Digital Signatures and PKI - II

Dr. Mohammed Misbahuddin
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Agenda

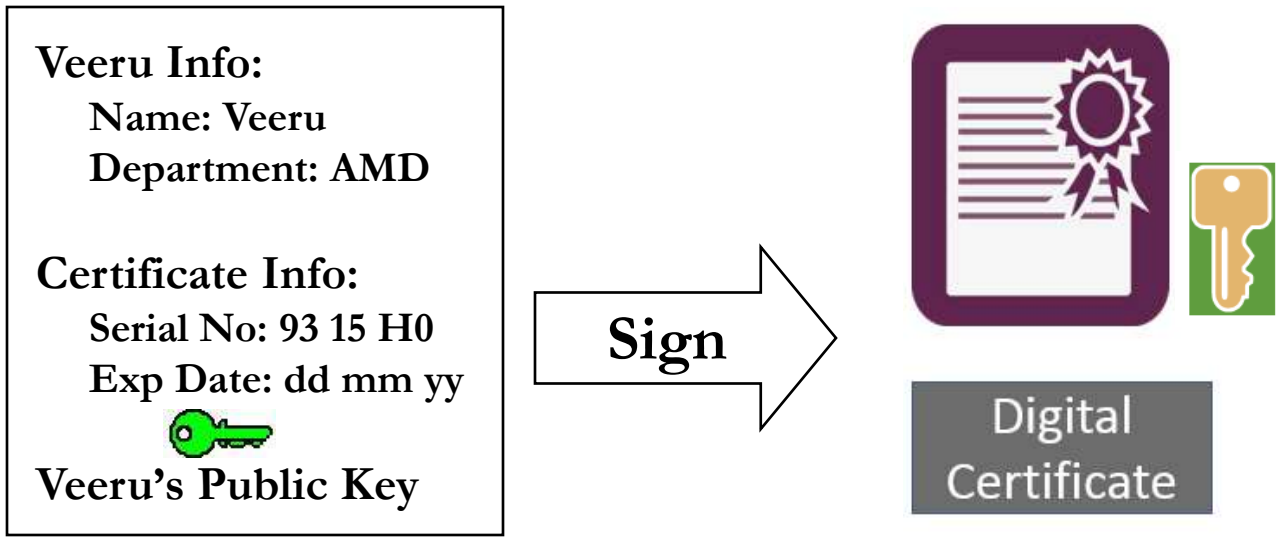
- ✓ Digital Certificate
- ✓ Certifying Authority
- ✓ Trust Model
- ✓ Certificate Issuance Process
- ✓ Types of Certificate
- ✓ Certificate Classes
- ✓ Certificate Life Cycle Management
- ✓ Certificate Validation Methods
- ✓ CRL
- ✓ Legal aspects
- ✓ PKI applications in India

Digital Signature Certificate (DSC)

What is Digital Signature Certificate (DSC)?

DSC is an electronic document used to prove ownership of a public key. The certificate includes

- Information about its owner's identity,
- Information about the key,
- The Digital Signature of an entity that has verified the certificate's contents are correct.



Certifying Authority (CA) ?

