Certificate Life Cycle & CRL, OCSP

Sunil Kumar Yadav
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Some Important Terms

- Certificate:
  - A *certificate* is a digital document that ***certifies*** that a certain **public key is owned by a particular user** This document is signed by Certificate Authority (CA).
- Certificate/Certification Authority (CA)
  - **Certification authority** (**CA**) is an entity that **issues digital certificates** for use by other parties.
- Registration Authority (RA)
  - A ***Registration Authority (RA)*** is an authority in a network that verifies user request for a **digital certificate** and tells the Certificate Authority (CA) to issue certificate.

Certificates and Encodings

- .DER - Distinguished Encoding Rules (DER) encoded certificate. It is a machine-friendly format. A *DER* file is a binary encoded copy of attributes and values.
- .cer & .crt - usually in binary DER form (same as .der)
- .PEM - (Privacy Enhanced Mail) - format also used in grid.
  - Base64 encoded DER certificate, enclosed between

    -----BEGIN CERTIFICATE-----

    -----END CERTIFICATE-----
- .P12 & PFX - PKCS#12, contains certificate(s) public and private keys (password protected)

Certificate Authority Lifespan

- Authorities has a defined validity period
- Validity period factors :
  - Deploying an authority is a lot of work
  - Certificates issued must expire before authorities certificate
  - Subordinate authorities must expire before superior authorities

Typical Lifecycle of Certificates

- Typical Life cycle scenario of Digital Certificates
  - Certificate Issuance
  - Certificate Distribution
  - Certificate Expiration
  - Certificate Renewal/Rekey/Re-Issuance
  - Certificate Revocation

Mechanisms for Certificate Life Cycle

- To manage the certificate lifecycle, a public key infrastructure must provide mechanisms to support the following management activities:
  - Enroll users and computers for certificates.
  - Distribute certificates for public use.
  - Publish certificate revocation lists (CRLs).
  - Renew/Rekey/Re-Issuace of certificates.
  - Maintain a certificate audit trail.

Generating CSR

- CSR(Certificate Signing Request) Generation
  - 2 Ways of Generating CSR
    - On server using openssl cryptographic library
    - Online enrollment form through CA web portal

openssl cryptographic library

- Using openssl cryptographic library
  - Openssl command to generate the CSR

```
openssl req -nodes -newkey rsa:2048 -keyout myserver.key -out server.csr
```

- You will now be asked to enter details to be entered into your CSR based on openssl configuration.

Country Name (2 letter code) [AU]: **IN**

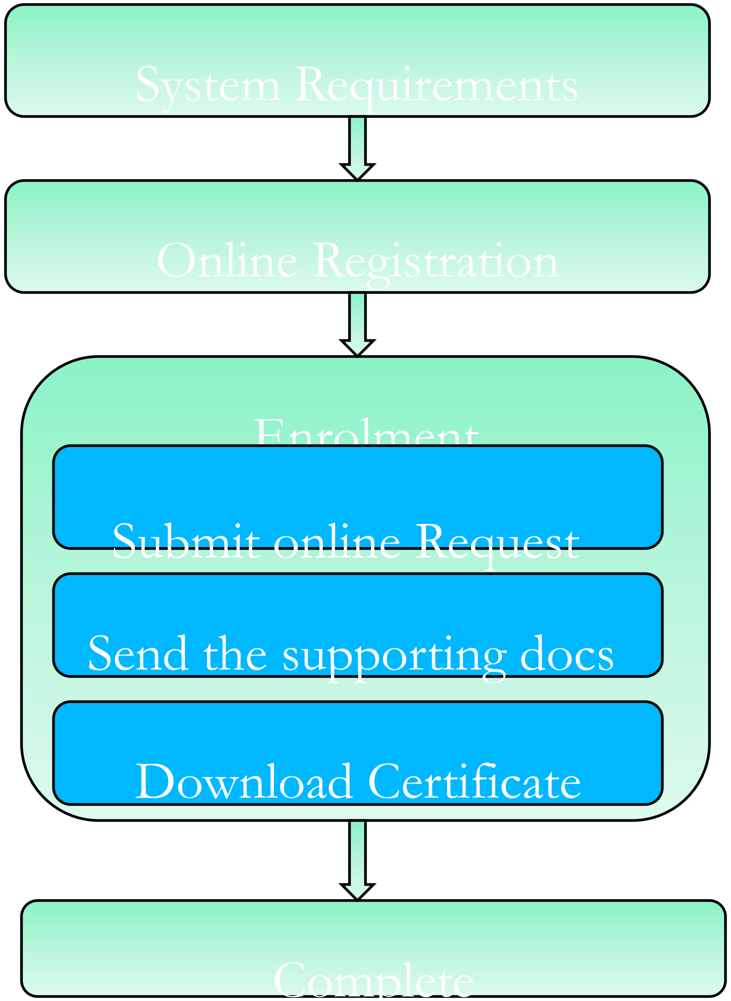
State or Province Name (full name) [Some-State]: **Telangana**

