PKI Components

Anoop Kumar Pandey
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Agenda

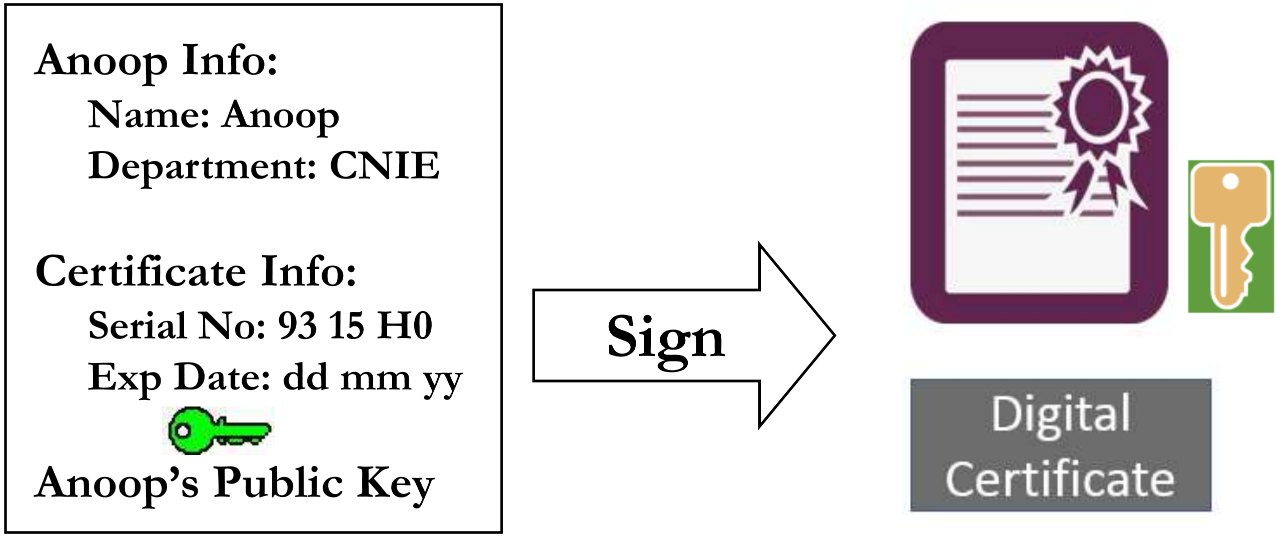
- ✓ Digital Signature Certificate
- ✓ Certifying Authority & Trust Model
- ✓ Certificate Issuance, Types, Classes
- ✓ Certificate Life Cycle Management and Validation Methods
- ✓ Dimensions of PKI
- ✓ PKI Applications in India

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.



Anoop Info:
Name: Anoop
Department: CNIE

Certificate Info:
Serial No: 93 15 H0
Exp Date: dd mm yy

Anoop's Public Key

Certifying Authority (CA) ?

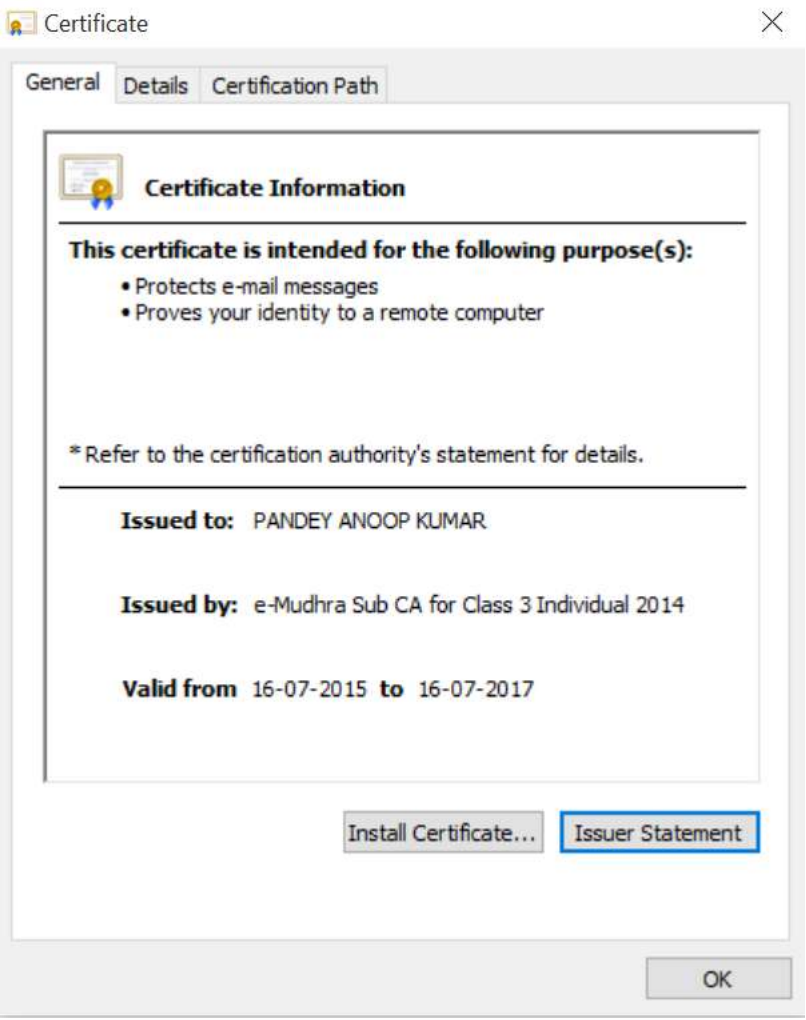
Certifying Authority (CA)

