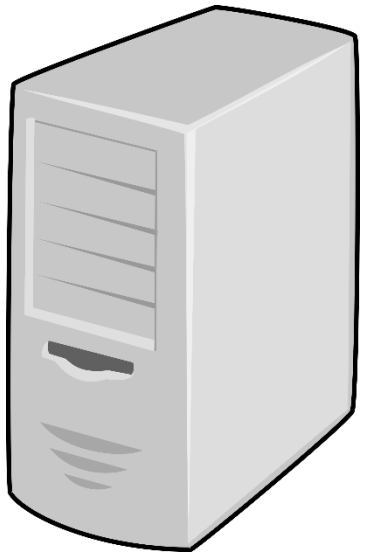
TLS

Anoop Kumar Pandey
Joint Director
Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore 560 100

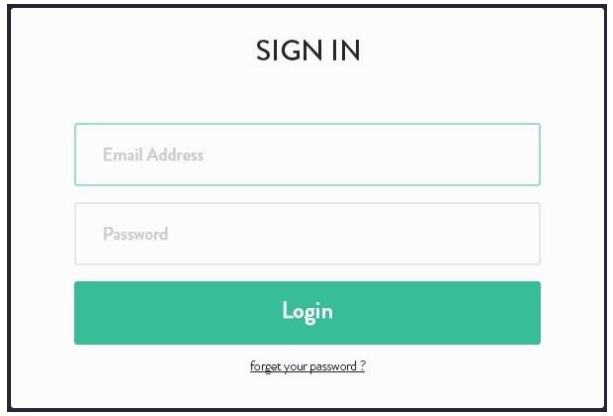
National Cyber Security Awareness Month (NCSAM-2022)
21st October 2022

