Understanding HTTPS CRL and OCSP

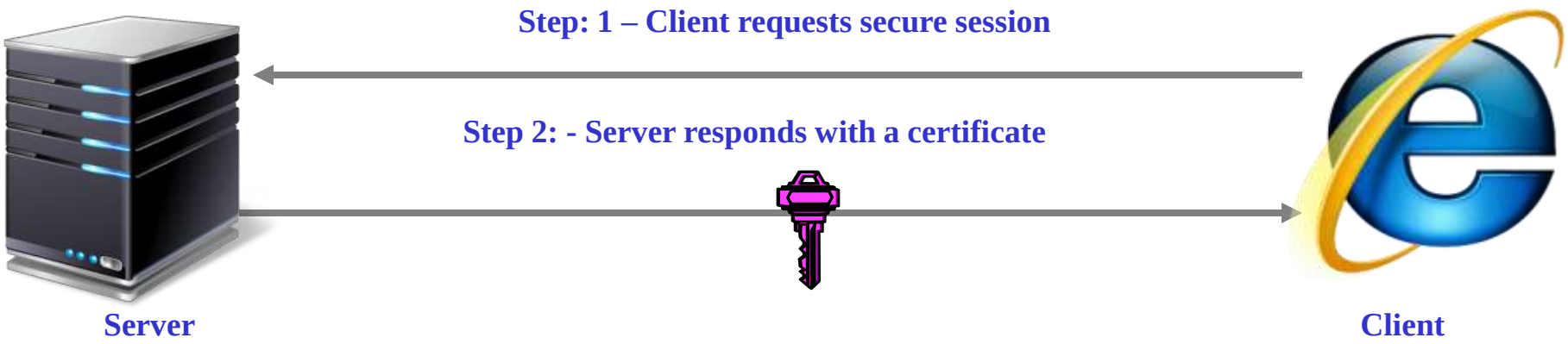
Santhosh J

PKI Body of Knowledge: Development & Dissemination
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Understanding HTTPS



Understanding HTTPS

Client validates Server's Certificate

```
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-----
```

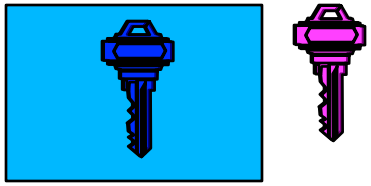
Client

Step 3: Verifies CA's digital signature To ensure Server certificate is valid & not tampered.

