be both a branching diagram and a Segment Table, with loops showing the segments in the message type, their sequence, status, repetitions allowed, nestings and groupings. (An example of a Segment Table representation is provided in Appendix 2. Figure A2.3 for the Purchase Order message.)

In the branching diagram, the sequence of the segments is top-to-bottom and left-to-right. A segment is indicated by its three-letter tag and underneath it is its status, Mandatory(M) or Conditional(C), and allowed number of occurrences. Groups of segments are represented by boxes showing a unique group number, its status and the maximum number of allowed occurrences of the group. All segments and groups within a group box, belong to that group.

In the Segment Table, the segments are listed in the order of occurrence in the message. They are identified by their tags and names. In addition, the status M or C is stated together with the number of times each may be repeated at that occurrence. A mandatory segment must appear at least once. Each segment group has a number, and an indication of M or C together with a number indicating the number of times the group may appear within the message or within another group. In the Segment Table, loop lines indicate the segments within the group, its beginning and its end. A segment group must contain at least one mandatory segment which must be the first segment in the group.

Of the many messages that have been standardised, a United Nations Standard Message (UNSM) is one which:

- has been registered, published, and which is maintained by the United Nations Economic Commission for Europe;
- has the values contained in the Controlling Agency, Message Type, Message Version Number and Message Release Number fields (the requirements for the use of which are

specified in ISO 9735), allocated and controlled by the UN/ECE;

- always has the code value 'UN' in the Controlling Agency field.

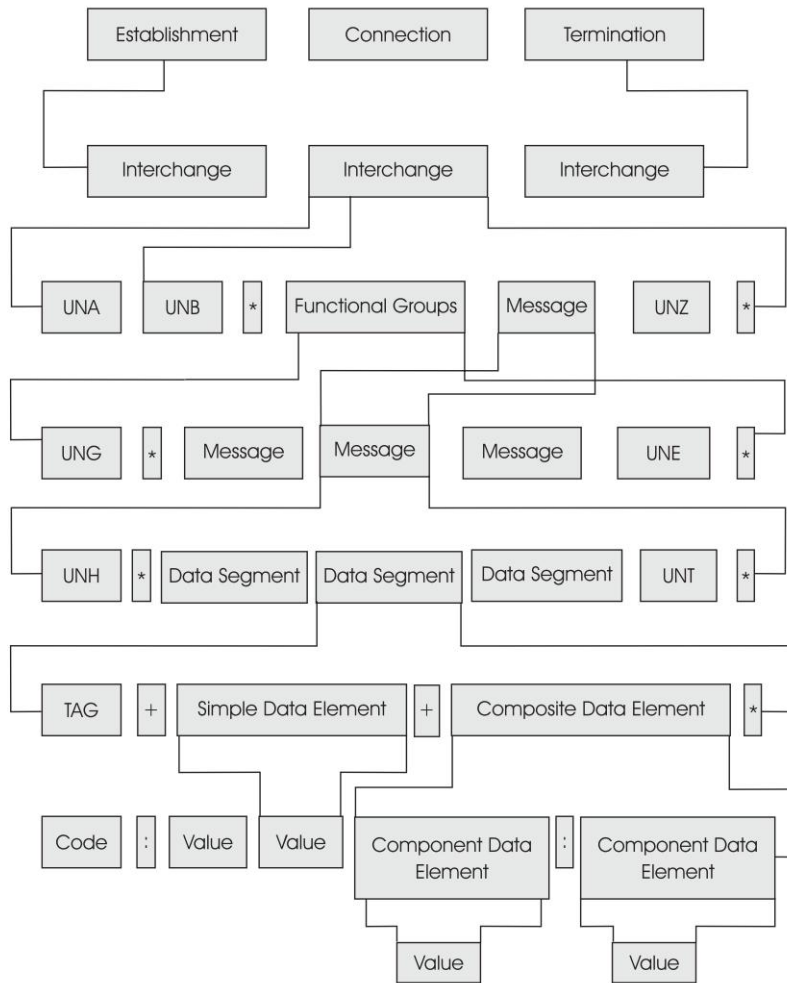
A sub-set of a UNSM is a message which is directly derived from an approved UNSM, has the same function as the UNSM from which it is derived, and which contains all of the groups and segments defined as having a mandatory status within the message, and the mandatory data elements within them. There can be no change to the status, order or content of the groups, segments, and composite data elements and data elements contained within the segments. Although many UNSMs contain Conditional Groups of segments which may contain one or more mandatory segments, providing the complete conditional group is omitted from the sub-set, this does not break the rule regarding the inclusion of mandatory segments. A sub-set of a UNSM therefore:

- does not change the status, order or content of the segments, composite data elements and data elements in the conditional segments chosen for use from the UNSM;
- does not add any segments, composite data elements or data elements to the message;
- contains the identical values specified for use in the Message Type, Controlling Agency, Message Version Number and Message Release Number fields, as are specified for the UNSM from which the sub-set is derived.



8.3 Interchange Structure

The basic unit of communication between trading partners, as defined by UN/EDIFACT is an *interchange*. Figure 8.1 shows the structure of an EDIFACT interchange. An interchange consists of functional groups of messages. Each functional group contains one or more messages of the same type. A collection of segments ('sentences') makes up a message ('paragraph'), with



➡ **Fig. 8.1** *Structure of an UN/EDIFACT Interchange*

each segment comprising data elements ('words')—both composite and otherwise. The special delimiters which have been used as separators between data elements, component data elements and segments are specified in a special service segment called the Service String Advice. Each segment begins with a tag—a 3-character code which identifies the segment. The 3-character strings beginning with 'UN' are tags for control segments in the interchange.

In an interchange the Service String Advice, identified by the tag, 'UNA', and the service/ control segments appear in the following order (Table 8.4).

Table 8.4

Service String Advice	UNA	Conditional
Interchange Header	UNB	Mandatory
Functional Group Header	UNG	Conditional
Message Header	UNH	Mandatory
User Data Segments		As required
Message Trailer	UNT	Mandatory
Functional Group Trailer	UNE	Conditional
Interchange Trailer	UNZ	Mandatory

In addition to the above service segments, the service segment UNS can, when required, be used to divide a message into sections. There may be several functional groups or messages within an interchange and several messages within a functional group.

A *connection* contains one or more interchanges. The technical protocols for establishment, maintenance and termination, etc. are not part of the UN/ EDIFACT standard. Table 8.5 below shows what the parts of an *interchange* contain.

Table 8.5

An *interchange* contains:

UNA — Service string advice, if used

UNB — Interchange header

Either only functional groups, if used, or only messages

UNZ — Interchange trailer

(Contd)

Table 8.5 (Contd)

A <i>functional group</i> contains
UNG — Functional group header; Messages of the same type
UNE — Functional group trailer
A <i>message</i> contains:
UNH — Message header
— Data segments
UNT — Message trailer
A <i>segment</i> contains:
— A segment TAG
— Simple data elements or
— Composite data elements
— or both as applicable
A <i>segment tag</i> contains:
— a segment code and, if explicit indication, repeating and nesting value(s).
A <i>simple data element</i> contains:
— single data element value
A <i>composite data element</i> contains:
— component data elements
A <i>component data element</i> contains:
— a single data element value.
UNA, UNB, UNZ, UNG, UNE, UNH and UNT are service segments



8.4 UN/EDIFACT Message Directories

It is essential that messages should be capable of being identified in relation to the current version of the directory from which they are derived, i.e. the code lists, data elements, composite data elements and segments.

Whenever a new Standard directory set is published, it contains the message specifications for all registered UNSMs and their supporting segments, composites, data elements and codes.

Draft directory sets contain all Status 1 (Draft Recommendation) messages and all Status 2 (UNSM) messages in their latest

form and the supporting segments, composites, data elements and codes.

A directory is identified by an issue number, allocated and controlled under UN/ EDIFACT procedures. The issue number is a single character indicating whether the directory contains Draft or Standard material (S or D) followed by a period separator, followed by the last two digits of the year in which the directory is agreed upon, followed by a sequential alpha character assigned by the UN/ ECE. This sequential alpha character begins with A at the start of each year and is incremented if more than one directory of the same type (S or D) is published during the same year. For example, D.96A, D.96B and so on.

When a document related to a UNSM under development reaches a Status of 2 (i.e. the status of 'Recommendation'), and the UNSM is agreed upon and published in a new issue of UN Trade Interchange Directory (UNTDID), i.e. in the Standard Directory, the values in the following fields of the UNH/ UNG segments used for the message (or a sub-set of the message) will be:

- *Controlling Agency (data element 0051)*—always the two characters 'UN';
- *Message Version Number (data element 0052)*—always 'S' when published in a Standard Directory;
- *Message Release Number (data element 0054)*—The last two digits in the year of agreement followed by a single, sequential alpha character assigned by the UN that starts with A at the beginning of each year and is incremented if more than one directory of the same type (S or D) is published in the same year.

When a document related to a UNSM under development reaches a status of 1 (i.e. the status of 'Draft Recommendation'), and is agreed upon and published in a new issue of the Draft directory, the values in the following fields of the UNH/ UNG

segments used for the message (or a sub-set of the message) will be:

- *Controlling Agency (data element 0051)*—always the two characters ‘UN’.
- *Message Version Number (data element 0052)*—always ‘D’.
- *Message Release Number (data element 0054)*—the last two digits in the year of agreement followed by a single, sequential alpha character assigned by the UN that starts with A at the beginning of each year and is incremented if more than one directory of the same type (S or D) is published in the same year.

If users wish to test messages (or sub-sets of messages) which have not yet reached the ‘Draft for formal trial’ stage (i.e. messages under development which have a document status of ‘O’ or ‘P’), a different procedure must be followed.

The full procedures for the identification of documents containing messages under development are contained in the UN paper WP.4/ GE.1/ R.785. Such documents will have a Status of ‘O’, plus a ‘Revision’ number controlled by the Rapporteur’s Team (RT) where the request for the new UNSM originated.

Users wishing to test such messages must always use a Message Version number of zero, a Message Release number equivalent to the Revision number of the document revision upon which they are basing their test, and a Controlling Agency code of ‘RT’. (Users should not test such messages until they have been passed by the relevant Technical Assessment Group of the RT where the request for the message originated. Further, users are strongly recommended to delay testing of messages under development until the point where the development is fairly stable, and even then, they must be aware that the message content may well change before it reaches the status of ‘Draft for formal trial’.) Table 8.6 gives an example of one type of message.

Table 8.6

Example: (Document Status 'O' or 'P')		
S009	MESSAGE IDENTIFIER	
* 0065	Message type	: NEWMSG
0052	Message version number	: O
0054	Message release number	: 'n'
0051	Controlling agency	: RT
0057	Association assigned code	: (not used)

where 'n' in the release number field is equal to the Revision number of the development document used as the basis of the message being tested.

United Nations Standard Messages are structured in such a way that they can be used by companies and organisations in many different industries. For example, the invoice UNSM contains data elements and segments which are in common use in the majority of invoicing applications. Other data elements and segments specified for use in the message have a more restricted application, and will probably be required by only a few industry applications. Thus, in the vast majority of cases, industries will choose and become responsible for specific industry-related sub-sets from the total message structure.

However, still abiding by this principle, users may wish to go beyond the standard sub-set definition, and for reasons of integrity, agree between a group of participants that certain data elements and/ or segments which are conditional in a UNSM should always be required in their application. In choosing to go beyond the true sub-set definition set out above, users must bear in mind that to comply with the spirit of sub-sets, any sub-set must always be more restrictive than its parent UNSM.

To provide a unique identification for any particular subset of a UNSM, users may wish to assign a code for use in the

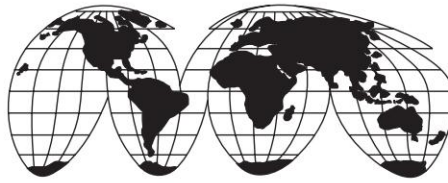
‘Association assigned code’ field of the UNH and/ or UNG segments. Further, if it is considered that there may be a problem in assigning a code which may be duplicated by another group of users, it is suggested that the local Rapporteur’s Team be consulted regarding the allocation of a code value.

As UNSMs are used by more industries, it is quite likely that some messages will be found not to cover some of the specific requirements of those industries. To provide these requirements so that the messages can be used, immediate changes to (or additions of) segments and elements may be necessary by use of the official UN/ EDIFACT ‘Change Request’ procedures.

Since the standards maintenance time-scales may delay the implementation of the required modifications to the UNSM for some time, users may wish to implement the changes immediately so that the message can be used in their application.

In order to identify the amended message (which then is not a UNSM) during the interim period, the user group concerned should consider including an appropriate code in the ‘Association assigned code’ field of the UNH and/ or UNG segments. Where it is thought that there may be problems of duplicated Association assigned code values, the local Rapporteur’s Team should be consulted regarding the allocation of a code value.

As an alternative, in order to identify the group of users requesting the amendments to the UNSM, in the interim period of use of the message, the ‘Controlling Agency’ data element should be used for this purpose.



Chapter 9

The Internet and Extranets



9.1 E-Commerce

The Internet and the web have revolutionised commerce and created new paradigms. The new business paradigm is based on the virtual corporation which has come into being through a combination of intranets and extranets. Universal access to information, enabled by the Internet, intranet and extranet, is at the heart of new business models for e-commerce. The limitations of conducting e-commerce tasks across LANs and WANs, with very little interaction between department functions, in a company no longer exist. Today, an enterprise is an internetworking organisation. The following three types of e-commerce, supported by networks, have emerged:

- Business to consumer
- Business to business
- Internal procurement

9.1.1 Business-to-Consumer E-Commerce

Electronic malls and virtual storefronts allow individual consumers to browse for products and shop by using credit cards—more like an extension of catalogue shopping, through mail order and telephone ordering by using credit cards for

making payments. This form of e-commerce is Internet-based, with unrestricted access to consumers. Credit card payments have to be secured against unauthorised access by intruders on public networks.

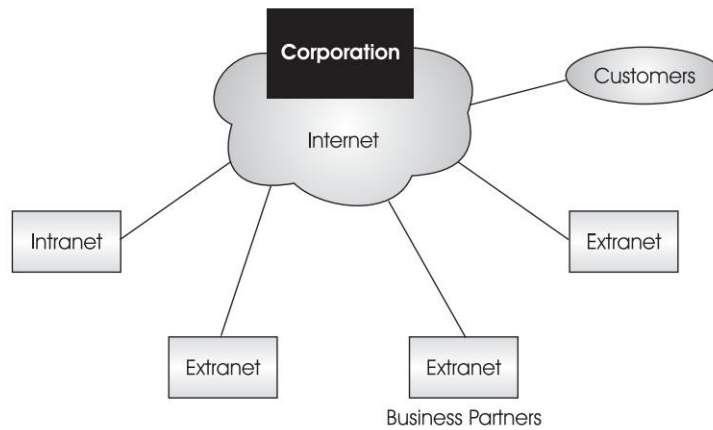
9.1.2 Business-to-Business E-Commerce

This type of e-commerce comprises the bulk of commerce conducted over networks—as high as 70 percent. Business-to-business procurement and fulfilment including financial transactions have traditionally been conducted over private networks. This segment of e-commerce drives extranets. It is restricted to business partners and uses secure procedures based on firewalls, intrusion detection system, encryption, authentication and authorisation, with payment on pre-determined credit terms.

9.1.3 Internal Procurement

Business transactions which are internal to an enterprise, across its departments and subsidiaries, also come under e-commerce. Internal sales, order processing, intra-company charging and billing, and funds transfer for accounting purposes are some of the transactions which can be very large and voluminous depending upon the size and nature of a corporation. This can span the entire globe in case of multinationals. Intranets are responding to this challenge of internal procurement.

E-Commerce on the Internet, intranets, and extranets uses the common standard namely, TCP/IP on the internetworked information infrastructure that spans the whole world. EDI capabilities can be added to the existing business applications of organisations, and enabled on the web for e-commerce. Typical commercial EDI transactions on sale-purchase between companies, illustrated earlier in Fig. 7.2, are integrated into e-commerce servers, to seamlessly integrate e-commerce across the boundaries of an organisation, with the internal systems of automated workflow, ERP, etc.



➤ **Fig. 9.1** *Extranet-Intranet-Internet relationship*



9.2 Commerce over the Internet

Commerce over the Internet is conducted essentially in two ways: EDI over the Internet and web-based EDI.

9.2.1 EDI over the Internet

Internet mail is used as a means for transmitting EDI messages. The IETF-MIME (Internet Engineering Task Force—Multipurpose Internet Mail Extensions) specification is used to envelope the EDI data within the e-mail message. With the issues of security, integrity and reliability of the Internet having been addressed, cost-effective solutions have been created by a number of companies.

EDI over the Internet is more flexible, since there is no need for a prior network connection. In this way, more and more firms including smaller firms can exchange EDI messages. EDI networks are typically set up as a hub with spokes; a buyer at the hub conducting business with its suppliers at the spokes, which cannot communicate among themselves. Since the Internet replaces much of this limited network with its own links, which

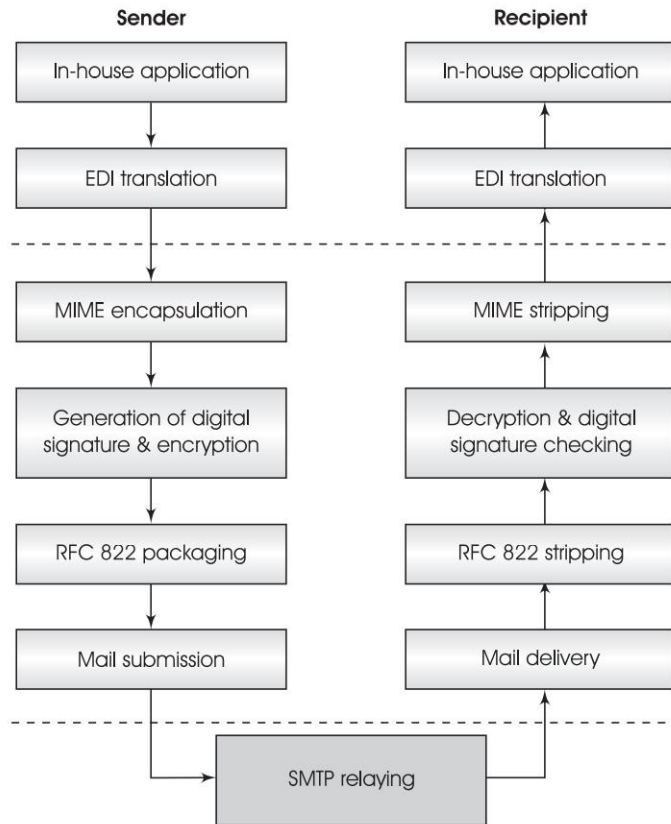
are everywhere, virtual trading communities get formed over it.

Individual trading partners register their businesses as domain names on the Internet. Even if they change network service providers, their own domain names remain the same. EDI messages arrive via the Internet in a particular mailbox under the domain name. Filtering software, based on rules, processes the EDI messages, and issues an auto response for information about setting up a trading partner relationship. Mechanisms are in position that allow the delivery of EDI messages directly to EDI document processing machines without the usual store and forwarding, which greatly simplifies EDI over the Internet. The filtering programs analyse values in MIME headers, and forward messages to appropriate applications. It is through this approach that the EDI messages get directed to EDI translator programs, which retrieve the business interchange for further processing in the recipient's computer system.

The standard e-mail model of Mail Transfer Agent/ User Agent is used to transfer EDI messages via standard exchange protocols. The MIME encoded EDI message has the following parts:

<i>Headers:</i>	Author and Recipient Addresses
	Subject Summary
	Creation Date
	Handling Node Name, etc.
<i>Body:</i>	Structured Body Parts
	Conforming to MIME
	(Text, Different types e.g. voice, graphics)

These are transmitted by using SMTP protocol over the Internet. A typical MIME-encoded EDI message transaction on the Internet, illustrated in Fig. 9.2 may appear as follows:



➡ Fig. 9.2 EDI over Internet

Business Data from Database
 EDI Translator
 MIME Encapsulation
 RFC 822 Packaging
 Mail Submission
 SMTP Relaying
 Mail Delivery
 RFC 822 Stripping
 MIME Stripping
 EDI Translator
 Business Data Recovery

The IETF-EDI specifications define the security standards for EDI messages. The implementation will require secure e-mail software as a layer between the mailer and the mail processing program, which will perform security functions such as encryption/ decryption, digital signatures, receipts, problem handling, etc.

9.2.2 FTP-based Messaging for EDI

FTP is an information transfer method on the Internet. It can be used to exchange EDI messages between trading partners, after appropriate trading partner agreements are put in place. Each trading partner would be allowed FTP access through a login with password. The FTP server contains the EDI messages stored in a file as per conventions defined in the trading partner agreement. The latter includes: FTP login name and password, machines from which login is accepted, security protocols, directory and file naming conventions and file encryption protocols and keys.

9.2.3 Mailing Lists for EDI

Mailing Lists are used for making announcements to a specific group instead of a large Usenet news group. Only those who subscribe to a mailing list receive the intended messages. Vendors might subscribe to a number of lists related to their products or services in order to receive messages, such as EDI RFQs (Request For Quote) sent by potential customers. LISTSERV and LISTPROC are two popular mail list techniques. EDI-L is one such mailing list based on the LISTSERV technique.

9.2.4 Web-based Commerce

The web with its capability to play audio, display graphics, pictures and video, enables Internet users to request information and order products instantly. All this is possible in interactive mode, thus making it an excellent choice for companies

and organisations to display their wares including products and services. It is this capability, coupled with the worldwide reach of the web that has led to the phenomenal growth of commercial sites with Internet registrations (.com addresses). In January 1998, commercial domains registered with InterNIC were 82,01,511. By July 2004, this number had reached 5,33,90,597. The growth of websites continues exponentially.

The commercial websites of companies have web documents that offer useful product information, interactive brochures, news, reviews, etc. The companies can create electronic brochures in colour with graphics, audio and video, and can reach customers worldwide for a few pennies, instead of printing brochures and mailing them at a much higher cost. The electronic malls and stores on the web enable one to see and order merchandise by using a form interface, an electronic form that contains blank boxes for the user to enter information on product codes, quantity ordered, credit card number, etc.

The websites, in turn, are connected to manufacturers' companies/ warehouses, which receive the orders in EDI mode, i.e. there is back-end EDI-based integration of websites. Dell was acknowledged as the largest online commercial seller of computer systems, with \$ 50 million per day in online sales in 2001. Intel was the world's largest e-commerce company by the year 2000, with more than \$1 billion a month in online sales.

Netscape not only sells, but also transmits its products from the web because they are digital. Outside the digital technology sector, e-commerce on the web is being conducted in the following sectors:

- Financial services
- Travel
- Retailing
- Music
- Books
- Cars
- Advertising and marketing
- Pornography

While the services sector is doing comparatively better on the web, retailing on the electronic malls has still not reached a level of profitability. E-Commerce on the Internet is enabling new industry communities to take shape. Steel Authority of India Ltd (SAIL) adopted e-procurement. Initially input materials (consumables) were procured from techno-commercially acceptable bidders through on-line reverse auction. SAIL has initiated steps to create Internet-based e-procurement modules for moving towards complete paperless transaction and conducting the entire procurement process on-line. Pharmabiz.com is a comprehensive portal on the Indian pharmaceuticals industry. PolySort is a web marketplace of the plastics and rubber industries with 550 members. These marketplaces are evolving into communities with the enabling tools of Internet commerce. The web is at the hub now.



9.3 Commerce Over Extranets

An extranet is an extension of an intranet which makes the latter accessible to outside companies or individuals with or without an intranet. It is also defined as a collaborative Internet connection with other companies and business partners. Parts of an intranet are made available to customers or business partners for specific applications. The links between an intranet and its business partners are achieved through TCP/ IP, the standard Internet protocol. The extranet is thus an extended intranet, which isolates business communication from the Internet through secure solutions. Extranets provide the privacy and security of an intranet while retaining the global reach of the Internet.

The key characteristic of an extranet is that it extends the intranet from one location to another across the Internet by securing data flows, using cryptography and authorisation procedures, to another intranet of a business partner. In this way, the intranets of business partners, material suppliers,

financial services, distributors, customers, etc. are connected into extranets through agreements of collaborating parties. The emphasis is on allowing access to authorised groups through strictly controlled mechanisms. This has led to the true proliferation of e-commerce. It is the combination of intranets with extranets which has established the virtual corporation paradigm. This business paradigm is turning out to be critical for e-commerce, as it allows corporations to take advantage of any market opportunity anywhere, anytime, by offering customised services products. E-Commerce is perceived to be a business avenue for reducing the cost of sales and time of marketing, as well as for providing more targeted marketing.

Business-to-business e-commerce is growing on extranets. Companies gain a competitive advantage through speedier transactions and access to newer markets, as also by simplified and faster distribution of information, products and services.

Finally, it is worth noting that extranets do not involve a new technology. Businesses have been trying to develop secure links with trading partners and customers for years. The use of IP to support secure inter-company virtual private networks has created extranets. This does not create any new physical networks. Instead, access privileges and routing tables are overlaid on the existing intranet and the Internet infrastructure. Security of transactions with permitted corporate websites and databases is then enabled on the extranet. In addition to simple commercial transaction of sale-purchase, collaborative activities between business partners on the extranet are enabled at much lower costs than over other networks.

9.3.1 Internet Standards for E-Commerce—XML

Extensible Markup Language (XML) allows the creation of common information formats so that data and its formats can be shared on the World Wide Web, intranets, and elsewhere. Dynamic tagging or marking of text in documents makes it possible to use the resulting marked text in computer

applications. For example, vendors of television sets can agree on a standard way to describe the information about televisions such as screen size, power output, speakers, etc. and then describe the information format using XML.

XML can be used by any individual or group of individuals or organisations which want to share information in a consistent way. A formal recommendation for XML has been issued by the World Wide Web Consortium (W3C). XML is similar to the language of today's web pages, HTML. Both XML and HTML contain markup symbols to describe data. HTML describes the presentation of the contents of web pages, which consist mainly of text and graphic images. HTML only defines how the data is to be displayed and interacted with.

On the other hand, XML describes the content in terms of the data that is being described. It contains no indication of how the data is to be displayed. For example, a `<SCREENSIZE>` could indicate that the data that follows it is the size of the television screen. These are known as tags similar to the HTML world. Tags can be defined for different sectors of industry and users.

XML is 'extensible' because, unlike HTML, in the case of XML, the markup symbols are unlimited and self-defining. XML is a simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML)—the standard for creating document structures.

Almost all new software from Netscape, Microsoft, IBM and others are enabled to use XML. Most e-commerce/ EDI product manufacturers are also addressing this issue to make their products XML-enabled. XML can be used not only for the transmission of data from server to browser, but also for passing data from application to application. New tags that are created can be understood by all browsers with XML parsers.

The challenge lies in creating standards for XML tags. Mapping now needs to be handled between EDI messages and XML documents. The existing base of EDI directories can be used for

names and codes instead of generating a fresh set of tags for XML directories. A sample XML document is given below—

```
<lists xmlns="http://tvsets.com/products"
xmlns:it="http://tvsets.com/itinerary">
  <product model="A1334" size="21" type="standard">
    <it:itinerary>
      <it:sold>120</it:sold>
      <it:onhold>45</it:onhold>
      <it:returned>10</it:returned>
    </it:itinerary>
  </product>
  <product model="B2345" size="29" type="FlatScrn">
    <it:itinerary>
      <it:sold>283</it:sold>
      <it:onhold>232</it:onhold>
      <it:returned>23</it:returned>
    </it:itinerary>
  </product>
  <product model="A6734" size="36" type="Flatscrn">
    <it:itinerary>
      <it:sold>342</it:sold>
      <it:onhold>54</it:onhold>
      <it:returned>5</it:returned>
    </it:itinerary>
  </product>
</lists>
```

 **Fig. 9.3** *Sample XML document*

The above illustrates a simple product catalog with details like product model, size and type of product, all of which are in the `http://tvsets.com/products` namespace. Also included is itinerary information on what has been sold, what is on hold, and what has been returned, which are in the `http://deltabis.com/itinerary` namespace. An XML namespace is a collection of names, identified by URI references, which are used in XML documents as element types and attribute names.

Data about data can be used to describe websites or describe a collection of related pages. With XML content markup,

queries are more likely to retrieve relevant files due to contextual information. Search engines can retrieve a specific portion of a file; they can also be much faster if the added context eliminates numerous irrelevant matches.

XML enables client-side data manipulation—the user selects one, several, or all records, sorts by different attributes, switches to graphical view, etc. without requesting data from the server each time. Similarly, the same data can be presented differently, perhaps as a sub-set, depending on the viewer's role with respect to the data (e.g., the accounting department sees more details than the purchaser).

In a three-tier architecture, XML can be used in the middle tier to integrate data from various back-end databases. Style sheets can be used to describe how to render the same data on different devices (monitors, printers, palm pilots, etc.).



9.4 Storage Area Networks

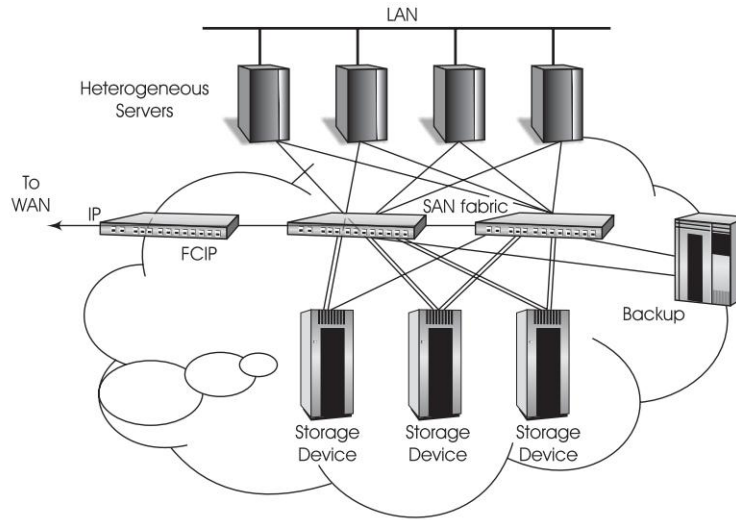
The growth of e-commerce and e-governance has brought in its wake the need for storing and transmitting vast amounts of information. Technologists are engaged in continually devising new products and technologies to meet these challenges.

A Storage Area Network (SAN) is a network of shared storage devices, which contain disks for storing data. All these devices are made available over the network to the servers in an organisation.

SANs provide network storage, which is scalable independent of the associated server systems. A cluster of servers can be connected to the storage sub-system using a switch known as the SAN fabric. The storage sub-system could comprise hard disk arrays and back-up systems, centralising all storage requirements within an organisation.

All storage requirements of an enterprise will then be met by the SAN, which should match, if not exceed, the performance

of storage directly attached to servers, providing security and data availability, as well as transparency to the operating system of the accessing server.



➡ **Fig. 9.4** *Fibre channel storage area network*

Data integrity and availability are critical requirements in SANs. Cyclic Redundancy Checks (CRC) and parity checks are carried out while RAID, redundant data links and processing systems, remote mirroring and tape back-up provide assurance of high availability. Business continuity is facilitated by a gateway called the Fibre Channel over Internet Protocol (FCIP) which allows remote site back-up and disaster recovery.

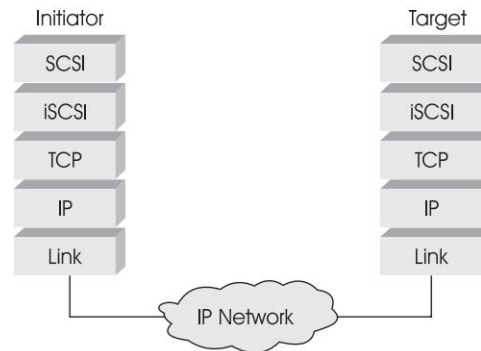
While in directly attached storage systems, the SCSI controller on the host system fulfils the SCSI requests, in a SAN, the Fibre Channel Protocol (FCP) specifies how the SCSI command should be executed over a dedicated fibre communication channel. A fibre channel host bus adapter replaces the SCSI controller in each server to connect to the SAN fabric, which, in turn, is connected to the disk arrays and tape drives.

The performance of SAN depends on the number of channel adapters and the maximum amount and type of disk storage.

Channel adapters connect the storage array to the switch and their number varies with the size of the SAN. High end SANs could have up to 16 channel adapters.

The widespread implementation of this technology has, however, been hampered by the high cost and complexity of deployment of fibre channel SANs.

Internet SCSI or iSCSI—a low cost alternative—specifies how SCSI command can be run over TCP/IP and thus reap many benefits of Storage Area Networking. This protocol was developed by the Internet Engineering Task Force (IETF).

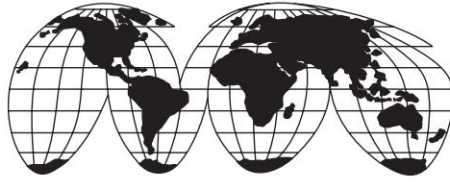


➡ **Fig. 9.5** iSCSI

SCSI commands are encapsulated into Ethernet packets for transport over TCP/IP networks. This enables servers to communicate with shared storage devices over TCP/IP infrastructure using standard SCSI storage commands.

Storage devices or *targets* are connected to the *initiator* in the host system over Ethernet. Initiators could be software drivers bundled with the host operating system or they could be special bus adapter cards on the host system for carrying out iSCSI processing.

iSCSI enables consolidation of storage in environments where costs have to be kept low. It also enables affordable disaster recovery, back-up and secondary storage solutions.



Chapter 10

Identification and Tracking Tools



10.1 The EAN System

To maximise the benefits of Electronic Commerce, in addition to more efficient movement of business documents, it is also extremely important to streamline information regarding the movement of goods that are being traded. While nations are improving their infrastructure for transport of goods, goods need to be tracked and identified so as to provide valuable information to the agencies involved. This has been made possible through the integration of EDI and identification/ tracking tools.

The Universal Product Code (UPC) system set up in the USA by the Uniform Code Council (UCC) was a forerunner to the formation of a council comprising manufacturers and distributors of twelve European countries, in 1974. The council was entrusted with the responsibility for examining the possibility of developing a standard article numbering system, compatible with UPC, for Europe. The European Article Numbering Association (EAN) was established in 1977 as a result of this effort. Steadily, EAN numbers began to be used outside of Europe and as a result, EAN became the International Article Numbering Association, known as EAN International. Presently, there are nearly one million member companies in the world using the

EAN system through an international network of 96 member organisations representing 98 countries.

Numbering Organizations are national associations that provide full EAN system implementation support, to their member companies. Their main responsibilities are:

- allocating numbers;
- providing training on numbering, bar coding and EDI;
- supplying information on the standards and the evolution of the system.

Even though it was first devised for the retail industry, the EAN system caters to commercial and industrial sectors for identifying consumer goods, books, textiles, healthcare products, automotive parts and many other products, services, utilities, transport units and locations. It develops and maintains coding standards for all users, and has the aim of developing a global, multi-sectorial standard with the objective of providing a common language for international trade.

The EAN system consists of the following elements:

- a system for numbering items so that they may be uniquely identified. These include consumer products and services, transport units and locations;
- a system for representing supplementary information such as batch number, date and measurement;
- standard bar codes to represent information so that it can be easily read by computers;
- a set of messages for EDI transactions (EANCOM messages).



10.2 EANCOM

The physical flow of goods using bar codes and the business document flow using EDI are integrated with one another through the use of the EAN label. The information contained in

the EAN label is transmitted using the EANCOM EDI messages. EANCOM, a subset of UN/ EDIFACT messages, is an implementation guideline of the UN/ EDIFACT standard messages. Clear definitions and explanations allow trading partners to exchange commercial documents in a simple, accurate and cost-effective manner. EANCOM messages then become much simpler and accurate as a result of which transmission costs are reduced and more efficient transaction processing is achieved.

EANCOM messages are developed and maintained by EAN and its Numbering Organizations and can be divided into the following categories:

1. *Master Data Messages.* Messages containing data which does not change very frequently. These include information such as names, addresses and production information.
2. *Commercial Transactions Messages.* These cover the entire trading cycle including Quotation, Purchase Order and Transport and Logistics related messages, starting from requests for quote up to the remittance advice that is transmitted on completion of payment.
3. *Report and Planning Messages.* These messages include general trading reports which allow the users to develop business plans. Acknowledgement messages also fall in this category.
4. *General Message.* The General message provides for data transmission in cases for which there is no specific standard message.



10.3 Article Numbering

The EAN Numbering system guarantees unique and unambiguous identification of articles. These numbers can be used by manufacturers, exporters, importers, wholesalers and retailers to communicate information regarding the goods or services

they trade in. Trade items are items which are not sold to consumers through a retail checkout but exchanged between companies. A trade unit may be a single product or a package which is used for storing and shipping.

EAN numbers are:

- unique;
- non-significant i.e. the EAN number in itself does not contain any product information. It is the key to access a database. Specific information on the unit is contained in the database;
- multi-industry and international;
- secure; a check digit in every number guarantees secure data capture.

EAN numbers are structured with 14, 13 or 8 digits as EAN-14, EAN-13 or EAN-8 as shown in Table 10.1 below:

Table 10.1

EAN-14	V123456789012C
EAN-13	0123456789012C
EAN-8	0000001234567C

V: Logistic Variant assigned by the manufacturer for trade items, is a number between 1 and 8 and is used in EAN-14. It is chosen by the manufacturer according to its specific needs for representing a packaging configuration.

C: The last digit is a check digit which serves to check that those preceding have been correctly captured. It is always calculated using the previous digits.

EAN-13 is used to identify retail items, i.e. consumer items sold at the point-of-sale. EAN-14 is used for identifying trade units such as packages where the content items are identical to each other.

The 12 digits in the EAN code (other than the logistic variant and the check digit) has the following general structure (Table 10.2):

Table 10.2

First	Next
3 digits	9 digits
PPP	XXXXXXXXXX
EAN	<i>Company prefix & Item numbers</i>
<i>Prefix</i>	

PPP: EAN International allocates a prefix to the EAN Numbering Organization of a country or region.

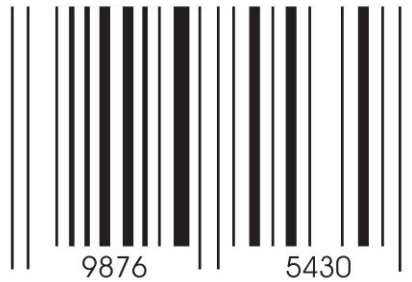
XXXXXXXXXX: The EAN Numbering Organization allocates these 9 digits to member organizations. These 9 digits contain the number allocated to the company as well as the number assigned by the company to an item. Each member company allocates an item number to identify each item. The company can issue these numbers in any order.

Exceptionally, when an item is very small, an 8-digit number, the EAN-8, may be used. Due to the limited capacity of the EAN-8, these numbers are assigned directly by EAN Numbering Organizations for each item.

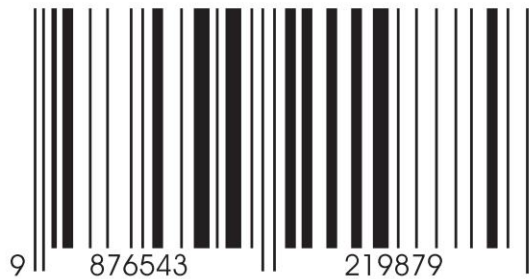


10.4 Bar Coding

EAN numbers which are used for identifying items can be represented by bar codes. Bar codes allow numbers to be encoded in machine-readable form. The data can then be captured automatically, quickly and securely. The numeric value of the code is printed beneath the bar code symbol which can be read omnidirectionally by a scanner. Figures 10.1 and 10.2 depict EAN-13 and EAN-8 numbers represented by bar codes.



➞ **Fig. 10.1** Bar Code representation of EAN-8 number



➞ **Fig. 10.2** Bar Code representation of EAN-13 number

Black bars set against a white background is the safest representation of article numbers to ensure correct scanning. The size and the light margins at each end of the bar code are the other components of a bar code.

The Interleaved Two of Five (ITF) methodology of bar code symbols is especially suited to the inferior quality of packaging materials which are often used for trade items. The ITF symbol can be read both by fixed and portable bi-directional scanners and is used in the shipping and warehousing industry.

The UCC/ EAN-128 Symbology for bar coding uses Application Identifiers (AIs) to define the data structure. AIs are prefixes which define the meaning and format of the data that follows. The UCC/ EAN-128 allows the representation of Application Identifiers. It is, however, not allowed to be used at the point of sale. UCC/ EAN-128 bar codes always contain a special

non-data character known as 'function 1' (FNC 1), which follows the start character of the bar code. It enables scanners and processing software to automatically discriminate between UCC/ EAN-128 and other bar code symbologies, and subsequently only process relevant data. The UCC/ EAN-128 bar code comprises:

- a light margin
- a start character A, B or C
- a FNC 1 character
- data (Application Identifier + data field)
- a symbol check character
- a stop character
- a light margin



10.5 The Serial Shipping Container Code and the EAN Label

Packages created for storing and transporting goods are known as logistic units. Examples are barrels, crates, boxes, containers and pallets. The need for individual logistic units to be identified gave rise to the development of the standard EAN identification number known as the Serial Shipping Container Code (SSCC). The SSCC is a non-significant, fixed length, 18-digit number.

The first digit 'p' of the SSCC contains the packaging indicator while the last digit 'c' is a check digit. The company prefix and the serial reference number come in-between these two digits. The packaging indicator generally has the value '3' which indicates an undefined packaging type. The UCC/ EAN-128 symbology and the associated AIs are used to represent the SSCC. AI 00 identifies that the encoded data that follows is a SSCC.

The EAN label developed by EAN International is a standard for the numbering and bar coding of logistic units. The EAN label combines a worldwide unique reference number, the SSCC with a secure bar code symbology, UCC/ EAN-1210. This

combination allows all participants in the supply chain to use a common, standard solution for their individual tracking and tracing needs.

EAN labels are structured in three sections:

- The top section of the label contains free format information.
- The middle section contains text information comprising human readable interpretations of the bar codes.
- The lowest section includes the bar codes and their associated interpretation.

The physical flow of goods using bar codes and the business document flow using EDI are integrated with one another through the use of the EAN label. The information contained in the EAN label is transmitted using the EANCOM EDI messages.



10.6 EAN Location Numbers

EAN Location Numbers identify any location within a business or organisation. This includes companies, their subsidiaries and divisions, departments and physical units such as rooms. A unique 13-digit identification number with a 3-digit prefix is allocated to each location. The last digit is the check-digit which is calculated based on the first 12 digits and provides security from wrong data capture.

Table 10.3 gives an example of an EAN Location Number 4561234567898 and its components:

Table 10.3

456	234567898	1
<i>EAN</i>	<i>Company prefix & number</i>	<i>Check</i>
<i>Prefix</i>	<i>allocated by the company</i>	<i>Digit</i>

(Contd)

Table 10.3 (Contd)

EAN Prefix:	EAN numbering organization
Company Number:	Assigned by the numbering organization followed by the number allocated by the company to a specific location
Check-digit:	Calculated on the basis of the first 12 digits.

Names, addresses and information about different locations do not have to be included for every transaction. The information is communicated only once between trading partners, entered in the database and queried subsequently by referring to the unique, standard location number.

The EAN location number is recognised by the United Nations working party responsible for UN/ EDIFACT and by the International Standards Organization.



10.7 How it Works: Warehousing Example

The combination of EDI and the SSCC enables a large number of operations to be carried out, including confirmation of order, checking means of transport, verifying order completeness, printing bills of lading, sending a message of delivery and generating an invoice. For example, packaged goods ready for shipment are marked with an SSCC, which is informed to the receiver through the use of the Despatch Advice EDI message. This EANCOM EDI message would contain the SSCC and the EAN article numbers and quantities of the contents of the package. The receiver may know in advance which goods are coming and prepare for their receipt. On receiving the Despatch Advice, it is compared with the original Purchase Order and when the actual goods arrive, the SSCC can be scanned and a comparison

made to check delivery. Inventories may also then be automatically updated.

EAN International operates through a number of decision-making bodies and technical committees in carrying out development, support and promotion activities. Internationally too, EAN maintains very close links with organisations such as the United Nations, International Standards Organization (ISO) and Committee for Standardisation in Europe (CEN) to ensure a robust worldwide numbering system.



10.8 Radio Frequency Identification (RFID)

Product/ item data can be stored and accessed remotely by using Radio Frequency Identification (RFID). Small portable devices, known as RFID tags, are attached to products or containers and can then be used for tracking purposes. Radio frequency transceivers are used to send queries to these RFID tags, which are equipped with antennae. These antennae facilitate the receipt and transmission of queries and answers.

RFID tags can be used to provide identification or location information, or specific information about the product tagged, such as price, colour, date of purchase, etc. Because of its ability to track moving objects, RFID is being widely used in logistics support for supply chain management.

There are two types of RFID tags. *Passive* RFID tags do not have their own power supply. When there is an incoming radio frequency query, it induces a small electrical current which is enough for the tag to prepare and transmit the response. These devices are small enough to be practically invisible with a reading range varying from 10 mm to 5 m. On the other hand, *active* RFID tags have their own power source, longer reading ranges of tens of metres, larger memories and the ability to store additional information sent by the transceiver.

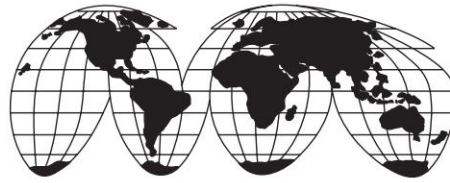
One of the important differences between RFID and bar code technology is that RFID does not need line-of-sight reading. RFID scanning can also be carried out at much greater distances than that for bar codes. RFID is therefore increasingly being used in industry as an alternative identification mechanism as compared to the bar code.

PART IV

Reengineering for Change

- Business Process Reengineering
- Management of Change

Business Process Reengineering discusses the need and methodologies available for looking afresh at the processes within an organization prior to the introduction of new technology tools. Management of Change, brings out the need for, and the ways of managing change as a result of introducing new ways of working.



Chapter 11

Business Process Reengineering



11.1 Introduction

The company in the last decade of the 20th Century was still largely founded on Adam Smith's principle of division of labour based on specialisation, which was enunciated by him in 1776 in his seminal work *The Wealth of Nations*. He saw that the industrial revolution had unleashed technology for increasing worker productivity, thereby reducing the cost of goods by orders of magnitude. The high productivity levels in manufacturing organisations emboldened followers such as Henry Ford, and Alfred Sloan to further refine this principle of specialised task methodology to apply in managing the manufacturing units, and extend the same to all other companies. The division of labour principle was thus extended to management of production, sales, marketing, etc. This led to the creation of specialised departments in organisations, irrespective of whether they were airlines, manufacturing companies, steel mills, retail outlets, accounting firms, computer companies, banking or insurance companies. Alfred Sloan perfected Adam Smith's principle of the division of labour in so far as it applied to management, by creating smaller decentralised divisions with focus on specific activities or units of work. The division executives had only

numbers to look at in order to manage their units of work—sales, market share, inventory levels, orders, profit and loss, production and so forth. These numbers were, and still are taken to be indicators of the performance of a company.

This way of doing business or running a company resulted in the overall processes of manufacturing a product, or delivering a service becoming increasingly complicated. This was entirely due to fragmentation of processes into a large number of tasks, which fell within the domains of different managers or units. Managing a process across a number of divisions, units, and/ or departments thus became more and more difficult. The old processes were modified in a nonsystematic fashion to deal with more and more complex product offerings by companies while accomodating demands for better value by the customer. For example, just-in-time systems were force-fitted with outdated material control and cost accounting systems. This has resulted in the evolution of processes.

Now, what is a process? Hammer and Champy define a business process as a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer.¹ Some of the business processes are: procurement, order fulfillment, product development, customer service and sales. In the existing, traditional departmental/ hierarchical structures of companies, the business processes are often fragmented and obscured. They are divided into a number of tasks which often fall under different departments. There is no one in charge of a process from one end to the last at which stage value is generated for the customer. For example, order fulfillment process includes all state changes from order-to-shipment; service process is from inquiry-to-resolution; sales process is from prospect-to-order; manufacturing process is from procurement-to-shipment; product development process is from concept-to-prototype. Studies have revealed that the order fulfillment process can take several days. In one company it took 11 days. At Motorola, order fulfillment for paging devices took 30 days or more to process. With Business Process

Reengineering (BPR) it was reduced to 28 minutes.² Progressive Insurance reduced the claims settlement from 31 days to four hours after reengineering.³ No wonder, BPR has become one of the important management issues of this decade.

The following forces are driving companies to embrace IT, the related technologies of e-commerce and EDI, including BPR, for sheer survival: the four Cs—Customers, Competition, Change, and Cost. **Customers'** demands and expectations have increased. **Competition** has intensified. IT is being leveraged to provide competitive edge in products and services at lower costs. **Change** characterises products and services. The pace of change has accelerated with liberalisation of economies and deregulation the world over. **Cost** of products and services is falling. These 4 Cs are together creating a new world for business. Companies have to dynamically respond to these forces and constantly adjust to the new parameters through the judicious use of IT, reengineering of their business processes, and aligning their business strategy with organisational infrastructure and IT infrastructure. It is IT which is a key enabler of reengineering. BPR uses IT to radically alter the business processes within organisations to dramatically increase their efficiency and effectiveness.

Now, what is BPR? How does this help organisations achieve such remarkable results? How is it associated with e-commerce and EDI? Why is it not only relevant, but also essential now?

When does reengineering of a process or multiple processes become a necessity? If answers to any of the following questions listed by Cross, Feather and Lynch⁴ is in the affirmative, the time for BPR is now:

- Are your customers demanding more for less?
- Are your competitors likely to provide more for less?
- Can you hand-carry work through the process five times faster than your normal cycle time?
- Have your incremental quality improvement efforts been stalled or been a disappointment?