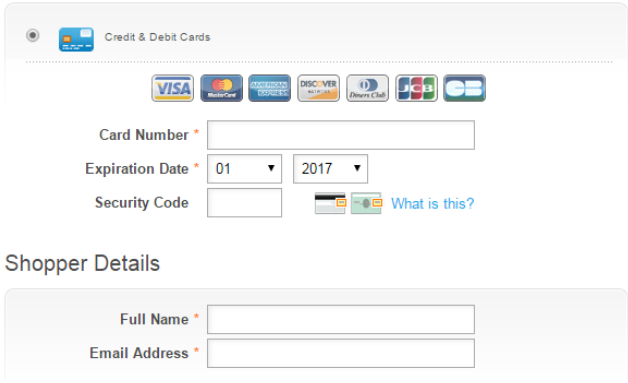


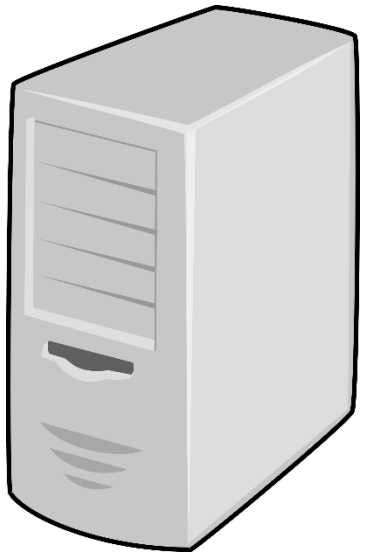
Shopping.com

Email: anoop@cdac.in
Password: ABCD1234

Card No:
34561234567
CVV: 1234 Expiry:
4/23



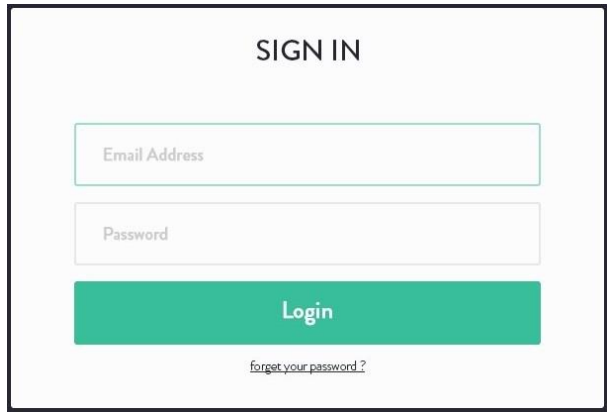


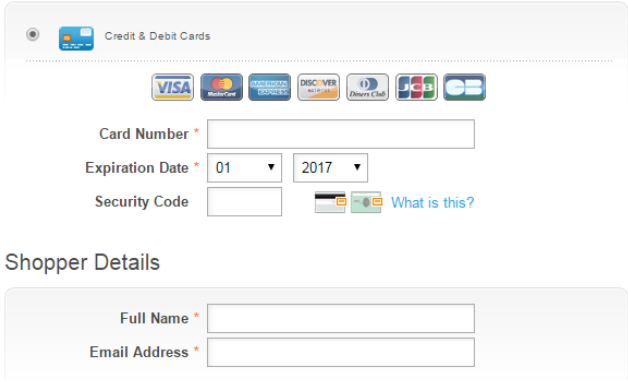


Shopping.com

$%#^DE*&^9845988
@

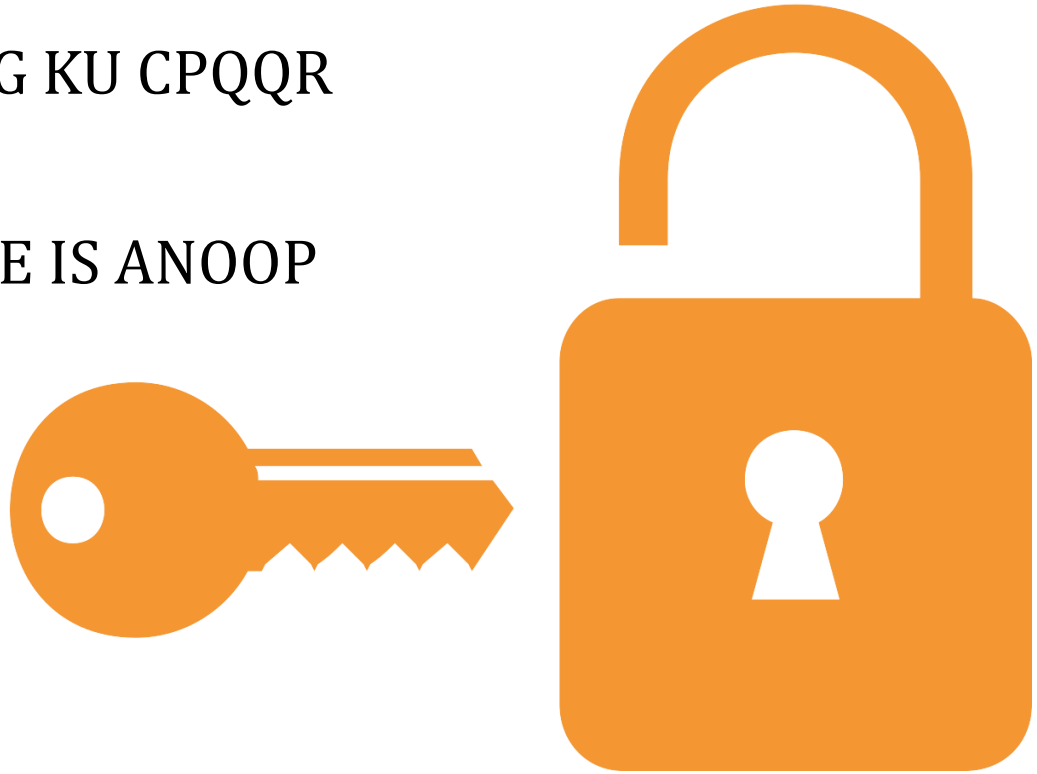
325435#$%$%@JFHS
G





Symmetric Key

- Key: 2
- Encryption
  - MY NAME IS ANOOP ----(+2)--→ OA PCOG KU CPQQR
- Decryption
  - OA PCOG KU CPQQR ----(-2)--→ MY NAME IS ANOOP



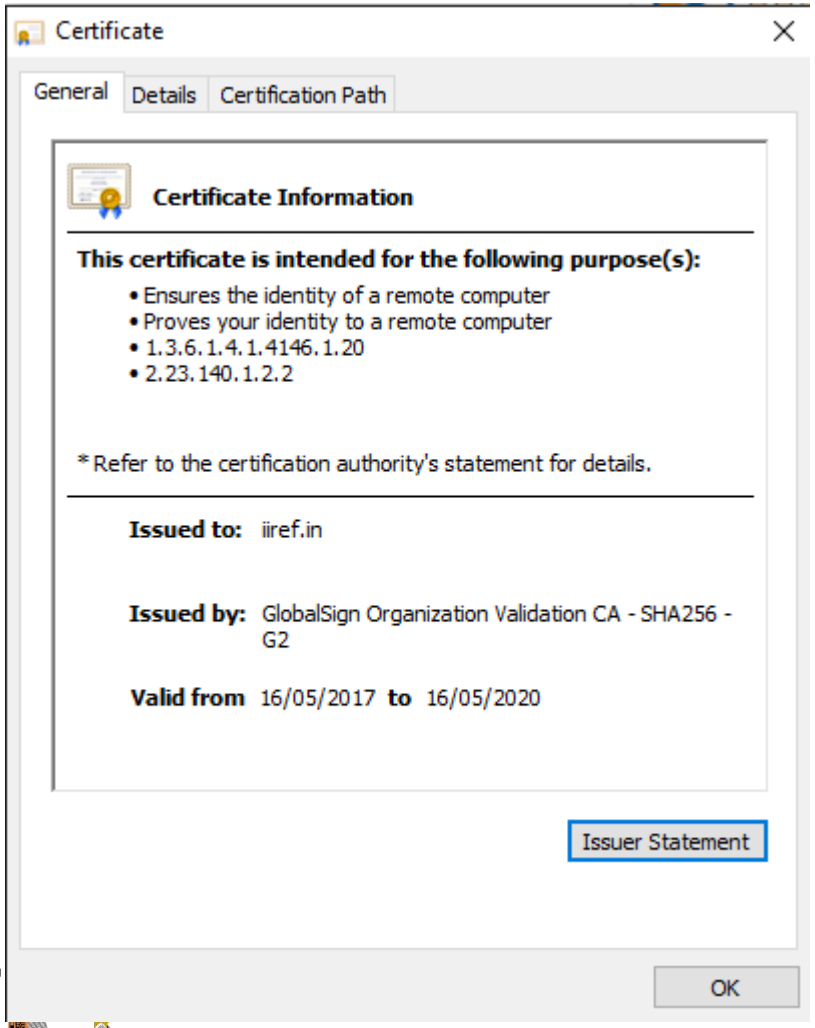
Asymmetric Key

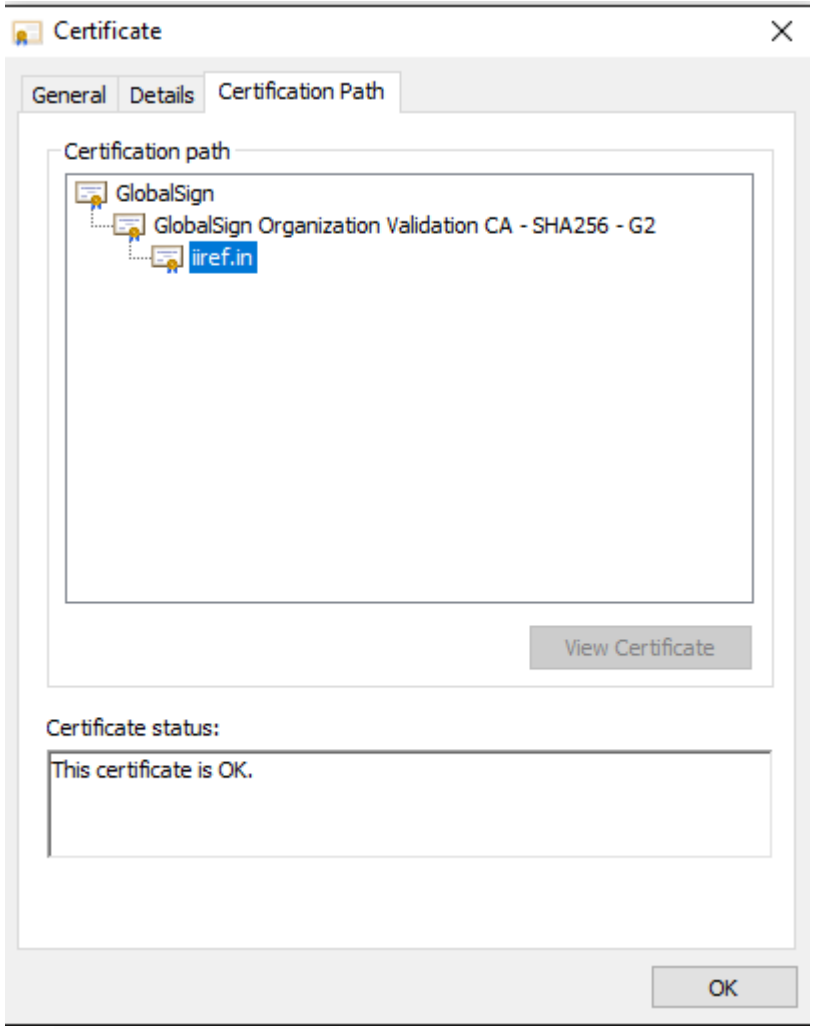
- Keys
  - Public (d, n): (7,33)
  - Private (e, n): (3,33)
- Encryption
  - Letter: c (3)
  - enc = (plaintext^d) mod n = 3^7 mod 33 = 9 (i)
- Decryption
  - Cipher Text: i (9)
  - enc = (ciphertext^e) mod n = 9^3 mod 33 = 3 (c)

