From the Perspective of Digital Signatures & PKI

# INTRODUCTION & IT ACT

# Agenda

- Need of Digital Signatures
- Electronic Transactions
- IT Legislation
- IT Act 2000/2008
- CCA

# Emergence of e-Commerce

- Increased use of electronic means of transactions
- Bulk of transactions occur in G2B, B2G and B2B space
- Use of array of different technologies:
  - Web-based applications
  - Emails
  - Instant messaging
  - Mobile devices
- Importance of building a solid enabling regulatory framework for electronic transactions is evident

# Electronic Transactions ???

- Challenges posed by e-Commerce:
  - Classification difficulties: the virtual goods
  - New contract types: web hosting, web server etc.
  - Transactions taking place in open platforms
- … but the essence of business transactions remains the same.
- Conventional law has not become obsolete...
  - “On line” contracts are not different from “off line”
  - Medium of a transaction is generally irrelevant for the law.
- …and nevertheless, it requires some adaptation.

# Legal Obstacles to e-Commerce

- Legal concepts are based on the existence of a tangible medium:
  - “instrument”, “document”, “original”, “signature”

- Legal concepts based on geographic  location:
  - “delivery”, “receipt”, “dispatch”, “surrender”
- Functional Equivalence needs to be established between the Manual and Electronic media used (electronic records, signatures, documents, communication)

# Key Principle of IT Legislation - Functional Equivalence

- Paper-based requirements (“writing”, “record”, “signature”, “original”) specify certain purposes and functions
- Consider criteria necessary to replicate those functions and give electronic data the same level of recognition as information on paper

- A paper document signed by an individual fulfils the following criteria:
  - The document can be attributed to the individual as the signature is unique to the person (authenticity, non repudiation and integrity)
- If the electronic document can replicate these functions (e.g. by use of a Digital Signature Certificate attached to the document), it is functionally equivalent to the paper document

# Providing legal backing for Functional Equivalence

If certain conditions are fulfilled, the legal value of electronic transactions shall be equivalent to that of other forms of communication, such as the written form.

This can be achieved by a single enactment of Law without having to review every single piece of existing legislation establishing formal requirements

Indian IT Act, 2000 achieves this by defining the conditions by which equivalence can be ascertained between paper based and electronic documents

# Electronic Transactions - Example

**Individual Income tax filing - manual**

- Citizen obtains the paper Income Tax Return form
- Citizen fills up details in the ITR form
- Authenticates the ITR form by affixing signature
- Submits the ITR form at the respective Income Tax office and obtains acknowledgement

**Individual Income tax filing - electronic**

- Citize downloads the return preparation software tool from Income Tax portal
- Income details are entered in the tool and the tool generates the ITR XML
- The XML is signed by the citizen using Digital Signature Certificate and submitted at the Income Tax portal
- The Portal provides acknowledgement of submission

- Does the Digitally signed XML submission have the same legal recognition as the paper return with handwritten signature??
- Can the acknowledgement be used as proof of IT return filing??

# Illustrative Example – Electronic Evidence

A terrorist attack has occurred at one of the important landmarks in the capital. The terrorists involved were gunned down by police, and laptops and hard disks were seized from them.

After inspection of the contents of the laptop and the hard disks, police have found incriminating evidence relating to the conspirators behind the attack.

Police arrests the conspirators based on the evidence collected from the electronic data, and builds a case around the evidence.

But will the evidence hold good in a Court of Law?

Yes! With the admissibility of electronic evidence under section 65B of the Indian Evidence Act, 1872.

This scenario actually happened during the Parliament attack of 2001!!

# Other Principles of IT Legislation (1/2)

Technology Neutrality

- Law should address all existing technologies and those that will be developed in the future
- Equal treatment of paper-based and electronic transactions
- Equal treatment of different techniques (EDI, e-mail, Internet, telegram, telex, fax)

Law should not mention any specific technology, and should allow Rules to be drafted under the law to provide recognition to specific technologies (Case of electronic signatures)

# Other Principles of IT Legislation (2/2)

Party Autonomy

- Primacy of party agreement on whether and how to use e-commerce techniques
- Parties free to choose security level appropriate for their transactions

# Other Aspects of Regulatory Framework (1/2)

- Admissibility and evidential weight of e-communication:
  - ✓ Evidence of record may not be excluded solely because it is in electronic form, and evidential weight to be given according to reliability of data
- Data Protection and Privacy
  - ✓ Clear distinction between personal and public data
  - ✓ Protection for personal data
- Cyber crimes & Offences
  - ✓ Specifying different types of Cybercrimes
  - ✓ Empowerment of law enforcement agencies

