CYBER
VATTAM

Public Key Infrastructure (PKI)

Presented by
Venkatesh Jambulingam
Cloud Security Expert

11-Jul-2021

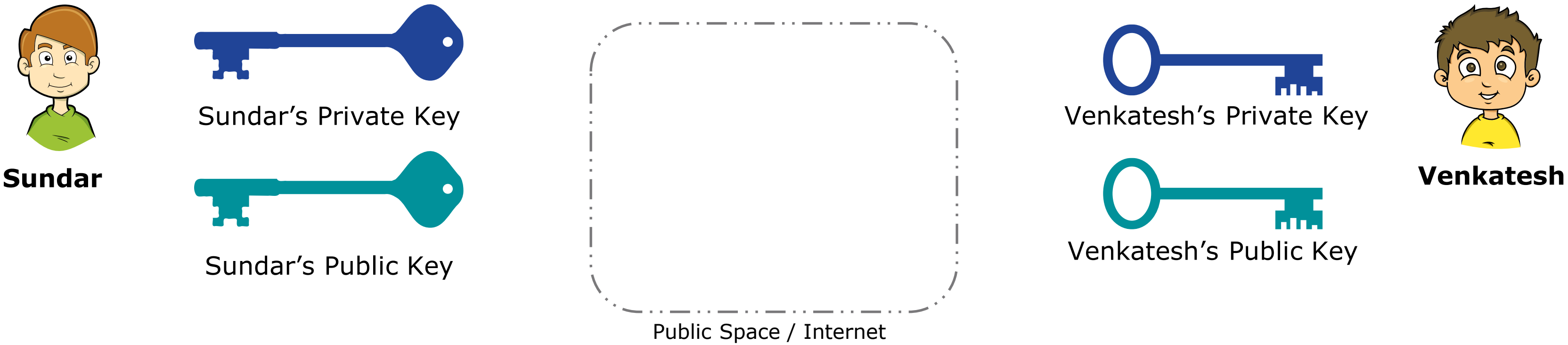
Contents

- Public Key Cryptography & Hashing
- Public Key Infrastructure (PKI)
- Digital Certificate
- Trust Services
    - Digital Signature Certificate
    - TLS Certificate
    - Code Signing Certificate
    - Time Stamping
    - Email Encryption Certificate

Public Key Cryptography & Hashing

Public Key Cryptography

- Each person will have two keys each
  - Public Key
  - Private Key
  - This is called a ‘Key Pair’
- Key Pair is mathematically linked to each other
  - You cannot guess or derive one key from the other key
  - One key is used for encryption and only the other key from that key pair can be used for decryption.
  - Public Key is shared in public space like internet, social media or email
  - Private Key is confidential and hence kept very securely