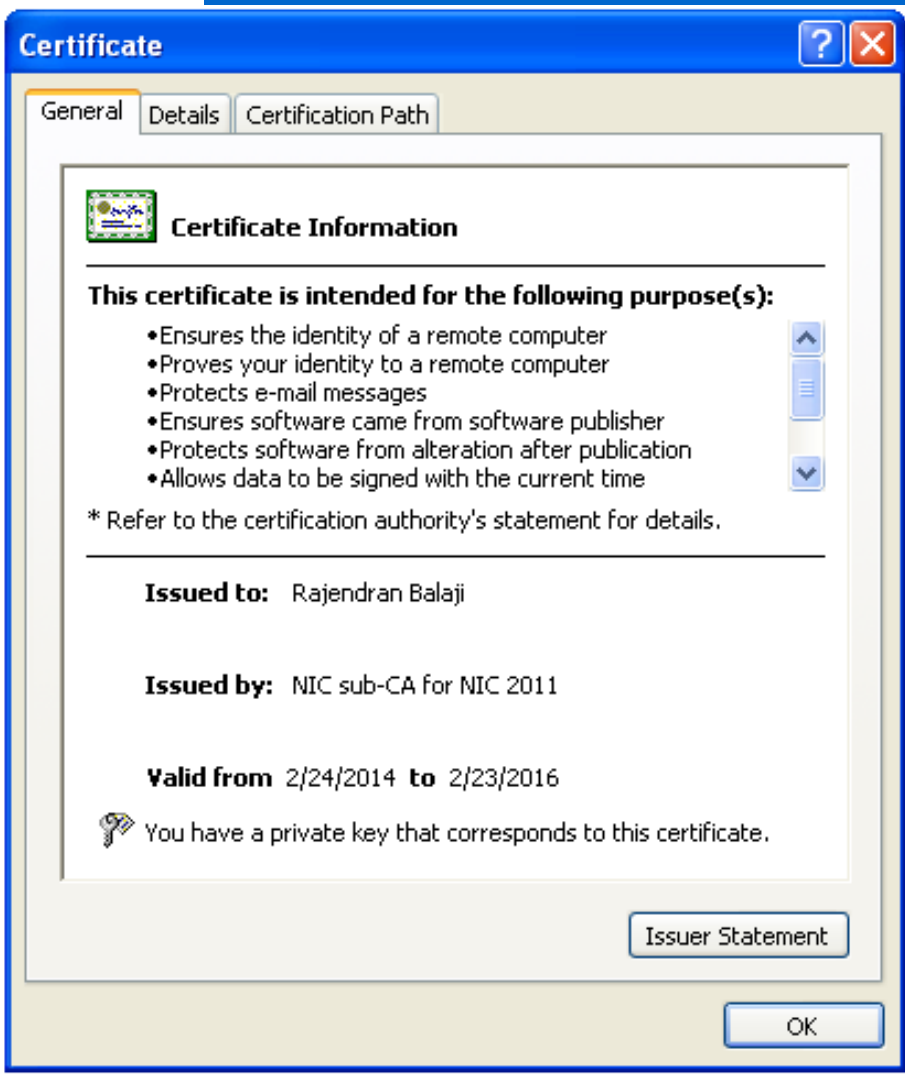
Certifying Authority (CA)

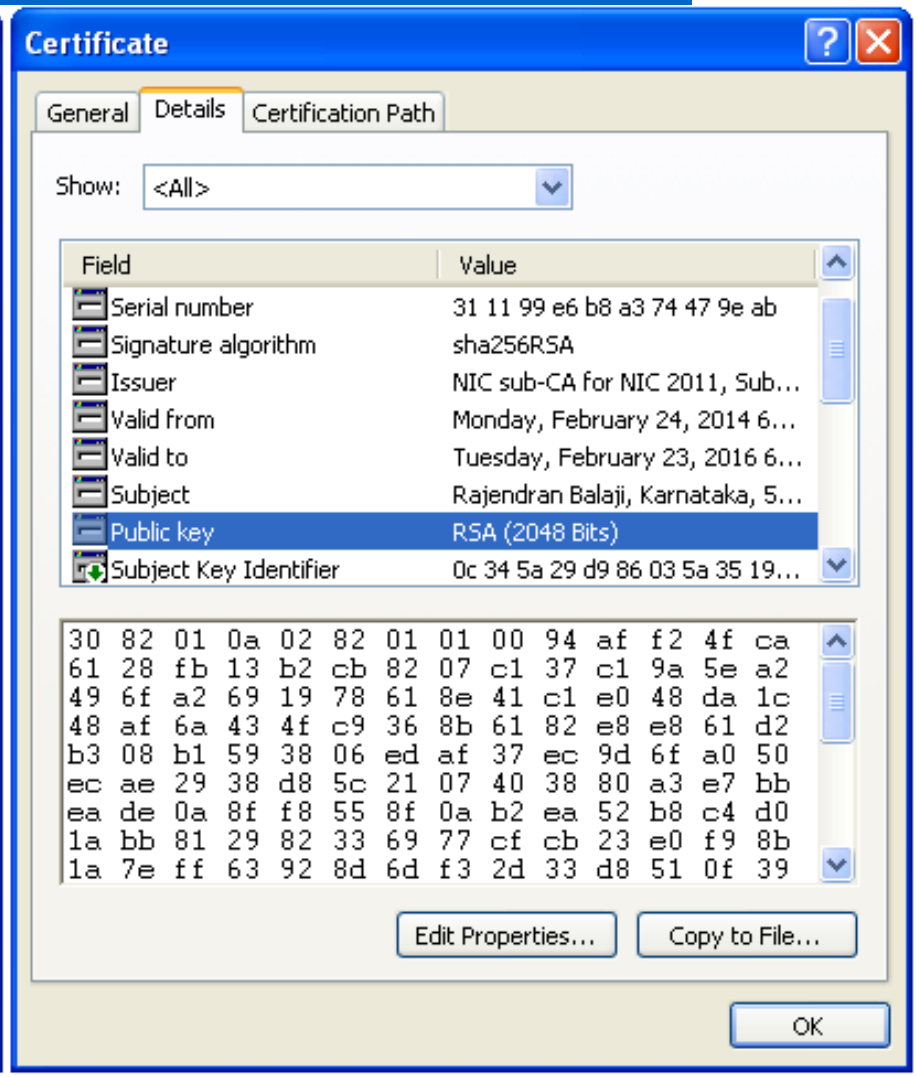
- Certifying authority is an entity which issues Digital Certificate
- It is a Trusted third party
- CA's are the important characteristics of Public Key Infrastructure (PKI)

