Online Certificate status Protocol (OCSP)

DITISS 2015

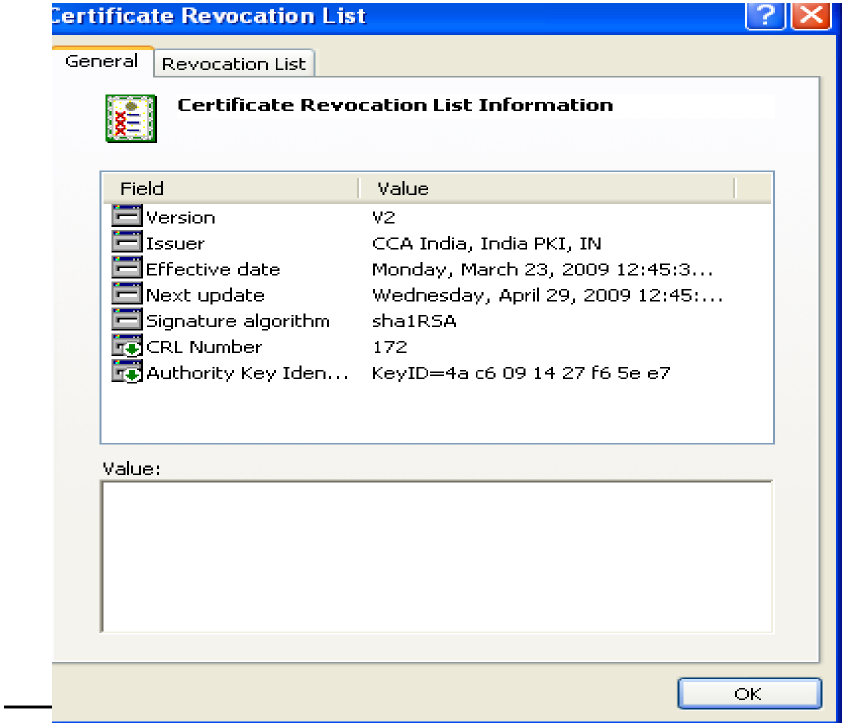
How can we validate digital certificate?

There are following two ways by which we can validate a digital certificate

1. CRL (Certificate Revocation List)
2. OCSP (Online Certificate Status Protocol)

CRL

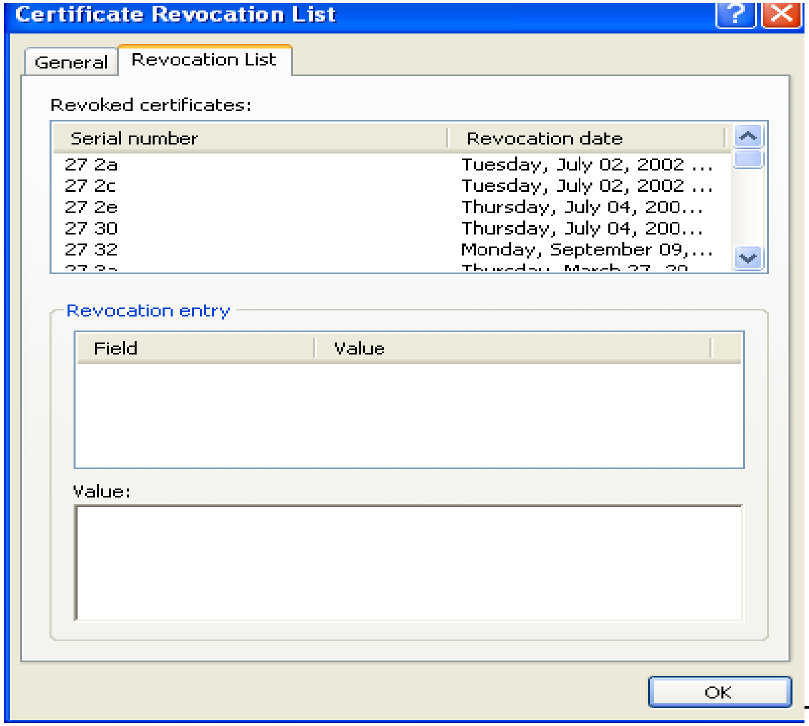
- In the operation of PKI, a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial number of certificates) that have been revoked or are no longer valid.



Certificate Revocation List Information

Field	Value
Version	V2
Issuer	CCA India, India PKI, IN
Effective date	Monday, March 23, 2009 12:45:3...
Next update	Wednesday, April 29, 2009 12:45:...
Signature algorithm	sha1RSA
CRL Number	172
Authority Key Iden...	KeyID=4a c6 09 14 27 f6 5e e7

Value:



Revoked certificates:

Serial number	Revocation date
27 2a	Tuesday, July 02, 2002 ...
27 2c	Tuesday, July 02, 2002 ...
27 2e	Thursday, July 04, 200...
27 30	Thursday, July 04, 200...
27 32	Monday, September 09,...

Revocation entry

Field	Value

Value:

Limitations of CRL

- CRL does not provide more timely information regarding revocation status of a digital certificate.