CA Public Key

Understanding HTTPS

Step 3: - Client creates symmetric key and encrypts it with public key

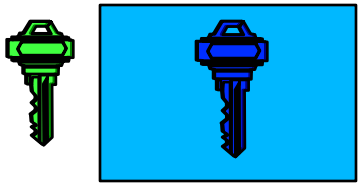


Step 4: - Encrypted symmetric key sent to the server

UcaNPA$$

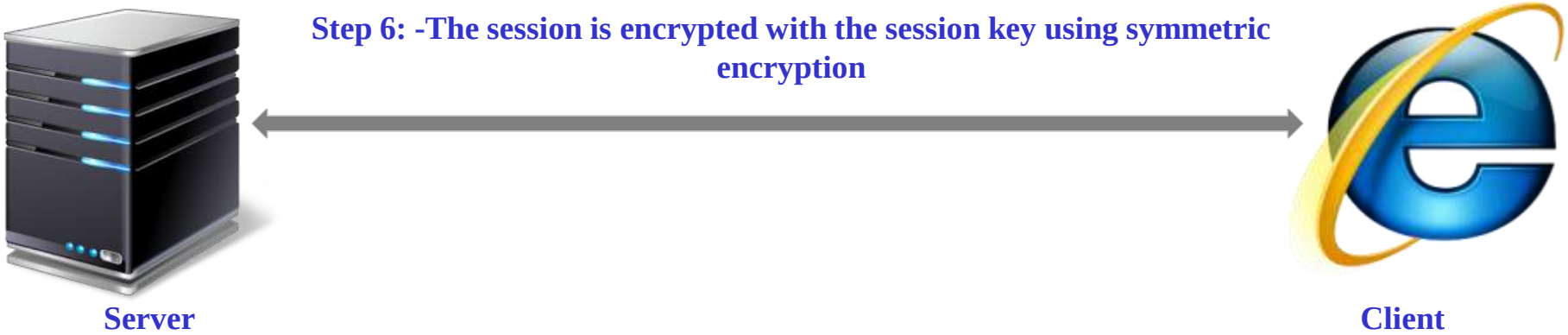
Server

Client



Step 5: - Server decrypts symmetric key with private key

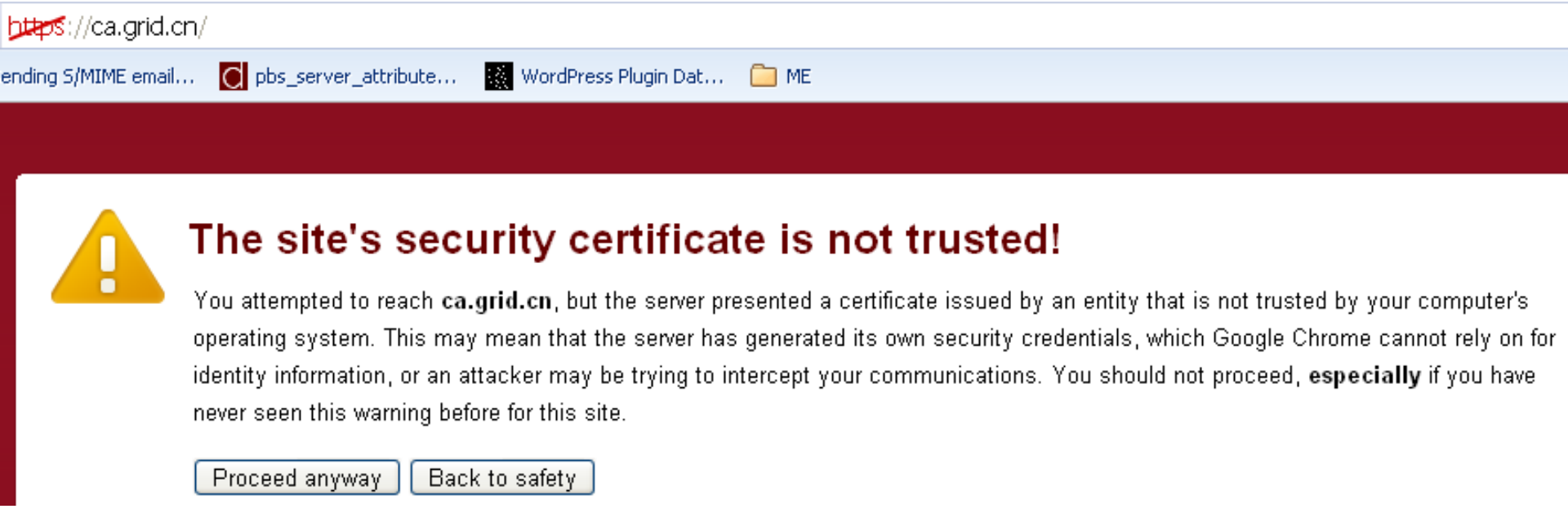