Sundar

Sundar’s Private Key

Sundar’s Public Key

Public Space / Internet

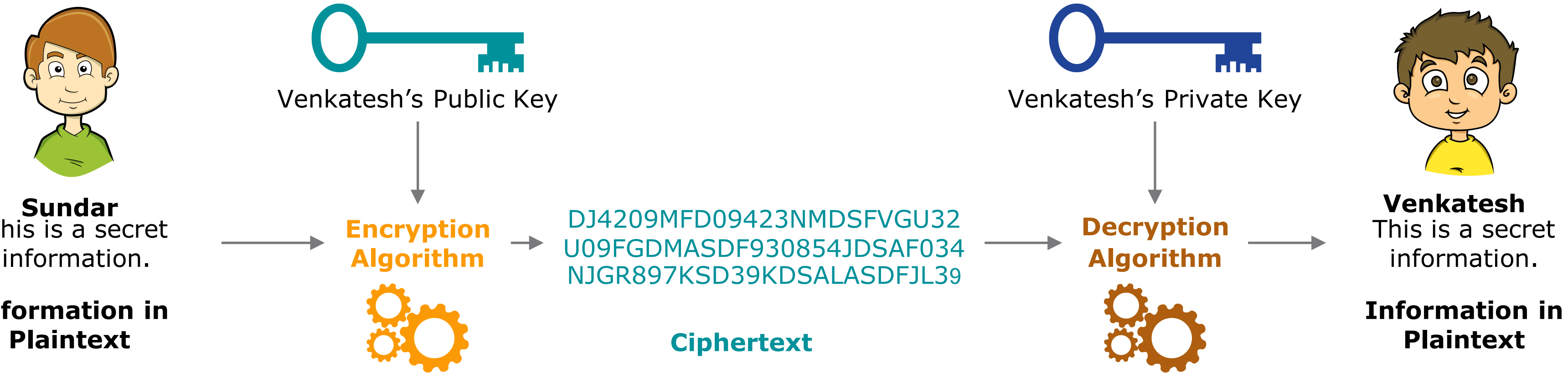
Venkatesh’s Private Key

Venkatesh’s Public Key

Venkatesh

Public Key Cryptography

- Let us assume Sundar wants to send a secret message to Venkatesh
- Sundar will encrypt the message with Venkatesh’s Public Key and send the ciphertext to Venkatesh
- As the key pair is mathematically linked, only Venkatesh’s private key can decrypt the message. No other key can decrypt this message. Venkatesh will decrypt the message using his private key to retrieve the original information
- As two keys are used for encryption/decryption process, it is called asymmetric key encryption. It is also known as Public Key cryptography as the public key is shared to ensure secure communication.



Sundar
This is a secret information.

Information in Plaintext

Venkatesh’s Public Key

Encryption Algorithm

DJ4209MFD09423NMDSFVGU32
U09FGDMASDF930854JDSAF034
NJGR897KSD39KDSALASDFJL39

Ciphertext

Venkatesh’s Private Key

Decryption Algorithm

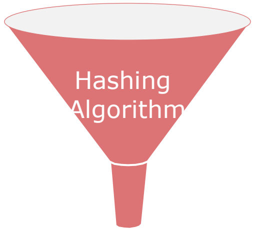
Venkatesh
This is a secret information.

Information in Plaintext

Hashing

- Hashing / Hash Function is a mathematical function used to convert any data of any arbitrary length to fixed length hexadecimal number. There are no keys required for this method to work.
- Irrespective of the length, type or nature of data, a hashing algorithm will always output a **fixed length hexadecimal number**
- This fixed length output is called Hash Value or Message Digest. Even a single change in character can result in a completely different hash value. Hence it is considered as the **digital thumbprint** of the data.
- From the hash value, you cannot retrieve original message that generated this hash value. Hence it is also called **one way encryption**

Input Data of varying length & type



Fixed Length Hash Value

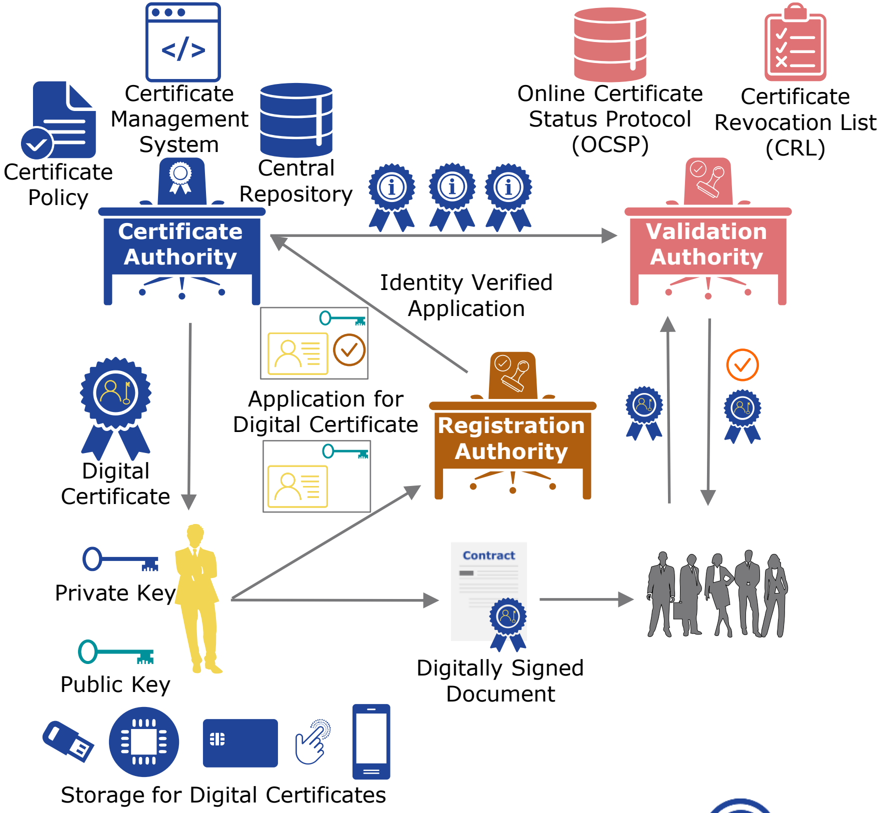
Algorithm	Output Length (Bits)	Output Length (Bytes)	Message	Hash Value	Hexadecimal Length (Binary bytes)
SHA256	256	32	Hello World	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e	64
SHA256	256	32	Hello World!	7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069	64
SHA256	256	32	Cryptography is awesome	2d601088ecb12661935f2d2c89e7fac71e314e83064ba1d6fdd9eb8ee5dffa98	64