- 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



Certificate Information

This certificate is intended for the following purpose(s):

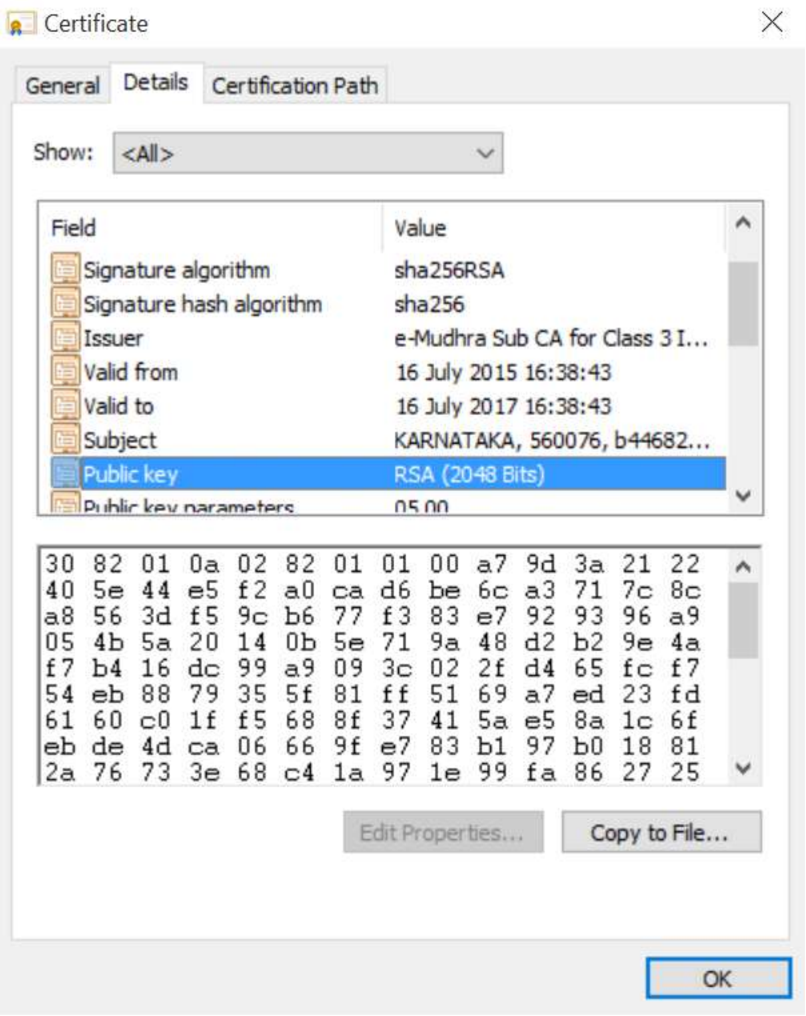
- Protects e-mail messages
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: PANDEY ANOOP KUMAR

Issued by: e-Mudhra Sub CA for Class 3 Individual 2014

Valid from 16-07-2015 **to** 16-07-2017



Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	e-Mudhra Sub CA for Class 3 I...
Valid from	16 July 2015 16:38:43
Valid to	16 July 2017 16:38:43
Subject	KARNATAKA, 560076, b44682...
Public key	RSA (2048 Bits)
Public key parameters	05 00

```
30 82 01 0a 02 82 01 01 00 a7 9d 3a 21 22
40 5e 44 e5 f2 a0 ca d6 be 6c a3 71 7c 8c
a8 56 3d f5 9c b6 77 f3 83 e7 92 93 96 a9
05 4b 5a 20 14 0b 5e 71 9a 48 d2 b2 9e 4a
f7 b4 16 dc 99 a9 09 3c 02 2f d4 65 fc f7
54 eb 88 79 35 5f 81 ff 51 69 a7 ed 23 fd
61 60 c0 1f f5 68 8f 37 41 5a e5 8a 1c 6f
eb de 4d ca 06 66 9f e7 83 b1 97 b0 18 81
2a 76 73 3e 68 c4 1a 97 1e 99 fa 86 27 25
```