Understanding HTTPS



Some real world examples… ☺

SSL : Site security certificate

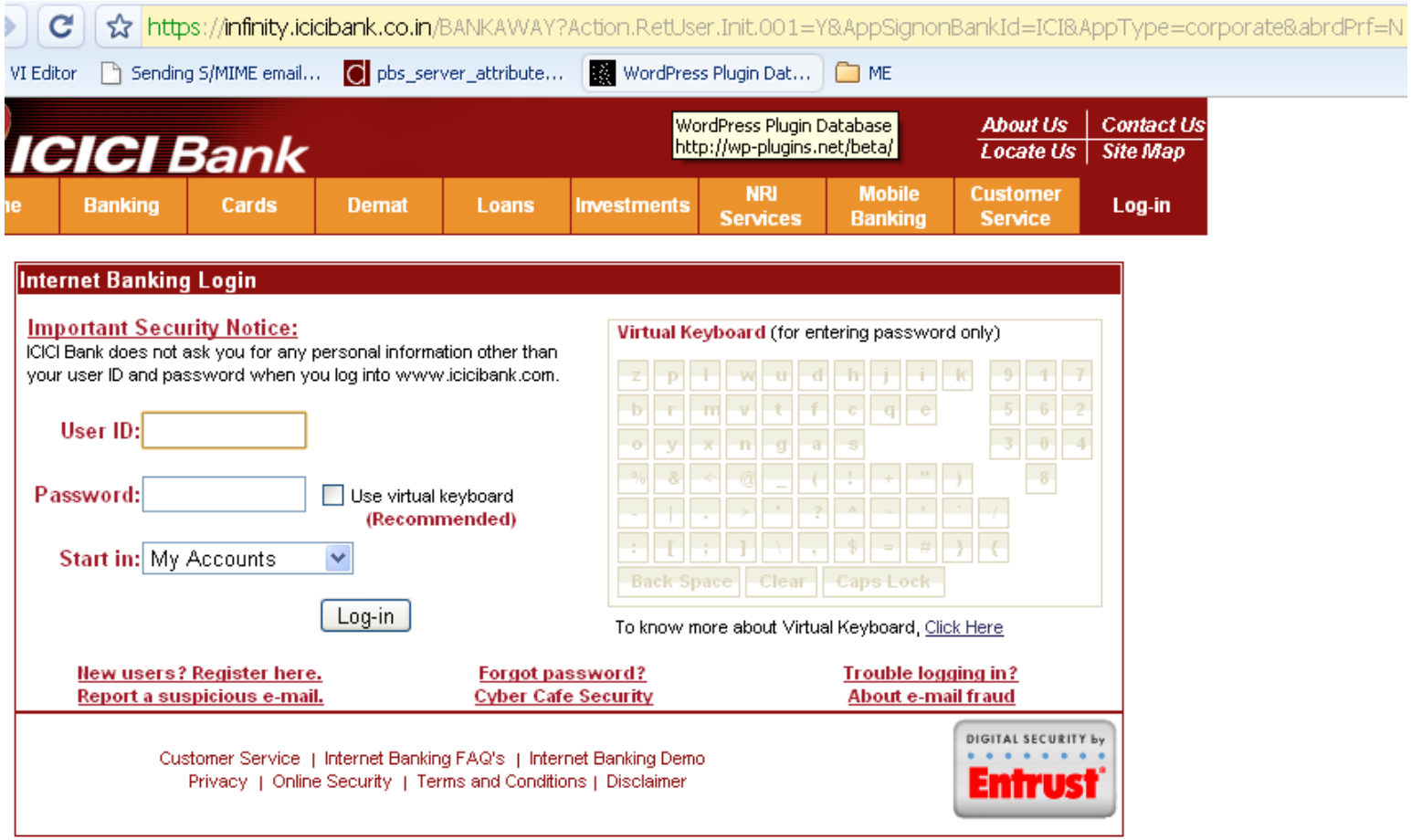
https://ca.grid.cn



Web browser doesn't trust the server certificate

SSL : Site security certificate

https://icicibank.com



Web browser Trusts the certificate issued to icicibank.com

CRL

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

Why Revoke?

