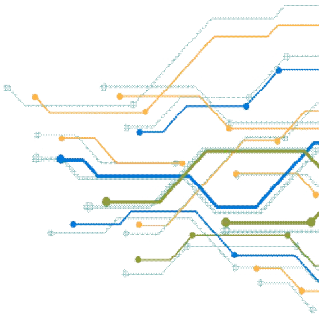
Cryptography
Digital Signature
Public Key Infrastructure (PKI)



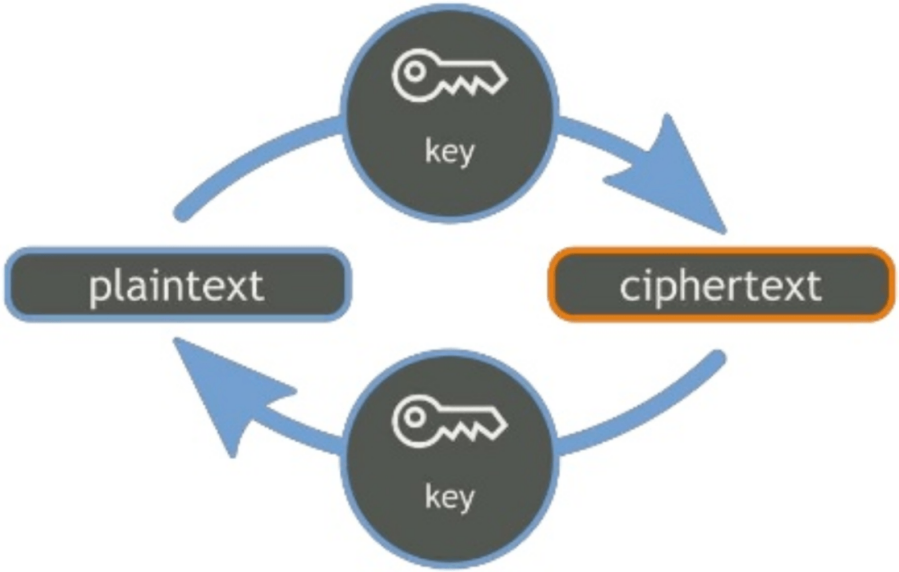
Outline

- Basics of Cryptography
- Digital Signatures – Introduction
- Digital Signature Certificate – Type of Certificates
- Public Key Infrastructure (PKI)
- Traditional modes of Digital Signature and eSign
- PKI Applications in India

Cryptography

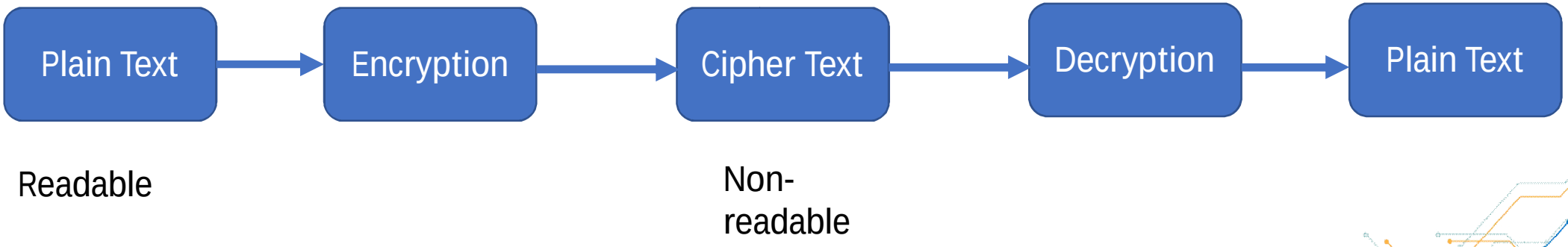
Cryptography

- Refers to method of achieving secure information and communication technique based on **mathematical model**
- Provides a mechanism to keep the information private
- Achieves privacy by converting plain text into an incomprehensible form known as **ciphertext**
- Conversion of data/text requires unique set of numbers known as **keys**



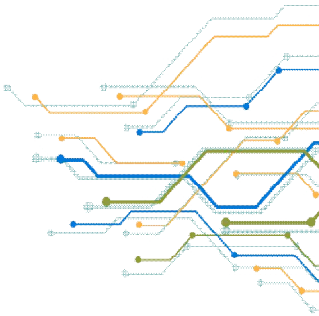
Cryptography

- Conversion of plain text to cipher text is known as **Encryption**
- Conversion of cipher text to plain text is known as **Decryption**
- Keys used for Encryption/Decryption can be **Symmetric or Asymmetric**



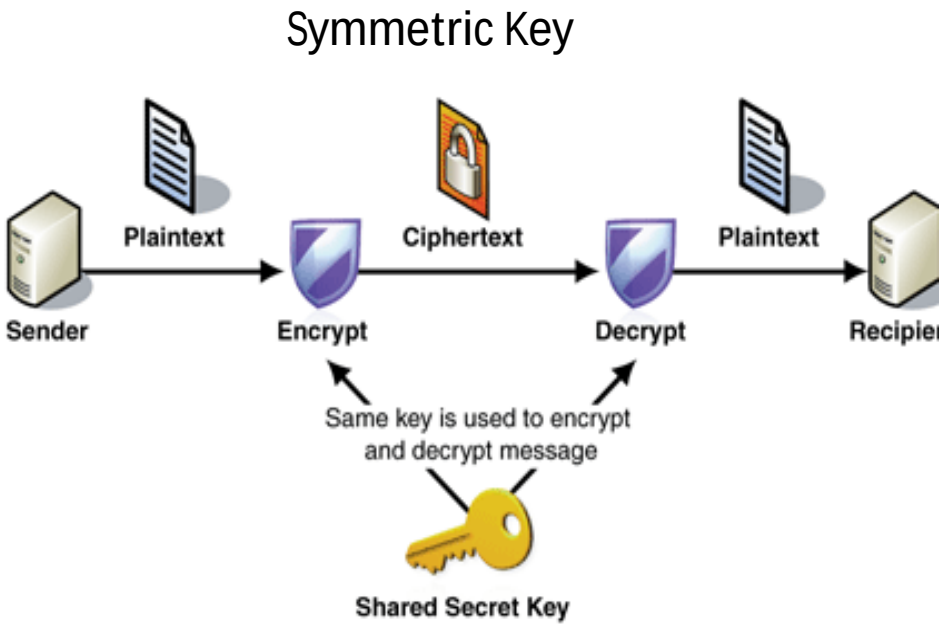
Objectives fulfilled by Cryptography

- Confidentiality – Data is transmitted/stored in a manner that can be understood by **intended party only**
- Integrity – **Any change** in data can be understood
- Non-repudiation – Creator of the data **cannot deny later** of not performing the transaction
- Authentication – Sender/Receiver of data **can recognize each other** in a unique manner



Symmetric Key

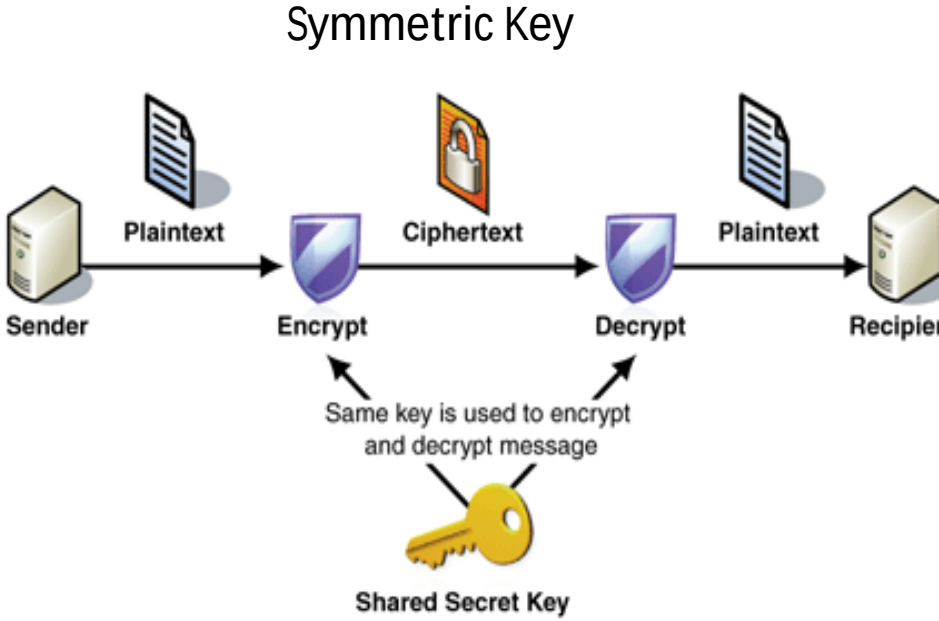
- Same key is used for encryption and decryption
- Some common techniques –
  - Data Encryption Standard (DES) – Block cipher based, 56 to 128 bit key
  - TripleDES – Applies DES algorithm three times to each block, 56 to 168 bit key
  - Advanced Encryption Standard (AES) – 128 bit block cipher, 128 to 256 bit key
  - Blowfish



Achieves **Confidentiality** of data

Symmetric Key

- Advantage: Faster
- Challenge
  - Key Distribution
  - Key Management – Avoid overuse
- Symmetric key algorithms are generally used for bulk encryption such as files, database
- Use Case: Authentication Factor is encrypted using AES 256 Key for Aadhaar Authentication



Achieves **Confidentiality** of data

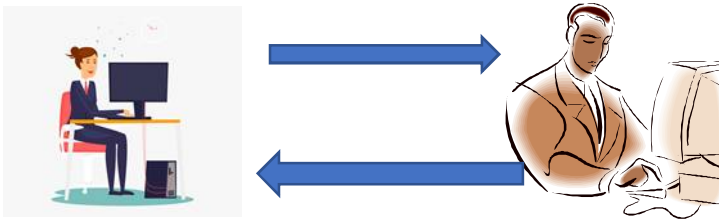
Diffie – Hellman Key Exchange Algorithm

Whitefield Diffie and Martin Hellman in 976

Key distribution algorithm – only for key xchange and not for encryption/decryption

specially for ***Symmetric Key***

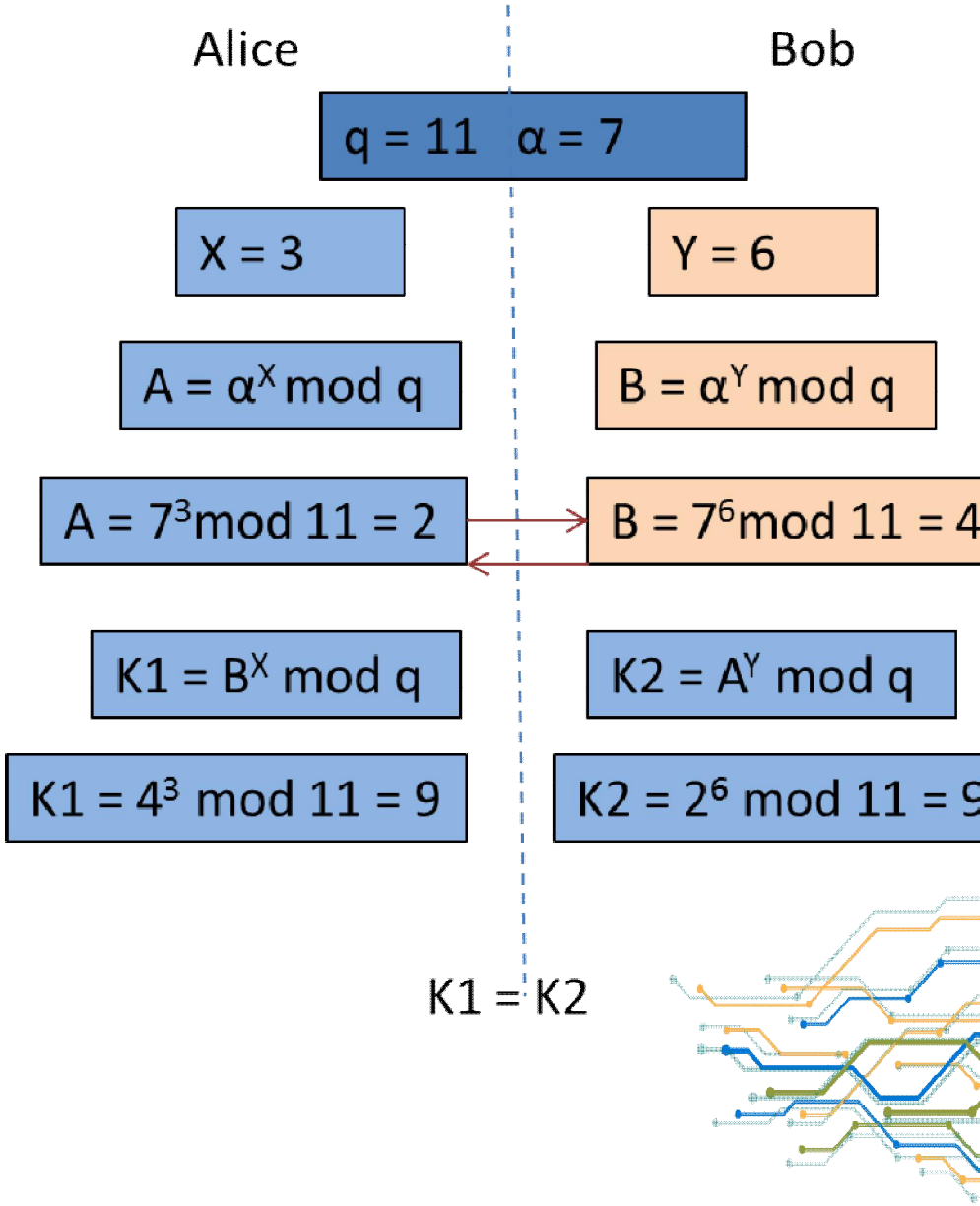
rime numbers are chosen as calculations ecomes complex



A B

Diffie-Hellman Algorithm

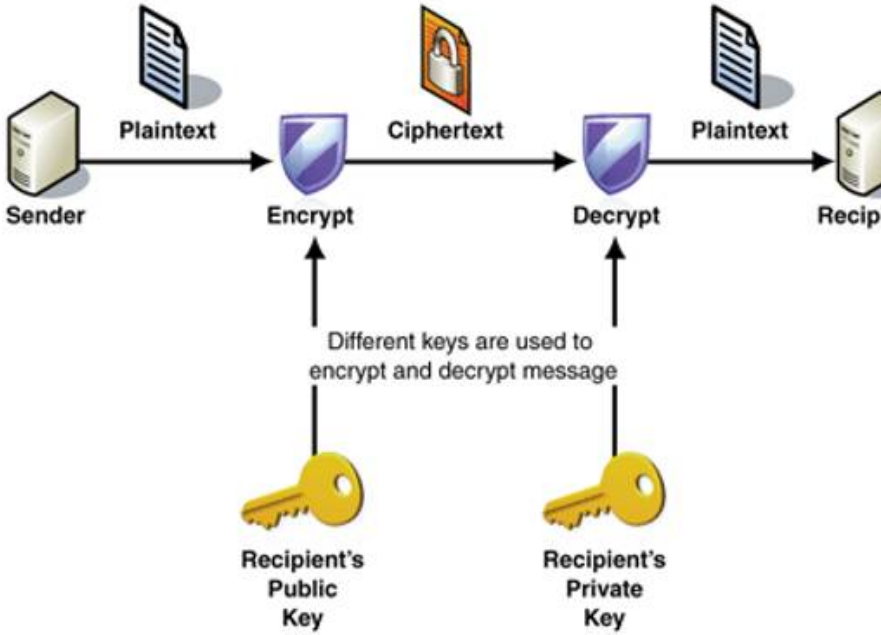
- A large prime number is identified as q and its prime root modulo α.
- Alice selects a random number X only known to her and Bob Selects Random number Y known only to him.
- They calculate (α^{number} mod q) and send it to one another.
- The Key is calculated using (ReceivedNumber) ^{chosenRandomNumber} mod q