- Have investments in technology not panned out?
- Are you planning to introduce radically new products and services or serve new markets?
- Are you in danger of becoming unprofitable?
- Have your downsizing and cost-cutting efforts failed to turn the ship around?
- Are you merging or consolidating operations?
- Are your core business processes fragmented and disintegrated?



11.2 Approach to BPR

Induction of e-commerce and EDI has to be used as an opportunity to examine the existing business practices and procedures to move organisations into fully electronic environment. Analysis of business procedures, not only of an organisation, but also of its trading partners, their boundaries and interface, helps in reengineering them from the viewpoint of achieving higher level of efficiency, reduced turnaround time, lower inventory level so that all the agencies, including the customer, benefit from the reengineered process. BPR is considered by some as a different way of management thinking.

Before we define BPR and the methodologies used to realise it, it may be in order to review a couple of examples/ cases where reengineering has resulted in dramatic gains.

Case 1 Ford Motor Co.¹

The Accounts Payable Department of Ford Motor Co. employed more than 500 people. Computerisation for automating some of the existing tasks in the department was estimated to result in 20 percent reduction in manpower. In an effort to reengineer for dramatic improvements, it was realised that BPR was about reengineering a process, and not a department. The process identified for reengineering was **procurement**, with the following stages:

- (a) An internal unit of the company generated a purchase order to a supplier outside the company. Copy sent to Accounts Payable.
- (b) The receiving department received the items against the purchase order from the supplier along with a delivery notice. Accounts Payable received the receiving document from the receiving clerk.
- (c) The supplier sent an invoice to Accounts Payable.

The Accounts Payable Department thus received three documents: purchase order, receiving document, and invoice. If they matched, as was the case in 80 percent transactions, payment was made. If not, enormous amount of time and manpower was utilised in tracing discrepancies and making the payment to the supplier.

The reengineered process is radically different, and is enabled by IT. A company-wide database with terminals connected in all the departments, allows a purchasing unit to enter the order into the system as soon as it is released to the vendor. The receiving department clerk has access to the same database, who on receipt of goods from the supplier, logs into it to ensure that what is being received is as per the purchase order. If yes, he accepts the delivery and directly authorises payment through the system. If not, the consignment is not accepted, and is returned to the supplier. The need for invoice was eliminated.

The reengineered process comes close to eliminating the Accounts Payable department. The number of people were reduced to 125 to handle some exceptional and complicated cases. BPR changed some of the unwritten rules:

From “We pay when we receive the invoice”

To “We pay when we receive the goods”

In the next logical stage of reengineering this rule was taken

To “We pay when we use the goods”

The company would order the parts on the day it required them, but the supplier would keep them ready in his own warehouses. This is the stage of partnership with the supplier of parts, in preference to maintaining multiple sources of supply.

Case 2 France Telecom: Minitel Information Services Project³

In the 1970s, France Telecom expanded its telephone services. More than 10,000 subscribers were added every day in the year 1979. Telephone directories were obsolete everyday, and the operations could respond to inquiries for directory assistance with response time of 15 to 20 minutes. New technologies available at that time allowed the operators to enter the name requested by the customer on a terminal for searching from a centralized directory database, and initiating an automated audio response. It was possible for operators to fulfill directory requests within 15 seconds with this technology.

France Telecom, however, decided to reengineer work through new business processes with IT with an eye on completely new services to enhance its business. It launched the Minitel Information Services Project in early 1980s involving an investment of nearly two billion dollars in building the world's largest packet-switching network. France Telecom designed, procured, and installed some six million terminals free of charge to customers to directly access the directory database. By 1992, more than 16,000 other public information services were made available over the Minitel system generating over two billion dollars in additional revenues.

The range of services offered by France Telecom has potential to transform the French society and economy. New business units are putting together new services: global telephone directory services, videotext based services. This is a case of re-engineering leading to transformation. It can be called a macro reengineering philosophy, which has brought about enterprise-wide transformation.



11.3 Strategic Alignment Model

As noted earlier, it is IT which enables BPR. But it is not enough to improve the internal Information System (IS) of an organisation. One has to examine the IT marketplace, the available technologies, and those just around the corner, and work out plans to integrate them with business, just as France Telecom did, in order to reap manifold gains while introducing re-engineering. We will now discuss the *Strategic Alignment Model (SAM)* due to *Henderson and Venkatraman*⁵, which provides a powerful framework for achieving alignment between business, organisation, and IT strategies. This model is used by the IBM Consulting Group, and is also part of management training in IBM.

In developing the SAM, Henderson and Venkatraman have viewed Business and IT in terms of *strategy* and *infrastructure*. The components of this model are:

- Business Strategy
- IT Strategy
- Business Infrastructure
- IT Infrastructure

SAM due to Henderson and Venkatraman can be pictorially represented as follows:

	Business	IT
Strategy	Business Strategy	IT Strategy
Infrastructure	Business Infrastructure	IT Infrastructure

➞ Fig. 11.1

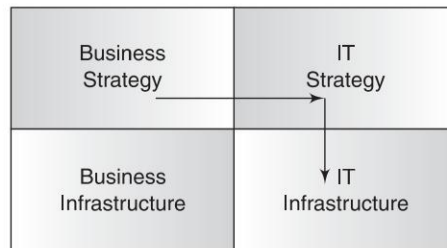
The model proposes to align IT with business by involving any three, or all the four components. Thus there are four

possible scenarios, which are based on dominant alignment perspectives.

1. Business Strategy as the driver: Technology transformation

- *Business Strategy–IT Strategy–IT Infrastructure*

In this perspective, Business Strategy drives the IT Strategy which in turn dictates the required IT Infrastructure and processes. This perspective is not constrained by the current organisational setup. The emphasis is on identifying the best possible IT in the market, and the corresponding internal IT architecture.



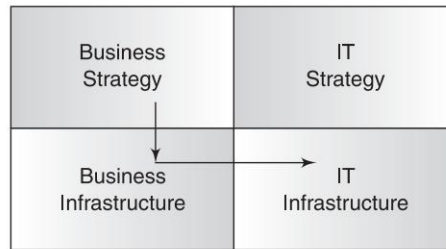
➞ Fig. 11.2

The role of executive management in this perspective is to provide technology vision to suit the chosen business strategy. The performance criteria are based on technology leadership of the firm in the IT marketplace.

2. Business Strategy as the driver: Strategy Execution

- *Business Strategy–Business Infrastructure–IT Infrastructure*

In this perspective, Business strategy drives the Business Infrastructure, which in turn drives the IT Infrastructure. This is the common, hierarchical view of strategic management. The role of management is critical in making this perspective succeed, since the top management has to act as the strategy formulator, whereas the IT manager is the strategy implementor. *This is the traditional BPR model.*



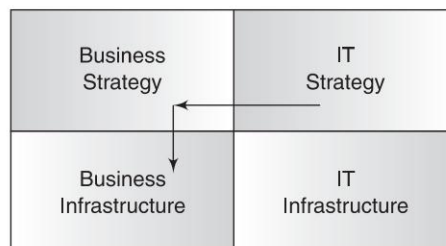
➞ Fig. 11.3

The performance criteria for assessing the IT/ IS function in this perspective are based on financial parameters.

3. IT Strategy as the driver/enabler: Competitive Potential

- *IT Strategy–Business Strategy–Business Infrastructure*

In this perspective, IT Strategy drives the Business Strategy which in turn drives the Business Infrastructure. The organisation tries to exploit emerging IT competencies to impact new products and services, and/ or enter new businesses. In this perspective, business strategy can be adapted via emerging IT capabilities.



➞ Fig. 11.4

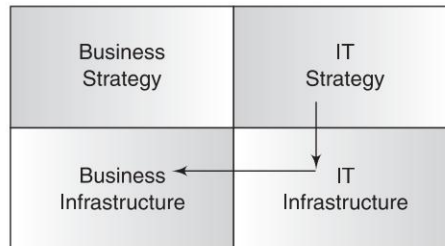
The top management has to act the role of the business visionary. It has to understand and articulate the impact of emerging IT competencies and functionality on the business strategy. The performance criteria in this perspective are based

on qualitative and quantitative measurements such as market share, growth or new product introduction.

4. IT Strategy as the driver/enabler: Service level

- *IT Strategy–IT Infrastructure–Business Infrastructure*

In this perspective, IT Strategy drives the IT Infrastructure, which in turn drives the Business Infrastructure. Here, the role of business strategy is indirect since this approach is expected to provide direction to stimulate customer demand. This perspective is also viewed as necessary to ensure the effective use of IT.



➞ Fig. 11.5

The role of top management in this model is that of prioritizer in allocating the scarce resources. The performance criteria are based on customer satisfaction obtained appropriately.

Henderson and Venkatraman list out the following four criteria which differentiate their SAM from other models:

1. The focus of the IS function shifts from an internal orientation toward one of strategic fit in the IT domain, i.e. existing and/ or emerging technologies in the marketplace.
2. Selection of one of the four alignment perspectives, to suit the business conditions and organisational objectives, is the challenge, rather than the traditional management objective of linking the IS function with business requirements.

3. The diversity of roles of management in different perspectives is highlighted in this model.
4. The criteria for performance assessment in various perspectives are analysed. They expand from cost and service considerations to a larger set involving multiple, strategic and operational goals.

Every organisation has to choose the perspective that is strategic for it. Depending upon its state, the competition, IT deployment within the organisation, IT marketplace, customer profile, etc. appropriate SAM choice needs to be made.



11.4 BPR Methodology

BPR seeks to radically redesign the business processes, and to change the organisational structures in conformance with the new processes. It leverages technology and empowers people. Although the top management commitment is enlisted for BPR, there is resistance to change at all levels. People well entrenched in current practices perceive threat to their position, power and even jobs. BPR projects are, therefore, difficult to implement. Consultants estimate that 70 percent of BPR projects fail⁶. Their analysis reveals that organisations create conditions for success or failure. Following issues are considered the biggest obstacles in the success of reengineering projects:

1. Lack of sustained management commitment and leadership.
2. Unrealistic scope and expectations.
3. Resistance to change.
4. Not helping people think in terms of business processes.
5. Neglecting to align measures and rewards with the new business process thinking.

Does this point towards the need for a BPR Methodology to enhance the chances of success of a reengineering project? There are many who do not favour a methodology; instead intuitive thinking and experience is taken as the guide to start on a clean slate. Many of the successful BPR case studies were intuitive,

primarily because no methodologies existed at the time the projects were done. We will describe two BPR methodologies which have developed since then.

1. Gateway's Rapid Re Methodology for BPR due to Klein.⁷
2. Process Reengineering Life Cycle (PRLC) approach due to Guha, Kettinger, and Teng.⁸

Every approach recommends that the top management must be committed to BPR, and that there should be a BPR Project Team, and that there should be a Steering Committee. Various authors assign responsibility and accountability to all the entities in different proportions. Broadly, the following 'instruments' should carry out the reengineering process:

1. Top management, through a senior executive as the *leader*, who initiates, authorises and motivates the reengineering project.
2. A *BPR Project manager* with responsibility to drive the analysis of specific processes and their reengineering.
3. A *core BPR team* comprising insiders who know the processes inside out, and outsiders who bring general experience and have questioning attitude on the very existence of current procedures. Team members to work full time on studying existing processes, diagnosing problems, and overseeing their redesign and implementation.
4. A *Steering Committee*, which has senior managers as its members, to develop BPR strategy for the organisation and to monitor its progress.
5. Individual *Task Teams* for Analysis, Design and Implementation in specific areas such as customer data collection, benchmarking, workflow design, application design etc.
6. A *reengineering guru* responsible for BPR techniques and tools within the organisation, and for synergizing the effect of various reengineering teams/ processes.

A BPR project involves analysis, design, and implementation phases. The *analysis phase* establishes understanding of customer

requirements, markets, current process flow in the company, benchmarking of best industries practices, target performance objectives. It helps determine the core business processes which are immediate candidates for BPR. This phase also leads towards a first level design specifications. At this stage management's mandate should be reconfirmed on management's expectations and direction for the reengineering project, and constraints placed on the outcome of the project.

The *design phase* of BPR has to deal with design principles in these categories:

Service quality	: design processes as they relate to customer contact
Workflow	: manage flow of work through a series of steps
Workspace	: economic issues and layout options
Continuous improvement	: incorporate continuous learning to improve
Workforce	: keep people in view at design stage of workflow, because only they make it work
Information Technology	: state-of-the-art IT to be kept in view as an enabler of reengineered processes.

The *implementation and transformation phase* of BPR has to plan training, logistics, facilities modifications, and to manage the transition. People have to be carried along by the BPR team through persuasion and the promised gains, in order to minimise their resistance to change.

Modelling and Simulation tools can help model a complex process and predict its performance. A model comprises objects and their relationships, and tries to replicate a real life system. These tools can help in the analysis stage. A business process model, on the other hand, can also be developed by combining a set of local workflow models. Flow of work for one or more

business processes can be detailed as a local workflow model. Workflow tools fall under the category of implementation tools for automating business processes. Analysis and design must lead to delineation of business tasks and their corresponding workflow oriented application system, as part of the business process model. Thus, this amounts to developing a two-stage modelling procedure. Business process modelling identifies business tasks, which in turn are detailed for their domains related requirements for workflow-oriented application systems through the use of workflow modelling. Workflow tools are available for the following four types of flow of work:

- Production Workflow : for back office activities
- Collaborative Workflow : for interactions among users
- Administrative Workflow : for electronic applications, forms, routing etc.
- Ad hoc Workflow : for user determined interactions and routing

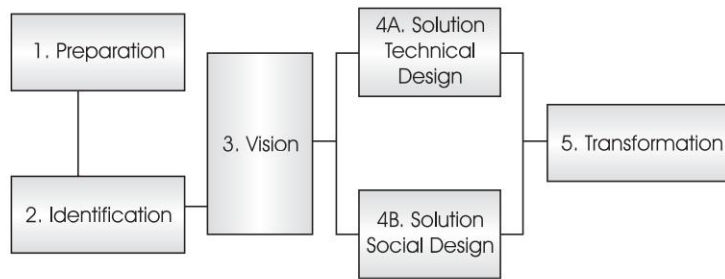
11.4.1 Rapid Re Methodology

This methodology has been taught in American Management Association seminars. There are five stages of the methodology:

1. **Preparation:** Mobilise, organise, and energise the people who are BPR team members. The BPR Project Team should have **insiders** with thorough knowledge of procedures, and **outsiders**, who are creative, experienced people and who have the ability to ask why things are done in a certain way.
2. **Identification:** Develop a Customer-oriented process model of the business. Include sections/ divisions or departments which are customers of other departments.
3. **Vision:** Select the processes to reengineer and formulate, redesign options capable of achieving breakthrough performance.

4. **Solution:** Define the technical and social requirements for the new processes and develop detailed implementation plans.
5. **Transformation:** Implement the reengineering plans.

The methodology lists out 54 tasks under these five stages. These stages are shown in Fig. 11.6. The tasks are given below:



➞ **Fig. 11.6** *Rapid Re methodology*

1. Preparation

- Recognise Need
- Executive Workshop
- Train Team
- Plan Change

2. Identification

- Model Customers
- Define and Measure Performance
- Define Entities
- Model Processes
- Identify Activities
- Extend Process Model
- Map Organisation
- Map Resources
- Prioritise Processes

3. Vision

- Understand Process Structure
- Understand Process Flow

- Identify Value-Adding Activities
- Benchmark Performance
- Determine Performance Drivers
- Estimate Opportunity
- Envision the Ideal (External)
- Envision the Ideal (Internal)
- Integrate Visions
- Define Subvisions

4A. Solution: Technical Design

- Model Entity Relationships
- Re-examine Process Linkages
- Instrument and Informate
- Consolidate Interfaces and Information
- Redefine Alternatives
- Relocate and Retime Controls
- Modularise
- Specify Deployment
- Apply Technology
- Plan Implementation

4B. Solution: Social Design

- Empower Customer Contact Personnel
- Identify Job Characteristic Clusters
- Define Jobs/ Teams
- Define Skills and Staffing Needs
- Specify Management Structure
- Redraw Organisational Boundaries
- Specify Job Changes
- Design Career Paths
- Define Transitional Organisation
- Design Change Management Program
- Design Incentives
- Plan Implementation

5. Transformation

- Complete Business System Design
- Perform Technical Design
- Develop Test and Rollout Plans

- Evaluate Personnel
- Construct System
- Train Staff
- Pilot New Process
- Refine and Transition
- Continuous Improvement

Each project has to customise the tasks to its needs. Not all the tasks may be required, and some of them may have to be grouped. Likewise, Stages 1 and 2 identify all key processes, but BPR may confine to only a few of them related to some divisions or departments, since the organisation may not be willing to undertake company wide reengineering. So, the methodology has to be tailored to the problem environment.

This methodology requires very few tools. Flowcharting template, and paper forms may suffice as manual tools. If required, the following six categories of *BPR tools* can be used in this methodology:

Project Management: Tools for planning, scheduling, budgeting, reporting and tracking projects.

Coordination: Tools like e-mail, bulletin boards, shared spreadsheets, groupware may be used to distribute plans and to communicate updated details of projects.

Modelling: Integrated Computer Aided Software Engineering (CASE) tools are used for integrated analysis, design, and development of computer systems.

Business Process Analysis: CASE tools can be used for business process analysis too. They help in the systematic reduction of a business into its constituent parts and their interactions.

Human Resource Analysis and Design: Some tools may be available for this purpose, basically for tracking candidate position and history.

System Development: These tools help automate the reengineered processes. CASE tools, visual programming,

application development framework, object oriented tools, etc. form part of this category.

Some of the questions which help decide the approach, and the tools that an organisation may take are the following:

- Is the BPR project a pilot or one of a series of similar projects?
- Scope of project—company wide or department specific?
- Who is the sponsor of the project?
- Who are the BPR team members? Their commitment in terms of time and support?
- Role of consultants, if any? Is an Outside Member of BPR Team Providing Methodology or Tools?
- What are Management's expectations of BPR?

11.4.2 Project Re-engineering Life Cycle (PRLC)

The PRLC approach as a BPR methodology identifies the following six stages in a reengineering project:

1. Envision

- Secure management commitment
- Identify reengineering opportunities.
- Identify enabling technologies: IT, EC, EDI, etc.
- Align with corporate strategy (develop a SAM)

2. Initiate

- Organise Reengineering Team
- Set Performance Goals in terms of time, cost, quality, etc.

3. Diagnose

- Document Existing Processes
- Uncover Pathologies

4. Redesign

- Design the New Process
- Design the Human Resources Architecture
- Develop Prototype

- Select an IT Platform
- Explore Alternate Design

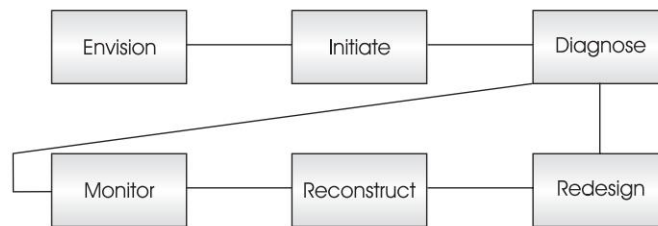
5. Reconstruct

- Install IT
- Reorganise

6. Monitor

- Measure Performance
- Link to Quality Improvement

The PRLC is shown in Fig. 11.7.



➞ **Fig. 11.7** *Six-stage process reengineering life cycle*

Thinking in terms of process types helps in identification of reengineering opportunities. There are three dimensions to a process: entities, objects, activities. Process entities are:

- Interorganisational processes
- Interfunctional processes
- Interpersonal processes

The business processes deal with objects which may be physical or informational. Activities could be classified as operational or managerial. This kind of analysis helps the BPR project identify problems, and to develop a baseline against which to compare new processes.

In diagnosing the processes for reengineering, **documenting the existing process** with the following criteria is of great help.

- Depict the process from start to finish, covering all the departments, users, and external linkages. It may cover several functions.
- Identify all components of the process: IS, human, physical, etc.
- Document the performance of the existing process in terms of customer satisfaction, cycle time, inventory turnover, waiting queues, defect rates, transfer rates, activity time, etc.
- Decompose a large process into a set of subprocesses and assign team members to subteams based on them
- Analyse flow of information, value added at various stages, time required for information processing, moving, and waiting may be recorded to indicate costs incurred.

This diagnosis uncovers the workflow activities, business policies, bureaucracies, and non-value-added roles that impede and fragment the overall effectiveness of a business process.

These findings help redesign a business process to achieve performance improvements in time, cost, productivity, quality, and capital investments. The redesign of process should break ground, and not be bound by existing organisational setup. IT, e-commerce, EDI should be used as enablers of new processes. The following elements may be considered in reengineering processes:

- Breaking unwritten, age old rules of the company.
- Aligning with performance goals.
- Redefining jobs of people around a process, instead of in a department.
- Eliminating hierarchies in favour of self organised teams working in parallel.
- Eliminating work fragmentation, and non-value-added paths.
- Improving productivity through task compression and integration.
- Embedding IT as an enabler to support and enable the reengineered processes.

The system should be put in position immediately through prototyping using CASE tools. Prototypes should be reviewed and evaluated by the reengineering team. The IT platform must be chosen carefully to support the reengineered processes. Communication between corporate systems, decentralised departmental systems, customers coming through various WANs, and the Internet may be essential. LAN based open systems using object-oriented technology, company-wide databases may have to be integrated. Imaging technology, CDROMs, barcoding and tracking systems may have to be incorporated. Transaction processing, decision support systems, data warehousing, EDI and web-based e-commerce systems may also be part of the solution.

The reengineered process, with all the enabling tools, has to be implemented. A new organisational structure consistent with the newly reengineered process should be put in place to empower people for the success of the BPR project. Appropriate training and educational programmes to highlight empowerment, control, and accountability are critical.

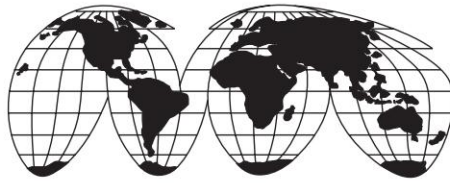
The level of success of the reengineering effort is determined by performance evaluation of the criteria set out as objectives of the project.



References

1. Hammer, Michael and James Champy, *Reengineering Corporation*, Harper Business, 1993.
2. Scherr, A. L., A new approach to business processes, *IBM Systems Journal*, Vol. 32, No. 1, 1993.
3. Davidson, W. H., Beyond reengineering: The three phases of business transformation, *IBM Systems Journal*, Vol. 32, No. 1, 1993.
4. Cross, Kevin F., John J. Feather, and Richard L. Lynch, *Corporate Renaissance: The Art of Reengineering*, Jaico Publishing House, 1997.

5. Henderson, J.C., and N. Venkatraman, Strategic Alignment: Leveraging Information Technology for Transforming Organisation, *IBM Systems Journal*, Vol. 32, No.1, 1993.
6. Bashein, Barbara J., M. Lynne Markus, and Patricia Riley, Preconditions for BPR Success And How to Prevent Failures, *Information Systems Management*, Spring, 1994.
7. Klein, Mark M., Reengineering Methodologies and Tools: Prescription for Enhancing Success, *Information Systems Management*, Spring, 1994.
8. Guha, S., W. J. Kettinger, and J. T. C. Teng, Business Process Reengineering: Building a Comprehensive Methodology, *Information Systems Management*, Spring, 1993.



Chapter 12

Management of Change



12.1 Change Management

Management of change in the wake of induction of e-commerce systems, and reengineered procedures is an important element in realising the targeted levels of performance, productivity, profitability and efficiency in an organisation. Old technology and old procedures have been in position for decades. People are used to them; they are comfortable with them. An organisation is a sociotechnical system comprising of people, technology and procedures which has hitherto revolved around paper documents. Management has been hierarchical, based on departments and divisions. Suddenly, people are asked to convert to teams, organised around business processes, with managers converted to coaches. They are to have an end-to-end view of a given business process, in its entirety, so that the projected benefits of reduced delivery time, better design, reduced transaction cost, etc. actually materialise to justify the use of e-commerce.

Old procedures and old methods of work are ingrained in people. They cannot be changed overnight because people don't like change; the power equilibrium is threatened. The change is not an event, it is a process. It does not happen. Change has to be consciously planned, and made to happen, to deliver the tangible and intangible benefits. It has to be embedded in the

work culture. This requires careful strategy on the part of management which is faced with the challenge of managing complex and dynamic process of change.

Individuals in organisations resist change because of perceived loss of power, threat to skills, end of monopoly of knowledge or power, loss of opportunity, loss of security, status loss, etc. This can be traced to a mental model which has not changed with time. The change strategy has, therefore, to focus on altering the mental model which has become frozen because of lack of insight. It has to draw upon behavioral science, since the issues at work relate to human psychology. Some of the Change Management Strategies are as follows:

1. **Education and communication:** This method which is time consuming is often used when lack of information is the perceived cause of resistance.
2. **Participation and involvement:** The entire department or unit of an organisation is enrolled. More empowerment to the people. It is however time consuming and risky.
3. **Facilitation and support:** This approach is recommended when an organisation suffers from morale decline. It deals with adjustment problems and is expensive.
4. **Manipulation:** This method is used to manage when time is of the essence. It can, however, result in staff reaction.
5. **Explicit coercion:** If the change agent has the power, and time is of the essence, this method works. But one has to be wary of long term consequences.

An analysis of case studies reveals that change methods may be crafted around 'indirection', and change packaged as natural evolution rather than revolution.¹ Decisive change may often require the creation of a pseudo crisis to shock an organisation out of its arrogance or misplaced confidence in its belief systems. Crisis can elevate change acceptance, from a state of extreme doubt and resistance to a state of new beliefs. And a state of belief in the new order is the prerequisite for change.

What are the barriers to change? Change management has to overcome the following three classes of barriers:

1. **General:** related to organisation's history, culture, style, etc.
2. **Role:** specific incumbent positions create trouble.
3. **Individual:** specific individual objections.

Typical barriers include fear of failure, disbelief, complacency, expediency, culture, inertia, fear of the unknown. The most difficult barrier, however, is organisational politics. An organisation is a socio-technical system in which different political interest groups exist. These may be based on division of work, training skills, allocation of resources, peer group leader and so on. Any change threatens to shake the existing equilibrium of status, power, resources, opportunities, importance, etc. Some political groups may gain while others may perceive threat. Hence, they attempt to maintain status quo. Preservation of group interests supersedes organisational interests.

Various interest groups can be seen to be active during the change debate. They attempt to control the issues to be debated, manner of division of resources, legitimacy of the proposed change, etc. They use all methods such as formal authority, access to information, control over physical resources and reputation. They will forge alliances to alter the change strategy to their advantage. The change management strategy has to deal with organisation politics, in political and diplomatic way. All sides realise that the change agent is both a creator, and an annihilator, since creation comes with complementary destruction. All the more reason for the expected behaviour: protect and defend "the present", than be at the mercy of the change agent.

Change management plan must, therefore, study the existing political groups in the organisation for their present power, authority, budget, importance, security, etc. and their profile on same parameters in the proposed setup. The change strategy

must be evolved taking these hard realities into account. Since the change management is a result of induction of IT tools and BPR, the compounded barrier comprises of both these:

1. Technology revolution is obsoleting the competencies of IT staff. They resist new technologies.
2. Embedded behavioral system in an organisation. They resist change in status quo.



12.2 Change Management in the Government

Public administration in developing countries is highly bureaucratised and centralised. It is also based on an authoritarian legal system which is the legacy of colonial systems which sought to control the local population. Almost overnight after the declaration of independence, most of these colonial governments became the governments of the 'free' countries. Their character was not changed. There was no change in their thinking or orientation. Bureaucratic controls from a highly centralised system still characterise this government. It views people with suspicion. It has no concept of providing service to people, because it was anathema to the aliens who created this government. Likewise, development for people was not on the agenda of colonial governments. It is the same administration that is charged with the task of planning and implementing the process of development. Restructuring and reengineering of the government is a must to alter its image, to make it more friendly to the people. Its performance has to improve through innovative and cost effective processes based on IT in general, and EDI/ e-commerce in particular. Industrialised countries are undertaking efforts to reengineer public administration. The concept of NII includes delivery of government services to citizens as one of its key pillars. Change management strategy for re-engineered processes in government has to keep in view the following characteristics of public administration.

- Highly bureaucratic structure with over commitment to rules, regulations and precedents. Monopoly or near monopoly service provided by bureaucratic setup.
- Budget allocations not based on results and performance of department. Hence, pressure to perform does not work.
- Salaries of government employees not related to their performance. Seniority, and no merit, determines promotion and recognition. Effective reward and punishment system absent.
- Political interference in working of departments. Top bureaucrats not free to effect change. Hence, no motivation to change.
- Changes called for in organisations and human arrangements to bring about radical improvements in time, customer satisfaction, service quality or cost-effectiveness are extremely difficult. The current mindset has to change from *control* to *facilitation*. This is extremely difficult because the concept of a customer is hard to define in public administration.
- Total replanning, concurrent redesign, and implementation of administrative processes; and organisational structure are essential.

Change management plan depends upon whether there is process improvement, process redesign or complete organisational transformation. In the first case, only a particular process for a given function is being improved; whereas in the second case end-to-end process is under redesign for radical process improvement. This requires full support of top bureaucracy. If the entire organisation is being revamped through its cultural transformation and new ways of service delivery, it amounts to 'reinventing the government'. The mindset has to be changed in all these cases, albeit to different degrees.



12.3 The Implementation Plan

The use of EDI and e-commerce creates a paperless or nearly paper free environment. An organisation has to perform tasks which have been redefined in the new environment in order to deliver a service or a product in a more efficient, cost-effective manner, taking advantage of new technology embedded in its cultural setup. Installation of EDI/ e-commerce systems has to make an organisation EDI-capable. Various stages of processing for a service are still there, but in a reengineered form, where presumably all non-value addition stages have been eliminated. Paper documents do not move from one stage to another; instead an electronic document moves from one workstation to another. Entire workflow has been redone. Frequent person-to-person interaction within, and without stands drastically reduced, if not, eliminated. Suddenly, the scenario has changed. From handling paper documents, people are now dealing with electronic documents on their workstations. They are not interacting with people, but with keyboards and mouse. Workflow has integrated individuals across their traditional department or hierarchical reporting relationships into a mere networked organisational structure. Electronic documents travel back and forth across the newly created structures with a turnaround time which is much faster. People have to get tuned to this.

The scenario is thus as follows. Documents from customers or users arrive in an office electronically over e-commerce/ EDI links, be it the Internet or any other network. Electronic documents get acted upon automatically by the organisation's computers, and/ or human intervention from their respective workstations. There may be various stages of processing or clearance for a given service. At each stage there is value addition or processing from a different angle. Through BPR, presumably all non-value addition stages have been dispensed with. There may be need for obtaining clarifications at certain stages, or for consultation with a database. Workflow automation does provide for that. Interpersonal communication and interaction stands reduced to a minimum. The work culture changes.

How to manage this change from a paper-based, hierarchical organisational structure to electronic environment where departmental boundaries have become thin and the structure is more networked? Some of the methods are as follows:

1. Top management should be fully committed to change.
2. Create a technical plan for e-commerce/ EDI and BPR for the organisation (Chapter 11).
3. Take a small segment of work, such as invoices dealing with a specific product or service related to a particular group, for a pilot project.
4. Identify key players in the organisation who are votaries of change, for one reason or another.
5. Associate this group of persons as part of the BPR team. Develop the software, and workflow based on their perception.
6. Identify customers/ users for this pilot who would use the e-commerce/ EDI technology to interact with the organisation.
7. Implement the pilot.
8. Take the feedback of this team very seriously to modify procedures/ software. Nothing is perfect, one is only moving towards better solutions. So, be ready for changing procedures when required.
9. Induct people who are neutral to change, i.e. those who are indifferent or not-bothered. Provide instant help to this group, wherever they are, from the core team, whenever they need it. Build their confidence in the new system. Win them over to change.
10. The last group, the hostile category, may then be taken on board. Provide instant help to them in case of need. Station core team members in close proximity for this purpose. Be patient with their problems, whether genuine or contrived.
11. Expand the pilot by including another large group of products or services.
12. Repeat the above steps 8 to 11.
13. Repeat 11 and 12 in as many stages as necessary.



References

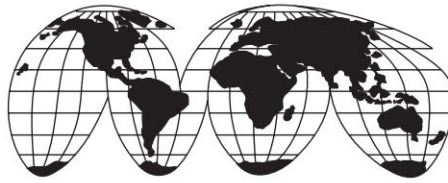
1. Boar, Bernard H, *The Art of Strategic Planning for Information Technology*.

PART **V**

Concerns for E-Commerce Growth

- Legal Issues
- Cyber Security
- Cyber Crimes

Legal Issues discusses the concerns that are raised as a result of introduction of e-commerce and e-governance, and highlights the need for cyber laws to create a predictable legal environment for e-transactions. Cyber Security covers the risks of using computers, networks and e-commerce tools and the measures that can be taken to counter these risks. Different cryptographic systems are also discussed and X.509 Public Key Certification is included. While crimes, as they have been traditionally known in the physical world, have adapted themselves to cyberspace, a number of new cyber crimes have emerged, challenging technologists and law makers. These are covered in the chapter on Cyber Crimes.



Chapter 13

Legal Issues



13.1 Legal Issues

The world is used to conducting business and commerce on signed paper documents. Two millennia of commerce has been based on the written document with its value 'authorised' by the signature of a duly authorised officer. The current legal practice has paper documents and signatures affixed thereon as a foundation. Electronic documents and messages, without the familiar signatures and marks, have changed the scene and trade wants to be assured that the electronic world is safe. The e-commerce system must, therefore, offer at least the same level of reliability as that which obtains in the paper world, notwithstanding the significant differences between the concepts embodied in electronic messages and paper documents. It is well known that frauds do take place in the traditional paper-based commercial transactions. Signatures can be forged, paper documents can be tampered with, and even the most secure marks, impressions, emblems and seals can be forged. But then these are known, and trade as well as the legal community know how to deal with these problems. Companies set aside funds to take care of losses due to such frauds. For example, credit card companies do know that a small percentage of transactions is fraudulent in nature. The world is 'comfortable' with these problems, since they have been there for as long as we have been trading.

The electronic world, on the other hand, exposes us to issues which were hitherto unknown, since they are directly the outcome of creating documents electronically, transmitting them over worldwide computer communication networks. Trading partners exchange documents electronically. They need to convince themselves that such documents are authentic when received over networks, and that their authentication can be established in case of dispute. Transactions may be electronic, but the key concepts of admissibility of evidence and evidential value of electronic documents, which are central to the law, remain the same. There must be a way to prove that a message existed, that it was sent, was received, was not changed between sending and receiving, and that it could not be read and interpreted by any third party intercepting it or deliberately receiving it. The security of an electronic message, a legal requirement, thus gets directly linked to the technical methods for security of computers and networks. From the legal angle, there is a further complication because the electronic message is independent of the actual medium used for storage of transmission. The message can be stored on a floppy, disk, or an optical disk. Likewise, it may be transmitted over a local area network, a Virtual Private Network (VPN), or the Internet. The physical medium could be coaxial cable, radio link, optical fibre or a satellite communication channel.

The legal issues of e-commerce have generated tremendous interest among technologists, traders and legal experts. Many of the early e-commerce experiments, and even production systems went into operation without any legal interchange agreement between trading partners, or between networks and their customers. No laws for e-commerce existed in India too. When the Indian Customs EDI System (ICES) project got off the ground in 1995, it was without any e-commerce/ EDI law, or even a proper interchange agreement. Since then, much has been achieved. The Indian Parliament passed the Information Technology Act in 2000, the details of which are given in Chapter 16. Technologists and users alike have shown confidence in e-commerce, though electronic messaging technology gives rise

to many legal questions and issues. As early as 1991, Benjamin Wright,¹ a Texas-based US attorney, expressed confidence in his book, *The Law of Electronic Commerce* that ‘if implemented intelligently, electronic communication can confidently be used for legal transactions’. He rejected ‘the attitude that technology deserves suspicion’.



13.2 Risks: Paper Document versus Electronic Document

The risks that afflict the traditional signing of a paper document are many. There is no standard method for signing in ink: signatures could be in created in any manner—strange, non-decipherable scribble, changed signatures with every transaction. Moreover, it is seldom compared against specimens for authenticity. But then this is accepted since we feel confident that signatures are there, though they may have been forged. There is no guarantee that any given ink signature can be verified by forensic science. Given a reasonable sample of specimen signatures, science can offer a probable, well-informed opinion on the authenticity of signatures in question. The originator may repudiate his own signatures on a document in an attempt to disown a transaction. The receiver may raise any number of objections. Moreover, some pages of a document may not have been signed, or may have been altered after the signed document was created. There are therefore myriad risks associated with a paper document, and these risks are distributed across a number of acts performed by various players in a commercial transaction. These include:

- The style of signing by the originator
- The secret choice of the originator to change his signature
- The content of the signed document
- The facts external to the document, but in historical context to it

- Competence of experts who opine on the authenticity of signatures, and pages of document
- The views of courts on the issues in case of a dispute.

It is clear that risks abound in the authentication of paper documents. The paper world has legally enforced documents, through the evidence of a 'document', a 'writing', and a 'signature'. In the electronic equivalent, it amounts to the following: 'writing' requires that a record is created, 'signature' reflects the desire for a 'legal and ritualistic symbol of finality, assent, and authenticity.' In e-commerce, there is concern that in the absence of proper controls, it is relatively easy to change an electronic record. Proper controls need to be enforced in e-commerce transactions. For example, business software used for e-commerce may be restricted to authorised users only and all uses of the same including unsuccessful attempts should get automatically logged in an audit log. Message confirmation, record making and control standards have emerged. These have been discussed in the chapters on Security Issues and PKI. Some of the techniques for ensuring integrity of messages during communication include:

- A professionally operated network supported by disaster recovery methods
- Communication protocols, network control and management software
- Data checking and preservation techniques
- Cryptography
- Use of Auditors

Since message authentication is linked to technical methods in that one has to prove to a court the source and integrity of a message, the security issues of e-commerce are intimately related to legal issues. Authenticity, integrity, confidentiality, and non-repudiation of origin and receipt of electronic transactions conducted over networks, are essential for authenticating electronic messages in case of a dispute. Authenticity may be the key to a legal dispute. Before evidence of an electronic message is admitted in a trial, a number of objections can be raised on the grounds of authenticity. According to Wright, the

principles of evidence law developed around paper documents are valid in e-commerce transactions, resulting in issues which arise as follows:

“In the classic trial, one party, the ‘proponent,’ seeks to ‘admit’ a bit of evidence (such as a record of an invoice) to prove a point that matters in the trial. Typically the proponent must ‘lay a foundation for the evidence to show its admissibility under evidence law (or the rules of evidence). The other party, the ‘opponent,’ may object if there is a basis for doing so under the law. If the judge allows the admission, the ‘trier of fact’ (normally the jury but sometimes the judge) may consider the evidence in deciding the case. A trier of fact generally decides a case only on the basis of evidence that is admitted.”



13.3 Technology for Authenticating Electronic Document

Techniques have been developed which can ‘authenticate’ e-commerce transactions with a degree of certainty which is the same or more than that obtainable with paper documents. Cryptography and digital signatures are the pillars of this technology. In fact, a digital signature is much more reliable than a handwritten signature since it is not subject to the originator’s will or intention to deliberately change his own signature. The use of Trusted Third Parties (TTPs) is essential for non-repudiation services. They perform the role of an independent witness, similar to the function of a notary public.

Cryptography techniques, based on symmetric and asymmetric methods of generating keys which are used to transform the message to encrypt it, have been discussed in Chapter 14. A cryptographic check value is a way of preserving the integrity of the message data. The sender binds his unique identifier onto a message in such a way that the message cannot be forged by the receiver, and cannot be denied by the owner of the secret key. A combination of public and private

cryptographic keys supports digital signatures. It is the independent certifying authorities that are expected to hold the public keys of all users, while the users would hold the public keys of the certifying authorities that they are connected to. Some certifying authorities, the unconditionally trusted ones, would actually generate the key pairs for digital signatures, and distribute them safely. Others would issue the certificate of the public keys that they hold in their register.

The state of Utah in USA, was one of the earliest to adopt a Digital Signature Act, which is known as the Utah code. This Act envisaged the global use of public key cryptography based on government licensed CAs. This concept was implemented in the Indian Information Technology Act, 2000, which is discussed in Chapter 16. The originator of a document has to keep his private key secret. In e-commerce transactions, it is the private key that becomes the object of fraud. The risk is completely shifted to the private key and concentrated there. As opposed to this, biometric technology implemented around some part of human beings distribute such risks. Biometrics measure individuals' unique physical or behavioural characteristics to recognise or authenticate their identity. Some of the technologies that are:

- Physical biometrics such as fingerprints, hand or palm geometry, retina, iris, or facial characteristics
- Behavioural biometrics including signature, voice (which also has a physical component), keystroke pattern, and gait.

The Organisation for Economic Co-operation and Development (OECD) recommended on March 27, 1997, that member countries should establish new, or amend the existing policies, methods, measures, practices and procedures to reflect and take into account the principles concerning cryptography policy set forth in the OECD Guidelines for Cryptography Policy. These guidelines are reproduced in Appendix 8.



13.4 Laws for E-Commerce

As discussed, the legal requirement is to establish the authenticity of an electronic message or document. This includes integrity, confidentiality and non-repudiation of origin and receipt of electronic document in case of dispute. The UNCITRAL Model EDI/ e-commerce Law defines an electronic data message as follows:

“2(a) Data message means information generated, stored or communicated by electronic, optical or analogous means including but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.”

The law proposes legal recognition of data messages, and defines ‘writing’ and ‘signature’, and their admissibility and evidential value. The model law as adopted by the UNO is reproduced in Appendix 3. Individual countries were advised to enact this law with suitable modifications that may be necessary in the national context. Rules and guidelines also need to be framed for those maintaining electronic records, providing network services, Internet service providers, electronic notaries, Trusted Third Parties (TTPs), Certifying Authorities, etc. to take care of general record keeping and control requirements, confidentiality and control of data, privacy controls, access of business software and use of digital signatures.

The Electronic Transactions Act (ETA) enacted by the Singapore Government in July 1998 sought to “create an environment of trust, predictability and certainty” to provide a conducive framework for electronic transactions and the electronic formation of contracts. The ETA addressed issues of electronic records and signatures, liability of network service providers, electronic contracts, digital signatures and the role of certification authorities. Additionally, the Computer Misuse Act and the Privacy code were proposed to be suitably adopted to protect computer systems and consumer data.

The Indian Government enacted the Information Technology Act in the year 2000. This Act is discussed in Chapter 16.



13.5 EDI Interchange Agreement

It is an established fact that certain discipline is required in the conduct of commerce in the paper world. Simple activities such as preparation of an invoice, drawing up a commercial contract, signing, despatch, receipt, etc. have to follow certain protocols agreed to by trading partners. These may be formal or informal. In addition, acceptable rules of conduct are also necessary to achieve the kind of discipline required for conducting smooth and effective trade and commerce. In the EDI world of electronic documents, such a discipline has been created through a set of rules that have developed in the form of interchange agreements within a number of user groups, national organisations, and regions. At the international level, the UN has adopted The Model Interchange Agreement for the International Commercial Use of Electronic Data Interchange, which applies to the interchange of data and not to the underlying commercial contracts between the parties. It addresses the need for uniformity of agreements so that there are no barriers to international trade on account of different solutions for various problems being adopted by countries. The UN has recommended that the member countries should take into account the terms and provisions of the Model Interchange Agreement when framing their own laws on e-commerce.

Notwithstanding the implementation of e-commerce laws, the EDI Interchange Agreements continue to be relevant even now.

An interchange agreement may be made between trading partners. It establishes the rules they will adopt for using EDI/ e-commerce transactions. It details the individual roles and legal responsibilities of trading partners for transmitting, receiving and storing electronic messages. The signing of an interchange agreement signifies that the parties intend to be bound by it,

and that they desire to operate within a legal framework. This can help reduce legal uncertainty in the electronic environment. Many of the conventions and agreements relating to international trade do not anticipate the use of e-commerce/ EDI. Many national laws, as noted above, also introduce uncertainty regarding the legal validity of electronic documents. There are still very few national and international judgements ruling on the validity of electronic document, messages or signatures. It is precisely in this kind of a scenario wherein clear legal rules and principles are absent, that an interchange agreement provides trading partners with readily available solutions for formalising the EDI/ e-commerce relationship between them. It provides a strong legal framework for ensuring that electronic documents will have a legally binding effect, subject to national laws and regulations.

The issues which were addressed by the working party which prepared this model Interchange Agreement, are:

- (a) Selection of EDI messages, standards and methods of communication
- (b) Responsibilities for ensuring that the equipment, software and services are operated and maintained effectively
- (c) Procedures for making any systems changes which may impair the ability of the trading partners to communicate
- (d) Security procedures and services
- (e) The points at which EDI messages have legal effect
- (f) The roles and contracts of any third party service providers
- (g) Procedures for dealing with technical errors
- (h) The needs (if any) for confidentiality
- (i) Liabilities in the event of any delay or failure to meet the agreed EDI communications requirements
- (j) The laws governing the interchange of EDI messages and the arrangements of the parties
- (k) Methods for resolving any possible disputes.

The interchange agreement is flexible enough to meet the requirements of all business sectors involved in international trade. Trading partners can feel confident that it addresses the

recognised legal issues arising from the commercial use of EDI in international trade, and provides a strong legal and practical framework for considering and recording the necessary business decisions.



13.5 Legal Issues for Internet Commerce

Internet commerce raises legal issues through the provision of the following services:

- Online marketing
- Online retailing: ordering of products and services
- Financial services such as banking and trading in securities
- Online publishing
- Exchange of electronic messages and documents EDI, electronic filing, remote employee access, electronic transactions
- Online contract formation

Trade and commerce over the Internet generate several legal issues^{3,4}, which are discussed below.

13.5.1 TradeMarks and Domain Names

Domain names have traditionally been assigned by the InterNic Registry in the USA. The .com domain used by commercial entities uniquely identifies them in cyberspace. The latter is worldwide since the Internet, like a river, is not confined to the geographical boundaries of a country. This advantage poses a problem too. A company takes a domain name from the Registry in its name. Unlike the traditional commercial world where different companies may have the same trademark in different products or services, in cyberspace, only one name can be assigned as Name.com. Thus the company which registers its name first for the domain name, eliminates all others from using that name in cyberspace. As one would expect, this has led to legal battles. It has been argued in courts in the USA and the

UK that a domain name functions as a trademark. Therefore, a person or a company not entitled to the trademark, but using it as a domain name is guilty of trademark infringement.

The infringement of trademarks by the use of domain names is essentially on two grounds: that of confusion, and that of dilution. In the US, the Lanhan Act, 1984 defines a trademark as “any word name, symbol, or device or any combination used or intended to be used to indicate the source of the goods”. Liability for infringement, when the infringer uses a mark that may be confused with the trademark of another, whether deliberately or through negligence, when seen to be used in the context of similar goods or services, is strictly on the infringer. The celebrated case of *Maritz Inc. vs. Cybergold Inc.* considered the issue of trademark confusion with domain names. The former was using unregistered ‘GoldMail’ with its GoldMail service on the Internet, with the URL *goldmail.com*. Cybergold, on the other hand, was developing a similar Internet service with the domain name *cybermail.com*. The issues debated included the matter of confusion between the marks ‘GoldMail’ and ‘CyberMail’, and the likelihood of confusion among appreciable number of buyers.

The trademark dilution issue came up in *Hasbro Inc. vs. Internet Entertainment Group Inc.* The court was convinced that Hasbro had been producing a game, Candy Land, for young children for several years and that 94 percent of the mothers were aware of this game. Internet Entertainment Group, on the other hand, registered a domain name *candyland.com* at which site they featured pornographic materials. The court granted an injunction preventing the latter from using the domain, and ruled that it rightfully belonged to Hasbro.

13.5.2 Copyright and the Internet

Copyright was developed in the printed world to protect the economic interests of creative writers. The copyright law protects only the expression of an idea and not the idea itself. In due course, it started protecting the originality of artists and

innovators too. In recent times, however, the subject matter of copyright has further expanded. For example, the Copyright Designs and Patent Act, 1988, in the UK, allows protection of the following subject matters:

- Original literary, dramatic, musical and artistic works
- The typographical arrangement of published editions of literary, dramatic or musical works
- Sound recordings
- Broadcasts
- Cable programs.

These have been broadly classified into two groups as ‘author works’ and ‘media works’ by Hector L. Macqueen. The multimedia capability of websites enables all types of works to be ‘published’ on the Internet in the sense that copies can be distributed to users/ customers. The problem, however, is that unlike a paper copy, this copy can be readily duplicated and distributed further by the recipient. If the material is in the public domain, there are no difficulties. But the copyright law applies to the downloaded matter, in much the same way that it applies to physical copies. There is a different dimension to this problem in the context of bulletin boards. Someone may post various works onto them giving the impression that they can be freely downloaded, whereas in the first instance, they were illegally pasted on the bulletin boards. The service provider who runs the bulletin board thus gets drawn into the dispute, though he may or may not have been aware of this. The website creator, or an Internet Service Provider, may be liable for secondary infringement due to his role in the distribution of the infringing copies.

It has been established in a number of disputes so far that a website is likely to enjoy copyright protection. However, a website operator has to ensure that he does not violate someone else’s copyright in creating the site. Websites, and distribution of material from them over the Internet, attract copyright provisions related to copying, issuing copies to the public, using copies, etc.

13.5.3 Jurisdiction Issues

While a number of countries have enacted special legislation to deal with legal issues pertaining to the widespread use of the Internet, most of these national legislations, can only be effective within the boundaries of the nation in which they are enacted, even though the law could provide for applicability to any offence or contravention committed outside the national boundaries.

The legal consequences, which accompany an Internet presence, are emerging as courts struggle to apply conventional legal concepts to e-commerce. A company's e-commerce strategy not only helps attract customers in new markets, but may also expose companies to the jurisdiction and laws of these new markets. The term 'jurisdiction' refers to a court's ability to hear a particular case.