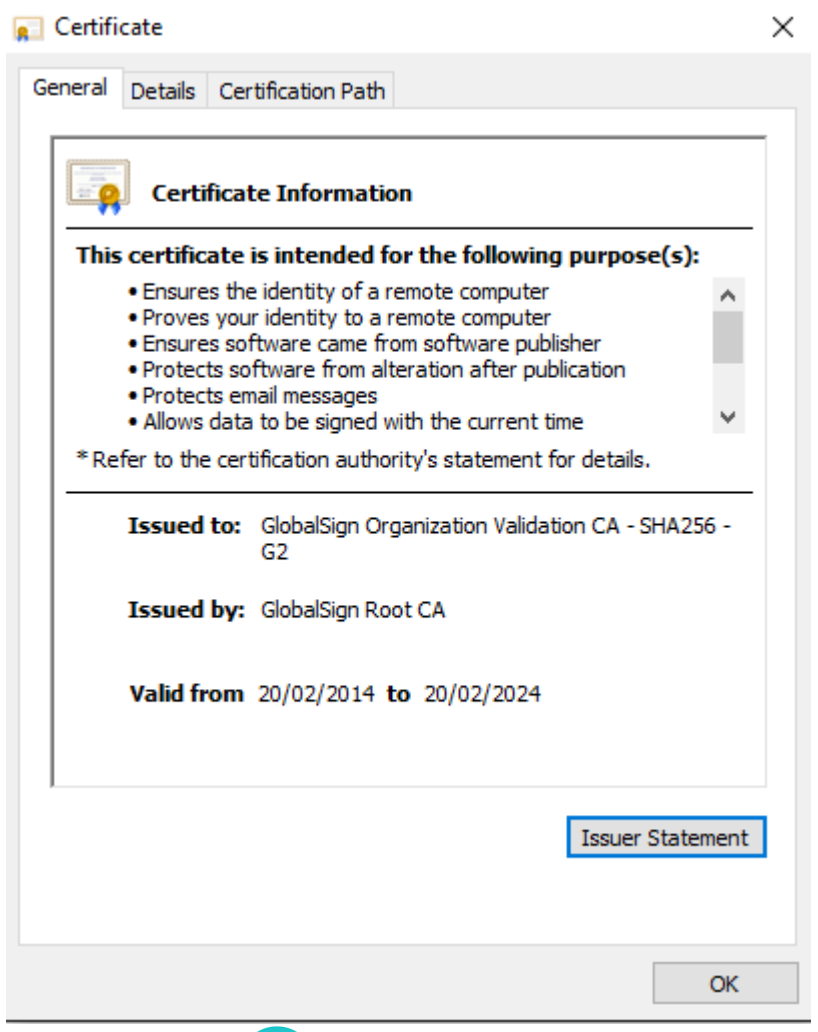
Digital Certificate

- Certifying Authority certifies a Public Key
- Trust propagates from Root Certifying Authority in general.
- A Certificate establishes the ownership of the public key and provides a mechanism for non-repudiation (inability to deny)
- Different Types
  - Digital Signature Certificate
  - Encryption Certificate
  - TLS Certificate

Sample Certificate







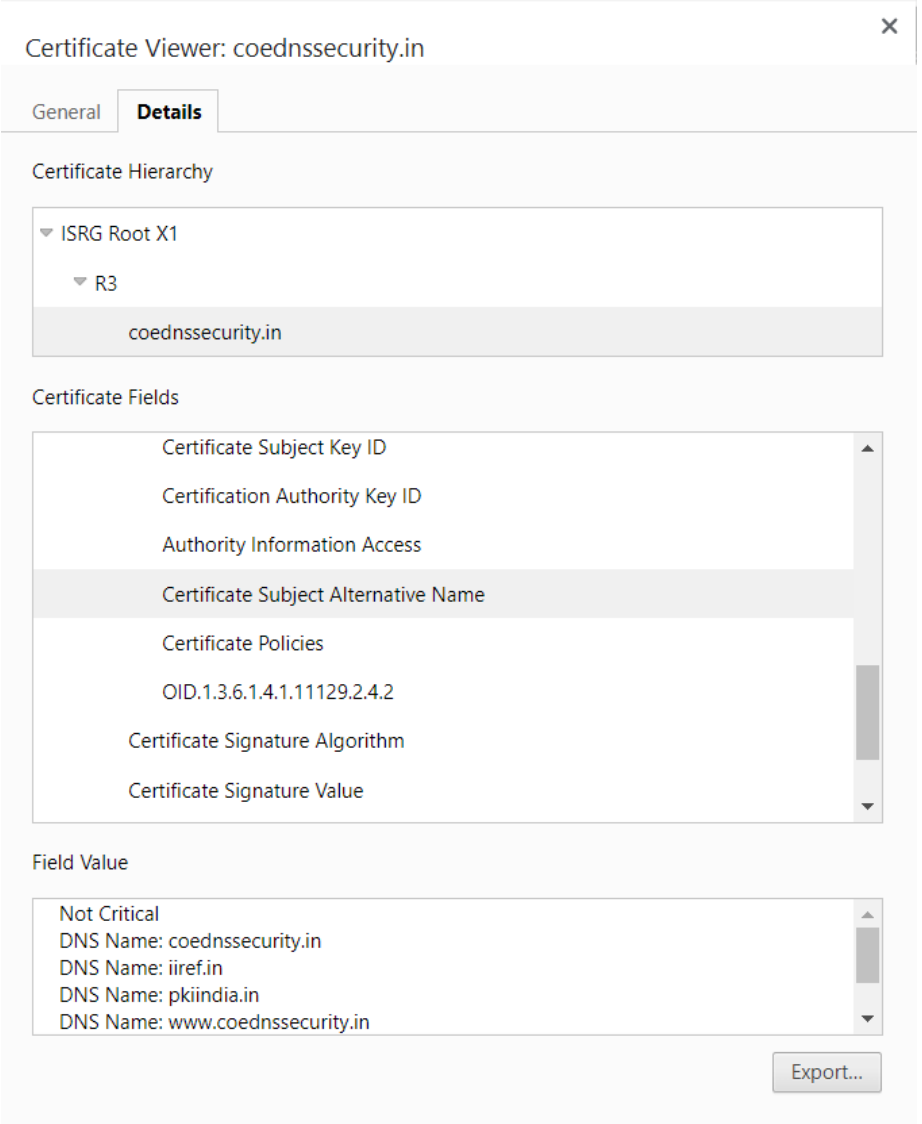
TLS Certification Issuance

- Key pair gets generated on web server
- Web server admin creates CSR (certificate signing request) and send it to CA (Certifying Authority)
- In Subject DN (Distinguished name) of CSR, common name should be same as fully qualified domain name.
- CA validates the domain and sign the certificate

