Digital Signatures and Public Key Infrastructure

Dr. Balaji Rajendran
Centre for Development of Advanced Computing (C-DAC)
Bangalore

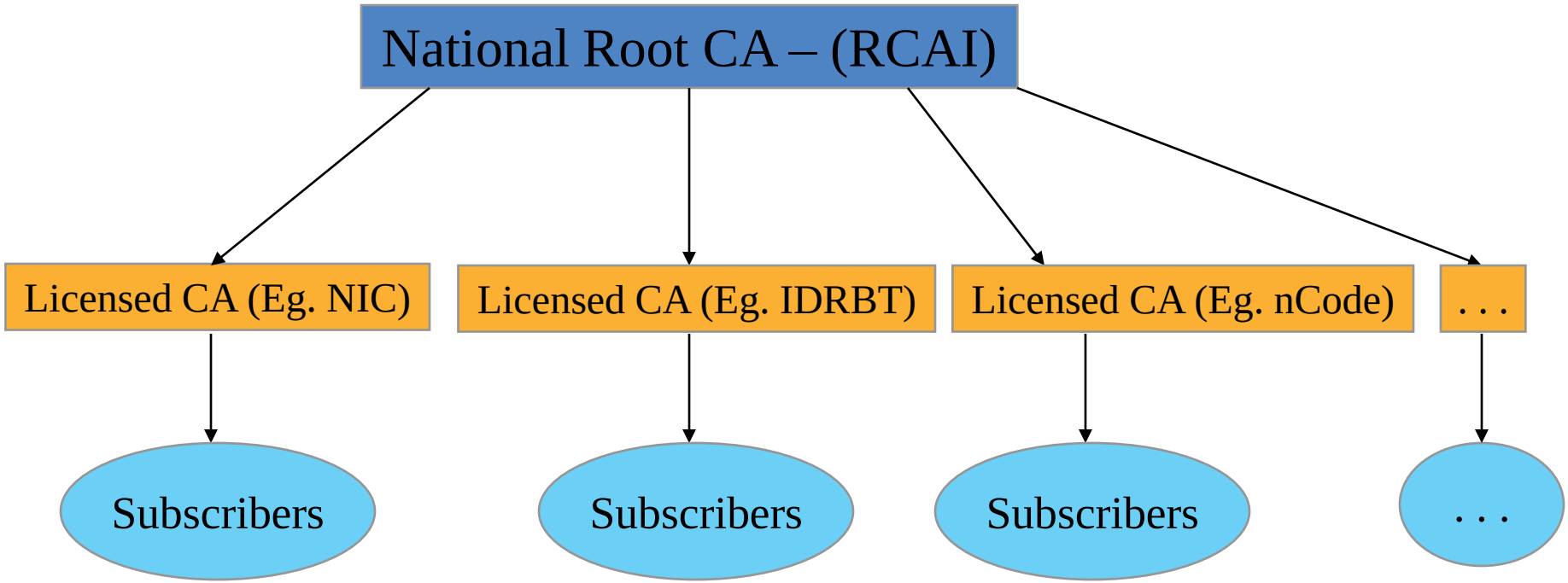
Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Trust Model

