Digital Signatures

Creating Trust in Electronic Environment

Electronic Signatures

Creating trust in electronic environment involves assuring the transacting parties about the integrity 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. The paper based concepts of identification; declaration and proof are carried through the use of electronic signatures in electronic environment. .

For an electronic signature to be legally accepted it shall possesses the following requirements.

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

Information Technology Act

The IT Act, 2000 provides the required legal sanctity to Digital signatures based on asymmetric crypto systems. Digital signatures are accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents signed in the traditional way. The act provides the basic legal and administrative framework for e-commerce, and promotes its growth by creating trust in electronic environment. It is based on the Model Law for e-commerce proposed by UNCITRAL. The IT Act 2000 originally recognised only Primary Key Cryptography based Digital signatures as legal. The Information Technology (Amendment) Act, 2008, technology-neutral and recognises electronic signatures which are notified under the Rules. At present PKI based digital signature is the only technology, which qualifies as an electronic signature under the IT Act

Digital Signatures, a form of electronic signatures, are created and verified using **Public Key Cryptography** that is based on the concept of a key pair public and private - generated by a mathematical algorithm. The private key which is used to digitally sign a document is securely held by the owner, while the public key is made known to everyone for verifying the digital signature. Knowing the public key, one cannot compute the private key belonging to its owner.

Controller of Certifying Authorities

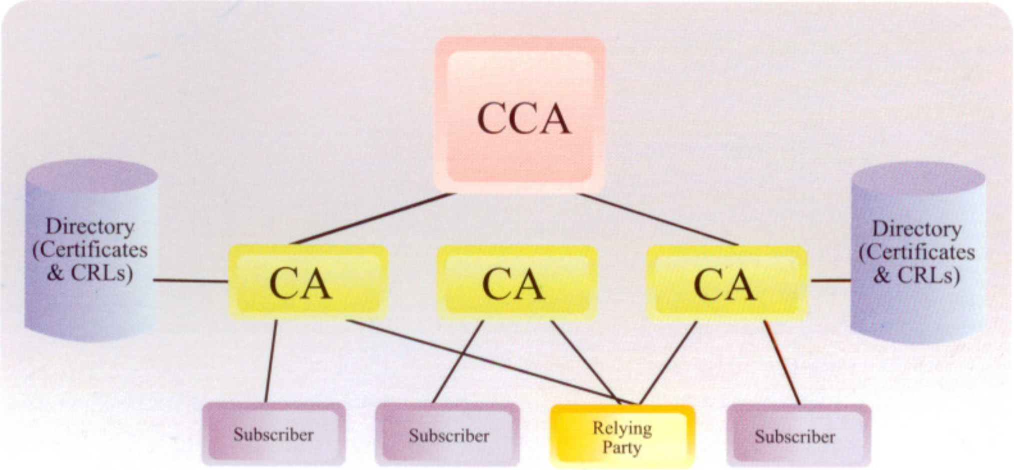
The IT Act provides for the **Controller of Certifying Authorities (CCA)** to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the Act are violated. **Certifying Authorities (CAs)** issue **Digital Signature Certificates** for authentication of users in cyberspace.

Digital Signature

- Digital signatures created and verified using Asymmetric keys.
- Public key cryptography based on Asymmetric Keys
  - An algorithm generates two different and related keys Public Key & Private Key
  - Public Key is used to verify the digital signature; also to encrypt text
  - Private key used to sign the text and create the digital signature; also to decrypt text

The CCA has prescribed technical standards for cryptography and physical security based on standards of ITU, IETE, IEEE and other international best practices. The CAs have to demonstrate compliance with these standards through the stringent audit procedure that has been put in place. The CAs also have to get their **Certification Practice Statement (CPS)** approved by the CCA. The CPS contains the practices and procedures followed by a CA. It deals with practices with regard to certificate issuance and user registration, certificate lifetime and revocation, identity verification procedure, class of certificates, certification publishing practices, and liability issues. An auditor, from the panel of auditors maintained by the CCA, conducts a detailed audit of the technical and physical infrastructure of the prospective applicants to ensure conformity with the technical standards and physical security standards laid down in the rules, Regulations and Guidelines under the Act and that its operations are in line with the approved CPS.

The **Public Key Infrastructure (PKI)** in the country is realized through the establishment of licensed CAs. The **India PKI** comprises the CCA and the CAs, with the CCA being at the root of the trust chain in India. As the foundation for secure Internet applications, it ensures authentic communications that cannot be repudiated.