Types of Certificate

- Based on Business requirement
  - Multi-domain Certificate
  - Wild Card Certificate
- Based on Validation
  - Domain Validated (DV) Certificates
  - Organization Validated (OV) Certificates
  - Extended Validation (EV) Certificates

MultiDomain Certificate



Wildcard Certificate

Certificate Viewer: *.whatsapp.net

General | Details

Issued To

Common Name (CN)	*.whatsapp.net
Organization (O)	Facebook, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	DigiCert SHA2 High Assurance Server CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

Validity Period

Issued On	Tuesday, July 26, 2022 at 5:30:00 AM
Expires On	Tuesday, October 25, 2022 at 5:29:59 AM

Fingerprints

SHA-256 Fingerprint	6F A4 D9 E9 1C 3C 52 4B 84 48 C5 87 3C 40 42 9F 71 7C 55 5A 0E 93 EC 68 17 4E 9C 31 4D 79 BC 8E
SHA-1 Fingerprint	22 5F A6 87 64 2F 4E 4F B3 6A 94 CF 32 DD 10 3E FE 02 5E F9

Certificate Viewer: *.whatsapp.net

General | **Details**

Certificate Hierarchy

- DigiCert High Assurance EV Root CA
  - DigiCert SHA2 High Assurance Server CA
    - *.whatsapp.net

Certificate Fields

- Certification Authority Key ID
- Certificate Subject Key ID
- Certificate Subject Alternative Name
- Certificate Key Usage
- Extended Key Usage
- CRL Distribution Points
- Certificate Policies
- Authority Information Access

Field Value

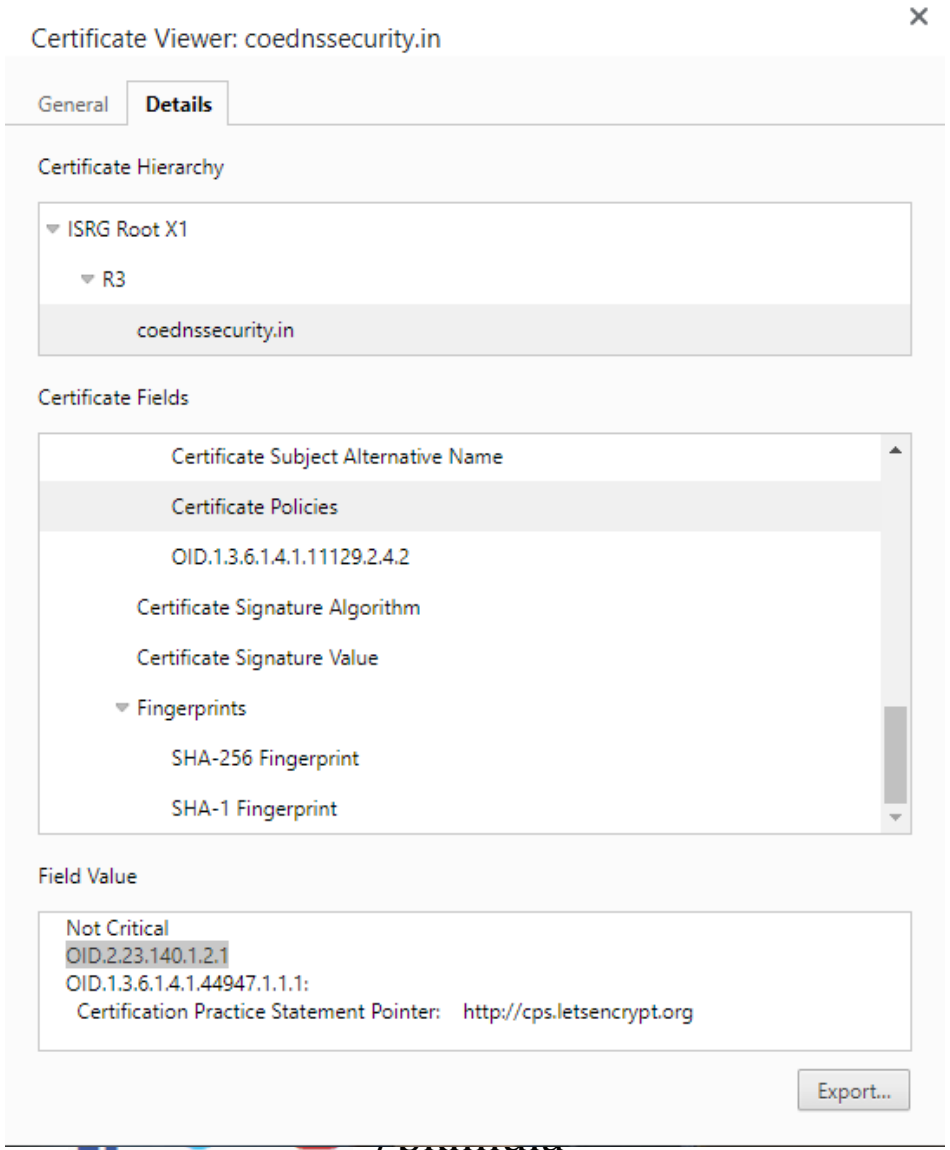
Not Critical
DNS Name: *.whatsapp.net
DNS Name: *.cdn.whatsapp.net
DNS Name: *.snr.whatsapp.net
DNS Name: *.whatsapp.com

Export...

Domain Validated Certificate

Domain Validated certificates are certificates that are checked against domain registry.