Asymmetric Key

- Based on key pair based encryption/decryption
- Known as Public-Private key pair
- Keys are mathematically related
- Some algorithms – RSA (1024 bit, 2048 bit…), ECC (256 bit, 384 bit, 521 bit ….)
- Private key is used in Digital Signature
- Public key is used for Decryption

Asymmetric Key (Public Key)



Provides

- **Confidentiality** of data
- **Authenticity**
- **Non-repudiation**

Asymmetric Key Pair

Private Key

```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83 463d e493 bab6 06d3
0d59 bd3e c1ce 4367 018a 21a8 efbcccd0 a2cc b055 9653 8466 0500 da44 4980 d854 0aa5 2586
94ed 6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc185e 47bc 3ab1 463d 1ef0 b92c 345f 8c7c
4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd
e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b2f0 1cd5 5ffb 6bed 6856 7b39
2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ced 9cbb f2cb
5b10 f82e 6135 c629 4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb
ff78 41bc bd71 28f4 bb90 bcff9634 04e3 459e a146 2840 8102 0301 0001
```

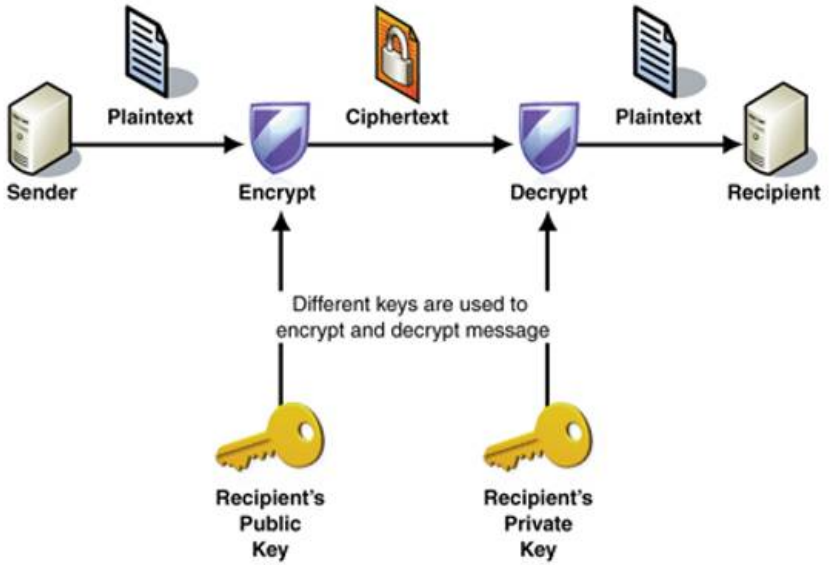
Public Key

```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2 0d83 463d e493 bab6 0673 0d59
bf3e c1ce 4367 012a 11a8 efbc ccd0 a2cc b055 9653 8466 0500 da44 4980 d8b4 0aa5 2586 94ed
6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc185e 47bc 3ab1 463d 1df0 b92c 345f 8c7c 4c08 299d
4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd e6b7 a991 942c
e478 4824 1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb 6bed 6856 7b39 2c72 38b0 ee93 a9d3
7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629 4c2a
d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90 bcff9634
04de 45de af46 2240 8410 02f1 0001
```

Asymmetric Key - Properties

- Strength lies in computational infeasibility in deducing Private key from Public key
- Security lies in protecting Private key
- Uses include Public key encryption and *Digital Signatures*
- Computational complexity limits usage for short messages
- Also used in hand shaking for secure exchange of symmetric keys in SSL/TLS
- Example: Use of RSA 2048 Key for signing Digital Certificate

Asymmetric Key (Public Key)



Provides

- **Confidentiality** of data
- **Authenticity**
- **Non-repudiation**

Hashing Algorithm

Creates a unique thumbprint of a message

Output is a fixed size string e.g. SHA 256 algorithm outputs 256 bit string

Any change in input, changes the output in a non-deterministic manner

One way Process

Provides **integrity** to data

Hi Jai,

I will be in the park at

3 pm

Veeru

35EA1EC376E61DB2680D0312FC26D3773F384E43

Hi Jai,

I will be in the park at

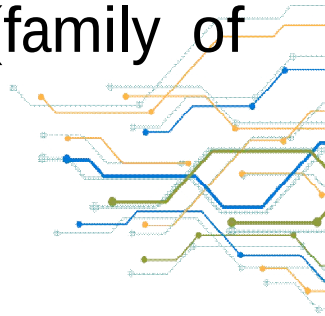
3 pm.

Veeru

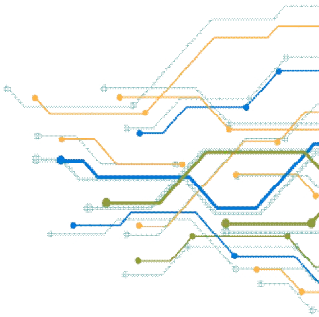
86D19C25294FB0D3E4CF8A026823439064598009

Hashing Algorithm

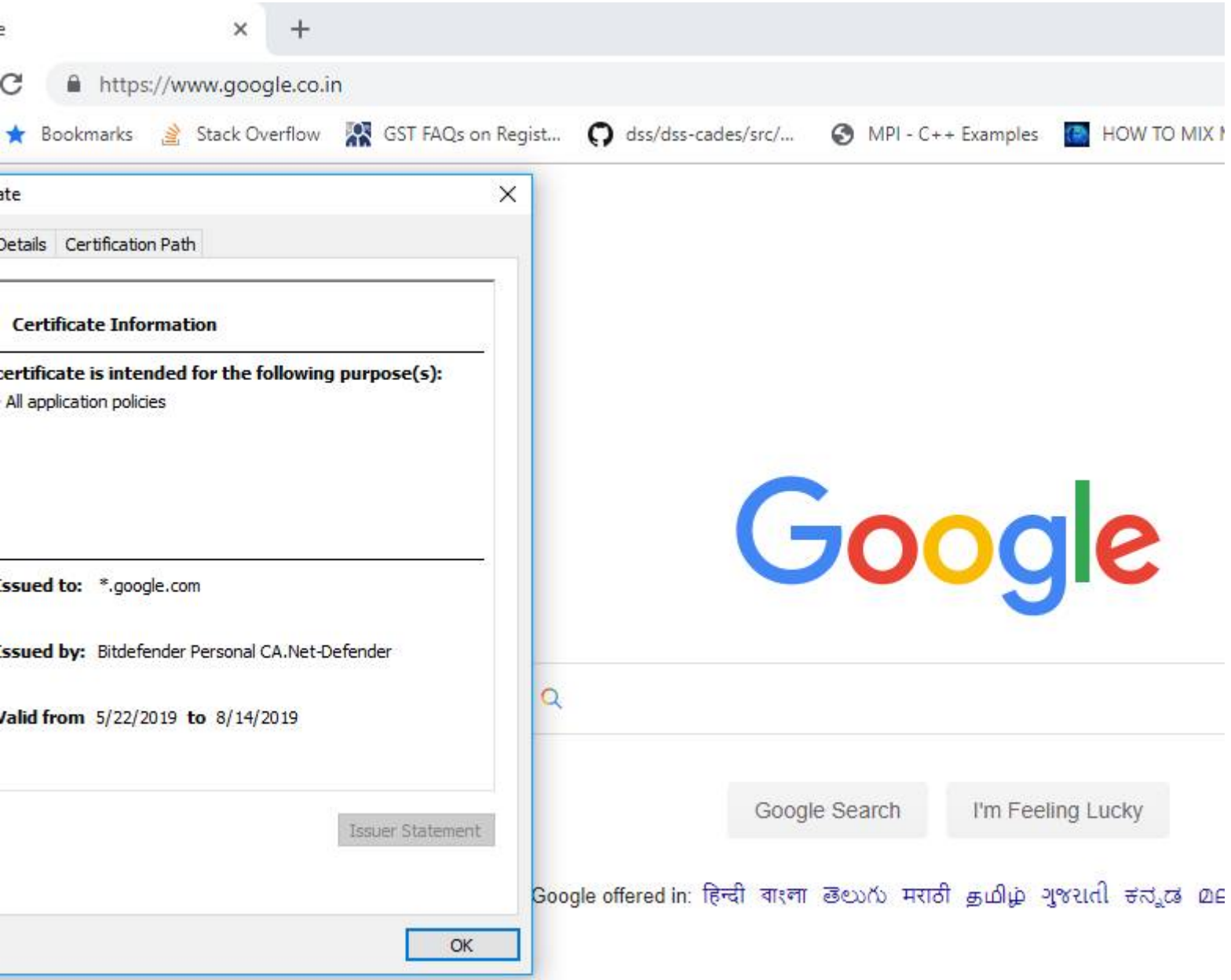
- Use cases : password, hash tables, finding duplicate records, data verification, Blockchain etc.
- Uses in cryptography - Digital Signatures
- Properties
  - Pre-image resistance :
    - Infeasible to generate a message from its hash
    - Given a hash, difficult to find another message with same hash
  - Collision resistance : No two different messages with same hash
- Common Algorithms:
  - MD5 (128 bit o/p, now broken), SHA-1 (160 bit o/p), SHA-2 (family of functions), SHA-256 (belong to SHA-2 family, 256 bit o/p)



https://blockchaindemo.io

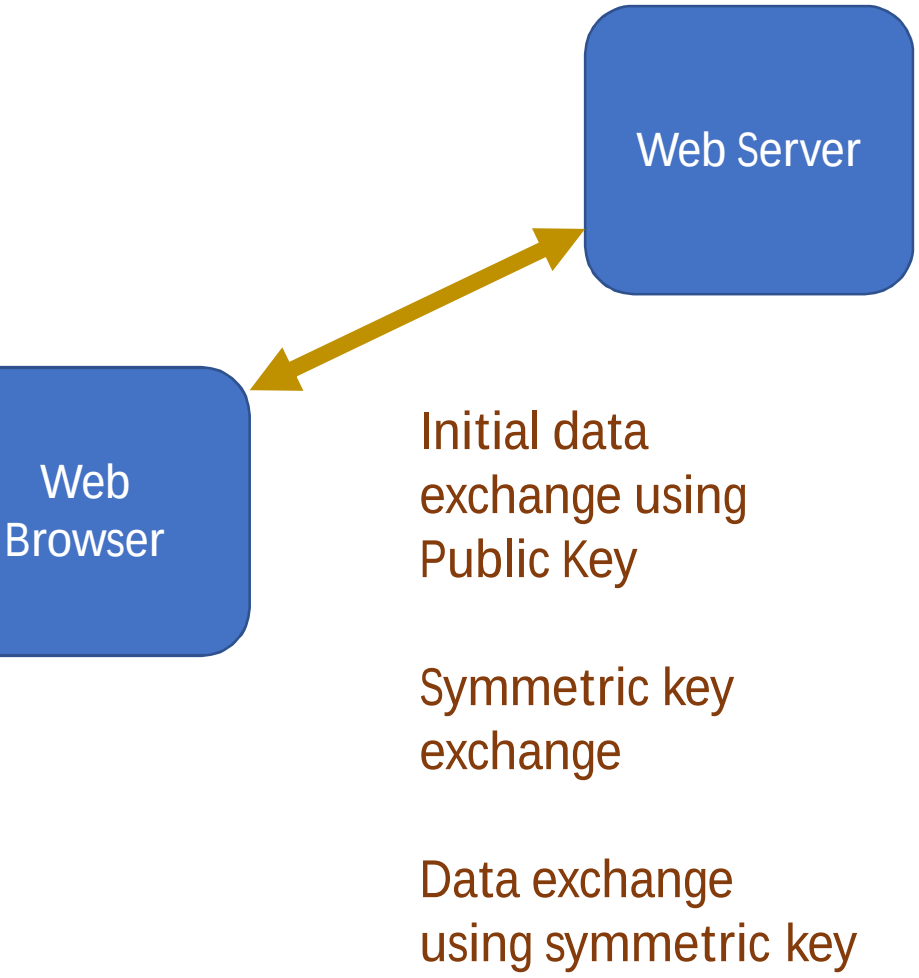


Example: HTTPS Usage (Based on Symmetric and Asymmetric Key)



- Provides data integrity privacy and authenticatio between communicatio applications
- HTTPS sends data fror browser to web server i encrypted format
- SSL certificate plays a important role in establishin trust between browser an server

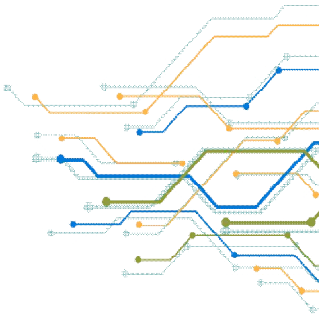
Example: HTTPS Usage



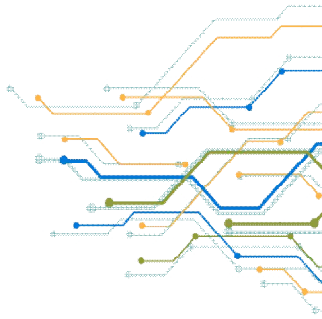
- On clicking https://www.google.in, web browser requests data from web server
- Web server responds with SSL certificate details containing Public Key (K1)
- Web browser verifies Digital Signature of SSL certificate
- Web Browser and Web Server work confidentially to create a shared symmetric key – using K1
- Web Browser and Web Server then use the shared symmetric key to exchange communications securely
- Data exchange starts

Demonstration

- Hash Calculation
  - https://www.tools4noobs.com/online_tools/hash/
- Symmetric Key Generation
  - https://asecuritysite.com/encryption/keygen
- Encryption and Decrytion using Symmetric Key
  - http://aes.online-domain-tools.com/
- Asymetric Key Generation
  - https://csfieldguide.org.nz/en/interactives/rsa-key-generator/