Responsibilities of CA

- Verify the credentials of the person requesting for the certificate (RA's responsibility)
- Issue certificates
- Revoke certificate
- Generate and upload CRL

Sample Certificate





Smart Cards

- The Private key is generated in the crypto module residing in the smart card.
- The key is kept in the memory of the smart card.
- The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.
- The card gives mobility to the key and signing can be done on any system. (Having smart card reader)

Hardware Tokens

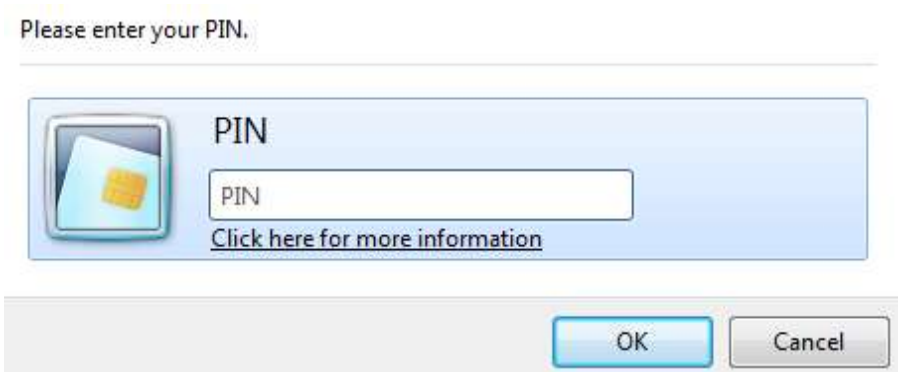
- They are similar to smart cards in functionality as
  - Key is generated inside the token.
  - Key is highly secured as it doesn't leave the token.
  - Highly portable.
  - Machine Independent.

- iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.

Private key protection

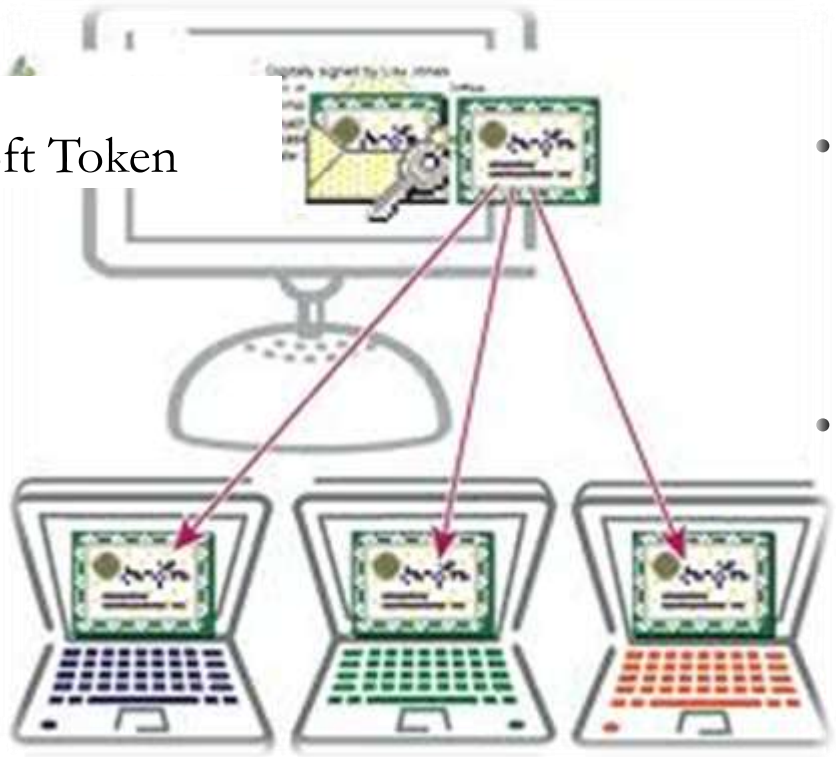
- The Private key generated is to be protected and kept secret. The responsibility of the secrecy of the key lies with the owner.