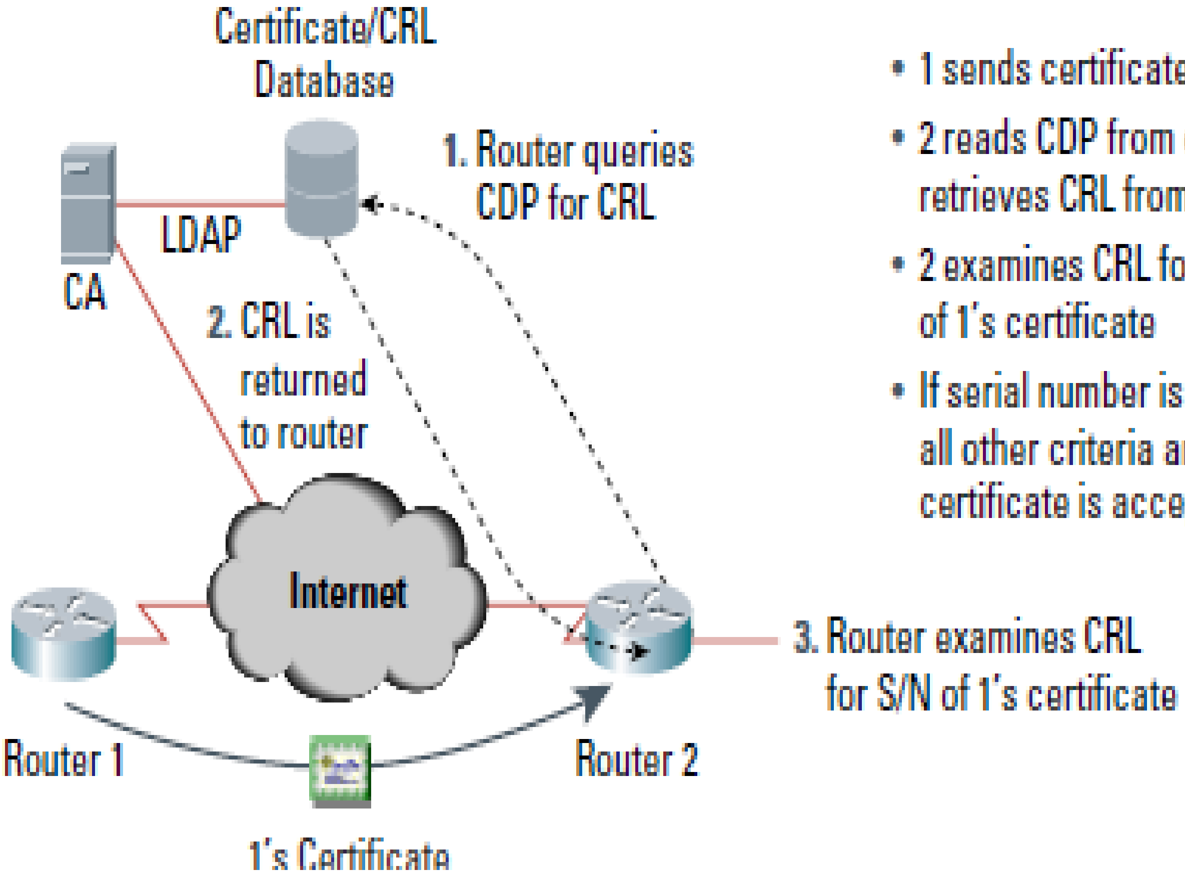
- Every time end user have to download crl and import it in browser or in other certificate repository for checking status of digital certificate.

- If serial number of digital certificate is not present in crl then we simply trust that certificate.