Locality Name (eg, city) []: **Hyderabad**

Organization Name (eg, company) [Internet Widgits Pty Ltd]: **ECIL**

Organizational Unit Name (eg, section) []: **IT**

Online Enrolment



System Requirements

Online Registration

Enrolment

Submit online Request

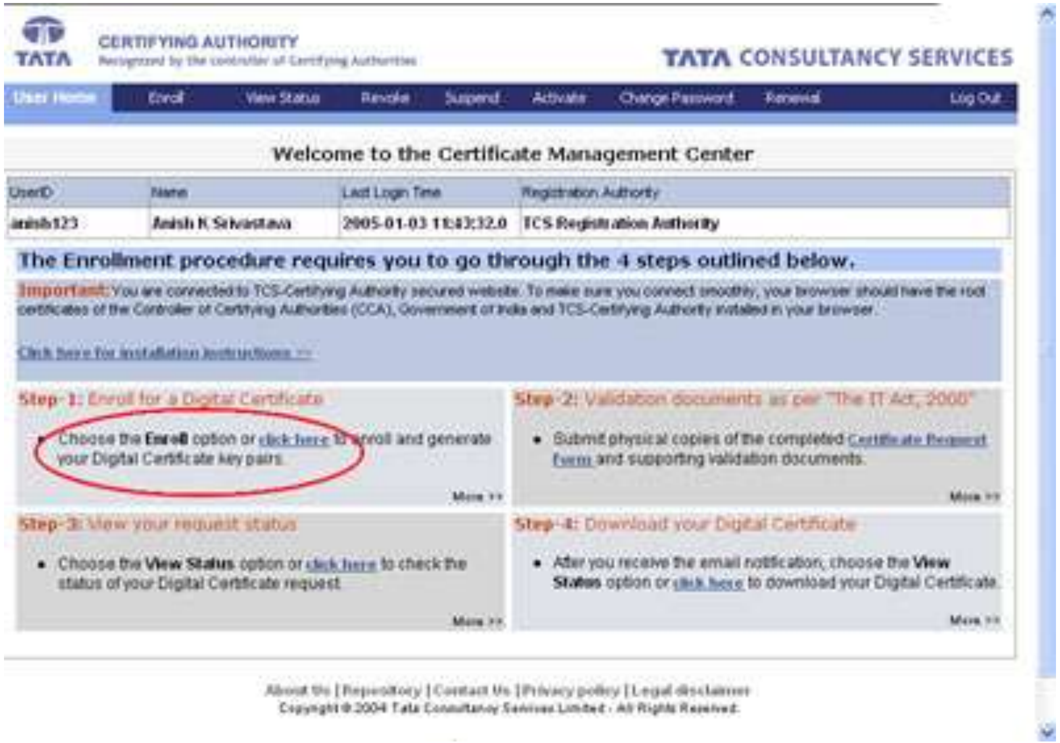
Send the supporting docs

Download Certificate

Complete

Online Enrolment

-



Welcome to the Certificate Management Center

UserID	Name	Last Login Time	Registration Authority
anish123	Anish K Srivastava	2005-01-03 11:43:32.0	TCS Registration Authority

The Enrollment procedure requires you to go through the 4 steps outlined below.

Important: You are connected to TCS-Certifying Authority secured website. To make sure you connect smoothly, your browser should have the root certificates of the Controller of Certifying Authorities (CCA), Government of India and TCS-Certifying Authority installed in your browser.

Click here for installation instructions >>

Step-1: Enroll for a Digital Certificate

- Choose the **Enroll** option or click here to enroll and generate your Digital Certificate key pairs.

More >>

Step-2: Validation documents as per "The IT Act, 2000"

- Submit physical copies of the completed Certificate Request Form and supporting validation documents.

More >>

Step-3: View your request status

- Choose the **View Status** option or click here to check the status of your Digital Certificate request.

More >>

Step-4: Download your Digital Certificate

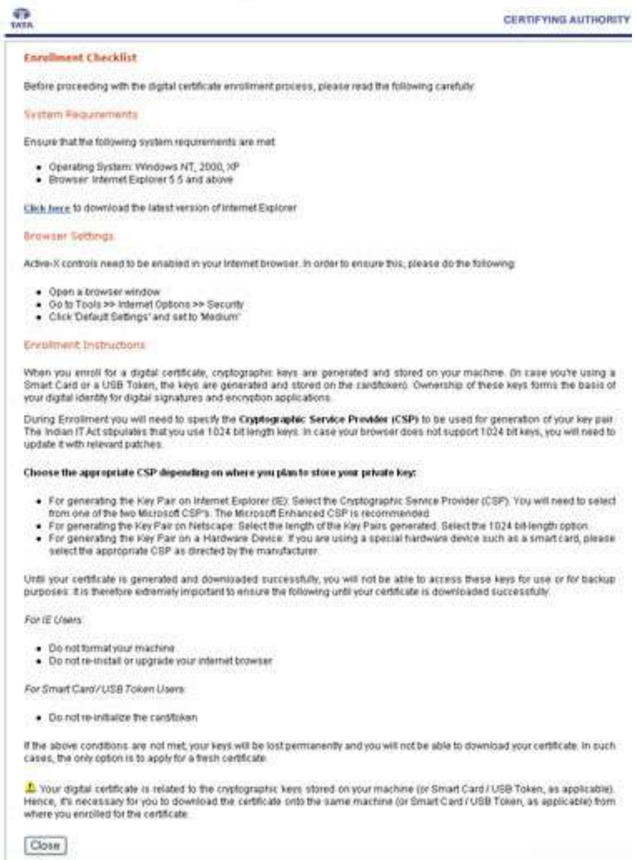
- After you receive the email notification, choose the **View Status** option or click here to download your Digital Certificate.

More >>

About Us | Repository | Contact Us | Privacy policy | Legal disclaimer

Copyright © 2004 Tata Consultancy Services Limited - All Rights Reserved.

Online Enrolment



TATA CERTIFYING AUTHORITY

Enrollment Checklist

Before proceeding with the digital certificate enrollment process, please read the following carefully

System Requirements

Ensure that the following system requirements are met

- Operating System: Windows NT, 2000, XP
- Browser: Internet Explorer 5.5 and above

Click here to download the latest version of Internet Explorer

Browser Settings

Active-X controls need to be enabled in your Internet browser. In order to ensure this, please do the following

- Open a browser window
- Go to Tools >> Internet Options >> Security
- Click 'Default Settings' and set to 'Medium'

Enrollment Instructions

When you enroll for a digital certificate, cryptographic keys are generated and stored on your machine. (In case you're using a Smart Card or a USB Token, the keys are generated and stored on the card/token). Ownership of these keys forms the basis of your digital identity for digital signatures and encryption applications.

During Enrollment you will need to specify the **Cryptographic Service Provider (CSP)** to be used for generation of your key pair. The Indian IT Act stipulates that you use 1024 bit length keys. In case your browser does not support 1024 bit keys, you will need to update it with relevant patches.

Choose the appropriate CSP depending on where you plan to store your private key:

- For generating the Key Pair on Internet Explorer (IE): Select the Cryptographic Service Provider (CSP). You will need to select from one of the two Microsoft CSP's. The Microsoft Enhanced CSP is recommended.
- For generating the Key Pair on Netscape: Select the length of the Key Pairs generated. Select the 1024 bit-length option.
- For generating the Key Pair on a Hardware Device: If you are using a special hardware device such as a smart card, please select the appropriate CSP as directed by the manufacturer.

Until your certificate is generated and downloaded successfully, you will not be able to access these keys for use or for backup purposes. It is therefore extremely important to ensure the following until your certificate is downloaded successfully.