Digital Signatures

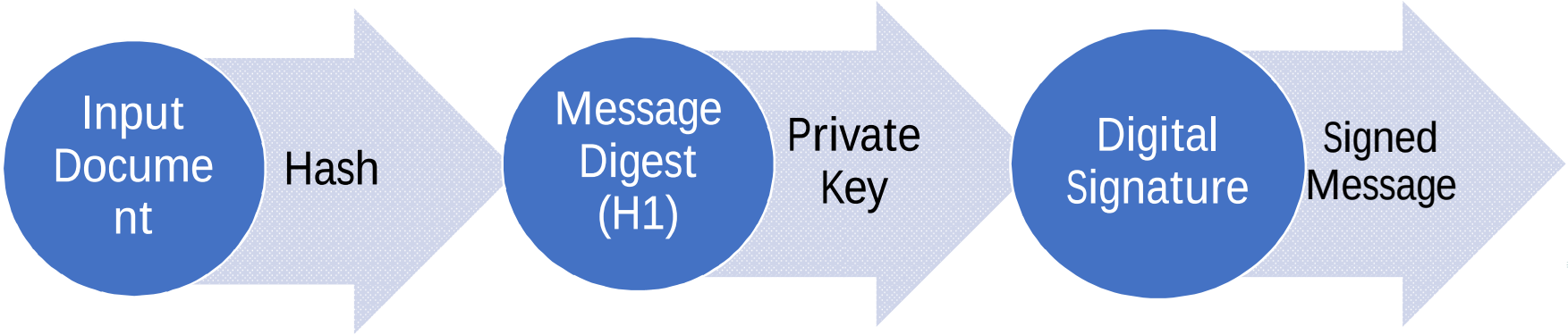


Digital Signatures

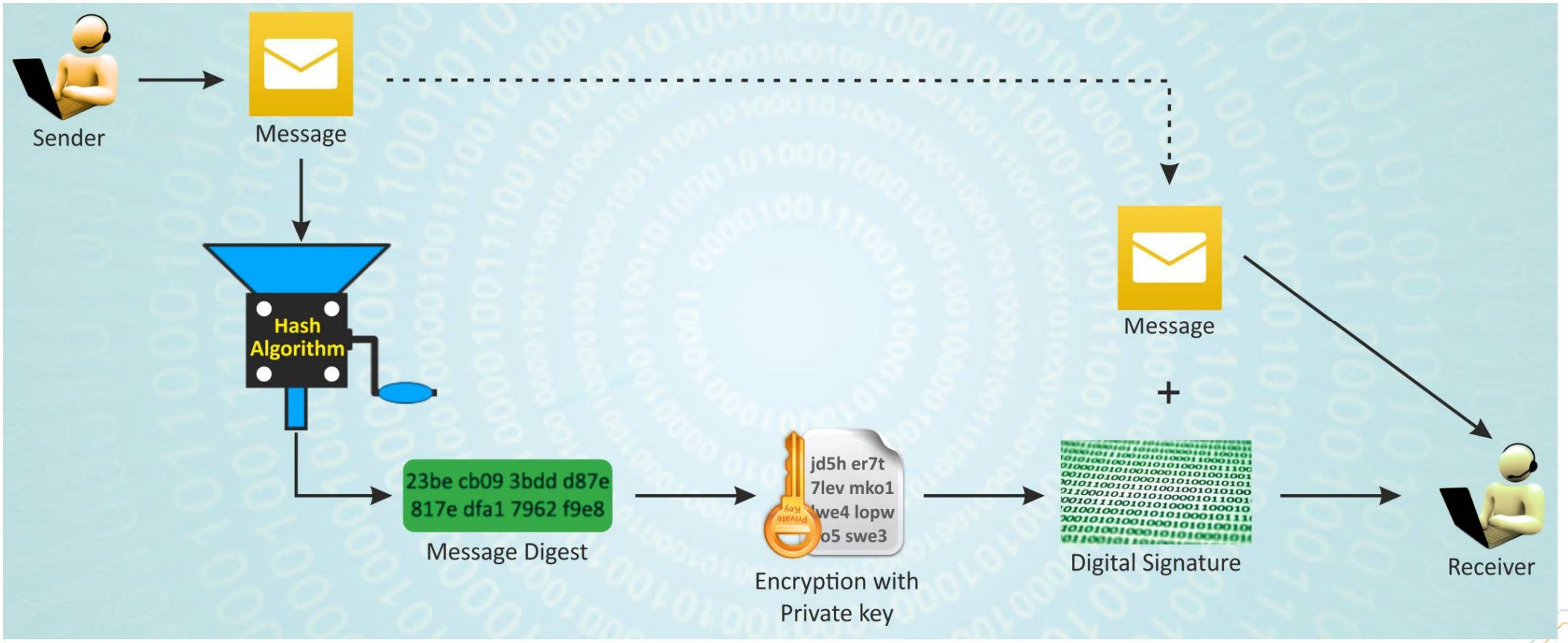
- Synonymous with Handwritten Signatures
- Based on **Asymmetric Key based cryptography**
- Is a number (thumbprint) based on
  - Content being signed
  - Private key of the signer
- Mathematical technique for validating
  - Authenticity and Integrity
- **Legal validity as per IT Act 2000**

Creating Digital Signature

- Signer has a key pair
  - Private key – known only to the signer
  - Public key – known to everyone
- Hashing algorithm is used to create **Message Digest**
- Private key is used to **Digitally Sign** the document
- Public key is used for verification of the signature

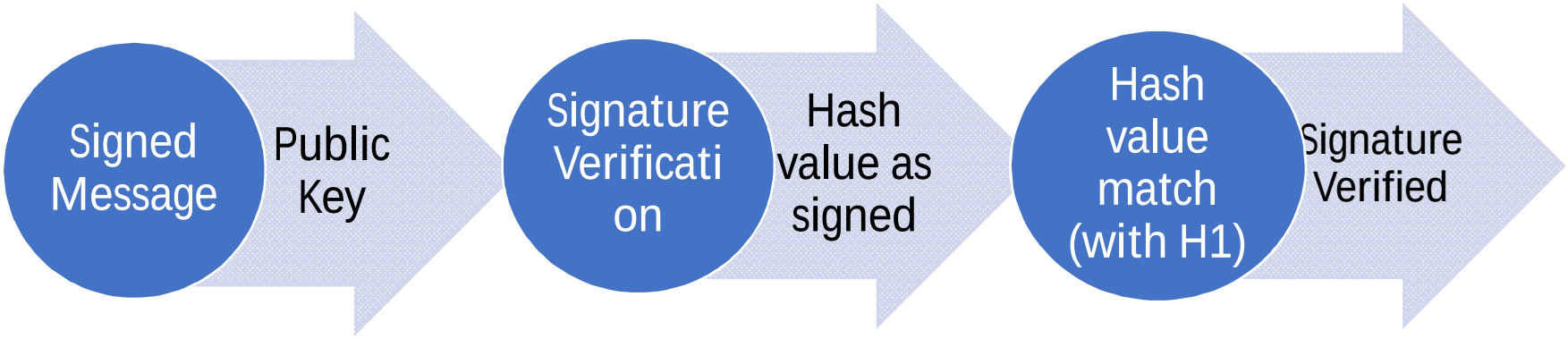


Digital Signature Creation Process

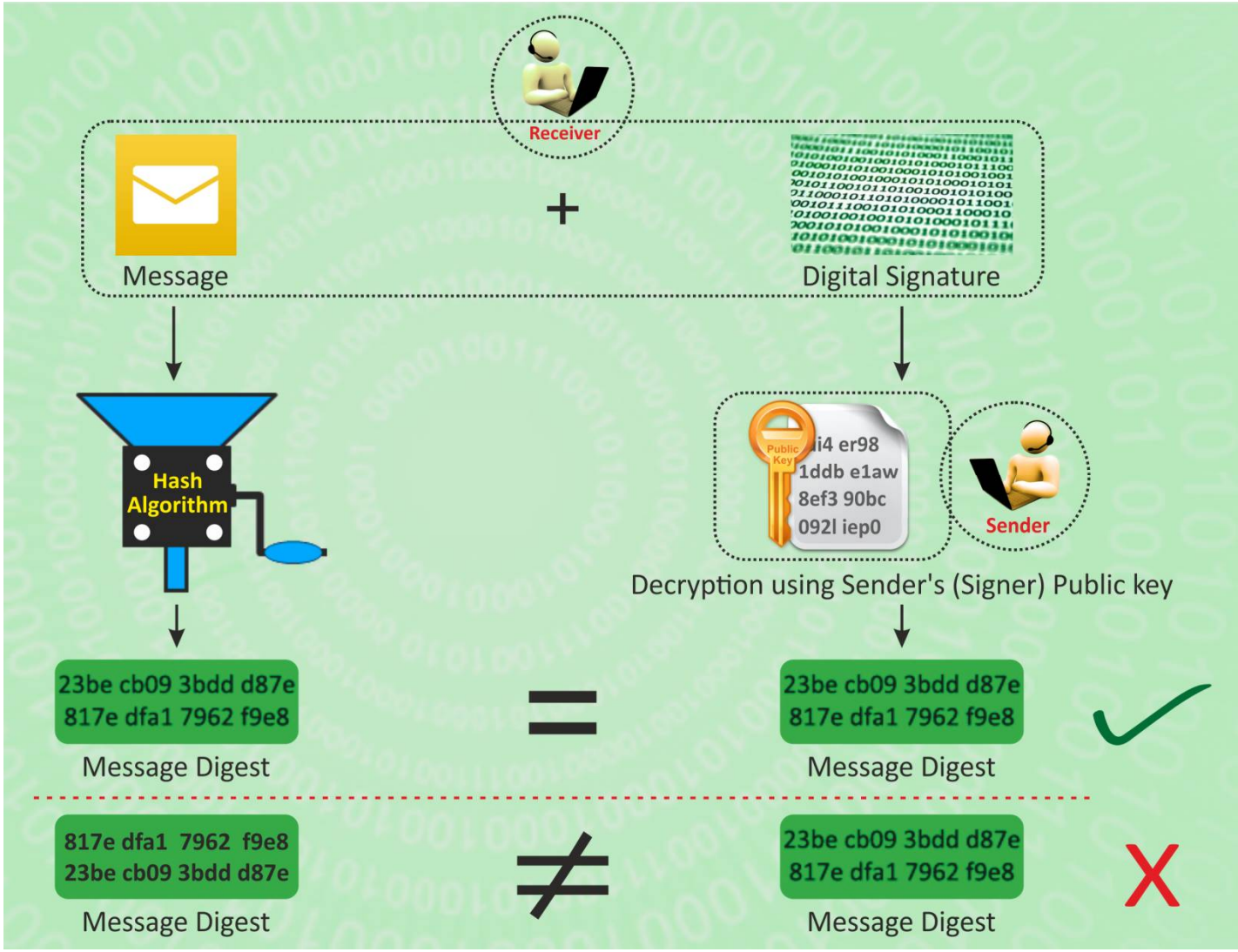


Digital Signature Verification

- Verifier receives Signed Message and Public Key
- Public key is used for signature verification
- On successful verification, signed message digest can be obtained
- Match the hash value obtained with the hash used for signing

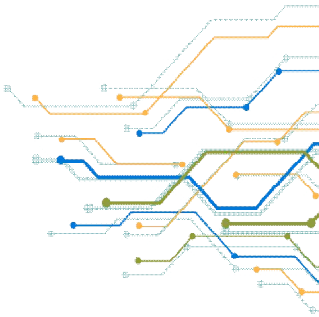


Digital Signature Verification Process



Demonstration

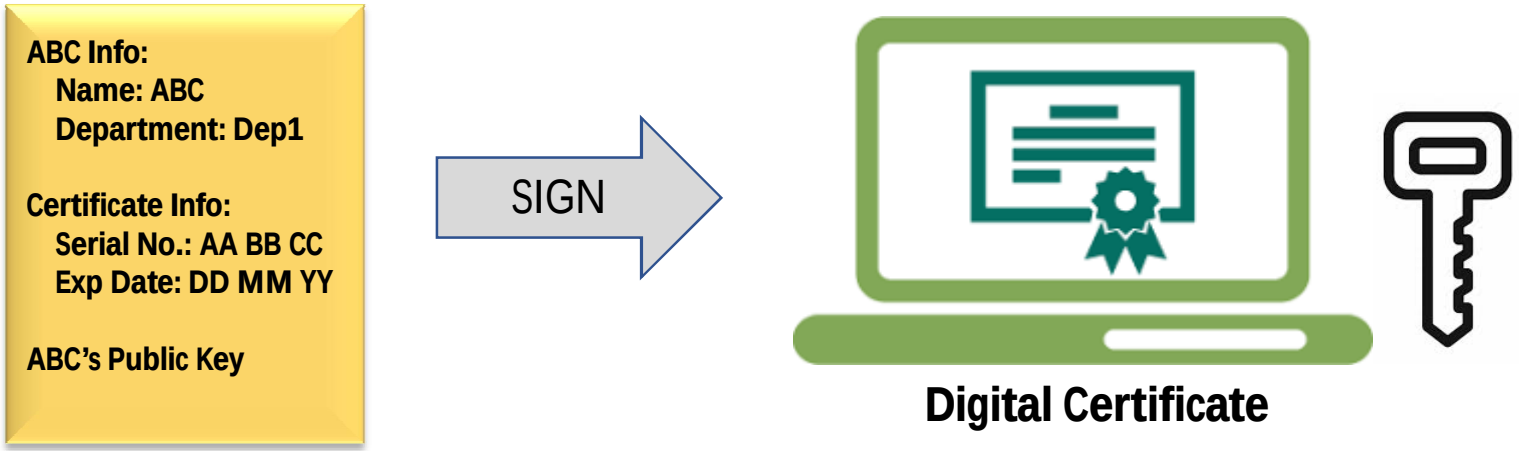
- Signature Generation using RSA key
  - https://8gwifi.org/RSAFunctionality?rsasignverifyfunctions=rsasignverifyfunctions&keysize=2048
- Signature Verification using RSA key
  - https://8gwifi.org/RSAFunctionality?rsasignverifyfunctions=rsasignverifyfunctions&keysize=2048



Digital Signature Certificate (DSC)

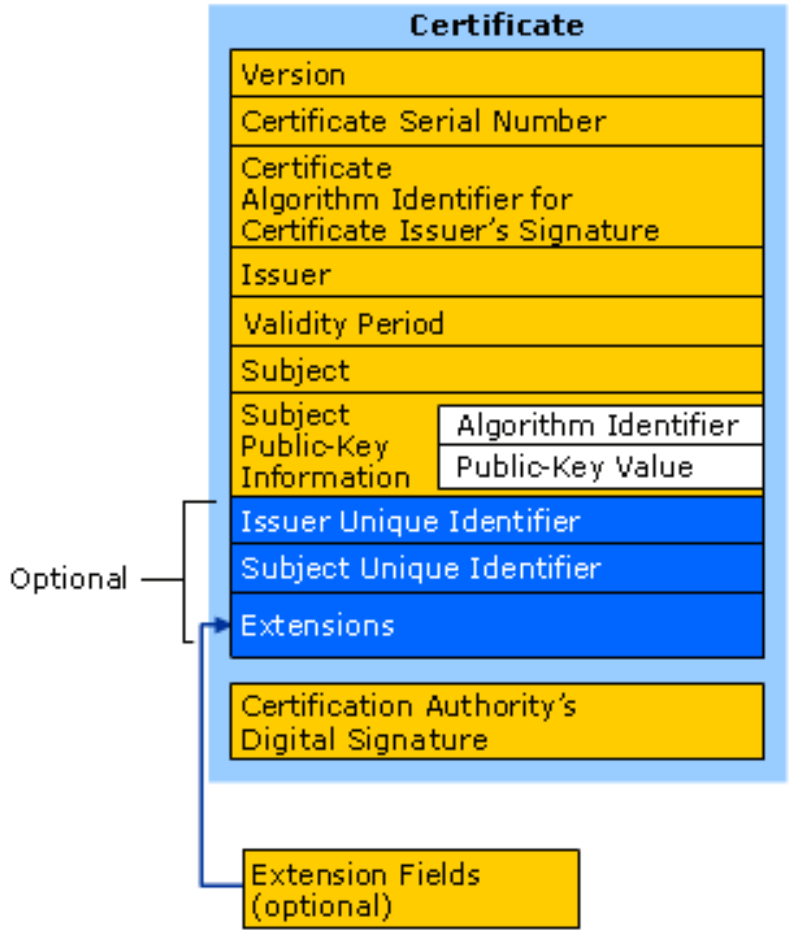
Digital Signature Certificate (DSC)

- DSC are required to
  - Establish ownership of the public key
  - Certify and provide a strong mechanism for non-repudiation
- DSC is an electronic document and contains
  - Information about the owner's identity
  - Information about the key
  - Digital Signature of an entity that has verified the certificate's content