- Key Compromise
- Forgotten Passphrase
- Lost Private Key

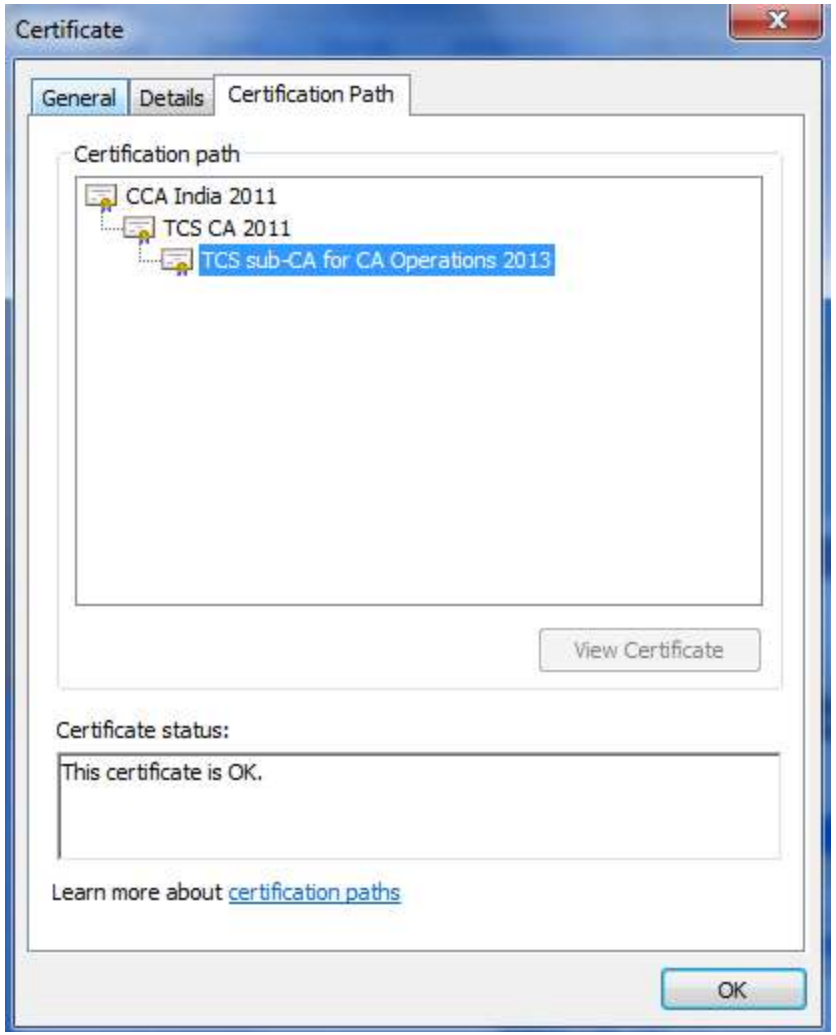
CRL

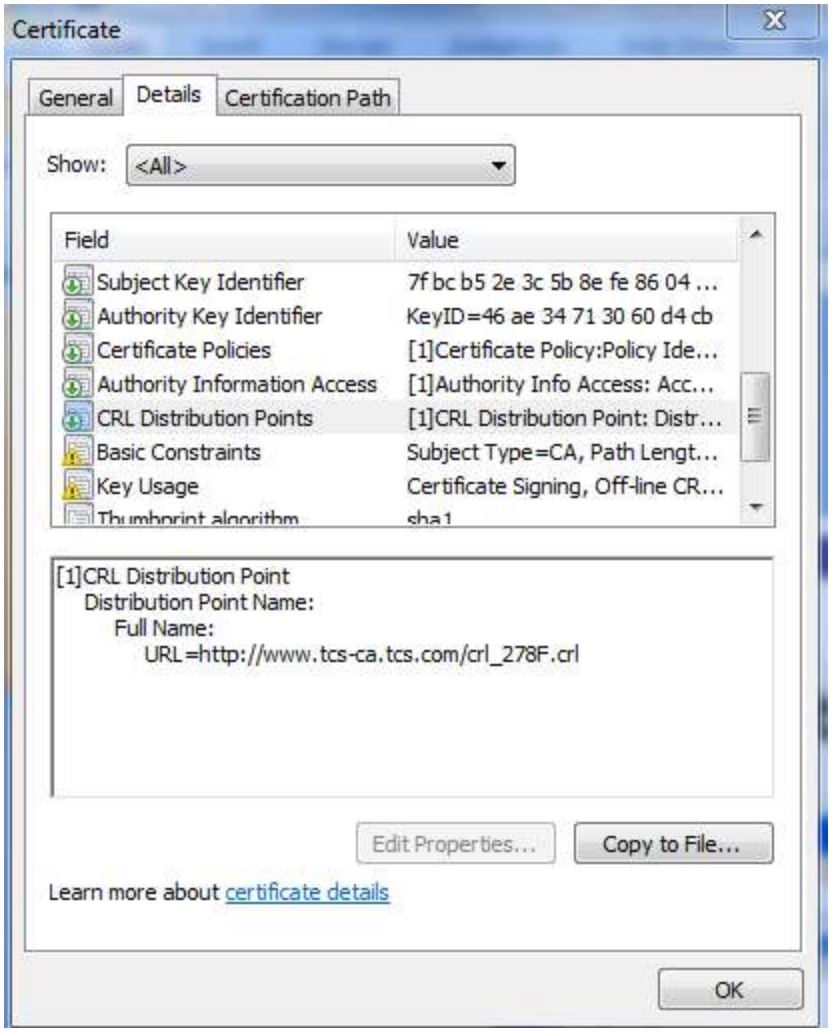
- CRL is a periodically issued list of digital signature certificates that have been suspended or revoked prior to their expiration dates. It is digitally signed by Certifying Authority.

