Indian IT Act: From the Perspective of Digital Signatures and PKI

Dr. Balaji Rajendran
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Policy Perspective

Policy Background

- UN Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996.
  - India is a signatory to this and therefore had to revise its laws accordingly
  - Indian IT Act follows the above model.
  - To facilitate e-commerce and e-governance the IT Bill, 1999 was introduced in the Indian Parliament
  - India enacted the Information Technology Act, 2000 that made changes to facilitate e-commerce and e-governance

Policy Background

- UNCITRAL Model law on e-commerce focuses on two basic functions of a signature
  - To identify the author of a document and
  - To confirm that the author approved the content of that document
- Functions of Article 7 of UNCITRAL Model Law
  - Identify a person
  - Associate that person with the content of a document
  - Provide certainty as to the personal involvement of that person in the act of signing
  - Attest to the intent of a person to endorse authorship of a text;
  - Attest to the intent of a person to associate itself with the content of a document written by someone else;
  - Attest to the fact that, and the time when a person had been at a given place

Adoption of UNCITRAL Model Law by other Nations

- 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

Legal aspects of Digital Signature as per Indian IT Act

Indian 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

Snapshot of IT Act and its Provisions

Chapter	Coverage
Chapter I: Preliminary	• Act extends to the whole of India (Section 1) • Exceptions to Applicability (Section 1(4))
Chapter II: Digital Signature	• Authentication of electronic records (Section 3) • 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) • Legal recognition of digital signatures (Section 5) • Retention of electronic record (Section 7) • Publication of Official Gazette in electronic form (Section 8)

Snapshot of IT Act and its Provisions

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) • Functions of Controller (Section 18) • Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities (Section 19) • Controller to act as repository of all digital signature certificates (Section 20)

Snapshot of IT Act and its Provisions

Chapter	Coverage
Chapter IX & XI	• Data Protection (Sections 43 & 66, 66B, 66C, & 66D) • 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) • 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) • Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court (Section 57) • Appeal from order of Cyber Appellate Tribunal to High Court (Section 62)

Snapshot of IT Act and its Provisions

Chapter	Coverage
Chapter XI & XII	• Interception of information from computer to computer (Section 69) & Protection System (Section 70) • Act to apply for offences or contraventions committed outside India (Section 75) • Investigation of computer crimes to be investigated by an officer not below the rank of an Inspector • 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) • Offences by the Companies (Section 85) • Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (Section 88)

Snapshot of IT Act and its Provisions

Chapter	Coverage
Schedule I	• Amendments to the Indian Penal Code (IPC)
Schedule II	• Amendments to the Indian Evidence Act, 1872 • 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

Objective of the Indian IT Act 2000

- To grant legal recognition to records maintained in electronic form
- To prescribe methods for authenticating electronic records
- To establish a hierarchical trust model with a root CA at the top - CCA to regulate the CAs
- To define computer system and computer network misuse and make it legally actionable

IT Act 2000

- IT Act 2000 made changes in the Law of Evidence, and provides
  - Legal recognition for electronic records and electronic signatures, which paves the way for
    - Legal recognition for transactions carried out by electronic communication
    - Acceptance of electronic filing of documents with the government agencies
    - Changes in the IPC and the Indian Evidence Act 1872 were made accordingly
    - IT Act 2000 has extra-territorial jurisdiction to cover any offense or contravention committed outside India

Authentication Method Prescribed by the Indian IT Act 2000

- The Act specifies that authentication must be by Digital Signatures based upon *Asymmetric Key Cryptography* and *Hash Functions*.
  - The National Root CA uses a 2048 bit RSA key pair
  - Other CA and end entities use 2048 bit RSA key pairs

Regulation of Certifying Authorities

- Under the Indian Law, section 35 of the IT (Amendment) Act, 2000 deals with certification and certifying authorities
  - The IT act mandates a hierarchical Trust Model
  - The IT Act provides the Controller for Certifying Authorities (CCA) to license and regulate the working of CA.
  - The CCA operates RCAI for certifying (signing) the public keys of CA's using it private key

IT Act 2000 on CCA and CAs

- IT Act 2000 recognizes even foreign CAs and gives the power to the CCA to decide on the same
  - CCA can also revoke the certificate for violation in any restriction or condition on which it was recognized by giving reasons in writing.

Indian IT Act (Amended 2008)

- IT Act 2000 took a technology-specific approach for electronic authentication, which was amended in 2008
  - For instance, MD5 hash algorithm was prescribed in Rule 6 of IT Act 2000
  - The term 'Digital Signature' is now superseded by 'Electronic Signature'
    - Electronic signature is a generalized term; while Digital signature is application of cryptographic techniques to avail a reliable electronic signature
    - Digital Signatures are therefore one type of electronic signature.
- A subscriber may authenticate any electronic record by **such electronic signature** or electronic authentication technique which is considered **reliable**

IT Act (Amended) 2008

- The signature creation data or the authentication data are within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;
- The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
- Any alteration to the electronic signature made after affixing such signature is detectable;
- Any alteration to the information made after its authentication by electronic signature is detectable;

IT Act - Digital Signature

- A 'Digital Signature' means an electronic signature created by transforming a data message using a message digest function and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key, such that any person having the initial untransformed data message, the encrypted transformation, and the signer's corresponding public key can accurately determine:
  - (i) transformation was created using the private key that corresponds to the signer's public key; and
  - (ii) whether the initial data message has been altered since the transformation was made.

Legal Validity of e-Sign

- eSign process involves consumer consent, DSC generation, Digital Signature creation and affixing and DSC acceptance in accordance with provisions of Information Technology Act.
- The Electronic Signatures facilitated through e-Sign Service are legally valid provided the e-Sign signature framework is operated under the provisions of Second Schedule of the Information Technology Act and Guidelines issued by the CCA.
- Please refer *Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 – e-Authentication technique using Aadhaar e-KYC services.*

Summary

- PKI is an ecosystem comprising of Technology, Policy and Implementations
  - Digital Signatures provide **A**uthenticity, **I**ntegrity, and **N**on-Repudiation for electronic documents & transactions
  - Asymmetric Key system enables **C**onfidentiality

Thank You

pki@cdac.in