IT Act 2000
PKI Standards
RCAI
NRDC
CA Certificates
Auditors
Adjudicating Officers
E-Commerce
E-Governance
PKI Initiatives
E-Security
Cybercrimes
FAQ
CCA
Contact Us

Trust in electronic environment through digital signatures

PKI Framework under the IT Act

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment. The future of e-commerce and e-governance depends on the trust that the transacting parties place in the security of transmission and the content of communication.

Creating trust in 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. The paper based concepts of identification, declaration and proof are carried through the use of digital signatures in electronic environment. 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 generated by a mathematical algorithm, the public and private keys.

The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India (RCAI). The CCA also maintains the National Repository of Digital Certificates (NRDC), which contains all the certificates issued by all the CAs in the country.

CCA at the root of the trust chain in India.

Licensed CAs

- Safescrypt
- NIC
- IDRBT
- TCS
- MTNL
- Customs & Central Excise
- (n)Code Solutions CA (GNFC)

What's New

- Guidelines for Storage of Private

- Keys
- Audit frequency modifications for CA audit
- Empanelment of Auditors for CA audit
- OID Allocation to CAs
- Guidelines for NRDC submission by CAs
- Site Preparation Guidelines
- Information under RTI Act,2005
- NEW Tender for Servers in CCA office
- NEW Tender -Expression of interest

Page Last Modified on 15 Nov 2006