# Other Aspects of Regulatory Framework (2/2)

- Intellectual Property Rights:
  - ✓ IPR for Software, source code, patents (for hardware & software), trademarks (in relation to domain names)
- Consumer protection:
  - ✓ Against invasion of privacy, spam, illegal or harmful content
- Liability and dispute settlement mechanisms
  - ✓ Adjudication mechanisms for cyber offences
- Jurisdiction & e-taxation
  - ✓ Jurisdiction for legal action and taxation

# IT Act 2000, its Amendments & related provisions

- Genesis of IT Act – UNCITRAL Model Law of e-Commerce
- Objectives of IT Act
- Snapshot of provisions of IT Act
- Admissibility of  electronic records

# Genesis of IT Act - The UNCITRAL Model Law

- As electronic transactions extends across national boundaries, there is a need for international harmonization in IT Laws
- The United Nations Commission on International Trade Law (UNCITRAL) is the legal body of the United Nations system in the field of international trade law
- UNCITRAL drafted the “UNCITRAL Model Law on Electronic Commerce - 1996” for adoption by countries
- The e-Commerce / IT Laws of most countries are modelled on UNCITRAL Model Law

# Adoption of UNCITRAL Model Law on e-Commerce

Australia (1999), Colombia * (1999), Bahrain (2002), Dominican Republic * (2002), Ecuador * (2002), France (2000), India* (IT Act 2000), Ireland (2000), Jordan (2000), Mauritius (2000), Mexico (2000), New Zealand (2000), Pakistan (2000), Panama * (2001), Philippines (2000), Republic of Korea (1999), Singapore (1998), Slovenia (2000), South Africa* (2002), Thailand (2003), and Venezuela (2001), United States (Uniform Electronic Transactions Act 1999)

* Except for provisions on electronic signatures

# Objectives of the Model Law

- To *facilitate* rather than *regulate* electronic commerce
- To *adapt* existing legal requirements
- To provide basic *legal validity* and raise *legal certainty*

- Basic Principles of Model Law
  - Functional Equivalence
  - Media and Technology Neutrality
  - Party Autonomy

Law to provide conditions for equivalence of handwritten (manual) and electronic records, signatures etc

Law to treat all technologies on an equal footing

Law to provide the transacting parties the autonomy to choose to use e-Commerce and decide security levels

# IT Act, 2000

- Came into effect from October 17th, 2000 on the lines of the UNCITRAL Model Law
- India is the 12th nation in the world to adopt digital signatures
- The Act applies to the whole of India and also applies to any offence or contravention there under committed outside India by any person *irrespective of his nationality*, if such act involves a computer, computer system or network located in India
- 90 Sections segregated into 13 Chapters and 2 Schedules
- IT Act 2000 was amended through the Information Technology Amendment Act, 2008 which came into effect from October 27, 2009

# Objectives of IT Act, 2000

- Legal Recognition for transactions carried out by means of electronic data interchange
  - Digital Signatures and Regulatory Regime for Digital Signatures
  - Admissibility of Electronic Documents at par with paper documents
- E-Governance
  - Use of electronic records & digital signatures by Government & its Agencies
- Define Civil wrongs, Offences, punishments
  - Investigation, Adjudication of Cyber crimes
  - Appeal provisions
- Amendment to the existing Acts to address IT Act provisions
  - Indian Penal Code & Indian Evidence Act - 1872
  - Banker’s Books Evidence Act – 1891 & Reserve Bank of India Act – 1934

# Snapshot of the IT Act and its provisions - 1

| Chapter | Coverage |
|---|---|
| Chapter I: Preliminary | • Act extends to the whole of India (Section 1)<br>• Exceptions to Applicability (Section 1(4)) |
| Chapter II: Digital Signature | • Authentication of electronic records (Section 3)<br>• Legal Framework for affixing Digital signature by use of asymmetric crypto system and hash function (Section 3) |
| Chapter III: Electronic Governance | • Legal recognition of electronic records (Section 4)<br>• Legal recognition of digital signatures (Section 5)<br>• Retention of electronic record (Section 7)<br>• Publication of Official Gazette in electronic form (Section 8) |