Domain Validated Certificate



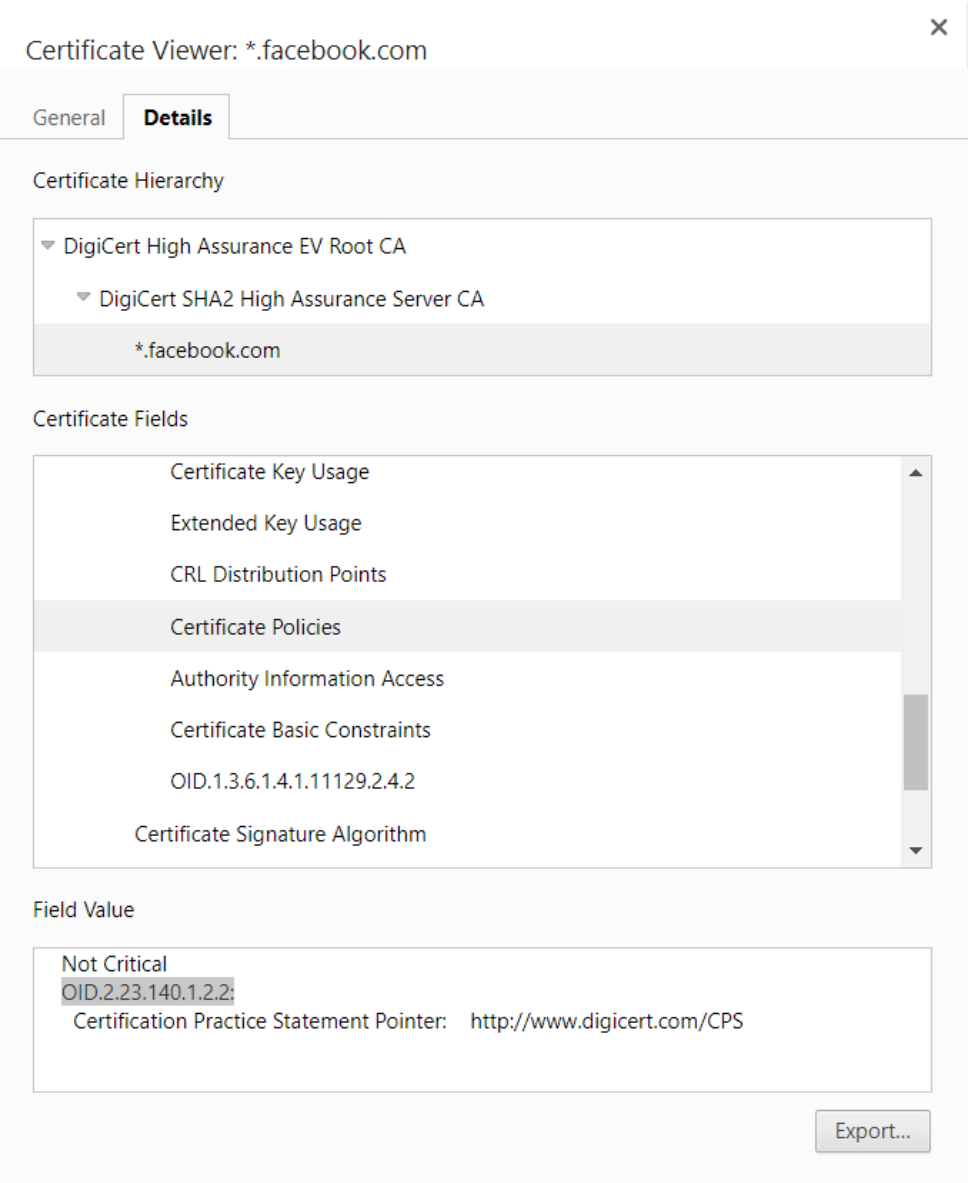
Organization Validated Certificate

For organization validation, the CA will verify the actual business that is attempting to get the certificate.

This is usually used by corporations, governments and others for TLS-enabled websites.

In Old Browsers, it activates the browser padlock and https, shows the corporate identity.

