Subject : Commerce

Lesson : Information Technology Act - 2000

Course Developer : Nidhi Dhawan

College /Department: Zakir Husan College, University of Delhi

Table of Contents

Introduction

The Information Technology Act 2000 came into force on 17th Oct., 2000. It consists of 13 Chapters divided into 94 sections. The Act has four schedules on consequential amendments in respect of certain other Acts. Chapters I to VIII are mostly Digital signature related. Chapters IX to XIII are regarding penalties, offences, etc.

Information technology (IT), "as defined by the Information Technology Association of America (ITAA), is "the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware." IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and securely retrieve information".

Objects and Reasons:

The Information Technology Act, 2000 provides legal recognition for transactions carried out electronically or by other means as an alternative to paper-based transactions.

The need for designing the Information Technology Act, 2000 was to give boost to e-transactions, e-commerce and similar activities associated with commerce and trade and to facilitate e- governance thus making a trouble free interaction of between citizens and government offices.

The inspiration for the ACT was a Model Law about electronic commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996. The ACT was passed in the year 2000 as Information Technology ACT, 2000.

The Information Technology Act, 2000 has introduced for the first time in India, a range of e-commerce and Internet related criminal offences, and executive powers that will significantly impair the rights of privacy and free speech of both citizens of India and of other countries.

E-Commerce refers to the trading of goods over the internet. It refers to the business transacted electronically. It is an online buying and selling of products and services for value using Internet Technologies such as e-mail, www, web browsing, etc. **The IT Act has been designed to give boost to electronic commerce, e-transactions and also to facilitate e-Governance by means of electronic records.**

For commercial transcations, signed and written documents were traditionally used as an evidence as also required by an indian law. Authentication of the document and at the same time to identify and bind the person who signs the documet is the major requirement.

In todays world, where everything is communicated online and also all the contracts are completed through electronic communication process, it is important to sign them also digitally fo the purpose of authentication and so is the need for cyber laws has arisen.

Applicability of the Act

"The Act extends to the whole of India (including Jammu and Kashmir). It applies also to any offence or contravention committed outside India by any person, irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India."

Figure: The Act

Exceptions to the Act

Exceptions [Sec 1(14)] "the provisions of the IT Act shall not apply to the following documents:

"Negotiable Instruments" under the Negotiable Instruments Act, 1881.

"Power of Attorney" under the Powers of Attorney Act, 1882.

"Trusts" define in section 3 of the Indian Trusts Act,1882.

"Will" define in clause (h) of Sec(2) of the Indian Succession Act, 1925 including any other testamentary dispositions;

Entering into a contract for sale or conveyance of immovable property or any interest in such property.

Any such class or document which Central Government may notify".

Basic Characteristics of the Act

The basic characteristics of the ACT are stated as follows:

a. Extends to the whole of India.
b. Validating all electronic communication contracts legally.
c. Digital signatures legal recognition and security procedures for them is provided for.
d. Use of cryptography for digital signatures.
e. Controller of Certifying Authorities appointment for the grant of license, for certifying keys, for maintaining repositories of digital signaturs and regulating the Certifying Authorities.
f. Computer related crimes are mentioned in the ACT and accordingly penalties are defined.
g. Appointment of Adjudicating Officer
h. Establishment of Cyber Regulatory Appellate Tribunal under the Act.
i. ACT for offences or contraventions committed outside India.
j. No liability of Network service providers in certain cases.
k. Police officers right to inspect and search
l. Advisory Committee to advise the Central Government and the Controller.

Objectives of the Act

The Information Technology (IT) Act, 2000, provides a framework to promote electronic communications in secured environment legally. Information stored in electronic form has many advantages. It is cheaper, creates paper free environment, easier to store and retrieve. But due to lack of appropriate legal framework and security of transactions, users are reluctant to conduct business online. IT Act provides for a regulatory regime to facilitate reliable e-commerce and e-governance. **The basic objectives of the IT Act are stated as under:**

1. Legal recognition of Electronic records.
2. Legal recognition of digital signatures.
3. Secured electronic communication
4. Accesing and retrieving records electronically
5. Submission of contracts and records electronically
6. Use of authentication in case of digital signatures
7. Message integrity by maintaining all standards uniformily
8. Use of electronic means for acceptance of contracts and their publication in official gazette
9. To prevent all types of crimes related to electronic records such as fraud, forgery etc

Briefly stated, the IT Act mainly contains provisions to e-commerce, e-governance, and electronic record and digital signature.