Internet communications know no geographical boundaries, whereas jurisdiction under traditional legislation incorporates a notion of territoriality. The very origin of an e-mail message may be unknown. It may have traversed through a number of sovereign nations. Information on websites is not to be confined to a target audience, but is disseminated simultaneously to a global audience, thus affecting individuals and organisations in a number of jurisdictions, all of which have their own particular local laws.

Different laws are applicable under different jurisdictions. A number of questions which are vital to the legality of commerce in cyberspace have arisen. These are:

- Who has the authority to prescribe the law in a given area (for example, e-commerce)?
- Where can the action commence and the entity be subjected to legal proceedings?
- How and when will a court judgment or arbitral award rendered in one jurisdiction be enforced in another?

It is likely that personal jurisdiction will exist when a company clearly conducts business over the Internet, with persons in a foreign jurisdiction. Thus, the use of the Internet to make contracts, to transmit computer files or to accept purchase orders from a distant venue may subject the defendant to jurisdiction in foreign states. Conversely, where a corporation hosts a passive website which simply posts information accessible to residents of a foreign jurisdiction, a finding of necessary minimum contacts based solely upon the website is unlikely. In the middle, the more difficult cases involve interactive websites wherein a user can exchange information with the host computer. In these cases, 'the level of interactivity and commercial nature of the exchange of information that occurs on the website' determines the validity of personal jurisdiction.

Some companies have added to their website terms and conditions requiring that any dispute must be at a certain venue. While the enforceability of these provisions varies on the basis of the facts and jurisdiction, several companies have successfully invoked such clauses when defending cases brought in foreign jurisdictions.

The US courts have been among the first to address jurisdictional issues raised by Internet transactions, and US cases determining such issues may serve as indicators of the direction that other countries may take.

13.5.4 Service Provider Liability

Many ISPs provide users access to shared websites, Usenet news, e-mail distribution lists, etc. These facilities can be used by their users to upload unlawful, defamatory, copyright or trademark infringing material. Unlawful material includes banned publications, hate propaganda, pornography and obscene material, without the ISP having a chance to review it. Liability for materials distributed on the Internet may be different for the website operators and the ISPs. An ISP could be held liable for the bulletin boards, and for aiding and abetting the commission

of an offence such as the distribution of pornography. Similarly, third party liability for defamation is also a cause for serious concern of ISPs, online service providers, websites, etc. Thus the concerns include libel and defamation, liability for infringement of third party rights, and liability for hosting of unlawful materials.

Under the IT Act, 2000, Section 79, network service providers will not be liable for any third party information or data made available by them if they can prove that the offence or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such offence or contravention.

13.5.5 Formation of an Enforceable Online Contract

The growth of e-commerce on the Internet depends, to a large extent, on the confidence of traders in forming legally enforceable contracts online. The key activities associated with the formation of an enforceable contract do take place on the Internet, viz. the offer is communicated by the offeror, and acceptance is received back by the offeror from the acceptor. An offer can be communicated orally or in writing; and in the e-commerce environment, through the Internet. Electronic acceptance of the contract through e-mail, e-form is valid, in much the same way that a fax message is. The offeror can display terms and conditions as a legal notice, on his website. Visitors to the site, who choose to proceed further, even after reading the notice, may be construed to accept the conditions imposed by it. However, the timing of acceptance of the offer determines when the contract is formal. In this case, the e-mail of acceptance has to reach the offeror who may say that the contract will get formed only after its receipt (in his conditions on the website).

There are problems associated with jurisdictions of the parties, and that of the website, since it is the jurisdiction which determines the laws that would be applicable in case of a dispute. Then there are issues related with the identity of parties and the

role of digital signatures on the Internet. Writing and signing requirements in print may be a requirement for some sort of a tangible or permanent form. Yet another issue related to electronic contracts is to establish the competency or authority of a party to enter into a transaction.

All these issues and a few others are critical to the creation of an enforceable electronic contract. In case of postal mail, it has been held that once the acceptor has mailed the contract, it becomes valid irrespective of whether it reached the offeror. However, some of the proposals under consideration in some countries reject this rule for electronic communications.

The IT Act, 2000 covers these issues under Sections 11, 12 and 13. The major topics covered are:

- Attribution of electronic records
- Acknowledgement of receipt
- Time and place of dispatch and receipt of electronic record

It is worth observing here that UNCITRAL is still grappling with the issue of creation of a model online contract law. A working group has held a number of meetings in an effort to finalise the UNCITRAL E-Contracting Law. The draft convention which has been on the agenda of the E-Commerce Working Group essentially includes the following provisions:

- Dealing with the sphere of application of the instrument concerning the formation of contracts
- Dealing with specific rights and obligations of the parties in the context of contract formation by electronic means.

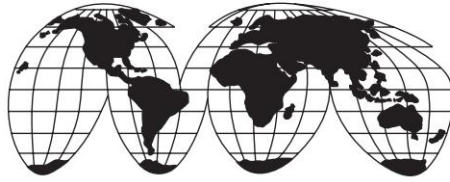
Legal issues are manifold. Whether the issue is EDI over networks, or e-commerce over the Internet, the primary concern of users is the existence and enforceability of appropriate laws for e-commerce. In case of dispute, electronic documents must be acceptable as legal evidence in courts of law. While the problems of acceptance of, and confidence in electronic transactions do exist, they are not insurmountable. There is sufficient awareness in, and synergy of action among trade,

legal and e-commerce technology communities to make e-commerce happen through appropriate developments in their respective areas.



References

1. Wright, Benjamin, *The Law of Electronic Commerce*, Little, Brown, and Company, 1991.
2. Wright, Benjamin, 'Eggs in Baskets: Distributing the Risks of Electronic Signatures', in *From EDI to Electronic Commerce* edited by K.K. Bajaj and Debjani Nag, Tata McGraw-Hill, 1996.
3. Rosenoer, Jonathan, *Cyberlaw: The Law of the Internet*, Springer-Verlag, 1997.
4. Edwards Lilian and Waelde, Charlotte, *Law and the Internet: Regulating Cyberspace*, Hart Publishing, Oxford, 1997.
5. Schneider, Bruce and David Banisar, *The Electronic Privacy Papers*, Wiley, 1997.
6. United Nations Commission on International Trade Law (UNCITRAL); Working Group IV.
[http:// www.uncitral.org/ english/ workinggroups/ wg_ec/ index.htm](http://www.uncitral.org/english/workinggroups/wg_ec/index.htm)



Chapter 14

Cyber Security

With the Internet making inroads into almost all facets of everyday life, not only business information, but a large amount of personal information too is now digitised and stored on computers connected to the Internet. Information has its own value and can either be destroyed or used with malicious intent or for commercial interest.

Systems connected to the Internet are potential targets for eavesdropping and destruction/ tampering of the data stored in them. A website offering services on the Internet is vulnerable to attacks, which render the site non-functional resulting in denial-of-service. Carrying out traffic analysis could reveal valuable information regarding the channels of communication from a server. Masqueraders pretending to be authorised users could gain access to privileged areas. Authorised e-commerce or e-governance transactions could be modified or replayed for commercial gain.

Attacks like the above, when carried out, could result in crisis situations due to service outages, unauthorised use of computing systems, compromise of data and direct financial losses. In the case of a successful attack on critical infrastructure such as power grid, the consequence could even be the loss or endangerment of human life. With the growing Internet economy, such incidents would result in loss of trust in computers and networks, and be detrimental to the growth of public confidence in the Internet.

Systems, networks and data have to be protected to guard against such attacks which could originate from within the organisation or from outside. It is extremely important to secure internal information systems from being attacked. With client machines on an organisation's internal LAN routinely accessing the Internet, they too become targets for attack by unscrupulous elements. Most surveys carried out worldwide have indicated that the threat to an organisation is much higher from within the organisation than from outside.



14.1 Cyber Attacks

Attacks can be classified as executable-based or network-based. In the case of the former, the attack happens only when a program is executed on the targeted computer system through either of the following:

- **Trojan**—a computer program that appears to have a useful function, but also has hidden and potentially malicious functions that evade security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program. The idea of modifying a normal program to do nasty things in addition to its usual function and arranging for the victim to use the modified version is known as a Trojan horse attack.
- **Virus**—a program fragment that is attached to a legitimate program with the intention of infecting other programs. It is hidden, self-replicating computer software, usually malicious logic, that propagates by infecting, i.e., inserting a copy of itself into and becoming part of another program. A virus cannot run by itself; it requires its host program to be run to make the virus active.
- **Worm**—a computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. It differs from a virus only in that

a virus piggybacks on an existing program, whereas a worm is a complete program itself. Viruses and worms both attempt to spread themselves and both can do severe damage.

- **Spam**—is also a major source of cyber attacks. There are some estimates according to which 70 percent of all e-mail is junk mail, or spam. While spam by itself has nuisance value in that it clogs most of the Internet highways around the world causing losses by way of improper utilisation of bandwidth, it is used to propagate viruses and worms. Junk mail appears to be promotional material, similar to advertisements and catalogues in the physical world. Unsuspecting users become victims as soon as they click on attachments. Trojans and spy-ware get installed on their systems. Information and data on all activities of interest thus gets reported from users' computers to sites whose forwarding addresses have been installed as part of spy-ware. This is a form of information espionage, which may be used by competitors. At the national level however, intelligence agencies may collect useful data from important systems that may have been compromised by sending spam.

In order to protect systems from executable-based attacks, anti-virus measures must be deployed on desktops and servers and on the corporate gateway for data coming in from external sources.



14.2 Hacking

Externally accessible systems are targets of *hacking*. Hackers can deface websites and steal valuable data from systems resulting in a significant loss of revenue if it is a financial institution or an e-commerce site. In the case of corporate and government systems, loss of important data may actually result in the launch of information espionage or information warfare. Using *IP spoofing*, attackers often hide the identity of machines used to

carry out an attack by falsifying the source address of the network communication. This makes it more difficult to identify the sources of attack traffic and sometimes shifts attention onto innocent third parties.

14.2.1 Phishing

Phishing is the creation of e-mail messages referencing web pages that are replicas of existing sites to make users believe that these are authentic sites. Unsuspecting users are made to submit personal, financial, or password data to such sites from where the data get directed to fraudsters' chosen sites. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5 percent of the recipients to respond to them. According to a tech-security company MessageLabs, the number of phishing attacks increased ten-fold during the year 2004 as compared to 2003. In the month of November, 2004, phishing attacks rose to 4.5 million. Phishing has indeed emerged as a major threat to any organisation or individual conducting business online. Yet another trend associated with these attacks is the singling out of certain companies, especially financial institutions, to be the victim of phishing attacks. This signals the beginning of a wider trend. From a random, scattergun approach there emerge customised attacks designed to take advantage of weakness of some businesses.

14.2.2 IP Spoofing

IP Spoofing is used by intruders to gain unauthorized access to computers. Messages are sent to the computer with the sender IP address of a trusted system. Packet headers of the message are modified to make it appear that the message is coming from a trusted system.

For externally accessible systems such as web, e-mail and FTP servers, protection can be accorded in the following ways.

- Use **Scanning** tools to scan systems connected over an IP network and report on the systems they encounter, the ports available, and other information, such as OS types.
- Put them behind an appropriate Firewall (defined in section 14.3), —preferably in a demilitarised zone (DMZ).
- Disable all services except those absolutely needed.
- Filter all except port-specific traffic to systems (e.g., FTP servers should only receive *ftp* requests and nothing else).
- Turn on system and firewall logs.
- Review the logs on a daily basis.
- Implement Intrusion Detection Systems.
- Establish proxy servers, so that internal client requests for accessing external services are routed through the proxy server. This ensures that the client and the external server are not in direct communication with each other.
- Establish an additional network as a buffer between the internal and external networks



14.3 Firewalls

A *Firewall* is a system or group of systems that enforces an access control policy. Firewalls operate on the basis of a set of user defined rules. These rules govern the flow of data into and out of the firewall. The rule base is created to enforce a specific security policy on the firewall. Rules could decide, for example, which packets of data, depending on the originating IP address, should be allowed to pass into the organisation's network.



14.4 Intrusion Detection Systems

Intrusion Detection Systems (IDS) complement the firewall to detect whether or not those communication channels through the firewall are being exploited. Firewalls can filter incoming and outgoing traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can

connect to the internal intranet via an unauthorised modem that does not pass through the firewall. If the threat comes from within the organisation, the firewall does not recognise those threats because it monitors only traffic between the internal and external network.

There are two types of Intrusion Detection Systems—Host-based (HIDS) Intrusion Detection works based on a reactionary approach in which the Intrusion Detection software monitors system log files. When log activity matches a pre-determined attack signature, an alert is generated and Network-based (NIDS) IDS which works by monitoring real-time network traffic similar to the way a network sniffer functions. Malicious activity is identified by matching network traffic to predefined attack signatures.



14.5 Secure Sockets Layer

Web communications also require additional levels of security to protect against situations such as compromise of credit card numbers when transmitted across the network. Client-server authentication mechanisms (dealt with later in this chapter) must also be installed to guard against business malpractices.

The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications to provide security during a communications session. SSL operates above the TCP layer and provides protection to applications such as FTP, TELNET and HTTP. This includes services such as client and server authentication, data integrity and confidentiality.

Secure HTTP (SHTTP) was developed for CommerceNet, a consortium of companies promoting the establishment of electronic commerce on the Internet. SHTTP provides security to individual transactions.



14.6 Authentication and Assurance of Data Integrity

The electronic environment ushered in by e-commerce and e-governance, while allowing transactions to be conducted with the click of a mouse, also opened up new risks that were not inherent in the paper environment. Copies cannot be distinguished from originals. Information can be modified without leaving any trace.

In cyberspace, two transacting partners, Bob and Alice, need to be assured of each other's identities. When sending a confidential document, Bob must be sure that the document will only be available to Alice and no one else.

In an environment where business transactions take place on the basis of paper documents, a Purchase Order cannot be modified without leaving evidence. The payment amount on a cheque too cannot be modified without leaving a trace.

However, when the transacting parties operate on electronic documents, not only can changes be made in documents without leaving any visible signs, documents can also be 're-played' and made to appear as bona fide transactions. In providing security in the electronic environment, there should be therefore an integration of manual and technical controls appropriate to the risks that a business believes it is exposed to. With the introduction of e-commerce, the new system should offer at least the same reliability as the paper system that it replaces.

Whatever the environment, paper or electronic, securing it necessarily implies the prevention of (a) destruction of information, and (b) unauthorised availability of information through mechanisms for guaranteeing confidentiality, integrity, authenticity, and non-repudiability of business documents and transactions. These are listed as follows:

- *Confidentiality*: Information should be protected from prying eyes of unauthorised internal users and external hackers,

and from being intercepted during transmission on communication networks. The content should be made unintelligible to the attacker so that it is not decipherable by anyone who does not know the transformation algorithm.

- *Integrity*: On retrieval of a stored document or on receipt at the other end of a communication network, the information should appear exactly as was stored or sent. It should be possible to detect any modification, addition or deletion to the original content. Integrity also precludes information 're-play', i.e generation/ re-transmission of a fresh copy of the data using the authorisation features of the earlier authentication.
- *Authenticity*: No entity should be able to masquerade as another entity. When information is retrieved or received it should be possible to verify whether it has indeed been sent by the entity claiming to be the originator. Similarly, it should also be possible to ensure that the message is delivered to the intended recipient.
- *Non-repudiability*: After sending/ authorising a message, the sender should not be able to, at a later date, deny having done so. Similarly, the recipient of a message should not be able to deny receipt at a later date. Messages and message acknowledgments must be bound to their originators.

Implementing a security solution in an e-commerce environment therefore, necessitates an analysis of the risks the business is exposed to so that information infrastructure is protected from intentional and accidental destruction. In the case of some transactions, confidentiality might be a critical requirement whereas in others it may only be data integrity that is of paramount importance.



14.7 Cryptography-based Solutions

Implementation of technology solutions for all the security services listed above is based on cryptographic techniques.

Cryptography comprises encryption, i.e. the process of making information unintelligible to the unauthorised reader, and decryption, i.e. reversing encryption to make the information intelligible once again. Conventional cryptography uses a secret code or key to encrypt information. The same secret key is used to decrypt the encrypted information.

A simple encryption scheme could be one in which all alphabetic and numerical characters are shifted by a fixed number of positions in the encrypted text. If the characters are to be shifted by, say five places, then the result would be as follows:

<i>Character</i>	<i>Represented as</i>
A	F
B	G
C	H
V	A
W	B
X	C
y	D
Z	E

Using this encryption scheme, where the key is a 5-character shift, the plaintext message THIS IS A BOOK would be encrypted to read YMNX NX F GTTP, which would not be very easily decipherable to the casual reader.

Over time, many encryption systems have developed and with the increased availability and advancement of computing resources, the level of sophistication of these systems has also increased. While the most obvious application of these processes is in ensuring confidentiality of information, advances in the science of cryptography have also made possible the provision of other security services such as integrity, authentication and non-repudiation.

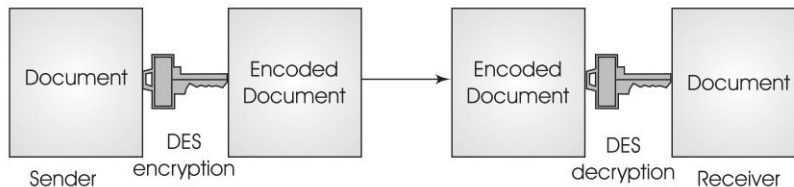
Cryptographic systems or cryptosystems are symmetric or asymmetric. The symmetric system is based on a single secret key which is shared by the parties engaging in secure

communication. The asymmetric system hinges on the possession by these parties of a pair of keys—one private and the other public.

14.7.1 Symmetric Cryptosystems

Major commercial use of symmetric cryptosystems began in 1977 when the Data Encryption Standard (DES) was adopted as a United States Federal standard. DES and other symmetric cryptosystems work on the concept of a single key being shared between two communicating entities. Essentially, therefore, for every pair of partners engaging in secure communications, a new key has to be generated and securely maintained.

Since, in the symmetric system, the secret key is shared between two persons or entities, it is very important to be able to ensure the secure exchange of the secret key. However, if indeed such a secure channel existed, it would not be necessary to encrypt data in the first place. How to circumvent this will be discussed in the section on Asymmetric or Public Key Cryptosystems. Figure 14.1 illustrates the use of symmetric keys.



➞ **Fig. 14.1** *Symmetric keys*

Symmetric systems operate either in the block cipher or in the stream cipher mode. In the block cipher mode, the data to be encrypted is broken up into fixed size blocks. Each of these fixed size blocks is encrypted and on decryption is again presented back with data in blocks of the same size. The stream cipher mode can operate on data of any size and on encryption results in encrypted data of the same size as the plaintext data.

The DES cryptosystem operates in the block cipher mode. Data is encrypted in 64-bit blocks using a 56-bit key. After an initial permutation of the data bits, the result is passed through 16 rounds of processing using the 56-bit key. A final permutation generates the encrypted 64-bit data block. The decryption process is similar except that it is followed in the reverse order.

The strength of the encryption key is directly proportional to the key length, since a brute force attack using all possible combinations within the key length would yield the secret key. Increasing key length increases the strength but there is consequently a trade-off with the processing overhead and consequently the cost of key usage.

Triple-DES follows the same algorithm as DES, using three 56-bit keys. 64-bit data blocks are first encrypted using key1. The result is encrypted using key2 and again encrypted using key3.

Another popular cryptographic algorithm is the International Data Encryption Algorithm (IDEA) which uses 128-bit key for encryption. The Advanced Encryption Standard (AES), also known as Rijndael, operates in a block cipher mode. It was adopted by the National Institute of Standards and Technology (NIST) in November 2001 after a five year standardisation process. Adopted as an encryption standard by the US federal government, it is expected to be used extensively, as was DES before it. Key lengths of 128, 192 and 256 are being used with the AES Algorithm.

While the solutions presented above only provide data confidentiality, symmetric cryptosystems can also be used to support the requirements of message integrity and data authentication. This is done through the secret key based generation of a checksum from the contents of the original data. The checksum is sent along with the data. Any modifications made to the data en route will become known to the receiver since the new checksum created from the received data using the shared secret key will not match with the checksum which

has been sent by the originator. The Message Authentication Code (MAC) is an integrity checksum standardised in 1986 for use by the banking and financial sector. MAC uses DES algorithm for generating the integrity checksum.

In order to counter the problems of lost or duplicate messages, unique Message Serial Numbers are incorporated cryptographically into the message so that there is no message 're-play' or dropped messages.

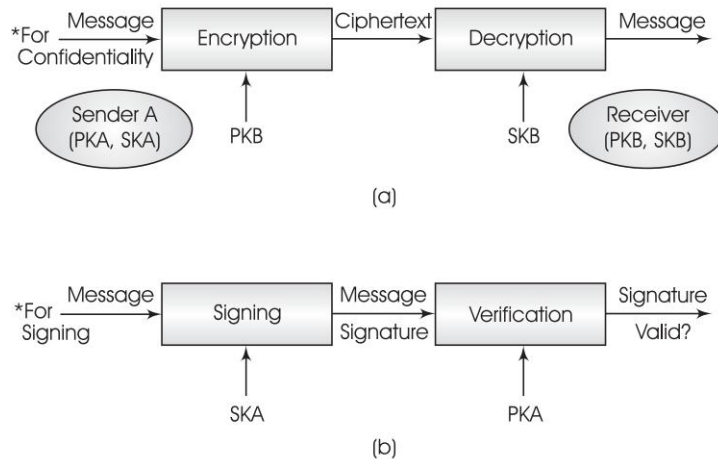
14.7.2 Asymmetric Cryptosystems

Asymmetric or public key cryptosystems are built around the possession of a pair of keys—a public key and a private key—by each entity wishing to engage in secure communication. While, as its name suggests, everyone knows the public key, only the owner knows the private key. The algorithm used to generate these keys is such that if either of the keys is used to encrypt a message, only the other corresponding key in the key pair will be able to decrypt it. Although these keys would then have to be related to one another, knowing the public key, it should be infeasible to obtain the private key. Public key cryptosystems are used to provide the services of confidentiality, integrity, authentication and non-repudiation.

To send a confidential message to UserB, UserA encrypts the message using UserB's widely known public key PKB. On receiving the encrypted message from UserA, the message is decrypted using UserB's private key SKB. Confidentiality is assured since the private key would have been carefully protected by UserB. Any third party, without knowledge of UserB's private key would not be able to decipher the encrypted message. This is explained through Fig. 14.2(a).

For UserB to receive an authenticated message from UserA, the message is encrypted using UserA's private key SKA. At the recipient end, the encrypted message is decrypted by UserA's public key PKA which is widely known. On validation, the message is assured to have been sent by UserA since the

corresponding private key is held securely by UserA. Any third party would also be able to verify the authenticity since the public key is known to everyone. Authentication is explained through Fig. 14.2(b).



➞ **Fig. 14.2** Asymmetric algorithm

In order to achieve both confidentiality and authenticity, the message can first be authenticated using the originators private key and the authenticated message can then be made confidential by encrypting with the recipients public key.

Since the secret key does not have to be shared between communicating entities in public key cryptosystems, the chances of the secret key being compromised is reduced. Although theoretically, the public key can be used to determine the corresponding private key, its infeasibility (within time and cost constraints) is built over the 'difficulty' of solving certain mathematical problems.

Digital signatures are created and verified by using public key cryptography. An algorithm generates the two different and related keys: a private key and a public key. The private key is used to sign the document. The result of this encryption process,

which depends on the private key and the contents of the document, is the digital signature. The corresponding public key is used to verify the digital signature, because it alone can decrypt the message.

The application of the signer's private key on a message generates the digital signature. For every new message, the digital signature of the same person will be different. Therefore, if the contents of a message are altered, the digital signature will not match when verified by the recipient with the signer's public key. The integrity of the message is thus ensured. Since the verification of the digital signature can take place only through the public key of the signer, the identity of the signer is established. However, the identity of the signer must be bound to his or her public key by some entity in the physical space. The onus of verification of the identity of the individual rests with Certifying Authorities.

As noted earlier, knowing the public key, one cannot compute the corresponding private key belonging to the owner of the key pair. This is because it is computationally infeasible to derive a user's, private key from his public key. 'Computational infeasibility' is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance. The user can keep the private key on a smart card for access through a PIN or biometric identification such as a fingerprint or a retinal print. Digital signatures are unforgeable as long as the private key is not compromised.

14.7.3 The RSA Algorithm

One of the most popular and widely used public key cryptosystems is the RSA algorithm, developed in 1978 by Ron Rivest, Adi Shamir and Len Adleman of the Massachusetts Institute of Technology (MIT).

Two large prime numbers p and q are randomly chosen and their product $N = p \times q$ is computed. From the product $(p - 1) \times (q - 1)$, a number, e , is chosen such that e is relatively prime to $(p - 1)(q - 1)$ i.e. both $(p - 1)$ and $(q - 1)$ do not have any common factors with e . Similarly d is chosen such that d satisfies

$$de = 1 \bmod (p - 1)(q - 1) \quad \text{i.e. } de - 1 \text{ is divisible by } (p - 1)(q - 1)$$

The public key is then (N, e) while the private key is (N, d)

In order to encrypt a message M using the public key (N, e) , the value of $M^e \bmod N$ is calculated to produce the encrypted message E . For decrypting, calculation of $E^d \bmod N$ yields the original message M .

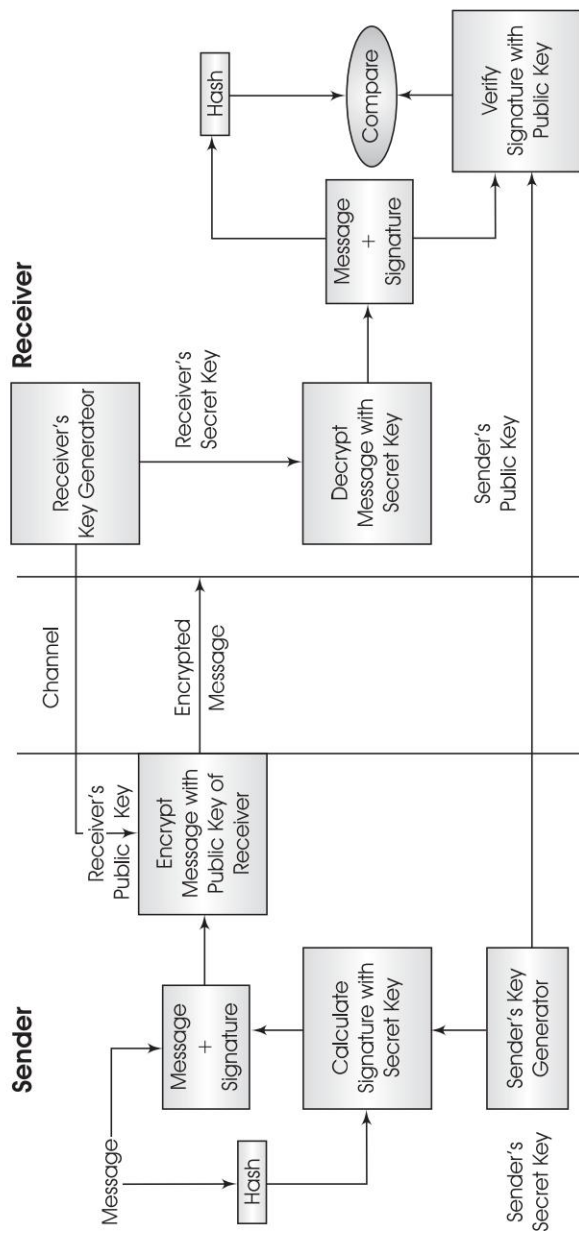


14.8 Digital Signatures

Digital signatures are used not only to verify the authenticity of the message and the claimed identity of the sender, but also to verify message integrity. The recipient, however, should not be able to use the received digital signature to falsely 'sign' messages on behalf of the original sender.

Using the RSA cryptosystem, a message is encrypted with the sender's private key to generate the 'signature'. The message is then sent to the destination along with this signature. The recipient decrypts the signature using the sender's public key, and if the result matches with the copy of the message received, the recipient can be sure that the message was sent by the claimed originator and that the message has not been modified during transmission, since only the originator is in possession of the corresponding encryption key. Figure 14.3 illustrates the implementation of Digital Signatures.

Although this is a highly secure way of digitally signing messages, it generates a large processing overhead. The size of the signature is the same as that of the original message, thereby resulting in a 100 percent increase in the data that is to be



➡ **Fig. 14.3** Implementation of digital signatures

handled. In order to reduce this processing load, hash functions are employed. Hash functions operate on large messages and generate message digests of fixed but much smaller lengths. These functions have the property that any change in the original message will result in a different message digest. Also, no two messages would result in the same message digest.

Processing overheads for implementing digital signatures can, therefore, be reduced by creating message digests and encrypting this digest with the private key to generate the signature. At the receiving end, the message digest is recalculated and compared with that generated by decrypting the received encrypted message digest using the sender's public key. If the two are the same, then the recipient is assured of the identity of the sender as well as the integrity of the message.

The RSA algorithm is widely used to implement digital signatures. The other popular algorithm is the Digital Signature Algorithm (DSA) developed by the US National Institute of Standards and Technology. The basic algorithm, which provides the security features, is different in DSA as compared to RSA, but the method of implementing digital signatures is essentially the same.

The hashing functions being used include algorithms such as Secure Hash Algorithm (SHA—160 bits, 224 bits, 256 bits, 384 bits, 512 bits) in conjunction with DSA and MD4 and MD5 (128 bits) Message Digest Algorithms from RSA Data Security Inc.

The most well-known and almost universally accepted method of electronic authentication including non-repudiation is the one based on asymmetric cryptosystems. This is also known as public key cryptography, and is the basis for creating digital signatures. However, rapid technological changes are challenging the supremacy of digital signatures as the only method of electronic authentication. Biometrics, are expected to be equally important in authentication for access control in the years to come.



14.9 The Public Key Cryptography Standards (PKCS)

The PKCS family of standards addresses the deployment of public key cryptography. PKCS covers several aspects such as RSA encryption, Diffie Hellman key exchange agreement, private key information syntax, etc. The standards consist of a number of components PKCS #1, #3, #5, #6, #7, #8, #9, #10, #11, #12 #13 and #15.

PKCS#1: RSA CRYPTOGRAPHY STANDARD

PKCS#3: DIFFIE-HELLMAN KEY AGREEMENT STANDARD

PKCS#5: PASSWORD-BASED CRYPTOGRAPHY STANDARD

PKCS#6: EXTENDED-CERTIFICATE SYNTAX STANDARD

PKCS#7: CRYPTOGRAPHIC MESSAGE SYNTAX STANDARD

PKCS#8: PRIVATE-KEY INFORMATION SYNTAX STANDARD

PKCS#9: SELECTED ATTRIBUTE TYPES

PKCS#10: CERTIFICATION REQUEST SYNTAX STANDARD

PKCS#11: CRYPTOGRAPHIC TOKEN INTERFACE
STANDARD

PKCS#12: PERSONAL INFORMATION EXCHANGE SYNTAX
STANDARD

PKCS#13: ELLIPTIC CURVE CRYPTOGRAPHY STANDARD

PKCS#15: CRYPTOGRAPHIC TOKEN INFORMATION
FORMAT STANDARD

For example, PKCS#7 is the standard for cryptographic message syntax. This includes data that may have cryptography applied to it for digital signatures.



14.10 The Protocols for Secure Messaging

Various messaging security protocols have been defined to provide security to messages that are being transmitted over the Internet. Security measures are applied to messages only

and are implemented at the user end itself. Some of the more well-known messaging security protocols are discussed here.

14.10.1 S/MIME

S/MIME or Secure MIME was developed by RSA Data Security Inc. for transporting secure messages, i.e. encrypted and/ or signed messages using MIME. The new content type application/ x-pkcs7-mime was defined to handle MIME body parts.

14.10.2 PGP

PGP or Pretty Good Privacy software was developed by Phil Zimmerman to provide security services such as encryption and digital signatures. PGP has been widely used and owes its popularity to the fact that it is freely available for non-commercial use. A commercial version of PGP is also available. However, the main difference is in its handling of public keys. It has its own certificates and certification is done by PGP users themselves through a web of trust.



14.11 Key Management

As seen in the previous sections, technology solutions have developed to implement different security services with varying degrees of strength and reliability. Whatever be the cryptographic scheme being used, all these solutions depend on encryption using keys—either single or in pairs.

In the symmetric method, there would exist unique secret keys for every partner with whom the originator wants to engage in secure communication. The asymmetric system is different. An organisation ABC needs to have only one secret key, no matter how many partners are to be securely communicated with. ABC's public key however should be known to each one

of those business partners, and, in turn, ABC should know the public key of each and every one of these business partners.

Proper management of these keys is critical in ensuring secure storage and transmission to communication partners. This includes key generation, distribution, key revocation, key destruction and, in some cases, key escrow. From the method of key generation discussed earlier, it is evident that to generate keys that are not susceptible to attack, the randomness of the initial number(s) selected plays a very important role. Key revocation could become necessary when there is evidence that a key has been compromised. Key escrow allows the recovery of a key if it is lost or otherwise unobtainable. This could be accidental, or in the case of an employee who is leaving, the organisation would not have to rely on the employee for 'returning' the keys. Key escrow could be a statutory requirement in some countries.

There are two aspects to key distribution—one where secret keys in the symmetric method are exchanged, and the other where public keys are made known to everyone. The case of symmetric keys can be handled either by the use of 'master' keys (there will be one for each pair of communicating systems; symmetric key will be encrypted by the 'master' key before transmission), or by using the Diffie-Helman method. In this method, each party in a pair of communicating parties calculates public values based on separately generated secret values. These public values are then exchanged and in conjunction with the secret value both these systems generate the same key, which can be used as a secret symmetric key. The RSA algorithm-based public key cryptosystem can also be used to achieve confidential key exchange.



14.12 Public Key Certificates

In the case of public key cryptosystems, the secret private key is not shared with anyone; it is closely held by the owner of the

key. While it is important for the public key to be made 'public', what is also important is the fact that the user of the public key should be assured that it is indeed the public key of the entity to whom it is purported to belong. The public key should be available to anyone who wants to engage in secure communication with the owner of the corresponding private key.

Public keys are normally distributed in the form of certificates which are issued by Certification Authorities or CA. The CA 'signs' the certificate which legally binds the public key with the claimed identity of the owner of the public key. This prevents a miscreant from masquerading as someone else and getting hold of secret communications, i.e. it ensures that the key obtained from the certificate is the correct public key of the intended recipient.

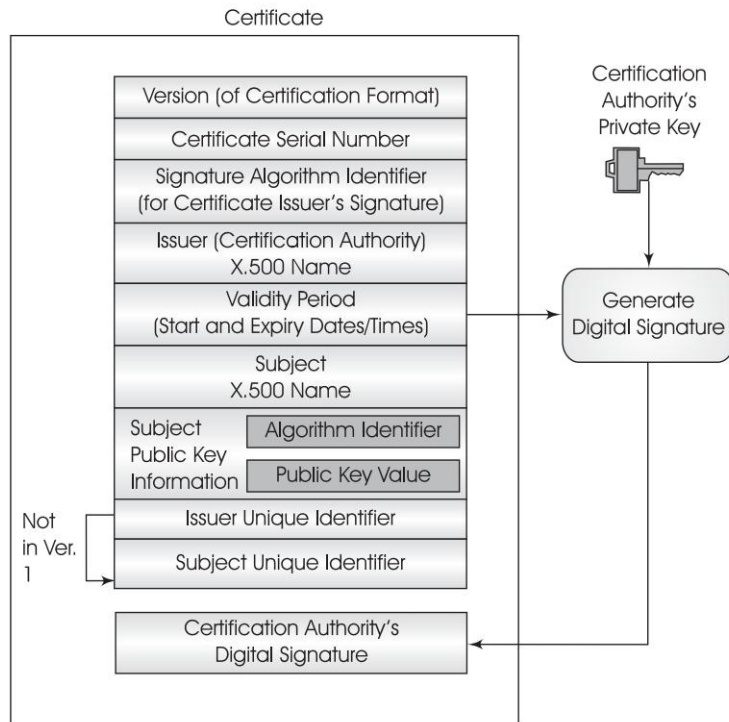
Given the nature of trust required to be established in a Certification Authority and the potential number of users of certified public keys around the world, it is not feasible to have a single CA serving the entire user community. Multiple CAs would therefore be required to be set up. The most suitable model is the hierarchical one in which a chain of CAs called the Certification path is built up with each CA being certified by a CA at the immediately higher level.

14.12.1 X.509 Certificates

Certificates are issued by Certifying Authorities to users who wish to engage in secure communication. While the private key is securely held by the owner of the private-key/ public-key pair, the public key is made available in the form of certificates for everyone else to use. Along with the public key, the certificate which has to be digitally signed by the CA also contains other relevant information such as validity period and details about the CA which has issued the certificate.

The standard certificate format is the X.509 certificate format which is contained in the Authentication Framework of the X.500

Directory. The versions 1 and 2 of the X.509 certificate format are as shown in Fig. 14.4.



➞ **Fig. 14.4** X.509 versions 1 and 2 certificate format

Individually the fields contained in the X.509 certificate format described above are as follows:

- Version, whether 1 or 2
- Serial Number issued by the CA
- Signature Algorithm which has been used by the CA for signing the certificate
- Issuer's (i.e. the CA's) name
- Validity period of this certificate
- Subject containing the X.500 name of the holder of the corresponding private key

- Subject public key information comprising the key value and the algorithm to be used when encrypting with this public key
- Issuer unique identifier for unique identification of the CA (not in version 1)
- Subject unique identifier for unique identification of the subject (not in version 1)
- CA's digital signature

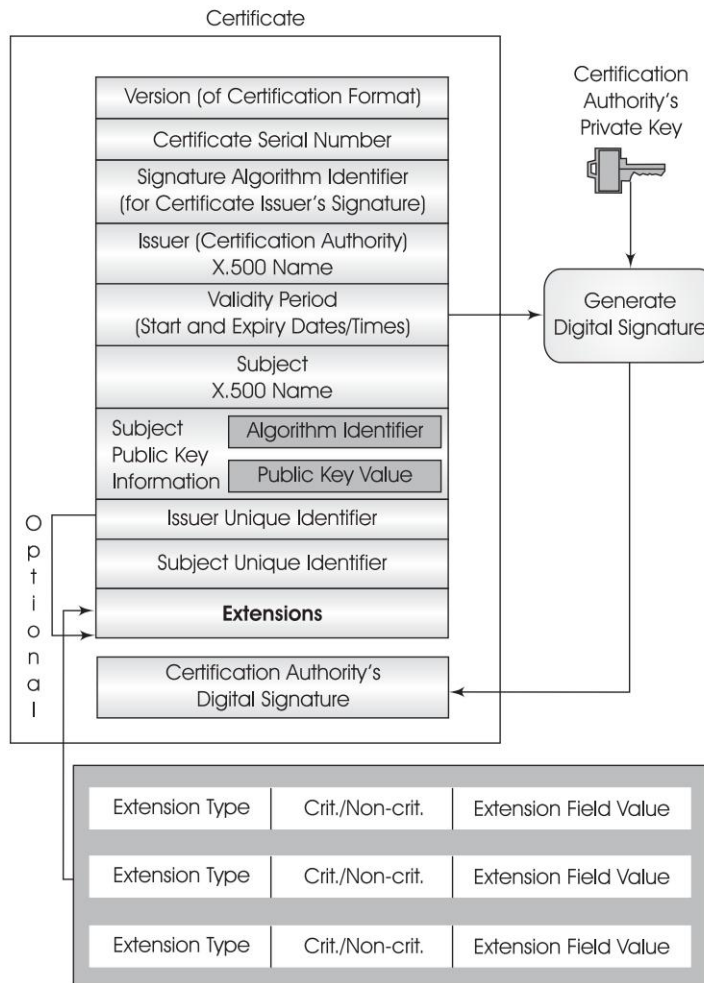
Version 1 was developed in 1988, whereas version 2 was developed in 1993. During the 1993–94 period when trials were on, it was discovered that X.509 was deficient in certain respects. This included the need to support multiple certificates (corresponding to different uses) for any individual user and identification of users by means other than X.500 name e.g., e-mail address and also additional identification information. In order to counter this, version 3 was developed to contain extension fields in addition to the information already contained in version 2 of the X.509 certificate format. This is shown in Fig. 14.5.

Each extension has to be identified by a type (beyond the scope of this discussion) and followed by the actual value and its criticality factor.

A standard format for a Certificate Revocation List(CRL) is also defined by X.509. This X.509 CRL format contains information on:

- Version
- Signature of the CA
- Issuer (identification of CRL issuer)
- Date and Time of release of this CRL
- Date and Time of release of next CRL
- Serial number(s) of the certificate(s) being revoked
- Date of revocation of the certificate(s)
- Extensions as in X.509 (version 3) certificate format

Before using any public key certificate, the CRL of the issuing CA should be checked. If the public key certificate is on the CRL, it should not be relied on in any communications.



➞ **Fig. 14.5** X.509 version 3 certificate



14.13 Other Authentication Mechanisms

Authentication mechanisms are used to satisfy the user that entities—people, data, applications or computers—are actually what they claim to be. One of the most commonly used mechanisms for authenticating people has been the password. Passwords are expected to be known only by the owner. The

onus is on the owner to keep his password secret. However, passwords can be guessed or learnt by intruders through interception of communications networks or re-use of encrypted passwords. Re-use of passwords can be prevented by time-stamping or by using passwords only once. Another mechanism is the challenge-response system in which the host throws a random 'challenge' to the entity being authenticated, which, in turn, has to send an appropriate 'response' for validation at the host.

Kerberos, developed at the Massachusetts Institute of Technology (MIT), is an authentication mechanism entirely based on symmetric cryptosystems based on DES. Although Kerberos provides adequate protection, its limitations are in the need for ensuring reliable servers with high degrees of availability and in synchronising time clocks throughout so that the re-use of passwords can be detected. Kerberos is also not highly scalable.

Smart Cards are similar to credit cards except that they have chips embedded in them. These cards can be used to carry authentication information.

Other technologies (biometrics) that are being used to provide authentication services include recognition of fingerprints, voice and handwriting, retinal scan and resultant measurements of the signing event such as typing rhythm and pressure exerted during input.

Digital signature, which is discussed earlier in this chapter, is also used for providing authentication based on two-key cryptosystems.



14.14 Guidelines for Cryptography Policy

Although technology solutions have been developing for the provision of a variety of security requirements, the deployment of these technologies by companies and organisations can often turn out to be in disagreement with the security rules as laid down by national governments for their own countries.

In March 1997, the Organisation for Economic Co-operation and Development (OECD) adopted the guidelines for cryptography policy identifying eight principles for national legislation. These are:

- The cryptography methods should be trustworthy in order to generate confidence in their use.
- Users should be free to choose any cryptography method based on their security requirements.
- Cryptography methods should be developed in response to the needs of businesses, individuals and governments.
- Technical standards and protocols for cryptography should be developed and promulgated at the national level.
- The fundamental rights of individuals to privacy should be protected.
- National policies may allow lawful access to plaintext, cryptographic keys and encrypted data.
- Liabilities of individuals and entities that offer cryptographic services should be clearly stated.
- Governments should co-operate in co-ordination with cryptographic policies.

Although the guidelines recognise the need for some state controls over the use of cryptography, it is stressed throughout that these must ‘respect user choice to the greatest extent’.

Similar considerations exist in the framework for providing electronic commerce services on the Global Information Infrastructure. The requirements have evolved from the use of e-commerce over the Internet, which has been the forerunner of the National Information Infrastructure and the GII.

According to the framework for Global Electronic Commerce, a secure GII requires:

- secure and reliable telecommunications networks
- effective means for protecting the information systems attached to those networks
- effective means for authenticating and ensuring confidentiality of electronic information to protect data from unauthorised use

- well-trained GII users who understand how to protect their systems and data.

Accomplishing this goal requires a range of technologies such as encryption, authentication, password controls, firewalls, etc., and consistent use of these technologies. All this should be supported by trustworthy key and security management infrastructures.

The OECD Guidelines for Cryptography Policy are available in Appendix 8.



14.15 Virtual Private Networks

A Virtual Private Network (VPN) uses the open, distributed infrastructure of the Internet to transmit data securely between corporate sites.

Connections are set up to the local points-of-presence (POP) of their ISP, which ensures that the data is transmitted to the appropriate destinations. Since the Internet is an open public network, Internet-based VPNs encrypt data passed between VPN sites, thus making sure that the data is secured against eavesdropping and tampering by unauthorised parties.

If VPNs are to be relied on by corporates and other institutions as they would upon dedicated leased lines or other WAN links, security and network performance must be guaranteed on the Internet.

The four critical functions of authentication, access control, confidentiality and data integrity must be maintained during data transmission from source to destination.

In the past, private networks were created by leasing hard-wired connections between sites; these connections were devoted to the traffic from a single corporate customer. On the Internet, where the traffic from many users usually passes over the same connection, tunneling allows senders to encapsulate their data

in IP packets that hide the underlying routing and switching infrastructure of the Internet from both senders and receivers. At the same time, these encapsulated packets can be protected against snooping by outsiders by using encryption techniques.

Unlike the leased lines used in traditional corporate networks, VPNs do not maintain permanent links between the sites that make up the corporate network. Instead, when a connection is needed between two sites, it is created; when the connection is no longer needed, it is torn down.

The protocol, IPSec, grew out of the need to secure IP packets as the next generation of IP (IPv6) was being developed; it can be used with IPv4 protocols as well. For exchanging and managing the cryptographic keys used to encrypt session data, Internet key exchange (IKE) is an IETF standard protocol for securing VPNs.

IPSec allows the sender (or a security gateway acting on his behalf) to authenticate and/ or encrypt each IP packet. Security gateways prevent unauthorised intrusion into the private network, in addition to providing tunnelling and encryption capabilities. These could be in the form of routers, firewalls, integrated VPN hardware or VPN software.

IPSec is built around a number of standardised cryptographic technologies to provide confidentiality, data integrity and authentication. For example, IPSec uses:

- Diffie-Hellman key exchanges to deliver secret keys between peers on a public net
- Public key cryptography for signing Diffie-Hellman exchanges, to guarantee the identities of the two parties and avoid man-in-the-middle attacks
- Data encryption standard (DES) and other bulk encryption algorithms for encrypting data
- Keyed hash algorithms (HMAC, MD5, SHA) for authenticating packets
- Digital certificates for validating public keys.

IPSec is often considered the best VPN solution for IP environments, as it includes strong security measures—notably encryption, authentication, and key management—in its standards set.



14.16 Developing a Security Policy

14.16.1 Thumb-rules

- Maintain and enforce organisational information systems security policies.
- Strictly enforce the physical security of the computer and network equipments.
- Harden the operating system; disable any unwanted services.
- Ensure that the audit trails are turned on.
- Track and audit defensive steps. Regularly check logs.
- Install adequate security software to recognise attacks.
- Use strong passwords; choose passwords that are difficult or impossible to guess. Give different passwords to different accounts.
- Make regular back-ups of critical data; maintain current back-ups of all important data. Back-ups may be made at least once each day. Larger organisations may perform a full back-up weekly and incremental backups every day. At least once a month, the back-up media may be verified.
- Do not keep computers online when not in use. Either shut them off or physically disconnect them from the Internet connection.
- Do not open e-mail attachments from strangers, regardless of how enticing the subject line or attachment may be. Be suspicious of any unexpected e-mail attachment from someone you do know because it may have been sent without that person's knowledge from an infected machine.
- Regularly download and update security patches, and signatures from your software vendors.

- Report security incidents to Incident Response Teams, and Law Enforcement.
- Maintain back-ups of all original operating system software and applications.
- Place a banner on the system to notify unauthorised users that they may be subject to monitoring.
- Routinely test the computers and network for vulnerabilities.
- Keep an up-to-date inventory of the hardware, software operating system and applications to speed up the identification of specific vulnerabilities that could affect the organisation.
- Prioritise vulnerabilities based on the potential risk to the business and address those with the highest level of risk first.
- Develop procedures for quickly applying fixes to particular vulnerabilities.
- Keep track of who is responsible for specific vulnerabilities and whether the correct fixes were successfully applied.
- Change logins/ passwords frequently.
- Cancel logins/ passwords when employees leave your organisation.
- Install vendor patches for known vulnerabilities
- Maintain most current updates to anti-virus software.
- Restrict/ monitor network access to internal hosts.
- Develop an organisational computer incident response plan and establish contact with the national Incident Response organisation, namely CERT-In.

14.16.2 Security Technologies

- Access control to computer facilities and network infrastructure must be adhered to at all times. The use of advanced technologies like biometrics and digital IDs is recommended.
- Encrypted logins and encrypted files should be used wherever possible.

- Enable packet filtering and access control list on routers.
- Use a firewall as a gatekeeper between the organisation and the Internet.
- Use an Intrusion Detection System (IDS) for identifying/thwarting network-based attacks.
- Anti-virus software must be used to help protect against executable based attacks.
- For an organisation, a three-tier virus protection strategy may be considered which includes virus protection at the gateway level, server level and the client level.
- Install anti-virus software on the computer in the first place, check periodically for new virus signature updates, and then actually scan all the files on the computer periodically.
- Use authorisation tools to validate users for remote access.



14.17 CERT-In

The Indian Computer Emergency Response Team (CERT-In) was established in 2003 to be a part of the international CERT community with the specific mandate to respond to computer security incidents reported by the entire computer and networking community in the country. Its express responsibility is to enhance cyber security in the country. CERT-In was established with the mission to enhance the security of India's communications and information infrastructure through proactive action and effective collaboration. The purpose of CERT-In is to become the nation's most trusted referral agency of the Indian community for responding to computer security incidents as and when they occur. CERT-In will also assist members of the Indian community in implementing proactive measures to reduce the risks of computer security incidents. The objectives, functions, role and activities are available in detail in Appendix 10.



