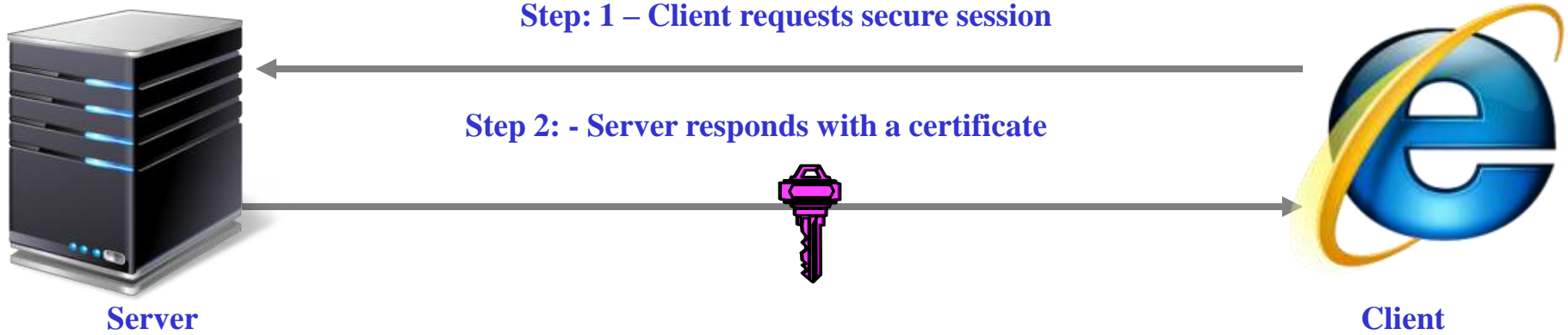


Understanding HTTPS CRL and OCSP

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



Client validates Server's Certificate

Certificate:

Data:



```

Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha1withRSAEncryption
Issuer: CN=Indian Grid Certification Authority, DC=CA, DC=IN, DC=GOV, DC=IN
Validity
  Not Before: Oct  7 06:55:17 2008 GMT
  Not After : Oct  7 06:55:17 2009 GMT
Subject: CN=
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
  Modulus (2048 bit):
    .....
  Exponent: 65537 (0x10001)
x509v3 extensions:
  .....
  
```



Client

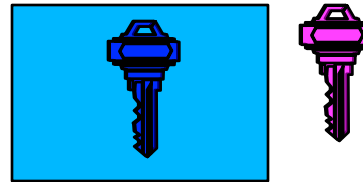
```

Signature Algorithm: sha1withRSAEncryption
.....
-----BEGIN CERTIFICATE-----
.....
-----END CERTIFICATE-----
  
```

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

CA Public Key

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

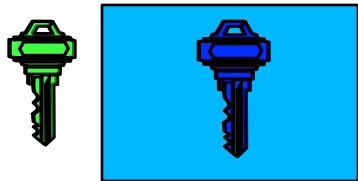


Server



Client

Step 4: - Encrypted symmetric key sent to the server



Step 5: - Server
decrypts symmetric
key with private key



Server

Step 6: -The session is encrypted with the session key using symmetric encryption



Client

Some real world examples... 😊

<https://ca.grid.cn>

~~https://ca.grid.cn/~~

ending S/MIME email...  pbs_server_attribute...  WordPress Plugin Dat...  ME



The site's security certificate is not trusted!

You attempted to reach **ca.grid.cn**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway

Back to safety

Web browser doesn't trust the server certificate

<https://icicibank.com>



ICICI Bank WordPress Plugin Database <http://wp-plugins.net/beta/> [About Us](#) [Contact Us](#)
[Locate Us](#) [Site Map](#)

[Home](#)
[Banking](#)
[Cards](#)
[Demat](#)
[Loans](#)
[Investments](#)
[NRI Services](#)
[Mobile Banking](#)
[Customer Service](#)
[Log-in](#)

Internet Banking Login

Important Security Notice:
 ICICI Bank does not ask you for any personal information other than your user ID and password when you log into www.icicibank.com.

User ID:

Password: Use virtual keyboard
(Recommended)

Start in:

Virtual Keyboard (for entering password only)


z	p	l	w	u	d	h	j	i	k	9	1	7
b	r	m	v	t	f	c	q	e		5	6	2
o	y	x	n	g	a	s				3	0	4
%	&	<	@	_	(:	+	")	8		
-		.	>	'	?	^	-	^	^			
:	!	!	!	!	!	!	!	!	!			
Back Space			Clear			Caps Lock						

To know more about Virtual Keyboard, [Click Here](#)

[New users? Register here.](#)
[Forgot password? Cyber Cafe Security](#)
[Trouble logging in? About e-mail fraud](#)

[Report a suspicious e-mail.](#)