Definitions

- **(Section 2)** some important definitions are given below for understanding the concepts and legislative intents. Some illustrations are also given below for the same purpose. These are:

Figure: Concepts and Legislative Intents

- **Access** means "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**";**

Illustration
Reena wants to use the computer system by instructing and communicating it through its logical, arithmetical, or memory functions. It includes the use of both the physical and virtual access.

- **Addressee "**means a person who is intended by the originator to receive the electronic record but does not include any intermediary";
- **Adjudicating officer** "means an adjudicating officer appointed under subsection (1) of section 46;"
- **Affixing digital signature "**means 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";

Illustration
Mina wants to authenticate its message to be sent by signing it electronically. She can make use of encryption technique to do the same.

- **Appropriate Government "**means as respects any matter,-

  Enumerated in List II of the Seventh Schedule to the Constitution, 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";

- **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";

Illustration

Mohan has sent a digitally signed message using his private key to the shyam and shyam has verified the same by using the public key. This is a dual-key approach where one key (private key) is used to encrypt and other key (public key) to decrypt.

- **Certifying Authority** "means a person who has been granted a license to issue a Digital Signature Certificate under section 24";
- **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";

Illustration

The Certification Practice Statement explains the specific public certification services of ABC Company (a Certifying Authority). These services include certificate application, application validation, certificate issuance, acceptance, use, suspension, activation, revocation and renewal of a Digital Signature Certificate, operational security procedures for audit logging and records retention. It is a contractual obligation to be fulfilled by ABC Company vis- a - vis Controller and Subscriber.

- **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";

Figure: Definitions

- **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";

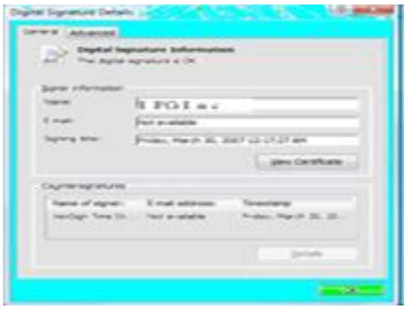
- **Computer resource** “means computer, computer system, computer network, data, computer data base or software”;
- **Computer system** “means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions”;
- **Controller “**means the Controller of Certifying Authorities appointed under sub-section (l) of section 17”;
- **Cyber Appellate Tribunal “**means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48”;

Illustration
PCS Company, a certifying authority wants to make an appeal against the order of the controller of certifying authority for the revocation of its certificate without being given an opportunity of being heard. PCS Company can make an appeal to the Cyber Appellate Tribunal.

- **Data** “means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized 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”;
- **"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 the section.
- The pictorial representation of Digital Signature details of the Company is shown below:

Illustration
In E-environment, Krisna authenticates the information send by him to his friend Mohan by using a digital signature technology(private key for encryption) and Mohan transforms it(public key for decryption) and a hash algorithm.

- **Digital Signature Certificate “**means a Digital Signature Certificate issued under sub-section (4) of section 35”;
- **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”;



Digital Signature Information

This digital signature is OK.

Signer information

Name: [illegible]

E-mail: Not available

Signing time: Friday, March 30, 2007 12:17:27 am

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	Friday, March 30, 20...

- **Electronic Gazette "**means the Official Gazette published in the electronic form";
- **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";
- **Function**, "in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer";
- **Information** "includes data, text, images, sound, voice, codes, computer program, software and databases or micro film or computer generated micro fiche":
- **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";
- **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";
- **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 there under";
- **License** "means a license granted to a Certifying Authority under section 24";
- **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";
- **Prescribed "**means prescribed by rules made under this Act";
- **Private Key** "means the key of a key pair used to create a digital signature";
- **Public key** "means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate";
- **Secure system "**means computer hardware, software, and procedure that- Are reasonably secure from unauthorized access and misuse; Provide a reasonable level of reliability and correct operation; Are reasonably suited to performing the intended functions; and Adhere to generally accepted security procedures";
- **Security procedure** "means the security procedure prescribed under section 16 by the Central Government";
- **"Subscriber** "means a person in whose name the Digital Signature Certificate is issued";
- **Verify "**in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether- the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature".