Hierarchical Trust Model

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

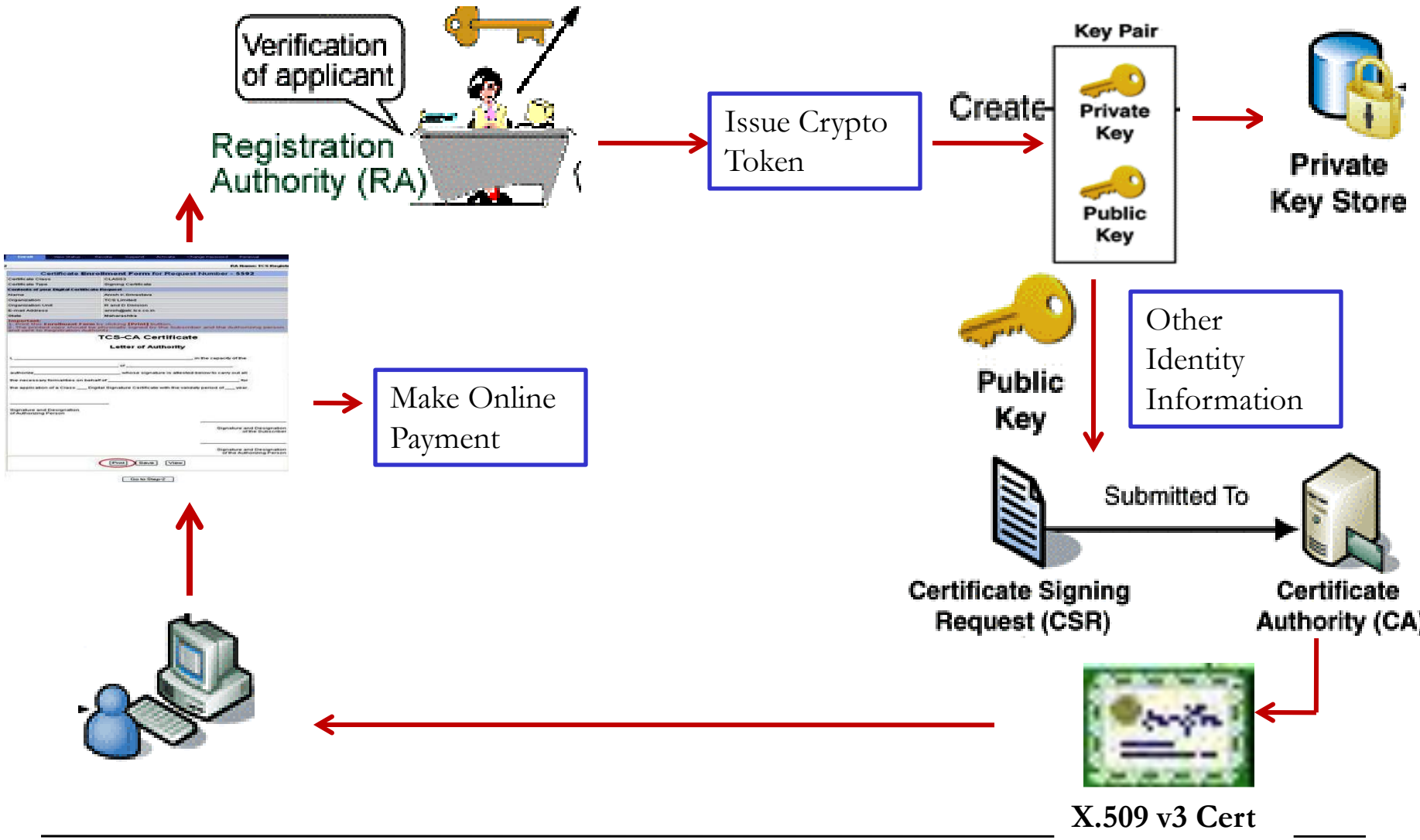


Licensed CA's in India

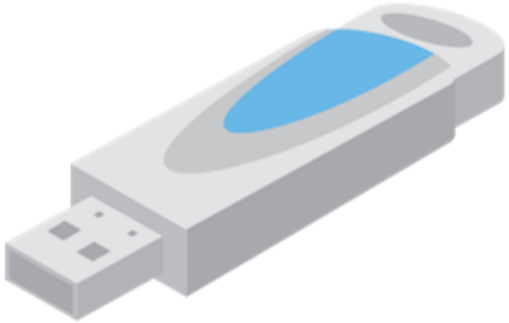
- National Root CA (RCAI) – operated by **CCA**
  - Only issues CA certificates for licensed CAs
- CAs licensed under the National Root CA
  - National Informatics Centre (https://nicca.nic.in)
  - eMudhra (www.e-mudhra.com)
  - TCS (www.tcs-ca.tcs.co.in)
  - nCode Solutions CA(www.ncodesolutions.com)
  - SafeScrypt (www.safescrypt.com)
  - IDRBT CA (www.idbrtca.org.in)
  - C-DAC (http://esign.cdac.in) – Only e-Sign
- As of Jan, 2015 approx. 9 Million+ DSCs have been issued