For IE Users:

- Do not format your machine
- Do not re-install or upgrade your internet browser

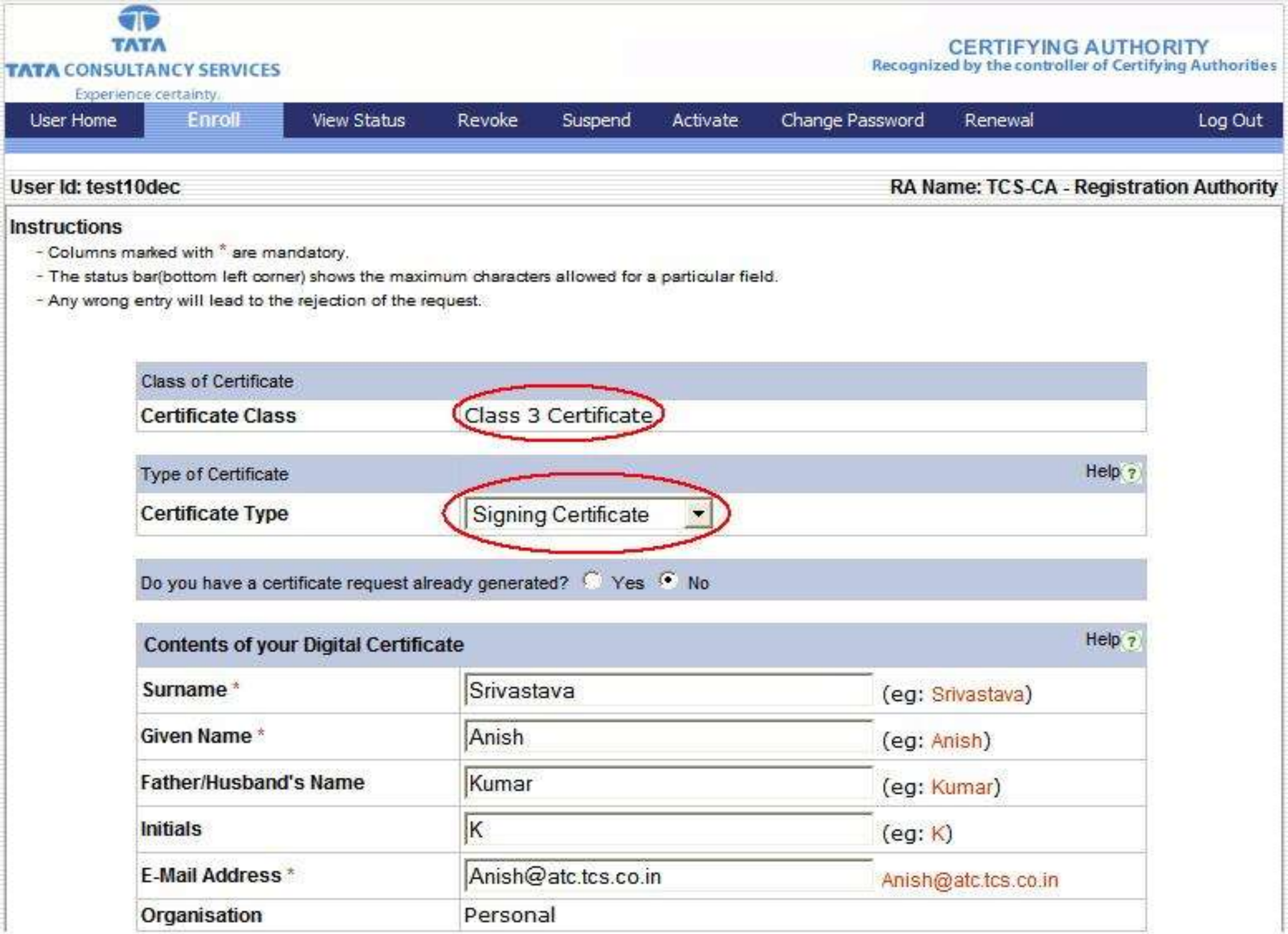
For Smart Card / USB Token Users:

- Do not re-initialize the card/token

If the above conditions are not met, your keys will be lost permanently and you will not be able to download your certificate. In such cases, the only option is to apply for a fresh certificate.

⚠ Your digital certificate is related to the cryptographic keys stored on your machine (or Smart Card / USB Token, as applicable). Hence, it's necessary for you to download the certificate onto the same machine (or Smart Card / USB Token, as applicable) from where you enrolled for the certificate.

Online Enrolment



User Id: test10dec

RA Name: TCS-CA - Registration Authority

Instructions

- Columns marked with * are mandatory.
- The status bar(bottom left corner) shows the maximum characters allowed for a particular field.
- Any wrong entry will lead to the rejection of the request.

Class of Certificate	
Certificate Class	Class 3 Certificate
Type of Certificate	
Certificate Type	Signing Certificate

Do you have a certificate request already generated? ○ Yes ● No

Contents of your Digital Certificate

Surname *	Srivastava	(eg: Srivastava)
Given Name *	Anish	(eg: Anish)
Father/Husband's Name	Kumar	(eg: Kumar)
Initials	K	(eg: K)
E-Mail Address *	Anish@atc.tcs.co.in	Anish@atc.tcs.co.in
Organisation	Personal	

Online Enrolment

- Enter the contents of your Digital Certificate

  Common Name = *Full Name of the applicant*

  E-mail Address = *Your E-mail Address*

  Organization = *Organization Name*

  Organization Unit = *Organization Unit/Division*

  Locality/ City = *(Example - hyderabad)*

  State = *(Example - Telangana)*

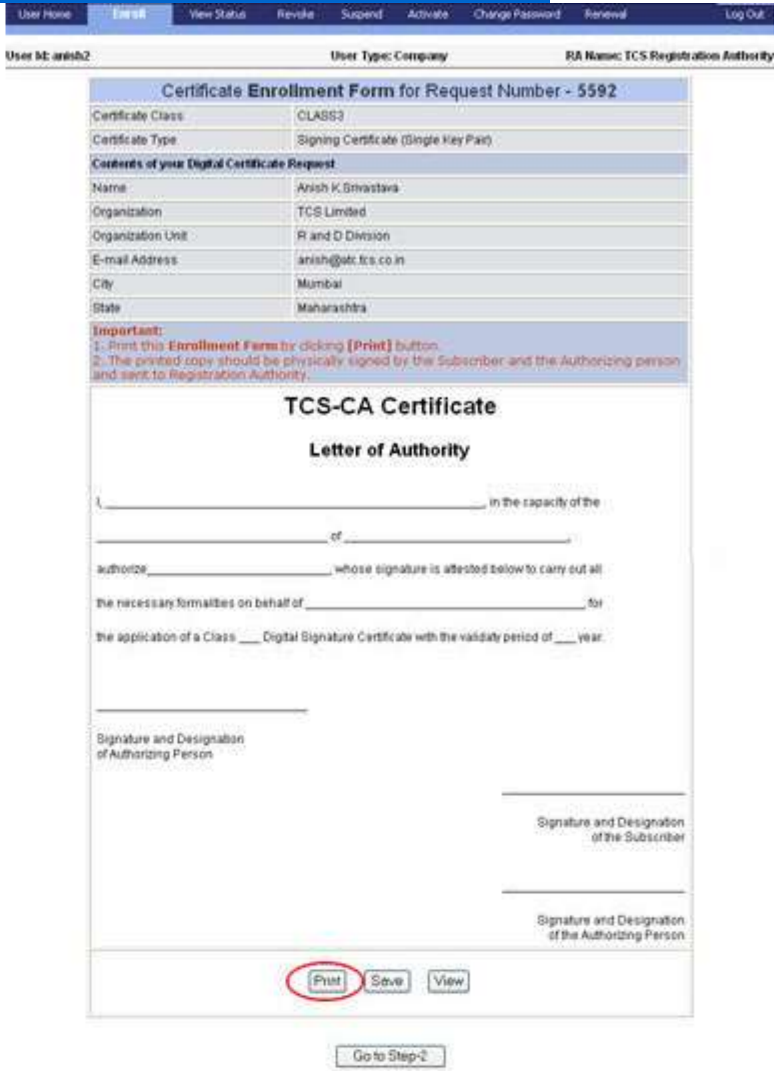
  PAN = (Example - AAAAA1111A)