Digital Signature Certificate Format – X.509

- X.509 is ITU-T standard for PKI
- X.509 v3 version

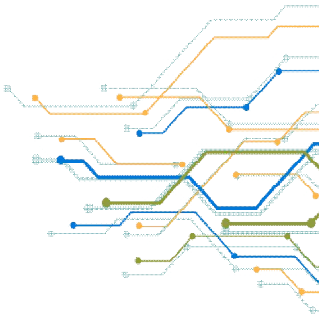


google.cer

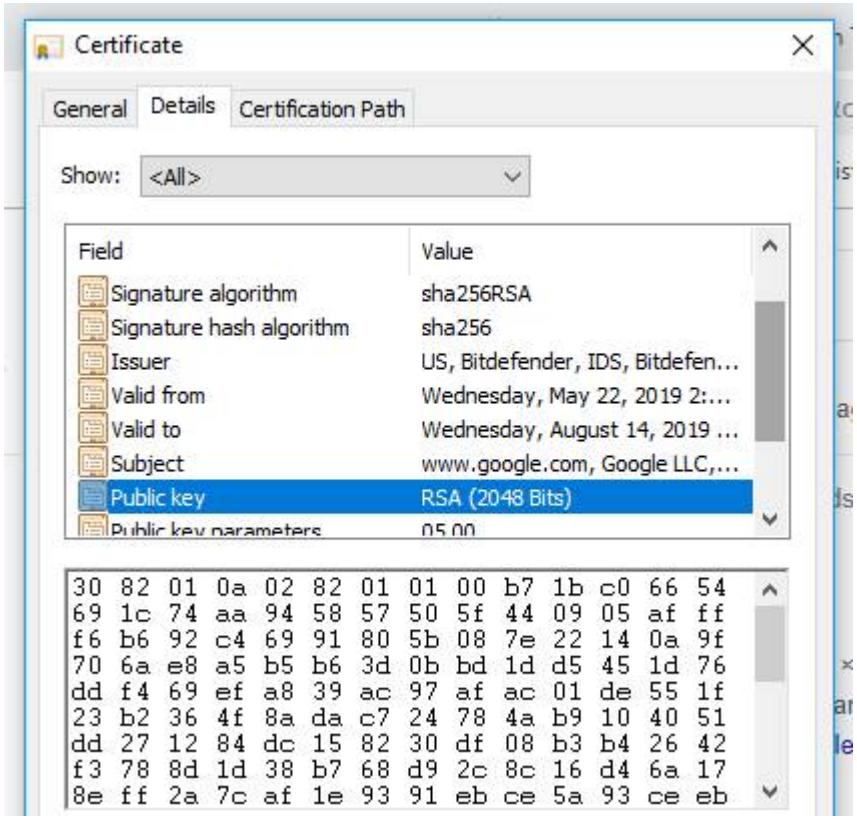
Sample Certificate File

X.509

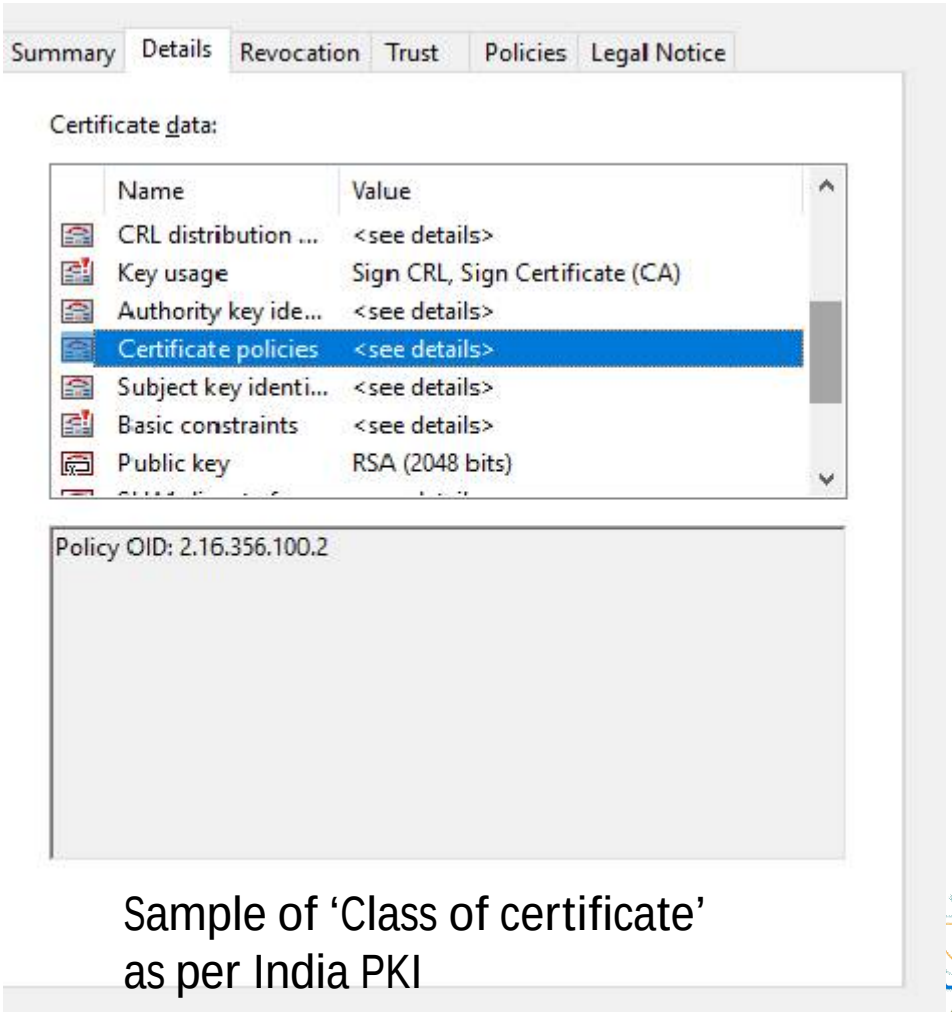
Applications	Authentication & encrypted web browsing using SSL/TLS and HTTPS.
	Signed and Encrypted emails via S/MIME protocol
	Code Signing
	Document Signing
	Client Authentication
	Government Issued Electronic ID



Sample Digital Certificate

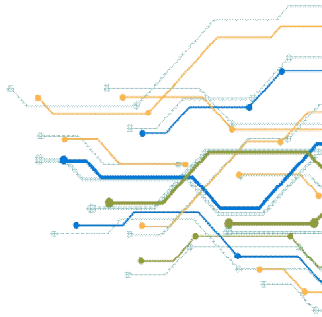


Google.com certificate



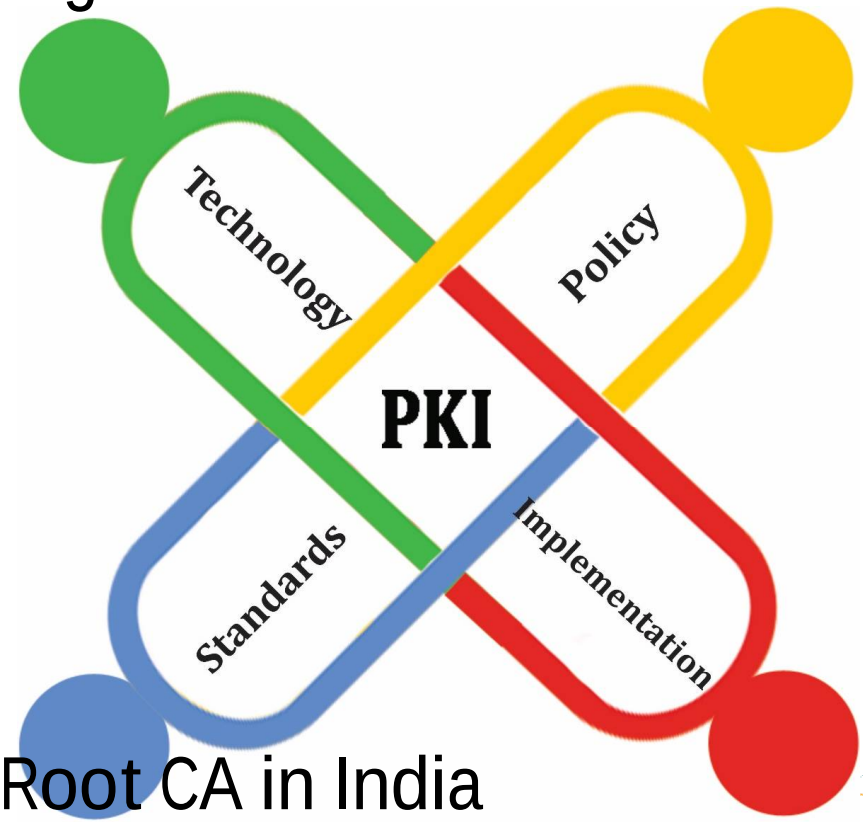
Sample of ‘Class of certificate’ as per India PKI

Public Key Infrastructure (PKI)

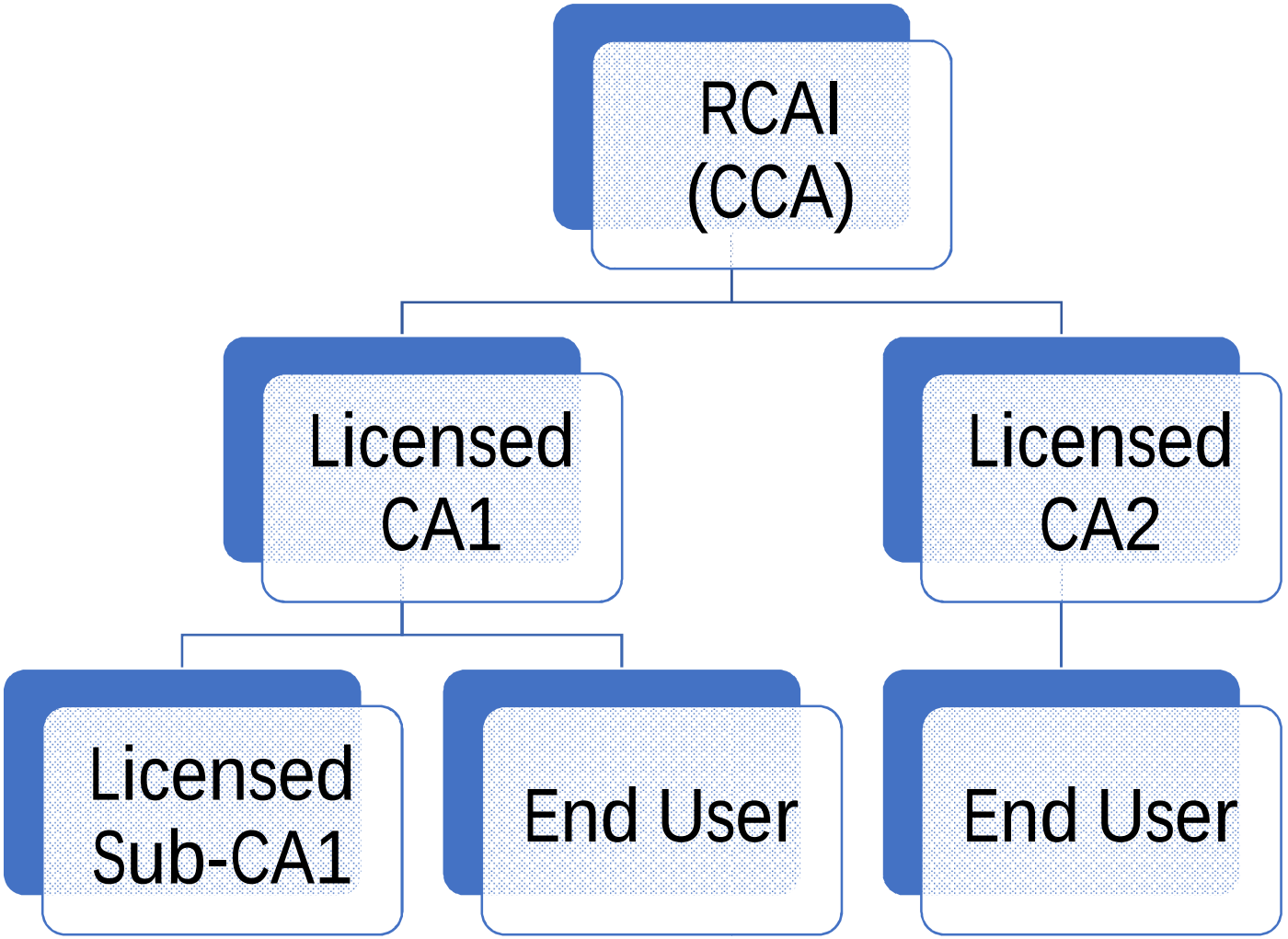


Public Key Infrastructure (PKI)

- Provides public-key encryption and digital signature services
- Manages key and certificates
- Key elements include
  - Root CA,
  - Registration Authority,
  - Sub CAs,
  - Certificate Status
- Provides the **trust** in the certificate chain
- Controller of Certifying Authority (CCA) is Root CA in India



Trust Model in India

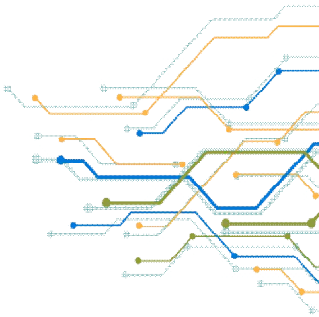


Certifying Authority (CA)

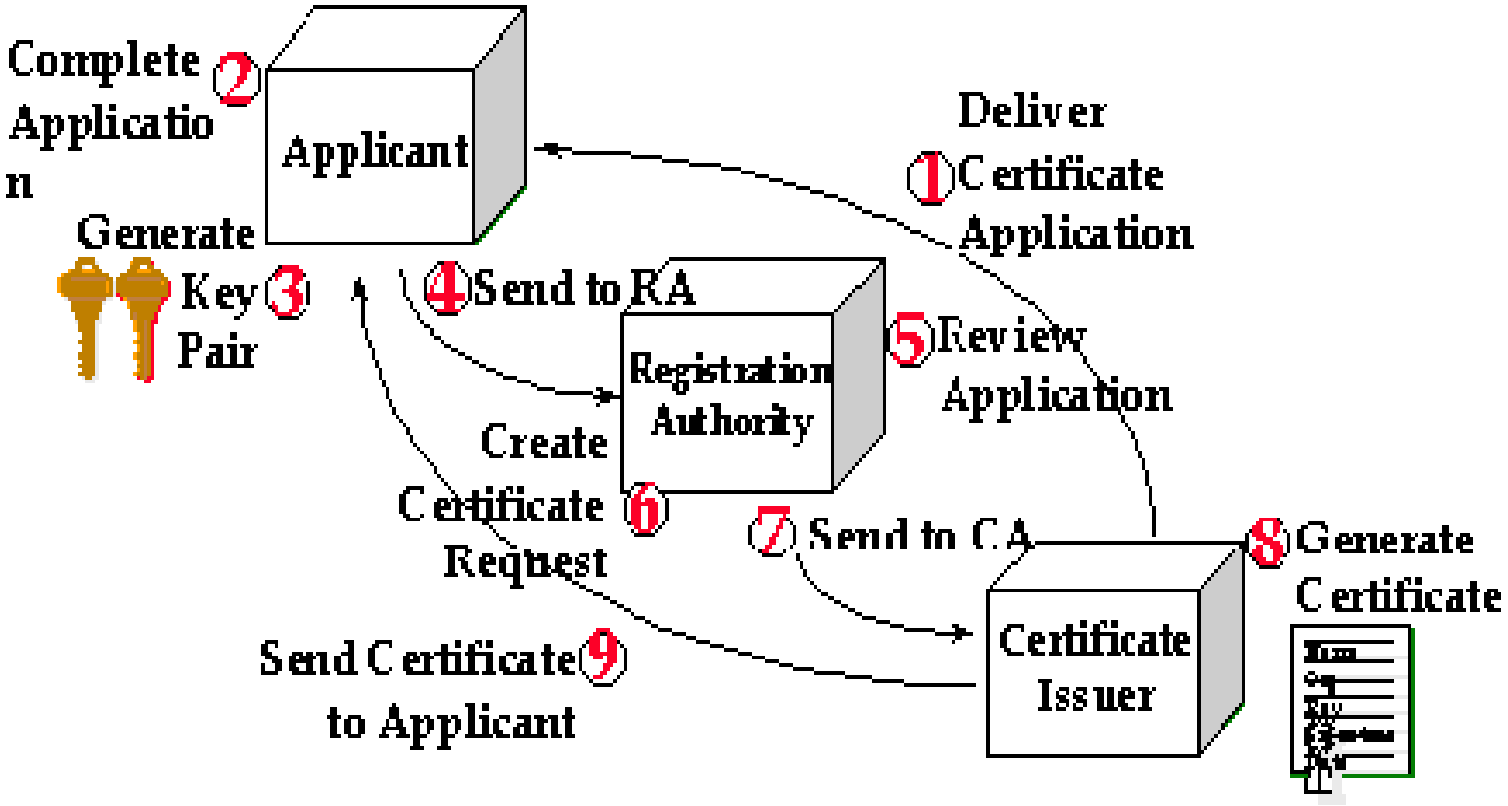
- Certifying authority is an entity which issues Digital Certificate
- It is a Trusted third party
- CA's are the important part of Public Key Infrastructure (PKI)