Secure E-Commerce

Basic Components of security The use of internet and its various sources for electronic communication calls for a security. All electronic communications must meet the fundamental requirements:

Figure: Secure E-Commerce

Authenticity-The sender authenticates the message so that recipient can determine the sender.

Message integrity- checks whether the message is received as it was sent or altered

Non-repudiation-It means sender cannot deny sending the message.

Privacy-The message must be secure from any unauthorized person.

Security Measures

What are the various ways to get the online security? The basic requirement of securing electronic transactions on the internet can be fulfilled by following one or more security measures. They can be adopted to ensure safe online communications during ecommerce.

These security measures are enumerated below:

Digital Signatures- "It 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."

Encryption- It is a procedure to convert a regular text into a coded or secret text.

Digital Signature Certificate-It is an instrument of trust identifying the subscriber over the networks.
All the above stated security measures are discussed hereunder in detail:

A. **Digital signature**

A signature used for authenticating the identity of the sender of the message on electronic communication in order to ensure that message or data has not been altered on network.

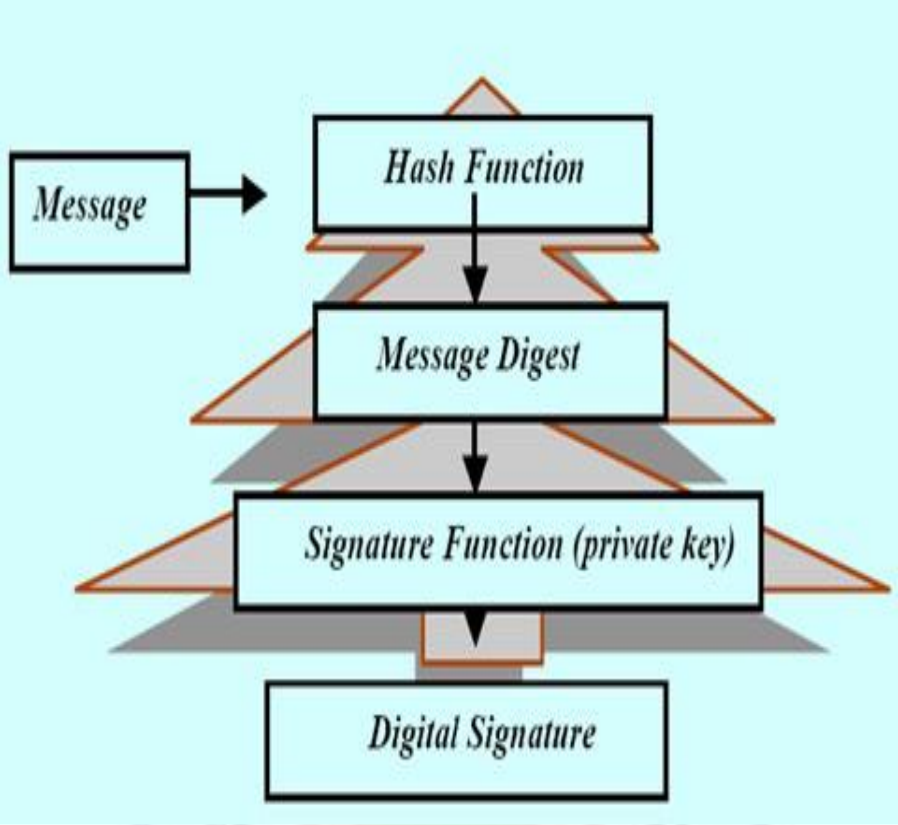
Ensure non-denial by the sender. He becomes committed to the contents of the document and the intentions expressed therein.

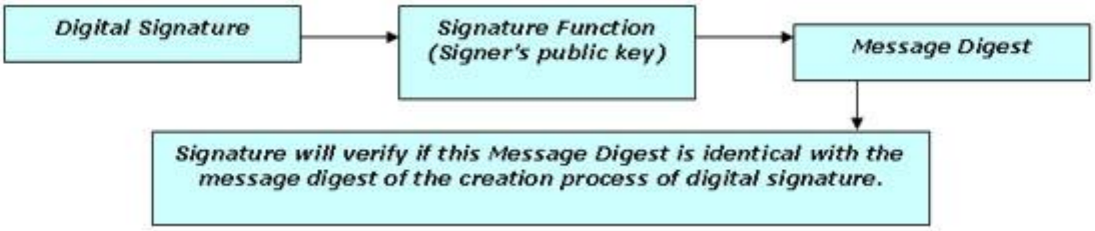
Certificate issuing authority digitally signs all the digital certificates. It helps everyone in verifying that the certificate is of true nature.