- Select Cryptographic Service Provider
  - *The Cryptographic Service Provider (CSP) is the software that generates the cryptographic keys for your digital certificate. These keys form the basis of your digital identity and will be used for digital signing and encryption operations.*

Online Enrolment

- The Indian IT Act stipulates that you use 2048 bit length keys. In case your browser does not support 2048 bit keys, your browser has to be updated with the relevant patches.
- On successful completion of Certificate request and key pair generation, you will be issued a Request Number.

Online Enrolment



User Id: anish2 User Type: Company RA Name: TCS Registration Authority

Certificate Enrollment Form for Request Number - 5592

Certificate Class	CLASS3
Certificate Type	Signing Certificate (Single Key Pair)
Contents of your Digital Certificate Request	
Name	Anish K.Srivastava
Organization	TCS Limited
Organization Unit	R and D Division
E-mail Address	anish@atc.tcs.co.in
City	Mumbai
State	Maharashtra

Important:
1. Print this **Enrollment Form** by clicking **[Print]** button.
2. The printed copy should be physically signed by the Subscriber and the Authorizing person and sent to Registration Authority.

TCS-CA Certificate

Letter of Authority

I, ______________________________, in the capacity of the

______________________ of ______________________,

authorize ____________________ whose signature is attested below to carry out all

the necessary formalities on behalf of ____________________________ for

the application of a Class ___ Digital Signature Certificate with the validity period of ___ year.

____

Signature and Designation
of Authorizing Person

____

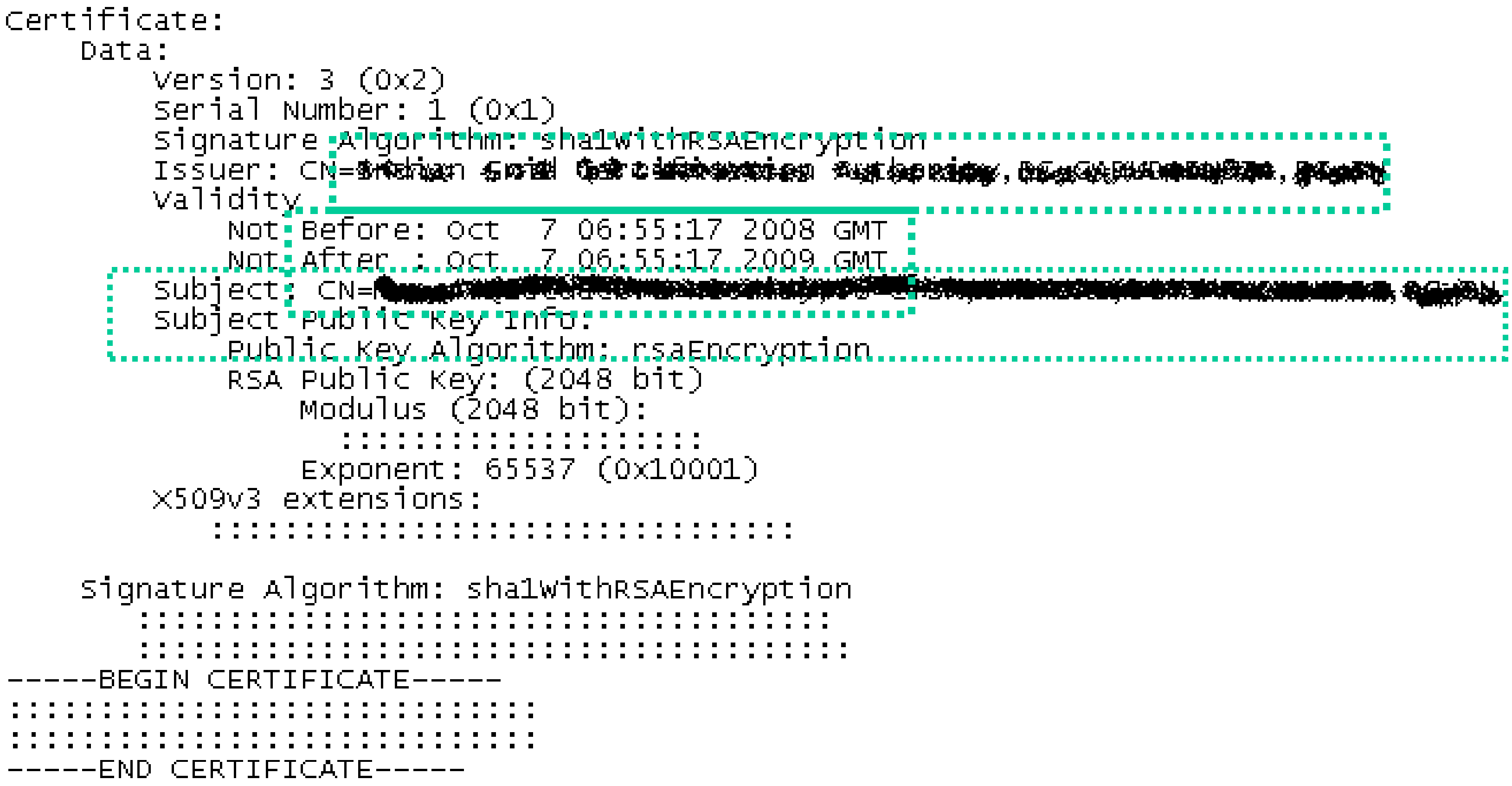
Signature and Designation
of the Subscriber