Chapter 15

Cyber Crimes



15.1 Introduction

In the preface to the first edition of this book, we observed that, “the Internet knows no geographical boundaries in the world. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet.” The Internet has indeed grown very rapidly, and permeated every sphere of human activity. Diffusion of the Internet in society has taken place at a pace which was unknown with earlier technologies such as the radio and TV. Internet commerce tools are at the heart of applications in the fields of communication, work, study, education, interaction, leisure, health, trade and commerce. This has resulted in redefining some of these activities such as e-learning, e-business, e-books, e-entertainment, and e-health similar to e-commerce, and e-governance.

While this presents an unparalleled opportunity for the people of the world to improve the quality of their lives and for the betterment of society, there is a price to be paid for the same. Like the other side of a coin, Internet commerce tools can be used for evil purposes too. This is because Internet systems are vulnerable targets for attack. Systems that are not securely configured, and/ or not patched for known vulnerabilities are easy prey to cyber attacks. Criminals and ill-motivated persons can

attack and disrupt computers and computer networks. They can promote hatred and racism, advocate violence and promote acts of destruction and vandalism using the same Internet. A new breed of computer criminals has come into being to disrupt the Internet, and all Internet-based applications such as e-commerce, electronic banking and dissemination of information by the governments and other commercial enterprises. They are also threatening the society in newer ways. Criminals can conduct their operations from any of the computers located anywhere in the world leaving no trail to track them. It can be extremely difficult to track the source of a crime. Even if they can be tracked, it is difficult to bring the culprits to book because of the lack of laws in dealing with crimes that are committed in a country while they may have originated in a different country.

The Internet had its origins in the academic and research world and was subject to no central control. There was no effective regulation to govern the Internet. It was supposed to be all about freedom and democracy without any obligation. The healthy self-regulation imposed upon the Internet by its creators, and which was responsible for its tremendous growth, was found to be inadequate to cope with the crimes that began to be committed in cyberspace. The governments and international bodies gradually stepped in to regulate the Internet through Cyber Laws. The widespread reaction of the governments to control cyber crimes has led to the enactment of laws for controlling computer misuse and frauds. Law enforcement agencies are being vested with powers to intercept online communications. For example, The Regulation of Investigatory Powers Act in Britain gives police access to e-mail and other online communications. Singapore has blocked access to pornography sites. South Korea has blocked access to gambling sites. The United States has passed a law which requires schools and libraries that receive federal funds to install software on the computers to block material that is harmful to the youth. The PATRIOT Act of USA gives law enforcement agencies powers to intercept any online communications. The Information Technology Act, 2000 in India also provides for

interception under certain conditions. The Council of Europe has passed the Cyber Crimes Treaty, which aims to harmonise laws against hacking, cyber fraud, and child pornography.

Cyber crimes can be effectively managed with whatever laws are in place provided they can be investigated in a way to gather sufficient evidence for prosecuting criminals. The examination of computers, communication equipment and systems for obtaining information for criminal or civil investigations has come to be known as forensic computing, or cyber forensics. This field is presently in its infancy, but is growing. The requirements of forensic computing are beginning to impact future telecommunication systems and services. On the one hand, it seeks to make computer and communication systems more secure, while on the other, cyber forensics helps investigators unearth evidence from cyberspace since the scene of the crime may well be spread all over it. Evidence thus collected is known as digital evidence.

There is a view, which has gained ground in recent years, that since the Internet does away with geographical boundaries, it also does away with territorial-based laws. Individuals and businesses are establishing their websites in various countries depending upon the advantages they perceive because of local laws. This has led to the creation of competition between jurisdictions. For example, the United States with its constitutional guarantee of the right to free speech, has become a safe haven for neo-Nazi propaganda and memorabilia that are illegal under the German Law. Recently a French Court has ordered the Internet portal Yahoo; to find ways of blocking the nasty neo-Nazi materials posted on its American websites so that the French could not see them. Likewise, a number of pornography sites located in the US are perfectly legal there, but other countries are trying to block access by their citizens as per their own territorial laws. Legal cases launched for prosecution in one country run into problems of jurisdiction. The question of jurisdictional problems created by the Internet will take quite some time to resolve through the laws. These have been addressed in Chapter 13 on legal issues.

The Internet is an easy tool for committing traditional crimes in cyberspace at a speed which is unknown. Individuals and groups can actively engage in crimes using the very tools that the Internet provides for the benefit of people at large. For example, criminals can exchange information through e-mail, post data and innocuous looking messages in chat sites, encrypt messages using cryptographic techniques, and hide messages in innocent images such as photographs. They can keep in touch and form groups. The crimes they can commit include cyber thefts, financial embezzlement, banking frauds and economic espionage. Some of the other areas which affect society include harassment of citizens in cyberspace, cyber defamation, threats to life, cyber frauds, spreading obscenity, spreading hate messages and spreading racism. Websites can be destroyed by people for competitive gains in business, or the websites of the competition can be made ineffective. There are other cyber crimes which are unique to cyberspace, i.e. they have no equivalents in the real physical world. Hacking as a term was invented only in the context of a computer code which can destroy working computer systems partially or completely. Child pornography, though present in society in a very restrictive manner earlier, has become an evil of menacing proportions in cyberspace, which can harm innocent children connected to the Internet for learning and games. Yet another area which has been spawned by the Internet is information warfare. It takes the form of economic espionage, on the one hand, while on the other, it can create a situation wherein the information infrastructure of an organisation is made ineffective. The most common known method for the latter category is the denial of service. The list of cyber crimes is endless.

Cyber crimes are expanding with the growth of the Internet. As the Internet leads to a more connected society and citizens use it more and more to gain full advantages of the information age, governments have the onerous responsibility of protecting them in cyberspace. Countries are enacting laws to deal with computer misuse and frauds; international organisations like the UN, G8, and OECD countries are creating model cyber crime

laws as a guide to enactment by member countries. The European Cyber Crimes Treaty, signed by member countries of the European Union and some other observer countries, is the most comprehensive regime to deal with the new menace facing the global world.

This chapter is organised as follows. Section 15.2 defines cyber crimes. The adequacy of the IT Act, 2000 for dealing with cyber crimes is examined in section 15.3. Cyber forensics is discussed in section 15.4. The European Cyber Crimes Treaty is analysed in section 15.5. The role of the Computer Emergency Response Team in enhancing cyber security to prevent the occurrence of cyber crimes is briefly covered in the last section.



15.2 Cyber Crimes

Cyber crimes use computers and networks for criminal activities. Computers can be used for committing a crime in one of the following three ways:

- As a tool
- As a target
- Both as a tool and a target.

The first type of crime is basically an extension of 'real world' crimes, such as forgery, fraud or copyright piracy using computers. Existing laws can be used to bring criminals to justice.

The second type of crime is a real cyber crime in which culprits damage or modify the victims' computer systems and networks through illegal access, and cause heavy loss to the victims. They are unique in that they occur in cyberspace. There is no physical equipment of such a cyber crime, since the target of attack is a computer system. A criminal may launch a virus, worm, or a Trojan to attack a target computer system or network. Existing laws are inadequate to prosecute such crimes. They require special computer crime, and/ or misuse laws.

Hackers exploit known vulnerabilities in various systems. They write codes to exploit these vulnerabilities to gain unauthorised entry into systems and networks, and engage in activity that threatens their security. The malicious code created may be in the form of viruses, worms, or Trojans. These have been defined in Chapter 14 on security issues.

The third type of crime is the one in which computers are used both as a tool as well as a target.

A partial list of cyber crimes is as follows:

- Hacking of computer systems and networks
- Cyber pornography involving production and distribution of pornographic material, including child pornography
- Financial crimes such as siphoning of money from banks, credit card frauds, money laundering
- Online gambling
- Intellectual property crimes such as theft of computer source code, software piracy, copyright infringement, trademark violations
- Harassments such as cyber stalking, cyber defamation, indecent and abusing mails
- Cyber frauds such as forgery of documents including currency and any other documents
- Launching of viruses, worms and Trojans
- Denial-of-service attacks
- Cyber attacks and cyber terrorism
- Economic espionage
- Consumer harassment and consumer protection
- Privacy of citizens
- Sale of illegal articles such as narcotics, weapons, wildlife, etc.

Cyber crimes that can generally occur within organisations are as follows:

- E-mail abuse
- Spam mails
- Cyber defamation

- Theft of source code
- Exchange of business secrets and documents
- Insider attacks on personnel databases
- Use of office computer for running other businesses
- Transmission and viewing of pornographic materials
- External cyber attacks on an organisation resulting in denial-of-service
- Information espionage



15.3 Cyber Crimes and the Information Technology Act, 2000

The IT Act, 2000 notified for implementation in October 2000, explicitly deals with the following categories of cyber crimes only:

- Tampering with a computer source code
- Hacking
- Publishing any information which is obscene
- Breach of privacy
- Misrepresentation
- Publishing digital signature which is false in certain particulars or for fraudulent act.

It is obvious that it is silent on many types of cyber crimes. It was probably logical since the Act was written with a view to promote the growth of e-commerce and e-governance as is stated in its preamble. Its primary object was to create trust in the electronic environment by providing electronic authentication through the use of digital signatures based on asymmetric cryptosystems. Some types of crimes which relate to e-commerce and e-governance were included in the Act with a view to increasing trust in the smooth conduct of these activities over the Net. It is not a special Act for preventing abuse and misuse of computer systems using networks in the normal social intercourse of individuals and organisations in the context of the multifarious uses of the Internet. Many countries have

enacted specific laws dealing with Internet crimes or cyber crimes. For example, USA has the PATRIOT Act. Singapore, Malaysia, Britain, South Korea, and Japan have implemented similar laws.

Chapter XI of the IT Act lays down offences that are criminal in nature, and prescribes punishments. Section 65 describes tampering with computer source documents as an offence. Section 66 defines hacking as, “whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.” This definition of hacking covers virus, worm and Trojan. It is an all-inclusive way to define ‘malicious code’.

Section 67 deals with pornography, and prescribes punishments for publishing obscene information on a website, which increase if the offence is repeated.

Section 69 provides for interception, under certain conditions, of any information transmitted through any computer resource by law enforcement agencies. Section 70, on the other hand, describes unauthorised access to ‘protected systems’ as an offence, and prescribes very severe punishment.

It is interesting to observe that gaining unauthorised access to computer systems with a view to download data, or damage the system, or alter the data, or disrupt services, so as to cause loss to the victim, is deemed as a civil offence too. Section 43 defines this in detail, and prescribes the damages that may be payable as compensation by the offender. The damages may be assessed by an adjudicating officer, appointed by the government, to whom an application can be made by the victim. The relevant sections are detailed in Chapter IX of the IT Act. Civil case for claiming compensation due to damages caused by an intruder or hacker can be filed by the victim in addition to filing a criminal complaint with the police under Section 66 for hacking.

Cyber laws, in general, need to take into account the fact that in a cyber crime, the computer is used either as a tool, or as a target, or both as a tool and target. In the former category, the computer is used as a tool to commit a crime in the physical world such as a forgery, fraud, financial embezzlement, etc. Such crimes can be dealt with to punish criminals under existing laws, for example, the Indian Penal Code.

In attacks on computers as a target, however, issues related to confidentiality, integrity and availability of information systems and services are at stake. Launching of viruses, worms and Trojans to damage computer systems and networks is a major cyber crime. This is because it can disrupt services. A cyber attacker or hacker can launch these attacks from anywhere in the world. Tracking the criminal can be very difficult, especially because there is no physical evidence at the scene of crime. In fact, the scene of crime may well be extended over several computer servers and networks across the globe. The laws must, therefore, be supported by appropriate procedural laws, rules and procedures to preserve evidence, and collect the same.

The rules must provide for the preservation of records on Internet servers, routers and other devices of ISPs and organisations. In the absence of this, there would be no digital data available as evidence to help prosecute a criminal. Appropriate procedures and forensic tools must also be available to collect digital data from the 'scene of crime' in such a manner that it is acceptable in a court of law. Moreover, there must be ways and means to collect data from abroad. Either the criminal may be located abroad, or servers, from where attacks are launched, may be located abroad. With the growth of cyber crimes it has become imperative for countries to designate point-of-contact on a 24 × 7 basis so that crimes reported by any country are acted upon immediately by another country hosting criminals or servers. This necessitates the availability of computer forensic experts and laboratories for gathering digital evidence. India is in the process of setting up cyber forensic laboratories.

Finally, cyber laws must recognise jurisdictional issues, and address them appropriately. Section 75 of the IT Act provides for bringing a cyber criminal to justice irrespective of his nationality and location anywhere in the world. US laws also have similar statutes. In practice, however, problems of jurisdiction are proving to be rather difficult to surmount by the investigators and law enforcement agencies. Different countries have differences about perception and definitions of crimes. An activity deemed criminal in a target country may not be considered so in the country from where the offending action was launched. For example, pornography websites are perfectly legal in the US, while accessing them from India may be an illegal activity. The cyber world is indeed complex. The borderless nature of transactions in cyberspace calls for innovation in framing national laws so as to protect the national ethos and yet bring criminals to justice.



15.4 Cyber Forensics

Cyber servers accessed via network routers and other network devices such as firewalls, and intrusion detection systems, by individuals from their PCs in homes and organisations, form the scene of investigation when a cyber crime is committed. In the latter case, routers and proxy servers as well as firewalls, IDS may contain important data. The servers, firewalls and routers of an ISP may also contain data significant to the investigation of a crime, and these may be located anywhere in the world. Thus the scene of crime may be 'all over the place'. This makes the task of investigation extremely difficult. Coupled with this is the possibility that the data at any of the locations may have been deleted or overwritten. There may not be laws, or procedural laws mandating ISPs and organisations to preserve data for a certain period of time, say three months to a year.

Crimes can be committed by using open proxy servers, spoofing IP addresses, installing viruses on victim machines and using these to launch attacks on other systems and

networks. A spam can be generated to target a system. Criminals can erase evidence, and all footprints that they were ever there, can be erased. In fact, digital evidence can be modified by them in such a way that the attacks may appear to have been launched from an innocent victim's system. This makes it even more challenging for the investigator to unearth evidence. The challenge is, therefore, to devise techniques to gather evidence and prepare it effectively before the court so that the criminal is brought to justice. This area of crime analysis is called cyber forensics.

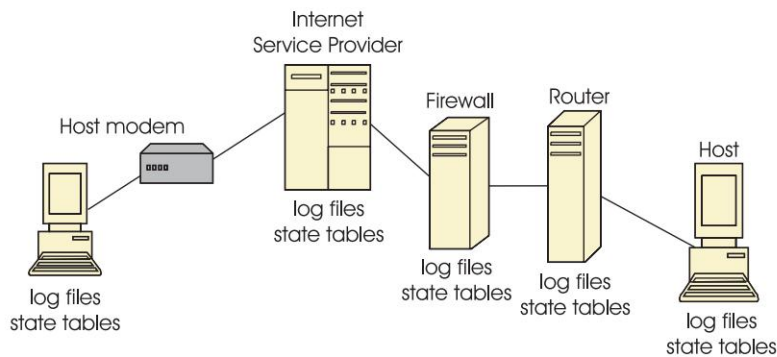
Cyber forensics can be defined as the process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability. The challenge, of course, is actually finding this data, collecting it, preserving it, and presenting it in a manner acceptable in a court of law.

Electronic evidence is fragile and can be easily modified. Additionally, cyber thieves, criminals, dishonest and even honest employees hide, wipe, disguise, cloak, encrypt and destroy evidence from storage media using a variety of freeware, shareware and commercially available utility programs. The technology used by cyber forensics should be able to face these challenges.

There are two distinct areas in cyber forensics, i.e. computer forensics and network forensics. Computer forensics entails gathering of evidence from computer media seized at the crime scene. The concerns at this stage involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes. In this case, evidence resides on computer systems, essentially under file system and slack space. Unallocated space too has a bearing on evidence. Specifically, the following are examined:

- Logical file system
 - File system
 - Files, directories and folders, FAT, clusters, partitions, sectors

- Random Access Memory (RAM)
- Physical storage media
- Magnetic force microscopy, which can be used to recover data from an overwritten area
- Slack space
 - Space allocated to a file but not actually used due to internal fragmentation
- Unallocated space

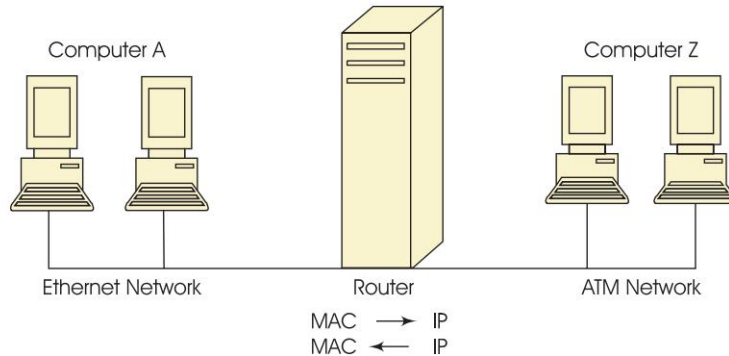


➞ **Fig. 15.1** Evidence on transport and network layers

Network forensics, on the other hand, is technically more challenging. It gathers digital evidence that is distributed across large-scale, complex networks. Often this evidence is transient in nature and is not preserved within permanent storage media. Network forensics deals primarily with an in-depth analysis of computer network intrusion evidence, which may be spread over distributed resources. Evidence in this case resides on routers and other network devices. Each of the following layers under the Internet Protocol has to be examined for evidence:

- Application Layer (web pages, online documents, e-mail messages, news group archives, archive files, chat room archives)
- Transport Layer (log files/ state tables)

- Network Layer (log files/ state tables)
- Data Link Layer (machine (MAC) address vis-à-vis IP address).



➞ **Fig. 15.2** *Evidence on the data link and physical layers*

In order to prevent the inadvertent loss of digital evidence, specific procedures are prepared. Cyber forensics experts perform the following duties:

- Seizing and collecting digital evidence at a crime scene
- Conducting an impartial examination of submitted computer evidence
- Testifying in a court of law as required.

This requires that investigating officers of law enforcement agencies are trained to address the following issues:

- To secure the crime scene
- To seize a computer
- To acquire the evidence
- To preserve the evidence
- To analyse the evidence
- To present the evidence.

Computer forensics is a complicated technical process wherein computer media is first imaged by the examiner. This is required to keep the authenticity of the original evidence. In computer forensics, the analysis is done only on the image of the

suspect hard disk. This brings in another issue of ensuring authenticity of the evidence. For this, a technology called hashing is used to assert that if the hash value of the original evidence is equal to the hash value of the image, then the image is as authentic as the original. Hashing has been described in detail earlier in the context of digital signatures.

The analysis involves recovering of deleted files and folders, and examining evidence. The history of the usage of the files is one of the important aspects in creating the report. This provides the investigator with enough information to corroborate with other evidence. The analyst has to create a detailed report and present it to the court. The court, in turn, must be trained enough to appreciate the presented digital evidence



15.5 The European Cyber Crimes Treaty

Various countries have responded to the rising cyber crimes in different ways. Some have enacted laws to deal with specific crimes. Some other countries have tried to use technical means to block some offensive websites. Governments have used powerful Internet tools for the purpose. Filtering is one such tool. It is a software installed on a PC in an ISP's gateway that can help block access to certain websites for all its subscribers. The websites themselves can also block users. This technology was the basis for the French ruling against Yahoo! in the sale of Nazi memorabilia from its US websites. This is known as the IP-address tracking. But both filtering and IP-address tracking are far from perfect. Filters can block too much or too little. Smart Internet users can block IP-address tracking by using other tools.

The global nature of cyberspace and its relationship with the physical world, spanning all countries connected to the Internet, calls for global action to fight cyber crimes. The role of governments, and co-operation among investigating agencies is central to this effort. The Cyber Crimes Treaty prepared by the Council of Europe addresses major issues of crimes, and also

makes it contingent upon member states to enact laws in their respective countries to deal with them.

The object of the Treaty, as stated in the preamble, is to pursue, “a common criminal policy aimed at the protection of society against cyber crime, *inter alia* by adopting appropriate legislation and fostering international co-operation.” It recognises the profound changes being brought in society by the convergence of computer, communication and broadcasting due to digitalisation, and the continued globalisation of networks. These very computer networks and electronic information exchange and delivery methods are also being used for committing criminal offences. The Treaty is aimed at member states adopting sufficient powers “for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation”. While it aims at harmonising laws against hacking, Internet fraud and child pornography in member states, it is equally alive to protecting the privacy of individual, and all the human rights. It reaffirms “the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.”

The Treaty advises all members to take measures at the national level in the form of enacting substantive criminal laws which provide for offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; offences related to infringement of copyright and related rights; ancillary liability and sanctions. Child pornography is explicitly included as an offence. Illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud are clearly defined. While IPRs are protected, corporate liability is also sought to be fixed.

The Treaty also advises member states to clearly establish appropriate procedural laws to deal with cyber crimes, through

the adoption of suitable legislative and other measures. Collection of evidence in electronic form for criminal offences committed by means of a computer system shall be through such procedural laws for the purpose of specific criminal investigations or proceedings. It includes guidelines for the expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data. Moreover, it mandates that the competent authorities can order “a person in its territory to submit specified computer data in that person’s possession or control which is stored in a computer system.” Similarly, authorities should also be empowered to order a service provider, offering services in its territory, to submit subscriber information relating to such services for purposes of investigation.

The Treaty also includes search and seizure of stored computer data. Member states are advised to adopt legislative and other measures to collect or record, through application of technical means, on their territory, all the real-time traffic data. The service providers must be made to comply with this, as also to help in interception of content data.

Issues related to jurisdiction over any offence, and international co-operation relating to extradition and mutual assistance in dealing with computer crimes have been addressed too. Mutual assistance regarding investigative powers is the highlight of the Treaty, so much so that each country is supposed to designate a point-of-contact available on a 24-hour, 7-day per week basis in order to ensure the provision of immediate assistance for the purpose of investigation. Laws along these lines are likely to be enacted by member states of the Council of Europe, and observer states such as the USA, Canada, and Japan, which have signed the Treaty. The world is thus gearing up to face the challenge of cyber crimes through the enactment of new laws, investigative procedures, and international co-operation in dealing with cyber criminals on a global basis. It must be borne in mind that all the traditional crimes in the society with all the plethora of national and international laws,

international treaties have not been eliminated. In fact, crimes have continued to rise with the growth and development of mankind. The new laws cannot therefore, be expected to solve the problems of rising cyber crimes. But they will certainly deter cyber criminals, and make their apprehension somewhat easier.

The Internet advocacy groups, however, view the Cyber Crime Treaty as a document that “threatens the rights of the individual while extending the power of police authorities”. The struggle between freedom and state control on the Internet may continue, but the rise in cyber crimes is likely to tilt the scales in favour of the state. When the final word about the Internet is written, will that ironically be about its total control—the antithesis of what it was created for!

The treaty is placed at Appendix 9 under the title European Union Convention on Cyber Crimes.



15.6 Role of CERT in Mitigating Cyber Crimes

We have seen that cyber crimes occur when unauthorised persons gain access into systems and networks causing breach of security. Such incidents are known as intrusions and the people gaining such access are referred to as intruders or more commonly as hackers. In the early days of the Internet, a hacker was someone who had a strong interest in computers, and who enjoyed learning about them and experimenting with them. Today hacker means someone who gains unauthorised access to computers and networks with a view to cause disruption. He engages in network or host activity that potentially threatens the security of computer systems.

A computer security incident is any real or suspected adverse event in relation to the security of computer systems or networks. It is an act of violating explicit or implied security policy resulting in one or more of the following:

- Unauthorised access

- Denial of service/ disruption
- Unauthorised use of a system for processing or storage of data
- Changes to systems software, hardware, firmware characteristics without the owner's knowledge.

Hackers create a malicious code in the form of viruses, worms and Trojans; and propagate them over the Internet causing major disruption of servers. Critical infrastructures of nations such as telecommunication, transportation, financial systems can get threatened; services can get disrupted; major catastrophes can happen as a result of computer security incidents. While cyber crimes committed as result of such attacks are handled by law enforcement agencies, there is another entity that has been created in different countries, known as the Computer Emergency Response Team (CERT), with the explicit mandate of responding to security incidents reported to it by the affected organisations. CERT, as part of its reactive services, advises members on how to contain damage due to a security incident, eradicate the malicious code, restore systems back to operation, and take necessary follow-up measures.

As part of its proactive services, CERT issues vulnerability notes, advisories, alerts, security guidelines and other best practices to educate users to implement them in order to secure their systems and networks. This helps in reducing exposure to threats and vulnerabilities. Statistics have shown that the implementation of CERT guidelines by organisations indeed reduces the risks of cyber attacks, thereby preventing crimes from taking place.

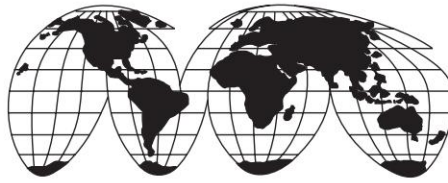
In India too, Indian Computer Emergency Response Team (CERT-In) has been established to provide reactive, proactive and security audit services to its constituency. As part of the latter, expert security auditors of CERT-In can help conduct information security audits of organisations to check for compliance with their declared security policies, and for vulnerability assessment through penetration testing. CERT-In became operational in January 2004. Its website address is <http://www.cert-in.org.in>.

PART VI

Creating Trust in the Electronic Environment

- Information Technology Act, 2000
- Public Key Infrastructure
- Electronic Payment Systems and Internet Banking

Information Technology Act, 2000, introduces the Indian IT Act, 2000, which provides legal recognition to electronic records and digital signatures, and also covers computer misuse and crime. The PKI framework, which forms the basis for electronic authentication, made legally valid by the IT Act, 2000 is covered in the chapter on Public Key Infrastructure. The chapter on Electronic Payment Systems & Internet Banking discusses payment mechanisms associated with completing e-commerce and e-governance transactions.



Chapter 16

Information Technology Act, 2000



16.1 Trust in the Electronic Environment

Central to the growth of e-commerce and e-governance is the issue of *trust* in the electronic environment. The future of e-commerce and e-governance depends on the trust that transacting parties place in the security of transmission and the content of communication. Electronic transactions over the Internet include formulation of contracts, delivery of information and services, delivery of content, exchange of business documents related to transactions, etc.

Can an electronic document be relied upon as an authentic document, much like an original paper document? A sheet of paper carries information and data about the transaction and the originator along with measures to verify the authenticity of the document through written signatures. In the electronic world, a copy is indistinguishable from the original and it can be deleted/ modified without leaving a trace. Furthermore, how can one be sure that the electronic signature on the document belongs to the person claiming to have signed it? Indeed, has the person actually *signed* the document to demonstrate his/ her will to sign and certify the contents of the document and close them so that any unauthorised alteration may be detected?

Addressing these very issues, the Government of India enacted the Information Technology Act, 2000 (IT Act) on June 9, 2000, and notified its implementation on October 17, 2000 with the publication of Information Technology (Certifying Authorities) Rules, 2000. The IT Act is modelled on the UNCITRAL Model E-Commerce Act, that was developed by the United Nations with the aim of encouraging nations to adopt a similar law for providing recognition to e-transactions. The UN Model Law has defined the basic concepts of electronic message, electronic signatures, originator and recipient of electronic messages so as to ensure the acceptance of signed electronic messages. The integrity, confidentiality and non-repudiation of the messages in addition to electronic authentication of the transacting parties involved, is to be ensured in transactions. The electronic records are sought to be made at par with the paper records. The electronic signatures are brought at par with the handwritten signatures.

The IT Act takes the basic framework of the UN Model E-Commerce Law. The preamble states that it is an, “Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ‘electronic commerce’, which involves the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies...”. It extends to the whole of India. The IT Act provides legal recognition to electronic records, and to digital signatures. Digital signature is one special form of the more general concept of electronic signatures, or e-signatures, based on the asymmetric key pairs generated by specific mathematical algorithms. It is the most widely used e-signature as of now. The IT Act recognises only the digital signature in the electronic world for it to be legally valid. It is thus technology-specific.

The Act is, however, an omnibus Act in that it includes computer misuse and crimes, so as to address some of the issues related to cyber crimes. It also modifies the Indian Evidence

Act, 1872, the Bankers' Book Evidence Act, 1891, the Reserve Bank of India Act, 1934 and the Indian Penal Code in line with electronic environment. The IT Act is thus a single Act encompassing several aspects relevant to the growth of e-commerce, and e-governance.



16.2 Electronic Authentication

Creating trust in an electronic environment involves assuring the transacting parties about the integrity and confidentiality of the content of documents along with authentication of the sending and receiving parties in a manner that ensures that both the parties cannot repudiate the transaction. This requires that the paper-based concepts of identification, declaration and proof should be suitably available in the electronic environment. All these are subsumed in what is referred to as electronic authentication. Electronic authentication can be performed by a variety of technologies and processes. The concept of electronic authentication has to be provided legal sanctity through appropriate legislation.

UNCITRAL has proposed a model law for e-commerce covering the major concerns: legal recognition of data messages, writing, original signatures, admissibility and evidential weight of data messages, retention of data messages, formulation and validity of contracts, recognition of parties by data messages, attribution of data messages, acknowledgement of receipt, time and place of dispatch and receipt of data messages. UNCITRAL has also promoted a model law for electronic signatures (e-signatures). Many countries have developed their legislations on the basis of these model laws and have created legal frameworks that provide legal sanctity to e-documents as well as to e-signatures.

The most well known and almost universally accepted method of electronic authentication is the one based on asymmetric cryptosystems. This is also known as public key cryptography,

and is the basis for creating digital signatures. However, rapid technological changes are challenging the supremacy of digital signatures as the only method of electronic authentication. Biometrics and dynamic signature analysis, among other technologies, are expected to be equally important in the years to come. It is said that some of the techniques based on biometrics may prove to be more reliable and less susceptible to compromise than digital signatures. In any case, given the pace of technological developments, no single technology can prevail as the sole means of electronic authentication.

Digital signature, a form of electronic signature, created and verified by using public key cryptography has been explained in Chapter 14.

Electronic authentication using digital signatures requires Certifying Authorities (CAs), who act as trusted third parties or electronic notaries in cyberspace, to issue digital signature certificates or Public Key Certificates (PKCs) to individuals to establish their identity by binding a public key with attributes such as name, address, telephone number, passport number, etc. CAs and the regime governing their operations are together known as Public Key Infrastructure (PKI). PKI is thus the foundation for secure transactions in cyberspace.

Different countries have taken different legislative approaches to electronic authentication. Countries like Australia and the US have taken an all-encompassing approach towards e-signatures whereby any technology can be accommodated. Countries like Germany and Japan have focused on technical standards for the operations of PKI. Singapore and Malaysia have included the entire range of issues associated with legal effects of e-signature, PKI and the establishment of a regulator to oversee CAs. The legal framework in India also belongs to the latter category. In fact, the IT Act, as noted above, is based on the public key asymmetric cryptosystem as the basis for digital signatures to provide electronic authentication. The law is thus tightly coupled with the dominant form of technology available for e-signatures.



16.3 Paper vs Electronic World

In the traditional world, a paper document consists of four components: the carrier (the sheet of paper), text and pictures (the physical representation of information), information about the originator and measures to verify the authenticity (written signature). All the four components are physically connected. There is only one original from which several copies can be made using different methods. The handwritten signature is supposed to be unique, and difficult to be reproduced. It is neither changeable nor reusable. Its main functions are identification, declaration, and proof.

The signature is used to identify a person and to associate the person with the content of that document. It is thus always related to a physical person. In all legal systems, there is no prescription of an exclusive modality of signing, e.g. full name, initials, nickname or any symbol. The act of signing is a token acknowledgement of responsibility for the contents of the document. It also seals the document in the sense that anything written after the signature is generally not taken to be part of the document.

Parties to contracts have the right to rule their own contractual relations, defining the way each one can sign the agreements. From a legal point of view, there is nothing against the introduction of new types or technologies for signatures. Digital signature is one such new technology. Document/ signature forgery is part of the paper world that people have learnt to live with for two millennia. But while making a transition to a new type of signature (digital signature), there are genuine issues of concern about new technologies with respect to their security and forgery.

In the electronic world, a document is produced by a computer and is stored in digital form. It cannot be accessed without using a computer. It can be deleted, modified and rewritten without leaving a trace. The integrity of an electronic document is genetically impossible to verify. A copy is indistinguishable

from the original. It cannot be sealed in the traditional way, where the author affixes his/ her signature. E-Commerce transactions such as formulation of contracts, delivery of information and services, and delivery of content, among others, are based on electronic juridical statements—statements that are telematically prepared. Computers are the only means by which contracting parties prepare their agreements.

Examples of electronic juridical statements include electronic fund transfers, teleshopping, telereservations, e-contracts, e-governance, etc. The trust that the transacting parties repose in the security of the transmission and content of an electronic document during communication will ultimately decide the future of e-commerce/ e-governance. Such documents need to be authenticated. The traditional functions of identification, declaration, and proof of electronic documents can be carried out by using a digital signature based on cryptography.

The digital signature is a set of alphanumeric characters resulting from mathematical operations of cryptography, carried out on an electronic document on a computer. From a technical point of view, it is a numerical value that is affixed to a data message—a cryptographic transformation of a data unit that allows the recipient of that data to prove the source and integrity of that data unit. It protects against forgery, even by the recipient. Digital signature is an electronic procedure attesting the source of the transaction and guaranteeing the integrity of its contents.

Digital signatures are created and verified by using public key cryptography. An algorithm generates two different yet related keys—private key and public key. The private key is used to sign a document. Digital signatures have been dealt with in Chapter 14. The corresponding public key is used to verify the digital signature, because it alone can decrypt the message.

As noted earlier, even with the knowledge of the public key, one cannot compute the private key belonging to its owner. This is because it is computationally infeasible to derive a user's private key from his/ her public key.

The key pairs fulfil all the requirements of electronic authentication. Two unknown parties entering into a business transaction can conclude the same ensuring confidentiality, integrity, authentication and non-repudiation of the transaction. For a transaction between A and B, these are realised as follows:

- A signs a message with his own private key.
- A then encodes the resulting message with B's public key to achieve confidentiality.
- B decodes the message with his own private key.
- B applies A's public key to verify the digital signature.

The significance of the above signing and decoding process is given below.

- When A uses his own private key, it demonstrates that:
 - He wants to sign the document.
 - He wants to reveal his identity.
 - He shows his will to conclude that agreement.(The encoded message travels on the net, but nobody else but B can read it).
- B needs to know that A and only A has sent the message. To do that:
 - B uses A's public key on the signature.
 - Only A's public key can decode the mail.
 - A cannot repudiate his signature.(Digital signature cannot be reproduced from the message. No one can alter a ciphered message without changing the result of the decoding operation).



16.4 The IT Act, 2000

The IT Act defines the following key concepts related to electronic records, digital signatures, and Certifying Authorities*:

- Asymmetric cryptosystem
- Certifying authority

*The IT Act, 2000 has chosen the nomenclature of "Certifying Authority" instead of the international practice of "Certification Authority".

- Certification practice statement
- Computer
- Computer network
- Computer systems
- Data
- Digital signature certificate
- Electronic form
- Electronic record
- Key pair
- Originator
- Private key
- Public key
- Secure system

16.4.1 Legal Recognition to Electronic Records

Section 3 of the IT Act provides for authentication of an electronic record by a person by affixing his digital signature, “which shall be effected by the use of an asymmetric crypto system and hash function.” This is explained in detail in Chapter 17 on Public Key Infrastructure (PKI).

Section 4 of the Act provides legal recognition to records, while Section 5 provides legal recognition to digital signatures. Section 6 allows filing of electronic records in the form of electronic forms, with digital signatures of persons, to be filed with Government organisations in lieu of paper-based forms, when prescribed by any of them.

Section 7 of the Act provides legal recognition to electronic records that are stored in the original formats in which they were generated. Retention of electronic records has thus been legalised. The Government has been further authorised to have an Official Electronic Gazette which will have the same legal recognition as the paper gazette for all rules, regulations, orders, bye-laws, notifications, or any other matter published in it.

16.4.2 Formation of Online Contracts

Sections 11 to 13 of the IT Act relate to the formation of an online contract between two parties that is solely mediated electronically. The originator of an electronic record sends it as a message which is deemed to have been received by the addressee, if he sends an acknowledgement, or conducts himself in a manner so as to let the originator know that the message has been received by him. The two parties can agree on the formation of the contract depending on whether the acknowledgement of receipt of the electronic record by the addressee has been stipulated as a condition by the originator. If it has been mandated, then the contract will be deemed to be formed only after receipt of the acknowledgement from the addressee. In the alternative case, if the originator does not receive any acknowledgement, nor any indication that the addressee has received the electronic record sent by him, the originator, he can re-transmit the message stating the time frame by which the acknowledgement should come, failing which the originator can treat the electronic record as though it had never been sent.

The time of dispatch of the electronic record is deemed to be the time at which the electronic record enters a computer resource outside the control of the originator. Likewise, the time of receipt of an electronic record is taken to be the time it enters the computer resource designated by the addressee. These sections further clarify that the place of business of both the parties will be taken to be the place(s) where the electronic record will be deemed to have originated, and received, respectively. This will be the case irrespective of where the computer resources of both parties may be located.

16.4.3 Digital Signatures and Certifying Authorities

Sections 14 through 42 in Chapters V to VIII of the IT Act deal with digital signatures, regulation of Certifying Authorities (CAs), Digital Signature Certificates (DSCs), and the duties of

subscribers. The method of creating a secure electronic record and digital signatures is described here. This is elaborated upon in Chapter 17 on PKI .

The process of licensing a CA, and monitoring of its subsequent compliance with the terms and conditions of the licence, including adherence to technology standards and the procedures of issuing DSCs to the users as laid in the rules and regulations under the IT Act, are described in these chapters. A Controller of Certifying Authorities (CCA) is to be appointed for the purpose of exercising supervision and control over the CAs. The CCA itself is expected to observe the same technical standards in discharge of its functions that are technical in nature. It has to operate its own infrastructure to certify the public keys of CAs, in much the same way that a CA has to for certifying the public keys of its subscribers. In addition, he has to maintain a national repository of all the DSCs issued by the CAs in the country.

A CA has to declare its practices in public in the form of what is known as its Certification Practice Statement (CPS). As part of the CPS, it describes the classes of DSCs to be issued by the CA, and the physical verification procedure that it follows to issue the certificates. The certificate, as seen in Chapter 17, binds a physical person with a public key. The attributes of the person are given in the certificate. It is his authentication token in the electronic world. Depending upon the level of physical verification, as described in the CPS, a particular class of DSC may be used for high value transactions. The CA is also expected to state in the class of certificate issued by it, the type of transaction or the end-use, it may be put to. A relying party, on seeing a certificate, can thus decide on the level of authentication that is necessary for his transaction.

The digital signature regime works on the private-public key pair that is generated by an asymmetric cryptosystem algorithm, such as the RSA Algorithm. While the private key is used to sign an electronic record by encrypting it suitably, it is the corresponding public key that alone verifies that the record was

indeed signed by its owner's private key. So, the owner of a DSC has to ensure that he keeps his private key in safe custody. In fact, the very first step of generation of the key pair should be initiated by the user so that he retains control of his private key. The Act enjoins upon the user responsibilities related to protection of his private key.



16.5 Cyber Crimes Under the IT Act

Cyber crime under the IT Act have been covered in Section 15.3. As observed, it is not a special Act dealing with Internet crimes or cybercrimes *per se*. Hence it does not appear to highlight the enormity of cyber crimes. Many of the now well known cyber crimes do not even find a mention in the IT Act.

The very first case which was booked under this Act could not be cracked by CBI. The accused had misused an AIIMS doctor's credit card to view pornographic sites on the Net. The AIIMS server used by the accused did not maintain any details of login of users. The CBI could not get any evidence. The investigating agencies feel that the Act is soft on ISPs. There is no statute mandating the ISPs to maintain login records. They also claim that it does not empower the investigating agencies adequately.

The Act does not cover common cyber crimes such as cyber stalking, cyber harassment, stealing of Internet hours, cyber defamation, etc. In a recent case, a teenaged girl's name and phone number were maliciously put on a dating website, where she was portrayed as soliciting casual sexual affairs. Complaints were made, but it seemed that no law could be invoked to punish the culprit. Cyber stalking and e-mail harassment are emerging as major crimes which are increasing by the day, but are not covered by the present IT Act. Hacking and pornography are covered in the Act in a fairly reasonable way so as to bring the perpetrators of these crimes to justice. The Act also provides for data protection in a limited way through sections on cyber contraventions covering unauthorised access to computer system or computer network and cyber offences

dealing with computer, computer system or computer network related serious offences. While cyber contraventions may result in civil prosecution, criminal prosecution could be brought against the more serious cyber offences.

Economic offences resulting in financial losses are the key drivers for motivating the protection of sites, data and e-transactions. Online trading firms and stock brokers in Mumbai suffered due to virus attacks. The loss in terms of money has not been adequately quantified. A survey found that 49 percent of the top corporates and industries in India suffered virus attacks resulting in huge loss of revenue and service outages. The situation in the more developed world is similar. For example, a 1997 Special Report by the American Society for Industrial Security on Trades in Intellectual Property Loss estimated that US-based companies suffered in excess of US\$ 250 billion in losses in a year due to hacking and theft.

Cyber crimes are, therefore, very real. They can result in huge financial losses to the society. They can also harass citizens in other ways. A more comprehensive Cyber Crime Bill or Internet Crime Bill may be required, in due course, to deal with these crimes. For now, the IT Act has created the necessary legal and administrative framework to promote the growth of e-commerce and e-governance through the establishment of PKI, and by including the necessary clauses for providing punishment for computer misuse and frauds rolled into this omnibus Act. It thus seeks to build confidence among the public that frauds in cyber space will not go unpunished.

Sections 65 through 78 of the IT Act deal with offences, and prescribe punishment in the form of fines and imprisonment. Specifically, as noted above, hacking, pornography, and law and order, have been addressed in a focused way. All other cyber crimes are left uncovered. On the other hand, government systems have been given the status of protected systems under Section 70, provided they have been notified to that effect in the Official Gazette. In such a case, an intruder into such a system can be punished with imprisonment of upto 10 years.



16.6 Adjudication Under the Act

The Act also deals with damage caused to a computer system or a computer network through unauthorised access. These are dealt with as civil offences in Sections 43 to 47 of the Act. Penalties have been provided for different types of damages. These are very important for enhancing trust in electronic environment. It assures the e-commerce sites that data and content on their sites has the protection of the law, and that in case of vandalism, severe damages in the form of compensation of upto Rs one crore can be awarded against the wrongdoers through a fast-track adjudicating mechanism. The Act prescribes appointment of serving government officers, atleast of the rank of Director, as Adjudicating Officers to try such cases with the powers of civil courts.

Section 43 of the Act provides penalty for damage to computer systems and networks by any unauthorised person gaining access to a computer, or network, copying data from it, introducing a computer virus, disrupting any computer or network, causing denial of service, etc. by way of compensation. Sections 46 and 47 delegate the powers to adjudicate, as a civil court, to the Adjudicating Officers. The Adjudicating Officer, while deciding on a complaint to decide on the quantum of compensation, has to take into consideration the amount of gain of unfair advantage made as a result of default, and the amount of loss caused to any person as a result of the default.

16.6.1 Cyber Regulations Appellate Tribunal

The institution of the Cyber Regulations Appellate Tribunal, (CRAT) presided over by a judge of the High Court, shall be the appellate authority against all the decisions, and rulings of the CCA, and the Adjudicating Officers under the IT Act. He has been vested with the powers of a Civil Court under the Code of Civil Procedure, 1908 under Section 58(2), though not bound by the same procedure as per Section 58(1).

16.6.2 Other Provisions

Section 79 of the IT Act absolves a Network Service Provider of any liability if he can prove that an offence or contravention was committed without his knowledge, or that he had exercised due diligence to prevent the occurrence of such an offence.

Section 80 empowers police officers of the rank of Deputy Superintendent to enter, and search any premises, without a warrant, on suspicion of any offence being committed under the Act. This is a very sweeping power that has been given to the law enforcement agencies for preventing cyber crimes.

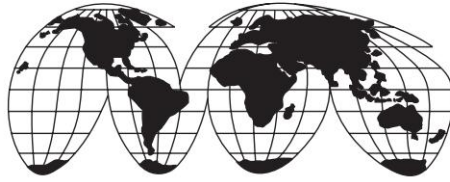
Section 1(4) of the Act has specifically noted the paper instruments that will not have an equivalent in the electronic world. These include the negotiable instrument, power of attorney, trust, will, and conveyance deed. Subsequently, in November, 2002, through an amendment to the Negotiable Instruments Act, a cheque as a negotiable instrument was brought under the purview of the IT Act. Electronic cheques are therefore legally valid.

The Indian Evidence Act has been suitably amended to allow all electronic records to be accepted as evidence in a court of law. After Section 65 of this Act, new Sections, 65A and 65B have been inserted which describe in detail the admissibility of electronic records as evidence. New sections have been added after Sections 67, 73, 81, 85, 88, 90. These relate to proof as to digital signature, verification of digital signature, Gazette in electronic form, presumption as to electronic records and digital signatures, and presumption as to electronic messages.

Similarly the Bankers' Book Evidence Act, 1891, has been amended to allow printouts of computer records as evidence.

The Reserve Bank of India Act, 1934 has been amended through insertion of a new clause (pp) after Section 58(2)(p), on the regulation of electronic fund transfer through electronic means among the banks, or between the banks and other financial institutions.

Finally, the Indian Penal Code has been amended by including the electronic record in a new Section, 29A, which will have the same definition as in the IT Act. All sections on forgery get extended to the electronic records, thereby making the provisions of the penal code applicable to forgery in the electronic world.



Chapter 17

Public Key Infrastructure

The most well-known and almost universally accepted method of electronic authentication is the one based on asymmetric cryptosystems, which has already been discussed in the previous chapter. This is also known as public key cryptography, and is the basis for creating digital signatures. Digital signatures created and verified by using public key cryptography that is based on the concept of a key-pair, generated by a mathematical algorithm—the public and private keys has already been discussed in Chapter 14.

The main challenge faced in implementing digital signatures based on asymmetric cryptosystems was in making all the public keys widely available while ensuring that the relying party can be assured that the corresponding private key has indeed been used to create the digital signature.

Electronic authentication using digital signatures requires Certifying Authorities (CAs), who act as trusted third parties or electronic notaries in cyberspace, to issue Digital Signature Certificates or Public Key Certificates (PKCs) to individuals to establish their identity in the cyberspace by binding a public key with attributes such as name, address, telephone number, passport number, etc. while ensuring that the entity possessing these attributes owns the corresponding private key. The CAs and the regime governing their operations are together known as Public Key Infrastructure (PKI). PKI is thus the foundation for secure transactions in cyberspace.



17.1 PKI and Certifying Authorities (CAs)

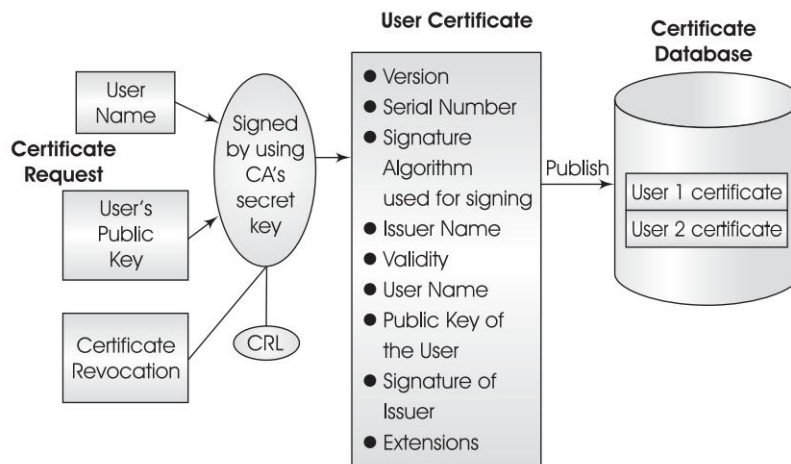
A CA is a trusted third party which issues digital certificates, the PKCs, that bind a public key to its owner. The digital signature created by using a private key gets verified by the corresponding public key in such a PKC. The PKC contains critical information which is signed by the CA. The CA as a trusted third party, performs the function of identity verification of the applicant before issuing a PKC to him. The distinguished name is a set of values that identifies the entity being certified. This includes country, organisation, organisation unit, name, etc. Additionally, other attributes describing the entity being certified such as address, telephone number, passport number, driving licence, election card number, etc., can also be included in the PKC. The public key belonging to this entity being certified is of course, a part of this PKC. The CA's digital signature on the certificate imparts it security and trust. A valid digital signature on a certificate is a guarantee of its integrity. Since the CA has signed the certificate with its private key, anyone verifying the CA's signature on the certificate is guaranteed that only the CA could have created and signed the user's certificate. Finally, the CA with strict security criteria for securing his own private key cannot deny having signed the certificate.

A CA therefore performs the following functions:

1. Reliably identifies persons applying for digital signature certificates,
2. Confirms the attribution of a public key to an identified physical person by means of a digital signature certificate,
3. Issues digital signature certificates and Certificate Revocation Lists,
4. Always maintains online access to certificates and CRLs,
5. Takes measures to operate its infrastructure in conformance with the IT Act, and as per its approved Certification Practice Statement (CPS), and
6. Provides the desired level of assurance for its various classes of certificates; undertakes liability as per the approved CPS.

The contents of a digital signature certificate are as follows:

1. Version
2. Serial number of the certificate
3. Signature algorithm used for signing
4. CA's distinguished name
5. Validity period of the Certificate
6. Distinguished name of the user
7. Public key of the user
8. Signature of the CA
9. Extensions



➞ Fig. 17.1 CA Operations

One of the main functions of a CA is to make available all the certificates issued by it online, in the form of a directory, to its subscribers and relying parties. Relying parties wishing to enter into a contract with a subscriber of a CA can confirm the validity of the certificate from the CA's directory, and through it, the identity of the subscriber and other credentials that may be part of the certificate.