The procedure of creating a digital signature, sending it with the message and receiving it at the other end is explained with the help of an illustration.

Illustration

Rena sends a digitally signed message to sheikh by using a hash algorithm and applying a private key. Sheikh decrypts the message by applying signer's public key and computes a new hash result of the original message and comparing it with the original hash result extracted from the digital signature during the verification process.




Digital Signature
Signature Function
(Signer's public key)
Message Digest
Signature will verify if this Message Digest is identical with the message digest of the creation process of digital signature.

It is important to know about the digital signature technology being used in creating a digital signature.

(A) Digital Signature Technology

A digital signature is not a digitized code or image of a handwritten signature. **It is a block of data at the end of the electronic message that attest to the authenticity of the said message.** It is unique to its message. Digital signatures are actual transformation of an electronic message using cryptography. It is used to protect e-mail messages, credit card information, and corporate data.

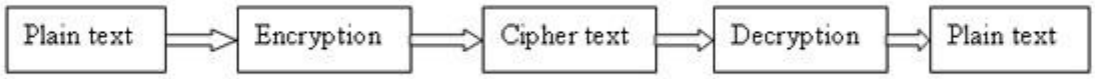
(B) Cryptography (Data Encryption Technique)

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

Figure: Digital Signature

(B) Cryptography (Data Encryption Technique)

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.



Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. It is a procedure to convert a regular text into a coded or secret text. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information; usually referred to as **a key** (Key is a combination of digits representing a huge number generated by mathematical formulae.) Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. **A basic task in cryptography is to enable users to communicate securely over an insecure channel in a way that guarantees their transmissions privacy and authenticity. Providing privacy and authenticity remains a central goal for cryptographic protocols.**

Cryptography has also two types.

Kinds of cryptography: There are basically two kinds of cryptography in use.

I Secret key (symmetric)

With secret key, the same key is used to encrypt information and decrypt information. Hence the operation is symmetric. With secret key systems you don't know who sent the message or if it is for a specific recipient, because anyone with the secret key could create or read the message.

II Public/private key (asymmetric)

An algorithm generates two different and related keys: public and private key.
(1)”Private Key" for creating a digital signature;

(2)"Public key" for verifying a digital signature.

For encryption, one key is used out of the two keys and other key is used for decryption. This is called the assymmetric operation of the keys. Everyone can use your public key by encrypting the document to be sent to you and then you can decrypt it with using your private key. In the same way, one can use its private key for encrypting the document and sending it and the reciever can decrypt it by using ones public key.

Use of cryptography for digital signatures is done with a view to highly secure the information transmission on the internet. This is explained below:

Digital Signature Using Encryption Technique:

Digital signatures are actual transformation of an electronic message using cryptography. it enables security by providing authentication of the sender, the message integrity and the receiving party identity.

After becoming aware of the techniques used in securing the message or any information in the electronic environment with the help of digital signature, it is important to know the procedure involved in the creation and verification of digital signature. They are enumerated below:

Creation of Digital Signature

According to the Act, Asymmetrical or ‘public key cryptography’ involving a pair of keys (private and public key is used) is used for creating a digital signature.