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

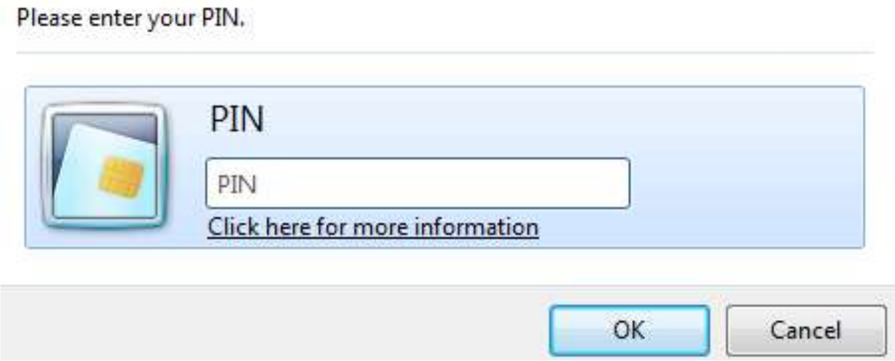
- They are similar to smart cards in functionality as
  - Key is generated inside the token.
  - Key is highly secured as it doesn’t leave the token.
  - Highly portable.
  - Machine Independent.

- USB Crypto-Tokens
- AudioPass

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.

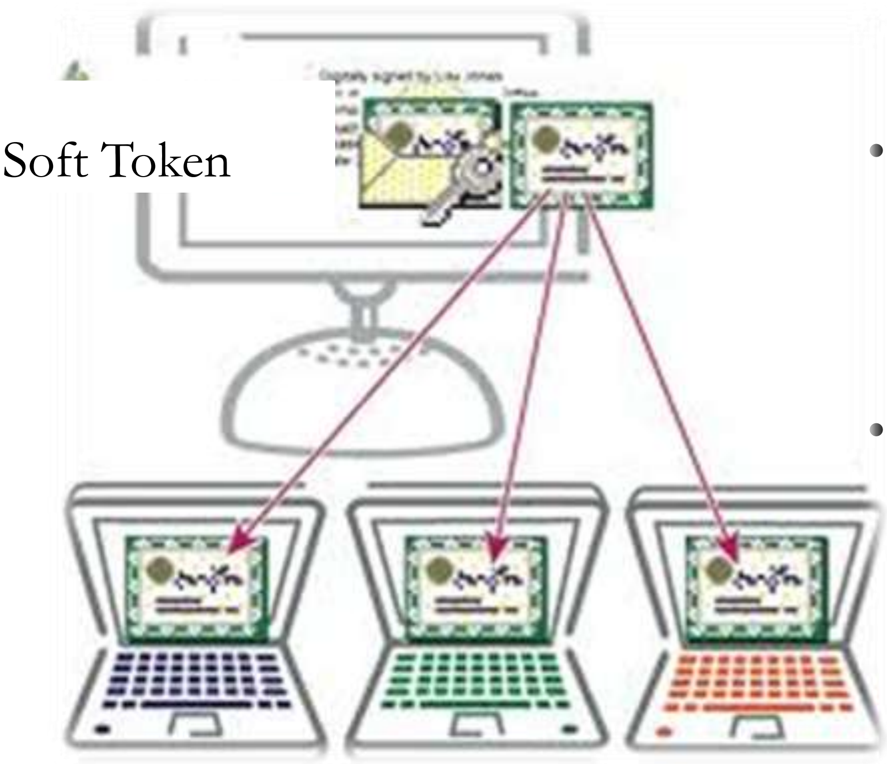
- The key is secured using
  - PIN Protected Soft token
  - Smart Cards
  - Hardware USB Tokens



Please enter your PIN.

PIN

PIN protected Soft Tokens (Not Safe and Not Used Now)



- 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.