CCA
Directory (Certificates & CRLs)
CA
CA
CA
Directory (Certificates & CRLs)
Subscriber
Subscriber
Relying Party
Subscriber

PKI Hierarchy

Public Key Infrastructure

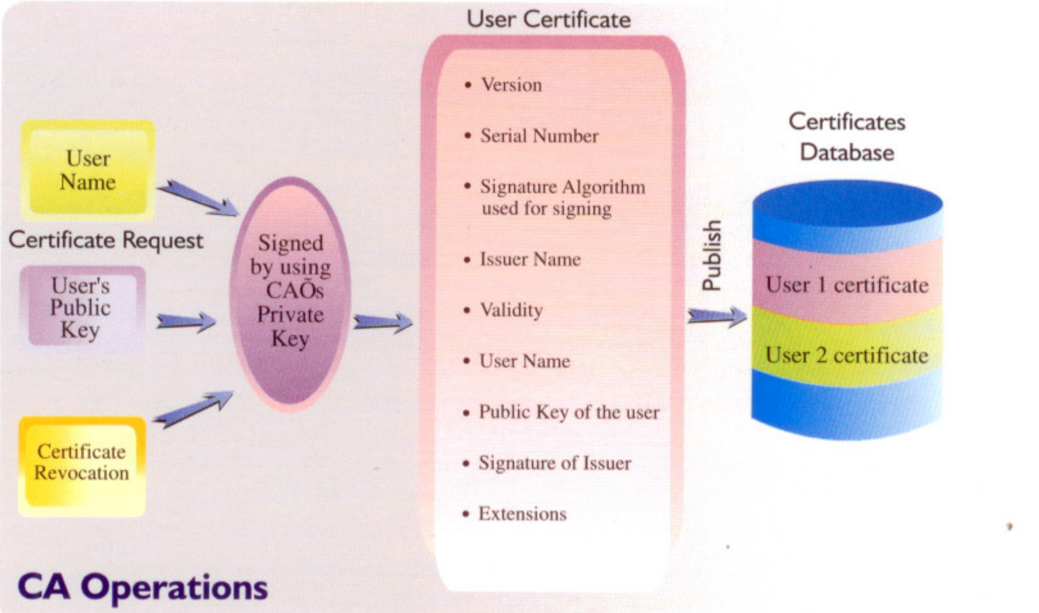
- Allow relying parties to have free access to the signer's public key.
- Public key is freely distributed while private key is securely held by the owner.
- Assurance that the public key corresponds to the signer's private key enables Trust between parties as if they know one another.

CAs, Certificates, CRLs

Certifying Authority

- A C A performs the following functions.
  - Reliably identifies persons applying for Digital Signature Certificates
  - Confirms the attribution of a public key to an identified physical person by means of a Digital Signature Certificate
  - Issues Digital Signature Certificates and Certificate Revocation Lists (CRL)
  - Always maintains online access to the Digital Signature Certificates and CRL and takes measures to operate their infrastructure in conformance with the IT Act, Rules, Regulations and Guidelines and also as per its approved Certification Practice Statement (CPS)
  - Provides the desired level of assurance to the relying parties for various classes of certificates issued to its subscribers and undertakes liability as per the approved CPS.

The public key is bound to the subscriber by a Digital Signature Certificate issued by a CA. The Digital Signature Certificate contains details about the subscriber identity, issuer CA details validity period etc. in addition to the subscriber's public key. Moreover, different classes of certificates provides different levels of assurance depending upon the identity verification method followed by the CA. A certificate may be revoked by a CA under certain conditions as detailed in the Act, in which case it must figure in the **Certificate Revocation List (CRL).** Subscribers and relying parties should access the **Directory of Certificates and CRLs** maintained by a CA to confirm the validity of a certificate.