In the event of compromise of a subscriber's private key, he may request the revocation of his digital signature certificate.

The CA is obliged to issue a Certificate Revocation List (CRL) as and when such a request is received. There may be other circumstances that can warrant the revocation of a certificate. This includes circumstances wherein facts come to light, which, if known earlier, would have resulted in the non-issuance of the certificate.

The CA is also expected to perform some other functions that include time-stamping service, and making available reliable cryptographic software to subscribers for generating key-pairs.

The CA is expected to inspire confidence among its subscribers on the security of its infrastructure, the practices followed in its operations, and the liability that it is willing to take in respect of the digital signature certificates issued. This is done by the CA through its Certification Practice Statement (CPS)—a document published as the sum total of the practices followed by it. The CPS deals with practices with regard to certificate issuance and user registration, certificate lifetime and revocation, identity verification procedure, classes of certificates, certification publishing practices, and liability issues. On the basis of the recommendations of the Internet Engineering Task Force as contained in the document RFC 2527, the CAs normally cover the following areas in their CPs:

1. General Provisions including Obligations, Liability, Financial Responsibility, Interpretation and Enforcement, Fees, Publication and Repositories, Compliance Audit, Policy of Confidentiality and Intellectual Property Rights
2. Identification and Authentication
3. Operational Requirements
4. Physical, Procedural and Personnel Security Controls
5. Technical Security Controls
6. Certificate and CRL Profiles
7. Specification Administration.

A PKI manages the generation and distribution of key-pairs, and publishes the public keys as part of the PKCs and CRLs in open repositories such as X.500 directories. Subscribers and

relying parties can access these directories to verify the credentials of a person before completing a transaction in cyberspace.

The relying party, on receiving a public key certificate, authenticates the public key by virtue of its having been certified by a CA. If the relying party does not possess an assured copy of the public key of the CA who issued the certificate in question, a certificate containing the issuing CA's public key must be obtained. This process continues up the hierarchy until the verifying key is one of the widely trusted public keys. The trust path thus established would normally lead up to the root of the trust chain for a PKI.

Having established the trust path, the relying party has to decide how much a specific certificate can be trusted. This could depend on knowledge about the security controls, practices, identification and authentication methods, etc., followed by the CA in issuing these public key certificates. While practices and security controls are part of the Certification Practice Statement, the relying party should also be able to find out whether the certificate is adequate for the current requirement. Certificate policies are defined in X.509 recommendations as 'a named set of rules that indicates the applicability of a certificate to a particular community and/ or class of application with common security requirements specifically meeting this need of the relying party.' Certificates may be issued by a CA under different certificate policies, while there may be a single CPS. However, multiple CAs may support the same policy.

For a relying party to trust the certificate, a mechanism is required to link the certificate to the applicable certificate policy. In X.509 Version 3, certificate policy information is included through the optional certificate extensions. Certificate policies applicable to a specific certificate are indicated by unique registered object identifiers.

The relying party may also be faced with the need for evaluating different certificate policies. Comparison is normally based on factors such as forbidden applications, the required minimal

length of signature keys, public key protection methods and the verification methods of private key possession.

Certificate policies play a central role in public key infrastructure. Since certificates are issued by CAs for a variety of purposes, the certificate policies also constitute a critical component of the basis of the trust reposed by relying parties in a Public Key Certificate.

The trust chain from a subscriber of a CA to a subscriber of another CA can be formed through cross-certification arrangements between the two CAs. When two CAs enter into such an arrangement, each vouches for the certificates issued by the other. From a technical perspective, the process involves the creation of 'cross-certificates' between two CAs. When a CA cross-certifies another CA, he actually creates and digitally signs a certificate containing the public key of the latter. In a similar manner, the second CA creates and signs the public key of the former CA. The users in one domain are thus assured of the trust extended by their CA to the CA of another domain. Since cross-certification extends third party trust, the CAs entering into such an arrangement are expected to be completely comfortable with each other's security policies and practices employed in issuing certificates and in carrying out their operations.

A PKI enables such arrangements. It comprises CAs, certificate and CRL repositories, key management, back-up and recovery systems, timestamping services, cross-certification arrangements, client-side software for users interfacing with their applications and certificates in a consistent and trustworthy manner. The standards for the operations of CAs, certificates, CRLs, protection of their private keys in hardware security modules, standards for physical security of the infrastructure, audit standards, CPS framework and so on, are also part of the definition of a given PKI.

The PKI thus has the following features:

1. It allows parties to have free access to the signer's public key available in the directories of CAs

2. Public keys are freely distributed while private keys are securely held by the owners
3. It entails an assurance that the public key corresponds to the signer's private key, implying:
—Trust between parties as if they know one another
4. Parties with no prior agreements, operating on open networks, can have the highest level of trust in one another.

The central issue governing the operation of CAs is whether they are to be licensed or accredited by the government or some voluntary association or a central body. The extent to which the government exercises some sort of regulatory authority over CAs tends to increase the level of trust that the subscribers can repose in e-transactions, especially in developing countries, since the legislation invariably provides for their smooth operation. This is the case in India. It will be discussed in the next section.

Liability is one of the most complicated issues surrounding PKI. What is the extent to which the law should define or limit the liabilities of the following players: the person who digitally signs the message, the person who relies on its validity, and the CA who vouches for the identity or some other attribute of the sender? The CA may be liable for any inaccuracies or misrepresentations in the certificate that may have been used by a relying party in trusting the sender for a transaction. The CA may also be liable if he has not revoked a certificate in time. It is for the CA to verify the identity of the subscriber, through a thorough investigation, before issuing a digital certificate. Depending on the class of certificate issued by the CA, digital signatures may be used for high value transactions. This can increase the risk of a CA, and hence his potential liability. A CA has to declare in his CPS the liability he is willing to accept for different classes of certificates.

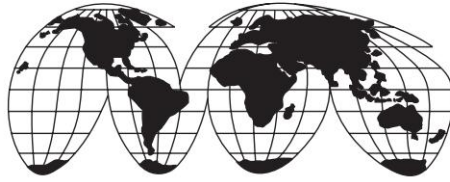


17.2 PKI in India

In India, the Certifying Authorities (CAs) are licensed by the

CCA under the Information Technology (IT) Act. The rigorous process of audit of the infrastructure of the CAs at the pre-licensing stage and also the audit on a regular basis conducted by an auditor from the CCA panel of auditors, ensures that CAs conform to the international technology and practice standards, as also to the rules and regulations laid down under the IT Act. The business and corporate world and other individuals can safely place trust in the certificates issued by the CAs.

This lends certainty to the business transactions based on digital signatures, since the identity of the parties is authenticated. So is the integrity of transactions. Confidentiality of transactions and their non-repudiability are also ensured. The public key infrastructure realised in the form of licensed CAs and other provisions, as part of the legal and administrative framework of the IT Act will help promote the growth of e-commerce and e-governance applications in cyberspace.



Chapter 18

Electronic Payment Systems and Internet Banking

Electronic payment systems comprise payment services over the network for goods and services procured. They are integral to the completion of e-commerce transactions. Goods can include physical items such as books, CDs, garments and electronic content, while hotel booking, railway/ airline reservations, stock trading, etc. are examples of services offered and procured over the Internet. Authentication, integrity, authorisation and confidentiality are the basic security requirements that must continue to be met when payments are made electronically for such procurement.

An electronic payment system consists of the following components:

- Buyer
- Seller (merchant)
- Payment gateway
- Buyer's bank (issuer of the payment instrument)
- Seller's bank (acquirer).

When a buyer procures goods or services electronically from a merchant, the method of payment could be chosen to be a credit card. Before the merchant agrees to supply the item to the buyer, the merchant looks for the assurance that the payment will be fulfilled. A request containing the transaction

details is sent to the payment gateway by the merchant. The payment gateway, in turn, interacts with the issuer bank on the financial network to carry out the verification. The result is sent back to the merchant to enable the merchant to decide on whether the goods/ services should be supplied or not.

Other payment methods such as electronic cheque, funds transfer through Internet banking and innovative schemes like PayPal adopted by eBay are also widely used. When the buyer uses credit cards, the details of the transaction are posted to the buyer's account and processed in a cumulative manner. If, however, debit cards are used, then the buyer's account is debited automatically. These payment methods are discussed in the following sections.



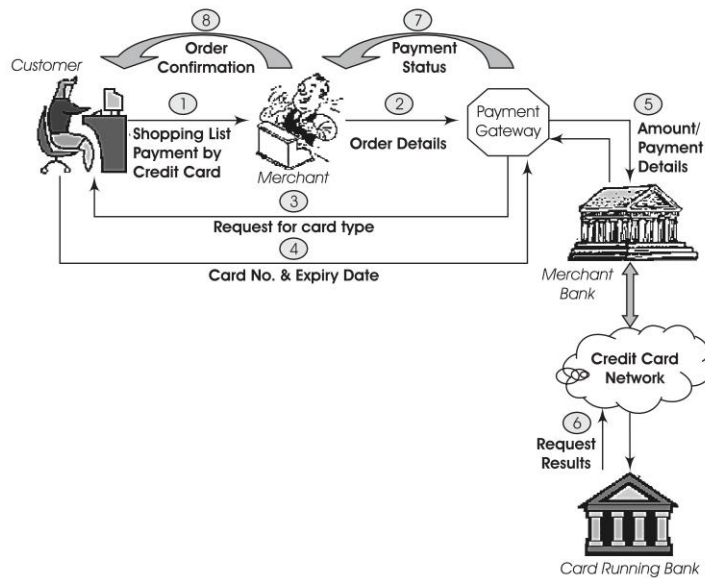
18.1 Payment Gateway

Payment gateways handle all the payment operations that are needed for operating e-commerce sites. The servers on these sites have to be secured and duly certified by a Certifying Authority. Payment gateways can process multiple payment mechanisms including debit cards and smart cards. Normally, there are two functions within payment gateway software. These are:

- The **authorisation** function which performs certification and issuance of digital identification to the entities that would be interacting with the payment gateway.
- The **settlement** function which facilitates the carrying out of actual inter-bank transactions.

The entire system provides facilities like formatting, encrypting and digital signing of the orders for transferring to the financial network.

In India, payment gateway services are offered by ICICI, Citibank, Global Telesystems and HDFC Bank. These systems enable the seller to perform real-time credit card authorisation

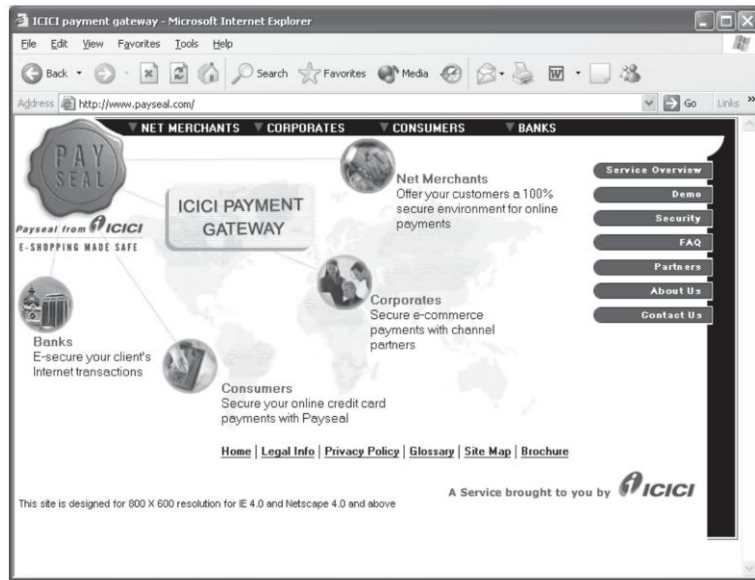


➞ **Fig. 18.1** *Payment gateway*

or debit card settlements from a website over the Internet. Payment can be made within seconds after the gateway obtains authorisation from the credit card institutions.

Most credit cards such as MasterCard, Visa, American Express, etc. are acceptable to these payment gateways. Any credit card information submitted as a part of completing a transaction is encrypted before it is transmitted over the Internet to the acquiring bank. Most of these payment gateway servers are placed behind security firewalls and are integrated with risk management components so that the security is effectively managed.

For example, Payseal, the payment gateway operated by ICICI, ensures that the customer's credit card details are kept secure while transacting on the Net, thereby preventing unauthorised access to customer information. The card details would not be disclosed even to the merchant. Payseal which adopts the SSL (Secure Socket Layer) technology, is an integrated solution employing 128-bit encryption to secure online transactions. The



➞ Fig. 18.2 *www.payseal.com*

client software, installed at the client's end, encrypts transaction information using 280-bit RSA before passing it through an SSL pipe using 128-bit encryption. The data is stored at ICICI's own data centre, which is secured by firewalls and other network security infrastructure. Physical access to the data centre is restricted by the use of biometrics. The gateway server has been assigned a server certificate by a certifying authority.

In the business-to-business sector, HDFC Bank's payment gateway, EPI, provides real-time transfer of funds transacted on the portal. EPI has been successfully implemented by fifteen B2B portals such as VSNL, Sifymall, Fabmart, etc. The entire operation takes place through a secure channel realised through Firewalls, 128-bit encryption and digital signatures.

In the 'Direct Pay' mode of payment, online payments are accepted from clients/ customers who are HDFC Bank account holders. The account is automatically credited with the corresponding transaction amount instantaneously. Since the

customer is an HDFC Bank account holder, the bank takes all the responsibility of verifying the customer's identity. HDFC Bank's Direct Pay facility is a banking channel wherein purchases are debited directly to the customer's account and credited to the account of the establishment (or the website where the purchases were made).

If a customer is an account holder with HDFC Bank, all he has to do is to register for the Netbanking facility to use this option. Security is facilitated through 128-bit SSL (Secure Socket Layer) encryption. The NetBanking details of the customer (customer ID and password) are kept confidential and cannot be viewed by the merchant.

The Direct Pay process flow involves the following steps:

- The customer browsing on the merchant site, finalises his/her purchase.
- The customer decides to make payments for the transaction that he/she has finalised.
- The customer selects 'Debit my HDFC Bank A/ C'.
- The customer clicks on the pay button and he/she is traversed to page to make payments.
- The customer enters his/her Netbanking ID and password.
- The customer then selects the account, from which he/she wants to make the purchase.
- The customer account with HDFC Bank is debited online and the transaction is over for the customer.
- The merchant account is credited for the transaction amount, less the transaction fee.
- The customer is honoured with the purchase made as per the terms of the merchant agreed upon by the customer.



18.2 Internet Banking

Internet banking allows any user with a PC and a browser to get connected to his bank's website to perform any of the virtual banking functions and avail himself of any of the bank's

services. There is no human operator present in a remote location to respond to his needs such as in telephone banking, or in a call centre. The bank has a centralised database that is web-enabled. All the services that the bank has permitted on the Internet are displayed in a menu. Any service can be selected and further interaction is dictated by the nature of the service.

With the expansion of the Internet, more and more banks and financial institutions are using the Internet and the Web to offer an additional channel for their services as well as to improve communication with their customers. Convenient and safe 'anytime anywhere' banking can be carried out over the Internet.

However, new challenges have to be addressed to ensure that security is not compromised. When one is using online banking systems, it is extremely important for the customer to assure himself that the online bank is a legitimate site, preferably certified by a certifying authority. Customers will be exchanging personal information in addition to giving out the account number and the corresponding password in any such online session. Some websites deliberately use names, which are very similar to those of reputed organisations and use this tactic to trick customers into revealing information, which would not otherwise be divulged.

In India, a number of banks have introduced Internet banking. While most of them are restricted to information about the customer's own account and transactions between different accounts belonging to the same customer, some banks have enhanced their services by including funds transfer between different customers.

The Reserve Bank of India has issued guidelines for Internet banking, covering:

1. Technology and security standards
2. Legal issues
3. Regulatory and supervisory issues

Technology and Security Standards

The need for banks to define security policies has been emphasised. Although the use of Public Key Infrastructure (PKI) has been suggested, the use of at least 128-bit SSL for server authentication and for securing browser-to-web server communication has been mandated.

Legal Issues

The asymmetric cryptosystem as advocated in the IT Act, 2000 has been recommended as the security procedure for digital signatures for authenticating electronic records. Other methods of authentication have been highlighted as a source of legal risk. The RBI has also warned against the enhanced risk of liability to customers on account of breach of secrecy, denial of service, etc. caused by hacking or other attacks.

Regulatory and Supervisory Issues

The following guidelines apply for these issues:

- Internet banking service can only be offered to the account holder of the bank and only for Indian local currency products.
- All banks that offer transactional services on the Internet will do so after obtaining approval from the RBI.
- Any breach or failure of security systems is to be reported to the RBI.
- Interbank payment gateways can only be set up by those institutions that are members of the cheque clearing systems in the country.

The detailed guidelines issued by the Reserve Bank of India in respect of Internet Banking are available at www.rbi.org.in.



18.3 PayPal

PayPal, an eBay company, has a unique payment model wherein

money can be sent to anyone who has an e-mail address. Founded in 1998, PayPal was acquired by eBay Inc. in October, 2002. PayPal enables any individual or business with an e-mail address to send and receive payments online. PayPal's service builds on the existing financial infrastructure of bank accounts and credit cards. With 56 million account members worldwide, PayPal is available in 45 countries around the world. Buyers and sellers on eBay, online retailers, online businesses, as well as traditional offline businesses are transacting payments on PayPal.

PayPal is not a payment gateway. Customers of PayPal are allowed to move money electronically from their bank account to other PayPal account holders, unlike traditional banks wherein such transfers require cheques. Account holders can send money to non-account holders by creating a virtual account attached to an e-mail address. In PayPal's model, when the recipient gets a 'you've got cash' e-mail and is directed to go to PayPal's website, he has to open an account by filling out a one-screen form providing his name, phone number and e-mail address. PayPal then sends e-mail for confirmation following which an account is created for that customer.

Once the account is opened, the recipient claims the payment. The payment appears in the recipient's PayPal account balance. The recipient can choose to transfer the funds to a bank account, request a cheque, or send the funds to someone else.

Payments are made digitally and instantly, and can be sent in US dollars, Canadian dollars, euros, pounds sterling, and yen. Person-to-person payments were introduced in thirty-six countries in the European Union (EU) and Asia in the year 2001. The widespread acceptance and convertibility of these payments were the key to PayPal's strategy. Customer service agents of PayPal, reachable by e-mail or telephone, deal with customer problems ranging from lost passwords to disputes over payments.

Customers are offered money market returns on their account balances as well as instant access to their money. From December



➡ Fig 18.3 *www.paypal.com*

2000, PayPal began to offer an ATM/ debit card co-branded by MasterCard. Cardholders could convert their PayPal account balances to cash at an ATM or use the debit card to pay for products and services.

In order to make sure that accounts were opened by a human being, and not by an automated entity, a security measure called the Turing Test was devised. Characters are presented on a changing chequered background so that automated character recognition programs are unable to correctly identify the characters. The re-entry of these characters is therefore only possible by humans.

Customers were encouraged by PayPal to register their bank accounts so that the PayPal account could be funded from a bank account through the ACH. A customer who opened an account and provided a verified bank account number was rewarded with a bonus of US\$ 5. The account was then verified by a process for which PayPal had applied for a patent: PayPal would randomly deposit two small amounts (less than a dollar)

in the customer's bank account. If the customer could tell PayPal what the amounts were, PayPal knew that the customer could control the account, and that the customer had opened the account and had been screened by the bank. Once the customer's bank account was verified, there was no limit to how much could be spent from that bank account.

In September 2000, PayPal introduced a payment capability for wireless devices and cell phones. In this case, the notification was sent to a wireless device instead of PC-based e-mail. If one person wanted to send money to another and they both had web-enabled cell phones, the sender would access the PayPal server via the cell phone to carry out the transaction. The recipient could indicate whether the payment notification should be sent to the web-enabled cell phone or to the e-mail inbox.

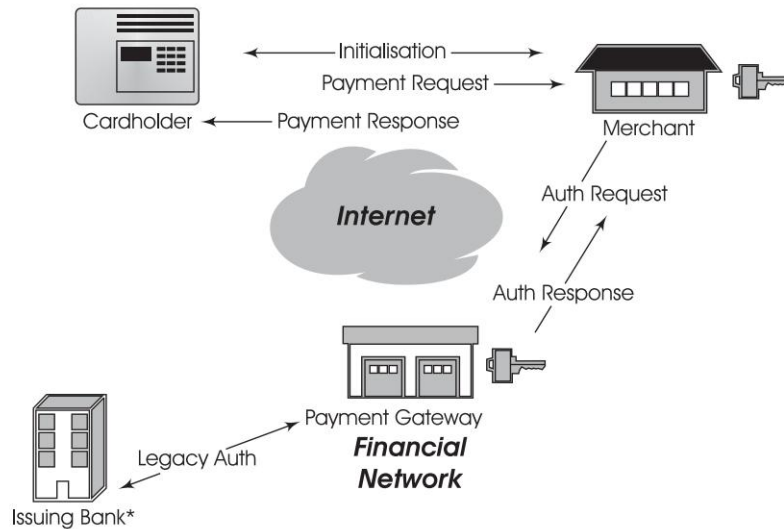


18.4 The Secure Electronic Transaction (SET) Protocol

The SET protocol was developed by Visa and MasterCard to provide security for credit card-based payment transactions on the Internet. Figure 18.4 exhibits the SET protocol.

SET addresses the following business requirements of confidentiality, integrity, authentication and interoperability:

- Confidentiality of payment information and order information that is transmitted along with the payment information
- Integrity of all data that is transmitted
- Authentication that a cardholder is a legitimate user of a branded payment card account
- Authentication that a merchant can accept branded payment card transactions through his relationship with an acquiring financial institution
- Use of the best practices for security and system design so as to protect all legitimate parties in an electronic commerce/ payment transaction



➡ **Fig. 18.4** SET protocol

- Independence from transport layer security mechanisms
- Interoperability among software and network providers.

When SET is used for completing an e-commerce transaction, the entire process can be broken up into the following activities:

- The cardholder selects items for procurement.
- The cardholder is presented with an order form containing the list of items, their prices, and a total price including shipping, handling and taxes. This order form can be obtained from the website of the merchant or can be created on the cardholder's computer by special purpose electronic shopping software.
- The cardholder selects the means of payment—in this case, a payment card is selected.
- The cardholder sends the merchant a completed order form along with the payment instructions. The order and the payment instructions are digitally signed by the cardholder who is already in possession of digital signature certificates.
- The merchant requests payment authorisation from the cardholder's financial institution.

- On receiving authorisation, the merchant sends confirmation of the order.
- The merchant ships the goods or performs the requested services from the order.
- The merchant requests payment from the cardholder's financial institution.

In a SET transaction, the electronic processing begins with the cardholder. A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder's interactions with the merchant, the payment card account information remains confidential. An issuer is a financial institution that establishes an account for a cardholder and issues the payment card. The issuer guarantees payment for authorised transactions using the payment card in accordance with payment card brand regulations and local legislation. Merchants offer goods for sale or provide services in exchange for payment. With SET, a merchant can offer his cardholders secure electronic interactions. A merchant who accepts payment cards must have a relationship with an acquirer—the financial institution that establishes an account with a merchant and processes payment card authorisations and payments. The payment gateway is operated by an acquirer or a designated third party which processes merchant payment messages, including payment instructions from cardholders.

Within SET, public key cryptography is extensively used. Payment instructions are encrypted so that credit card numbers are not intelligible to anyone. Cardholders, merchants and acquirers are authenticated to each other and the integrity of the data contained in the payment instruction is maintained.



18.5 Electronic Cash

Electronic or digital cash (e-cash) facilitates the execution of cash payments for transactions on the Internet. Electronic cash refers to prepaid, stored value that can be used for electronic

purchases in lieu of cash. It is easily exchangeable in an electronic format and is tamper-resistant. The anonymity of the payer is maintained when he is using electronic cash. Privacy concerns thus get addressed into its use while making purchases. But the challenge faced by the bank is to have the ability to create and track authentic electronic cash notes and coins without linking the purchases made to the individual who bought the electronic cash from a bank.

In many cases, the transactions may be small in terms of monetary value (micro-payments) and would therefore not be cost-effective through other payment mediums such as credit cards. In fact, transactions under US\$ 10 cannot generally be paid for by using credit cards.

Using software on a customer's computer, the customer can withdraw e-cash from his/ her own account in a bank. The e-cash is stored online in the hard disk of the customer's computer in an electronic wallet. This e-cash can be spent by the customer for the purchase of items from any merchant accepting e-cash.

For using e-cash offline, the desired amount of money is loaded onto a Smart Card, and special electronic wallets are used to offload the money. The e-cash can also be removed from the Smart Card and moved to a bank account. E-Cash can be used for making/ receiving payments between the customer and the merchant or for any money transaction. A Smart Card is like a standard plastic credit card, except that it contains a microprocessor and a storage unit. It can hold a large amount of information about the cardholder, including digital certificates, and can be used in all banking transactions. It can also be used as an electronic wallet into which monetary value has been loaded.

A customer can use a browser to see products offered for sale on the Internet. Web pages can be scanned, and products available on different shops can be identified alongwith their sale prices. While doing so, the customer browses through web pages on the merchant's servers.

After identifying the products that he wants to buy, the customer sends a request to the customer's bank server for sending electronic cash from his account to his own system. The message is in enciphered form. After checking authenticity, balance, etc. the bank server sends back a secure e-cash packet which is stored in an electronic wallet in the customer's hard disk. The money is converted into a digital token secured through public key cryptography. Having obtained e-cash in his computer, the customer sends an order to the merchant's server alongwith his billing and shopping address, the quantity ordered and the e-cash required for the purchase from the electronic wallet in the computer.

The merchant, after receiving the order alongwith e-cash, issues a receipt electronically to the customer and sends the e-cash to his account in the merchant's bank. The merchant takes the desired steps for the delivery of items to the customer. The merchant's bank sends the e-cash packet to the customer's bank. The customer's bank, after using the customer's public key alongwith the secure packet received, verifies and remits actual fund to the merchant's bank which transfers this money to the merchant's account. The customer gets the items despatched by the merchant at the shipping address.

The e-cash flows to the destination site through the use of any computer network or Internet which has open architecture, due to which the security of the system is very important. Security is provided by using encryption, digital signatures and passwords. Since e-cash is digitally signed by the customer, there is no room for dispute over payment. The implementations could, however, vary from one solution provider to another.

While paying in the form of e-cash, the customer has the option to reveal or conceal his identity. If the customer wants to conceal his identity, the merchant cannot find it out. During clearing, the payee is identified by the bank and the merchant does not know of this identity.

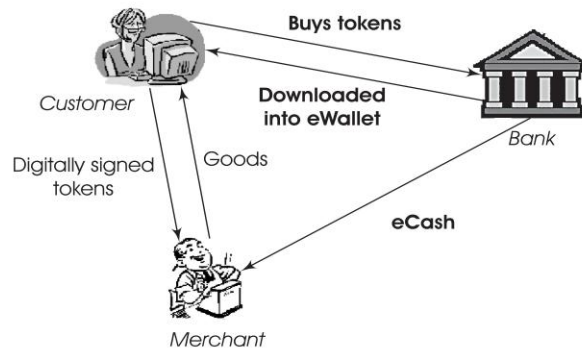


Fig. 18.5 eCash

Electronic cash applications include debit cards, vending, telebanking, teleshopping, phone cards, parking systems, public transit systems and automatic toll collection.



18.6 Electronic Cheque

Electronic cheque is yet another mechanism for Internet payments. This facility is the Internet version of Financial EDI systems which have allowed these functions to be performed over VANs. The electronic cheques provide Internet websites with the ability to perform the following functions:

- Present the bill to the payer
- Allow the payer to initiate payment of the invoice
- Provide remittance information
- Allow the payer to initiate automatic payment authorisations for a pre-specified amount or range of amount
- Interface with financial management software and transaction processing software
- Allow payments to be made to new businesses with which the payer has never before transacted.



18.7 Elements of Electronic Payments

Client Software

This is available from various solution providers. It entails the use of web browser for browsing encrypted information. In most of these cases, the software at the customer site is free. Almost all solutions require a TCP/ IP network connection.

Merchant Server Software

Some solution providers design custom application software for the merchant, while others integrate functions with the web server.

Payment by the Customer

The customer can make payment using a credit card, buy e-cash from a participating bank, or through an Automated Clearing House (ACH). Again the option depends on the solution being provided by the service provider.

Payment to Merchant

In debit-based transactions, the merchant gets payment immediately, from the customer's bank in his account, through ACH, through a bank transfer, or within a day of the clearing period. In credit transactions, the merchant gets paid through a bank transfer or through a normal credit card processing cycle.

A few tools provide this feature of subscription accounting, cumulative billing, etc. In the remaining cases, the merchant's server has to support these functions.

Transaction Cost

The cost per transaction varies for credit and debit transactions

and with the service provider. In some cases, there is a fixed amount per transaction, whereas others charge a certain percentage of the amount of transaction.

Risk

In most of the solutions provided, the risk is that of the merchant for fraudulent transactions. In case of disputed debit transactions or after payment in case a merchant is unable to deliver, the customer loses.

As e-cash works like traveller cheques, in case the customer loses e-cash, the bank has to be provided with details about the serial numbers of the lost e-cash so that the bank can refund the money.



References

1. ICICI Payment Gateway—<http://www.payseal.com/security/>
2. HDFC Bank Direct Pay—<http://www.hdfcbank.com/Companies/sme-inter-business-con.htm>
3. HDFC Bank EPI—<http://www.hdfcbank.com/Companies/inter-business.htm#1>
4. RBI—Report on Internet Banking <http://www.rbi.org.in>.
5. www.paypal.com.

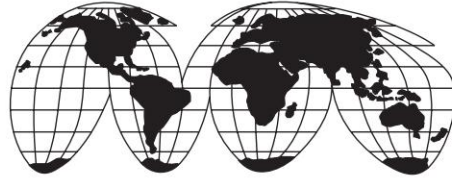
PART

VII

Case Studies in India

- E-Commerce
- E-Governance

Case studies across B2B, B2C and C2C e-commerce implementations in India covering different facets of the economy, including rural economy, are discussed in the chapter on e-commerce. The chapter on e-governance covers some of the success stories at Central and state Government levels.



Chapter 19

E-Commerce—Case Studies



19.1 E-Commerce in India

It is against the backdrop of the world at large, as introduced in Chapter 2, that the status of e-commerce in India should be viewed. Deeper penetration of IT applications in the economy, and in society as a whole, can help boost the economy. Development of the IT industry and the information infrastructure are therefore the twin engines for the growth of the economy. E-Commerce applications can make it easier for the country to better integrate with global markets—the e-marketplace. Liberal policies for the development and growth of the IT industry, telecom connectivity, and Internet penetration have indeed led to the growth of e-commerce.

While a number of horizontal portals are operational in the country, specialised e-marketplaces and vertical portals or vortals have also developed. The horizontal portals provide access to a wide range of information and services while the e-marketplaces and vortals confine themselves to meeting the requirements of relatively closed communities.

In this chapter, we examine some of these initiatives. This includes three popular horizontal portals—indiatimes, rediff and

baazee—along with eChoupal of ITC, which has changed the life of many a farmer, Steel Authority of India Ltd (SAIL) which has adopted e-procurement and Amul, which has used IT to integrate retailers and distributors in a web-enabled supply chain.



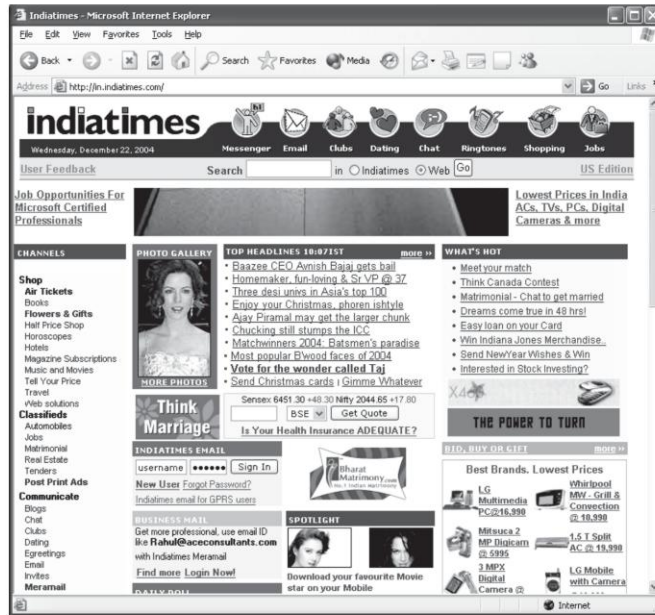
19.2 Indiatimes.com

www.indiatimes.com is an online portal providing information relating to news, insurance, learning, jobs, matrimonials, astrology, cricket and a plethora of other information and services in addition to the newspapers which are published by the Times of India Group. The Indiatimes.com portal is a venture of Times Internet Limited, a subsidiary of the media conglomerate, The Times of India Group.

Indiatimes.com launched Indiatimes Shopping in May 2001. It offers a range of products from books and music to kitchenware, clothes and food. Indiatimes Shopping ships items within India, and a limited selection of items to the US. However, the majority of its customers live outside India, primarily in the US and UK. The online mall is only a click away, making it a convenient place to shop or to buy presents for family members and friends who are far away.

Through DNV's EBtrust, a third party certification of infrastructure, security and processes, Indiatimes has sought to assure visitors to the site that the site has been audited and found to work properly, not just in terms of security but also in respect of the processes being followed at the back-end.

With around twenty million Indians living outside the country, most of whom possess Internet access and credit cards, Indiatimes.com focuses mainly on the international market. However, they realise that with a population of over one billion, the domestic market in the country also offers a huge potential. The portal is tapping the same.



➞ Fig. 19.1 *www.indiatimes.com*

Payment for goods and services transacted on indiatimes.com can be carried out in a number of ways. The cash on delivery (cod) mode of payment is open for self-purchase and payment can be made for the order only when it is actually received. However, this option is available only for residents of Delhi, Noida, Gurgaon, Ghaziabad, Faridabad, Mumbai, Bangalore, Chennai and Hyderabad. Using credit cards such as VISA and MasterCard, payments can be processed through an online payment gateway system. For payment by cheque/ Demand Draft payable at New Delhi/ Delhi, the printed order form has to be submitted along with the cheque/ DD to Times Internet Limited. In the case of payment by cheque, order is shipped only when the cheque has been cleared for payment. If the buyer has an account with HDFC, Centurion Bank, ICICI Infinity, UTI or IDBI, the order can be paid for through any of these banks' payment options and the amount will be automatically debited from the buyers' account through an online payment gateway system.



19.3 Rediff.com

Rediff.com is an online provider of news, information, communication, entertainment and shopping services mainly targeted at Indians. Founded in 1996, Rediff.com is headquartered in Mumbai with offices in New Delhi and New York, USA.

The Rediff.com India website consists of information, communication and content services, free and paid community features and products, including e-commerce and mobile services. Information and content channels currently include news, business, movies, cricket/ sports, auto, health, food, books, gaming, astrology, contests, lifestyle, home décor, women and several other topics of interest.

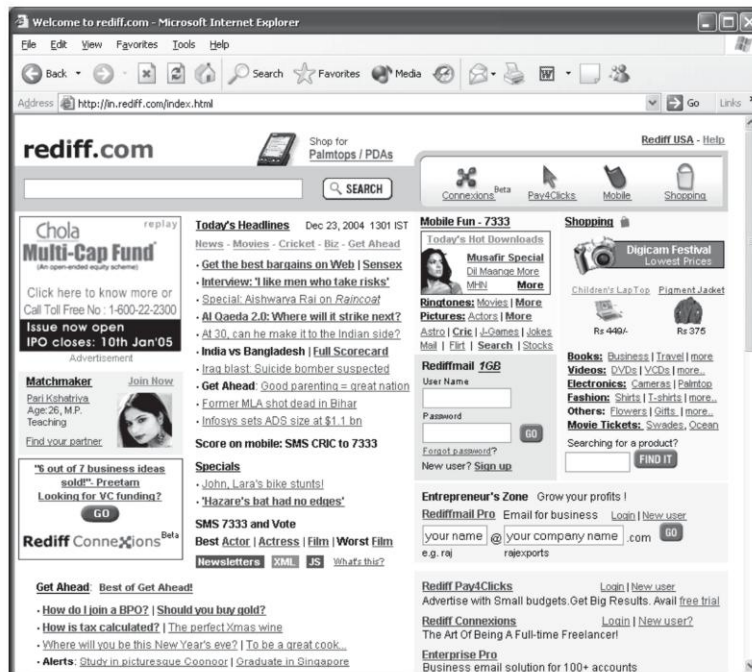


Fig. 19.2 *www.rediff.com*

Through a single login facility, Rediff.com provides a combination of free and paid community features and products to consumers and businesses. These offerings include e-mail, instant messaging, chat, e-cards, matchmaker, astrology services, blogs, message board, mobile services and online shopping.

As far as e-commerce is concerned, Rediff Shopping is an online marketplace which allows users to purchase products and services from various merchants. Rediff.com offers products and services in more than fifty categories, the most popular of which are apparel, personal accessories, footwear, electronics, flowers and jewellery. Users can avail of a variety of payment options such as cash on delivery (COD), Internet banking, credit card and cheques.

Rediff.com is the only Indian portal listed on the Nasdaq.

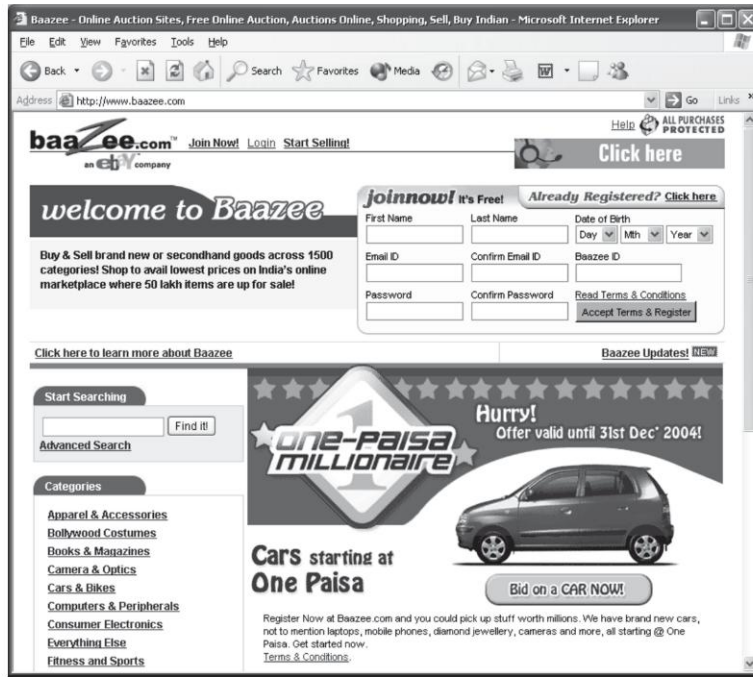


19.4 Baazee.com

Baazee.com India Pvt. Ltd, a subsidiary of the US-based Baazee.com, Inc., started its operations in India in January 2000. Headquartered in Mumbai, Baazee is India's biggest marketplace where anyone can sell or buy almost anything. Over one million registered users trade in a wide range of item categories including electronics, cameras, phones, computers, movies, mobiles, fashion, music, homes, toys and travel.

In August 2004, Baazee.com along with its Indian subsidiary Baazee.com India Pvt. Ltd., was acquired by eBay, one of the most popular shopping destinations on the Internet. With this acquisition, Baazee has become a part of a global community of eBay users which number more than one hundred million and hail from 29 countries across the world. Although the portal calls itself a marketplace, its association with eBay fosters the impression of it being an auction site.

Payments for certain items on Baazee.com can be made through the online payment facility provided by PaisaPay (www.paisapay.com). At present, PaisaPay supports credit card payments and online bank transfers. Online bank transfers can



➡ Fig. 19.3 *www.baazee.com*

be done through the Internet banking services of ICICI Bank—Infinity, UTI Bank—iConnect, IDBI Bank—inetbanking, Oriental Bank—ipay@obc, Centurion Bank—ePay, HDFC Bank—DirectPay, Bank of Punjab—ePayments and Federal Bank—FedNet.

All sales and purchases on the site continue to be bipartite contracts and Baazee/ PaisaPay disclaims any responsibility for any non-performance or breach of any contract entered into between the buyers and the sellers. Baazee positions itself as a platform for communication only.



19.5 Steel Authority of India Ltd. (SAIL)

Steel Authority of India Limited is the number one manufacturer of steel in the country. Being a manufacturing organisation,

where more than 50 percent of the expenditure is on account of raw material, stores and spares, SAIL had identified 'input cost reduction and revenue maximisation' as the thrust areas to improve its bottomline.

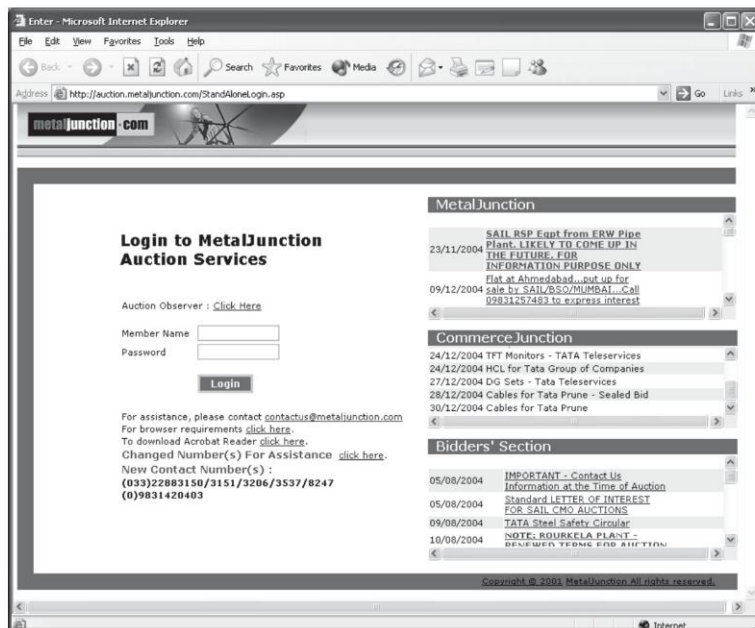
Well-established procurement system and procedures have to keep pace with the latest trends in procurement. SAIL decided to adopt e-procurement in its effort to reduce input cost. Towards this objective, an e-arm of the company, Metaljunction.com was created as a joint venture agreement with M/s Tata Steel.

Initially, input materials (consumables) were procured through online reverse auction with the technical/ market making services support from Metaljunction.com.



➡ Fig. 19.4 *www.metaljunction.com*

Reverse auction (RA) is a procurement tool available under e-commerce through which the techno-commercially acceptable bidders simultaneously bid their price online leading to price discovery. Also known as buyers auction, in reverse auctions, the buyer invites bids from multiple sellers. The price decreases as sellers compete for the buyer's business with the lowest bid considered as the winner. Many large corporations may use a reverse auction as an alternative to the more traditional tendering process. It creates an intensely competitive environment leading to efficient price discovery and reduction in procurement cost. Except for the online price bidding, all other processes like issuing of tender document, submission of tender document, techno-commercial discussion/ clarifications, etc. are being done manually as of now. However, SAIL has initiated steps to create Internet-based e-procurement modules for moving towards complete paperless transactions and conducting the entire procurement process online. This is now at the development/ trial stage.



➞ Fig. 19.5 Auction services at metaljunction.com

E-commerce being a comparatively new area, SAIL initially took steps to devise internal systems and procedures for conducting RA. The first three trial reverse auctions were conducted till March 2002.

During 2002–03, 18 RAs were conducted and during 2003–04, more than 50 RAs were conducted. This has resulted in savings of 8–10 percent in processing by SAIL. The system of procurement through RA has been fully established today in SAIL and RAs have been conducted even in its smaller plants.

SAIL is the first public sector unit (PSU) in the country to have conducted RA successfully and its effort in this regard has been widely appreciated. Other public sector undertakings have also tried to emulate this effort of SAIL and SAIL has been approached for providing guidance/ consultancy in this regard.

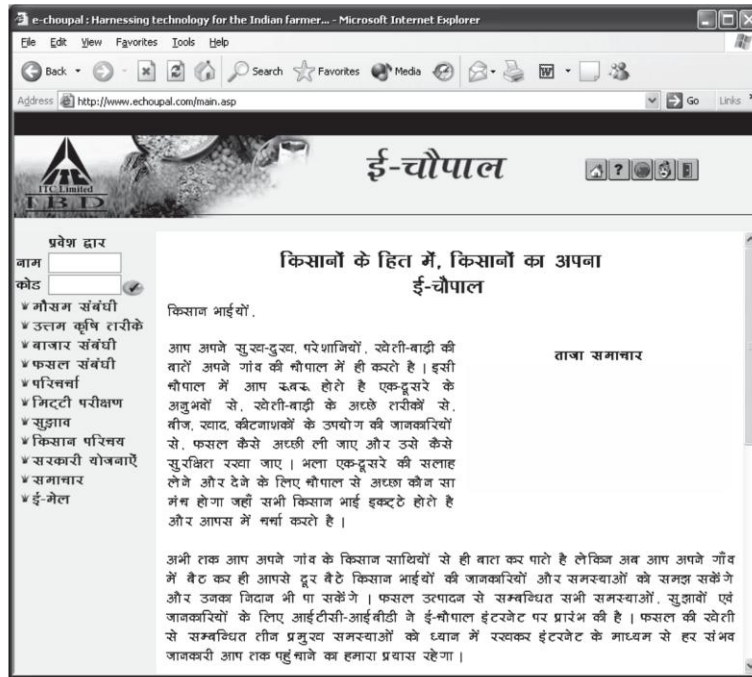


19.6 ITC—Empowering Farmers through E-Choupal

ITC Ltd., a leading fast moving consumer goods (FMCG) cigarette major, while being renowned for its cigarette business, also has business interests in hotels, paperboards, paper and packaging; agri-exports and some other FMCG products like branded packaged foods, safety matches, incense sticks and greeting cards. ITC is one of the country's biggest foreign exchange earners (US\$ 2 billion during the last decade).

ITC's agri-business is one of India's largest exporters of agricultural products. Traditional methods of procurement through intermediaries were initially being followed by ITC, which resulted in lower compensation to the farmers.

With its innovative web-based e-choupal initiative, ITC has sought to plough back a larger share of the product price in the market to the farmer in respect of its agri-business. The distribution process has been adapted to meet the needs and challenges of consumers at the bottom of the economic pyramid.



➡ Fig. 19.6 *www.echoupal.com/main.asp*

E-Choupal has become the subject matter of a case study at Harvard Business School, and is expected to progressively create for ITC a huge rural distribution infrastructure, significantly enhancing the company's marketing reach.

With e-choupal, the farmers, who participate in this initiative, benefit from higher price returns. ITC operates at a lower cost, having re-engineered the supply chain—the intermediaries in the supply chain between the farmer and ITC, have retained their functions of aggregation, logistics and financing, but have been removed from the chain of information flow and market signals.

E-Choupal was launched in June 2000 and is one of the pioneering initiatives for rural India. Its services are now offered to more than three million farmers in over 29,500 villages through around 5,050 Internet kiosks across villages in Madhya Pradesh,

Rajasthan, Karnataka, Andhra Pradesh, Maharashtra and Uttar Pradesh. E-Choupal is expanding into 30 new villages every day. The products covered include soyabean, coffee, wheat, rice, pulses and shrimp. The e-choupal portals are based on Indian languages like Hindi, Kannada and Telugu.

e-choupal kiosks are managed by *sanchalaks*, who are farmers themselves. The *sanchalaks* selected by ITC to run the service in the village are educated at least up to the high school level. In many instances, the children of the *sanchalak* too help out in the running of the Internet kiosk. Information relating to the weather, market prices, farm practices and risk management, along with facilitation of sale of farm produce and procurement of farm inputs, is provided through these kiosks, all in the local language.

The following five distinct services are offered to the farmers by e-choupal:

- Information in the local language on the weather, crop prices, e-mail and news
- Knowledge on farming methods
- Purchase of seeds, fertilisers, pesticides and services
- Sales of their produce
- Development.

The Indian farmer is now linked to consumers in the local and global markets through e-choupal. A farmer who would earlier find out the price for his produce after he had incurred costs of transportation, thereby selling at whatever price he got, can now make a decision before leaving the village.

Meanwhile, ITC now buys more than 25 percent of its commodities through the e-choupals. E-Choupal transactions worth \$100 million were carried out in 2003.

In view of the positive response received from farmers in the four states where e-choupal has been implemented, ITC now plans to extend e-choupal to eleven other states in India in the next six years to cover 100,000 villages, and reach out to 10

million farmers. By 2010, the turnover of the e-choupals is projected to reach over Rs 9,000 crores.



19.7 Amul—The Taste of India

Formed in the year 1946, Amul initiated the dairy co-operative movement in India and formed an apex co-operative organisation called the Gujarat Co-operative Milk Marketing Federation (GCMMF). This organisation is today spread over 70,000 villages which spans 200 districts of India. This ‘white revolution’ has made India the largest producer of milk in the world today. Amul has not only spearheaded this revolution but has also become a symbol of IT implementation in rural areas. It has successfully utilised IT to bridge the digital divide and to take IT to the masses.

The GCMMF comprises 12 affiliated member dairies and district milk unions with each union having its own manufacturing unit. These unions have, among themselves, about 2.2 million milk producing members, supplying milk twice a day. The amount of milk collected is about 6 million litres per day with an annual turnover of approximately Rs. 27 million.

Earlier, members of the co-operative were given passbooks containing personal details and details about the quantity and quality of the milk like percentage of fat, volume, etc. When members came with the milk, the volume of the milk was recorded in the passbook and a small sample of milk was taken for testing of the quality. The testing of the milk was done at a later date and the payment was made accordingly to the members. This caused a delay of about a week in making payments, besides which there was also a lot of room for fraud in the process.