Steps

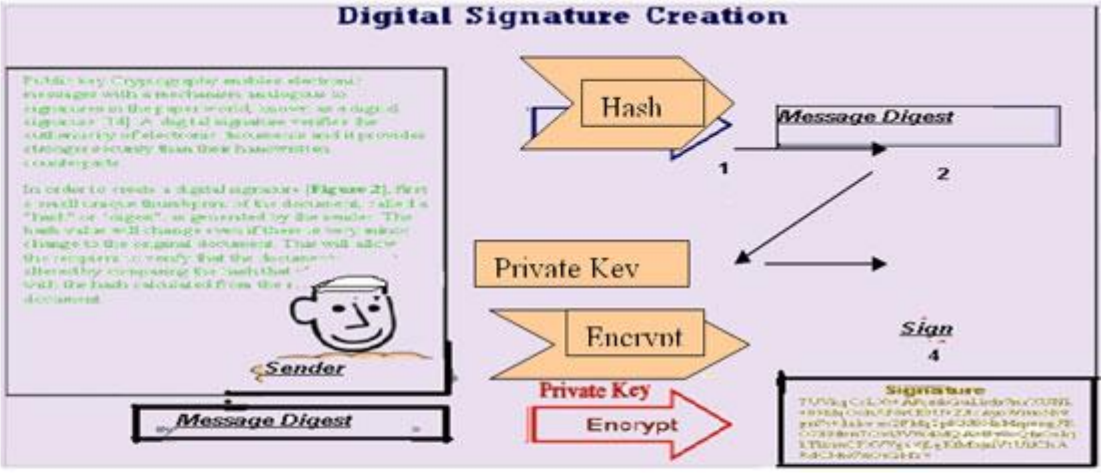
Signer demarcates the message.

Hash function in the software computes a hash result unique to the message.

The signer software then transforms (encrypts) the hash result into a digital signature using a signer’s private key.

Figure: Steps

Digital signature is unique to its message. Signer sends both digital signature and message to the recipient The pictorial representation of the creation of digital signature is shown below:



“A hash value (or simply hash), also called a message digest, is a number generated from a string of text”. The value of the hash is a small value than the text. The hash is created, encrypted and send with the message by the sender and is decrypted by the recipient giving him the new hash value. This new hash is compared with the senders hash value, if it turn out to be same, it means that message is same as it was sent otherwise altered.

Verification of Digital Signature

Once the message is received, the recipient verifies the identity of the sender of the message and also the integrity of the message. It also checks the non- repudiation which means, that later, sender cannot deny that he has not sent the message.

Steps:

Digital signature is received along with the message by the reciever

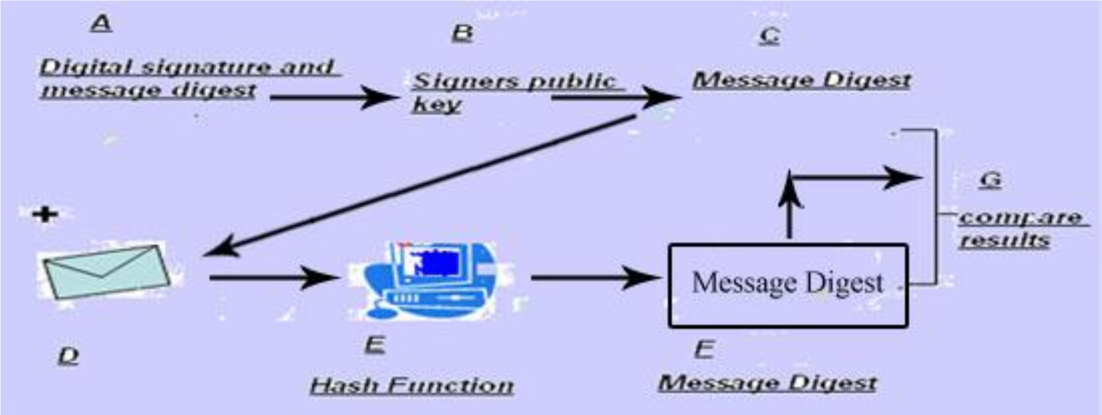
By using public key of the sender on the message, recipient gets the hash value and by using this value, he generates the new hash value.

The two values are used by recipient to check the integrity of the message. If the value is same, no alteration of the message has been done. And in case of different values, it means that the message is modified somewhere and then send, in such a case, the recipient can reject the message.

Digital signatures are created and verified using a data encryption technique known as cryptography. Digital Signature operates on online software driven space so, both the sender and the receiver must have digital signature software at their respective ends.

The entire process ensures high level of security to the transactions on the internet.

This is the pictorial representation of the verification of digital signature explained above:



Difference between the handwritten and digital signatures

In case, the private key is lost by the signer, then forged digital signatures can be created. Handwritten signatures can be attested by the Notary public/witnesses. Digital Signatures are certified by the certifying authority.

The purpose of both the handwritten and digital signature is to authenticate the message \document originated from the signer.