Certificate Issuance Process

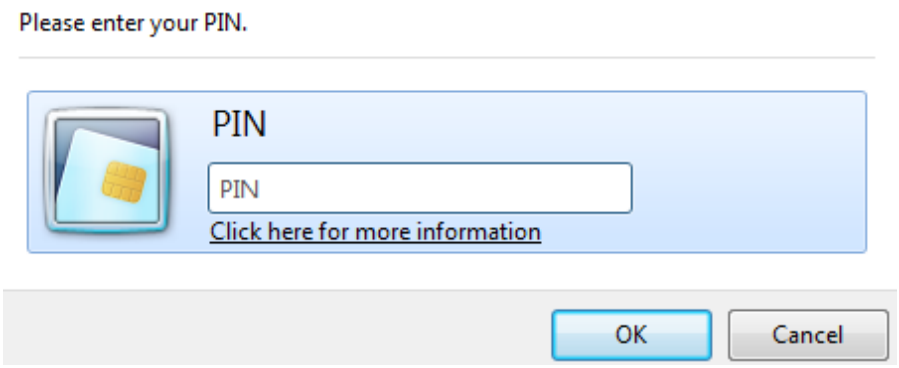
Certificate Issuance Process



Crypto Tokens



- Contain a Cryptographic co-processor with a USB interface
  - Key is generated inside the token.
  - Key is highly secured as it doesn't leave the token
  - Highly portable and Machine-independent
  - FIPS 140-2 compliant; Tamper-resistant;



Certificate Classes

Classes of Certificates

- Classes define the level of assurance for a Digital Certificate
- 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 **encryption certificate** to be used for encryption requirement as per his/her official capacity