Responsibilities of CA

- Verify the credentials of the person requesting for the certificate (RA's responsibility)
- Issue certificates
- Revoke certificate
- Generate and upload Certificate Revocation List (CRL)



Certificate Issuance Process

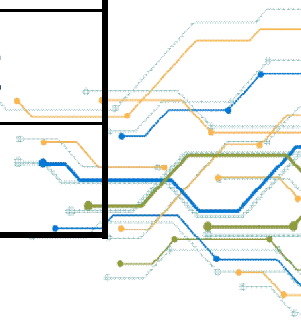


- Application
- Subject Authentication
- Certificate Generation

- Certificate Distribution
- Certificate Revocation

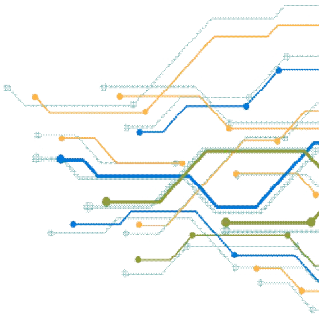
Certificate Extensions

File Formats with Extensions	Description
.CER	Contains only Public Key
.CRT	Contains only Public Key
.DER	Contains only Public Key
.P12	Contains Public and Private Key
.PFX	Contains Public and Private Key
.PEM, .KEY, .JKS	Contains Public and Private Key
.CSR	Certificate Signing Request
.CRL	Certificate Revocation List



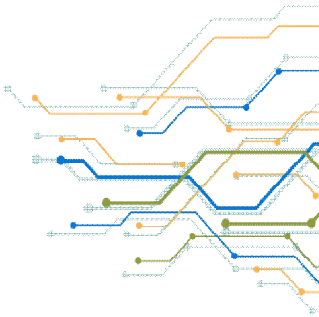
Certificate Classes

- Certificate classes define **level of assurance** for a Digital Certificate
- 3 Classes of Certificates
  - **Class1 Certificate**: Individuals/Private subscribers- E-mail usage.
  - **Class2 Certificate**: Both business personnel and private individuals use.
  - **Class3 Certificate**: issued to individuals as well as organizations, high assurance. Certificates, primarily intended for e-commerce applications, issued to individuals only on their personal, physical appearance before the Certifying Authorities.



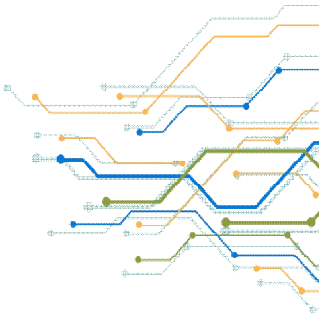
Types of Certificates

- Types define the purpose for which a Digital Certificate is issued
- Signing Certificate (DSC)
  - Issued to a person for signing of electronic documents
- Encryption Certificate
  - Issued to a person for the purpose of Encryption
- SSL Certificate
  - Issued to a Internet domain name (Web Servers, Email Servers etc...)

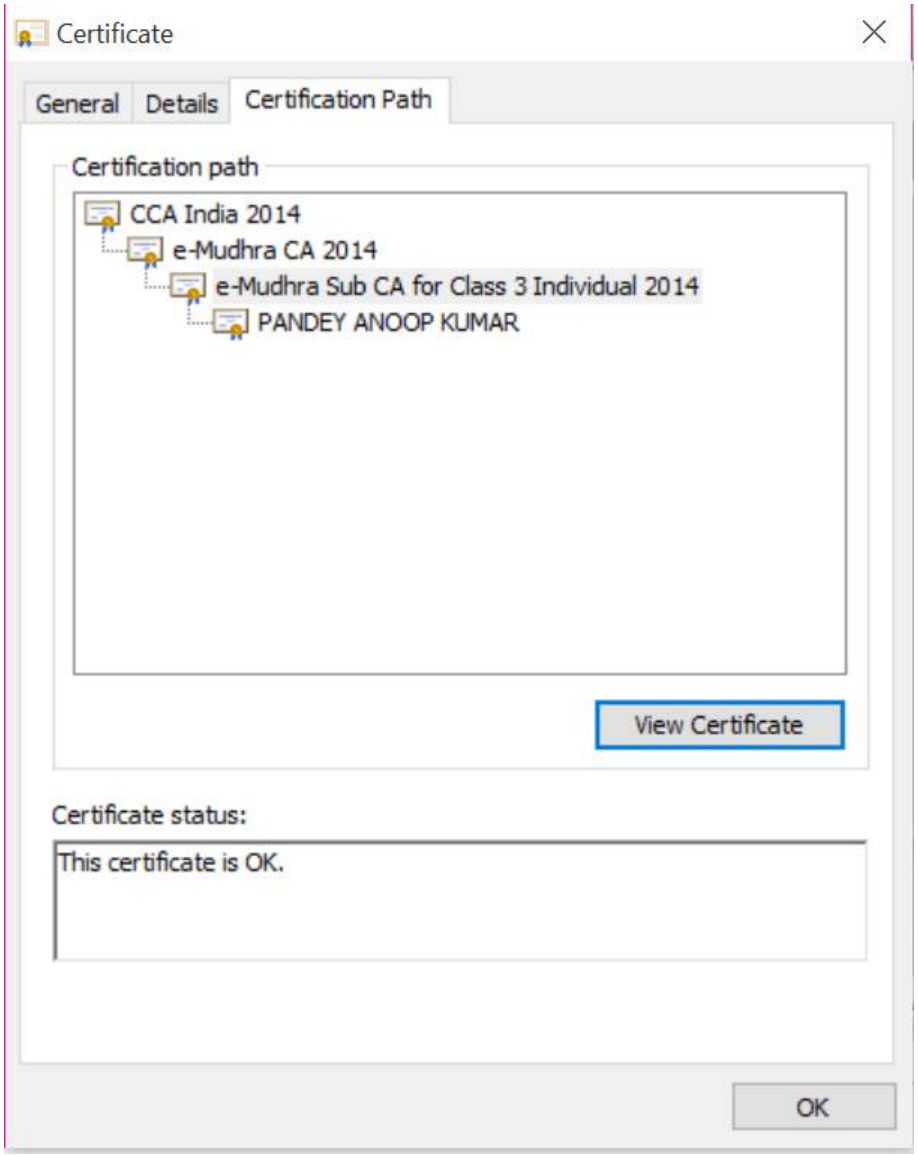


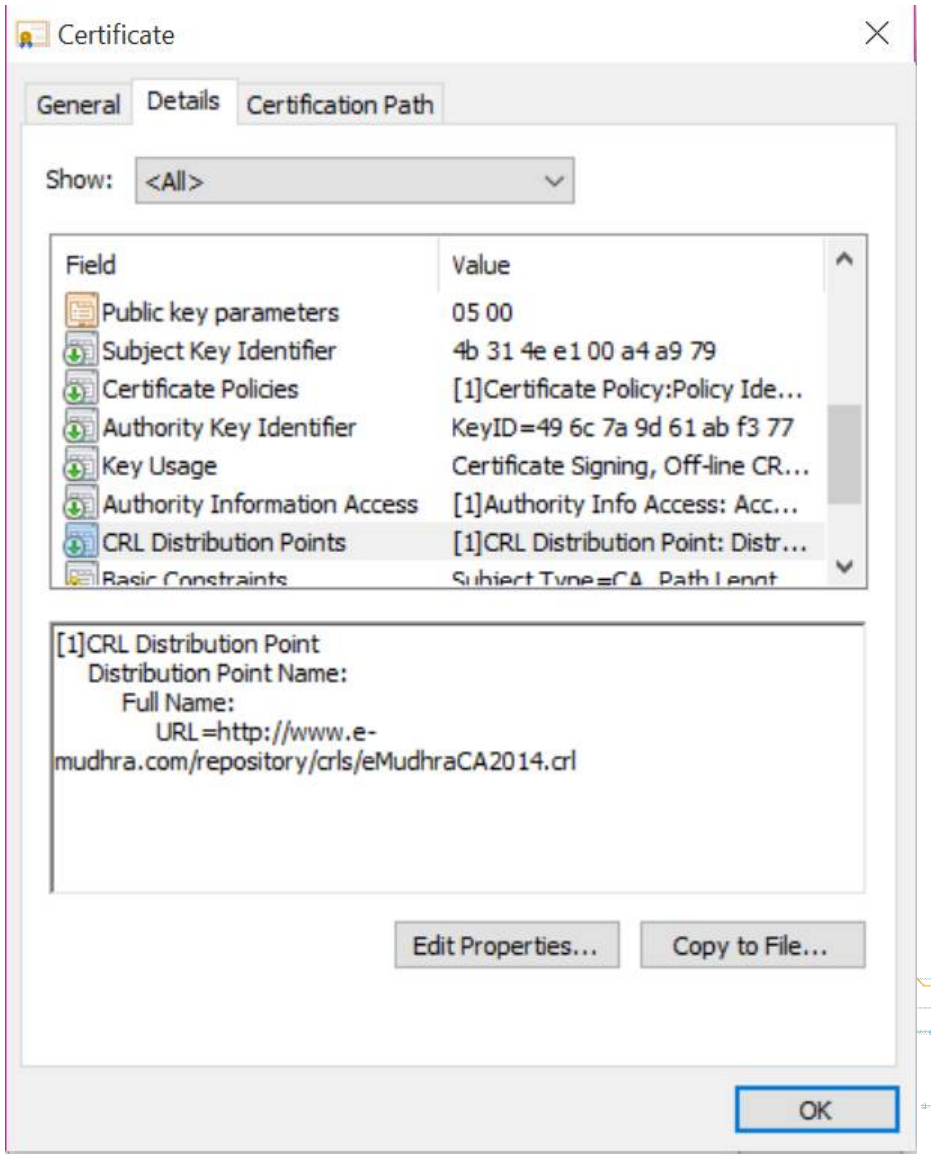
Certificate Revocation Check

- Certificate revocation is defined for **non-expired** certificates
- Can be checked in two ways
  - Certificate Revocation List (**CRL**)
  - Online Certificate Status Protocol (**OCSP**)
- CRL
  - Is a list containing serial numbers of the certificates that have been revoked signed by CA's private key
  - URL is part of Certificate
  - Is updated based on CA's policy
- OCSP
  - Is an online method to check certificate status
  - OCSP URL is part of Certificate