Legal Recognition of Digital Signatures

According to section 5 of the Act, "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, 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".

(C) Digital Signature Certificate

Digital Signature Certificate is an instrument of trust created by PKI (Public key infrastructure) system to provide for encryption and digital signature services. Digital signature an be ued legally only after obtaining a digital signature certificate from the certifyiyng authority.

CERTIFICATE

Certificate of Insurance as per form 51 in terms of rule 141 of Central Motor Vehicle rules 1989

Figure: Certificate

A certification authority (a third party) signs the digital signature certificate and their responsibility is to check the subcribers identity.

According to the Act, "a certificate consists of the following three elements:

Name and Other Extensions

This part of the certificate contains information about the entity to which the certificate is issued. Such information could include one's name, nationality and email address, details of ones work place etc. It could also include the DSC holders picture, a layout of his fingerprints, passport number etc.

Public Key Information

The DSC also contains information about the public key of the holder. The certificate acts to bind the public key of the holder to him and attribute information described above. The public key is usually a part of the asymmetric key of the signature holder usually an RSA key.

Certifying Authority (CA)

A CA is a relied-upon entity that issues, publishes, suspends and revokes digital certificates. The CA's role is to verify the identity of subscribers and provide certificate management services. A CA acts like a trusted electronic notary Public, telling everyone who the valid users are and what their digital signatures should look like.

DSC creates a "binding linkages" between the subscriber and the issuer and not only confirms the identity of the subscriber, but also certifies other relevant information such as subscriber's pubic key and bona fides of the issuer of the certificate. This certification is important for the relying party that trusts on the accuracy of the said certificate".

The elements of digital certificate includes the name of the individual or company, address, digital signaure, key, serial number and expiry date.

Summary

Introduction

The Information Technology Act came into force on 17th Oct., 2000

It is a first cyber law in India

Basis of the Act - Model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL)

The Act extends to the whole of India (including Jammu and Kashmir)

It gives boost to E-commerce, E-transactions and also facilitates E-governance by means of E-records.

Meaning ,Objectives and Some Important Features

“Act provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication

It aims to provide a legal and regulatory framework for promotion of e-Commerce and e-Governance

Electronic contracts will be legally valid

Legal recognition of digital signatures

Controller to certify the public keys of the Certifying Authorities (CAs)

Controller to act as repository of all digital signature certificates

Certifying Authorities to get License from the Controller to issue digital signature certificates”

Basic components of security for E-commerce

Authenticity

Message Integrity

Non-repudiation

Privacy

Methods adopted for securing online transactions

Digital Signatures

Encryption

Digital Signature Certificate

Digital Signature-Meaning

It is an electronic signature for authenticating the senders identity and integrity of the message.

Creation and verification of Digital Signature

Asymmetrical or ‘public key cryptography’ is used

Key pair is required

Private key

Public key

Encryption

It is a process of encrypting and decrypting the message.

Protects data against unauthorized access

Discloses unauthorized tampering

Authenticates the identity of the sender

Two types: symmetric and asymmetric cryptography

Digital Signature Certificate(DSC)

It is an instrument of trust

Three elements of DSC

Name and Other Extensions

Certifying Authority (CA)

Public Key Information

References

Aggarwal S.K. and Singhal K. (2006): *Business and Corporate Law, Galgotia Publications*, New Delhi, India Chapter 28

Kuchhal M.C. (2007): *Business Law*, Vikas Publishing House Pvt. Ltd. Delhi, India, Chapter 31.

Sharma Vakul (2007): *Information Technology Law and Practice law and emerging technology cyber law and E-commerce*, Universal Publishing Company, Delhi, India (Chapter1-9)

Goyal B.K. (2005): *Business Law*, R.Chand & Co, New Delhi, India, Chapter 35

Websites:

http://www.x5.net/faqs/crypto/q1.html

http://webopedia.internet.com/TERM/h/hashing.html

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html

http://searchsqlserver.techtarget.com/sDefinition/0,,sid87_gci212230,00.html

http://www.mca.gov.in/MinistryWebsite/dca/dsc/faq_dsc.html

http://www.cca.gov.in

http://images.google.co.in

Refer to bare ACT for the sections and the related site-
http://india.gov.in/outerwin.php?id=http://www.mit.gov.in/content/view-it-act-2000.