Current Standard

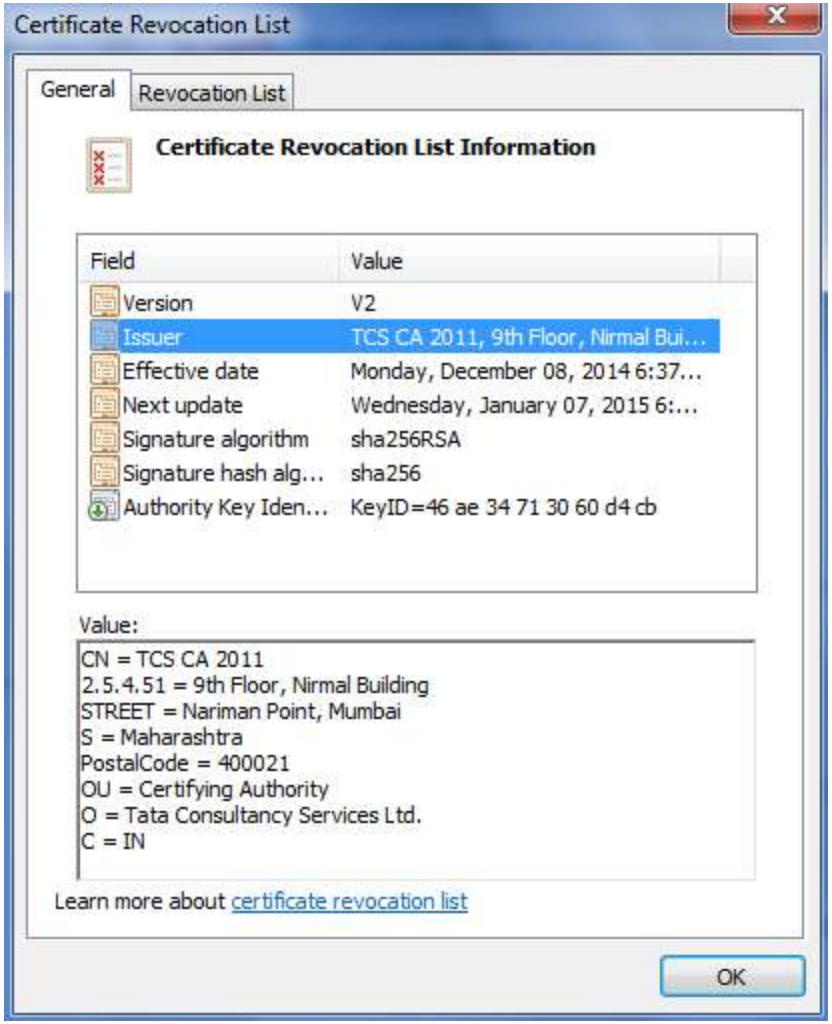
- Certificate Revocation Lists (CRLs)
  - Serial Numbers
  - Revocation Date
  - Effective Date
  - Next Update Date
  - CA Signed
  - *Should Be* Publically Available.