Organization Validated Certificate



www.pkiindia.in

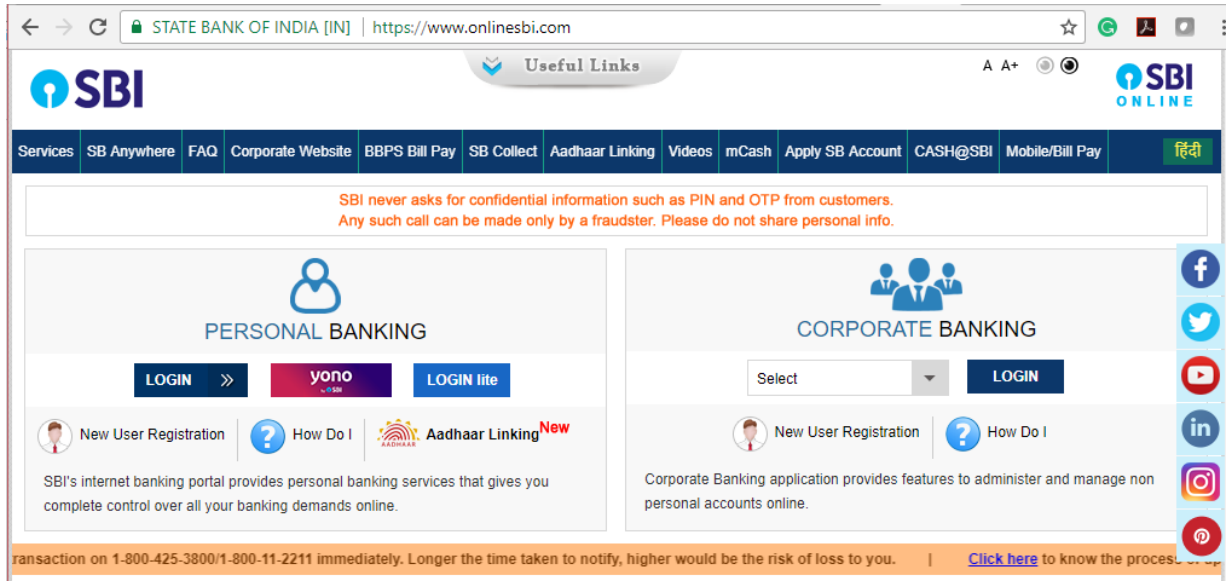
Extended Validated Certificate

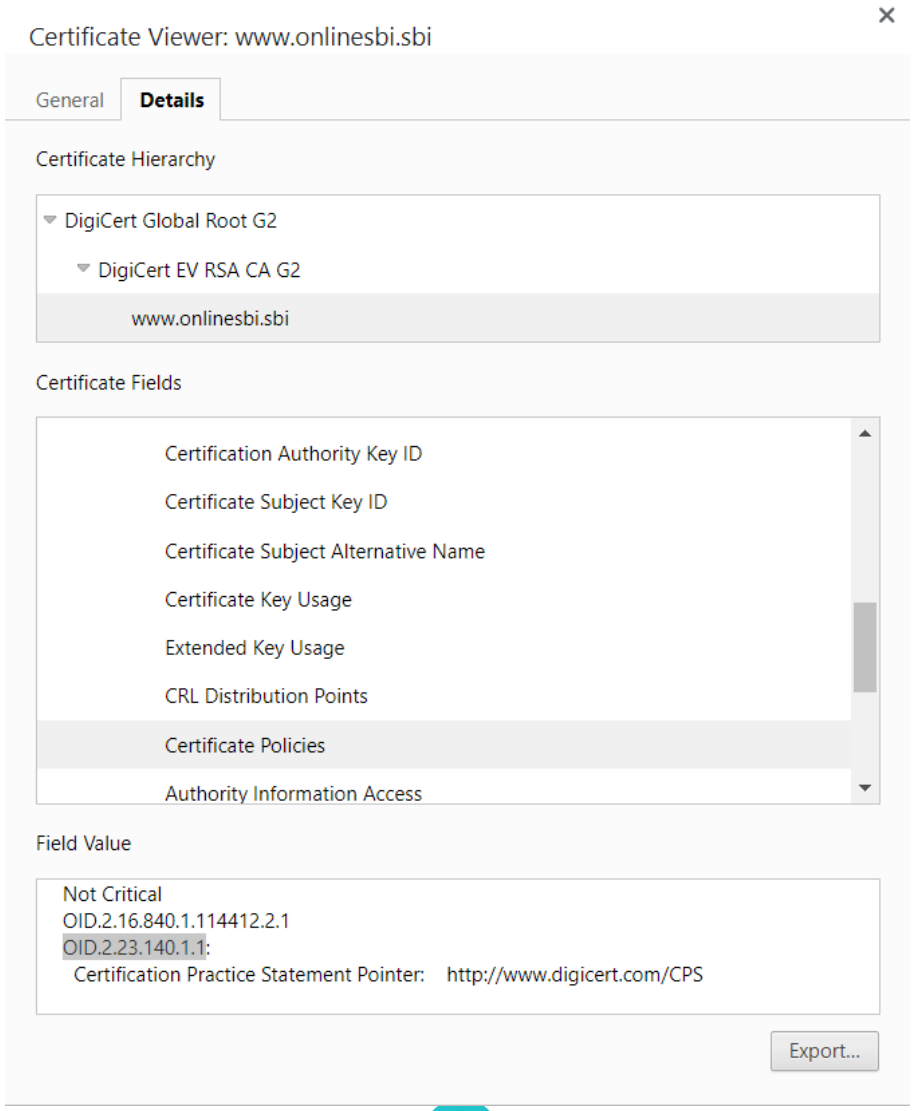
An **Extended Validation Certificate** (EV) is a certificate issued according to a specific set of identity verification criteria.

These criteria require extensive verification of the requesting entity's identity by the CA before a certificate is issued.

In Old Browsers, Extended TLS activates the green address bar and displays the organization name in the browser interface.