____

Signature and Designation
of the Authorizing Person

Digital Certificate

- A digital certificate has a defined validity period



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=[redacted]
        Validity
            Not Before: Oct  7 06:55:17 2008 GMT
            Not After : Oct  7 06:55:17 2009 GMT
        Subject: CN=[redacted]
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                  :::::::::::::::::::
                Exponent: 65537 (0x10001)
        X509v3 extensions:
           :::::::::::::::::::::::::::::::

    Signature Algorithm: sha1WithRSAEncryption
       :::::::::::::::::::::::::::::::::::::
       ::::::::::::::::::::::::::::::::::::::
-----BEGIN CERTIFICATE-----
::::::::::::::::::::::::::::
::::::::::::::::::::::::::::
-----END CERTIFICATE-----
```

Certificate Distribution

- CA acts as a trusted third-party issuing certificates to users.
  - Direct to owner (Email)
  - To repository
  - Both

Certificate Expiration

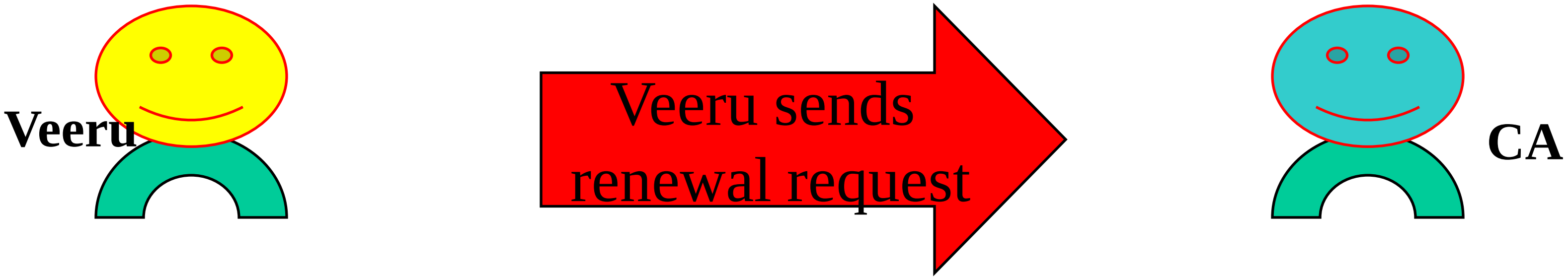
- Certificate Expiration
  - Natural “peaceful” end of life
  - No action

Certificate Renewal/Rekey/Re-Issuance

Procedure	Identifying Info	Public Keys	Validity Period
Renewal	Same	Same	Different
Rekey	Same	Different	Different
Re-Issuance	Different	Different	Different

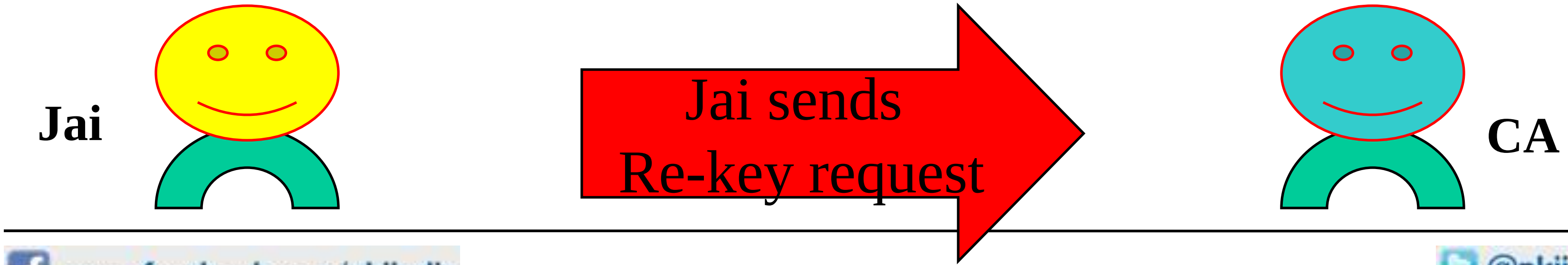
Certificate Renewal

- If Veeru wants renew his expiring certificate he sends a renewal request to CA, and digitally signs with his old certificate.
- CA issues a new certificate with new validity period
  - If there is an overlap in the validity periods, CA can place the old certificate in his CRL



Certificate Re-keying

- Suppose Jai decides to change his public and private key pairs (Old keys need not necessarily be compromised)