Customer Service | Internet Banking FAQ's | Internet Banking Demo
 Privacy | Online Security | Terms and Conditions | Disclaimer



Web browser Trusts the certificate issued to icicibank.com

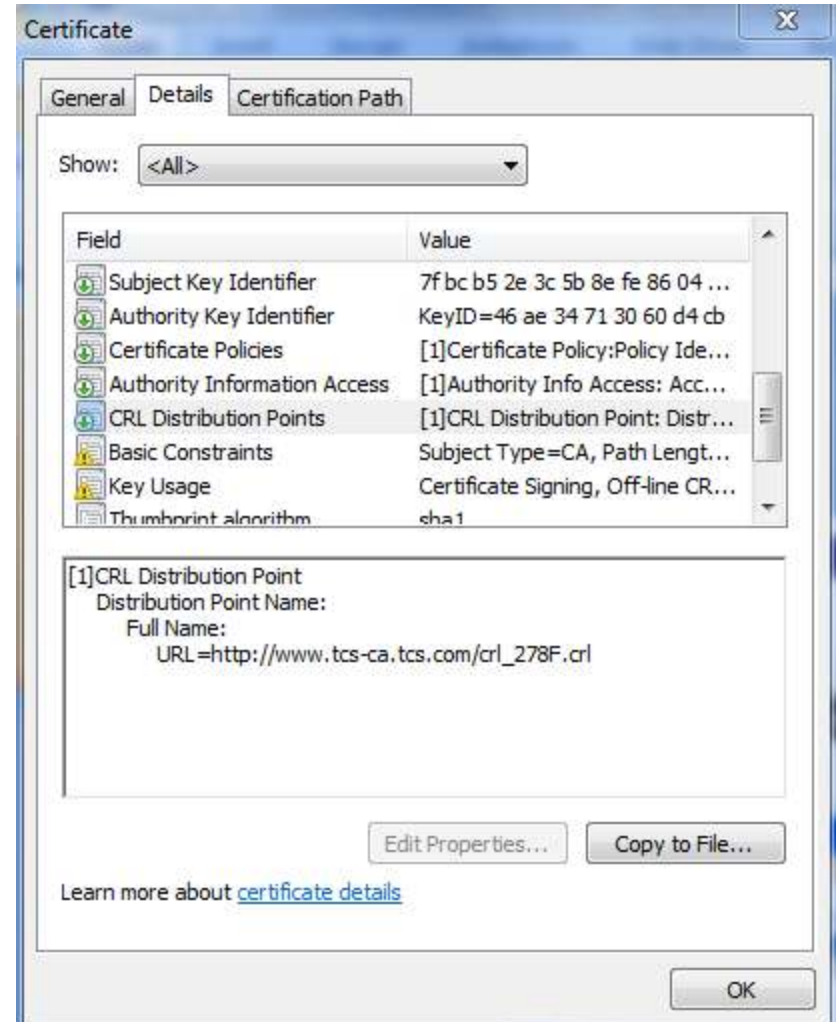
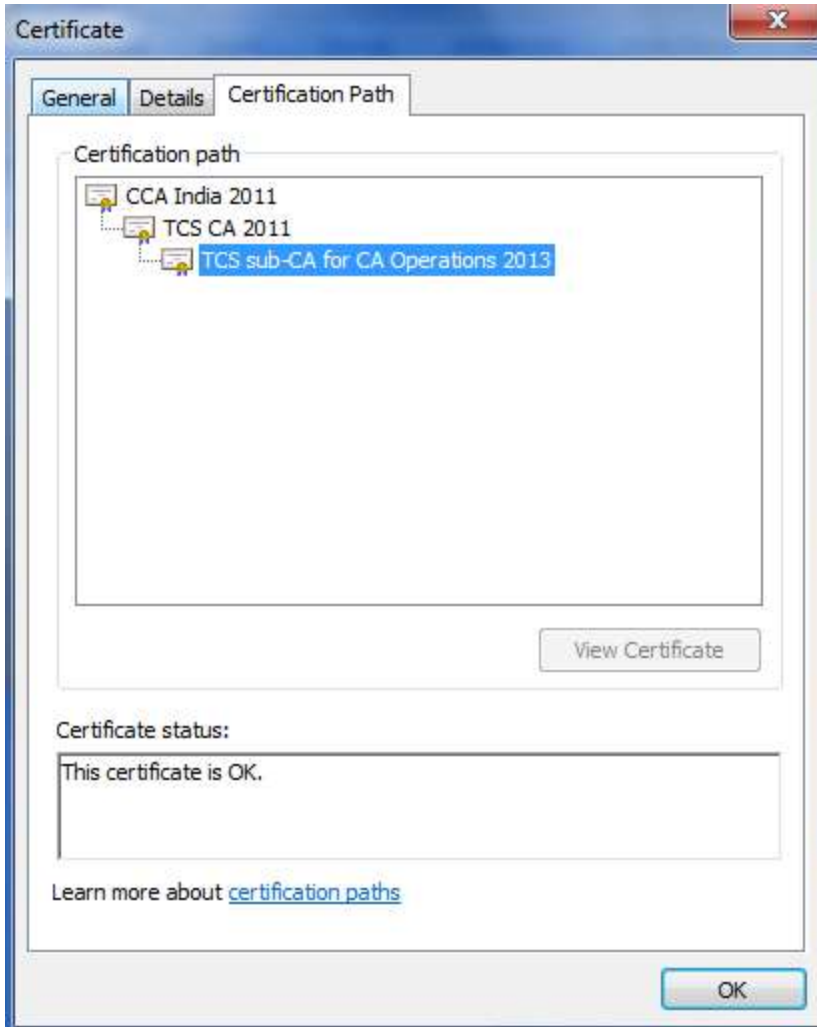
- What is revocation?
- Why do we need it?
- What is currently being done?

