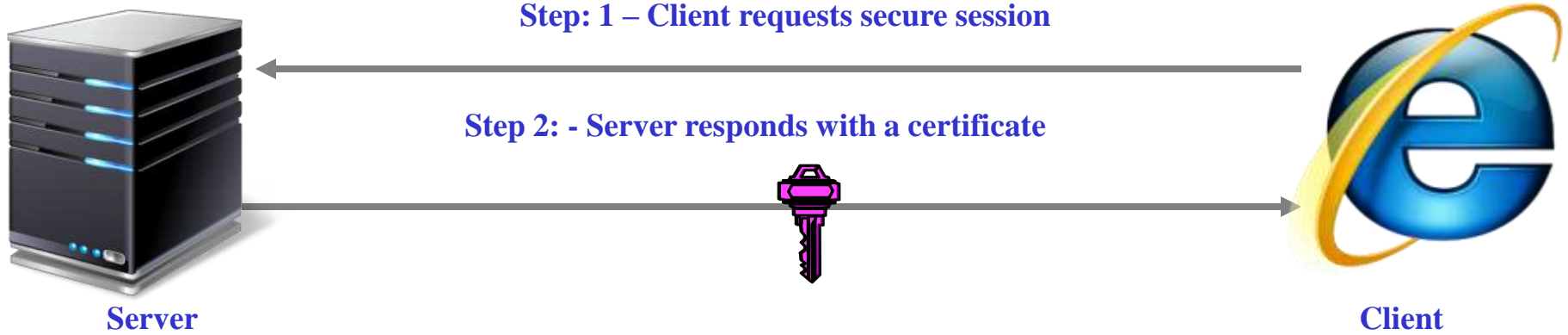


# Understanding HTTPS CRL and OCSP

**Sanjay Adiwai**

**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:
  .....
  
```

```

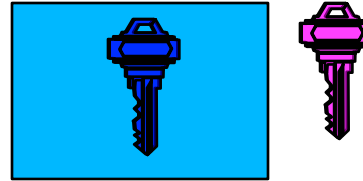
Signature Algorithm: sha1withRSAEncryption
.....
-----BEGIN CERTIFICATE-----
.....
-----END CERTIFICATE-----
  
```

**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

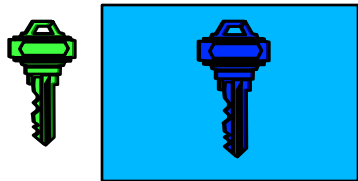


Server



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: My Accounts ▼


**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**



- [www.ietf.org/rfc/rfc2560.txt](http://www.ietf.org/rfc/rfc2560.txt)
- Cryptography and Network Security - Atu Kahate

Thank You