ssh-keygen, openssl

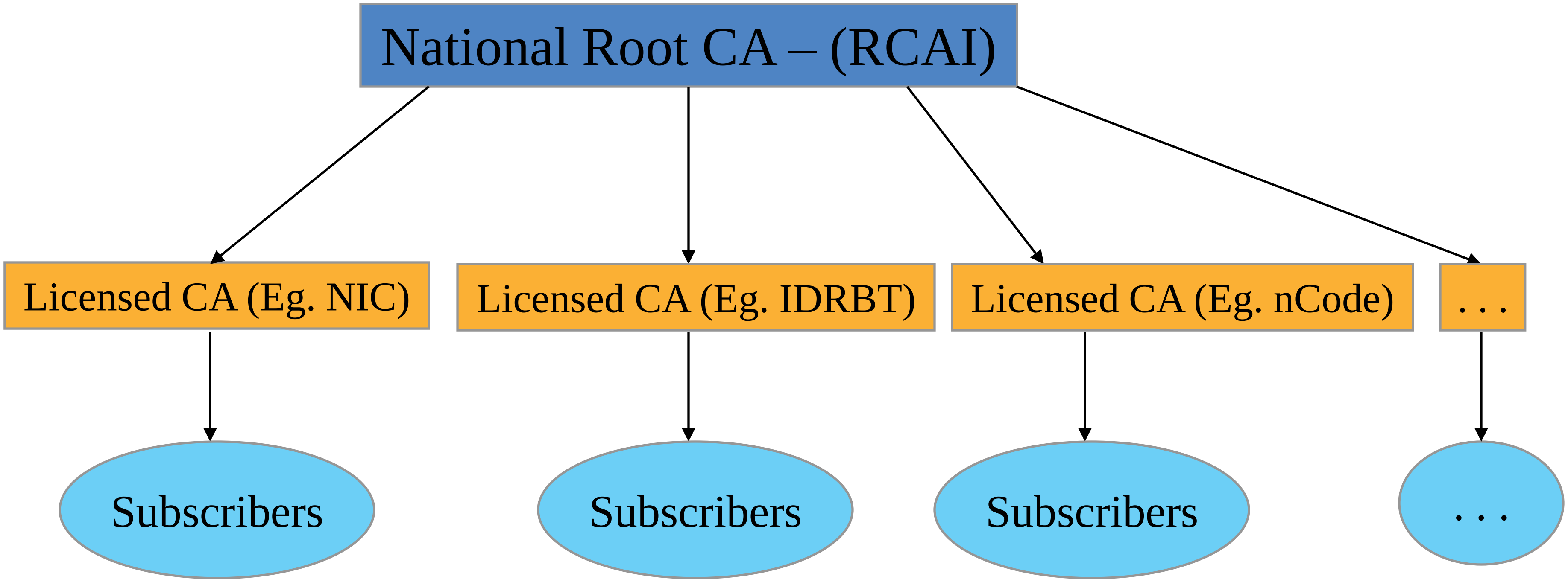
A word of Caution!

- 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!