- The key is secured using
  - PIN Protected Soft token
  - Smart Cards
  - Hardware USB Tokens



PIN protected Soft Tokens

Soft Token



- The Private key is encrypted and kept on the Hard Disk in a file, this file is password protected.
- This forms the lowest level of security in protecting the key, as
  - The key is highly reachable.
  - PIN can be easily known or cracked.
- Soft tokens are not preferred because
  - The key becomes static and machine dependent.
  - The key is in a known file format.

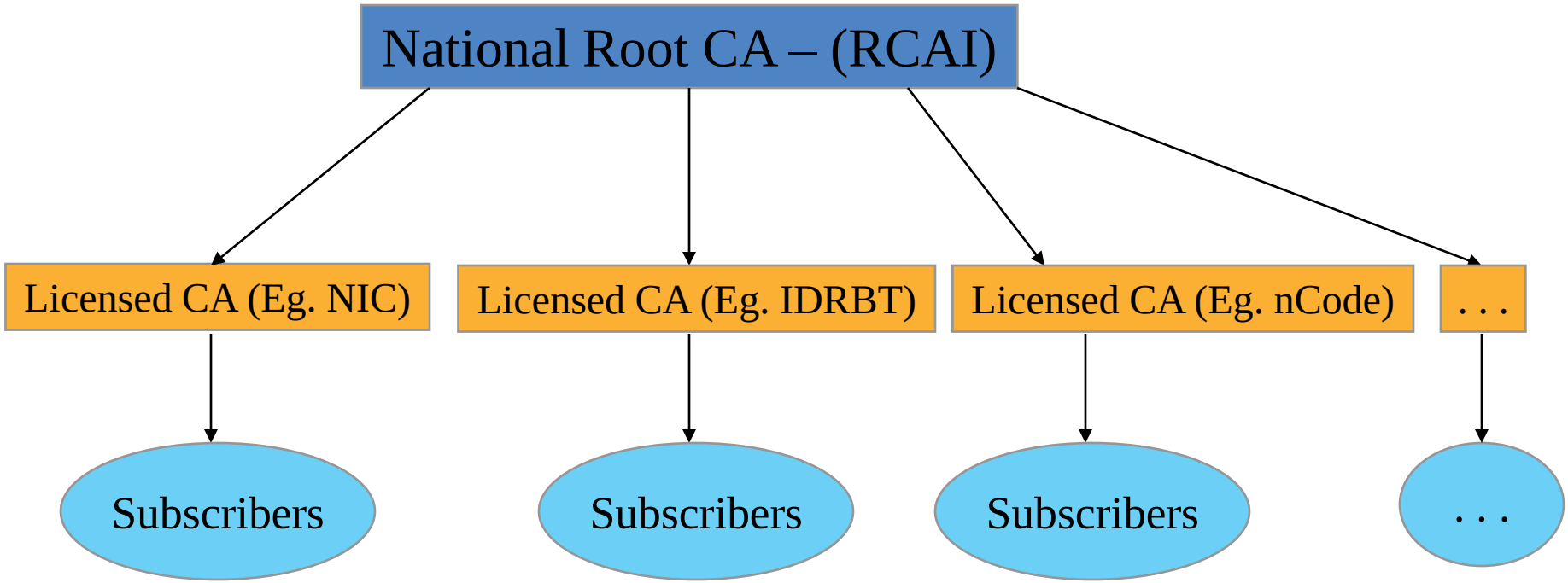
General Security Lessons

- Risks are inherent in any cryptographic system
- PKI is not a one-stop solution for all your security needs
- Any security system is only as safe as the weakest link in a security chain!