Checking status with CRL

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

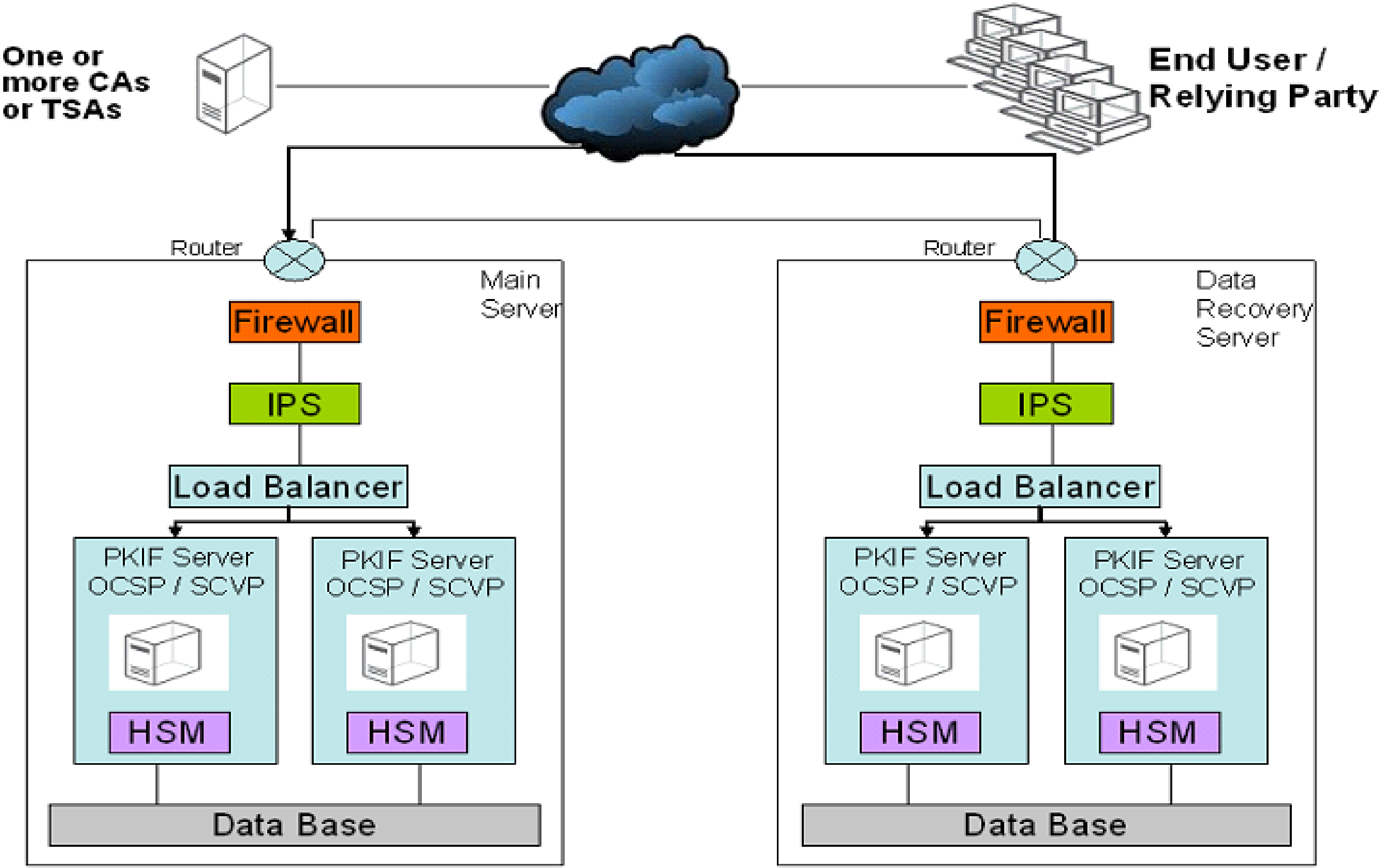
OCSP

- The Online certificate status protocol 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.

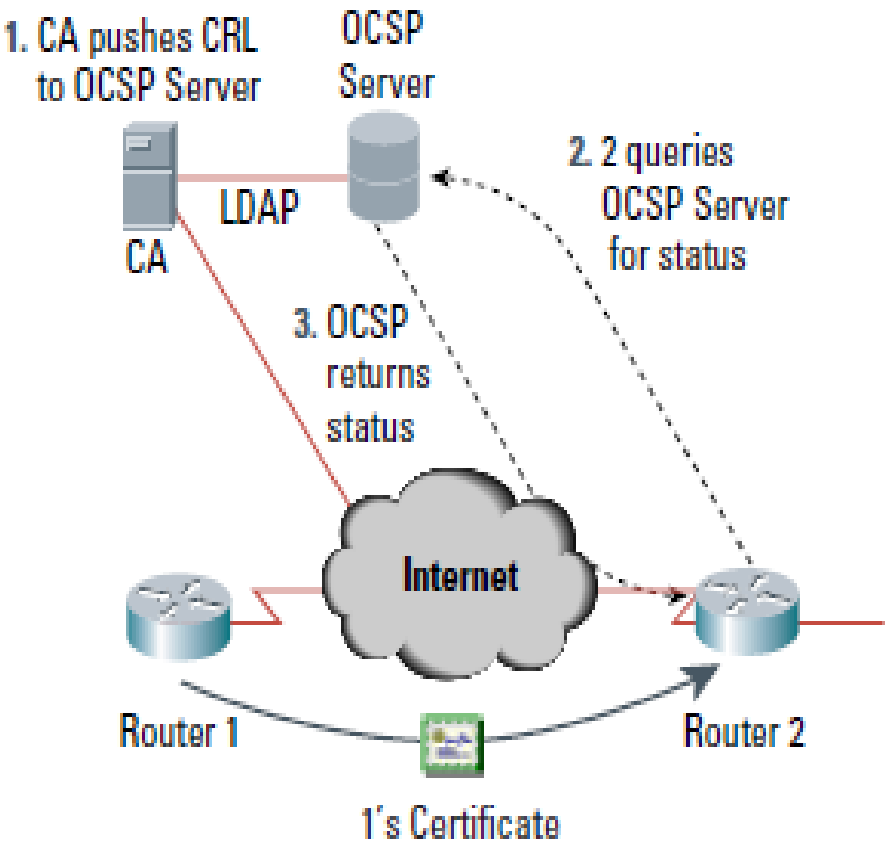
OCSP Architecture



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-complaint 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 validity of the certificate.
- 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