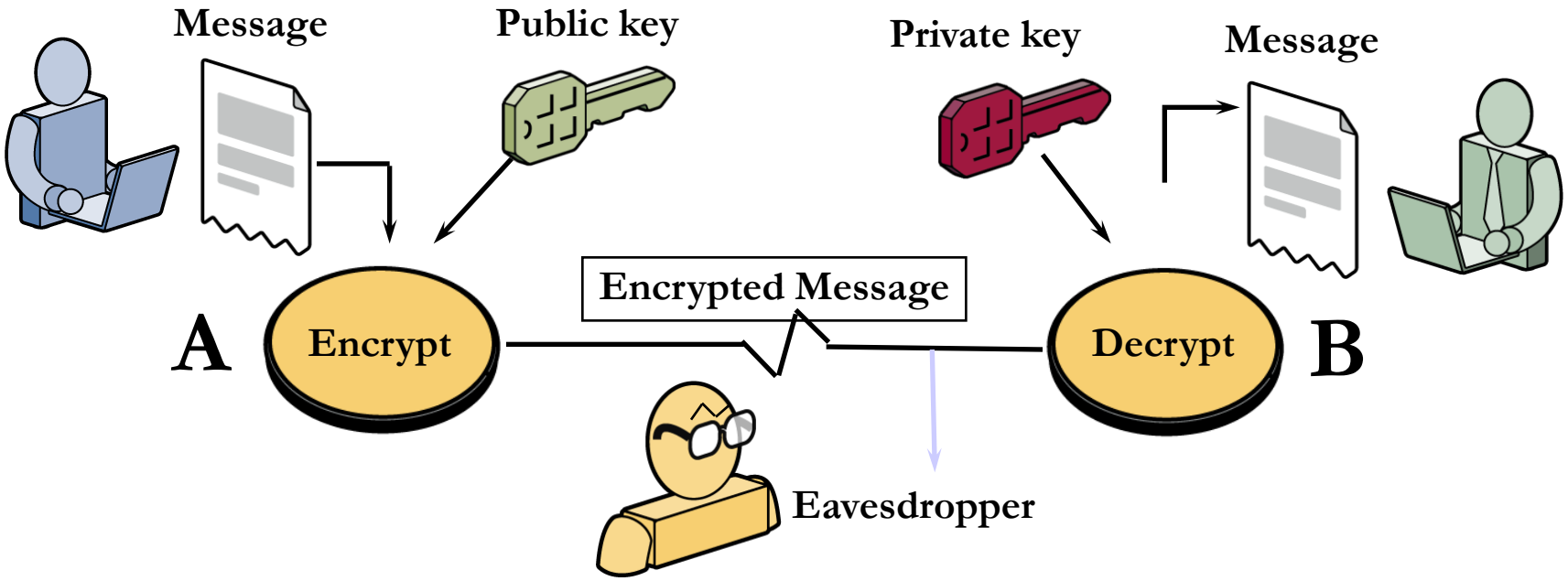
Types of Certificates

Types of Certificates

- Types define the purpose for which a Digital Certificate is issued
- Signing Certificate (**DSC**)
  - 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…)

Achieving Secrecy

Achieving Secrecy through Asymmetric Key Encryption



General Conventions

- Encryption – Public Key of the Receiver
- Decryption – Private Key of the Receiver

Achieving PAIN !

- How to achieve Privacy, Authenticity, Integrity and Non-repudiation all together in a transaction

Signcryption

- Why do you need Signcryption ?
  - The intended receiver alone should know the contents of the message
    - **Secrecy / Confidentiality / Privacy**
  - The receiver should be sure that
    - The message has come from the claimed sender only
      - **Authentication**
    - The message has not been tampered
      - **Integrity**
    - Signer has used a valid and trustable certificate
      - **Non-Repudiation**

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 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

