SOS POL. SC. & PUB. ADMN. ,
JIWAJI UNIVERSITY, GWALIOR (M.P.)

MBA HRD IV SEM
PAPER- E-BUSINESS & CYBER LAW(401)

TOPIC: ELECRONIC RECORDS & DIGITAL SIGNATURE

DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

DIGITAL SIGNATURE

- Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure.
- **CREATION OF DIGITAL SIGNATURE**
- To sign an electronic record or any other item of information the signer shall first apply the hash function in the signers software.
- The signers software transform the hash result into a digital signature using signers private key.
- The digital signature shall be attached to its electronic record and stored or transmitted with the electronic record.

- **Manner in which information be authenticated by means of digital signature :**
- A digital signature shall-

a. Be created and verified by cryptography

b. Use what is known as "PUBLIC KEY CRYPTOGRAPHY".

- **Verification of digital signature**
- Verification means to determine whether:-

a. The initial electronic record was affixed.

b. The initial electronic record is retained.

- DIGITAL SIGNATURE CERTIFICATE
- REPRESENATION UPON ISSUANCE OF DIGITAL SIGNATURE CERTIFICATE
- EXPIRY OF DIGITAL SIGNATURE CERTIFICATE
- FEES FOR ISSUE OF DIGITAL SIGNATURE CERTIFICATE
- CONTENT OF DIGITAL SIGNATURE CERTIFICATE

- GENERATION OF DIGITAL SIGNATURE CERTIFICATE
- COMPROMISE OF DIGITAL SIGNATURE CERTIFICATE
- SUSPENSION OF DIGITAL SIGNATURE CERTIFICATE.
- ARCHIVAL OF DIGITAL SIGNATURE CERTIFICATE

ELECTRONIC SIGNATURE

- Electronic signature means authentication of any electronic record by a subscriber of the electronic technique specified in the second schedule and includes digital signature.
- The electronic signature was adopted by the United Nation Commission on International Trade Law in the year 2001 which came into force from 27.10.2009

- **Rules In Respect Of Electronic Signature :**
- Electronic Signature Certificate
- Certification Practice Statement
- **SUBSCRIBER**
- Subscriber means a person in whose name the digital/electronic signature certificate is issued.
- The method used to verify and authenticate the identity of a subscriber is known as "Subscriber Identity Verification Method".
- **Duties Of Subscriber**

1. Generating key pair
2. On acceptance of Digital Signature Certificate
3. Control of private key

Electronic Governance & Electronic Records

Electronic Commerce

- EC transactions over the Internet include
  - Formation of Contracts
  - Delivery of Information and Services
  - Delivery of Content
- Future of Electronic Commerce depends on

  "the trust that the transacting parties place in the security of the transmission and content of their communications"

Electronic World

- Electronic document produced by a computer. Stored in digital form, and cannot be perceived without using a computer
  - It can be deleted, modified and rewritten without leaving a mark
  - Integrity of an electronic document is “genetically” impossible to verify
  - A copy is indistinguishable from the original
  - It can’t be sealed in the traditional way, where the author affixes his signature
- The functions of identification, declaration, proof of electronic documents carried out using a digital signature based on cryptography.

Electronic World

- Digital signatures created and verified using cryptography
- Public key System based on Asymmetric keys
  - An algorithm generates two different and related keys
    - Public key
    - Private Key
  - Private key used to digitally sign.
  - Public key used to verify.

Public Key Infrastructure

- Allow parties to have free access to the signer's public key
- This assures that the public key corresponds to the signer's private key
  - Trust between parties as if they know one another
- Parties with no trading partner agreements, operating on open networks, need to have highest level of trust in one another