Trust Model

Hierarchical Trust Model

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

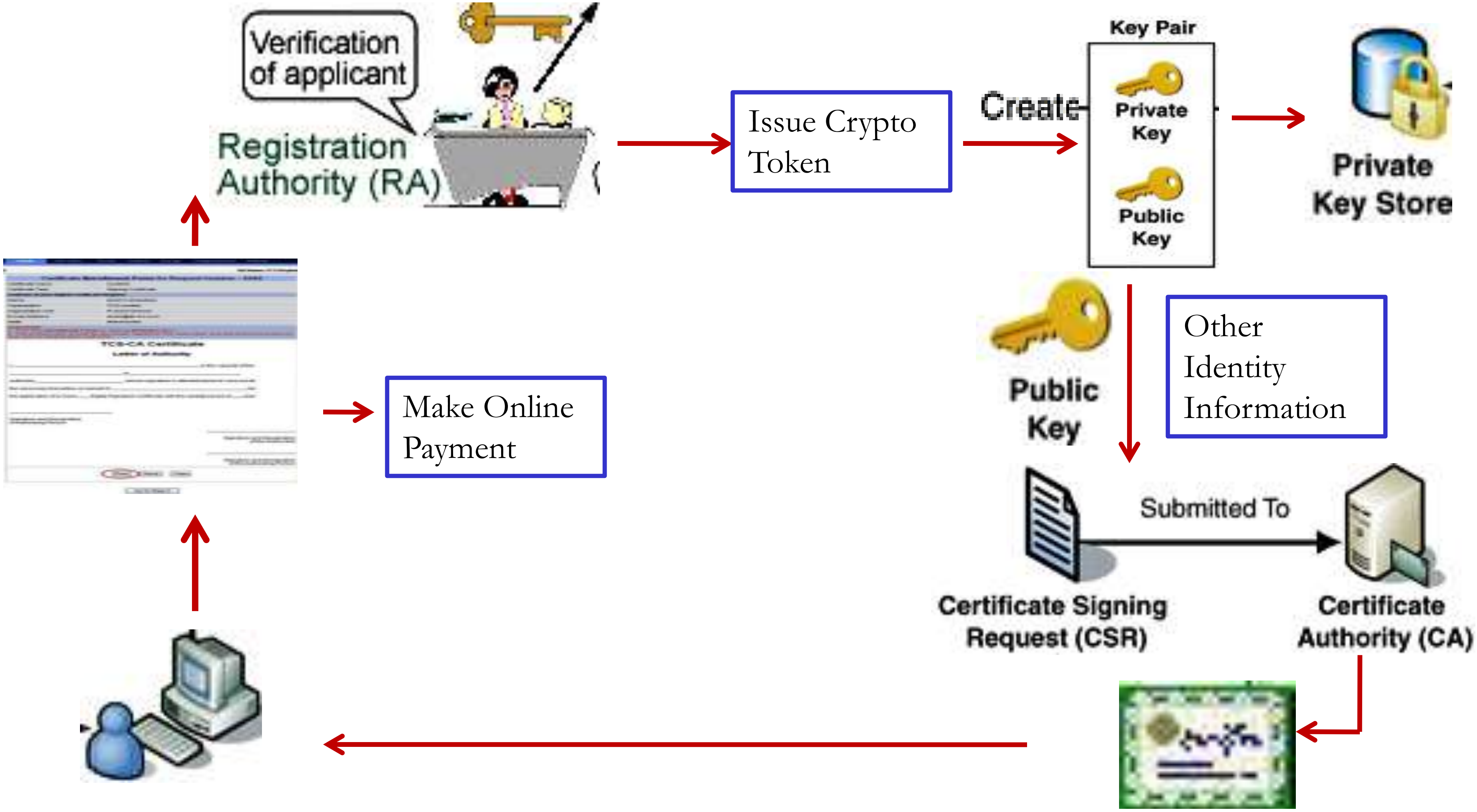


Licensed CA's in India

- National Root CA (RCAI) – operated by **CCA**
  - Only issues CA certificates for licensed CAs
- 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.idrbtca.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


Verification of applicant
Registration Authority (RA)
Key Pair
Create
Private Key
Public Key
Private Key Store
Public Key
Submitted To
Certificate Signing Request (CSR)
Certificate Authority (CA)

Issue Crypto Token

Make Online Payment

Other Identity Information

X.509 v3 Cert

e-Mudhra Example

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 **encryption certificate** to 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 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