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)

Introduction

- ▸PKI is a collection of hardware, software, policies, procedures, people and roles
- ▸It helps to create, manage, distribute, use, save, verify and revoke digital certificates and manages the lifecycle of the digital certificate
- ▸It helps in identifying the parties involved in a transaction and verifying the integrity of the information shared.
- ▸The purpose of PKI is to simplify the security of the online transactions like Email and internet banking
- ▸It is used in situations where password based authentication is not sufficient and requires a strong authentication mechanism to verify the identity of the parties involved in a transaction
- ▸PKI creates a **Digital Certificate**. It contains the link between the public key and the person/entity to whom the certificate was issued.

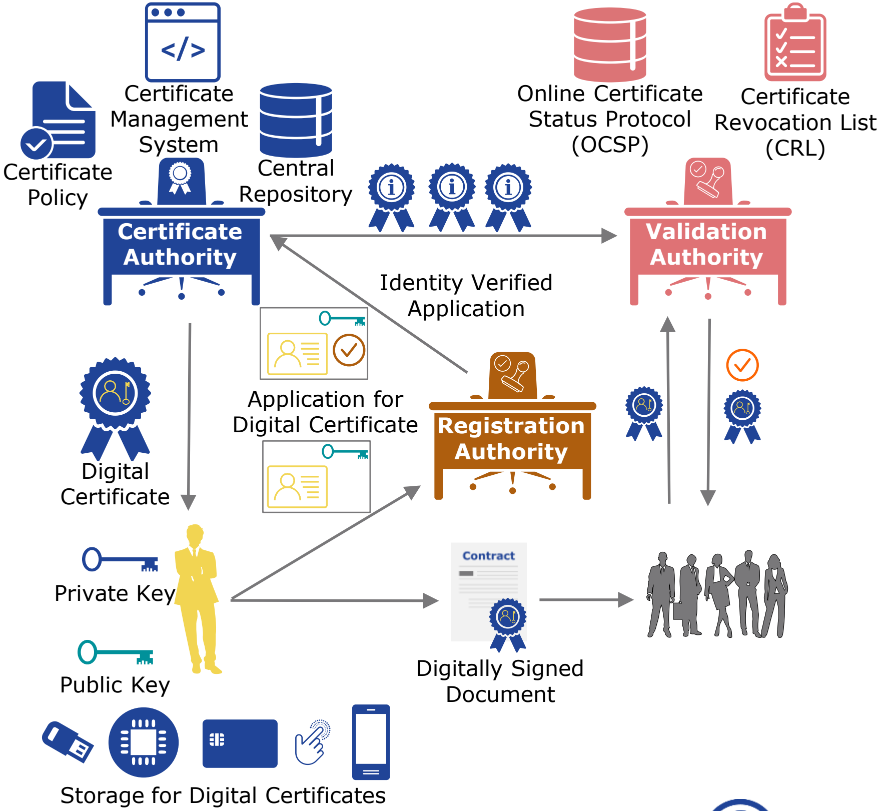


Certificate Policy
Certificate Management System
Central Repository
Online Certificate Status Protocol (OCSP)
Certificate Revocation List (CRL)
Certificate Authority
Validation Authority
Identity Verified Application
Application for Digital Certificate
Registration Authority
Digital Certificate
Private Key
Public Key
Contract
Digitally Signed Document
Storage for Digital Certificates

Public Key Infrastructure (PKI)

Components

- **Registration Authority**
  - It verifies the identities of the persons/organizations requesting digital certificate against known databases. It forwards the verified application to certificate authority
- **Certificate Authority**
  - It issues, stores and signs the digital certificates
- **Central Repository**
  - A secure storage space where keys are stored and indexed
- **Certificate Management System**