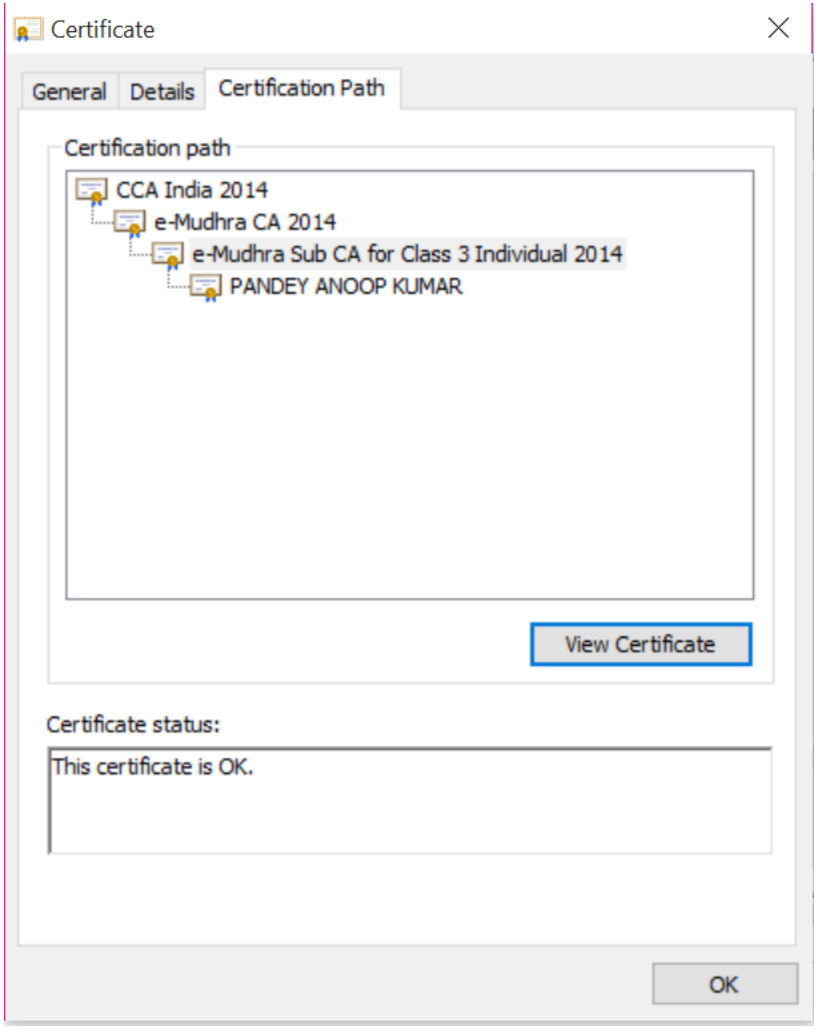
CRL – Certification Revocation List

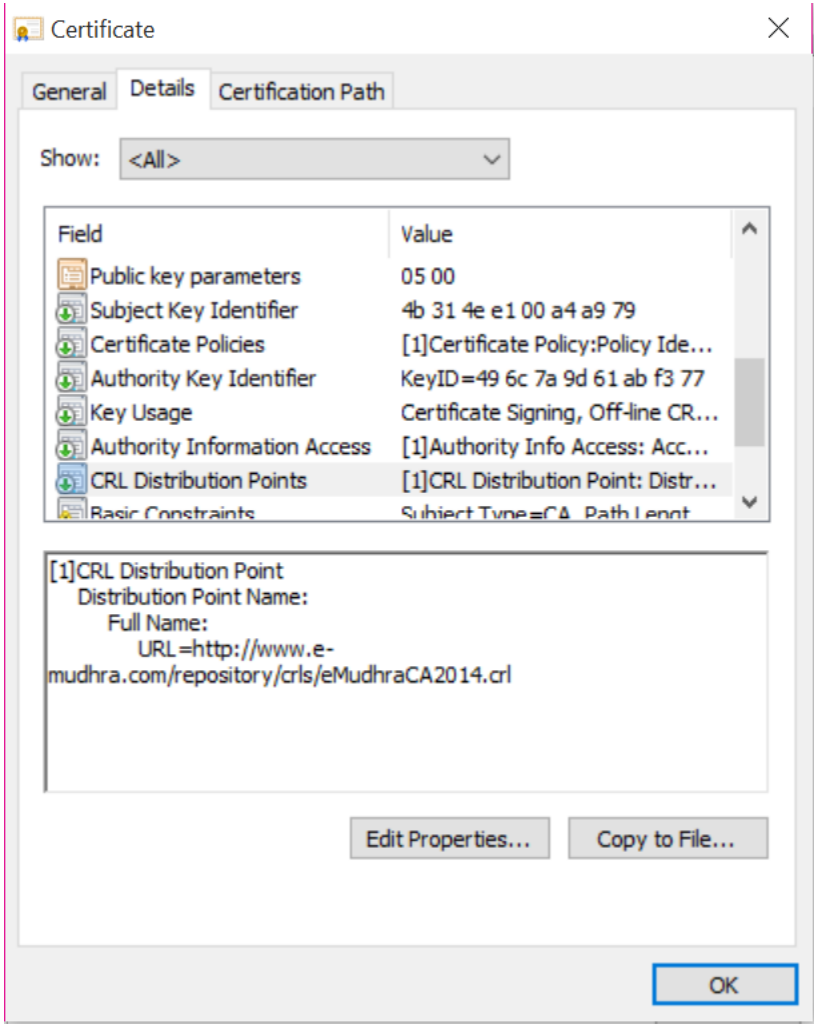
- A list containing the serial number of those certificates that have been revoked
- Why they have been revoked?
  - If keys are compromised and users reports to the CA
  - If CA discovers, false information being used to obtain the certificate
- Who maintains CRLs ?
  - Typically the CA's maintain the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