Why Revoke?

- Key Compromise
- Forgotten Passphrase
- Lost Private Key

- 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.

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



Certificate Revocation List

General 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](#)

OK

Certificate Revocation List

General 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...

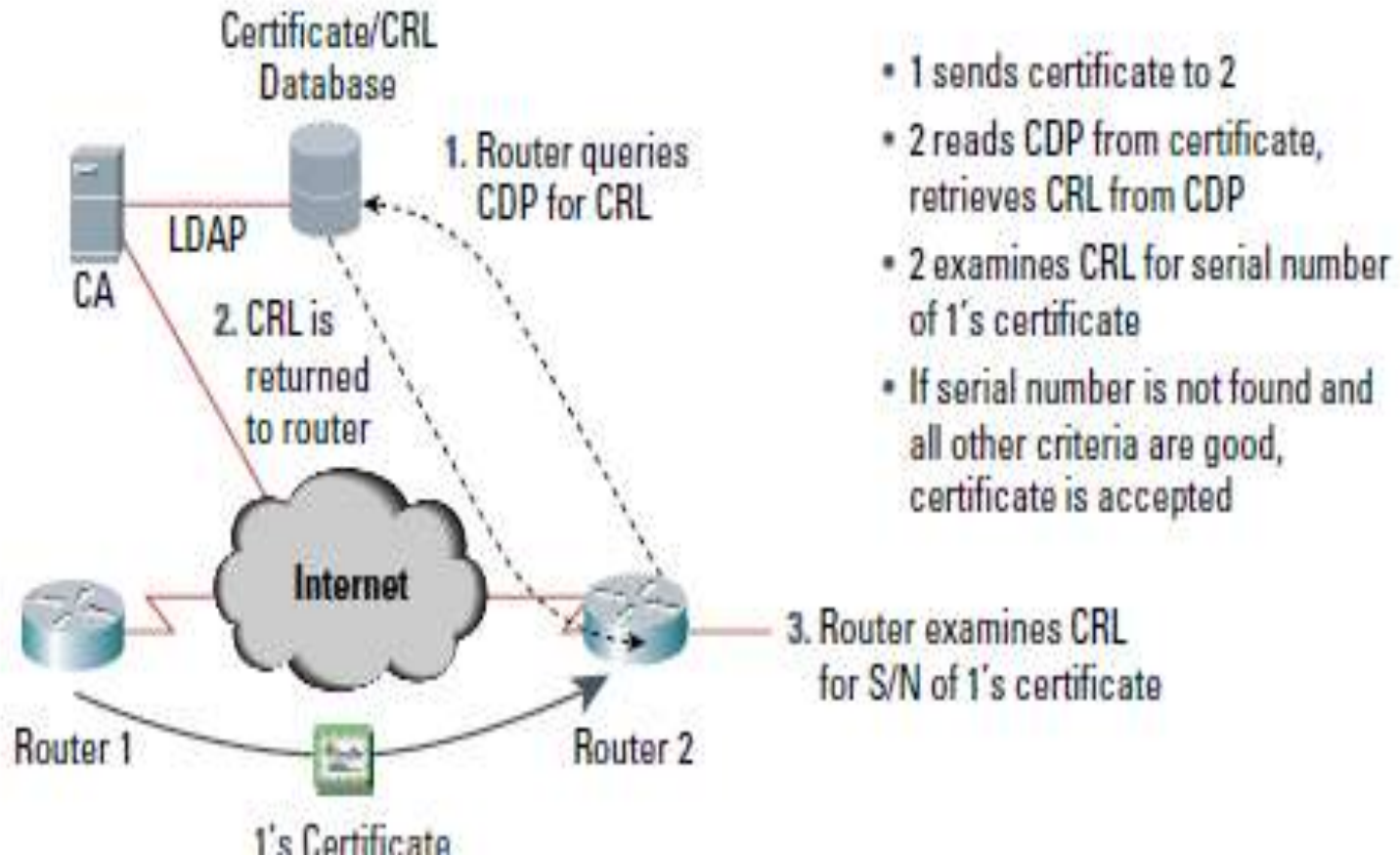
Value:

Learn more about [certificate revocation list](#)

OK

CDP – CRL Distribution Point

Figure 1
Cert Validation with CRL

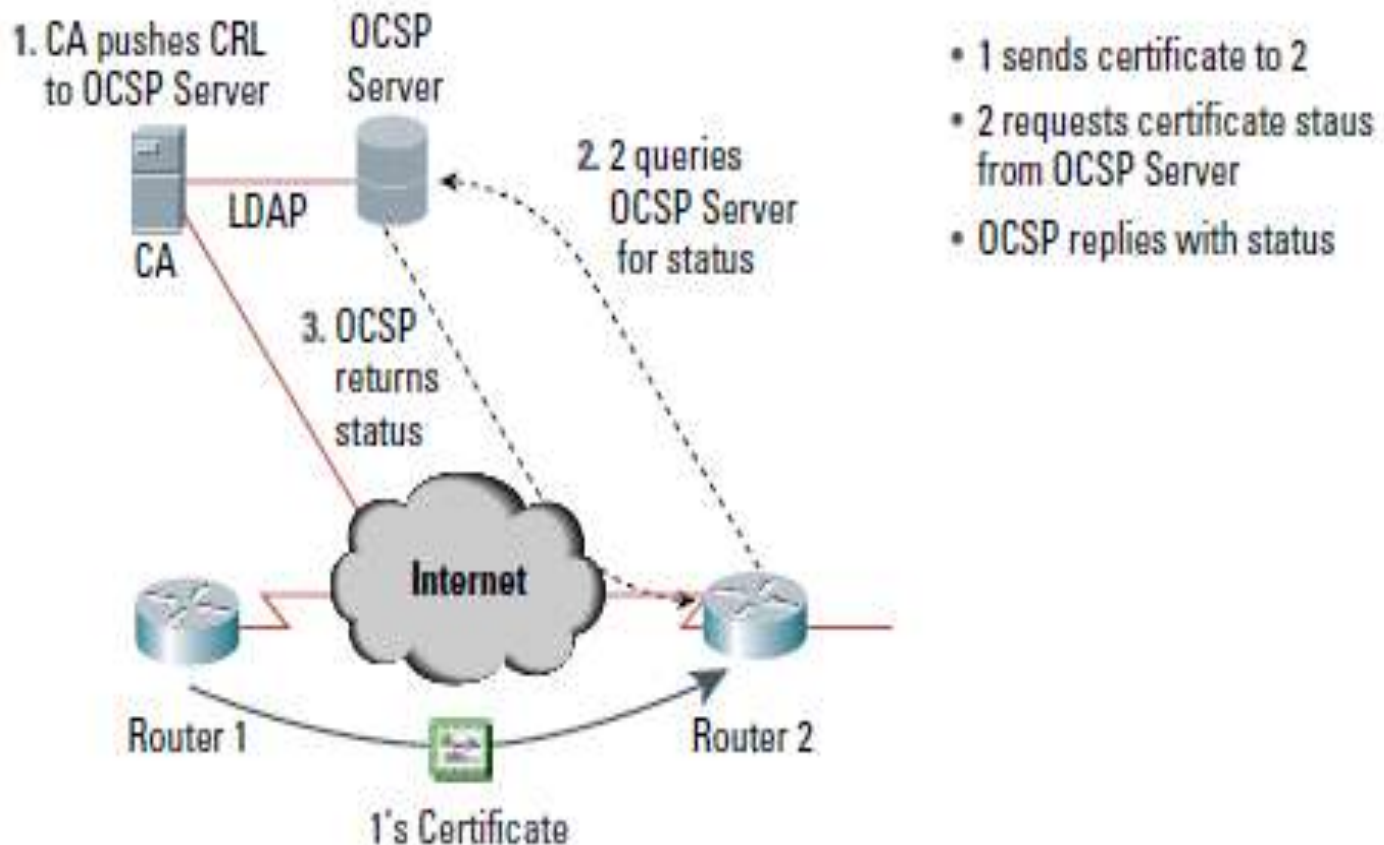


- 1 sends certificate to 2
- 2 reads CDP from certificate, retrieves CRL from CDP
- 2 examines CRL for serial number of 1's certificate
- If serial number is not found and all other criteria are good, certificate is accepted

- 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(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.

Figure 2
Cert Validation with OCSP



- 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.

- 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 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.
-

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.

- www.ietf.org/rfc/rfc2560.txt
- Cryptography and Network Security - Atu Kahate

Thank You