Trust Model

Hierarchical Trust Model

- For a Digital Signature to have legal validity, it must derive its trust from the Root CA certificate

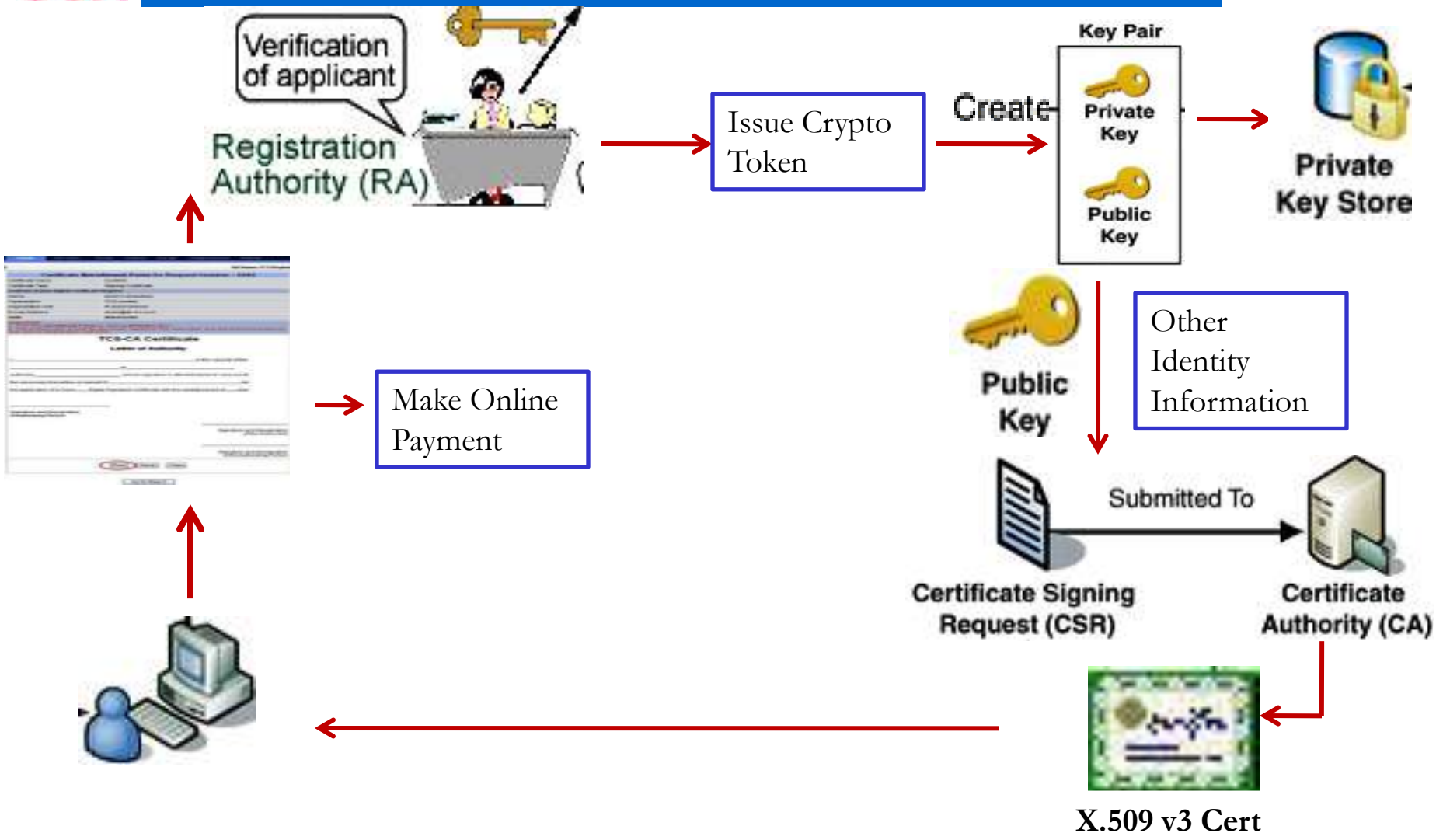


Licensed CA's in India

- National Root CA (RCAI) – operated by CCA
  - Only issues CA certificates for licensed CAs
- 6 CAs licensed under the National Root CA
  - National Informatics Centre (https://nicca.nic.in)
  - eMudhra (www.e-mudhra.com)
  - TCS (www.tcs-ca.tcs.co.in)
  - nCode Solutions CA(www.ncodesolutions.com)
  - SafeScrypt (www.safescrypt.com)
  - IDRBT CA (www.idbrtca.org.in)
- As of Sept 2014, approx. 8 Million DSCs have been issued

Certificate Issuance Process

Certificate Issuance Process



Types of Certificates

Types of Certificates

- Signing Certificate
  - Issued to a person for signing of electronic documents
- Encryption Certificate
  - Issued to a person for the purpose of Encryption;
- SSL Certificate
  - Issued to a Internet domain name (Web Servers, Email Servers etc…)