CRL – Certification Revocation List

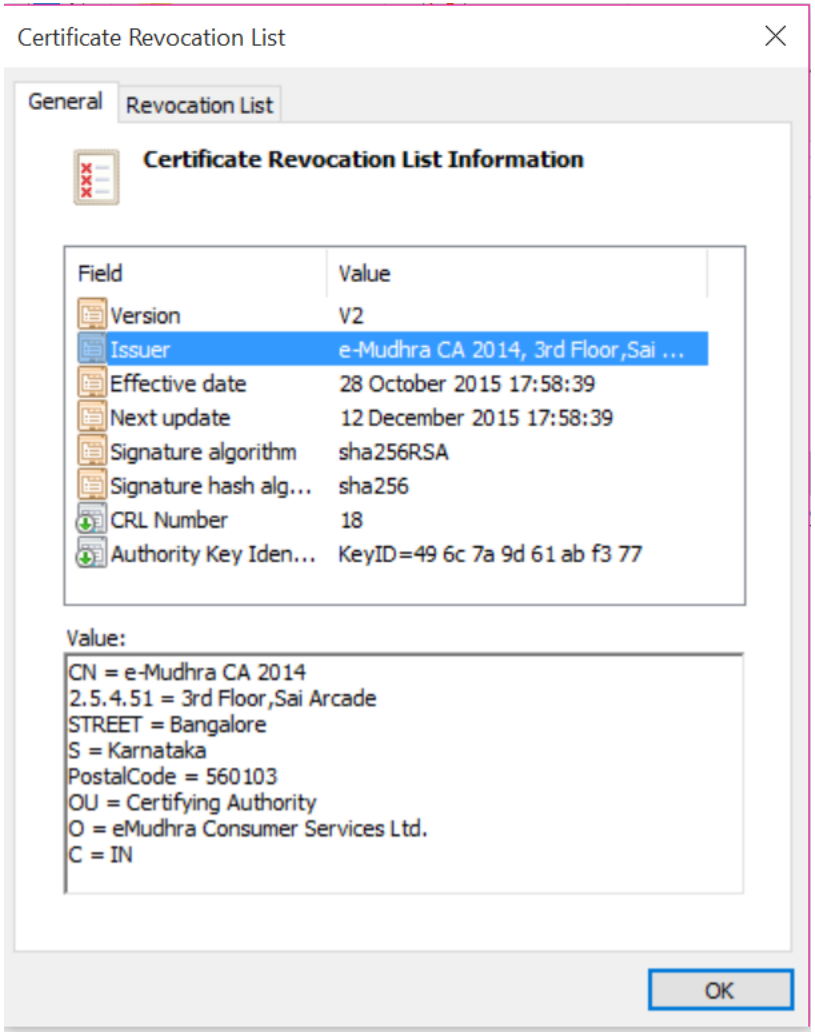
- How frequently the CRL is updated ?
  - Generally twice a day; based on CA's policies
- Is there any automated system in place for accessing the CRL?
  - OCSP