As an IT initiative, Amul introduced Automatic Milk Collection System Units (AMCUS). Over 3000 units were installed at the village societies. These units are capable of capturing member information, milk fat content, volume collected and amount

payable to the member. Each member is given a plastic card for identification. The farmer drops the card into a box and the identification number is transmitted to the unit. The milk from the farmer is measured and a small sample is put in an electronic fat testing machine. Both these readings are recorded by the computer and the amount to be paid is calculated on the basis of the fat content of the milk. The amount of money to be paid is printed on a slip and given to the farmer who then collects his payment from the counter. The AMCUS installation has made sure that payments are made on an immediate basis. This has also reduced the amount of possible fraud. In 2002, Amul made around 10 million payments daily amounting to Rs 170 million in cash.

Since milk is a highly perishable commodity, AMCUS has made a vital difference in milk collection and supply. More than 5000 trucks move milk from villages to the 200 dairy processing plants twice a day according to a precise schedule. The supply chain management is also facilitated by other IT initiatives.

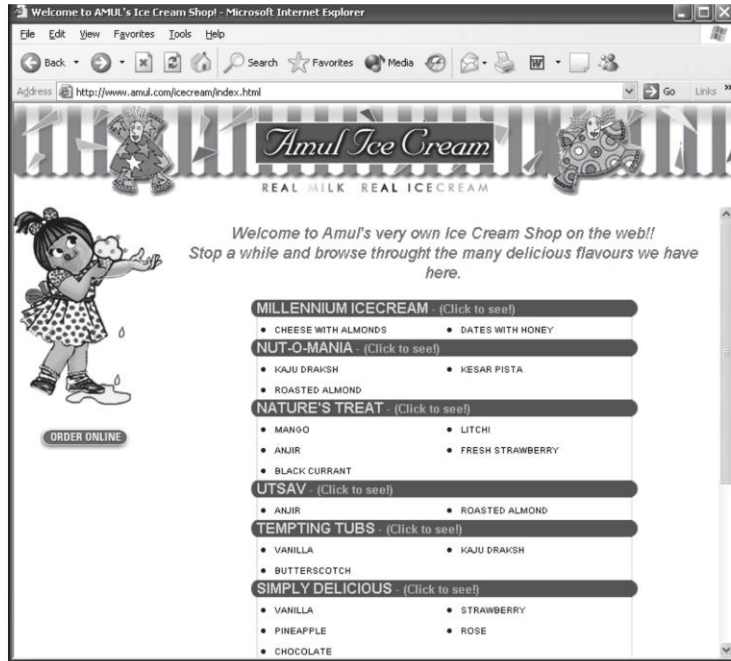
When Amul took the decision of using IT for the integration of its operations, it started with re-design and re-organisation of all applications so as to provide a seamless flow of information. It started with the implementation of an ERP solution called the enterprise-wide integrated application system (EIAS). This system covers multitude of operations like marketing, planning, advertising and promotion, distribution network planning, stock control, sales, quality control management, etc. The software is platform-independent and can be plugged at any point of the supply chain process. All zonal offices, regional offices and member dairies of Amul are interconnected through VSATs for seamless exchange of information. Each of Amul's offices is connected by e-mail. They send their daily reports to the main system at Anand in Gujarat.

Another innovation is the way GIS has been used by Amul. Amul has used GIS to plot zone/ depot boundary and also pointer for zone, depot and distributor locations, which are

superimposed by the product sales data. All the census information on farmer members including the animal census information is also captured. This enables Amul to mine information regarding milk production and productivity of animals region-wise in Gujarat. The same system can also be used for monitoring veterinary health and controlling animal diseases.

One of the members of GCMMF, Banas Dairy, has started a unique initiative, an Internet Sewa project called Banaskantha. In collaboration with IIM, Ahmedabad's e-governance centre, it has developed a Dairy Information System Kiosk (DISK) for Amul. DISK gives a front-end for all applications and modules. Apart from automating the collection of milk, the system would be used for data analysis and decision support to assist in improving milk collection. DISK will also contain an extensive database on the history of cattle owned by a farmer, containing details like medical history, reproductive cycle and history of diseases. The farmer is also given access to a multi-media database on innovations captured by Srishti, an NGO working with IIM, Ahmedabad. Since a large amount of data on milk production is available in the database, the system can also be used to monitor milk production from individual sellers, and forecast the amount of milk which will be collected.

Amul was one of the first five Indian organisations to have a web presence. It also adopted the .coop domain to make its presence distinctly. Currently Amul is in the process of web-enabling the entire supply chain so that it can capture key information and use the same for decision making. Amul has also linked its distributors and incorporated web pages of top retailers on their site as a part of their B2B initiative. Distributors can also place orders on the website, www.amulb2b.com. Because of this kind of web presence, the company has been receiving enquiries from countries like US, Britain and New Zealand, and the value of its exports has grown to Rs 100 crore. It has also started an online ordering facility for all Amul products including ice cream. Presently, it has the capacity to service consumers in more than 125 cities.



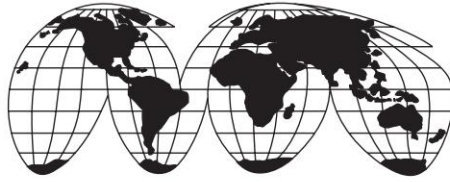
➞ Fig. 19.7 E-Commerce at Amul

Amul has proven to the world that investments in information technology in rural India can be made productive. As a leader of the co-operative movement in India, it has also shown how information technology can be used to its full potential.



References

1. Indiatimes portal www.indiatimes.com.
2. Rediff portal www.rediff.com.
3. Baazee marketplace www.bazee.com.
4. ITC's e-choupal initiative; *India Today*, December 13, 2004.
5. www.amulb2b.com.



Chapter 20

E-Governance—Case Studies



20.1 E-Governance for India

The direction shown by the governments, as seen in section 2.7 of Chapter 2, in transforming themselves into electronic governments, is applicable in India as well. This transformation is all the more essential for India because existing government practices include the procedures of not only the industrial government but that of the colonial era as well. India has to respond to the emerging needs of the digital economy, and for integration into the networked world.

The Government of India has recently approved the National E-Governance Action Plan for implementation during the years 2003–2007. The Plan seeks to lay the foundation and provide an impetus for long-term growth of e-governance within the country. It seeks to create the right governance and institutional mechanisms, set up the core infrastructure and policies, and implement a number of mission mode projects at the Centre, state and integrated service levels, to create a citizen-centric and business-centric environment for governance. Overall the programme content, implementation approach and governance structures are in the process of being established.

In an earlier exercise in 1998, the National IT Task Force had set up a Citizen–IT Interface Working Group with the mandate of formulating projects as well as policy guidelines for promoting

the beneficial impact of IT to deliver government services to citizens electronically. The Working Group recognised that IT is an agent of change, an agent which can transform every facet of human life, and that it is possible to bring about revolutionary changes in the lives of citizens through the deeper penetration of IT in society. It examined the use of IT both at the Central Government and the State Government level.

The existing methods and procedures, which were introduced more than a century ago, needed to be re-examined with a view to re-engineer them through Business Process Re-engineering (BPR) techniques. The induction of IT, especially direct interface of citizens through networks, messaging over networks, electronic commerce systems, smart cards, and other enabling IT tools, could help bring about transparency in governance and remove unnecessary bureaucratic intervention.

The Working Group under the National IT Task Force had made 25 recommendations under the following five broad categories:

- Government-wide information infrastructure
- Re-engineering of government processes
- Service delivery to citizens
- Service delivery on commercial basis
- Best practices
- HRD requirements

The Government of India needs to create websites for the effective dissemination of information, i.e. the publish mode, or the first generation of electronic delivery of information. The websites have to be designed with a view to move from the publish mode of information dissemination to the interact mode and then to the transact mode. The necessary infrastructure that is required for this to happen includes the following:

- STD booths to be upgraded into info kiosks that can deliver Internet-enabled IT services to citizens
- Computers to be made cheaper and computer awareness to be increased
- Telecommunication costs to be made cheaper

Unless the cost of telecommunication comes down and computers become cheaper, the utilisation of IT will not gather momentum.

The Working Group under the National IT Task Force had also identified area-wise requirements of citizens to include public grievances, rural services, police, judiciary, social services, registration of licences and certificates, public information, economically weak section (EWS) services, agriculture sector, utility payments/ billing, commercial taxes and returns filing, and government procurement.

The Citizen–IT Interface Working Group under the IT Task Force had identified the following ten major areas for launching pilot projects in one or more states:

- Government tendering/ electronic procurement
- Utilities payment/ billing
- Education (results, career consulting)
- Employment opportunities
- Health (LAN-MIS for hospitals)
- Judiciary
- Land records
- Agriculture related (weather forecasting, crop diseases, agriculture prices)
- Ration cards issuance
- Driving licence issuance, motor vehicles registration
- Pension
- Government regulatory information
- Public grievance filing/ tracking
- Railway/ road/ airline time tables/ fare charts

While endorsing the National E-Governance Action Plan in 2004, the Citizen IT Interface Working Group made the following key observations:

- Adequate weightage must be given for quality and speed of implementation in procurement procedures for IT services.

- Suitable system of incentivisation of states should be incorporated to encourage adoption.
- Delivery of services through common service centres should be encouraged and promoted.
- Wherever possible, services should be outsourced.
- The full potential of the private sector investment should be exploited.
- Connectivity should be extended up to the block level through National Informatics Centre's Network (NICNET)/ State Wide Area Networks (SWAN).
- R&D should be undertaken in government systems.

The Plan includes the following components:

1. Core policies
2. Core projects
3. Core infrastructure
4. Integrated services projects
5. Support infrastructure
6. Human resource development/ training
7. Technical assistance
8. Awareness and assessment
9. Organisational structures
10. R&D

The criteria for selecting mission mode projects under this Plan included the impact in terms of the number of people likely to be affected, likely improvement of the quality of service, the economy or economic environment in the country, the likely cost benefit of investments in the project, readiness and willingness of the ministry/ department to position a National Mission Project, and feasibility of implementing the project from a financial, administrative and political perspective within a reasonable time frame. These projects include income tax, passports and immigration, national citizen database, department of company affairs' DCA21, banking, land records, road transport, EDI(e-commerce), India portal, e-procurement and E-Biz among others.

It is against the backdrop of these initiatives of the government that e-governance projects have taken off in the country. Some projects, which had already been initiated, benefited from the new directions, while newer projects could start off with some measure of infrastructural and legal framework already in place. Four projects which have been implemented and are benefiting both the government and citizens are covered in the following sections of this chapter.



20.2 Indian Customs EDI System

Indian customs has been among one of the first government regulatory agencies, in various parts of the world, to have introduced EDI in its interface with importers, exporters, and other players involved in international trade. It has carried out a major BPR exercise to improve its efficiency, and change its image from control to facilitation. The transition from customs controls to facilitation represents an attitudinal change on the part of customs agencies, which have traditionally been viewed as regulatory in nature. IT in general, and EDI in particular, have helped re-engineer the processes related to customs clearance.

The Indian Customs EDI System (ICES), designed, developed and implemented jointly by the National Informatics Centre (NIC) and the Customs Department, heralded an era of paperless trade in the country. ICES has transformed the custom house into a paperless office. The working of the office has been re-designed according to re-engineered procedures through appropriate application software in ICES with a view to link the same with EDI transactions from across the organisational boundaries of the custom house.

The pilot EDI project implemented at Delhi Custom House in May 1995, facilitated online clearance of import documents filed electronically by importers, and/ or their clearing agents over NICNET. ICES was extended to white shipping bills in May

1996, and to duty drawback shipping bills with effect from November 1996. Importers, customs house agents (CHA), and exporters would transmit bills of entry, shipping bills, and other related documents such as invoice, licence, etc. over dial-up links to the NICNET EDI server, which, in turn, would submit them to the customs computer system for clearance. A CHA does not have to chase his documents physically from table to table in the Custom House for clearance. The project has since been extended to cover all custom houses in the country.

ICES comprises two main sub-systems, namely ICES/ I for processing of bills of entry; and ICES/ E for processing of shipping bills. Service centre modules have been incorporated in both these sub-systems, which allow entry of documents from the service centre located in the Custom House. CHAs who do not have their own computer systems, can bring their documents to the service centre for data entry and submission to the Customs system.

Indian Customs EC/ EDI Gateway (ICEGATE) was implemented in 2001–02. It has also been licensed by the Controller of Certifying Authorities to operate as a Certifying Authority (CA) under the IT Act, 2000. The iCERT CA—the legal CA entity under which the Customs CA operates—serves the community of users in ICES including customs officials, Custom House agents and importers/ exporters.

CHAs can use the Remote EDI System (RES) which is a stand-alone software package for preparation of bills of entry (BEs), shipping bills (SBs) and other related documents. It has been developed by NIC as part of the ICES project. Documents transmitted electronically are submitted to ICEGATE for clearance.

20.2.1 Customs Clearance

These documents are reviewed by different officers of the Custom House at various stages of processing and final clearance is accorded on the computer system after all the formalities,

including physical examination of the goods at the air cargo sheds, are over. ICES keeps track of officers who have handled documents at various stages of processing. The trail of the processing cycle is available to superior officers at any time. A CHA, in turn, can enquire about the status of his documents from his own system. He can view any memo or objections on his documents as soon as they are posted in the system.

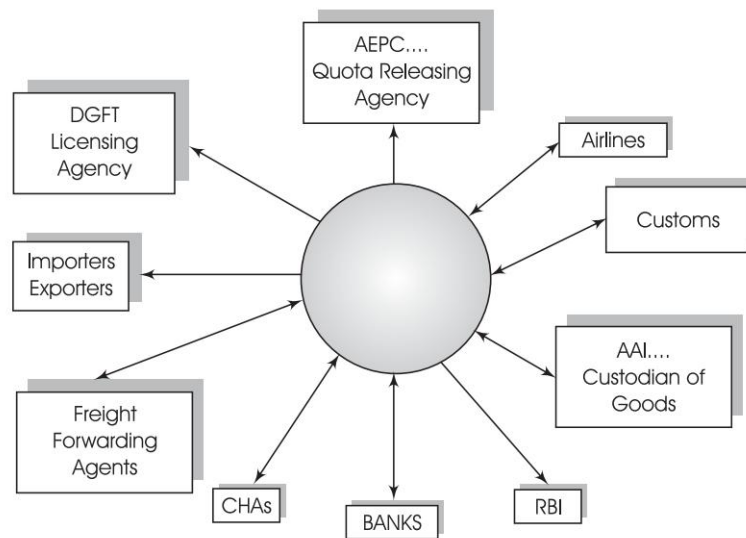
20.2.2 Service Centre

CHAs who do not have access to computer systems use terminals in the service centre for having their documents entered into the computer system for processing. They are able to see the status of their documents from the enquiry counter terminals positioned at the service centre. CHAs do not interact with the customs staff until the stage of physical examination of goods. On the basis of pre-determined criteria, ICES suggests the specific packages which may be checked by the customs staff in the examination unit.

In addition to CHAs, importers, and exporters, ICES provides for integration of other agencies involved in the customs clearance through EDI technology. The Customs EDI Community System includes the following:

- Directorate General of Foreign Trade (DGFT)
- Punjab National Bank (PNB), and other banks
- Airports Authority of India (AAI)
- Apparels Export Promotion Council (AEPC)
- The Reserve Bank of India
- Custom House Agents (CHAs)
- Importers/ exporters
- Airlines
- Port authorities
- Shipping lines
- Shipping agents

This is shown in Fig. 20.1.



➞ **Fig. 20.1** Customs EDI community system

Import licences issued by DGFT, the quota release position of AEPC, are directly available in the customs computer system through these EDI linkages. With this arrangement, there is no need for an exporter to get the allocation number endorsed on the body of the SB from AEPC. The DEEC and EPCG certificates are no longer required from importers since they can be downloaded from DGFT computer systems. The GR-1 form required by the RBI can be directly transmitted from the customs computer system to the RBI computer system.

During the very first stage of implementation, the computer system of PNB, which is within the premises of New Custom House, was integrated with ICES. The advice for duty payment goes directly to PNB in addition to the printing of a TR-6 *challan* form in the service centre for the CHA, if he wishes to have a copy. The advice on the payment of duty is sent directly from PNB to ICES, and the information is available on the terminals in the examination unit at the import cargo shed.

AAI is also a part of the customs EDI community system. Data about imports and exports are downloaded from ICES to

its cargo management system. Similarly, Import General Manifests (IGMs) and Export General Manifests (EGMs), filed by the airlines with customs, are downloaded to AAI. The attempt in ICES is thus to capture the data only once from the agency that deals with that subject matter, and then make it available to others who need the same.

ICES facilitates payment of duty drawback without the exporter having to submit a large number of documents for the purpose. In fact, he is no longer asked to submit any additional documents other than those submitted at the examination stage. No separate account numbers or ledger numbers are to be maintained by the exporter for the purpose of making drawback claims. The work related to the scrutiny of SBs for drawback claims has been integrated with appraising in ICES. Assessing officers verify the claims with respect to the drawback rates, quantity and value exported, and pass the bills for payment at the designated levels of Superintendent/ Assistant Collector. All these documents are further examined by audit through an appropriate software module.

No cheques are prepared unless an exporter asks for them. The system automatically generates a payment file which is sent electronically to the bank connected to the computer system at the Custom House. A majority of exporters have opened accounts with the bank in the Custom House for this purpose. The payment file generated according to the bank account numbers helps the bank to credit the accounts of the exporters directly. The drawback payments are thus automatically generated for each shipping bill unlike the earlier practice of consolidating a number of shipping bills and making the payments only once a month.

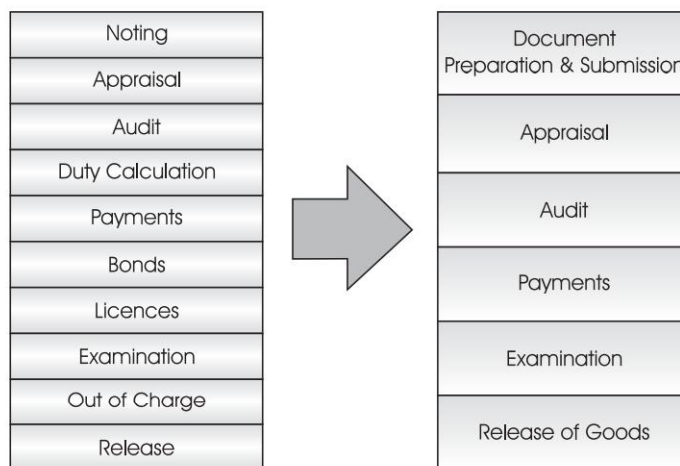
ICES has eliminated a number of processes which were part of the erstwhile manual system. Some of the stages have been merged, while a few have been eliminated altogether. For example, at every stage, there were noting registers wherein entries would be made for the same document. The


re-engineering introduced in imports and exports processing is briefly explained below.

20.2.3 Imports

The Bill of Entry (BE), the import declaration, was assigned a unique number in the noting section, in a register. At all stages of processing, viz. appraising, comptist, Asst. Commissioner, audit, cash, bonds, licence, bank, guarantee, examination, etc. entries would be made corresponding to the BE No. of the document being processed. The workflow software implemented in ICES keeps track of the movement of the BE. All registers stand eliminated. The noting section has been eliminated since ICES allocates a BE number automatically. Comptist has been eliminated, since ICES computes the duty once assessment has been completed by the assessing officer and/ or the Assistant Commissioner.

ICES sends the assessed document to the bank connected with it on EDI. If the importer maintains an account there, and keeps a sufficient balance in it to enable automatic debit of the same, the duty payment becomes instantaneous. The BPR thus enables immediate transmittal of the BE to the examination sheds.



 **Fig. 20.2** *Process reengineering for imports*

ICES has provision for system appraisal of the import declarations. The documents need not be appraised on the screen by assessing officers. System appraisal is carried out routinely in respect of imports of the following items:

- Diplomatic goods
- Defence supplies
- Gold
- Books
- Aircraft parts.

These account for nearly five percent of the imports at IGI Airport, New Delhi.

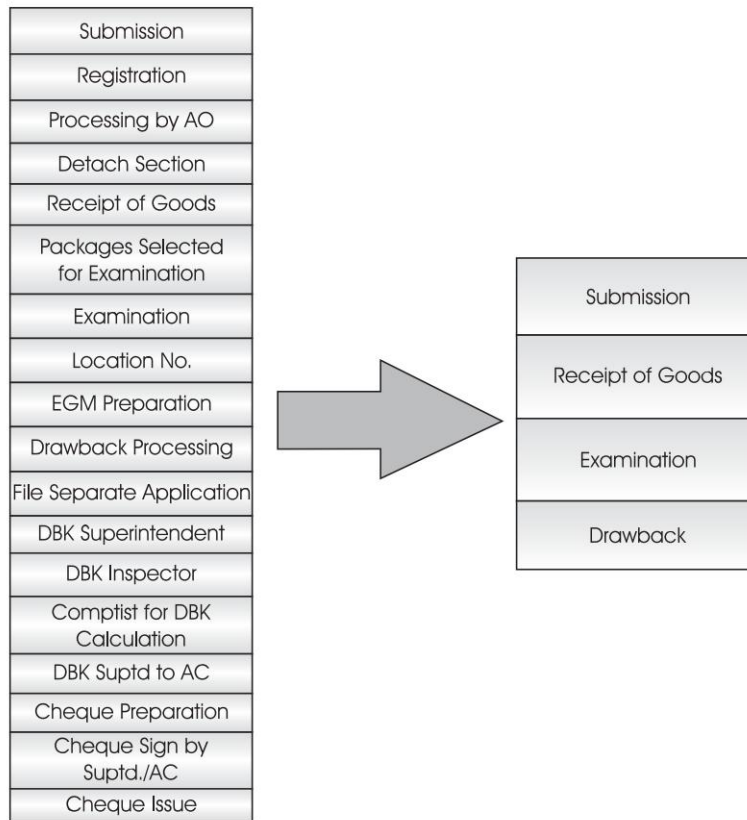
ICES has facilitated green channel clearance for a number of importers with a good track record. On the basis of their reliability and reputation, importers are allowed to clear their consignments without any examination. But appraising is performed in a routine way. At Delhi, nearly 15 percent of the imports are allowed through this channel.

In the scheme of fast track clearance, there is no appraising and no examination. There is an automatic system appraisal of the BE, after which it directly goes for duty payment. This track is permitted to importers who register themselves for it, and deposit some advance money with the customs. They are also required to declare the items for which fast track clearance will be used by them.

20.2.4 Exports

ICES has introduced more radical procedural changes in exports processing. In addition to eliminating the noting stage and all registers, appraising itself has been done away with for shipping bills related to non-drawback exports. In the case of drawback exports, an exporter is not required to file any separate application for release of duty drawback. No physical cheques are issued, instead the drawback payment is directly credited to the exporter's bank account.

Reduction in the number of processing stages, for a drawback Shipping Bill (SB), through BPR in ICES is illustrated in Fig. 20.3.



 **Fig. 20.3** *Process reengineering for exports*

The most salutary gain of the ICES project at the Custom House is the achievement of the objective of 'customs facilitation' through an attitudinal change among customs officers. They accepted the system in a very positive manner. The trading community is happy about the transparency of procedures and new processes, and the accountability that goes along with it. The benefits of ICES can be summarised as follows:

- Transparency of the system

- No physical movement of document, thereby reducing processing time
- Faster clearance of consignment
- Minimum interaction with customs officers
- Online enquiry
- Nearly 50 percent of consignments being given green channel (i.e. no examination of documents as assessed by the system)
- Uniform assessment
- Precedent search
- Electronic submission of documents over the network from anywhere
- Higher efficiency in customs operations
- Truly a trade facilitator
- Customs EDI community system links all agencies



20.3 Indian Railways

The Indian Railway Catering and Tourism Corporation Limited (IRCTC) is a public sector company set up and fully owned by the Ministry of Railways. The IRCTC has been incorporated under the Companies Act, 1956 and has its registered office at New Delhi. This company has been formed to function as an extended arm of the Indian Railways to upgrade, professionalise and manage catering and hospitality services at stations, on trains and at other locations, and to promote domestic and international tourism through the development of budget hotels, special tour packages, information and commercial publicity and global reservation systems.

Indian Railways has the distinction of being the second largest railway network in the world under a single management. Traversing through the length and breadth of the country covering approximately 63,140 route kms, Indian Railways is the principal constituent of the nation's transport system. It owns a fleet of 2,16,717 wagons (units), 39,236 coaches and 7,739

locomotives and manages to run 14,444 trains daily, including about 8,702 passenger trains. More than a million tonnes of freight traffic and about 14 million passengers covering 6,856 number of stations, are transported daily by Indian Railways.

Indian Railways started its tryst with Internet-based information systems when its website *www.indianrailways.gov.in* started answering simple queries, based on trains running between important stations, train schedules, information about special trains, train fares, PNR number status, etc. This was just the beginning. In line with changing times, IRCTC, the marketing arm of the Indian Railways, in collaboration with the Centre for Railway Information Systems (CRIS), launched the Internet Rail Ticketing service for the Indian Railways at *www.irctc.co.in* on 3 August, 2002.

The website has a simple design and easy to browse links. Persons interested in using the online reservation feature need to register once with the website. This registration is free of charge. During the registration process, personal details like name, age, sex, etc. are submitted and a user name and password given to the person. Tickets can then be booked for any rail journey in India. The payment has to be made through credit card, and tickets are delivered by courier at the doorstep after verification of the credentials of the recipient. It is also possible to pick up tickets from IRCTC offices in the metros. These tickets can be cancelled from any normal booking counter and the amount will be credited to the credit card. IRCTC has tied up with ICICI and Citibank payment gateways to enable online transactions. It has also entered into an agreement with ICICI, Housing Development Finance Corporation (HDFC) and Industrial Development Bank of India (IDBI) to facilitate direct debit facilities for account holders of these banks. Several other banks are also in the process of being integrated with IRCTC. Currently the tickets which are being booked online, are printed in Delhi and then distributed to different destinations within 48 hours through courier.

The IRCTC also offers a 24 hour helpline and e-mail support to assist customers with time table enquiries, train timings, e-mail alerts and online consignment tracking system to find out the delivery status of tickets. The website handles approximately 1.3 million enquiries per day.

Starting with a daily average of 115 bookings per day, the website today boasts of over 2500 tickets daily all over the country. Not only do domestic customers use the website, but more than 100 foreign tourists use the website weekly for 'e-ticketing'. They accept the delivery of tickets at hotels and addresses of their choice in India or IRCTC's offices in the metros. The average monthly turnover of the website is over Rs 80 million making it the fastest growing credit card-based transactor in Asia Pacific.

One of the benefits of online booking is that the long unwieldy queues at the counters are a thing of the past. Tickets can be booked faster. The person manning the counter is friendlier, making the customers visit to the booking centre a pleasant experience. Frequent travellers who used to rely on booking agents to book their tickets are also moving on to Internet booking, since they have a more reliable alternative. One of the reasons for this is that IRCTC has a flat charge for upto six passengers, unlike the high charges of travel agents who charge anything from Rs 25 to Rs 50 per passenger.

The online booking facility currently is only for a point-to-point journey. IRCTC does not offer the facility for cluster stations with provision for halting at different destinations. However, it is slated to offer this facility very soon.

The application and database management components run on four separate four-way servers. The web servers have been put on another set of four servers. The system on the whole links legacy applications to cost-effective, scalable and reliable servers.

In view of the popularity of its website, IRCTC has tied up with two websites, *timesofmoney.com* and *bazee.com*, to offer

exclusive services like tax planning and discounts apart from a weekly lottery that will refund one lucky passenger his travel expenses. Similarly ICICI Prudential, Citibank and VIP luggage are planning to offer value-added services like discount coupons to costumers.

The online passenger reservation system is a significant step ahead for the Indian Railways. It is a working example of e-enabling the lives of Indian citizens. Although computer literacy in India is far below that in many of the other developing countries, the popularity of this site shows that there is will among the people of India to make the best use of technology.



20.4 Government of Andhra Pradesh—eSeva

The Twin Cities Network Services (TWINS) project of the Government of Andhra Pradesh, focusing on Hyderabad and its sister city Secunderabad, was launched in December 1999. It provided selected services and information on various departments and agencies of the state and Central governments. The TWINS project proposed one-stop services to the public, eventually through multiple delivery channels like Integrated Citizen Service Centres (ICSCs), electronic kiosks and access through the Web.

Eighteen services of six departments were proposed to be made available. These cover electricity bills, water and sewage bills, property tax, registration of births, issuance of birth certificates, registration of deaths, issuance of death certificates, caste certificates, trade licence, issuance of learner's licence, issuance/ renewal of driving licence, and registration of certificates of new vehicles. Procedures of the transport department, details of building permits issued, market value assistance, change of address and transfer of ownership of non-transport vehicles were also to be made available through the system.

The Government of Andhra Pradesh set out to re-define citizen services through eSeva, by building on the TWINS project and extending the services to major towns, municipalities and other parts of the state.

The eSeva project sought to encompass the following:

- Integration of Central and state governments
- Integration of services
- Integration of G2C and B2C.

Forty-six eSeva centres have been established with 400 service counters spread across the twin cities of Hyderabad and Secunderabad, and Ranga Reddy district. Each of these service counters is equipped with an electronic queuing system. Operating from 8.00 am to 8.00 pm, on all working days and 9.00 am to 3.00 pm on holidays, these service centres serve as one-stop shops for over sixty-six G2C and B2C services incorporating online services of e-forms, e-filing and e-payments. Along with electronic payments over the Internet, payments through cash, cheque, demand draft and credit card are also accepted. No jurisdiction limits are imposed—any citizen in the twin cities can avail of the services at any of the service centres.

The services that are currently provided by eSeva are delineated below.

20.4.1 Payment of Utilities Bills

- Electricity bills
- Water and sewerage bills
- Telephone bills (BSNL and TATA Tele Services)
- Property tax
- Sales tax

20.4.2 Certificates

- Registration of births/ deaths
- Issue of birth/ death certificates

20.4.3 Labour Department

- Licence new registration
- Licence renewal

20.4.4 Permits/Licences

- Issue/ renewal of trade licences

20.4.5 Transport Department Services

- Change of address of a vehicle owner
- Transfer of ownership of a vehicle
- Issue of learners' licences
- Issue/ renewal of driving licences (non-transport vehicles)
- Registration of new vehicles

20.4.6 Reservation

- Reservation of APSRTC (Andhra Pradesh State Road Transport Corporation) bus tickets
- HMWSSB (Hyderabad Metropolitan Water Supply and Sewerage Board): Reservation of water tanker

20.4.7 Other Services at eSeva Centres

- Sale of passport application forms
- Receipt of passport applications
- Registration Department: Sale of non-judicial stamps

20.4.8 Internet Services

- Internet-enabled electronic payments
- Downloading of forms and Government Orders (GOs)
- Filing of applications on the Web

20.4.9 B2C Services

- Cell phone bill payments

20.4.10 Police Services

- Payment of Inquest/ *Panchanama* fees Rs 50
- Payment for First Information Report Rs 50
- Payment for Post Mortem Report Rs 50

Since August 25, 2001 when they were launched, more than twenty million transactions have been handled by eSeva. The ePayments service launched in 2001 has also processed more than 36,000 payment transactions. (These figures are as of December 2004.)



20.5 Government of Karnataka—Bhoomi

Under this e-governance project, the Government of Karnataka has computerised all 20 million land records of 6.7 million land owners in 176 *talukas* of the state.

Bhoomi is a comprehensive software which provides for printing of land records as and when required. It incorporates the process of online updation to ensure that the Records of Rights, Tenancy and Cultivation (RTC) provided to farmers are synchronised with time. Manual land records have been declared illegal in *talukas* where Bhoomi has been implemented. All mutations to the land records database are done on the computer itself so as to ensure that the data on computer remain consistent.

Users are authenticated through state-of-the-art bio-logon metrics system on the basis of fingerprints, ensuring that no impersonation is possible. The replacement of the password security system by the fingerprint authentication system ensures that databases are secure and that non-repudiation is in place.

The software also has the provision of scanning of original mutation orders of the revenue inspector (who is the authorised person to pass orders in the mutations in the field) and notices served on interested parties. Both documents are scanned to ensure not only that responsibility can be fixed on officials by virtue of the original documents signed by them, but also to ensure that interested parties do not claim in a court that they were not served with the notice before effecting the mutation.

The first land records kiosk was inaugurated in the town of Maddur in February 2001. Bangalore district's first computerised *taluka*, Bangalore (South), was inaugurated in July 2001.

The Bhoomi project includes the following components:

- The computer centres where mutation and updation are done are equipped with finger-print-based authentication mechanisms and provision of scanning of important documents
- At the land records kiosks, the farmers can collect a copy of their record by paying Rs 15. They can also lodge requests for mutation to their land records. Kiosks are fully funded by the State Government.

Farmers can see their land-related information on touch screen kiosks without anybody's intervention or help. They can quickly get their land records from kiosks and are protected from harassment and extortion. As against an earlier time delay of 3 to 30 days, they now get their records in less than two minutes. No overhead cost is incurred. No application is required to be submitted at the kiosk. The records are authentic and legible. The use of a biometrics-based authentication system for updation of records has freed farmers from the worry of probable manipulation of their records.

Applications for mutation to land records can be lodged at the computerised kiosks, their acknowledgement received, and progress monitored by using touch screen kiosks available at some Bhoomi centres. Farmers then get their updated land record in a fixed time frame without the need for approaching any

authority. As against an earlier time of 70–200 days, mutation now requires less than 35 days. Farmers can also get the official status report of their request for mutation to know the stage at which their request is pending. This status report helps them in enforcing their right of getting the record mutated in the prescribed time.

As far as administrators are concerned, the maintenance and updation of land records documents have become much easier. In manual system land records, updation could get delayed by as much as 1–2 years in some cases. Valuable land records data like various crops grown in a village or a sub-district, and the fertilisers and pesticide requirement in a season, provide support for development programmes of departments like agriculture, industries and planning. In the earlier system, this information became available to departments only after 2–3 years. It is now available almost immediately. Reports based on the type of soil, land holding size, and types of crops grown, are generated to aid in policy and decision making. Administrators are also able to ensure the accurate and timely preparation of annual records like land revenue, to monitor Government lands and to prevent encroachment.

Online connectivity also helps banks to effect better-informed planning for their farm credit-related activities. Banks are able to ensure that the revenue administration indicates the bank's charge on the land records of such farmers who have availed of crop loans. Farm credit to farmers in less than five days can also be assured as against 25–30 days in the manual system



References

1. Electronic Governance Division—Department of Information Technology—<http://egov.mit.gov.in>
2. Indian Railways—www.irctc.co.in
3. eSeva project—www.esevaonline.com
4. Bhoomi project—<http://www.revdept-0.1.kar.nic.in/Bhoomi/>

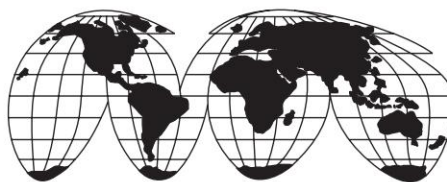
PART VIII

Appendices

1. UN/ EDIFACT Message Directory
2. Sample UN/ EDIFACT Mapping
3. UNCITRAL Model Law on E-Commerce
4. Information Technology Act, 2000
5. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
6. Public Key Infrastructure (PKI) Standards
7. European Union Directive on a Community Framework for Electronic Signatures
8. OECD Guidelines for Cryptography Policy issued by Organisation for Economic Co-operation and Development
9. European Union Convention on Cyber Crimes
10. Indian Computer Emergency Response Team (CERT-In)—profile of objectives, functions, role and activities (public brochure released on inauguration of CERT-In)
11. E-Commerce sites of interest
12. E-Governance sites of interest

The UN/ EDIFACT Message Directory contains the list of messages as contained in the UN/EDIFACT Directory D97B along with UN/EDIFACT Control Segments. Sample UN/ EDIFACT Mapping describes the mapping of a document onto an EDIFACT message. A sample Purchase Order is taken and the process of mapping to an UN/EDIFACT message is presented. UNCITRAL Model Law on E-Commerce, which covers the legal aspects of Electronic Data Interchange and e-commerce, is included. The Indian Information Technology Act, 2000, which provides legal recognition to electronic transactions and digital signatures, promotes trust in the

e-commerce and e-governance. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 provides a technology neutral legal framework for the use of electronic signatures. Standards to be followed for digital signatures using Public Key Cryptography are presented in Public Key Infrastructure (PKI) Standards. The framework proposed by the European Union for facilitation and legal recognition of electronic signatures is presented in the European Union Directive on a Community Framework for Electronic Signatures. The OECD Guidelines for Cryptography Policy issued by Organisation for Economic Co-operation and Development includes guidelines related to adoption of cryptographic methods & standards, implementation of privacy & data protection and encryption related legal & liability issues. European Union Convention on Cyber Crimes seeks to control cyber crimes through creation of a uniform body of laws by participating nations. The profile of objectives, functions, role and activities of the Indian Computer Emergency Response Team (CERT-In) are presented in the public brochure released on its inauguration. Some e-commerce sites of interest and e-governance sites of interest are listed in the last two appendices.



Appendix 1

UN/EDIFACT* Message Directory



A1.1 Message Type Directory as in D.97B (<http://www.unece.org/>)

<i>Code</i>	<i>Name</i>
APERAK	Application error and acknowledgement message
AUTHOR	Authorization message
BANSTA	Banking status message
BAPLIE	Bayplan/ stowage plan occupied and empty locations message
BAPLTE	Bayplan/ stowage plan total numbers message
BOPBNK	Bank transactions and portfolio transactions report message
BOPCUS	Balance of payment customer transaction report message
BOPDIR	Direct balance of payment declaration message
BOPINF	Balance of payment information from customer message
CALINF	Vessel call information message
CASINT	Request for legal administration action in civil proceedings message

(Contd)

* United Nations Electronic Data Interchange for Administration, Commerce and Transport.

CASRES	Legal administration response in civil proceedings message
COARRI	Container discharge/ loading report message
CODECO	Container gate-in/ gate-out report message
CODENO	Permit expiration/ clearance ready notice message
COEDOR	Container stock report message
COHAOR	Container special handling order message
COLREQ	Request for a documentary collection message
COMDIS	Commercial dispute message
CONAPW	Advice on pending works message
CONDPV	Direct payment valuation message
CONDRA	Drawing administration message
CONDRO	Drawing organisation message
CONEST	Establishment of contract message
CONITT	Invitation to tender message
CONPVA	Payment valuation message
CONQVA	Quantity valuation message
CONRPW	Response of pending works message
CONTEN	Tender message
CONWQD	Work item quantity determination message
COPARN	Container announcement message
COPINO	Container pre-notification message
COPRAR	Container discharge/ loading order message
COREOR	Container release order message
COSTCO	Container stuffing/ stripping confirmation message
COSTOR	Container stuffing/ stripping order message
CREADV	Credit advice message
CREEXT	Extended credit advice message
CREMUL	Multiple credit advice message
CUSCAR	Customs cargo report message
CUSDEC	Customs declaration message
CUSEXP	Customs express consignment declaration message
CUSPED	Periodic customs declaration message
CUSREP	Customs conveyance report message
CUSRES	Customs response message

(Contd)

DEBADV	Debit advice message
DEBMUL	Multiple debit advice message
DELFOR	Delivery schedule message
DELJIT	Delivery just in time message
DESADV	Despatch advice message
DESTIM	Equipment damage and repair estimate message
DGRECA	Dangerous goods recapitulation message
DIRDEB	Direct debit message
DIRDEF	Directory definition message
DOCADV	Documentary credit advice message
DOCAMA	Advice of an amendment of a documentary credit message
DOCAMI	Documentary credit amendment information message
DOCAMR	Request for an amendment of a documentary credit message
DOCAPP	Documentary credit application message
DOCARE	Response to an amendment of a documentary credit message
DOCINF	Documentary credit issuance information message
FINCAN	Financial cancellation message
FINSTA	Financial statement of an account message
GENRAL	General purpose message
GESMES	Generic statistical message
HANMOV	Cargo/ goods handling and movement message
IFCSUM	Forwarding and consolidation summary message
IFTCCA	Forwarding and transport shipment charge calculation message
IFTDGN	Dangerous goods notification message
IFTFCC	International transport freight costs and other charges message
IFTIAG	Dangerous cargo list message
IFTMAN	Arrival notice message
IFTMBC	Booking confirmation message
IFTMBF	Firm booking message

(Contd)

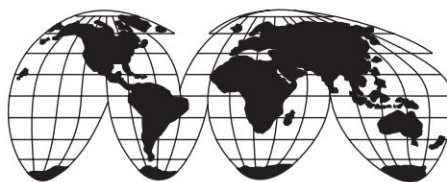
IFTMBP	Provisional booking message
IFTMCS	Instruction contract status message
IFTMIN	Instruction message
IFTRIN	Forwarding and transport rate information message
IFTSAI	Forwarding and transport schedule and availability information message
IFTSTA	International multimodal status report message
IFTSTQ	International multimodal status request message
INFENT	Enterprise accounting information message
INSPRE	Insurance premium message
INVOIC	Invoice message
INVRPT	Inventory report message
ITRRPT	Intransit report detail message
JAPRES	Job application result message
JINFDE	Job information demand message
JOBAPP	Job application proposal message
JOBCON	Job order confirmation message
JOBMOD	Job order modification message
JOBOFF	Job order message
LREACT	Life reinsurance activity message
MEDPID	Person identification message
MEDREQ	Medical service request message
MEDRPT	Medical service report message
MEDRUC	Medical resource usage and cost message
MEQPOS	Means of transport and equipment position message
MOVINS	Stowage instruction message
MSCONS	Metered services consumption report message
ORDCHG	Purchase order change request message
ORDERS	Purchase order message
ORDRSP	Purchase order response message
OSTENQ	Order status enquiry message
OSTRPT	Order status report message
PARTIN	Party information message

(Contd)

PAXLST	Passenger list message
PAYDUC	Payroll deductions advice message
PAYEXT	Extended payment order message
PAYMUL	Multiple payment order message
PAYORD	Payment order message
PRICAT	Price/ sales catalogue message
PRIHIS	Pricing history message
PRODAT	Product data message
PRODEX	Product exchange reconciliation message
PROINQ	Product inquiry message
PRPAID	Insurance premium payment message
QUALITY	Quality data message
QUOTES	Quote message
RDRMES	Raw data reporting message
REBORD	Reinsurance bordereau message
RECADV	Receiving advice message
RECALC	Reinsurance calculation message
RECECO	Credit risk cover message
RECLAM	Reinsurance claims message
REMADV	Remittance advice message
REPREM	Reinsurance premium message
REQDOC	Request for document message
REQOTE	Request for quote message
RESETT	Reinsurance settlement message
RESMSG	Reservation message
RETACC	Reinsurance technical account message
RETANN	Announcement for returns message
RETINS	Instruction for returns message
SAFHAZ	Safety and hazard data message
SANCRT	International movement of goods governmental regulatory message
SLSFCT	Sales forecast message
SLSRPT	Sales data report message
SSIMOD	Modification of identity details message
SSRECH	Worker's insurance history message
SSREGW	Notification of registration of a worker message

(Contd)

STATAC	Statement of account message
SUPCOT	Superannuation contributions advice message
SUPMAN	Superannuation maintenance message
SUPRES	Supplier response message
TANSTA	Tank status report message
VATDEC	Value added tax message
VESDEP	Vessel departure message
WASDIS	Waste disposal information message
WKGRDC	Work grant decision message
WKGRRE	Work grant request message



Appendix 2

Sample UN/EDIFACT Mapping

When mapping a business document to an UN/ EDIFACT Standard message (UNSM), the UNSMs for common documents such as Invoices, Purchase Orders, etc. are straightforward to identify. In other cases a study of the directory of UNSMs will be required to pinpoint the standard message which provides a 'best fit' for the business document. Here the objective is to describe what happens when a typical business document such as a Purchase Order is mapped to the UN/ EDIFACT standard message ORDERS.

Sample Mapping of a Purchase Order to the UN/EDIFACT Standard Message ORDERS

Purchase Order date :	25 December 1997	Ref: ABC 123	
Buyer :	ABC Company Ltd. (8901234567890) 5 Main Street, New Industrial Area, New Delhi 110 076		
Supplier :	XYZ Company Ltd. (8906543211234) 21 High Street, Super Estates, Calcutta, West Bengal 700 096		
Item No.	Description	QTY	Unit Price
ITM 111	Handbags	100	Rs 500
Total			Rs 50, 000

➞ **Fig. A2.1** *Sample purchase order*


```

UNH+MSG 00001+ ORDERS:D97B:UN:EAN007'
BGM+220+ABC 123'
DTM+137+19971225:102'
NAD+BY+8901234567890::9'
NAD+SU+8906543211234::9'

LIN+1+++4000862141404:EN'
PIA+1++ITM 111:SA'
IMD+C++TU+::9:Handbags'
QTY+21:100:PC E'
PRI+AAA+500:CA:PRP:1:PC E'
MOA+203:50000'
UNT+13+MSG 00001'

```

 **Fig. A2.2** *Corresponding UN/EDIFACT purchase order Message—ORDERS*

Figure A2.1 shows a sample purchase order from a company called ABC Company Ltd. to a company called XYZ Company Ltd. for the supply of 100 numbers of handbags at a unit price of Rs 500 amounting to a total cost of Rs 50,000. The segment table representation of the United Nations Standard Message ORDERS for Purchase Orders is given Fig. A2.3. Figure A2.2 shows the contents of the UN/ EDIFACT message—ORDERS—which has been created by “mapping” the ordering information from the original Purchase Order. The actual method of mapping the fields of the sample Purchase Order onto the standard segments and data elements will vary between vendors of EDI mapper/ translators. The objective of this section is to explain the representation of data when translated from the ‘human-readable’ form to the UN/ EDIFACT standard format.

The contents of the UN/ EDIFACT message normally appear as a continuous string of text. Here, however, it has been presented separately in the interest of readability.

Each line of information is called a segment identified at its beginning by a 3-character code. A segment contains data elements and codes. Delimiters such as + and : are used to separate data elements and codes. Details of the contents as they appear in Fig. A2.2 are represented as follows.

Header Section

When any UN/ EDIFACT message is being created, it is mandatory to have a Message Header segment which is identified by the UNH segment tag.