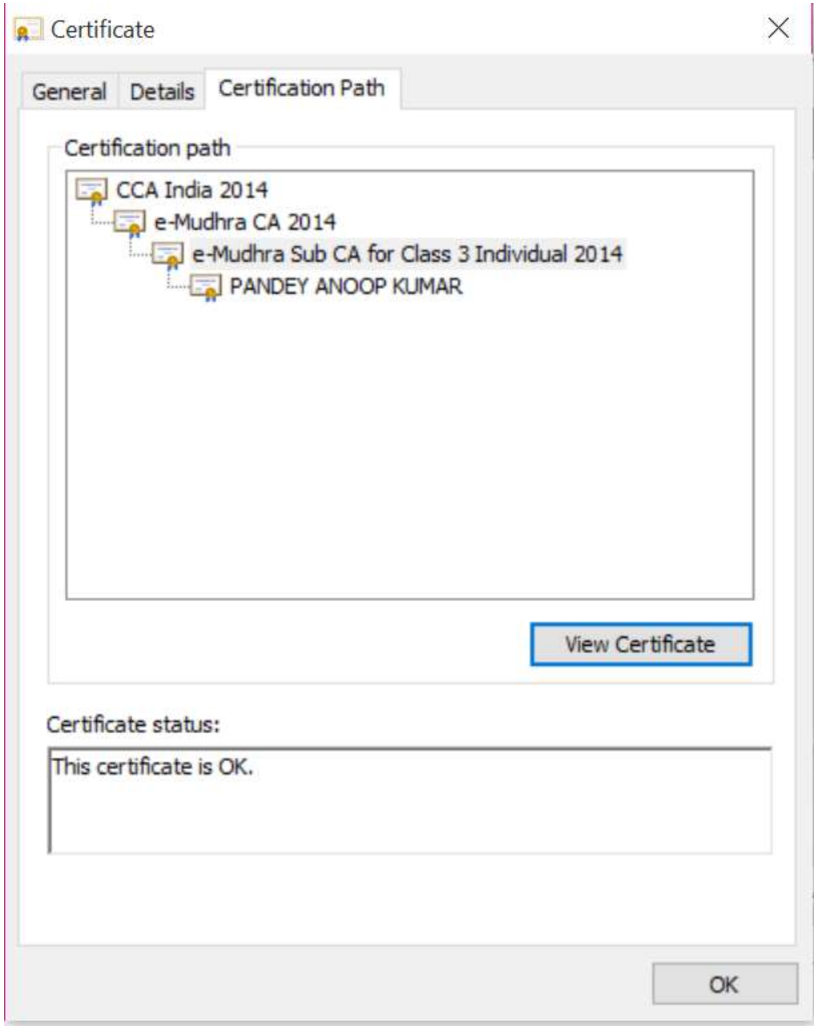
CRL – Certification Revocation List

- 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



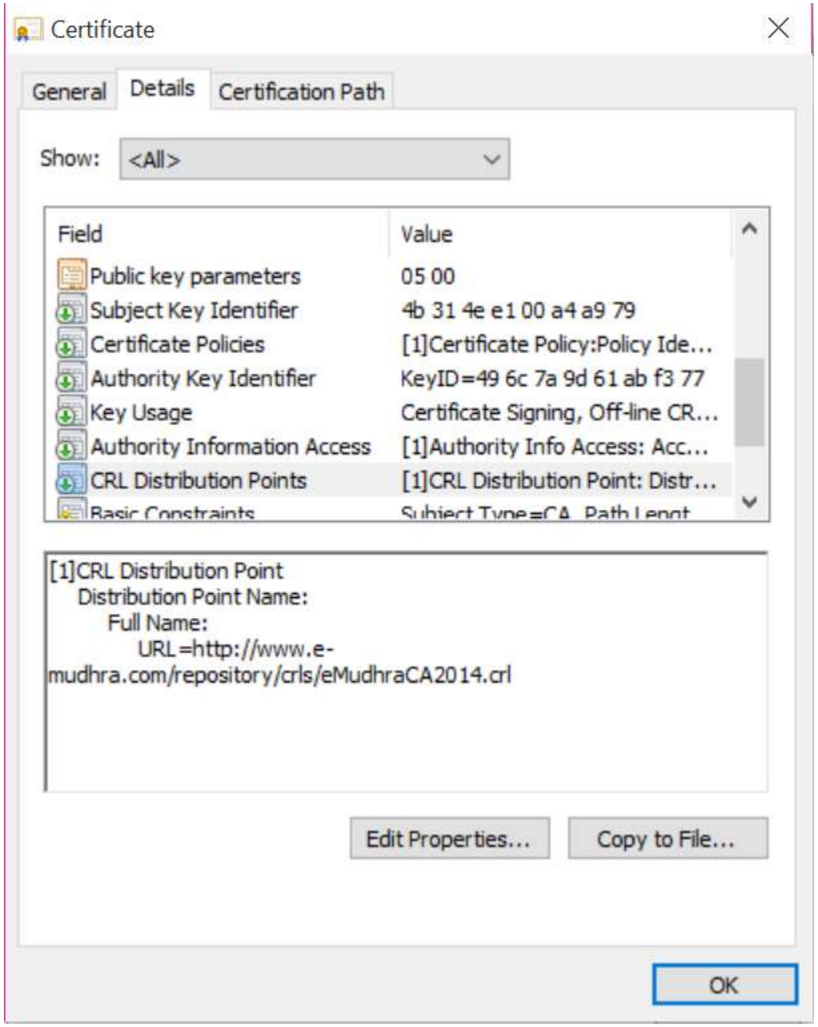
Certificate

Certification path

- CCA India 2014
  - e-Mudhra CA 2014
    - e-Mudhra Sub CA for Class 3 Individual 2014
      - PANDEY ANOOP KUMAR

Certificate status:

This certificate is OK.



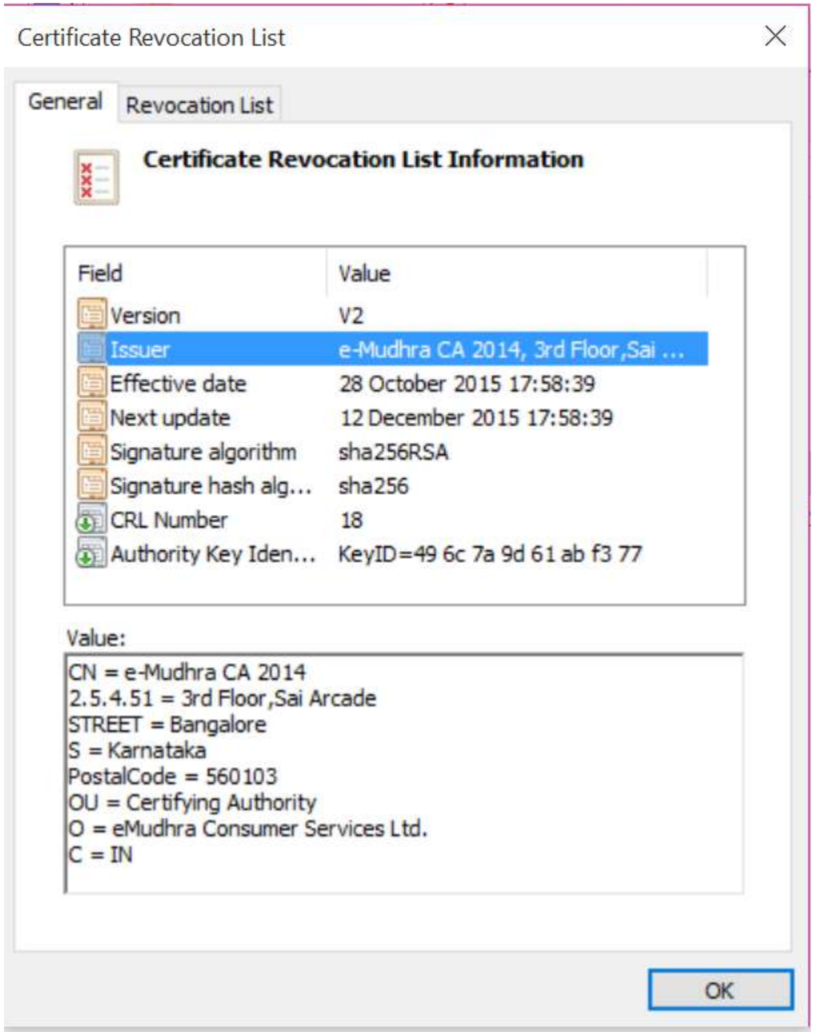
Certificate

Show: <All>

Field	Value
Public key parameters	05 00
Subject Key Identifier	4b 31 4e e1 00 a4 a9 79
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Key Identifier	KeyID=49 6c 7a 9d 61 ab f3 77
Key Usage	Certificate Signing, Off-line CR...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Basic Constraints	Subject Type=CA, Path Lengt