- He generates new key pair
- He creates a re-key request including his new public key, digitally signs with his old private key and sends request to CA
- CA creates new certificate with the new public key and adds the old certificate to CRL



Certificate Revocation

- Veeru’s private key has been compromised
  - Before some one uses his key, he wants to revoke his certificate
  - He generates a new key pair and sends public key to CA and obtains a new certificate
  - CA adds the old certificate to the CRL

CRL

- What is revocation?
- Why do we need it?
- What is currently being done?

Why Revoke?

- Key Compromise
- Forgotten Passphrase
- Lost Private Key

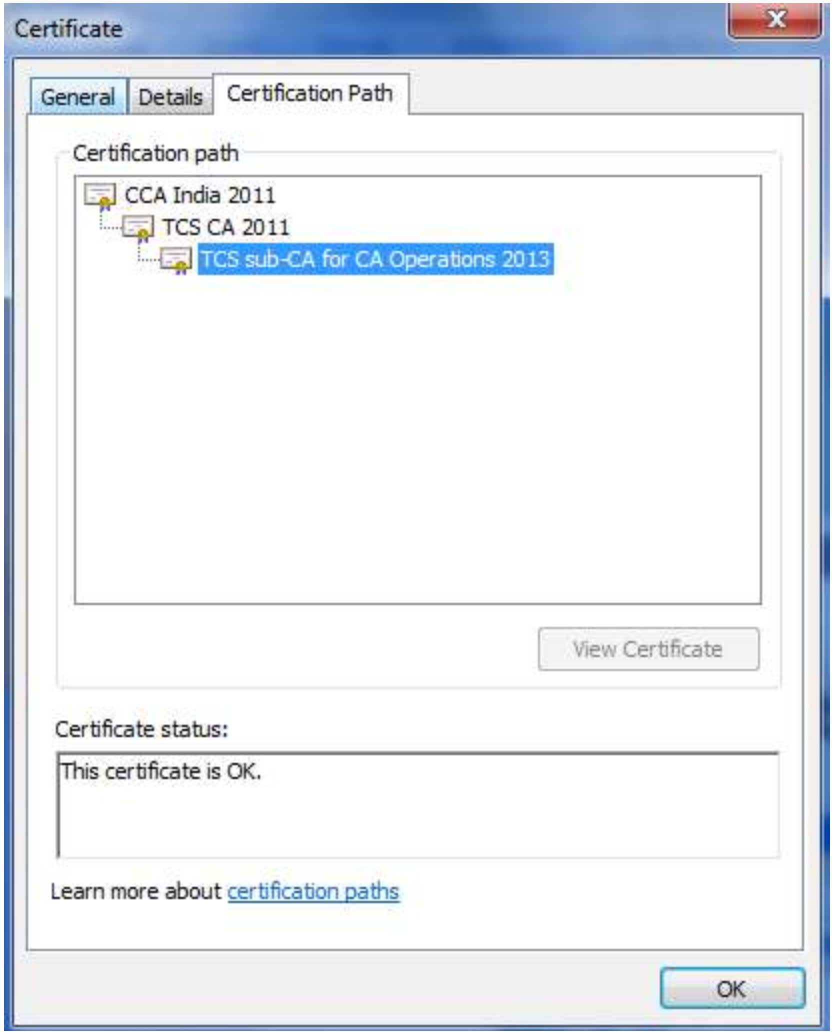
CRL

- CRL is a periodically issued list of digital signature certificates that have been suspended or revoked prior to their expiration dates. It is digitally signed by Certifying Authority.

Current Standard

- Certificate Revocation Lists (CRLs)
  - Serial Numbers
  - Revocation Date
  - Effective Date
  - Next Update Date
  - CA Signed
  - *Should Be* Publically Available.

Obtaining CRLs

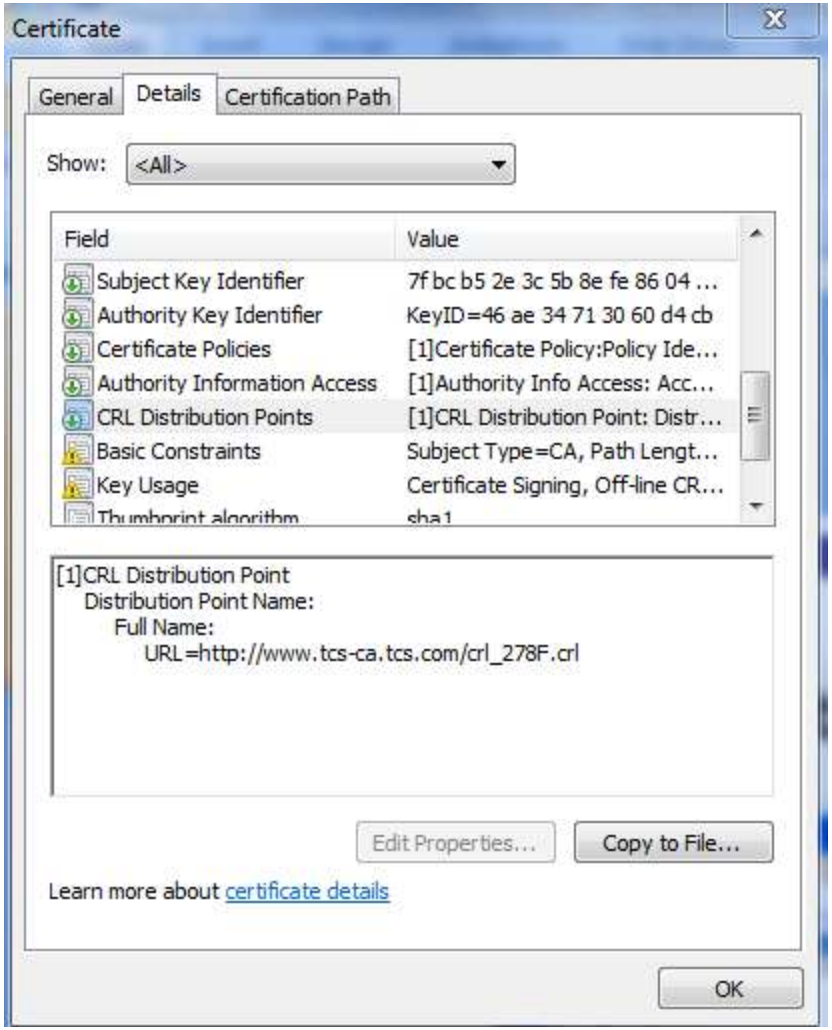


Certification path

- CCA India 2011
  - TCS CA 2011
    - TCS sub-CA for CA Operations 2013

Certificate status:

This certificate is OK.

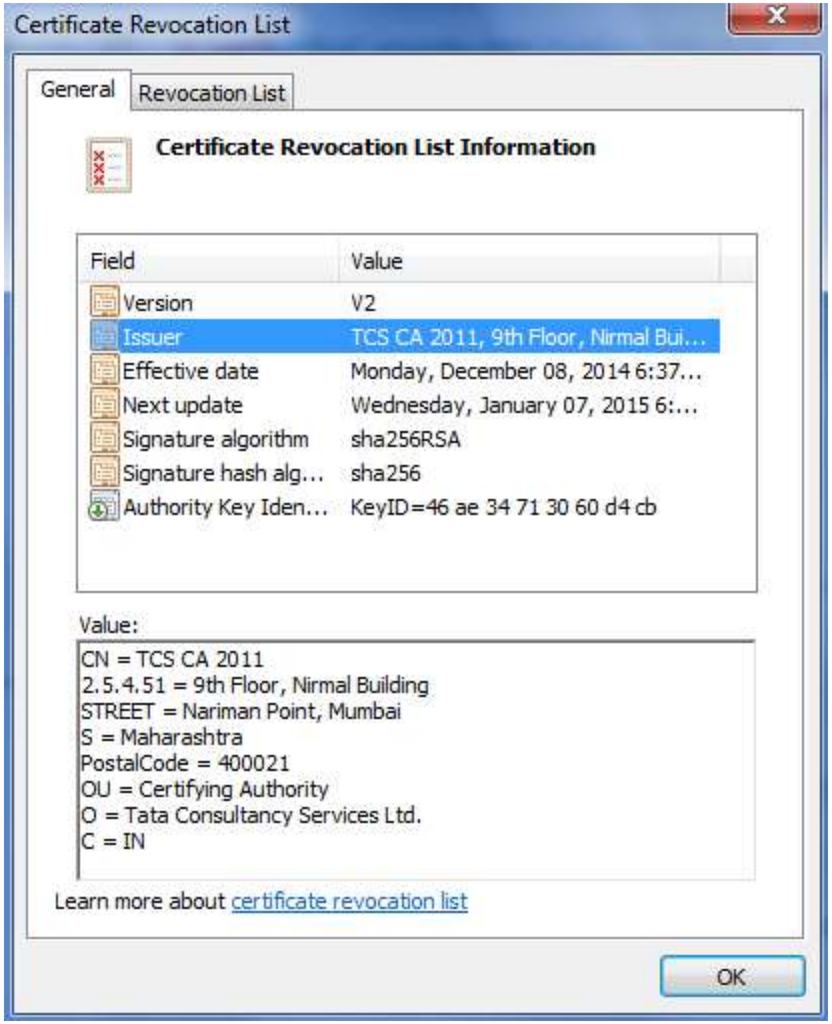


Show: <All>

Field	Value
Subject Key Identifier	7f bc b5 2e 3c 5b 8e fe 86 04 ...
Authority Key Identifier	KeyID=46 ae 34 71 30 60 d4 cb
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Certificate Signing, Off-line CR...
Thumbprint algorithm	sha1

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://www.tcs-ca.tcs.com/crl_278F.crl
```