Message Header	– UNH+MSG00001+ORDERS: D97B: UN:EAN007'
MSG 00001	– Unique Message Reference Number assigned by the sender
ORDERS	– Message Type which is interpreted by the receiving system and used for identifying and routing to the processing application, here Order Entry
D93A	– Release/ current version Number—Draft Directory for 1997, Ver B
UN	– Controlling Agency for the message type
EAN007	– Code assigned by agency responsible for design of the message type
Beginning of Message	– BGM+220+ABC123'
220	– Code for the Document/ message name, in this case, Order
ABC 123	– Document/ message number.
Date and Time	– DTM+137+19971225:102'
137	– Code indicating that the date is the Ordering Date
19971225	– Representation of 25 December 1997
102	– Code indicating that the date format is YYYYMMDD
Name and Address	– NAD+BY+8901234567890::9'
BY	– Code indicating that this segment contains Name & Address of the buyer
8901234567890	– Buyer Code
9	– Code identifying agency responsible for Buyer code

Name and Address	– NAD+SU+8906543211234::9'
SU	– Code indicating that Name & Address is of the supplier
8906543211234	– Supplier Code
9	– Code identifying agency responsible for supplier code

Detail Section

Line Item Segment	– LIN+1++4000862141404:EN'
1	– Serial number for the line item being considered
4000862141404	– Article number assigned to the product by the International Article Numbering Association (EAN)
EN	– the International Article Numbering Association (EAN)

Additional Product Id	– PIA+1+ITM111:SA'
1	– Code to indicate additional identification of product
ITM111	– Item number of the product
SA	– Code indicating that the above number is the suppliers article number

Item Description	– IMD+C++TU+::9: Handbags'
C	– Code indicating that the format of the description is from the industry code list
TU	– Industry code
9	– Code of the agency responsible for the code list
Handbags	– Item description

Quantity	– QTY+21:100:PCE'
21	– Code indicating that the quantity mentioned is the ordered quantity
100	– Quantity

PCE	– Code indicating that the unit of measurement in which the quantity is expressed is pieces, represented by PCE
<i>Price Details</i>	– PRI+AAA+500:CA:PRP:1:PCE'
AAA	– Mutually defined between trading partners
500	– Actual price
CA	– Code indicating that the type of price is a catalogue price
PRP	– Code identifying pricing specification as promotional price
1	– Basis on which the unit price/ rate applies
PCE	– Code indicating that the unit of measurement in which the quantity is expressed is pieces, represented by PCE
<i>Monetary Amount</i>	– MOA+203:50000'
203	– Code indicating that the amount is a line item amount
50000	– Actual Monetary Amount
<i>Summary Section</i>	
<i>Message Trailer</i>	– UNT+13+MSG00001'
13	– Total number of segments in this message
MSG00001	– Unique Message Reference Number assigned by the sender, as appearing in the corresponding message header

Pos	Tag Name	S	R
Header Section			
0010	UNH Message header	M	1
0020	BGM Beginning of message	M	1
0030	DTM Date/ time/ period	M	35
0040	PAI Payment instructions	C	1
0050	ALI Additional information	C	5
0060	IMD Item description	C	999
0070	FTX Free text	C	99
0080	——— Segment group 1 ———	C	9999
0090	RFF Reference	M	1
0100	DTM Date/ time/ period	C	5
0110	——— Segment group 2 ———	C	99
0120	NAD Name and address	M	1
0130	LOC Place/ location identification	C	25
0140	FII Financial institution information	C	5
0150	——— Segment group 3 ———	C	99
0160	RFF Reference	M	1
0170	DTM Date/ time/ period	C	5
0180	——— Segment group 4 ———	C	5
0190	DOC Document/ message details	M	1
0200	DTM Date/ time/ period	C	5
0210	——— Segment group 5 ———	C	5
0220	CTA Contact information	M	1
0230	COM Communication contact	C	5
0240	——— Segment group 6 ———	C	5
0250	TAX Duty/ tax/ fee details	M	1
0260	MOA Monetary amount	C	1
0270	LOC Place/ location identification	C	5
0280	——— Segment group 7 ———	C	5
0290	CUX Currencies	M	1
0300	PCD Percentage details	C	5
0310	DTM Date/ time/ period	C	5

(Contd)


Fig. A2.3

Fig. A2.3 (Contd)

0320	Segment group 8	C	10	
0330	PAT Payment terms basis	M	1	
0340	DTM Date/ time/ period	C	5	
0350	PCD Percentage details	C	1	
0360	Segment group 9	C	9999	
0370	MOA Monetary amount	M	1	
0380	GIR Related identification numbers	C	9	
0390	Segment group 10	C	10	
0400	TDT Details of transport	M	1	
0410	Segment group 11	C	10	
0420	LOC Place/ location identification	M	1	
0430	DTM Date/ time/ period	C	5	
0440	Segment group 12	C	5	
0450	TOD Terms of delivery or transport	M	1	
0460	LOC Place/ location identification	C	2	
0470*	Segment group 13	C	99	
0480	PAC Package	M	1	
0490	MEA Measurements	C	5	
0500	Segment group 14	C	5	
0510	PCI Package identification	M	1	
0520	RFF Reference	C	1	
0530	DTM Date/ time/ period	C	5	
0540	GIN Goods identity number	C	10	
0550	Segment group 15	C	10	
0560	EQD Equipment details	M	1	
0570	HAN Handling instructions	C	5	
0580	MEA Measurements	C	5	
0590	FTX Free text	C	5	
0600	Segment group 16	C	10	
0610	SCC Scheduling conditions	M	1	
0620	FTX Free text	C	5	
0630	RFF Reference	C	5	
0640	Segment group 17	C	10	
0650	QTY Quantity	M	1	
0660	DTM Date/ time/ period	C	5	

(Contd)

 **Fig. A2.3**

Fig. A2.3 (Contd)

0670	Segment group 18	C	25	
0680	APR Additional price information	M	1	
0690	DTM Date/ Time/ period	C	5	
0700	RNG Range details	C	1	
0710	Segment group 19	C	99	
0720	ALC Allowance or charge	M	1	
0730	ALI Additional information	C	5	
0740	DTM Date/ time/ period	C	5	
0750	Segment group 20	C	1	
0760	QTY Quantity	M	1	
0770	RNG Range details	C	1	
0780	Segment group 21	C	1	
0790	PCD Percentage details	M	1	
0800	RNG Range details	C	1	
0810	Segment group 22	C	2	
0820	MOA Monetary amount	M	1	
0830	RNG Range details	C	1	
0840	Segment group 23	C	1	
0850	RTE Rate details	M	1	
0860	RNG Range details	C	1	
0870	Segment group 24	C	5	
0880	TAX Duty/ tax/ fee details	M	1	
0890	MOA Monetary amount	C	1	
0900	Segment group 25	C	999	
0910	RCS Requirements and conditions	M	1	
0920	RFF Reference	C	5	
0930	DTM Date/ time/ period	C	5	
0940	FTX Free text	C	99999	
0950	Segment group 26	C	999	
0960	DGS Dangerous goods	M	1	
0970	FTX Free text	C	5	
0980	Segment group 27	C	99	
0990	CTA Contact information	M	1	
1000	COM Communication contact	C	5	

Fig. A2.3

(Contd)

Fig. A2.3 (*Contd*)**DETAIL SECTION**

1010	——— Segment group 28 ———	C	200000	
1020	LIN Line item	M	1	
1030	PIA Additional product id	C	25	
1040	IMD Item description	C	99	
1050	MEA Measurements	C	99	
1060	QTY Quantity	C	99	
1070	PCD Percentage details	C	5	
1080	ALI Additional information	C	5	
1090	DTM Date/ time/ period	C	35	
1100	MOA Monetary amount	C	10	
1110	GIN Goods identity number	C	1000	
1120	GIR Related identification numbers	C	1000	
1130	QVR Quantity variances	C	1	
1140	DOC Document/ message details	C	99	
1150	PAI Payment instructions	C	1	
1160	FTX Free text	C	99	
1170	——— Segment group 29 ———	C	999	
1180	CCI Characteristic/ class id	M	1	
1190	CAV Characteristic value	C	10	
1200	MEA Measurements	C	10	
1210	——— Segment group 30 ———	C	10	
1220	PAT Payment terms basis	M	1	
1230	DTM Date/ time/ period	C	5	
1240	PCD Percentage details	C	1	
1250	——— Segment group 31 ———	C	9999	
1260	MOA Monetary amount	M	1	
1270	GIR Related identification numbers	C	9	
1280	——— Segment group 32 ———	C	25	
1290	PRI Price details	M	1	
1300	CUX Currencies	C	1	
1310	APR Additional price information	C	1	
1320	RNG Range details	C	1	
1330	DTM Date/ time/ period	C	5	
1340	——— Segment group 33 ———	C	9999	
1350	RFF Reference	M	1	
1360	DTM Date/ time/ period	C	5	

Fig. A2.3*(Contd)*

Fig. A2.3 (Contd)

1370*	Segment group 34	C	99	
1380	PAC Package	M	1	
1390	MEA Measurements	C	5	
1400	QTY Quantity	C	5	
1410	DTM Date/ time/ period	C	5	
1420	Segment group 35	C	1	
1430	RFF Reference	M	1	
1440	DTM Date/ time/ period	C	5	
1450	Segment group 36	C	5	
1460	PCI Package identification	M	1	
1470	RFF Reference	C	1	
1480	DTM Date/ time/ period	C	5	
1490	GIN goods identity number	C	10	
1500	Segment group 37	C	9999	
1510	LOC Place/ location identification	M	1	
1520	QTY Quantity	C	1	
1530	PCD Percentage details	C	1	
1540	DTM Date/ time/ period	C	5	
1550	Segment group 38	C	10	
1560	TAX Duty/ tax/ fee details	M	1	
1570	MOA Monetary amount	C	1	
1580	LOC Place/ location identification	C	5	
1590	Segment group 39	C	999	
1600	NAD Name and address	M	1	
1610	LOC Place/ location identification	C	5	
1620	Segment group 40	C	99	
1630	RFF Reference	M	1	
1640	DTM Date/ time/ period	C	5	
1650	Segment group 41	C	5	
1660	DOC Document/ message details	M	1	
1670	DTM Date/ time/ period	C	5	
1680	Segment group 42	C	5	
1690	CTA Contact information	M	1	
1700	COM Communication contact	C	5	

(Contd)

 **Fig. A2.3**

Fig. A2.3 (Contd)

1710	Segment group 43	C	99	
1720	ALC Allowance or charge	M	1	
1730	ALI Additional information	C	5	
1740	DTM Date/ time/ period	C	5	
1750	Segment group 44	C	1	
1760	QTY Quantity	M	1	
1770	RNG Range details	C	1	
1780	Segment group 45	C	1	
1790	PCD Percentage details	M	1	
1800	RNG Range details	C	1	
1810	Segment group 46	C	2	
1820	MOA Monetary amount	M	1	
1830	RNG Range details	C	1	
1840	Segment group 47	C	1	
1850	RTE Rate details	M	1	
1860	RNG Range details	C	1	
1870	Segment group 48	C	5	
1880	TAX Duty/ tax/ fee details	M	1	
1890	MOA Monetary amount	C	1	
1900	Segment group 49	C	10	
1910	TDT Details of transport	M	1	
1920	Segment group 50	C	10	
1930	LOC Place/ location identification	M	1	
1940	DTM Date/ time/ period	C	5	
1950	Segment group 51	C	5	
1960	TOD Terms of delivery or transport	M	1	
1970	LOC Place/ location identification	C	2	
1980	Segment group 52	C	10	
1990	EQD Equipment details	M	1	
2000	HAN Handling instructions	C	5	
2010	MEA Measurements	C	5	
2020	FTX Free text	C	5	
2030	Segment group 53	C	100	
2040	SCC Scheduling conditions	M	1	
2050	FTX Free text	C	5	
2060	RFF Reference	C	5	

Fig. A2.3*(Contd)*

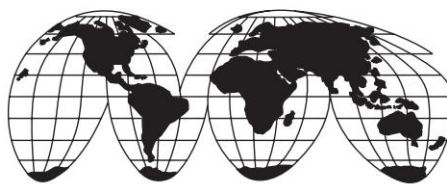
Fig. A2.3 (*Contd*)

2070	Segment group 54	C	10	
2080	QTY Quantity	M	1	
2090	DTM Date/ time/ period	C	5	
2100	Segment group 55	C	999	
2110	RCS REquirements and conditions	M	1	
2120	RFF Reference	C	5	
2130	DTM Date/ time/ period	C	5	
2140	FTX Free text	C	99999	
2150	Segment group 56	C	10	
2160	STG Stages	M	1	
2170	Segment group 57	C	3	
2180	QTY quantity	M	1	
2190	MOA Monetary amount	C	1	
2200	Segment group 58	C	999	
2210	DGS Dangerous goods	M	1	
2220	FTX Free text	C	5	
2230	Segment group 59	C	99	
2240	CTA Contact information	M	1	
2250	COM Communication contact	C	5	

Summary Section

2260	UNS Section control	M	1	
2270	MOA Monetary amount	C	12	
2280	CNT Control total	C	10	
2290	Segment group 60	C	10	
2300	ALC Allowance or charge	M	1	
2310	ALI Additional information	C	1	
2320	MOA Monetary amount	M	2	
2330	UNT Message trailer	M	1	

➡ **Fig. A2.3** *Message structure of UN/EDIFACT UNSM (D.97B) ORDERS for Purchase Order in segment table representation*



Appendix 3

United Nations Commission on International Trade Law (UNCITRAL)

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment

1996

with additional Article 5 bis as adopted in 1998

CONTENTS

GENERAL ASSEMBLY RESOLUTION 51/162 OF 16 DECEMBER 1996 UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

Part One. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application

Article 2. Definitions

Article 3. Interpretation

Article 4. Variation by agreement

Chapter II. Application of legal requirements to data messages

- Article 5. Legal recognition of data messages
- Article 5 bis. Incorporation by reference
- Article 6. Writing
- Article 7. Signature
- Article 8. Original
- Article 9. Admissibility and evidential weight of data messages
- Article 10. Retention of data messages

Chapter III. Communication of data messages

- Article 11. Formation and validity of contracts
- Article 12. Recognition by parties of data messages
- Article 13. Attribution of data messages
- Article 14. Acknowledgement of receipt
- Article 15. Time and place of dispatch and receipt of data messages

Part Two. Electronic commerce in specific areas

Chapter I. Carriage of goods

- Article 16. Actions related to contracts of carriage of goods
- Article 17. Transport documents

Paragraphs

GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE	1–150
Purpose of this Guide	1
<i>I. Introduction to the Model Law</i>	2–23
A. Objectives	2–6
B. Scope	7–10
C. Structure	11–12
D. A “framework” law to be supplemented by technical regulations	13–14
E. The “functional-equivalent” approach	15–18

F. Default rules and mandatory law	19–21
G. Assistance from UNCITRAL secretariat	22–23
<i>II. Article-by-article remarks</i>	24–122
Part One. Electronic commerce in general	24–107
<i>Chapter I. General provisions</i>	24–45
Article 1. Sphere of application	24–29
Article 2. Definitions	30–40
Article 3. Interpretation	41–43
Article 4. Variation by agreement	44–45
<i>Chapter II. Application of legal requirements to data messages</i>	46–75
Article 5. Legal recognition of data messages	46
Article 5 bis. Incorporation by reference	46–1–46–7
Article 6. Writing	47–52
Article 7. Signature	53–61
Article 8. Original	62–69
Article 9. Admissibility and evidential weight of data messages	70–71
Article 10. Retention of data messages	72–75
<i>Chapter III. Communication of data messages</i>	76–107
Article 11. Formation and validity of contracts	76–80
Article 12. Recognition by parties of data messages	81–82
Article 13. Attribution of data messages	83–92
Article 14. Acknowledgement of receipt	93–99
Article 15. Time and place of dispatch and receipt of data messages	100–107
<i>Part Two. Electronic commerce in specific areas</i>	108–122
<i>Chapter I. Carriage of goods</i>	110–122
Article 16. Actions related to contracts of carriage of goods	111–112
Article 17. Transport documents	113–122
<i>III. History and background of the Model Law</i>	123–150

Resolution Adopted by the General Assembly

[on the report of the Sixth Committee (A/51/628)]

51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law

The General Assembly,

Recalling its resolution 2205 (XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law, with a mandate to further the progressive harmonization and unification of the law of international trade and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade,

Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information,

Recalling the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session, in 1985,¹ and paragraph 5(b) of General Assembly resolution 40/71 of 11 December 1985, in which the Assembly called upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission, so as to ensure legal security in the context of the widest possible use of automated data processing in international trade,

Convinced that the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations,

Noting that the Model Law on Electronic Commerce was adopted by the Commission at its twenty-ninth session after

consideration of the observations of Governments and interested organizations,

Believing that the adoption of the Model Law on Electronic Commerce by the Commission will assist all States significantly in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists,

1. *Expresses* its appreciation to the United Nations Commission on International Trade Law for completing and adopting the Model Law on Electronic Commerce contained in the annex to the present resolution and for preparing the Guide to Enactment of the Model Law;
2. *Recommends* that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;
3. *Recommends* also that all efforts be made to ensure that the Model Law, together with the Guide, become generally known and available.

*85th plenary meeting
16 December 1996*

UNCITRAL Model Law on Electronic Commerce

[*Original: Arabic, Chinese, English, French, Russian, Spanish*]

Part One. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application*

*The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

“This Law applies to a data message as defined in paragraph (1) of Article 2 where the data message relates to international commerce.”

This Law* applies to any kind of information in the form of a data message used in the context** of commercial*** activities.

Article 2. Definitions

For the purposes of this Law:

- (a) “Data message” means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;
- (b) “Electronic data interchange (EDI)” means the electronic transfer from computer to computer of information using an agreed standard to structure the information;
- (c) “Originator” of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;
- (d) “Addressee” of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;
- (e) “Intermediary”, with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

*This Law does not override any rule of law intended for the protection of consumers.

**The Commission suggests the following text for States that might wish to extend the applicability of this Law: “This Law applies to any kind of information in the form of a data message, except in the following situations: [...]”

***The term “commercial” should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road

- (f) “Information system” means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

- (1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.
- (2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

- (1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.
- (2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in Chapter II.

Chapter II. Application of legal requirements to data messages

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 5 bis. Incorporation by reference

(as adopted by the Commission at its thirty-first session, in June 1998)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Article 6. Writing

- (1) Where the law requires information to be in writing, that requirement is met by a data message if the information

contained therein is accessible so as to be usable for subsequent reference.

- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.
- (3) The provisions of this article do not apply to the following: [...].

Article 7. Signature

- (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
 - (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
 - (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
- (3) The provisions of this article do not apply to the following: [...].

Article 8. Original

- (1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
 - (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
 - (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.
- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply

provides consequences for the information not being presented or retained in its original form.

- (3) For the purposes of subparagraph (a) of paragraph (1):
 - (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
 - (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.
- (4) The provisions of this article do not apply to the following: [...].

Article 9. Admissibility and evidential weight of data messages

- (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
 - (a) on the sole ground that it is a data message; or,
 - (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
- (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of data messages

- (1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

- (a) the information contained therein is accessible so as to be usable for subsequent reference; and
 - (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
 - (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.
- (2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.
- (3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Chapter III. Communication of data messages

Article 11. Formation and validity of contracts

- (1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.
- (2) The provisions of this article do not apply to the following: [...].

Article 12. Recognition by parties of data messages

- (1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

- (2) The provisions of this article do not apply to the following:
[...].

Article 13. Attribution of data messages

- (1) A data message is that of the originator if it was sent by the originator itself.
- (2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
 - (a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
 - (b) by an information system programmed by, or on behalf of, the originator to operate automatically.
- (3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
 - (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
 - (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.
- (4) Paragraph (3) does not apply:
 - (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
 - (b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.
- (5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator

and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

- (6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

- (1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.
- (2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by
 - (a) any communication by the addressee, automated or otherwise, or
 - (b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.
- (3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.
- (4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator

- (a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and
 - (b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.
- (5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.
- (6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.
- (7) Except insofar as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages

- (1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.
- (2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
 - (a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
 - (i) at the time when the data message enters the designated information system; or

- (ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;
- (b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.
- (3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).
- (4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:
 - (a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
 - (b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.
- (5) The provisions of this article do not apply to the following:
[...].

Part Two. Electronic commerce in specific areas

Chapter I. Carriage of goods

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

- (a) (i) furnishing the marks, number, quantity or weight of goods;

- (ii) stating or declaring the nature or value of goods;
 - (iii) issuing a receipt for goods;
 - (iv) confirming that goods have been loaded;
- (b) (i) notifying a person of terms and conditions of the contract;
- (ii) giving instructions to a carrier;
- (c) (i) claiming delivery of goods;
- (ii) authorizing release of goods;
 - (iii) giving notice of loss of, or damage to, goods;
- (d) giving any other notice or statement in connection with the performance of the contract;
- (e) undertaking to deliver goods to a named person or a person authorized to claim delivery;
- (f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;
- (g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

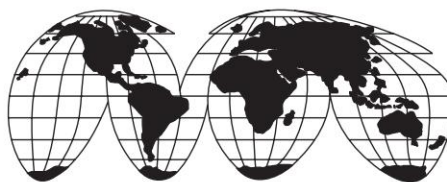
- (1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.
- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.
- (3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

- (4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.
- (5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of Article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.
- (6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.
- (7) The provisions of this article do not apply to the following: [...].

UNCITRAL

[http:// www.uncitral.org/ english/ texts/ electcom/ ml-ecomm.htm](http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm)

* * * * *



Appendix 4

The Information Technology Act, 2000

The Gazette of India

EXTRAORDINARY

PART II—Section 1

PUBLISHED BY AUTHORITY

**No. 27 NEW DELHI, FRIDAY, JUNE 9, 2000/
JYAISTHA 19, 1922**

Separate paging is given to this Part in order
that it may be filed as a separate compilation.

**MINISTRY OF LAW, JUSTICE AND
COMPANY AFFAIRS
(Legislative Department)**

*New Delhi, the 9th June, 2000/Jyaistha 19, 1922
(Saka)*

The following Act of Parliament received the
assent of the President on the 9th June, 2000,
and is hereby published for general
information:—

THE INFORMATION TECHNOLOGY
ACT, 2000

(No. 21 OF 2000)

[9th June, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/ RES/ 51/ 162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first
Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

1. (1) This Act may be called the Information Technology Act, 2000. Short title, extent, commencement and application.
- (2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.
- (3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.
- (4) Nothing in this Act shall apply to—
 - (a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881; 26 of 1881.
 - (b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882; 7 of 1882.
 - (c) a trust as defined in section 3 of the Indian Trusts Act, 1882; 2 of 1882.
 - (d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called; 39 of 1925.
 - (e) any contract for the sale or conveyance of immovable

property or any interest in such property;

- (f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Definitions 2. (1) In this Act, unless the context otherwise requires,—

- (a) “access” with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
- (b) “addressee” means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
- (c) “adjudicating officer” means an adjudicating officer appointed under sub-section (1) of section 46;
- (d) “affixing digital signature” with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;
- (e) “appropriate Government” means as respects any matter,—

- (i) enumerated in List II of the Seventh Schedule to the Constitution;
- (ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;
- (f) “asymmetric crypto system” means a system of a secure key-pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
- (g) “Certifying Authority” means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;
- (h) “certification practice statement” means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;
- (i) “computer” means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are

- connected or related to the computer in a computer system or computer network;
- (j) “computer network” means the interconnection of one or more computers through—
- (i) the use of satellite, microwave, terrestrial line or other communication media; and
 - (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;
- (k) “computer resource” means computer, computer system, computer network, data, computer data base or software;
- (l) “computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
- (m) “Controller” means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

- (n) “Cyber Appellate Tribunal” means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;
- (o) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
- (p) “digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
- (q) “Digital Signature Certificate” means a Digital Signature Certificate issued under sub-section (4) of section 35;
- (r) “electronic form” with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro-film, computer generated micro-fiche or similar device;

- (s) “Electronic Gazette” means the Official Gazette published in the electronic form;
- (t) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
- (u) “function”, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
- (v) “information” includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;
- (w) “intermediary” with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;
- (x) “key pair”, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
- (y) “law” includes any Act of Parliament or of a State Legislature,

Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

- (z) "licence" means a licence granted to a Certifying Authority under section 24;
- (za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
- (zb) "prescribed" means prescribed by rules made under this Act;
- (zc) "private key" means the key of a key pair used to create a digital signature;
- (zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
- (ze) "secure system" means computer hardware, software, and procedure that—
 - (a) are reasonably secure from unauthorised access and misuse;

- (b) provide a reasonable level of reliability and correct operation;
 - (c) are reasonably suited to performing the intended functions; and
 - (d) adhere to generally accepted security procedures;
 - (zf) “security procedure” means the security procedure prescribed under section 16 by the Central Government;
 - (zg) “subscriber” means a person in whose name the Digital Signature Certificate is issued;
 - (zh) “verify” in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—
 - (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
 - (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.
- (2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a

reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

DIGITAL SIGNATURE

3. (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

Authen-
tication of
electronic

- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation—For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
 - (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.

- (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

CHAPTER III

ELECTRONIC GOVERNANCE

4. Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—
- (a) rendered or made available in an electronic form; and
 - (b) accessible so as to be usable for a subsequent reference.
5. Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.
- Explanation*—For the purposes of this section, “signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression “signature” shall be construed accordingly.

Legal
recognition
of digital
signatures.

Legal
recognition
of
electronic
records.

6. (1) Where any law provides for—
- (a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
 - (b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;
 - (c) the receipt or payment of money in a particular manner;
- then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.
- (2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe—
- (a) the manner and format in which such electronic records shall be filed, created or issued;
 - (b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).
7. (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such

Use of
electronic
records
and digital
signatures
in
Government
and its
agencies.

Retention
of
electronic
records

documents, records or information are retained in the electronic form, if—

- (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
- (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
- (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Publication
of rule,
regulation,
etc., in
Electronic
Gazette.

- 8. Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is

published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

Sections 6,
7 and 8 not
to confer
right to
insist
document
should be
accepted in
electronic
form.

9. Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Power to
make rules
by Central
Government
in respect
of digital
signature.

10. The Central Government may, for the purposes of this Act, by rules, prescribe—
(a) the type of digital signature;
(b) the manner and format in which the digital signature shall be affixed;
(c) the manner or procedure which facilitates identification of the person affixing the digital signature;
(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(e) any other matter which is necessary to give legal effect to digital signatures.

CHAPTER IV
ATTRIBUTION, ACKNOWLEDGMENT
AND DESPATCH OF ELECTRONIC
RECORDS

Attribution
of
electronic
records.

11. An electronic record shall be attributed to the originator—
- (a) if it was sent by the originator himself;
 - (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
 - (c) by an information system programmed by or on behalf of the originator to operate automatically.

Acknow-
ledgement
of receipt

12. (1) Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—
- (a) any communication by the addressee, automated or otherwise; or
 - (b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
- (2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Time and
place of
despatch
and receipt
of
electronic
record.

13. (1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
- (2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:—
- (a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—
- (i) receipt occurs at the time when the electronic record enters the designated computer resource; or

- (ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;
- (b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
- (3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
- (4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
- (5) For the purposes of this section,—
 - (a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

- (b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
- (c) “usual place of residence”, in relation to a body corporate, means the place where it is registered.

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

- Secure electronic record. 14. Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
- Secure digital signature. 15. If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—
 - (a) unique to the subscriber affixing it;
 - (b) capable of identifying such subscriber;
 - (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.
- Security procedure. 16. The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial

circumstances prevailing at the time when the procedure was used, including—

- (a) the nature of the transaction;
- (b) the level of sophistication of the parties with reference to their technological capacity;
- (c) the volume of similar transactions engaged in by other parties;
- (d) the availability of alternatives offered to but rejected by any party;
- (e) the cost of alternative procedures; and
- (f) the procedures in general use for similar types of transactions or communications.

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

Appoi-
ntment of
Controller
and other
officers.

17. (1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
- (2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
- (3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
- (4) The qualifications, experience and terms and conditions of service of

Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

- (5) The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
- (6) There shall be a seal of the Office of the Controller.

Functions
of
Controller.

- 18. The Controller may perform all or any of the following functions, namely:—
 - (a) exercising supervision over the activities of the Certifying Authorities;
 - (b) certifying public keys of the Certifying Authorities;
 - (c) laying down the standards to be maintained by the Certifying Authorities;
 - (d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
 - (e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
 - (f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
 - (g) specifying the form and content of a Digital Signature Certificate and the key;

- (h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
 - (i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
 - (j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
 - (k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
 - (l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
 - (m) laying down the duties of the Certifying Authorities;
 - (n) maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.
19. (1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act. Recognition of foreign Certifying Authorities.
- (2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

- (3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.
20. (1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act. Controller to act as repository.
- (2) The Controller shall—
- (a) make use of hardware, software and procedures that are secure from intrusion and misuse;
 - (b) observe such other standards as may be prescribed by the Central Government; to ensure that the secrecy and security of the digital signatures are assured.
- (3) The Controller shall maintain a computerised database of all public keys in such a manner that such database and the public keys are available to any member of the public.
21. (1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates. Licence to issue Digital Signature Certificates.
- (2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are

necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this section shall—

- (a) be valid for such period as may be prescribed by the Central Government;
- (b) not be transferable or heritable;
- (c) be subject to such terms and conditions as may be specified by the regulations.

Application
for licence.

22. (1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by—

- (a) a certification practice statement;
- (b) a statement including the procedures with respect to identification of the applicant;
- (c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
- (d) such other documents, as may be prescribed by the Central Government.

Renewal of
licence.

23. An application for renewal of a licence shall be—

- (a) in such form;
- (b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

Procedure
for grant
or rejection
of licence.

24. The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application: Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Suspension
of licence.

25. (1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,—

- (a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
- (b) failed to comply with the terms and conditions subject to which the licence was granted;
- (c) failed to maintain the procedures and standards specified in section 30.
- (d) contravened any provisions of this Act, rule, regulation or order made thereunder,

revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence

under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him:

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

26. (1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

Notice of
suspension
or
revocation
of licence.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Provided that the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a website which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate.

27. The Controller may, in writing, authorise the Deputy Controller, Assistant

Power to
delegate.

Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. (1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

Power to investigate contraventions.

- (2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

43 of 1961

29. (1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

Access to computers and data.

- (2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the

computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Every Certifying Authority shall,—
 - (a) make use of hardware, software and procedures that are secure from intrusion and misuse;
 - (b) provide a reasonable level or reliability in its services which are reasonably suited to the performance of intended functions;
 - (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
 - (d) observe such other standards as may be specified by regulations.
31. Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.
32. Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.
33. (1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.
(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of

Certifying Authority to follow certain procedures.

Certifying Authority to ensure compliance of the Act, etc.

Display of licence.

Surrender of licence.

an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

- Disclosure. 34. (1) Every Certifying Authority shall disclose in the manner specified by regulations—
- (a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
 - (b) any certification practice statement relevant thereto;
 - (c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and
 - (d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.
- (2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—
- (a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

- (b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTER VII

DIGITAL SIGNATURE CERTIFICATES

Certifying
Authority
to issue
Digital
Signature
Certificate.

35. (1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

- (2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

- (3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
- (4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to

be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that—

- (a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
- (b) the applicant holds a private key, which is capable of creating a digital signature;
- (c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. A Certifying Authority while issuing a Digital Signature Certificate shall certify that—

- (a) it has complied with the provisions of this Act and the rules and regulations made thereunder;
- (b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
- (c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
- (d) the subscriber's public key and private key constitute a functioning key pair;

Representations upon issuance of Digital Signature Certificate.

- (e) the information contained in the Digital Signature Certificate is accurate; and
 - (f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).
37. (1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,—
- Suspension
of Digital
Signature
Certificate.
- (a) on receipt of a request to that effect from—
 - (i) the subscriber listed in the Digital Signature Certificate; or
 - (ii) any person duly authorised to act on behalf of that subscriber;
 - (b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.
- (2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.
- (3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. (1) A Certifying Authority may revoke a Digital Signature Certificate issued by it—
- Revocation of Digital Signature Certificate.
- (a) where the subscriber or any other person authorised by him makes a request to that effect; or
 - (b) upon the death of the subscriber; or
 - (c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
- (2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that—
- (a) a material fact represented in the Digital Signature Certificate is false or has been concealed;
 - (b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
 - (c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
 - (d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

- (3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.
- (4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.
- Notice of suspension or revocation. 39. (1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.
- (2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

CHAPTER VIII

DUTIES OF SUBSCRIBERS

- Generating key pair. 40. Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key-pair by applying the security procedure.
- Acceptance of Digital Signature Certificate. 41. (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the

publication of a Digital Signature Certificate—

- (a) to one or more persons;
- (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

- (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
- (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Control of
private
key.

42. (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.
- (2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall

communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation—For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX

PENALTIES AND ADJUDICATION

Penalty for
damage to
computer,
computer
system, etc.

43. If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network—
- (a) accesses or secures access to such computer, computer system or computer network;
 - (b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
 - (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
 - (d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

- (e) disrupts or causes disruption of any computer, computer system or computer network;
 - (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
 - (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
 - (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,
- he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation—For the purposes of this section—

- (i) “computer contaminant” means any set of computer instructions that are designed—
 - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
 - (b) by any means to usurp the normal operation of the computer, computer system, or computer network;
- (ii) “computer database” means a representation of information,

knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

- (iii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- (iv) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. If any person who is required under this Act or any rules or regulations made thereunder to—

- (a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- (b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations,

Penalty for failure to furnish information return, etc.

he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

- (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Residuary
penalty.

45. Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Power to
adjudicate.

46. (1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.
- (2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the

matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

- (3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.
- (4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
- (5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and—
 - (a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
 - (b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

Factors to
be taken
into
account by
the
adjudicating
officer.

47. While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:—

- (a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- (b) the amount of loss caused to any person as a result of the default;
- (c) the repetitive nature of the default.

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

Establish-
ment of
Cyber
Appellate
Tribunal.

48. (1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.
- (2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Composi-
tion of
Cyber
Appellate
Tribunal.

49. A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.
50. A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he—
- (a) is, or has been, or is qualified to be, a Judge of a High Court; or
 - (b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

Qualifica-
tions for
appoint-
ment as
Presiding
Officer of
the Cyber
Appellate
Tribunal.

51. The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he

Term of
office.

enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Salary, allowances and other terms and conditions of service of Presiding Officer.

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

Filling up of vacancies.

54. (1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Resignation and removal.

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon

his office or until the expiry of his term of office, whichever is the earliest.

- (2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.
- (3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

56. (1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that government may think fit.
- (2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

Staff of the Cyber Appellate Tribunal.

- Appeal to
Cyber
Appellate
Tribunal.
- (3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.
57. (1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

- (5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.
- (6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

Procedure
and
powers of
the Cyber
Appellate
Tribunal.

58. (1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings. 5 of 1908.
- (2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:— 5 of 1908.
 - (a) summoning and enforcing the attendance of any person and examining him on oath;
 - (b) requiring the discovery and production of documents or other electronic records;

- (c) receiving evidence on affidavits;
- (d) issuing commissions for the examination of witnesses or documents;
- (e) reviewing its decisions;
- (f) dismissing an application for default or deciding it *ex parte*;
- (g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Right to
legal
representa-
tion.

59. The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

36 of 1963

60. The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

Limitation.

61. No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Civil court
not to
have
jurisdiction.

62. Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Appeal to
High
Court.

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. (1) Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Compound-
ing of
contraven-
tions.

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

- (2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation—For the purposes of this sub-section, any second or subsequent

contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

- (3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

Recovery
of penalty.

CHAPTER XI

OFFENCES

65. Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Tampering
with
computer
source
documents.

Explanation—For the purposes of this section, “computer source code” means

the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

66. (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

Hacking
with
computer
system.

- (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

67. Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Publishing
of
information
which is
obscene in
electronic
form.

Power of
Controller
to give
directions.

68. (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such

measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

- (2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Directions
of
Controller
to a
subscriber
to extend
facilities to
decrypt
information.

69. (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.
- (2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.
- (3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

- Protected system.
70. (1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
- (2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).
- (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

- Penalty for misrepresentation.
71. Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

- Penalty for breach of confidentiality and privacy.
72. Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, informa-

tion, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalty for publishing Digital Signature Certificate false in certain particulars.

73. (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

- (a) the Certifying Authority listed in the certificate has not issued it; or
- (b) the subscriber listed in the certificate has not accepted it; or
- (c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Publication for fraudulent purpose.

75. (1) Subject to the provisions of sub-section (2), the provisions of this Act shall

Act to apply for offence or

apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

contraven-
tion
committed
outside
India.

- (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Confisca-
tion

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force. Penalties or confiscation not to interfere with other punishments.
- 2 of 1974. 78. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act. Power to investigate offences.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Network service providers not to be liable in certain cases.

Explanation—For the purposes of this section—

- (a) “network service provider” means an intermediary;
- (b) “third party information” means any information dealt with by a network service provider in his capacity as an intermediary;

CHAPTER XIII

MISCELLANEOUS

Power of
police
officer and
other
officers to
enter,
search, etc.

80. (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act. 2 of 1974.

Explanation—For the purposes of this sub-section, the expression “public place” includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

- (2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
- (3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section. 2 of 1974.

- Act to have overriding effect.
81. The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.
- Controller, Deputy Controller and Assistant Controllers to be public servants. Power to give directions.
82. The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code. ^{45 of 1860.}
83. The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.
- Protection of action taken in good faith.
84. No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.
- Offences by companies.
85. (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be

proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation—For the purposes of this section—

- (i) “company” means any body corporate and includes a firm or other association of individuals; and

- (ii) “director”, in relation to a firm, means a partner in the firm.

Removal of
difficulties.

86. (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order

published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

- (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

Power of
Central
Government
to make
rules.

87. (1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—
- (a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;
 - (b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;
 - (c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (2) of section 6;
 - (d) the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;

- (e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;
- (f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;
- (g) other standards to be observed by the Controller under clause (b) of sub-section (2) of section 20;
- (h) the requirements which an applicant must fulfil under sub-section (2) of section 21;
- (i) the period of validity of licence granted under clause (a) of sub-section (3) of section 21;
- (j) the form in which an application for licence may be made under sub-section (1) of section 22;
- (k) the amount of fees payable under clause (c) of sub-section (2) of section 22;
- (l) such other documents which shall accompany an application for licence under clause (d) of sub-section (2) of section 22;
- (m) the form and the fee for renewal of a licence and the fee payable thereof under section 23;
- (n) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;
- (o) the fee to be paid to the Certifying Authority for issue of a Digital

- Signature Certificate under sub-section (2) of section 35;
- (p) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;
 - (q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;
 - (r) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;
 - (s) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (3) of section 54;
 - (t) the salary and allowances and other conditions of service of other officers and employees under sub-section (3) of section 56;
 - (u) the form in which appeal may be filed and the fee thereof under sub-section (3) of section 57;
 - (v) any other power of a civil court required to be prescribed under clause (g) of sub-section (2) of section 58; and
 - (w) any other matter which is required to be, or may be, prescribed.
- (3) Every notification made by the Central Government under clause (f) of sub-section (4) of section 1 and every rule made by it shall be laid, as soon as

may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

Constitution
of
Advisory
Committee.

88. (1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.
- (2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.
- (3) The Cyber Regulations Advisory Committee shall advise—

Power of
Controller
to make
regulations.

- (a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;
 - (b) the Controller in framing the regulations under this Act.
- (4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.
- 89. (1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:—
 - (a) the particulars relating to maintenance of database containing the disclosure record of every Certifying Authority under clause (n) of section 18;
 - (b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 19;
 - (c) the terms and conditions subject to which a licence may be granted under clause (c) of sub-section (3) of section 21;

- (d) other standards to be observed by a Certifying Authority under clause (d) of section 30;
 - (e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;
 - (f) the particulars of statement which shall accompany an application under sub-section (3) of section 35;
 - (g) the manner in which the subscriber shall communicate the compromise of private key to the certifying Authority under sub-section (2) of section 42.
- (3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

90. (1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act. Power of State Government to make rules.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—
 - (a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
 - (b) for matters specified in sub-section (2) of section 6;
 - (c) any other matter which is required to be provided by rules by the State Government.
- (3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House. Amendment of Act 45 of 1860.
91. The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act. Amendment of Act 1 of 1872.
92. The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act. Amendment of Act 18 of 1891.
93. The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act. Amendment of Act 2 of 1934.
94. The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

THE FIRST SCHEDULE

(See section 91)

**AMENDMENTS TO THE INDIAN
PENAL CODE**

(45 OF 1860)

1. After section 29, the following section shall be inserted, namely:—
“29 A. The words “electronic record” shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000.”. Electronic record.
2. In section 167, for the words “such public servant, charged with the preparation or translation of any document, frames or translates that document”, the words “such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record” shall be substituted.
3. In section 172, for the words “produce a document in a Court of Justice”, the words “produce a document or an electronic record in a Court of Justice” shall be substituted.
4. In section 173, for the words “to produce a document in a Court of Justice”, the words “to produce a document or electronic record in a Court of Justice” shall be substituted.
5. In section 175, for the word “document” at both the places where it occurs, the words “document or electronic record” shall be substituted.
6. In section 192, for the words “makes any false entry in any book or record, or makes

any document containing a false statement”, the words “makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement” shall be substituted.

7. In section 204, for the word “document” at both the places where it occurs, the words “document or electronic record” shall be substituted.
8. In section 463, for the words “Whoever makes any false documents or part of a document with intent to cause damage or injury”, the words “Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury” shall be substituted.
9. In section 464,—
 - (a) for the portion beginning with the words “A person is said to make a false document” and ending with the words “by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration”, the following shall be substituted, namely:—

“A person is said to make a false document or false electronic record—*Firstly*—Who dishonestly or fraudulently—

 - (a) makes, signs, seals or executes a document or part of a document;
 - (b) makes or transmits any electronic record or part of any electronic record;

- (c) affixes any digital signature on any electronic record;
- (d) makes any mark denoting the execution of a document or the authenticity of the digital signature

with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.”;

- (b) after *Explanation 2*, the following Explanation shall be inserted at the end, namely:—

Explanation 3—For the purposes of this section, the expression “affixing digital signature” shall have the meaning assigned to it in clause (d) of sub-section (1) of section 2 of the Information Technology Act, 2000.’

- 10. In section 466,—

- (a) for the words “Whoever forges a document”, the words “Whoever forges a document or an electronic record” shall be substituted;
- (b) the following *Explanation* shall be inserted at the end, namely:—

Explanation—For the purposes of this section, “register” includes any list, data or record of any entries maintained in the electronic form as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000.

- 11. In section 468, for the words “document forged”, the words “document or electronic record forged” shall be substituted.
- 12. In section 469, for the words “intending that the document forged”, the words “intending that the document or electronic record forged” shall be substituted.
- 13. In section 470, for the word “document” in both the places where it occurs, the words “document or electronic record” shall be substituted.
- 14. In section 471, for the word “document” wherever it occurs, the words “document or electronic record” shall be substituted.

15. In section 474, for the portion beginning with the words “Whoever has in his possession any document” and ending with the words “if the document is one of the description mentioned in section 466 of this Code”, the following shall be substituted, namely:—
“Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.”.
16. In section 476, for the words “any document”, the words “any document or electronic record” shall be substituted.
17. In section 477A, for the words “book, paper, writing” at both the places where they occur, the words “book, electronic record, paper, writing” shall be substituted.

THE SECOND SCHEDULE

(See section 92)

AMENDMENTS TO THE INDIAN

EVIDENCE ACT, 1872

(1 OF 1872)

1. In section 3,—
 - (a) in the definition of “Evidence”, for the words “all documents produced for the inspection of the Court”, the words “all documents including electronic records produced for the inspection of the Court” shall be substituted;

(b) after the definition of “India”, the following shall be inserted, namely:—
 ‘the expressions “Certifying Authority”, “digital signature”, “Digital Signature Certificate”, “electronic form”, “electronic records”, “information”, “secure electronic record”, “secure digital signature” and “subscriber” shall have the meanings respectively assigned to them in the Information Technology Act, 2000.’.

2. In section 17, for the words “oral or documentary”, the words “oral or documentary or contained in electronic form” shall be substituted.

3. After section 22, the following section shall be inserted, namely:—

“22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.”.

When oral admission as to contents of electronic records are relevant.

4. In section 34, for the words “Entries in the books of account”, the words “Entries in the books of account, including those maintained in an electronic form” shall be substituted.

5. In section 35, for the word “record”, in both the places where it occurs, the words “record or an electronic record” shall be substituted.

6. For section 39, the following section shall be substituted, namely:—

“39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or

What evidence to be given when statement forms part of a conversation, document,

electronic
record,
book or
series of
letters or
papers.

is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.”.

Opinion as
to digital
signature
where
relevant.

7. After section 47, the following section shall be inserted, namely:—

“47A. When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.”.

8. In section 59, for the words “contents of documents” the words “contents of documents or electronic records” shall be substituted.

9. After section 65, the following sections shall be inserted, namely:—

‘65A. The contents of electronic records may be proved in accordance with the provisions of section 65B.

65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this

Special
provisions
as to
evidence
relating to
electronic
record.

Admissibi-
lity of
electronic
records.

section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in subsection (1) in respect of a computer output shall be the following, namely:—

- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
- (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
- (c) throughout the material part of the said period, the

computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

- (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.
- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—
- (a) by a combination of computers operating over that period; or
 - (b) by different computers operating in succession over that period; or
 - (c) by different combinations of computers operating in succession over that period; or
 - (d) in any other manner involving the successive

operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—
- (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
 - (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
 - (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
- and purporting to be signed by a person occupying a responsible official position in relation to the

operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

- (5) For the purposes of this section,—
- (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
 - (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

- (c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.’.

- 10. After section 67, the following section shall be inserted, namely:—

Proof as to digital signature.

“67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.”.

Proof as to verification of digital signature.

- 11. After section 73, the following section shall be inserted, namely:—

’73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

- (a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
- (b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Presump-
tion as to
Gazettes in
electronic
forms.

Explanation—For the purposes of this section, “Controller” means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000.

12. After section 81, the following section shall be inserted, namely:—

Presump-
tion as to
electronic
agreements.

“81A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.”.

13. After section 85, the following sections shall be inserted, namely:—

Presump-
tion as to
electronic
records
and digital
signatures.

“85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

85B. (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

- (2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by subscriber with

Presump-
tion as to
Digital
Signature
Certificates.

the intention of signing or approving the electronic record;

- (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Presump-
tion as to
electronic
messages.

85C. The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.”

14. After section 88, the following section shall be inserted, namely:—

’88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation—For the purposes of this section, the expressions “addressee” and “originator” shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.

Presump-
tion as to
electronic
records
five years
old.

15. After section 90, the following section shall be inserted, namely:—

“90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This *Explanation* also applies to section 81A.

16. For section 131, the following section shall be substituted, namely:—
- “131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.”
- Production of documents or electronic records which another person, having possession, could refuse to produce.

THE THIRD SCHEDULE

(See section 93)

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT 1891 (18 OF 1891)

1. In section 2—

- (a) for clause (3), the following clause shall be substituted namely:—
'(3) "bankers' books" include ledgers, day books, cash books, account books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device;
- (b) for clause (8), the following clause shall be substituted, namely:—
'(8) "certified copy" means when the books of a bank,—
- (a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

- (b) consist of printouts of data stored in a floppy, disc, tape or any other electromagnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.’.
2. After section 2, the following section shall be inserted, namely:—
- “2A. A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:—
- (a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and
 - (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of—
 - (A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;
 - (B) the safeguards adopted to prevent and detect unauthorised change of data;
 - (C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
 - (D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electromagnetic data storage devices;

Conditions
in the
printout.

- (E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;
 - (F) the mode of identification of such data storage devices;
 - (G) the arrangements for the storage and custody of such storage devices;
 - (H) the safeguards to prevent and detect any tampering with the system; and
 - (I) any other factor which will vouch for the integrity and accuracy of the system.
- (c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.”

THE FOURTH SCHEDULE

(See section 94)

AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934

(2 OF 1934)

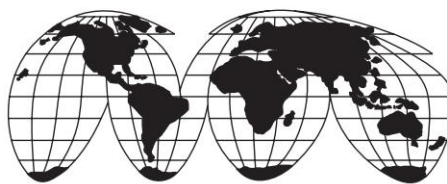
In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (p), the following clause shall be inserted, namely:—

“(pp) the regulation of fund transfer through electronic means between the

banks or between the banks and other financial institutions referred to in clause (c) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;”.

SUBHASH C. JAIN,
Secy. to the Govt. of India

Information Technology Act, 2000
<http://cca.gov.in/documents/act2000.pdf>



Appendix 5

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001

Contents

Resolution adopted by the general assembly	vii
--	-----

Part One

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

Article 1. Sphere of application	1
Article 2. Definitions	1
Article 3. Equal treatment of signature technologies	2
Article 4. Interpretation	2
Article 5. Variation by agreement	2
Article 6. Compliance with a requirement for a signature	2
Article 7. Satisfaction of article 6	3
Article 8. Conduct of the signatory	3
Article 9. Conduct of the certification service provider	4
Article 10. Trustworthiness	5
Article 11. Conduct of the relying party	5
Article 12. Recognition of foreign certificates and electronic signatures	6

*Part Two***GUIDE TO ENACTMENT OF THE UNCITRAL MODEL
LAW ON ELECTRONIC SIGNATURES (2001)**

Purpose of this Guide	7
Chapter I. Introduction to the Model Law	8
I. Purpose and Origin of the Model Law	8
A. Purpose	8
B. Background	9
C. History	11
II. THE MODEL LAW AS A TOOL FOR HARMONIZING LAWS	18
III. General REMARKS ON ELECTRONIC SIGNATURES ...	19
A. Functions of signatures	19
B. Digital signatures and other electronic signatures	20
1. Electronic signatures relying on techniques other than public-key cryptography	21
2. Digital signatures relying on public-key cryptography	22
(a) Technical notions and terminology	22
(i) Cryptography	22
(ii) Public and private keys	22
(iii) Hash function	23
(iv) Digital signature	24
(v) Verification of digital signature	24
(b) Public-key infrastructure and suppliers of certification services	25
(i) Public-key infrastructure	26
(ii) Certification service provider	27
(c) Summary of the digital signature process	30
IV. MAIN FEATURES OF THE MODEL LAW	31
A. Legislative nature of the Model Law	31
B. Relationship with the UNCITRAL Model Law on Electronic Commerce	32
1. New Model Law as a separate legal instrument	32

2. New Model Law fully consistent with the UNCITRAL Model Law on Electronic Commerce	32
3. Relationship with article 7 of the UNCITRAL Model Law on Electronic Commerce	33
C. “Framework” rules to be supplemented by technical regulations and contract	34
D. Added certainty as to the legal effects of electronic signatures	34
E. Basic rules of conduct for the parties involved	36
F. A technology-neutral framework	38
G. Non-discrimination of foreign electronic signatures	38
V. ASSISTANCE FROM THE UNCITRAL SECRETARIAT	38
A. Assistance in drafting legislation	38
B. Information on the interpretation of legislation based on the Model Law	39
Chapter II. Article-by-article remarks	39
Title	39
Article 1. Sphere of application	40
Article 2. Definitions	42
Article 3. Equal treatment of signature technologies	47
Article 4. Interpretation	48
Article 5. Variation by agreement	50
Article 6. Compliance with a requirement for a signature	51
Article 7. Satisfaction of article 6	57
Article 8. Conduct of the signatory	60
Article 9. Conduct of the certification service provider	63
Article 10. Trustworthiness	66
Article 11. Conduct of the relying party	67
Article 12. Recognition of foreign certificates and electronic signatures	69

Part One

Uncitral Model Law on Electronic Signatures (2001)

Article 1. Sphere of Application

This Law applies where electronic signatures are used in the context* of commercial** activities. It does not override any rule of law intended for the protection of consumers.

Article 2. Definitions

For the purposes of this Law:

- (a) “Electronic signature” means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message;
- (b) “Certificate” means a data message or other record confirming the link between a signatory and signature creation data;
- (c) “Data message” means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts

* The Commission suggests the following text for States that might wish to extend the applicability of this Law:

“This Law applies where electronic signatures are used, except in the following situations: [...]”

**The term “commercial” should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

either on its own behalf or on behalf of the person it represents;

- (d) “Signatory” means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
- (e) “Certification service provider” means a person that issues certificates and may provide other services related to electronic signatures;
- (f) “Relying party” means a person that may act on the basis of a certificate or an electronic signature.

Article 3. Equal Treatment of Signature Technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law.

Article 4. Interpretation

1. In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.
2. Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5. Variation by Agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Article 6. Compliance with a Requirement for a Signature

1. Where the law requires a signature of a person, that

requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
 - (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
 - (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
 - (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
 - (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
4. Paragraph 3 does not limit the ability of any person:
 - (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or
 - (b) To adduce evidence of the non-reliability of an electronic signature.
5. The provisions of this article do not apply to the following: [...].

Article 7. Satisfaction of article 6

1. *[Any person, organ or authority, whether public or private, specified by the enacting State as competent]* may determine which

electronic signatures satisfy the provisions of article 6 of this Law.