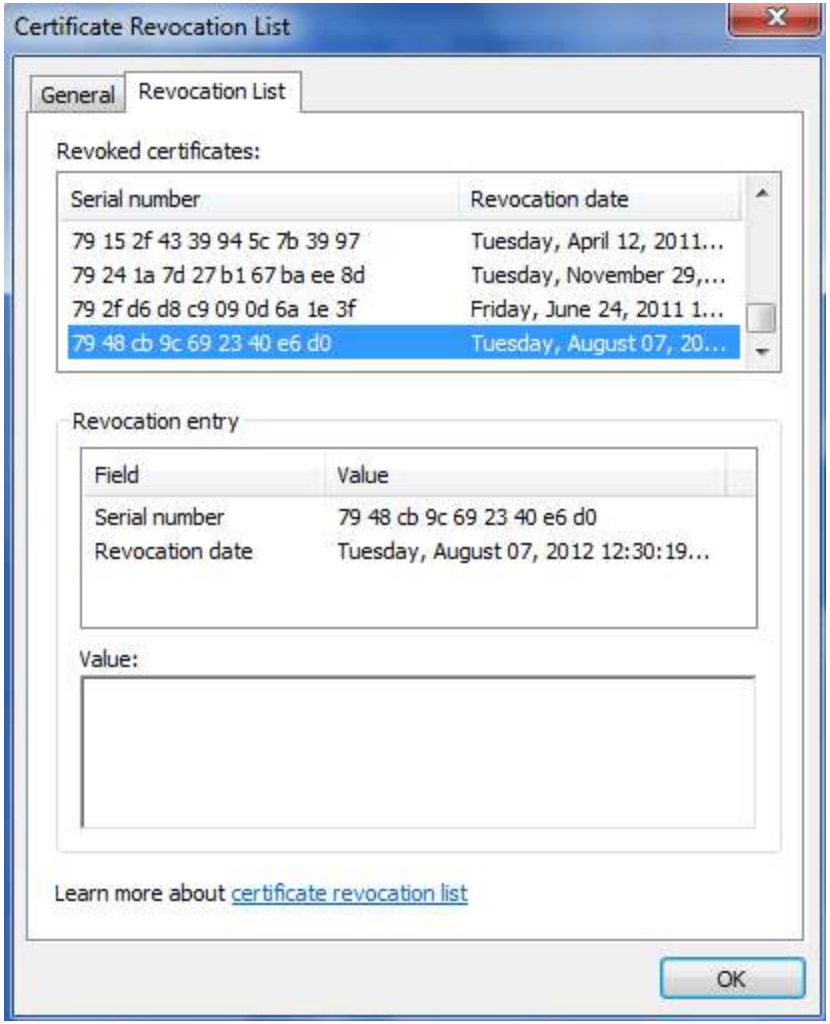
Obtaining CRLs





CRLs

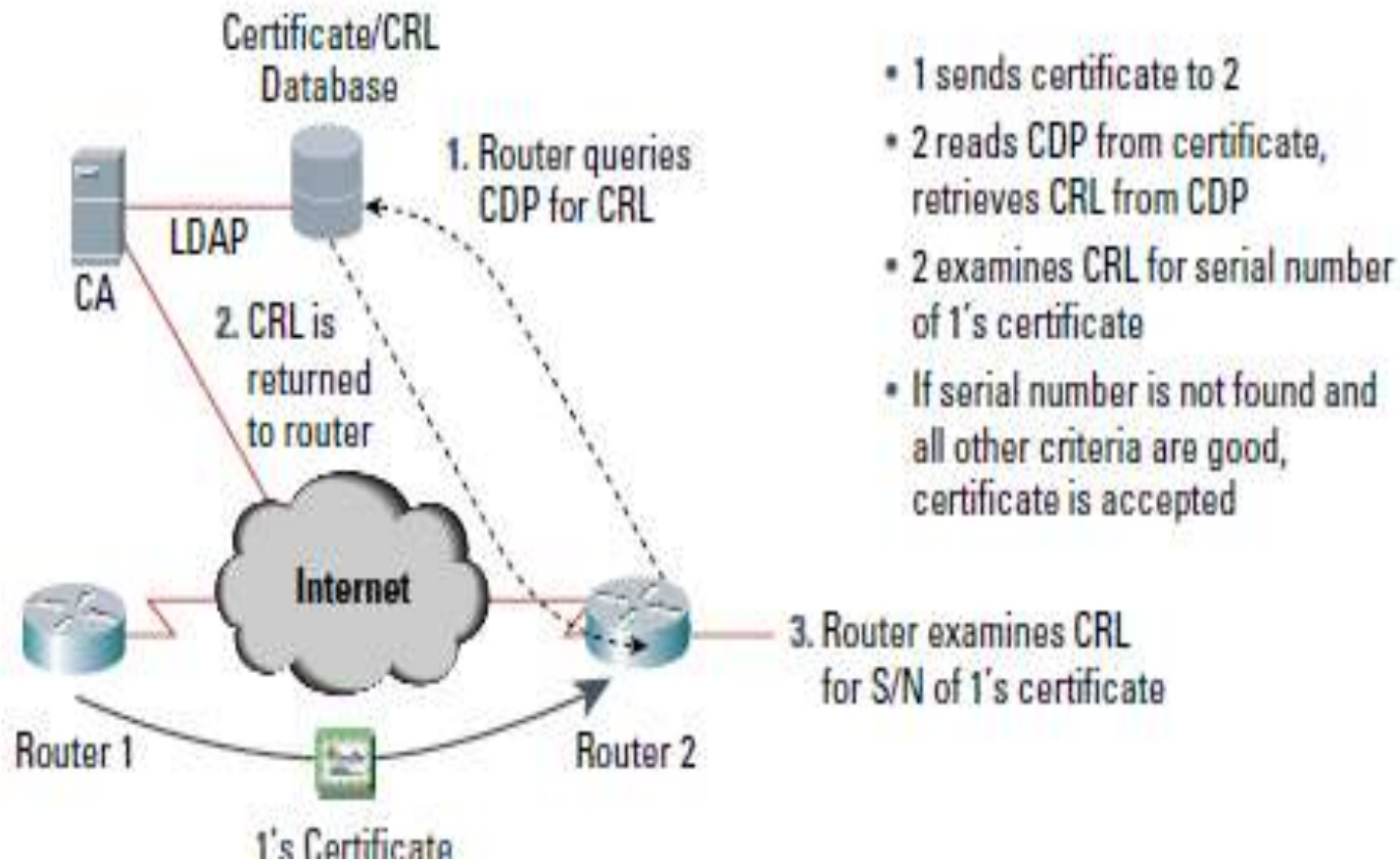




Checking status with CRL

CDP – CRL Distribution Point

Figure 1
Cert Validation with CRL



What are the problems…

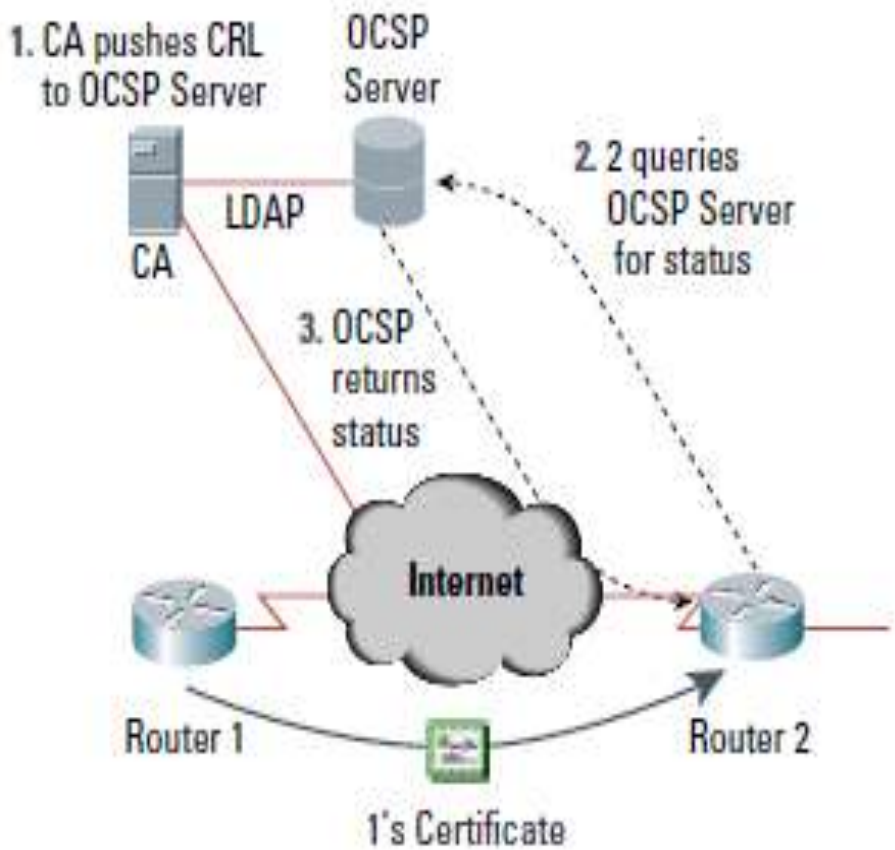
- CRL does not provide timely information regarding revocation status of a digital certificate.
- Every time end user have to download CRL and import it in the browser or in other certificate repository for checking status of digital certificate.
- If serial number of digital certificate is not present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