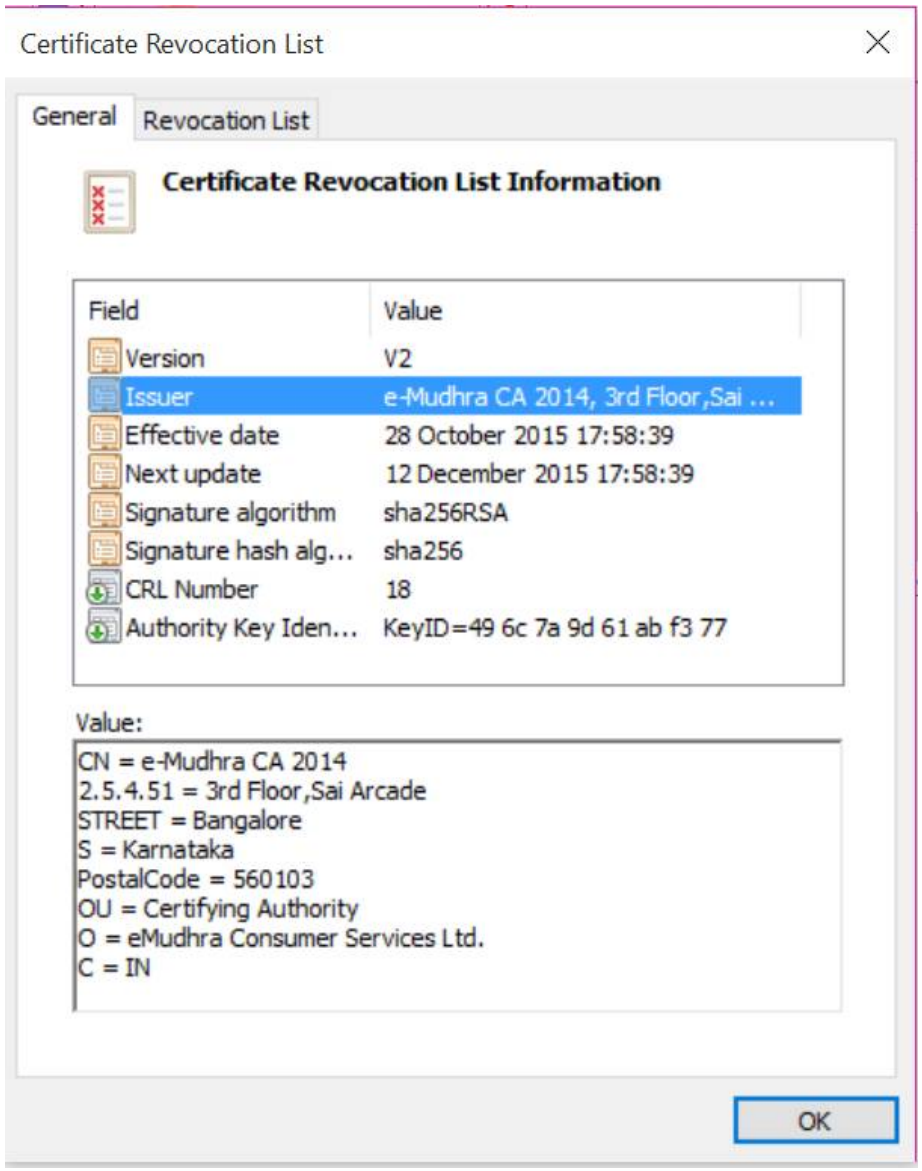


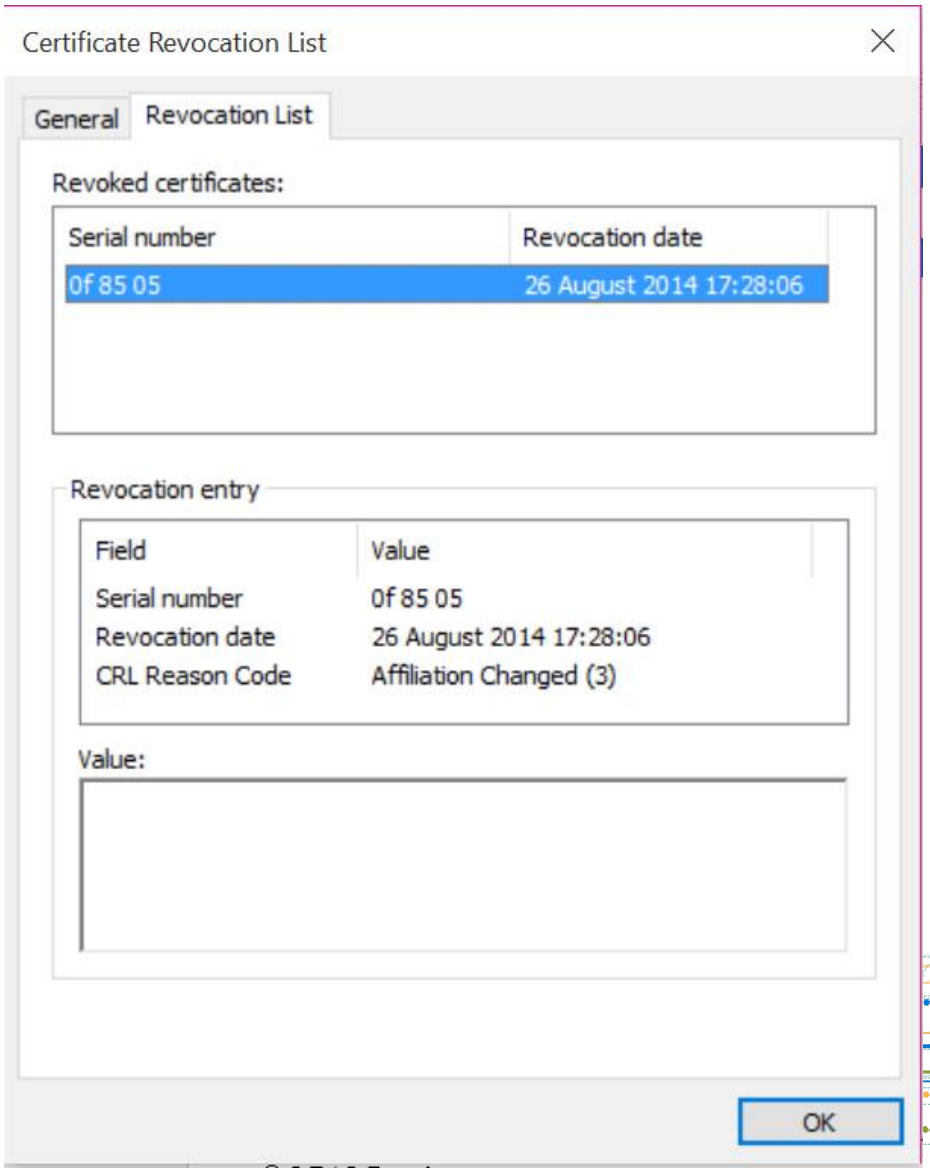
Obtaining CRL





Sample CRL


Certificate Revocation List
General
Revocation List
Certificate Revocation List Information
Field
Value
Version
V2
Issuer
e-Mudhra CA 2014, 3rd Floor,Sai ...
Effective date
28 October 2015 17:58:39
Next update
12 December 2015 17:58:39
Signature algorithm
sha256RSA
Signature hash alg...
sha256
CRL Number
18
Authority Key Iden...
KeyID=49 6c 7a 9d 61 ab f3 77
Value:
CN = e-Mudhra CA 2014
2.5.4.51 = 3rd Floor,Sai Arcade
STREET = Bangalore
S = Karnataka
PostalCode = 560103
OU = Certifying Authority
O = eMudhra Consumer Services Ltd.
C = IN
OK

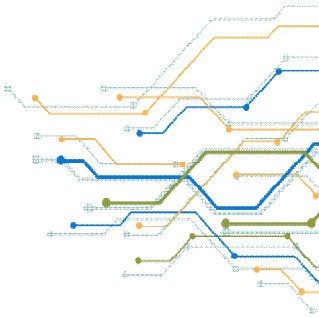

Certificate Revocation List
General
Revocation List
Revoked certificates:
Serial number
Revocation date
0f 85 05
26 August 2014 17:28:06
Revocation entry
Field
Value
Serial number
0f 85 05
Revocation date
26 August 2014 17:28:06
CRL Reason Code
Affiliation Changed (3)
Value:
OK

Use case - Digital Signature in PDF document

- Digital Signatures are commonly seen on PDF files
- Signature content is embedded into the document
- Common format of signature – PKCS7
- On opening document, Acrobat Reader performs signature check
  - Signature is valid ➔ Message digest has not been changed
  - Signature was performed during the validity period of certificate
  - Certificate was not revoked at the time of signing ➔ Revocation check
  - Complete certificate chain (till Trusted Root) is successfully formed
- Digital Signature on other format of documents
  - Can be done !!!
  - Standard APIs can be used for signature verification

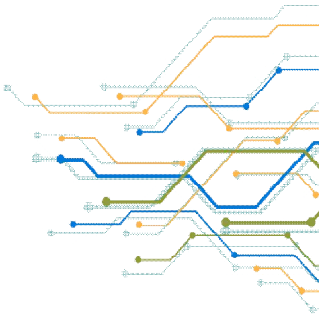
Test.pdf

Sample Signed PDF File



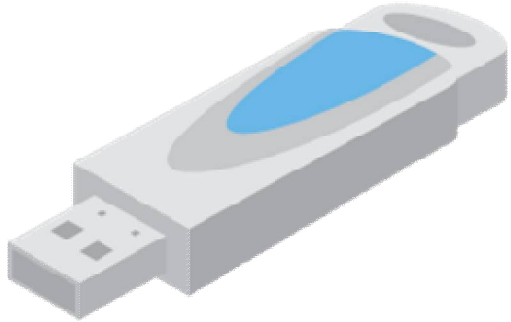
Digital Signature Validation

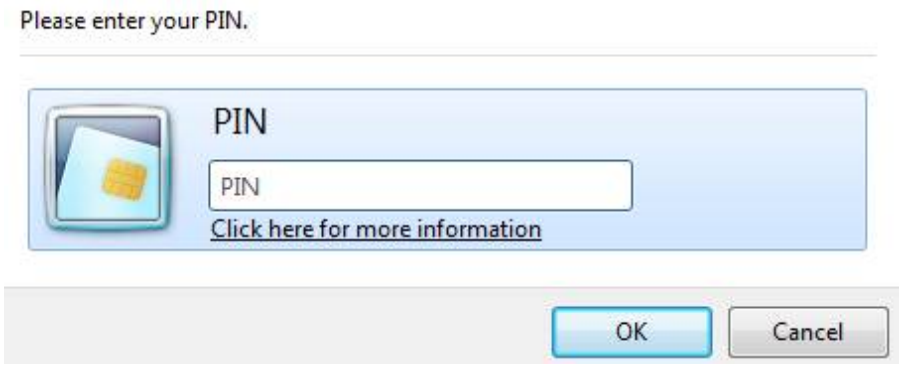
- Digital Signature Validation includes the following
  - Signature is valid ➔ Message digest has not been changed
  - Signature was performed during the validity period of certificate
  - Certificate was not revoked at the time of signing ➔ Revocation check
  - Complete certificate chain (till Trusted Root) is successfully formed



Traditional Methods of Digital Signing

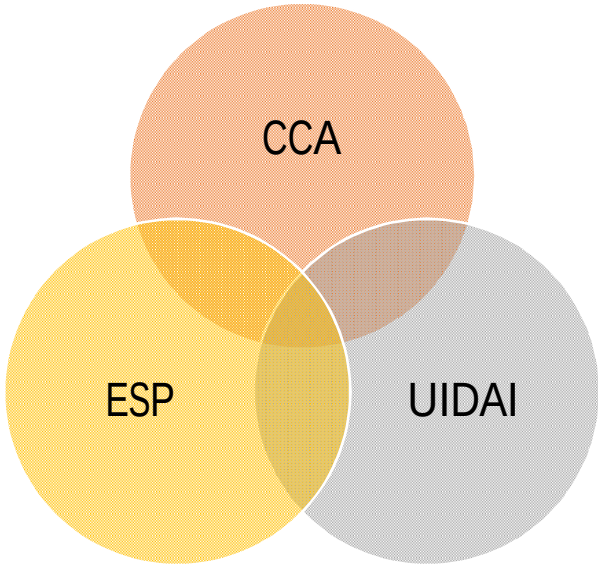
- Using Crypto Tokens
- Contain a Cryptographic co-processor with a USB interface
- Key is generated inside the token.
- Key is highly secured as it doesn't leave the token
- Highly portable and Machine-independent
- FIPS 140-2 compliant; Tamper-resistant;





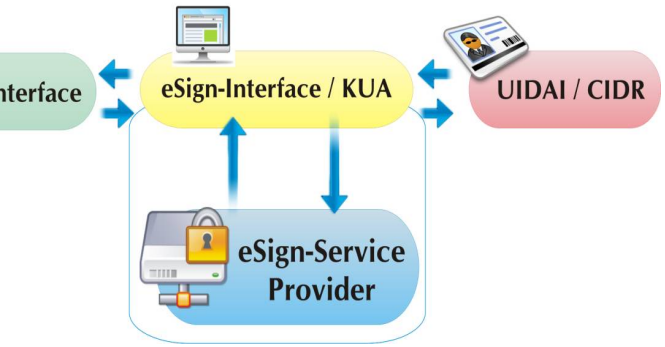
eSign – Online Digital Signing Service

- Government of India vide its Gazette Notification (REGD. NO. D. L.-33004/99 dated 28th January 2015) has announced – *"A method that facilitates CA to offer e-Sign service to citizens who have Aadhaar ID"*
- Objective of eSign service is to offer on-line service to citizens for instant signing of their documents securely in a legally acceptable form
- Two major challenges involved are
  - Authentication of the user - Uses authentication of signer through Aadhaar authentication and e-KYC service
  - Trusted method of signing - PKI method of signing
- Can be integrated within various service delivery applications via an open API to facilitate digitally signing a document by an Aadhaar holder
- Offers 2 class of certificates
  - Aadhaar-ekyc-OTP (OID: 2.16.356.100.2.4.1)
  - Aadhaar-ekyc-Bio (OID: 2.16.356.100.2.4.2)
- Paper to Digital Initiative
- Recently Offline Aadhaar Authentication based eSign announced



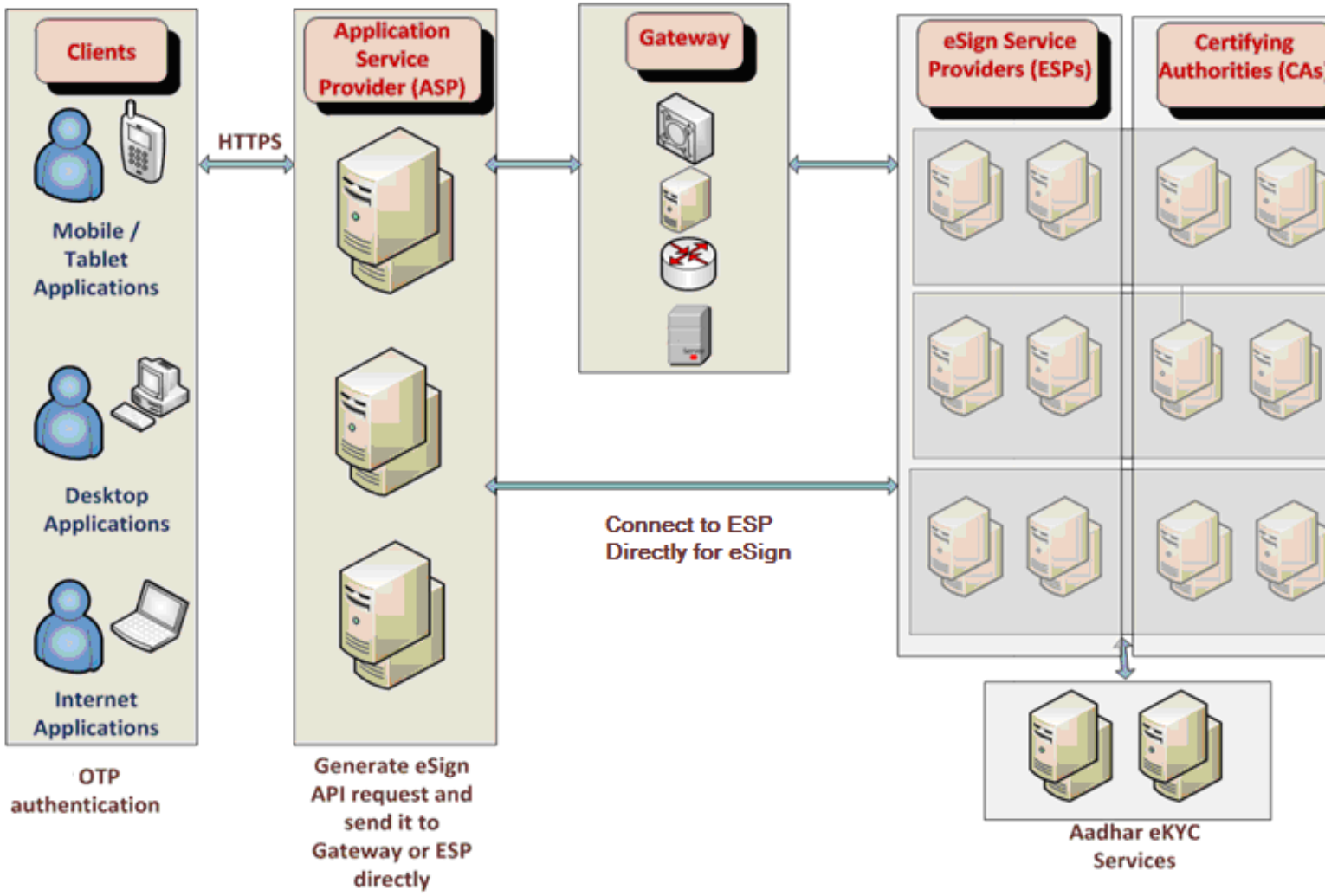
- **CCA**: Controller of Certifying Auth
- **ESP**: eSign Service Provider
- **UIDAI**: Unique Identification Auth of India

eSign Architecture

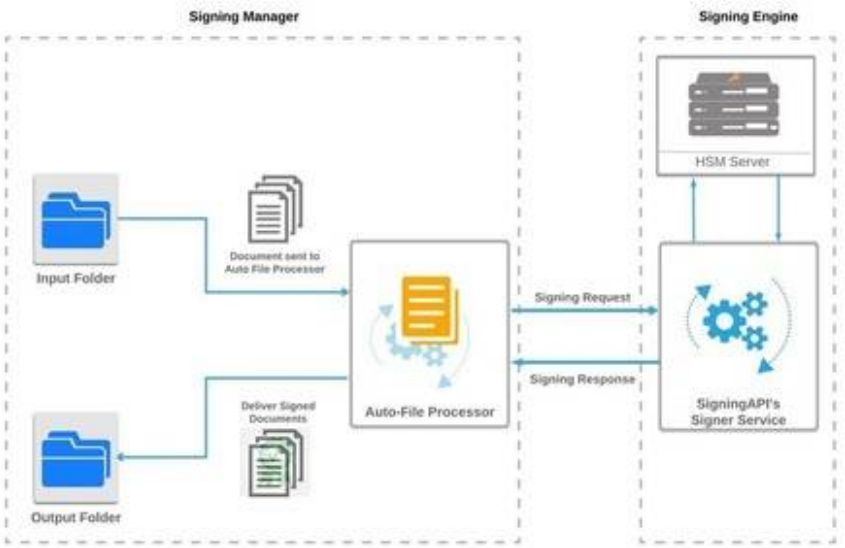


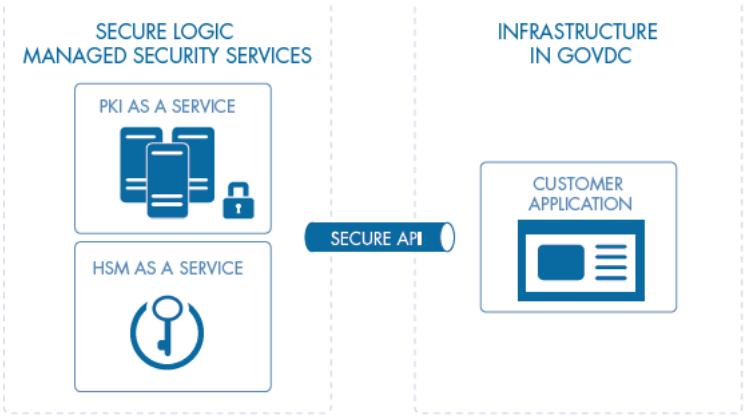
takeholders in eSign

- Document Signer
- Application Service Provider (ASP)
- eSign Service Provider (ESP)
- Certifying Authority (CA)
- UIDAI
- Controller of Certifying Authority (CCA)



HSM (Hardware Security Module)