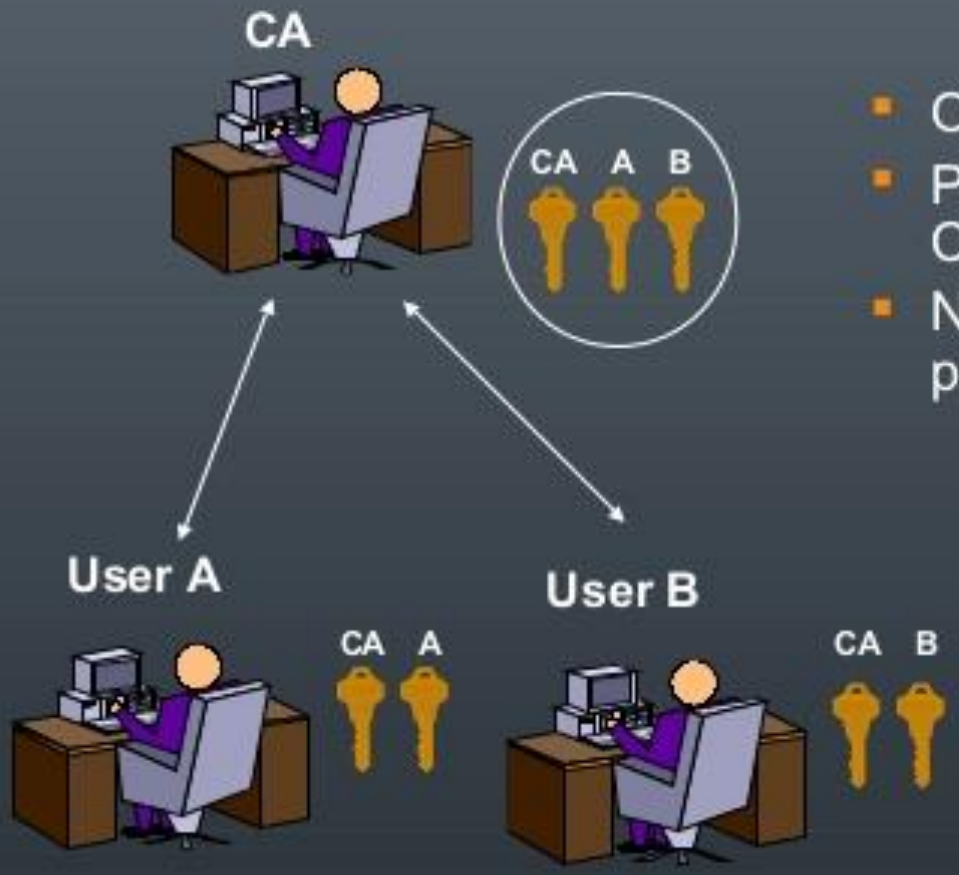
Public Key Infrastructure

- Allow parties to have free access to the signer's public key
- This assures that the public key corresponds to the signer's private key
  - Trust between parties as if they know one another
- Parties with no trading partner agreements, operating on open networks, need to have highest level of trust in one another

Role of the Government

- Government has to provide the definition of
  - the structure of PKI
  - the number of levels of authority and their juridical form (public or private certification)
  - which authorities are allowed to issue key pairs
  - the extent to which the use of cryptography should be authorised for confidentiality purposes
  - whether the Central Authority should have access to the encrypted information; when and how
  - the key length, its security standard and its time validity

Certificate based Key Management



- Operated by trusted-third party - CA
- Provides Trading Partners Certificates
- Notarises the relationship between a public key and its owner

Section 4- Legal recognition of Electronic Records

- If any information is required in printed or written form under any law the Information provided in electronic form, which is accessible so as to be usable for subsequent use, shall be deemed to satisfy the requirement of presenting the document in writing or printed form.

Sections 5, 6 & 7

- Legal recognition of Digital Signatures
- Use of Electronic Records in Government & Its Agencies
- Publications of rules and regulations in the Electronic Gazette.
- Retention of Electronic Records
- Accessibility of information, same format, particulars of dispatch, origin, destination, time stamp ,etc

CCA has to regulate the functioning of CAs in the country by-

- Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.
- Certifying the public keys of the CAs, i.e. their Digital Signature Certificates more commonly known as Public Key Certificates (PKCs).
- Laying down the standards to be maintained by the CAs,
- Addressing the issues related to the licensing process

THANK YOU!