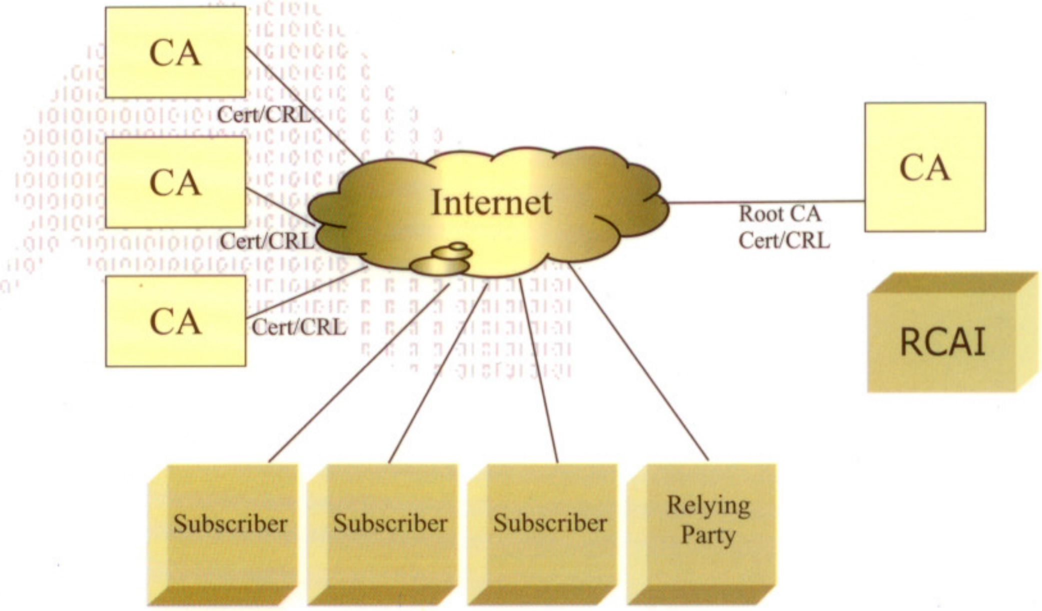
CA Operations

The Digital Signature Certificate issued by licensed CAs conforms to X.509 version 3 standard laid down by ITU, the CRL conforms to X.509 version 2 standard while the directory access is based on LDAP Version 3. Guidelines issued by CCA ensure interoperatibility between DSCs issued by different CAs. The certificates and CRLs issued by a CA are digitally signed by the CA using its own private key-the corresponding public key of which has been certified by the CCA. The CA protects its private key in a secure manner controlling access through a combination of physical, proximity & biometric systems, with additional hardware based security for the Private Key.

The CCA certifies the public keys of CAs using its own private key, which enables users in cyberspace to verify that the DSC has been issued by a licensed CA. The CCA operates its signing activity, through the Root

Certifying Authority of India (RCAI), in the Strong Room area, which has been built to the same standards as have been mandated for CAs.

All the above measures are essential for enhancing trust in electronic environment.



Classes of certificates

The Certifying Authorities issue Digital Signature Certificates, classes of which are based on identity verification methods. The DSCs issued fall under the following three classes

Class 1 Certificate: individuals/private subscribers- E-mail usage.

Class 2 Certificate: both business personnel and private individuals use.

Class 3 Certificate: issued to individuals as well as organizations, high assurance. Certificates, primarily intended for e-commerce applications, issued to individuals only on their personal physical appearance before the Certifying Authorities.

Awareness Programs

A number of nationally important e-Governance initiatives have already been embarked upon by the Government. Large-scale adoption of Digital Signatures will be one of the key success factors in these initiatives, as they will rely on Digital Signatures for their authentication requirements. Several Training programs for different user segments have been conducted nation-wide. On request, PKI & Digital Signature and cyber forensic awareness programmes are held for investigating agencies, judicial officers, and other agencies to benefit user organizations as well as service providers. Awareness generation programmes will continue to be supported by the office of CCA to promote the use of digital signatures in the country.

A flash demo on digital signature has been prepared and published on the web site of the office of CCA. Similarly tutorials for helping subscribers to know the process of digitally signing both documents and e-mail have been prepared and published on the office of CCAs web site.

India PKI Forum and ASIA PKI Forum

Inter-operability and mutual recognition of digital signature certificates between the CAs, within India, and with foreign CAs is an integral part of the IT Act. To address these, India PKI Forum has been established and is operating under active guidance from CCA for furthering the growth in use of Digital Signatures in the country. India has also become a principal Member of the Asia PKI Consortium. Asia PKI Consortium is one of the chapters of the Global PKI forum, which has chapters in different parts of the world. Its purpose is to promote joint work to secure interoperability among country's/area's PKI infrastructures in the Asia/Oceania Region.

PKI Standards

Public Key Cryptography

- RSA - Asymmetric Cryptosystem
- Diffie-Hellman-Asymmetric Cryptosystem
- Elliptic Curve Discrete Logarithm Cryptosystem

Digital Signature Standards

- RSA DSA and EC Signature Algorithms
- SHA-256, SHA-1-Hashing Algorithms

Directory Services (LDAP ver 3)

- X.500 for publication of Public Key Certificates and
- Certificate Revocation Lists
- X.509 version 3 Public Key Certificates
- X-509 version 2 Certificate Revocation Lists

PKCS family of standards for Public Key Cryptography from RSA

- PKCS#1- PKCS#15

Federal Information Processing Standards (FIPS)

- FIPS 140-1/2, Security Requirementof Cryptographic Modules

CONTROLLER OF CERTIFYING AUTHORITIES
6, CGO Complex, Electronics Niketan
Lodhi Road, New Delhi-110003
E-mail : info@cca.gov.in
Website : http://cca.gov.in