Certificate Classes

Classes of Certificates

- 3 Classes of Certificates
  - Class – 1 Certificate
    - Issued to Individuals
    - Assurance Level: **Certificate will confirm User's name and Email address**
    - Suggested Usage: **Signing certificate** primarily be used for signing personal emails and **encryption certificate** is to be used for encrypting digital emails and **SSL certificate** to establish secure communication through SSL

Classes of Certificates

- Class – 2 Certificate
  - Issued for both business personnel and private individuals use
  - Assurance Level: **Conforms the details submitted in the form including photograph and documentary proof**
  - Suggested Usage: **Signing certificate** may also be used for digital signing, code signing, authentication for VPN client, Web form signing, user authentication, Smart Card Logon, Single sign-on and signing involved in e-procurement / e-governance applications, in addition to Class-I usage

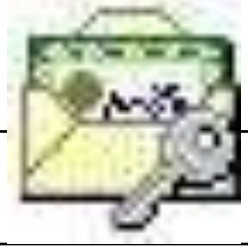
Classes of Certificates

– Class – 3 Certificate

- Issued to Individuals and Organizations
- Assurance Level: **Highest level of Assurance; Proves existence of name of the organization, and assures applicant's identity authorized to act on behalf of the organization.**
- Suggested Usage: **Signing certificate** may also be used for digital signing for discharging his/her duties as per official designation and also **encryption certificate** may also be used for encryption requirement as per his/her official capacity

Certificate Extensions

File Formats with Extensions	Description
.CER	Contains only Public Key
.CRT	Contains only Public Key
.DER	Contains only Public Key
.P12	Contains Public and Private Key
.PFX	Contains Public and Private Key
.PEM, .KEY, .JKS	Contains Public and Private Key
.CSR	Certificate Signing Request
.CRL	Certificate Revocation List



Certificate Life Cycle Management

Certificate Lifecycle Management

- A Digital Signature Certificate cannot be used for ever!
- Typical Life cycle scenario of Digital Certificates
  - Use until renewal
    - Certificates are to be reissued regularly on expiry of validity (typically 2 years)
  - Use until re-keying
    - If keys had to be changed
  - Use until revocation
    - If Certificate was revoked, typically when keys are compromised or CA discovers that certificate was issued improperly based on false documents

Certificate Revocation List (CRL)

CRL – Certification Revocation List

- A list containing the serial number of those certificates that have been revoked
- Why they have been revoked?
  - If keys are compromised and users reports to the CA
  - If CA discovers, false information being used to obtain the certificate
- Who maintains CRLs ?
  - Typically the CA's maintain the CRL

CRL – Certification Revocation List

- How frequently the CRL is updated ?
  - Generally twice a day; based on CA's policies
- Is there any automated system in place for accessing the CRL?
  - OCSP

Certificate Validation Methods

Certificate Validation Methods

- **How do you know that the certificate is valid and belongs to that owner ?**

- The validation process performs following checks
  - Digital Signature of Issuer (CA)
  - Trust (Public Key Verification) till root level
  - Time (Validity of the Certificate)
  - Revocation (CRL verification)
  - Format

Legal aspects of Digital Signature as per Indian IT Act

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

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

- 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

Conclusion

- PKI and Digital Signatures have been transforming the way traditional transactions happen
- PKI Ecosystem has the potential to usher
  - Transparency
  - Accountability
  - Time, Cost & Effort-savings
  - Speed of execution and to be an integral part of
  - **Digital India and bring in Digital Identity**

References

- Cryptography and Network security – principles and practice William Stallings
- Applied Cryptography, Second Edition: Bruce Schneier
- Ryder, Rodney D, Guide to Cyber Laws, 3rd Edition, Wadhwa & Company, New Delhi 2007
- Handbook of Applied Cryptography, by Menezes
- Cryptographic Techniques for N/w Security
- http://campustechnology.com/articles/39190_2
- http://csrc.nist.gov/
- http://www.productivity501.com/digital-signatures-encryption/4710/
- http://www.arx.com/digital-signatures-faq
- http://www.asclonline.com/images/d/d4/Simple_Guide_to_Digital_Signatures.pdf
- http://www.asianlaws.org/library/infosec/obtaining-digital-signature-certificate.pdf
- http://cca.gov.in/
- www.seekha.in/events/pki - for slides and resources