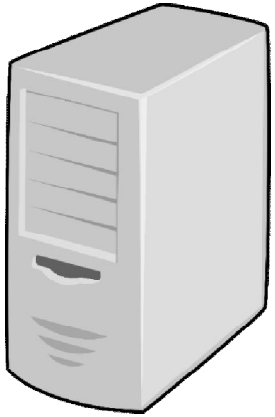


- Dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle
- Enterprise level solution for crypto key security
- Highest level of security
- Intrusion-resistant, tamper-evident, FIPS-validated appliance
- Also supports solutions on clouds (Cloud agnostic)
- Address compliance requirements with solutions for Blockchain, GDPR, IoT, paper-to-digital initiatives, PCI DSS, digital signatures etc..
- Strong logical role based access based on physical keys

- Example - Mandated by Aadhaar for authentication request

TLS – Transport layer security

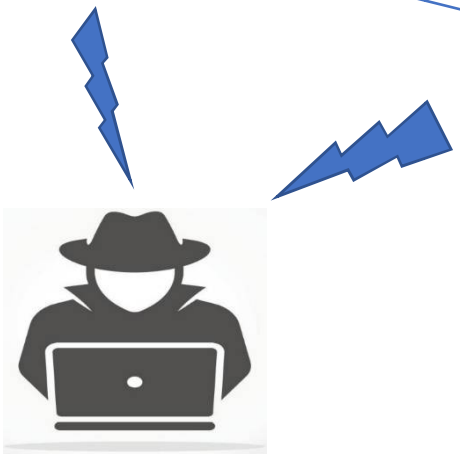
Without TLS

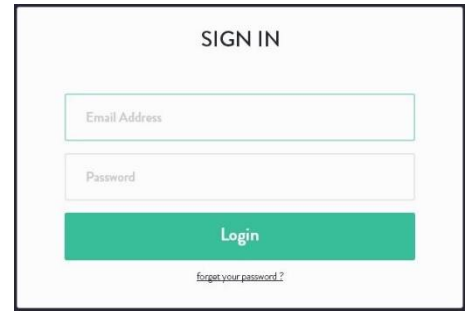


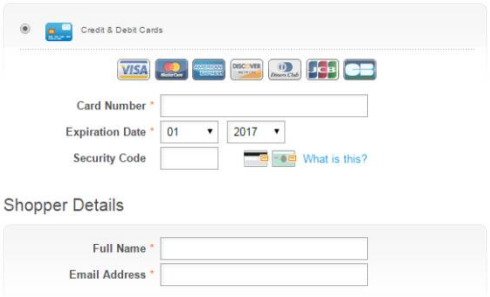
Shopping.com

Email: balaji@cdac.in
Password: ABCD1234

Card No: 34561234567
CVV: 1234 Expiry: 01/23

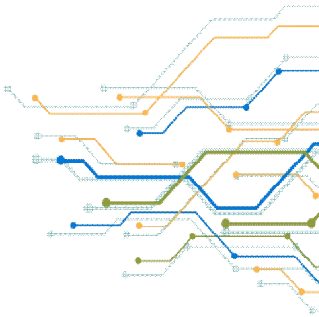




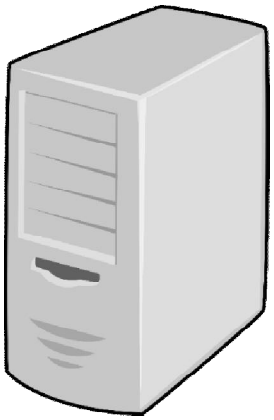


With TLS

- Servers use TLS (Transport Layer Security) certificates,
  - A certificate issued to a machine/server so as to establish a secure connection between the server and a browser using which we access the server.
  - Now all the information that is exchanged is in encrypted form and won’t make sense to anyone who tries to tap the information.



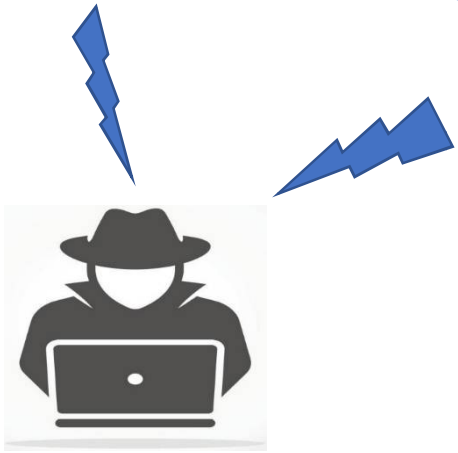
With TLS

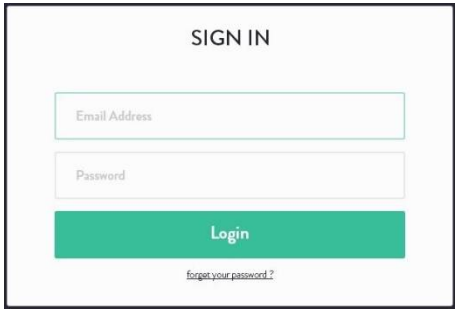


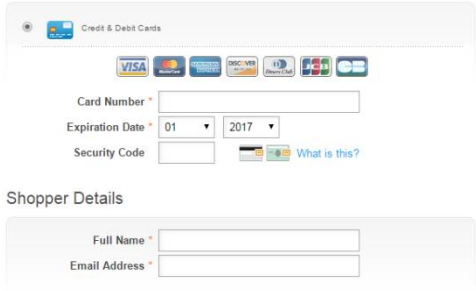
Shopping.com

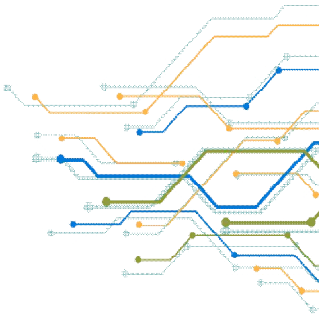
$%#^DE*&^9845988@

325435#$%$%@JFHSG

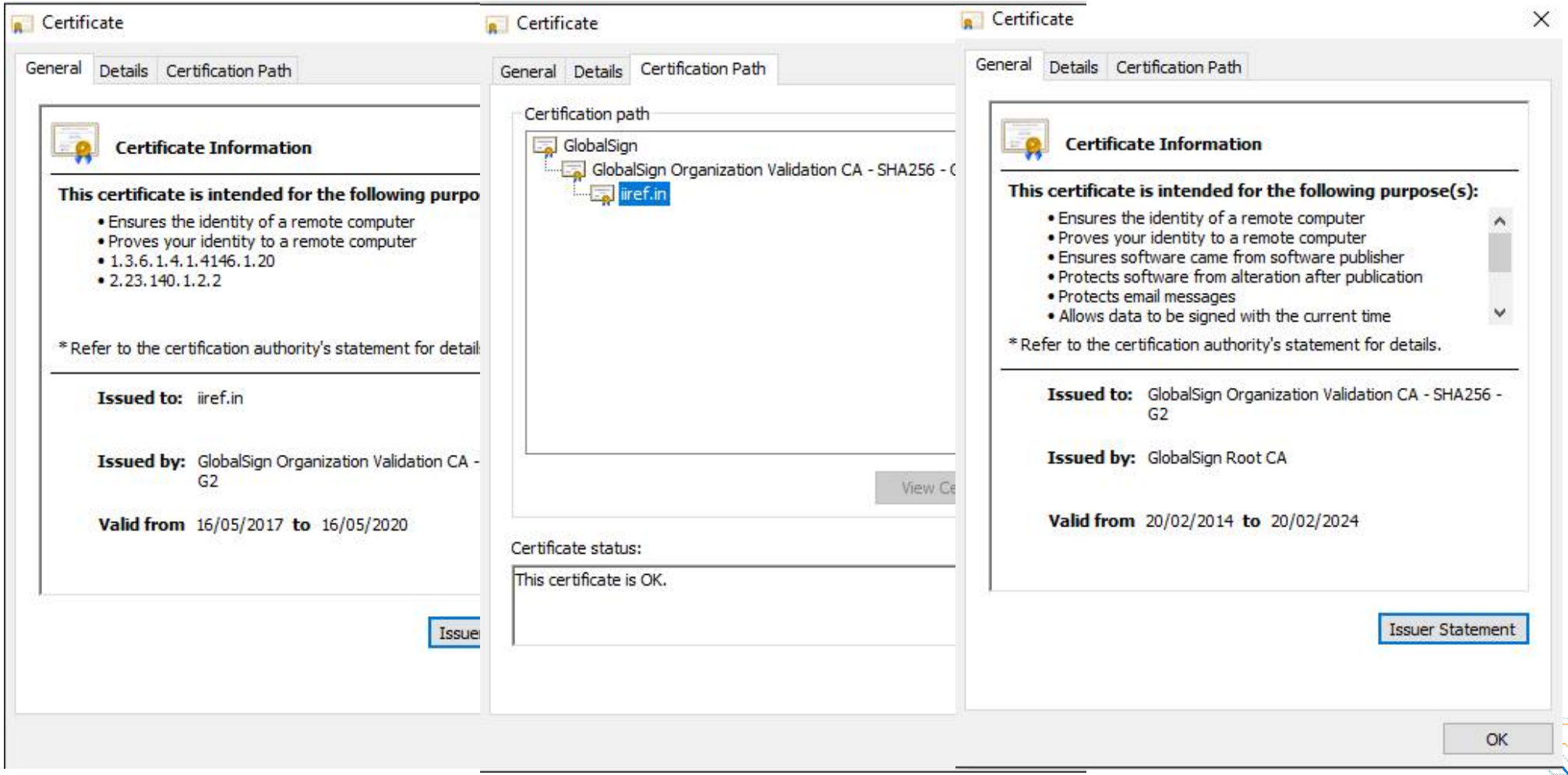






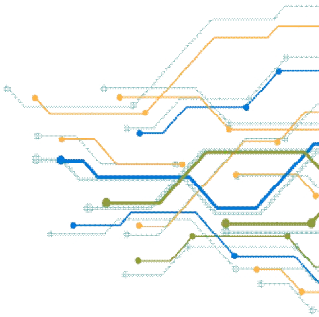


Sample Certificate



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 signs the certificate

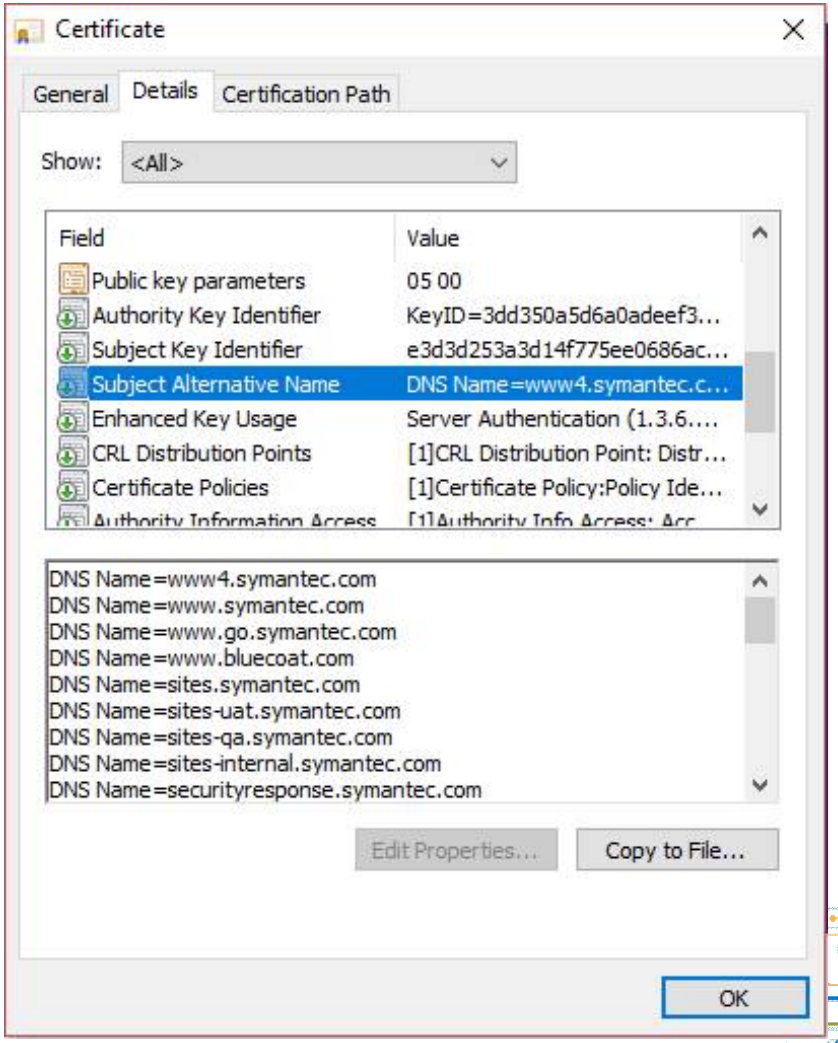


Types of TLS Certificates

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

Multi-Domain Certificates

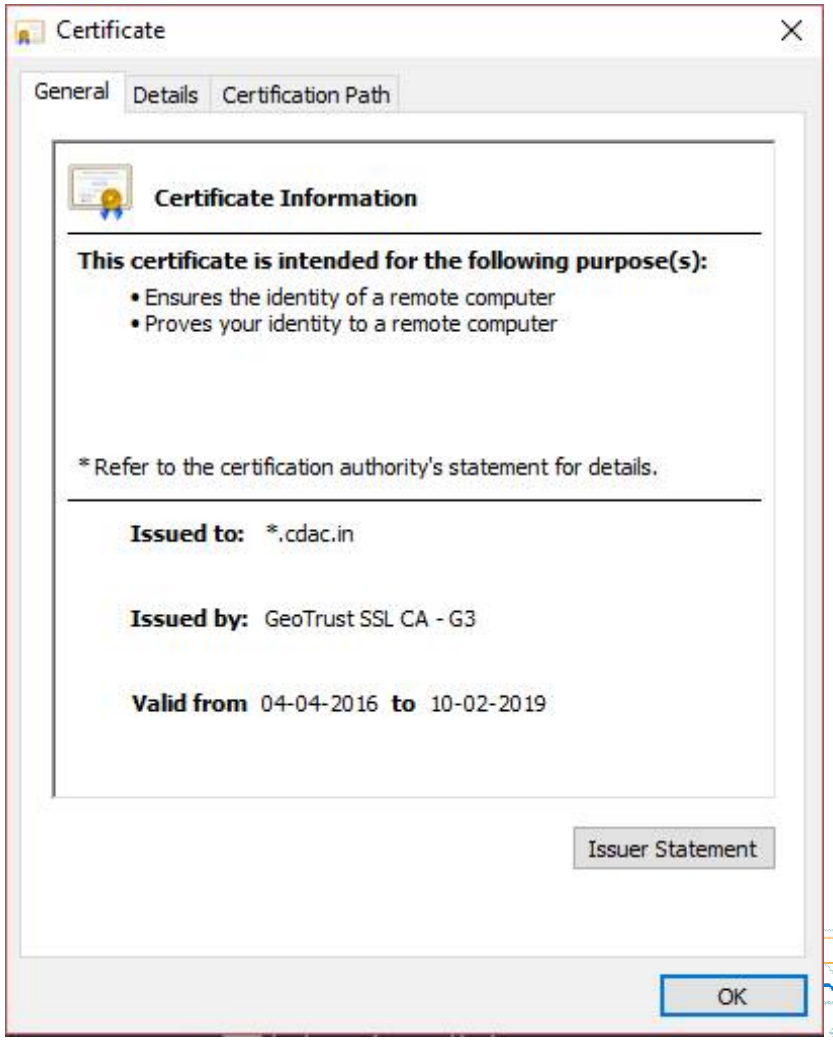
- Subject Alternative Names (SANs) Certificate
  - Can secure up to 100 different domain names, subdomains, and public IP addresses, using only one SSL Certificate and requiring only one IP to host the Certificate.