2. Any determination made under paragraph 1 shall be consistent with recognized international standards.
3. Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the Signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
 - (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;
 - (b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
 - (i) The signatory knows that the signature creation data have been compromised; or
 - (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;
 - (c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.
2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 9. Conduct of the Certification Service Provider

1. Where a certification service provider provides services to support an electronic signature that may be used for legal

- effect as a signature, that certification service provider shall:
- (a) Act in accordance with representations made by it with respect to its policies and practices;
 - (b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;
 - (c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:
 - (i) The identity of the certification service provider;
 - (ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
 - (iii) That signature creation data were valid at or before the time when the certificate was issued;
 - (d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:
 - (i) The method used to identify the signatory;
 - (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;
 - (iii) That the signature creation data are valid and have not been compromised;
 - (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;
 - (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law;
 - (vi) Whether a timely revocation service is offered;
 - (e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;
 - (f) Utilize trustworthy systems, procedures and human resources in performing its services.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 10. Trustworthiness

For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

- (a) Financial and human resources, including existence of assets;
- (b) Quality of hardware and software systems;
- (c) Procedures for processing of certificates and applications for certificates and retention of records;
- (d) Availability of information to signatories identified in certificates and to potential relying parties;
- (e) Regularity and extent of audit by an independent body;
- (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
- (g) Any other relevant factor.

Article 11. Conduct of the Relying Party

A relying party shall bear the legal consequences of its failure:

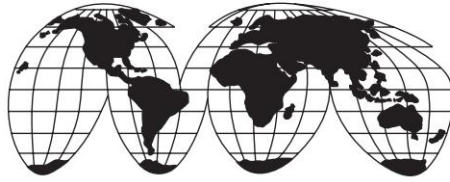
- (a) To take reasonable steps to verify the reliability of an electronic signature; or
- (b) Where an electronic signature is supported by a certificate, to take reasonable steps:
 - (i) To verify the validity, suspension or revocation of the certificate; and
 - (ii) To observe any limitation with respect to the certificate.

Article 12. Recognition of Foreign Certificates and Electronic Signatures

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
 - (a) To the geographic location where the certificate is issued or the electronic signature created or used; or
 - (b) To the geographic location of the place of business of the issuer or signatory.
2. A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.
4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.
5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURE
(2001)

<http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf>



Appendix 6

PKI Standards

(a) **PKIX (Public Key Infrastructure)**

- The latest road map for “Internet X.509 Public Key Infrastructure” notified by IETF or ITU
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

(b) **Public-Key Cryptography based on the Institute of Electrical and Electronics Engineers (IEEE) Standard P1363 for three families:**

- Discrete Logarithm (DL) systems
- Elliptic Curve Discrete Logarithm (EC) systems
- Integer Factorization (IF) systems

(c) **Public-key Cryptography Standards (PKCS)**

- PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
- PKCS#3 Diffie-Hellman Key Agreement Standard
- PKCS#5 Password Based Encryption Standard
- PKCS#6 Extended-Certificate Syntax Standard
- PKCS#7 Cryptographic Message Syntax Standard
- PKCS#8 Private-Key Information Syntax Standard
- PKCS#9 Selected Attribute Types
- PKCS#10 RSA Certification Request
- PKCS#11 Cryptographic Token Interface Standard
- PKCS#12 Portable format for storing/ transporting a user’s private keys and certificates

- PKCS#13 Elliptic Curve Cryptography Standard
 - PKCS#14 Pseudorandom Number Generation Standard
 - PKCS#15 Cryptographic Token Information Format Standard
- (d) **Federal Information Processing Standards (FIPS)**
- FIPS 180-2 Secure Hash standards,
 - SHA-1 (160-bit hash)
 - SHA-224, SHA-256, SHA-384 and SHA-512
 - FIPS
 - 186-2 Digital Signature Standard (DSS)
 - FIPS 140-2 Security Requirements for Cryptographic Modules
- (e) **Discrete Logarithm (DL) systems**
- Diffie-Hellman, MQV key agreement
 - DSA, Nyberg-Rueppel signatures
- (f) **Elliptic Curve (EC) systems**
- Elliptic curve analogs of DL systems;
- (g) **Integer Factorization (IF) systems**
- RSA encryption
 - RSA, Rabin-Williams signatures;
- (h) **Hash Algorithms**
- MD5 Message Digest Algorithm
- (i) **Key agreement schemes**
- (1) **Signature schemes**
- DL/ EC scheme with message recovery
 - PSS, FDH, PKCS #1 encoding methods for IF family
 - PSS-R for message recovery in IF family
- (2) **Encryption schemes**
- Abdalla-Bellare-Rogaway DHAES for DL/ EC family
 - FIPS Advanced Encryption Standard (AES)
- (j) **Directory Services X.500 and/or LDAP**
- For publication of Public Key Certificates and Certificate Revocation Lists

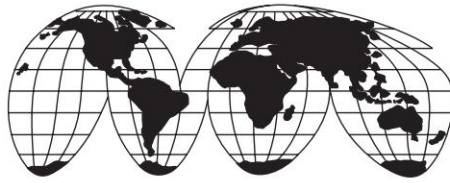
(k) **PKI Policy and Procedures**

- RFC 3647 for Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

(l) **Public Key Certificate Standard**

International Telecommunication Union (ITU) X.509 version 3

- X.509 (version 3 or higher) format for Certificates as specified by ITU from time to time
- X.509 (version 2 or higher) format for Certificate Revocation List as specified by ITU from time to time



Appendix 7

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures

The European Parliament and the Council of The European Union,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission⁽¹⁾,

Having regard to the opinion of the Economic and Social Committee⁽²⁾,

Having regard to the opinion of the Committee of the Regions⁽³⁾,

⁽¹⁾OJ C 325, 23. 10. 1998, p. 5.

⁽²⁾OJ C 40, 15. 2. 1999, p. 29.

⁽³⁾OJ C 93, 6. 4. 1999, p. 33.

Acting in accordance with the procedure laid down in Article 251 of the Treaty⁽⁴⁾,

Whereas:

- (1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;
- (2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication—towards a European framework for digital signatures and encryption;
- (3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;
- (4) Electronic communication and commerce necessitate ‘electronic signatures’ and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;
- (5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal

⁽⁴⁾Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14. 4. 1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243, 27. 8. 1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal). Council Decision of 30 November 1999.

frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/ 94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods⁽⁵⁾ and Council Decision 94/ 942/ CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods⁽⁶⁾;

- (6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;
- (7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;
- (8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;
- (9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;

⁽⁵⁾OJ L 367, 31. 12. 1994, p. 1. Regulation as amended by Regulation (EC) No 837/ 95 (OJ L 90, 21. 4. 1995, p. 1).

⁽⁶⁾OJ L 367, 31. 12. 1994, p. 8. Decision as last amended by Decision 99/ 193/ CFSP (OJ L 73, 19. 3. 1999, p. 1).

- (10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;
- (11) Voluntary accreditation schemes aiming at an enhanced level of service provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;
- (12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;
- (13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;

- (14) It is important to strike a balance between consumer and business needs;
- (15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;
- (16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;
- (17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;
- (18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;
- (19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public

procurement, taxation, social security, health and justice systems;

- (20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled;
- (21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;
- (22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;
- (23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;
- (24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

- (25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;
- (26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/ 468/ EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission⁽¹⁾;
- (27) Two years after its implementation, the Commission will carry out a review of this Directive so as, inter alia , to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;
- (28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,

Have Adopted This Directive

Article 1

Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain

⁽¹⁾ OJ L 184, 17.7. 1999, p. 23.

certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2

Definitions

For the purpose of this Directive:

1. 'Electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. 'Advanced electronic signature' means an electronic signature which meets the following requirements:
 - (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using means that the signatory can maintain under his sole control; and
 - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. 'Signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. 'Signature-creation data' means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. 'Signature-creation device' means configured software or hardware used to implement the signature-creation data;
6. 'Secure-signature-creation device' means a signature-creation device which meets the requirements laid down in Annex III;

7. 'Signature-verification-data' means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
8. 'Signature-verification device' means configured software or hardware used to implement the signature-verification-data;
9. 'Certificate' means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
10. 'Qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;
11. 'Certification-service-provider' means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
12. 'Electronic-signature product' means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
13. 'Voluntary accreditation' means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3

Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.
3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.
4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated. A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.
5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities . Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.
6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.
7. Member States may make the use of electronic signatures in the public sector subject to possible additional

requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4

Internal Market Principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.
2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal Effects of Electronic Signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
 - (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
 - (b) are admissible as evidence in legal proceedings.
2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
 - in electronic form, or
 - not based upon a qualified certificate, or

- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
 - (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
 - (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
 - (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;unless the certification-service-provider proves that he has not acted negligently.
2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.
4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.
5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/ 13/ EEC of 5 April 1993 on unfair terms in consumer contracts⁽¹⁾.

Article 7

International Aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
 - (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
 - (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

⁽¹⁾OJ L 95, 21. 4. 1993, p. 29.

- (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.
- 2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multi-lateral agreements with third countries and international organisations. The Council shall decide by qualified majority.
- 3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/ 46/ EC of the European Parliament and of the

Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁽²⁾.

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.
3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9

Committee

1. The Commission shall be assisted by an 'Electronic-Signature Committee', hereinafter referred to as 'the committee'.
2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/ 468/ EC shall apply, having regard to the provisions of Article 8 thereof.
The period laid down in Article 4(3) of Decision 1999/ 468/ EC shall be set at three months.
3. The Committee shall adopt its own rules of procedure.

Article 10

Tasks of the Committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature

⁽²⁾OJ L 281, 23. 11. 1995, p. 31.

products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:
 - (a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
 - (b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
 - (c) the names and addresses of all accredited national certification service providers.
2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12

Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.
2. The review shall, *inter alia*, assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13

Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

Entry into Force

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Communities*

Article 15

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 13 December 1999.

For the European Parliament
The President
N. FONTAINE

For the Council
The President
S. HASSI

Annex I

Requirements for Qualified Certificates

Qualified certificates must contain:

- (a) an indication that the certificate is issued as a qualified certificate;
- (b) the identification of the certification-service-provider and the State in which it is established;
- (c) the name of the signatory or a pseudonym, which shall be identified as such;
- (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
- (f) an indication of the beginning and end of the period of validity of the certificate;
- (g) the identity code of the certificate;
- (h) the advanced electronic signature of the certification-service-provider issuing it;
- (i) limitations on the scope of use of the certificate, if applicable; and
- (j) limits on the value of transactions for which the certificate can be used, if applicable.

Annex II

Requirements for Certification-service-providers Issuing Qualified Certificates

Certification-service-providers must:

- (a) demonstrate the reliability necessary for providing certification services;
- (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
- (e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
- (f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
- (g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
- (h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
- (i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

- (j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
- (k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
- (l) use trustworthy systems to store certificates in a verifiable form so that:
 - only authorised persons can make entries and changes,
 - information can be checked for authenticity,
 - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
 - any technical changes compromising these security requirements are apparent to the operator.

Annex III

Requirements for Secure Signature-creation Devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
 - (a) the signature-creation data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
 - (b) the signature-creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
 - (c) the signature-creation data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

Annex IV

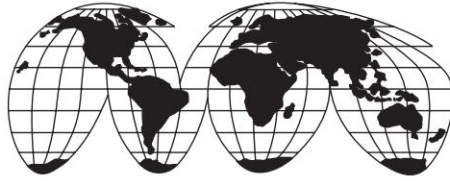
Recommendations for Secure Signature Verification

During the signature-verification process it should be ensured with reasonable certainty that:

- (a) the data used for verifying the signature correspond to the data displayed to the verifier;
- (b) the signature is reliably verified and the result of that verification is correctly displayed;
- (c) the verifier can, as necessary, reliably establish the contents of the signed data;
- (d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
- (e) the result of verification and the signatory's identity are correctly displayed;
- (f) the use of a pseudonym is clearly indicated; and
- (g) any security-relevant changes can be detected.

European Union Directive on a Community Framework for electronic signatures

[http:// europa.eu.int/ eur-lex/ pri/ en/ oj/ dat/ 2000/ 1_013/ 1_01320000119en00120020.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/1_013/1_01320000119en00120020.pdf)



Appendix 8

OECD Guidelines for Cryptography Policy issued by Organisation for Economic Cooperation and Development

I. AIMS

The Guidelines are intended:

- to promote the use of cryptography;
- to foster confidence in information and communications infrastructures, networks and systems and the manner in which they are used;
- to help ensure the security of data, and to protect privacy, in national and global information and communications infrastructures, networks and systems;
- to promote this use of cryptography without unduly jeopardising public safety, law enforcement, and national security;
- to raise awareness of the need for compatible cryptography policies and laws, as well as the need for interoperable, portable and mobile cryptographic methods in national and global information and communications networks;

Source: http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html OECD

- to assist decision-makers in the public and private sectors in developing and implementing coherent national and international policies, methods, measures, practices and procedures for the effective use of cryptography;
- to promote co-operation between the public and private sectors in the development and implementation of national and international cryptography policies, methods, measures, practices and procedures;
- to facilitate international trade by promoting cost-effective, interoperable, portable and mobile cryptographic systems;
- to promote international co-operation among governments, business and research communities, and standards-making bodies in achieving co-ordinated use of cryptographic methods.

II. Scope

The Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that they will be widely read and followed by both the private and public sectors.

It is recognised that governments have separable and distinct responsibilities for the protection of information which requires security in the national interest; the Guidelines are not intended for application in these matters.

III. Definitions

For the purposes of the Guidelines:

- “Authentication” means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.
- “Availability” means the property that data, information, and information and communications systems are accessible and usable on a timely basis in the required manner.

- “Confidentiality” means the property that data or information is not made available or disclosed to unauthorised individuals, entities, or processes.
- “Cryptography” means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/ or prevent its unauthorised use.
- “Cryptographic key” means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.
- “Cryptographic methods” means cryptographic techniques, services, systems, products and key management systems.
- “Data” means the representation of information in a manner suitable for communication, interpretation, storage, or processing.
- “Decryption” means the inverse function of encryption.
- “Encryption” means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.
- “Integrity” means the property that data or information has not been modified or altered in an unauthorised manner.
- “Interoperability” of cryptographic methods means the technical ability of multiple cryptographic methods to function together.
- “Key management system” means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.
- “Keyholder” means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.
- “Law enforcement” or “enforcement of laws” refers to the enforcement of all laws, without regard to subject matter.
- “Lawful access” means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.

- “Mobility” of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.
- “Non-repudiation” means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).
- “Personal data” means any information relating to an identified or identifiable individual.
- “Plaintext” means intelligible data.
- “Portability” of cryptographic methods means the technical ability to be adapted and function in multiple systems.

IV. Integration

The principles in Section V of this Annex, each of which addresses an important policy concern, are interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest.

V. Principles

1. Trust in Cryptographic Methods

Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

Market forces should serve to build trust in reliable systems, and government regulation, licensing, and use of cryptographic methods may also encourage user trust. Evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.

In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

2. Choice of Cryptographic Methods

Users should have a right to choose any cryptographic method, subject to applicable law. Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfil different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs.

In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection.

Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.

3. Market Driven Development of Cryptographic Methods

Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to information and communications systems security. The development of international technical standards, criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and co-operate with business and the research community in the development of cryptographic methods.

4. Standards for Cryptographic Methods

Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

In response to the needs of the market, internationally-recognised standards-making bodies, governments, business and other relevant experts should share information and collaborate to develop and promulgate interoperable technical standards, criteria and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such technical standards, criteria and protocols for interoperability, portability and mobility of cryptographic methods should be developed. To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should be encouraged.

5. Protection of Privacy and Personal Data

The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimise the collection of personal data, by enabling secure but anonymous payments, transactions and interactions. At the same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These implications, which include the collection of personal data and the creation of systems for personal identification, should be considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods.

6. Lawful Access

National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used

for lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of cryptographic methods.

Key management systems could provide a basis for a possible solution which could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key.

7. Liability

Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated. The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.

8. International Co-operation

Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for international use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

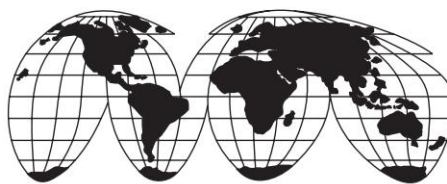
No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce.

Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.

OECD GUIDELINES FOR CRYPTOGRAPHY POLICY

http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html



Appendix 9

European Union Convention on Cybercrime

Budapest 23.XI.2001

<http://conventions.coe.int/Treaty/en/treaties/html/185.htm>

Explanatory Report Additional Protocol Francais

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cyber crime, *inter alia* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cyber crime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cyber crime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international levels, and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the

Protection of Individuals with Regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cyber crimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the

work carried out by the European Committee on Crime Problems (CDPC) on cyber crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cyber crime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10–11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I—Use of Terms

Article 1—Definitions

For the purposes of this Convention:

- a. “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b. “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c. “service provider” means:
 - i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

- ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
- d. “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II—Measures to be Taken at the National Level

Section 1—Substantive Criminal Law

Title 1—Offences Against the Confidentiality, Integrity and Availability of Computer Data and Systems

Article 2—Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3—Illegal Interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer

system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4—Data Interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5—System Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6—Misuse of Devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
 - a. the production, sale, procurement for use, import, distribution or otherwise making available of:
 - i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2–5;
 - ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and

- b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Title 2—Computer-related Offences

Article 7—Computer-related Forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8—Computer-related Fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

- a. any input, alteration, deletion or suppression of computer data,
- b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Title 3—Content-related Offences

Article 9—Offences Related to Child Pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a. producing child pornography for the purpose of its distribution through a computer system;
 - b. offering or making available child pornography through a computer system;
 - c. distributing or transmitting child pornography through a computer system;
 - d. procuring child pornography through a computer system for oneself or for another;
 - e. possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above “child pornography” shall include pornographic material that visually depicts:
 - a. a minor engaged in sexually explicit conduct;
 - b. a person appearing to be a minor engaged in sexually explicit conduct;
 - c. realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Title 4—Offences Related to Infringements of Copyright and Related Rights

Article 10—Offences Related to Infringements of Copyright and Related Rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from

the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5—Ancillary Liability and Sanctions

Article 11—Attempt and Aiding or Abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2–10 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12—Corporate Liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:
 - a. a power of representation of the legal person;
 - b. an authority to take decisions on behalf of the legal person;
 - c. an authority to exercise control within the legal person.
2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that

a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13—Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2-11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2—Procedural Law

Title 1—Common Provisions

Article 14—Scope of Procedural Provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:
 - a. the criminal offences established in accordance with articles 2–11 of this Convention;

- b. other criminal offences committed by means of a computer system; and
 - c. the collection of evidence in electronic form of a criminal offence.
- 3. a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
- b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system
 - i. is being operated for the benefit of a closed group of users, and
 - ii. does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15—Conditions and Safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it

has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Title 2—Expedited Preservation of Stored Computer Data

Article 16—Expedited Preservation of Stored Computer Data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17—Expedited Preservation and Partial Disclosure of Traffic Data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
 - a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
 - b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3—Production Order

Article 18—Production Order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
 - a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

- b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control;
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3. For the purpose of this article, "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:
 - a. the type of the communication service used, the technical provisions taken thereto and the period of service;
 - b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
 - c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Title 4—Search and Seizure of Stored Computer Data

Article 19—Search and Seizure of Stored Computer Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
 - a. a computer system or part of it and computer data stored therein; and
 - b. computer-data storage medium in which computer data may be stored in its territory.
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another

computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
 - a. seize or similarly secure a computer system or part of it or a computer data storage medium;
 - b. make and retain a copy of those computer data;
 - c. maintain the integrity of the relevant stored computer data; and
 - d. render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5—Real-time collection of computer data

Article 20—Real-time Collection of Traffic Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
 - a. collect or record through application of technical means on the territory of that Party, and
 - b. compel a service provider, within its existing technical capability, to:

- i. collect or record through application of technical means on the territory of that Party, or
 - ii. co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21—Interception of Content Data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
 - a. collect or record through application of technical means on the territory of that Party, and
 - b. compel a service provider, within its existing technical capability, to:
 - i. collect or record through application of technical means on the territory of that Party, or
 - ii. co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data of specified communications in its territory through application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3—Jurisdiction

Article 22—Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2–11 of this Convention, when the offence is committed:
 - a. in its territory; or
 - b. on board a ship flying the flag of that Party; or
 - c. on board an aircraft registered under the laws of that Party; or
 - d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b–(1) d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where

an alleged offender is present in its territory and it does not extradite him/ her to another Party, solely on the basis of his/ her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III—International Co-operation

Section 1—General Principles

Title 1—General Principles Relating to International Co-operation

Article 23—General Principles Relating to International Co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2—Principles Relating to Extradition

Article 24—Extradition

1. a. This article applies to extradition between Parties for the criminal offences established in accordance with

- Articles 2–11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
- b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
 2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
 3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
 4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.
 5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
 6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to

the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7. a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.
- b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3—General Principles Relating to Mutual Assistance

Article 25—General Principles Relating to Mutual Assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27–35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26—Spontaneous Information

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
2. Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4—Procedures Pertaining to Mutual Assistance
Requests in the Absence of Applicable International
Agreements

*Article 27—Procedures Pertaining to Mutual Assistance
Requests in the Absence of Applicable International
Agreements*

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2.
 - a. Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.
 - b. The central authorities shall communicate directly with each other.
 - c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.
 - d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to grounds for refusal available under Article 25, paragraph (4), refuse assistance if:
 - a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
 - b. it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
8. The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
9.
 - a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

- b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
- c. Where a request is made pursuant to sub-paragraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
- d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28—Confidentiality and Limitation on Use

- 1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation, is available unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2. The requested Party may make the furnishing of information or material in response to a request dependent on the condition that it is:
 - a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
 - b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.
4. Any Party that furnishes information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2—Specific Provisions

Title 1—Mutual Assistance Regarding Provisional Measures

Article 29—Expedited Preservation of Stored Computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under paragraph 1 shall specify:
 - a. the authority that is seeking the preservation;
 - b. the offence that is the subject of a criminal investigation or proceeding and a brief summary of related facts;
 - c. the stored computer data to be preserved and its relationship to the offence;
 - d. any available information to identify the custodian of the stored computer data or the location of the computer system;
 - e. the necessity of the preservation; and
 - f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or

similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data may, in respect of offences other than those established in accordance with Articles 2–11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
5. In addition, a request for preservation may only be refused if:
 - a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
 - b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 30—Expedited Disclosure of Preserved Traffic Data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if:
 - a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
 - b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2—Mutual Assistance Regarding Investigative Powers

Article 31—Mutual Assistance Regarding Accessing of Stored Computer Data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this Chapter.
3. The request shall be responded to on an expedited basis where:

- a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
- b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32—Trans-border Access to Stored Computer Data with Consent or where Publicly Available

A Party may, without obtaining the authorisation of another Party:

- a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33—Mutual Assistance Regarding the Real-time Collection of Traffic Data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed by the conditions and procedures provided for under domestic law.
2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34—Mutual Assistance Regarding the Interception of Content Data

The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data

of specified communications transmitted by means of a computer system to the extent permitted by their applicable treaties and domestic laws.

Title 3—24/7 Network

Article 35—24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:
 - a. provision of technical advice;
 - b. preservation of data pursuant to Articles 29 and 30; and
 - c. collection of evidence, giving of legal information, and locating of suspects.
2.
 - a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
 - b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter IV—Final Provisions

Article 36—Signature and Entry into Force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37—Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20 (d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force

on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38—Territorial Application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39—Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
 - the European Convention on Extradition opened for signature in Paris on 13 December 1957 (ETS No. 24);
 - the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 20 April 1959 (ETS No. 30);

- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).
- 2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
- 3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40—Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Article 2, Article 3, Article 6, paragraph 1 (b), Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

Article 41—Federal Clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide

for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42—Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43—Status and Withdrawal of Reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more

reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44—Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and, following consultation with the non-member State Parties to this Convention, may adopt the amendment.
4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45—Settlement of Disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other

peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46—Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:
 - a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
 - b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
 - c. consideration of possible supplementation or amendment of the Convention.
2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.
3. The European Committee on Crime Problems (CDPC) shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Article.

Article 47—Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48—Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

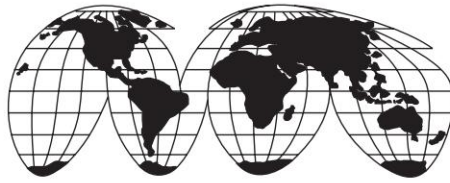
- a. any signature;
- b. the deposit of any instrument of ratification, acceptance, approval or accession;
- c. any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d. any declaration made under Article 40 or reservation made in accordance with Article 42;
- e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Convention on Cybercrime

<http://conventions.coe.int/Treaty/en/treaties/html/185.htm>



Appendix 10

Indian Computer Emergency Response Team



Mission

“To enhance the security of India’s Communications and Information Infrastructure through proactive action and effective collaboration”.



Charter

The purpose of CERT-In is, to become the nation’s most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur; the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.



Computer Security Incidents

The Internet continues to expand its reach and is becoming the most widely available communication medium on earth. Governments, corporations, banks, hospitals and schools conduct

their day-to-day businesses over the Internet through applications known as e-commerce and e-governance. The data that reside on and flow across the Internet range from banking and security transactions to proprietary data, personal correspondence and other data that must be protected during storage and transmission.

The Internet is easy and cheap to access but systems attached to it are not securely configured. Additionally, the underlying network protocols that support Internet communications are insecure. The combination of the data available on the network and the difficulties involved in protecting the data securely makes Internet systems vulnerable targets for attack. Unauthorised persons are able to get access into systems causing breach of security. Such incidents are known as Intrusions and the people gaining such access are referred to as Intruders or more commonly as Hackers. In early days of Internet, a hacker was someone who had a strong interest in computers, and who enjoyed experimenting with them. Today a Hacker means someone who gains unauthorized access to computers and networks with a view to cause disruption. He engages in network or host activity that potentially threatens the security of computer systems.

Computer Security Incident is any real or suspected adverse event in relation to the security of computer systems or networks. It is an act of violating explicit or implied security policy resulting in one or more of the following:

- Unauthorised access
- Denial of service/ disruption
- Unauthorised use of a system for processing or storage of data
- Changes to system software, hardware, firmware characteristics without the owner's knowledge

Hackers create malicious code in the form of viruses, worms and trojans; and propagate them over the Internet causing major disruption of servers. Critical infrastructures of nations such as telecommunication, transportation, and financial systems can

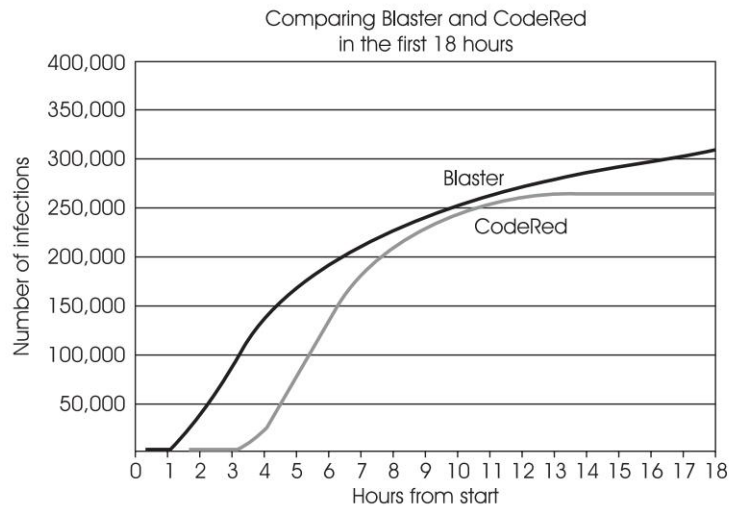
be threatened; Services can get disrupted; Major catastrophes can happen as a result of computer security incidents.

Computer crime and security surveys reveal that the dominant attacks include: denial-of-service, virus incidents, financial frauds and theft of proprietary information.

The findings also show the likely source of attacks as: foreign governments, foreign corporates, independent hackers and competitors.

The attacks are becoming more and more sophisticated. The body of technical knowledge available publicly enable attackers develop and launch viruses and worms much more rapidly causing substantial damage in the first few hours itself.

Information espionage and information warfare unleashed in the cyber space call for innovative ways to contain the threats and the resulting damage.



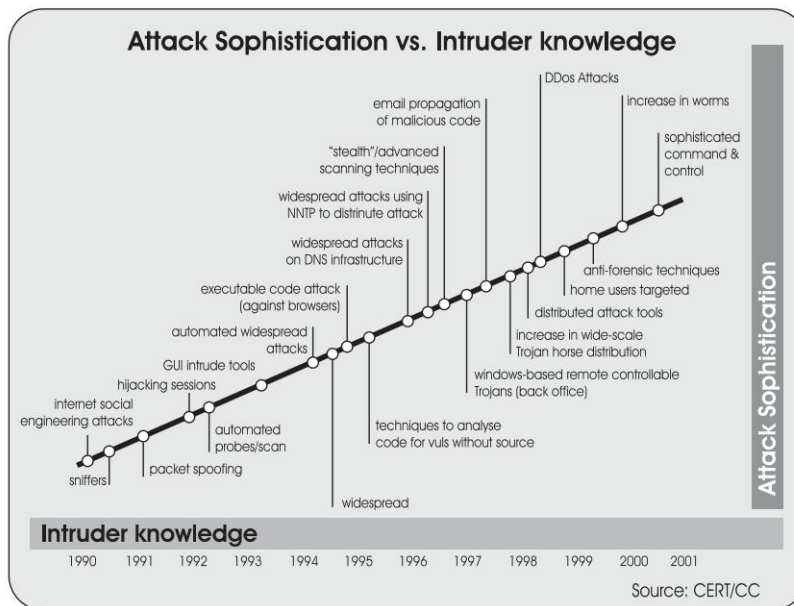
Source: CERT/CC



Computer Emergency Response Team

The concept of Computer Emergency Response Team (CERT)

was born in 1988, when the first “Internet Worm” incident occurred which resulted in a large percentage of the systems on the network being compromised and temporarily placed out of service. The CERT was meant to be a single point-of-contact for Internet security problems and was to act as a trusted clearing house for security information. The CERT Coordination Centre (CERT/CC) was formed to provide response on computer security incidents on the Internet. CERT provides an emergency response in the form of advice to the reporting organisation on how to handle an intrusion that may have affected their computer systems. Today CERT/CC has become the coordination centre for almost all the CERTs in the world.



When the first Internet Worm Incident occurred, the size of the network was estimated at 60,000 hosts. The January 2003 Internet Domain survey shows that there are 171.6 million hosts. Hundreds of CERTs have formed around the world since 1988 to take on the challenge of hacking and computer security incidents. With the Internet becoming pervasive, the community

of intruders and hackers has transformed into criminal groups those are engaging in terrorist activities and indulging in information warfare. More and more critical infrastructures, of not only the developed countries, but also those in the developing countries, depend on the information infrastructures. The need to deal with the attacks on such information infrastructures has become imperative for the protection of critical infrastructure of countries. The Indian Computer Emergency Response Team (CERT-In) has been established by the Department of Information Technology to be a part of the international CERT community with the specific mandate to respond to computer security incidents reported by the entire computer and networking community in the country.



CERT-In

Objectives

- Create an organisation that collaborates with other specialised sectoral and organisational CERTs in India to operate cohesively towards the mission.
- Serve as a central point for responding to computer security incidents as and when they occur.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Facilitate communication among experts working to solve computer security problems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Create a team of suitably qualified and empowered personnel to advance the mission of cyber security.

- To create trust in electronic environment.
- Establish international linkages in this area.

Constituency

The CERT-In's constituency is the Indian Cyber-community.

Functions

Reporting

- Central point for reporting incidents
- Database of incidents

Analysis

- Analysis of trends and patterns of intruder activity
- Develop preventive strategies for the whole constituency
- In-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident.

Response

- Incident response is a process devoted to restoring affected systems to operation.
- Send out recommendations for recovery from, and containment of damage caused by the incidents.
- Help the System Administrators take follow up action to prevent recurrence of similar incidents.

Role

Reactive Services

- Provide a single point of contact for reporting local problems.
- Assist the organisational constituency and general computing community in preventing and handling computer security incidents.

- Share information and lessons learned with CERT/ CC, other CERTs, response teams, organisations and sites.
- Incident Response.
- Provide a 24 × 7 security service.
- Offer recovery procedures.
- Artifact analysis
- Incident tracing

Proactive Services

- Issue security guidelines, advisories and timely advice.
- Vulnerability analysis and response
- Risk Analysis
- Security Product evaluation
- Collaboration with vendors
- National Repository of, and a referral agency for, cyber-intrusions.
- Profiling attackers.
- Conduct training, research and development.
- Interact with vendors and others at large to investigate and
- Provide solutions for incidents.



CERT-In

Types of Incidents & Level of Support

The order of incidents listed below shows the priority they receive from CERT-In. The support is provided in the form of advise over the phone, email, or fax to help resolve the incident at the earliest.

- Threats to the physical safety of human beings.
- Root or system-level attacks on any Management Information System, or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.

- Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.
- Denial-of-service attacks on any of the above.
- Large-scale attacks of any kind and/ or most frequent attacks, e.g. sniffing attacks, password-cracking attacks etc.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. netnews and e-mail forgery.
- Denial-of-service on individual user accounts, e.g. mail-bombing.
- Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.



CERT-In Activities

The Secure Network Operations Centre (S-NOC) for CERT-In has been established at the Department of Information Technology. The access is controlled through a combination of physical, proximity and biometric systems with the entire area being kept under CCTV surveillance. State-of-the art security systems are being used to secure the CERT-In computer network.

CERT-In is developing Security Guidelines for Operating Systems, Web Servers, Mail servers, Firewalls, Intrusion Detection Systems, Database Systems and other related areas. These guidelines are being issued in the form of best practices to advise the System Administrators of the entire cyber community in the country to take preventive steps so as to ensure that their computer systems and networks are not vulnerable to cyber attacks from intruders and hackers.

CERT-In is also developing Advisories, Alerts, Vulnerability Notes and Incident Notes, based on the practices followed by CERTs all over the world. It keeps track of latest activity on the Internet and issues the required advisories and vulnerability notes immediately.

A set of Standard Operating Procedures (SOPs) has been developed by CERT-In to help its teams discharge their functions effectively. A Vulnerability Database has also been developed for consultation and reference by Incident Response Teams to handle the incidents reported to them.

Appropriate Incident Response Teams have been created including the Triage Team with members who have expertise on different platforms such as Windows, Unix, Linux, IIS Web Server, Sendmail, Oracle DBMS, etc.

CERT-In receives incident reports through email, fax, telephone and web. It responds to the incidents with the objective of helping the reporting organisations take immediate steps to contain the damage, and to restore the systems to operation.

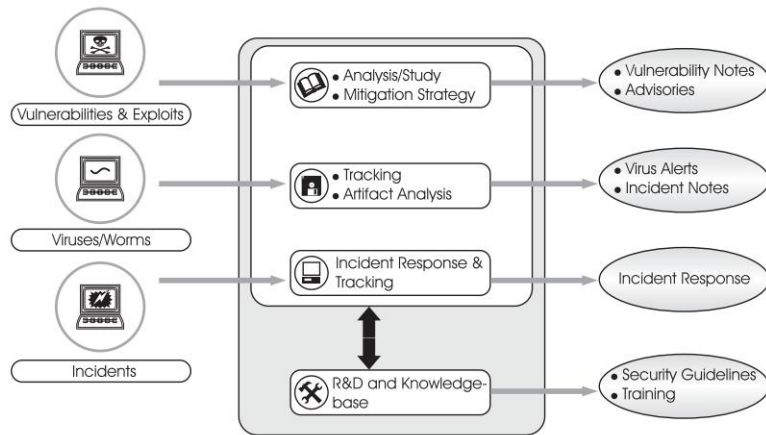
A Mirror CERT has also been funded by DIT at IISc, Bangalore. Major R&D activities related to vulnerabilities and artifact analysis, as also for preparing advanced software to guard against attacks, and to enable the computer systems for survivability in the network environment will be undertaken.

Ongoing Tasks

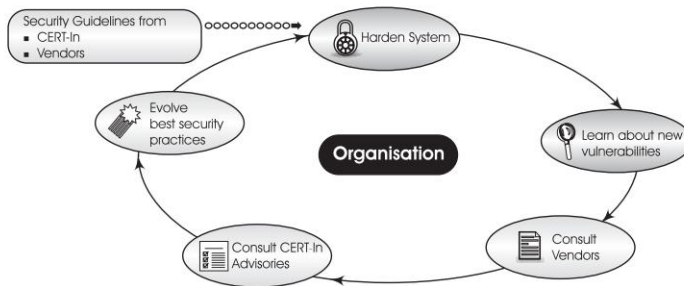
- Creation of internal Knowledgebase
- Formulation of Standard Operating Procedures
- Development of Incident Response & Tracking System
- Security Portal on the CERT-In website
- Issuance of advisories, vulnerability notes, incidents notes and security guidelines
- Vulnerability Database
- Preparation of training material for enhancing security awareness of System Administrators

- Work closely with CERT/ CC, FIRST, and other CERTs in India and abroad

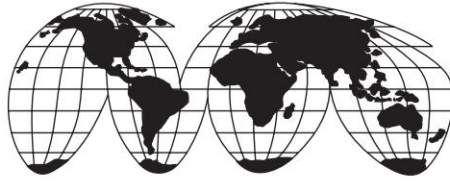
CERT-In Activities



Securing Systems: A Continuous Exercise for Organisations



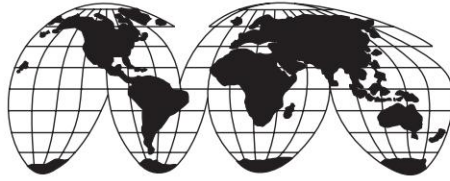
Indian Computer Emergency Response Team (CERT-In)
[http:// www.cert-in.org.in](http://www.cert-in.org.in)



Appendix 11

E-Commerce Sites of Interest

- Online bookstore www.amazon.com
Amazon.com
- Online marketplace eBay www.eBay.com
- eBusiness at Intel www.intel.com
- Online travel planning
and flight-booking www.expedia.com
- Portable music service www.napster.com
- Online portal of
The Times of India www.indiatimes.com
- News, information,
communication,
entertainment, and
shopping services www.rediff.com
- India's biggest
marketplace www.baazee.com
- Vertical portal for the
steel industry in India www.metaljunction.com
- E-Choupal of ITC [www.echoupal.com/ main.asp](http://www.echoupal.com/main.asp)
- E-Commerce at Amul www.amulb2b.com

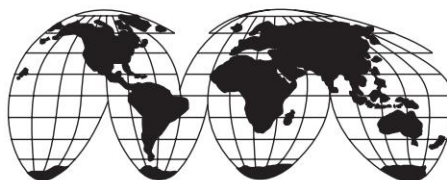


Appendix 12

E-Governance Sites of Interest

- US Electronic Government
www.firstgov.gov
- US General Services Administration
www.egov.gov
- Australia's Government Online
www.australia.gov.au
- Britain's Information Age Government
[www.direct.gov.uk/ Homepage/ fs/ en](http://www.direct.gov.uk/Homepage/fs/en)
- Singapore eGovernment
www.gov.sg
- United Kingdom Parliamentary Office of Science and Technology
[www.parliament.uk/ post/ egov.htm](http://www.parliament.uk/post/egov.htm)
- Department of Information Technology, Government of India
egov.mit.gov.in
- US General Services Administration
www.egov.gov
- National Informatics Centre
www.nic.in

- Indian Customs and Central Excise Gateway
icegate.gov.in
- Indian Railways' ticketing service
www.indianrailways.gov.in
www.irctc.co.in
- eSeva project of Government of Andhra Pradesh
www.e sevaonline.com
- Bhoomi—Government of Karnataka's Land Records project
www.revdept-01.kar.nic.in/ [Bhoomi](#)



Index

- Access Units (AU) 82
- Adjudication 313
- Administrative Directory
 - Management Domains (ADDMD) 98
- Administrative Management
 - Domain (ADMD) 86
- Amazon 36
- Amul 354
- Anonymous ftp server 123
- ANSI X12 Standards 147
- Applet 124
- Application Layer 78
- ARPANET 78
- Association 188
- Asymmetric 258, 261
- Authenticity 236, 257

- baazee.com 347
- Bar coding 191
- Bhoomi 376
- Bus 63
- Business Process Reengineering (BPR) 202, 211
- Business-to-Business (B2B) 18
- Business-to-Consumer (B2C) 18
- Buyers auction 350

- Cash on delivery (COD) 347
- Certificate policies 320
- Certificate Revocation List (CRL) 319
- Certification Authorities (CA) 270
- Certification Practice Statement (CPS) 310, 319
- Class A addresses 88
- Class B addresses 88
- Class C addresses 89
- Co-axial 67
- Code Division Multiple Access (CDMA) 71
- Component data elements 148
- Composite data element 148, 162
- Computer Emergency Response Team (CERT) 297, 298
- Computer forensics 291
- Confidentiality 236, 256
- Connection 167
- Consumer-to-Consumer (C2C) 18
- Controller of Certifying Authorities (CCA) 310
- Cross-certification 321
- Cryptography 258
- Cyber crimes 285
- Cyber forensics 290, 291
- Cyber frauds 286
- Cyber pornography 286
- Cyber Regulations Appellate Tribunal (CRAT) 313

- Data element 162
- Data Encryption Standard (DES) 259

- Data Interchange for Shipping (DISH) 147
- Data Link Layer 76
- Decryption 258
- Diffie-Helman 269
- Digital cash 335
- Digital Signature Algorithm (DSA) 266
- Digital Signature Certificates (DSCs) 309
- Digital signatures 262, 263, 264
- Directory D.97B 159
- Directory Information Base (DIB) 97
- Directory Systems Agent (DSA) 97
- Directory User Agents (DUA) 97
- Distinguished name 317
- Domain Name Server (DNS) 93
- Domain Name System 93
- Domain Names 29
- DOS 60

- E-Business 19
- E-cash 335
- E-Choupal 351
- E-Commerce 14
- E-Governance 20, 47, 358
- E-mail User Agent (UA) 100
- E-tailing 23
- EAN International 188
- EAN label 193
- EAN Location Numbers 194
- EAN-128 192
- EAN-13 190
- EAN-8 191
- EANCOM 188
- eBay 41
- EDI server 150
- EDI standards 147
- EDI translators 149
- EDIFACT message 159
- Electronic Authentication 303
- Electronic Cash 335
- Electronic Data Interchange (EDI) 15, 16, 141
- Electronic Funds Transfer (EFT) 16
- Electronic Mail 80, 81
- Electronic notaries 304
- Electronic payment systems 324
- Encryption 258
- Entities 75
- eSeva 373
- European Article Numbering Association (EAN) 187
- European Cyber Crimes Treaty 285
- Extensible Markup Language (XML) 181
- Extranet 138

- Fibre Channel over Internet Protocol (FCIP) 185
- Fibre Channel Protocol (FCP) 185
- File Transfer 80
- File Transfer Protocol (FTP) 114
- Firewalls 254
- Folders 100
- Frequency Division Multiple Access 70
- Frequency Time Division Multiple Access 71
- FTP 80, 117
- Fully Qualified Domain Name (FQDN) 93

- Generic Top Level Domains 94
- Google 40
- Government-to-citizen (G2C) 20
- Government-to-employee (G2E) 20
- Government-to-government (G2G) 20
- Growth indicators 29
- Guidelines for Internet banking 329

- Hackers 286
- Hacking 252
- Hash functions 266
- Hash value 294
- Hashing 294
- Host-based (HIDS) Intrusion Detection 255
- Hyperlinks 117
- Hypermedia 116
- Hypertext 116
- HyperText Markup Language (HTML) 117

-
- HyperText Transmission Protocol (HTTP) 117
 - HyperText Transport Protocol (HTTP) 123
 - iCERT CA 363
 - Indian Customs EDI Gateway (ICEGATE) 363
 - Indian Computer Emergency Response Team (CERT-In) 280
 - Indian Customs EDI System 362, 370
 - Indian Railways 370
 - Indiatimes.com 344
 - Information Technology (Certifying Authorities) Rul 302
 - Information Technology Act, 2000 282, 302
 - Integrity 236, 257
 - Intel 31
 - Inter-personal Messaging Protocol (P2) 84
 - Interchange 148, 165
 - International Article Numbering 187
 - International Data Encryption Algorithm (IDEA) 260
 - Internet 15, 103
 - Internet 2 125
 - Internet Assigned Numbers Authority (IANA) 106
 - Internet Banking 328
 - Internet Corporation for Assigned Names and Number 105
 - Internet Explorer 117
 - Internet Key Exchange (IKE) 277
 - Internet Mail Access Protocol 92
 - Internet Protocol (IP) 79
 - Internet Protocol Version 6 89
 - Internet Relay Chat 112
 - Internet SCSI 186
 - Internet Search 113
 - Intranet 129, 130
 - Intrusion Detection Systems (IDS) 254
 - IP addresses 88
 - IP spoofing 252
 - IPSec 277
 - (IRCTC) 370
 - iSCSI 186
 - Java 121, 124
 - Java Development Kit (JDK) 125
 - Just-In-Time (JIT) 144
 - Kerberos 274
 - Key 258
 - Key escrow 269
 - Key management 268
 - Key revocation 269
 - Layers 74
 - Lightweight Directory Access Protocol (LDAP) 99
 - Links 117
 - Local Area Networks 63
 - MD4 266
 - MD5 266
 - Mesh 65, 70
 - Message 148
 - Message Authentication Code (MAC) 261
 - Message digest 266
 - Message Handling Systems (MHS) 82
 - Message Store (MS) 81
 - Message Store Access Protocol (P7) 85
 - Message Transfer Agent 81
 - Message Transfer Protocol (P1) 84
 - Message Transfer System (MTS) 83
 - Metropolitan Area Network 63
 - Mozilla Fire Fox 117
 - MS-DOS 60
 - Multipurpose Internet Mail Extension (MIME) 91
 - Name servers 96
 - National E-Governance Action Plan 358
 - National repository 310
 - Netscape 117
 - Network 59

- Network Entry Points (NEP) 106
- Network forensics 291, 292
- Network layer 77
- Network topologies 63
- Non-repudiability 257
- Non-repudiation 236

- Online auctions 42
- Open Systems Interconnection(OSI)
Reference Model 74
- Opera 117
- Operating system 59
- Optical fibres 67
- Originator-Recipient Address 87
- Organisation for Data Exchange by
Tele Transmission 147
- Organisation for Economic Co-
operation and Develop 238

- PaisaPay 347
- PATRIOT Act 282, 288
- Payment Gateway 325
- PayPal 42, 330
- Pedi 151
- PGP 268
- Phishing 253
- Physical layer 76
- Point-of-Presence (POP) 106, 126
- Point-to-point 69
- Post Office Protocol (POP) 90, 92
- Presentation layer 78
- Private Directory Management
Domains (PRDMD) 98
- Private key 261
- Private Management Domain
(PRMD) 86
- Protocols 74
- Proxy Servers 136
- Public key 261
- Public Key Certificates (PKC) 269,
316
- Public key cryptosystems 261
- Public Key Infrastructure (PKI) 316

- Qualifier 162
- Quick response (QR) 145

- Radio Frequency Identification
(RFID) 196
- Rediff.com 346
- Remote Login 80
- Reservation Setup Protocol (RSVP)
119
- Reverse auction (RA) 350
- RFC-822 Addressing 95
- Ring 64
- Root Servers 96
- Routers 80
- RSA Algorithm 263

- S/ MIME 268
- Satellite communication 67
- Secure Electronic Transaction
(SET) 120
- Secure Electronic Transaction (SET)
Protocol 333
- Secure Hash Algorithm 266
- Secure HTTP (SHTTP) 255
- Secure Sockets Layer (SSL) 255
- Security Policy 278
- Segments 148, 159
- Serial Shipping Container Code
(SSCC) 193
- Session Layer 77
- Simple Mail Transfer Protocol
(SMTP) 80
- Single Channel Per Carrier 70
- Smart Card 336
- Solaris 60
- Spam 252
- Star 65, 70
- Steel Authority of India Ltd.
(SAIL) 348
- Storage Area Network (SAN) 184
- Strategic Alignment Model
(SAM) 207
- Submission and Delivery Protocol
(P3) 85
- SunOS 60
- Symmetric 258

- Tags 122
- TCP/ IP 78
- Telnet 80, 114

-
- The European Cyber Crimes Treaty 294
 - The HyperText Markup Language (HTML) 122
 - The Internet Architecture Board (IAB) 105
 - The Internet Engineering Task Force (IETF) 104
 - The Internet Research Task Force (IRTF) 104
 - The InterNIC 79
 - The IT Act, 2000 287
 - The Java virtual machine 125
 - Time Division Multiple Access 70
 - Trade Data Interchange (TDI) 147
 - Trading Partners 141
 - Transmission Control Protocol (TCP) 79
 - Transport layer 77
 - Tree 66
 - Triple-DES 260
 - Trojan 251
 - Trusted Third Parties (TTPs) 237
 - Tunneling 276
 - TWINS 373
 - Twisted pair 66

 - UN Trade Data Elements Dictionary 158
 - UN/ EDIFACT 147, 158
 - Uniform Communication Standard (UCS) 147
 - Uniform Resource Locator (URL) 117, 122

 - United Nations Standard Message (UNSM) 163, 164
 - Universal Product Code (UPC) 187
 - Unix 60
 - Unix-to-Unix Copy (UUCP) 108
 - UnixWare 60
 - UNTDED 158
 - User Agent (UA) 81, 155

 - Virtual Private Network (VPN) 234, 276
 - Virus 251
 - VSAT 69

 - Web browsers 121
 - WHOIS 115
 - Wide Area Network 63
 - Windows 60
 - Windows 2000 61
 - Windows 95 60
 - Windows 98 60
 - Windows Me 61
 - Windows Server 2003 61
 - Windows XP 61
 - World Wide Web (WWW) 115
 - Worm 251

 - X.400 81, 82
 - X.435 151
 - X.500 Directory Services 97
 - X.509 certificate format 270

 - Yahoo 40