Extended Validation Certificate

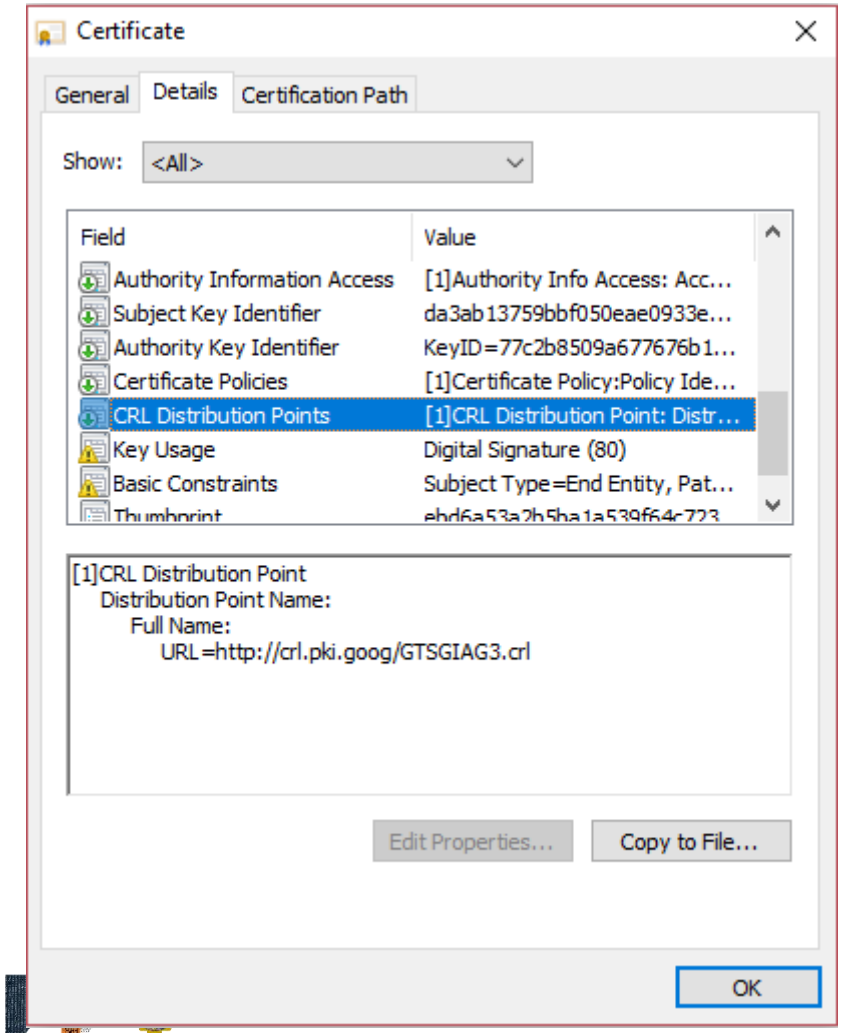


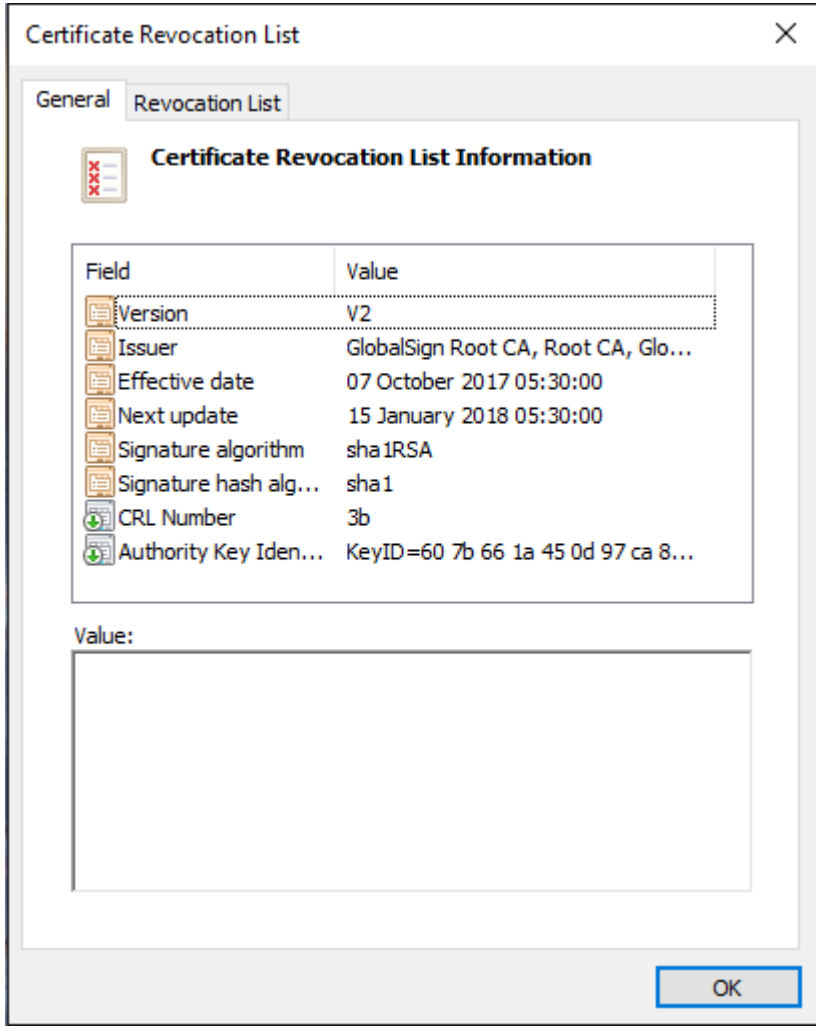


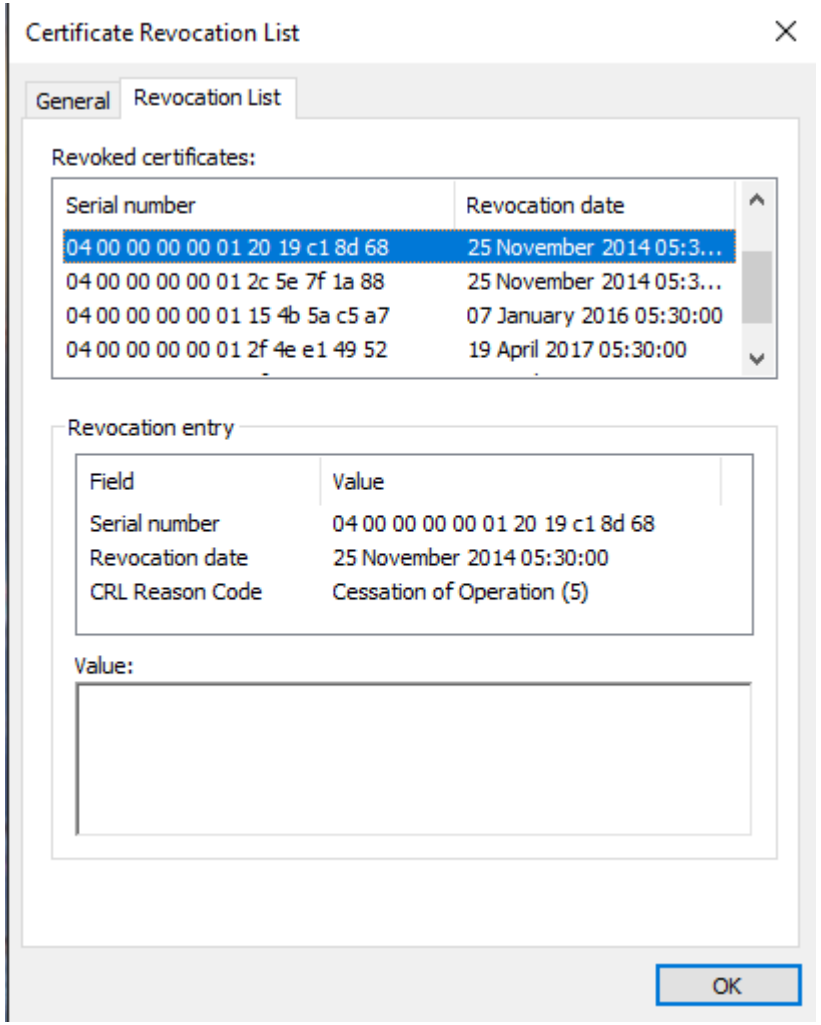
CRL – Certificate Revocation List

- Sometimes private keys might get compromised. The user, then, reports to the CA and CA revokes the certificate. Additionally if CA discovers that false information was used to obtain the certificate, then also they can revoke the certificate.
- CRL or Certificate revocation list is a list containing the serial number of those certificates that have been revoked by a particular CA. It is digitally signed and maintained by the CA. It is updated generally twice a day depending on CA's policies
- OCSP is an automated system in place for accessing the CRL

CRL


Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Authority Information Access
[1]Authority Info Access: Acc...
Subject Key Identifier
da3ab13759bbf050eae0933e...
Authority Key Identifier
KeyID=77c2b8509a677676b1...
Certificate Policies
[1]Certificate Policy:Policy Ide...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Key Usage
Digital Signature (80)
Basic Constraints
Subject Type=End Entity, Pat...
[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://crl.pki.goog/GTSGIAG3.crl
Edit Properties...
Copy to File...
OK


Certificate Revocation List
General
Revocation List
Certificate Revocation List Information
Field
Value
Version
V2
Issuer
GlobalSign Root CA, Root CA, Glo...
Effective date
07 October 2017 05:30:00
Next update
15 January 2018 05:30:00
Signature algorithm
sha1RSA
Signature hash alg...
sha1
CRL Number
3b
Authority Key Iden...
KeyID=60 7b 66 1a 45 0d 97 ca 8...
Value:
OK


Certificate Revocation List
General
Revocation List
Revoked certificates:
Serial number
Revocation date
04 00 00 00 00 01 20 19 c1 8d 68
25 November 2014 05:3...
04 00 00 00 00 01 2c 5e 7f 1a 88
25 November 2014 05:3...
04 00 00 00 00 01 15 4b 5a c5 a7
07 January 2016 05:30:00
04 00 00 00 00 01 2f 4e e1 49 52
19 April 2017 05:30:00
Revocation entry
Field
Value
Serial number
04 00 00 00 00 01 20 19 c1 8d 68
Revocation date
25 November 2014 05:30:00
CRL Reason Code
Cessation of Operation (5)
Value:
OK

OCSP

- Online Certificate Status Protocol
  - A request is **made by the browser** to the CA about the validity of a specific TLS Certificate
    - CA runs a OCSP Responder that checks and tells whether the certificate is valid or revoked
  - Response returned by the CA is digitally signed by it;
  - Status may be "current", "expired," or "unknown."
  - Defined in RFC 2560 and RFC 5019

Signcryption using Outlook-Signed.pdf - Adobe Acrobat Pro

File Edit View Window Help

Create Customize

1 / 5 103% Tools Sign Comment

At least one signature is invalid. Signature Panel

Click on Tools, Sign, and Comment to access additional features.