  - It enables access to digital certificates and issues them to the owner and manages the certificate lifecycle
- **Certificate Policy**
  - It contains the requirements and procedures for PKI. It enables 3rd party auditors to verify the integrity of the PKI
- **Validation Authority**
  - It verifies the validity of the digital certificates and ensures that the digital certificate has been issued by a trusted certifying authority


Certificate Management System
Certificate Policy
Central Repository
Online Certificate Status Protocol (OCSP)
Certificate Revocation List (CRL)
Certificate Authority
Validation Authority
Identity Verified Application
Application for Digital Certificate
Registration Authority
Digital Certificate
Private Key
Public Key
Contract
Digitally Signed Document
Storage for Digital Certificates

CYBER VATTAM

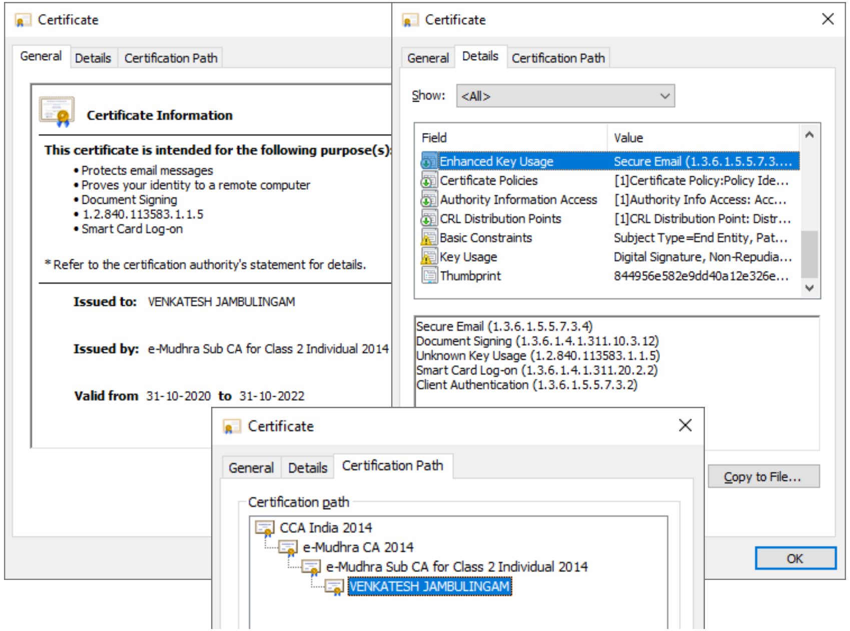
Digital Certificate

CYBER
VATTAM

Digital Certificate

Introduction

- ▸Digital certificate can be considered as an electronic identification
- ▸Digital certificates enables creation of a link between a public key and its owner
- ▸Digital certificates are issued by a certifying authority after strong verification of the identity of the requester
- ▸Owner of the digital certificate should keep it very secure
- ▸It is valid for a specific period of time
- ▸PKI manages the lifecycle of the digital certificates
- ▸They are also called X.509 certificates



Certificate Information

This certificate is intended for the following purpose(s):

- Protects email messages
- Proves your identity to a remote computer
- Document Signing
- 1.2.840.113583.1.1.5
- Smart Card Log-on

* Refer to the certification authority's statement for details.