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://www.e-
mudhra.com/repository/crls/eMudhraCA2014.crl
```

Sample CRL

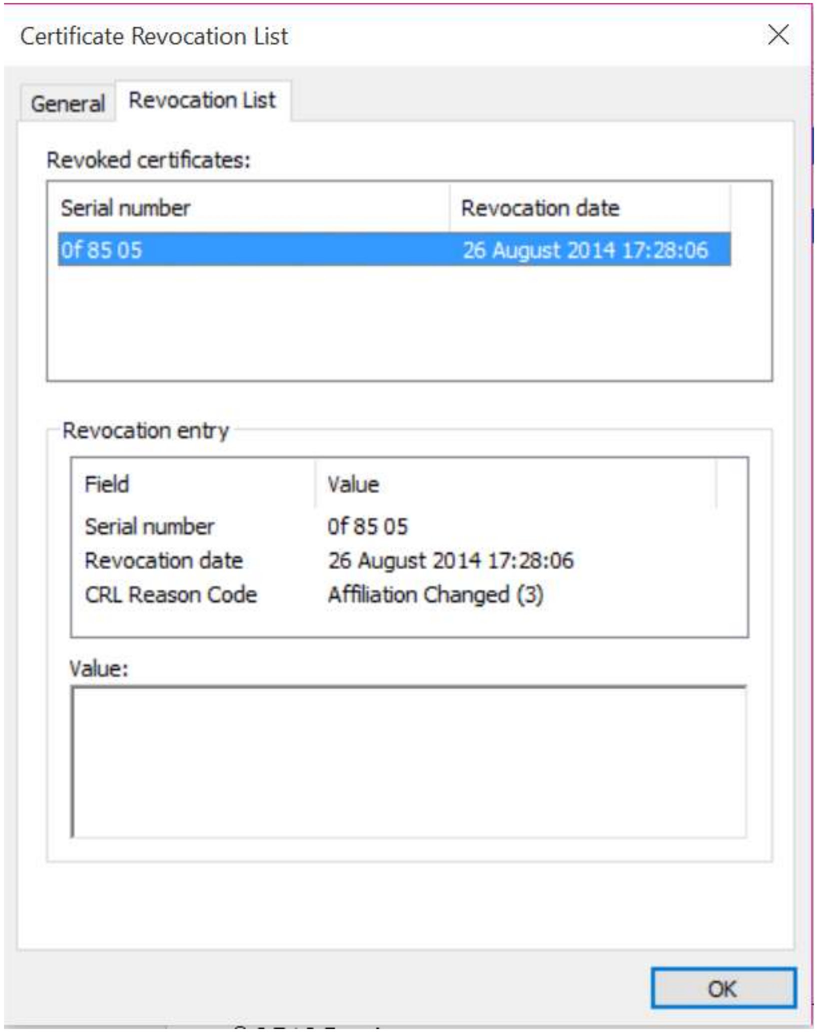


Certificate Revocation List Information

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



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:

Online Certificate Status Protocol

- Online certificate status protocol(OCSP) is an internet protocol used for obtaining the revocation status of an X.509 digital certificate.
- It was created as an alternative to certificate revocation list
- It gives status of certificate in real time.

OCSP Services

- The OCSP protocol enables OCSP-compliant applications to determine the state of a certificate, including revocation status.
- The validation authority which validates the status of certificate known as OCSP responder.
- CA periodically publishes CRLs to an OCSP responder.
- The OCSP responder maintains the CRL it receives from the CA.

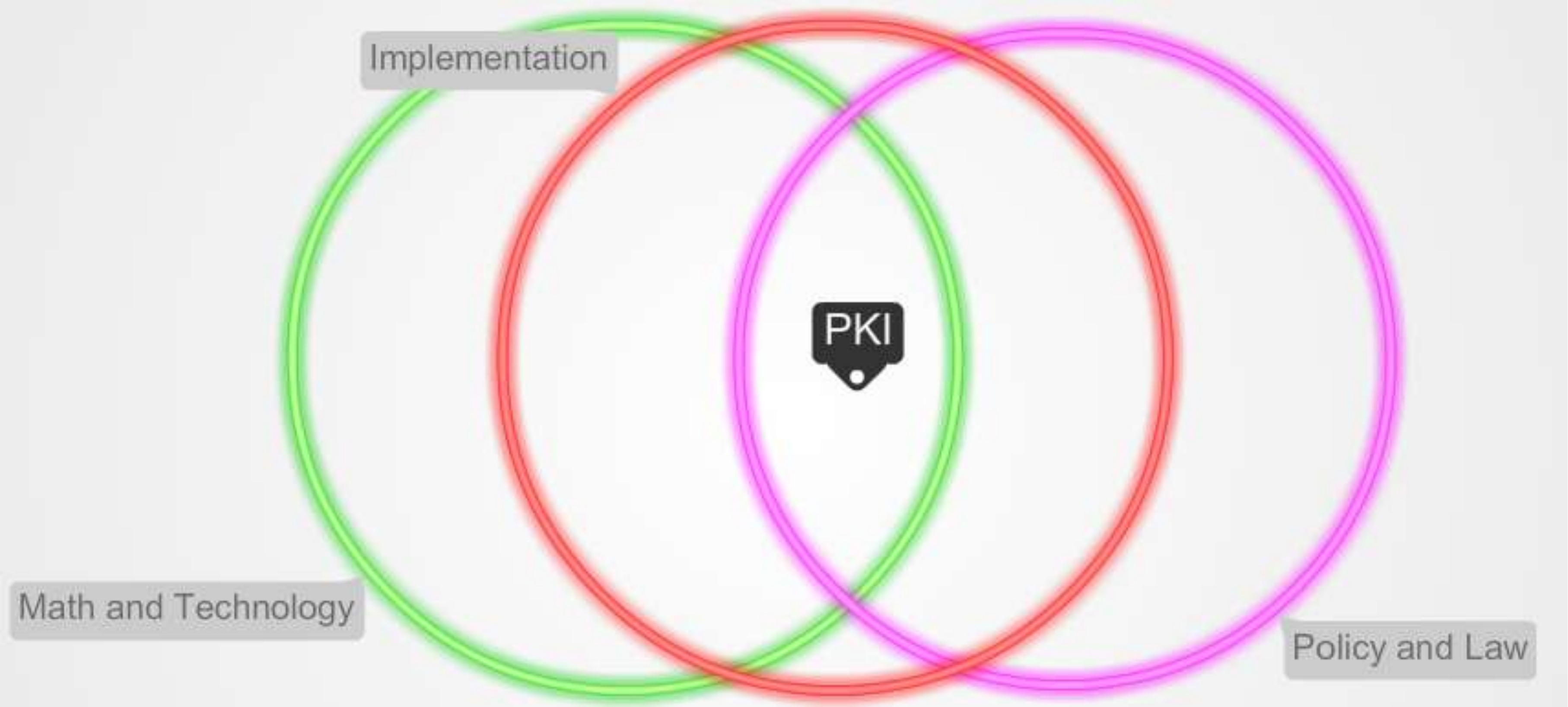
Contd.

- When end user wants to know about status of a digital certificate then he/she can send query to OCSP responder.
- The OCSP responder determines if the request contains all the information required to process the request sent by user.
- If it does not or if it is not enabled for the request service, a rejection notice is sent.
- If it does have enough information, it processes the request and sends back a report stating the status (Good/Revoked/Unknown) of the certificate.

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

Dimensions of PKI



- PKI – Public Key Infrastructure ecosystem is an intersection of:
  - Cryptography (Math) – Cryptographers/Researchers
  - Technology & Implementation – PKI System Developer
  - Policy & Law – PKI System & Users

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.

*Directorate General of Foreign Trade

Summary

- DSC is used to Signing and encryption processes
- CryptoTokens hold DSC
- There are different class of DSCs based on assurance level.
- Trust Model is used to derive trust for DSC
- DSC doesn't come with Life-Time Achievement Award. [Each DSC has a lifecycle].
- CRL and OCSP can be used for validating DSC.

CCA

References

स्रीडैक CDAC

- Cryptography and Network security – Principles and Practice by William Stallings
- Applied Cryptography: Protocols, Algorithms, and Source Code in C by Bruce Schneier
- Handbook of Applied Cryptography, by Alfred Menezes and Paul Van Oorschot
- Ryder, Rodney D, Guide to Cyber Laws, 3rd Edition, Wadhwa & Company, New Delhi
- Digital Certificates: What are they?: http://campustechnology.com/articles/39190_2
- Digital Signature & Encryption: http://www.productivity501.com/digital-signatures-encryption/4710/
- FAQ on Digital Signatures and PKI in India - http://www.cca.gov.in/cca/?q=faq-page
- Controller of Certifying Authorities – www.cca.gov.in
- e-Sign: http://www.cca.gov.in/cca/?q=eSign.html
- More Web Resources
  - Social Media: www.facebook.com/pkiindia @pkiindia

Thank You

pki@cdac.in

SSL

- ✓SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser.
- ✓To be able to create an SSL connection a web server requires an SSL Certificate.
- ✓SSL keep online interactions private even though secret data travel across the public Internet.