CRLs



Certificate Revocation List

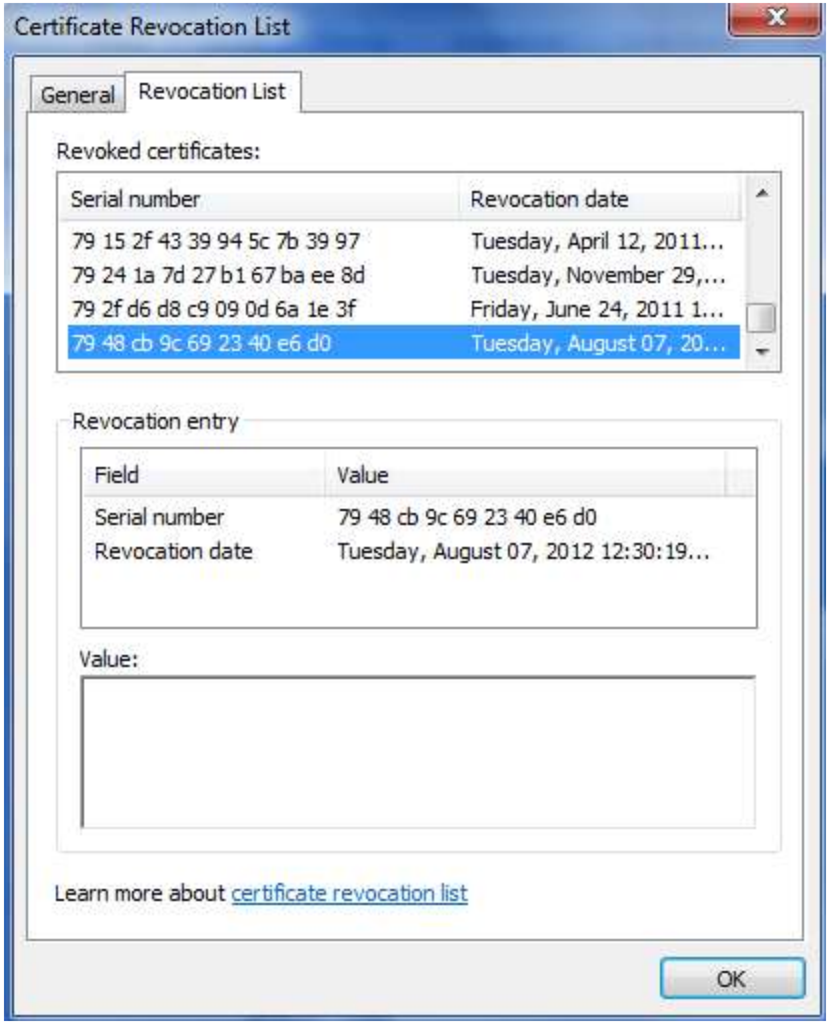
Certificate Revocation List Information

Field	Value
Version	V2
Issuer	TCS CA 2011, 9th Floor, Nirmal Bui...
Effective date	Monday, December 08, 2014 6:37...
Next update	Wednesday, January 07, 2015 6:...
Signature algorithm	sha256RSA
Signature hash alg...	sha256
Authority Key Iden...	KeyID=46 ae 34 71 30 60 d4 cb

Value:

```
CN = TCS CA 2011
2.5.4.51 = 9th Floor, Nirmal Building
STREET = Nariman Point, Mumbai
S = Maharashtra
PostalCode = 400021
OU = Certifying Authority
O = Tata Consultancy Services Ltd.
C = IN
```

Learn more about certificate revocation list



Certificate Revocation List

Revoked certificates:

Serial number	Revocation date
79 15 2f 43 39 94 5c 7b 39 97	Tuesday, April 12, 2011...
79 24 1a 7d 27 b1 67 ba ee 8d	Tuesday, November 29,...
79 2f d6 d8 c9 09 0d 6a 1e 3f	Friday, June 24, 2011 1...
79 48 cb 9c 69 23 40 e6 d0	Tuesday, August 07, 20...

Revocation entry

Field	Value
Serial number	79 48 cb 9c 69 23 40 e6 d0
Revocation date	Tuesday, August 07, 2012 12:30:19...

Value:

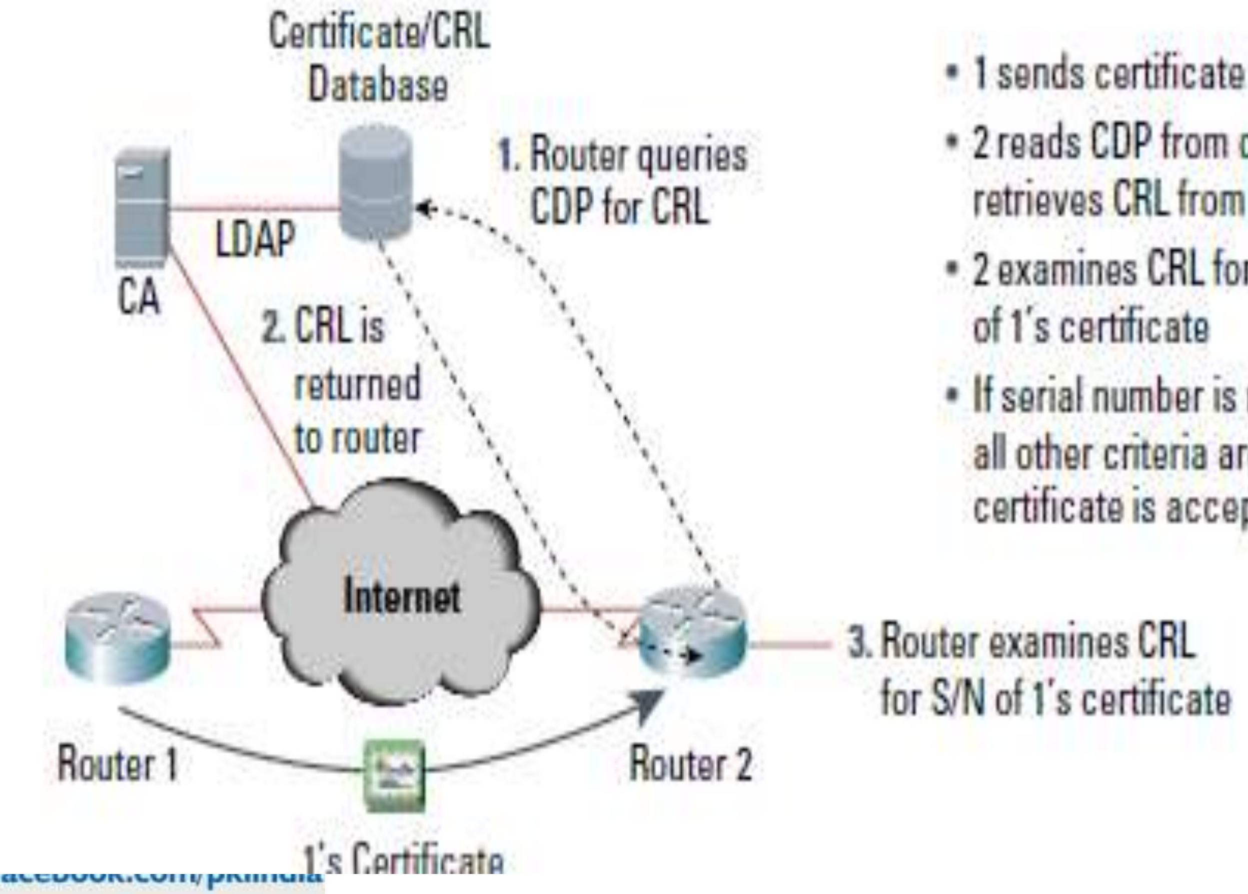
Learn more about certificate revocation list

Checking status with CRL

CDP – CRL Distribution Point

Figure 1

Cert Validation with CRL


Certificate/CRL Database
CA
LDAP
1. Router queries CDP for CRL
2. CRL is returned to router
Internet
Router 1
Router 2
3. Router examines CRL for S/N of 1's certificate
1's Certificate

- 1 sends certificate to 2
- 2 reads CDP from certificate, retrieves CRL from CDP
- 2 examines CRL for serial number of 1's certificate
- If serial number is not found and all other criteria are good, certificate is accepted

What are the problems…

- CRL does not provide timely information regarding revocation status of a digital certificate.
- Every time end user have to download CRL and import it in the browser or in other certificate repository for checking status of digital certificate.
- If serial number of digital certificate is not present in CRL then we simply trust that certificate.

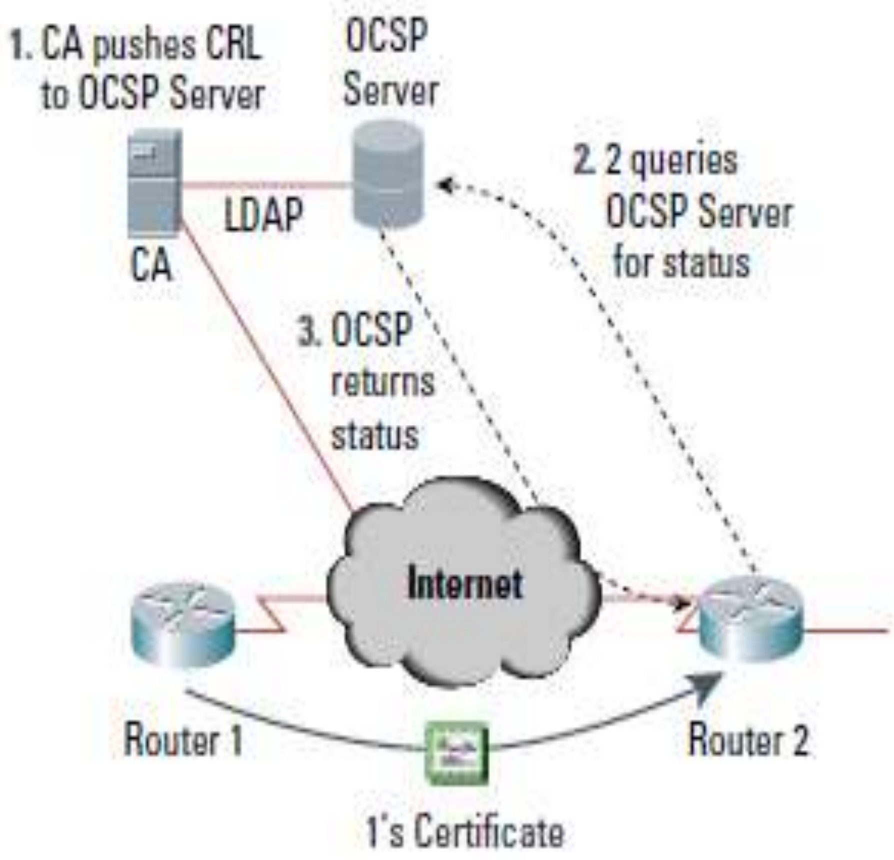
Online Certificate Status Protocol

- 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.

Checking status with OCSP

Figure 2

Cert Validation with OCSP



- 1 sends certificate to 2
- 2 requests certificate staus from OCSP Server
- OCSP replies with status

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 of the certificate.

OCSP - Response

OCSP responses are of 3 types & all response messages will be digitally signed.

- Good – Indicates that the certificate is not revoked, but does not indicate that certificate was ever issued or time at which response produced is within the certificate's validity interval.
- Revoked – Indicates that the certificate has been revoked.
- Unknown – Indicates that the responder doesn't know about the certificate being requested.

OCSP Exception/Error Messages

Error messages are not signed. Error are of following types:

- Malformed Request – When request received does not conform to the OCSP syntax.
- Internal Error – Due to inconsistent internal state.
- Try Later – When OCSP is unable to return a status for requested certificate.
- SigRequired – When server requires the client sign the request in order to construct a response.
- Unauthorized – When client is not authorized to make this query to the server.

References

- www.ietf.org/**rfc**/**rfc**2560.txt
- Cryptography and Network Security - Atu Kahate

Thank You