Wildcard Certificates

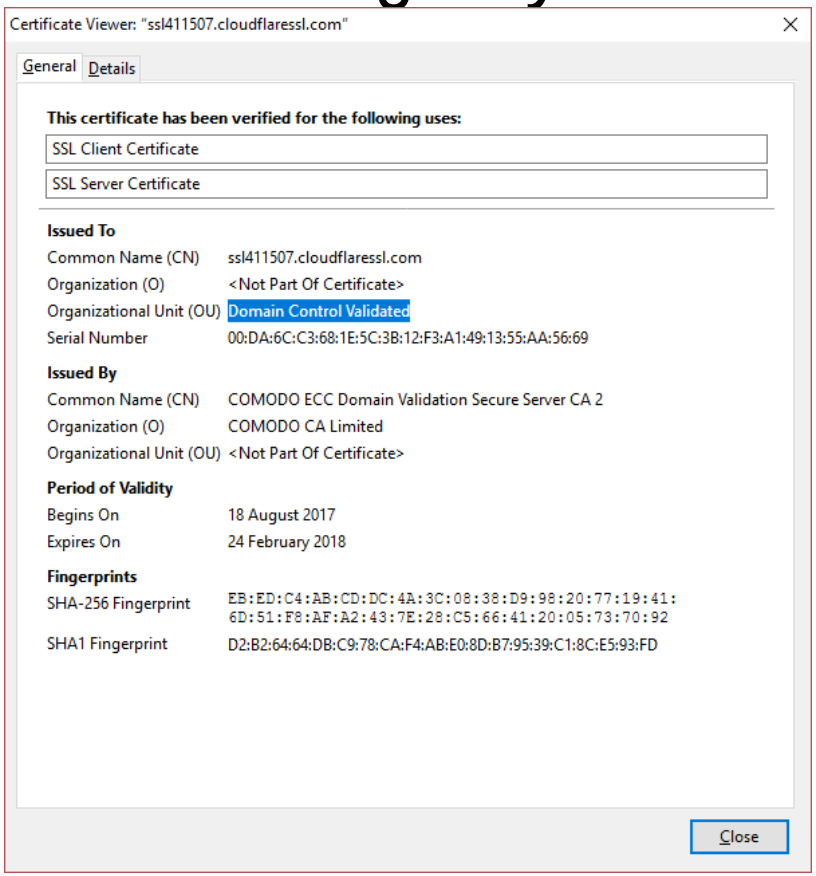
Wildcard certificate allows us to secure an unlimited number of subdomains on a single certificate.

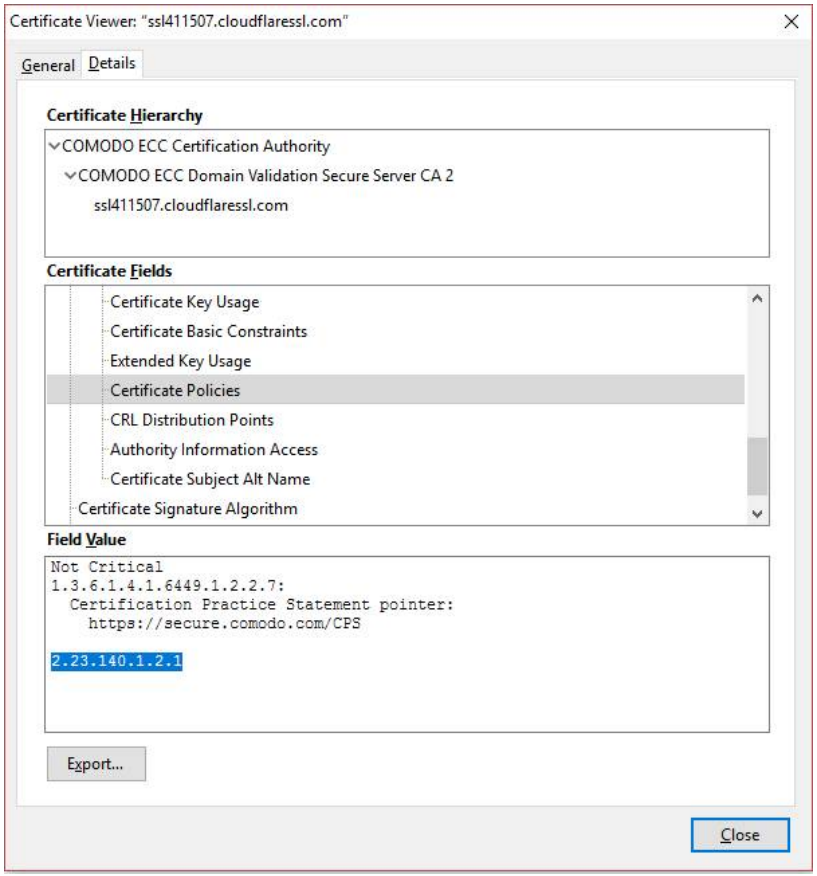
A Wildcard Certificate is issued to eg., *.cdac.in, where the asterisk represents all possible subdomains.

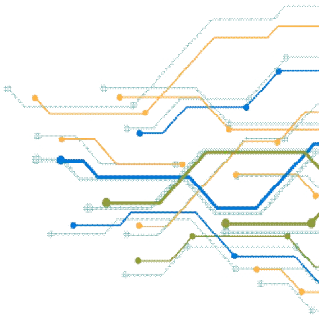


Domain Validated Certificate

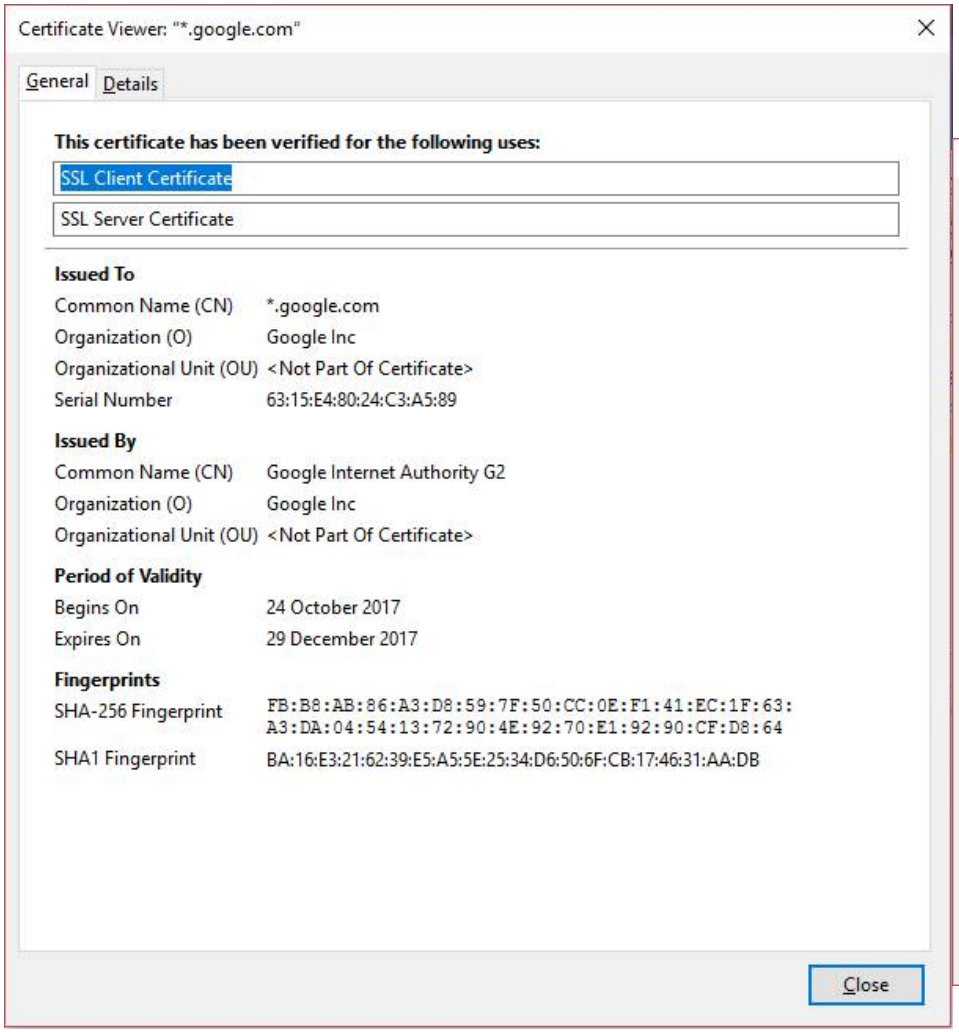
- Domain Validated certificates are certificates that are checked against domain registry.

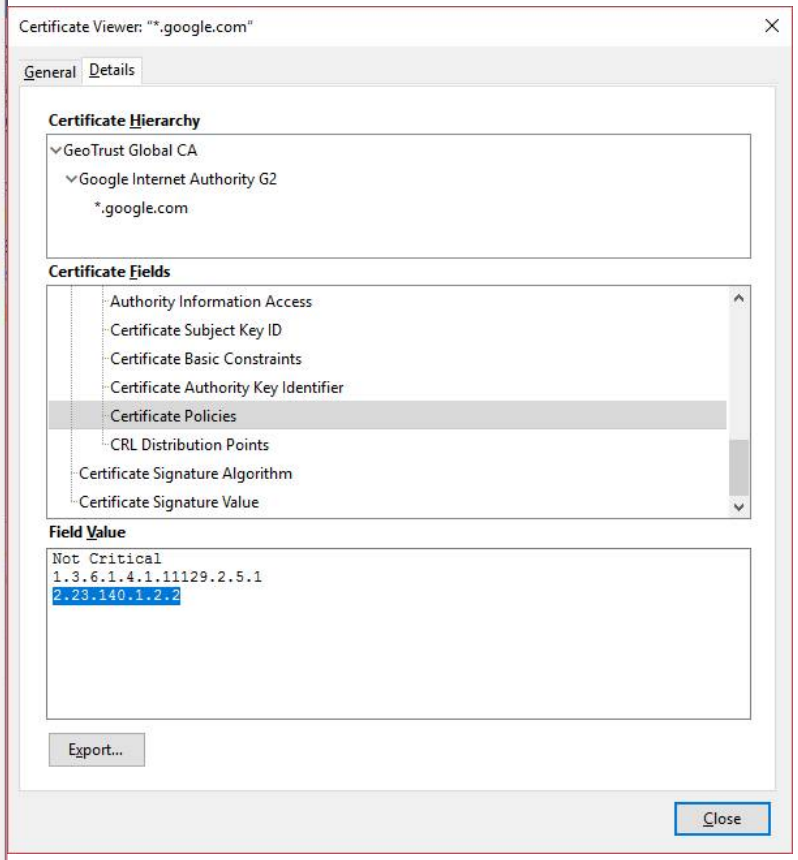






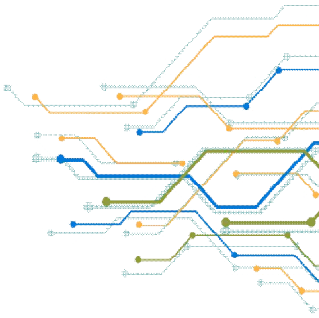
Organization Validated Certificate



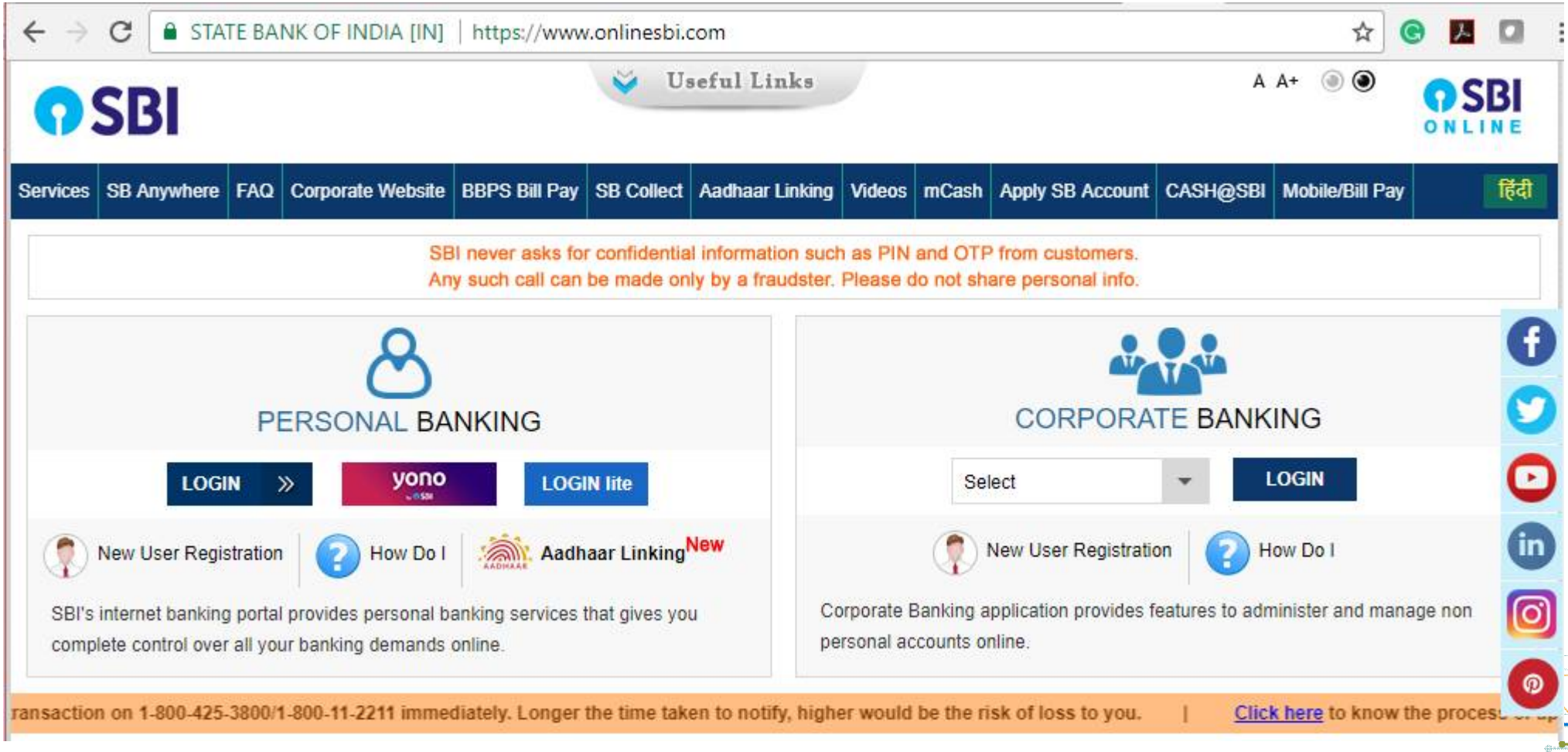


Organization Validated Certificate

- 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.
- It activates the **browser padlock** and https, shows the corporate identity

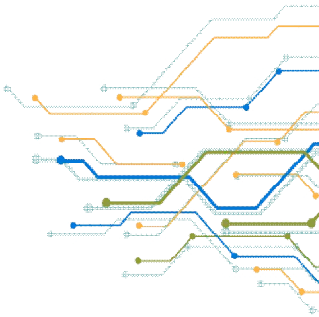


Extended Validation Certificate



Extended Validated Certificate

- An **Extended Validation Certificate** (EV) is a certificate issued according to a specific set of identity verification criteria.
- The criteria requires extensive verification of the requesting entity's identity by the CA before a certificate is issued.
- Extended TLS activates the green address bar and displays the organization name in the browser interface



Ministry of Electronics and
Information Technology
Government of India

CYBER SURAKSHIT
BHARAT

Digit
Power T

Thank You

nding
ners

Microsoft intel dimension data wipro redhat

wledge
ners

CDAC certin EY fido alliance IBM NeGD National e-Governance Division NATIONAL INFORMATICS CENTRE NIC paloalto NETWORKS