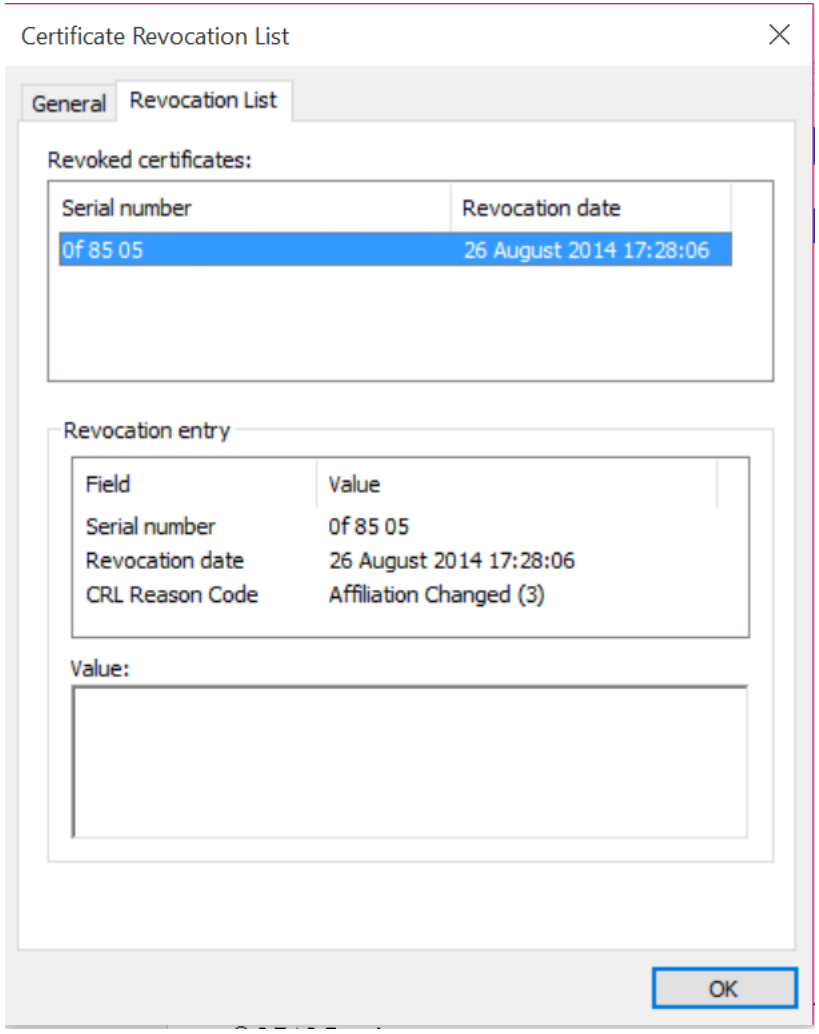
Obtaining CRL





Sample CRL


Certificate Revocation List
General
Revocation List
Certificate Revocation List Information
Field
Value
Version
V2
Issuer
e-Mudhra CA 2014, 3rd Floor,Sai ...
Effective date
28 October 2015 17:58:39
Next update
12 December 2015 17:58:39
Signature algorithm
sha256RSA
Signature hash alg...
sha256
CRL Number
18
Authority Key Iden...
KeyID=49 6c 7a 9d 61 ab f3 77
Value:
CN = e-Mudhra CA 2014
2.5.4.51 = 3rd Floor,Sai Arcade
STREET = Bangalore
S = Karnataka
PostalCode = 560103
OU = Certifying Authority
O = eMudhra Consumer Services Ltd.
C = IN
OK


Certificate Revocation List
General
Revocation List
Revoked certificates:
Serial number
Revocation date
0f 85 05
26 August 2014 17:28:06
Revocation entry
Field
Value
Serial number
0f 85 05
Revocation date
26 August 2014 17:28:06
CRL Reason Code
Affiliation Changed (3)
Value:
OK