# Snapshot of the IT Act and its provisions - 2

| Chapter | Coverage |
|---|---|
| Chapter IV | • Attribution, Acknowledgement and Receipt of Electronic Documents |
| Chapter V | • Security procedure for electronic records and digital signature (Sections 14, 15, 16) |
| Chapter VI - VIII | • Licensing and Regulation of Certifying authorities for issuing digital signature certificates (Sections 17-34)<br>• Functions of Controller (Section 18)<br>• Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities (Section 19)<br>• Controller to act as repository of all digital signature certificates (Section 20) |

# Snapshot of the IT Act and its provisions - 3

| Chapter | Coverage |
|---|---|
| Chapter IX & XI | • Data Protection (Sections 43 & 66, 66B, 66C, & 66D)<br>• Various types of computer crimes defined and stringent penalties provided under the Act (Section 43, 43A and Sections 66, 66B, 66C, & 66D, 67, 67A, 67B, 72, 72A)<br>• Appointment of Adjudicating officer for holding inquiries under the Act (Sections 46 & 47) |
| Chapter X | • Establishment of Cyber Appellate Tribunal under the Act (Sections 48-56)<br>• Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court (Section 57)<br>• Appeal from order of Cyber Appellate Tribunal to High Court (Section 62) |

# Snapshot of the IT Act and its provisions - 4

| Chapter | Coverage |
|---|---|
| Chapter XI & XII | • Interception of information from computer to computer (Section 69) & Protection System (Section 70)<br>• Act to apply for offences or contraventions committed outside India (Section 75)<br>• Investigation of computer crimes to be investigated by an officer not below the rank of an Inspector<br>• Network service providers not to be liable in certain cases (Section 79) |
| Chapter XIII | • Power of police officers and other officers to enter into any public place and search and arrest without warrant (Section 80)<br>• Offences by the Companies (Section 85)<br>• Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (Section 88) |

# Snapshot of the IT Act and its provisions - 5

| Chapter | Coverage |
|---|---|
| Schedule I | • Amendments to the Indian Penal Code (IPC) |
| Schedule II | • Amendments to the Indian Evidence Act, 1872<br>• Clauses relating to admissibility of electronic records as evidence |
| Schedule III | • Amendments to the Banker’s Book of Evidence Act, 1891 |
| Schedule IV | • Amendments to the Reserve Bank of India Act, 1934 |

Schedules III and IV deleted in IT Act Amendment 2008

# IT Act 2008

- The Information Technology (Amendment) Act, 2008 amends the technology dependent approach.

- It introduces the concept of ***electronic signatures*** in addition to digital signatures.

# Overriding effect of the IT Act

- Section 81: The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

- Only exceptions to the overriding effect of the IT Act are the Copyright Act and Patents Act:

***“Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970”***

# Specifics of IT (Certifying Authorities) Rules, 2000

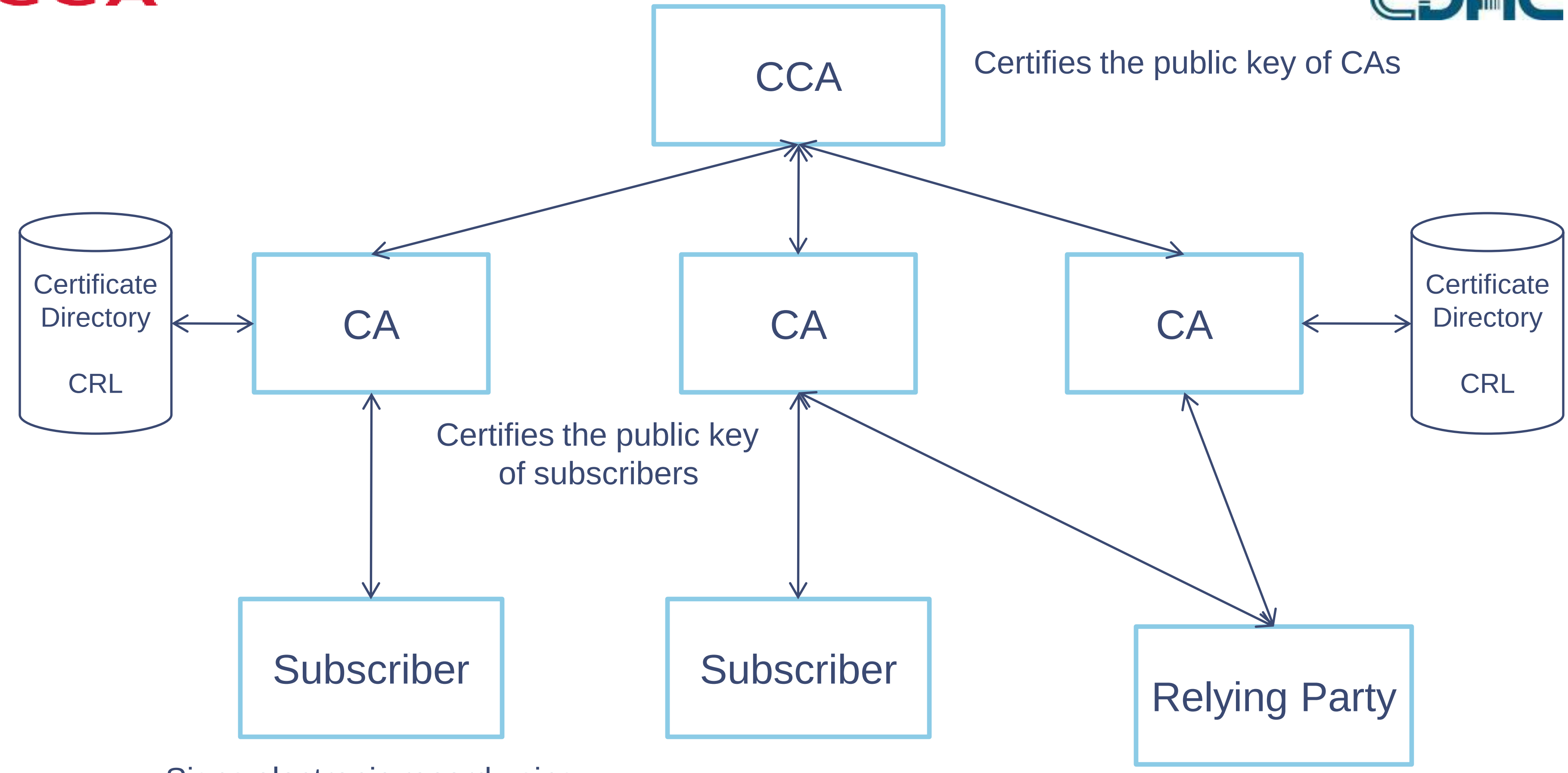
- Rules brought out by Central Government as per section 10 of IT Act
  - “Digital Signature shall be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again”;
  - Public Key Cryptography to be used for creation and verification of Digital Signatures
  - Prescribes ITU X.509 version 3 standard of Digital Signatures
  - Defines the Digital Signatures Regime including guidelines for Licensed Certifying Authorities

# Technology in IT Act

- An example of this is the MD5 hash algorithm that at one time was considered suitable.

- MD5 was prescribed as suitable by Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 .

# PKI Hierarchy in India



CCA

Certifies the public key of CAs

Certificate Directory

CRL

CA

CA

CA

Certificate Directory

CRL

Certifies the public key of subscribers

Subscriber

Subscriber

Relying Party

Signs electronic record using private key

Requests CA for certification of sender’s public key

# Digital Signature Regime in India

- Controller of Certifying Authorities
  - ✓ Set up as per IT Act, 2000 to license and regulate the working of Certifying Authorities
  - ✓ Lay down standards and conditions governing Certifying Authorities and specify various forms and content of Digital Signature Certificates
  - ✓ Certifies by the Public Key of the licensed CAs by operating the Root Certifying Authority of India (RCAI) key
- Licensed Certifying Authorities
  - ✓ Agencies authorised by CCA to issue Digital Signatures Certificates to end users and to certify the public key of the subscriber
- Registration Authorities
  - ✓ Agencies authorized by CA for operational activities like face to face verification, registration of certificate information etc
- Subscribers
  - ✓ End users who apply for Digital Signature Certificates to Licensed CAs

# Certifying Authorities in India

- Must be widely known and trusted
- Must have well defined Identification process before issuing the certificate
- Provides online access to all the certificates issued
- Provides online access to the list of certificates revoked (Certificate Revocation List)
- Displays online the license issued by the Controller
- Displays online approved Certification Practice Statement (CPS)
- Must adhere to IT Act/Rules/Regulations and Guidelines

**Licensed CAs**

- Safescrypt

- IDBRT

- NIC

-TCS

- MTNL

-GNFC

-E Mudhra CA

# Reference

- National e-Governance Plan
- NEGP Presentation Material