PANDEY
ANOOP
KUMAR

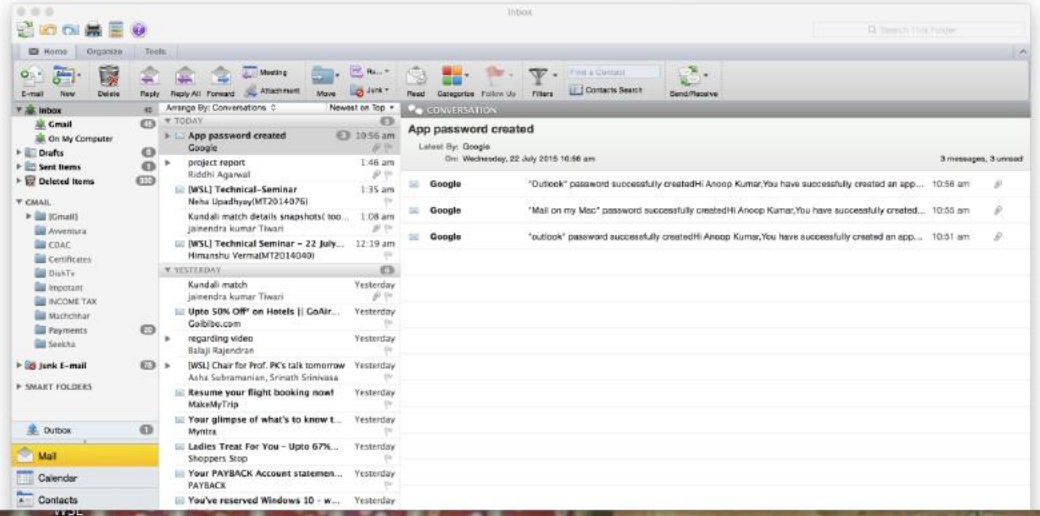
Digitally Signing and Encrypting an Email

- **Tools**
  - **Operating Environment:** Mac OS X 10.10.4 (Yosemite)
  - **Certificate Class:** Class 3 Digital Signature Certificate
  - **Certifying Authority:** E-Mudhra Limited
  - **Token Vendor:** Aladdin E-Token Pro 72K (Java) UR
  - **Token Driver:** http://emudhra.mu/repository/downloads/SAC8.2
  - **Token Application:** eToken PKI Client 5.1 SP1 (5.1.
  - **Email Application:** Microsoft Outlook for Mac 2011
  - **Email Application Screenshots**

Progress

Contacting http://ocsp.e-mudhra.com/ for OCSP based revocation checking, press ESC to cancel

Cancel



Search the web and Windows

13:44
16-12-2015

Signcryption using Outlook-Signed.pdf - Adobe Acrobat Pro

File Edit View Window Help

Create Customize

1 / 5 103% Tools Sign Comment

Signed and all signatures are valid. Signature Panel

Click on Tools, Sign, and Comment to access additional features.

PANDEY ANOOP KUMAR

Digitally signed by PANDEY ANOOP KUMAR

DN: c=IN, o=Personal, cn=PANDEY ANOOP KUMAR, serialNumber=b446d3d570885008b0acfbea3c48256389463d2ccb394c5416d44cb1247a600cb, postalCode=142074, st=KARNATAKA

Date: 2015.07.22 13:43:28 +05'30'

Digitally Signing and Encrypting an Email

- **Tools**

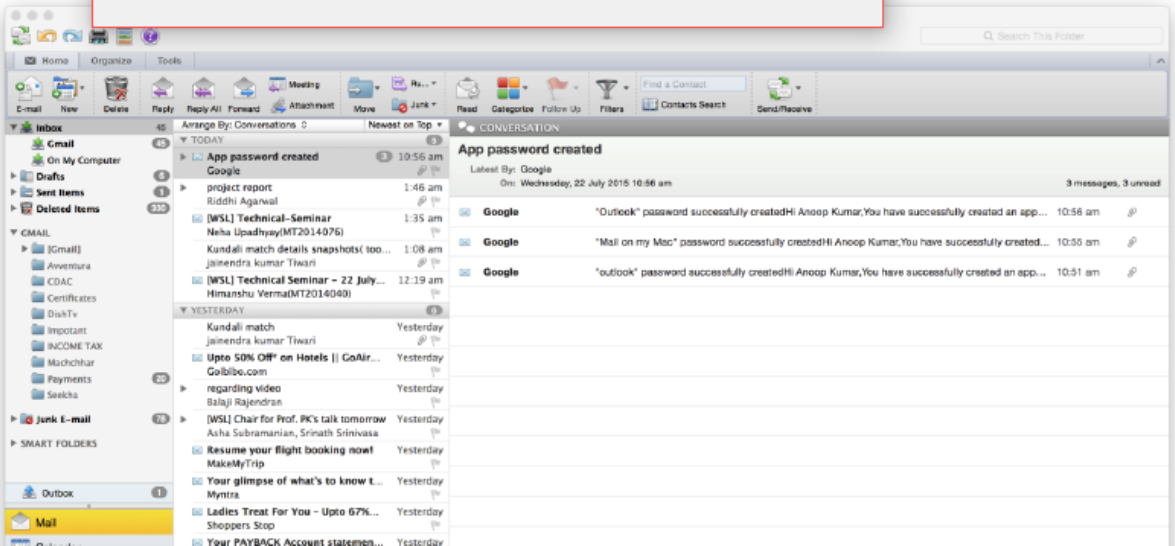
/aladdin.com

lac.zip

Signature Validation Status

Signature is VALID, signed by PANDEY ANOOP KUMAR <ANOOPMIS@GMAIL.COM>.
- The Document has not been modified since this signature was applied.
- The document is signed by the current user.

Signature Properties... Close



www.pkiindia.in

Certificate Validation

- Validating Chain of Trust - A recursive program!
  - As you go several levels deeper, complexity increases and potential of risk increases!
- It is implemented by PKI enabled Application (Eg: Browsers)
- The validation process performs following checks
  - Format of the certificate
  - Verifies the digital signature of the issuer (CA) and chain of trust (Public Key verification) till root level
  - Time (Validity of the certificate)
  - Revocation (CRL verification)

Certificate Validation Failures – Typical Cases

- Domain Mismatch
- Certificate Expired
- Could not find path to certificate

Ref: badssl.com