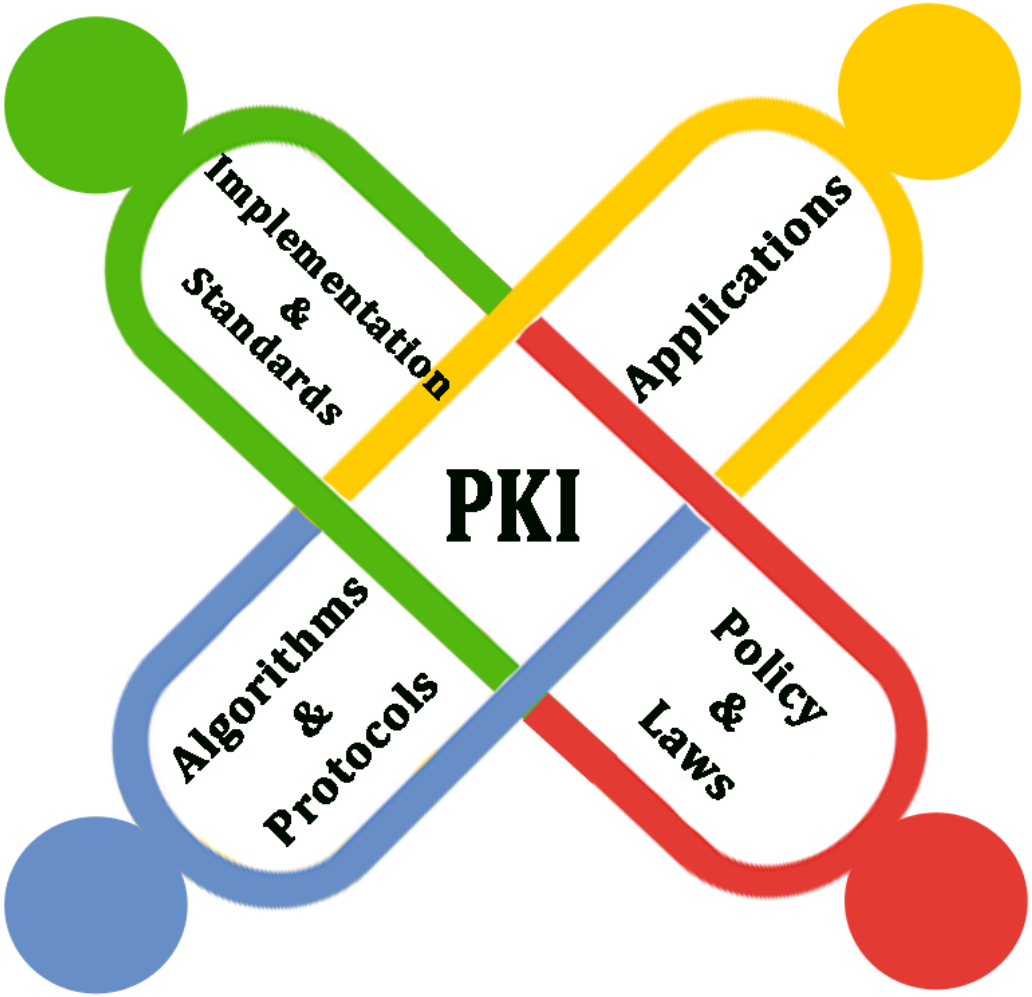
Certificate Validation Methods

- Validating a certificate is typically carried out by PKI enabled application
- The validation process performs following checks
  - Digital signature of the issuer (CA)
  - Trust (Public Key verification) till root level
  - Time (Validity of the certificate)
  - Revocation (CRL verification)
  - Format

A word of Caution!

- Keep your Digital Security Tokens Safe!
  - Report loss of tokens immediately and seek for revocation from the CA
  - If you have any doubts that private key has been compromised, inform the CA
  - Remember that risks are inherent in any system!
    - Any Security system is only as safe as the weakest link in the security chain!

Dimensions of PKI



What is PKI ?

- Public Key Infrastructure (PKI) is an ecosystem comprising of :
  - Algorithms & Protocols
    - Key Role Players: Cryptographers, Researchers
  - Implementation & Standards
    - Key Role Players: Application Developers, Standard developers
  - Policy & Law
    - Key Role Players: Regulatory bodies, Law Protection Agencies
  - Applications
    - Key Role Players: Users & Systems

Present Digital Signature & PKI Implementations in India

PKI enabled Applications

1	**e-Invoice**	**(B2C)**
2	**e-Tax Filing**	**(G2C)**
3	**e-Customs**	**(G2B)**
4	**e-Passport**	**(G2C) -** Presently in India, the Ministry of External Affairs has started issuing e-Passports in Karnataka state with the fingerprints and the digital photo of applicant
5	**e-Governance**	**Bhoomi (G2C)** a PKI enabled registration and Land Records Services offered by Govt. of Karnataka to the people. All the land records and certificates issued are digitally signed by the respective officer
6	**e-Payment**	**(B2B) -** In India, currently between banks fund transfers are done using PKI enabled applications whereas between customers and vendors such as online shopping vendor the payment is done through SSL thereby requiring the vendor to hold DSC)

PKI enabled Applications

7	**e-Billing**	**(B2C)** -The electronic delivery and presentation of financial statement, bills, invoices, and related information sent by a company to its customers)
8	**e-Procurement**	**G2B , B2B**
9	**e-Insurance Service**	**(B2C) -** Presently the users are getting the E-Premium Receipts etc. which is digitally signed by the provider
10	**Treasury Operations**	**(G2C)** ***Khajanae – II*** of Govt. of Karnataka uses Digital Signatures to automate and speed up the treasury operations

Other Implementations

- DGFT - Clearance of goods are now initiated by exporters through push of a button and in their offices;
  - Previously it used to take days; and requests are now cleared within 6 hours
- Indian Patent office has implemented e-filing of patents and allows only use of Class-3 Certificates
  - Around 30% of e-filing of patents is happening now, among the total filings.

Summary

- PKI is an ecosystem comprising of Technology, Policy and Implementations
  - Digital Signatures provide **A**uthenticity, **I**ntegrity, and **N**on-Repudiation for electronic documents & transactions
  - Asymmetric Key system enables **C**onfidentiality
- General Conventions
  - Signing – Private Key of the Signer
  - Verification – Public Key of the Signer
  - Encryption – Public Key of the Receiver
  - Decryption – Private Key of the Receiver

Thank You

pki@cdac.in

www.facebook.com/pkiindia

PKIIndia

@pkiindia