Issued to: VENKATESH JAMBULINGAM

Issued by: e-Mudhra Sub CA for Class 2 Individual 2014

Valid from 31-10-2020 **to** 31-10-2022

Show: <All>

Field	Value
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3....
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...
Thumbprint	844956e582e9dd40a12e326e...

Secure Email (1.3.6.1.5.5.7.3.4)
Document Signing (1.3.6.1.4.1.311.10.3.12)
Unknown Key Usage (1.2.840.113583.1.1.5)
Smart Card Log-on (1.3.6.1.4.1.311.20.2.2)
Client Authentication (1.3.6.1.5.5.7.3.2)

Certification path

```
CCA India 2014
  e-Mudhra CA 2014
    e-Mudhra Sub CA for Class 2 Individual 2014
      VENKATESH JAMBULINGAM
```

Digital Certificate

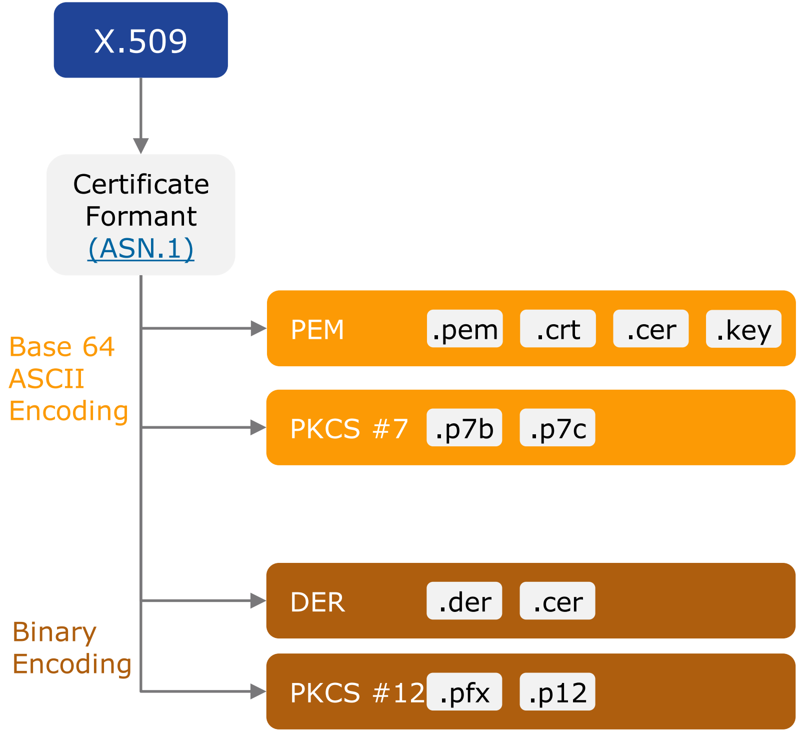
Formats

PEM format (Privacy Enhanced Mail)

- This is the most common format for X.509 certificates, certificate signing requests and cryptographic keys
- Most certifying authorities issue digital certificates that are encoded in base64 format.
- The certificates in this format have .pem, .crt, .cer, or .key as file extensions
- .pem format, the same file can store, end entity certificate, issuing authorities certificate and the private keys.
- End entity certificate and issuing authority certificate can be stored separately in .crt or .cer format.
- Private Keys are stored in .key format

PKCS #7 format (Public Key Cryptography Standard)

- Digital Certificate and certificate chain can only be stored in this format. Private keys cannot be stored.
- Digital certificates in this format are base64 encoded
- The certificates in this format have .p7b or .p7c as file extensions
- Usually, certifying authorities use this format to issue certificate chain



Digital Certificate

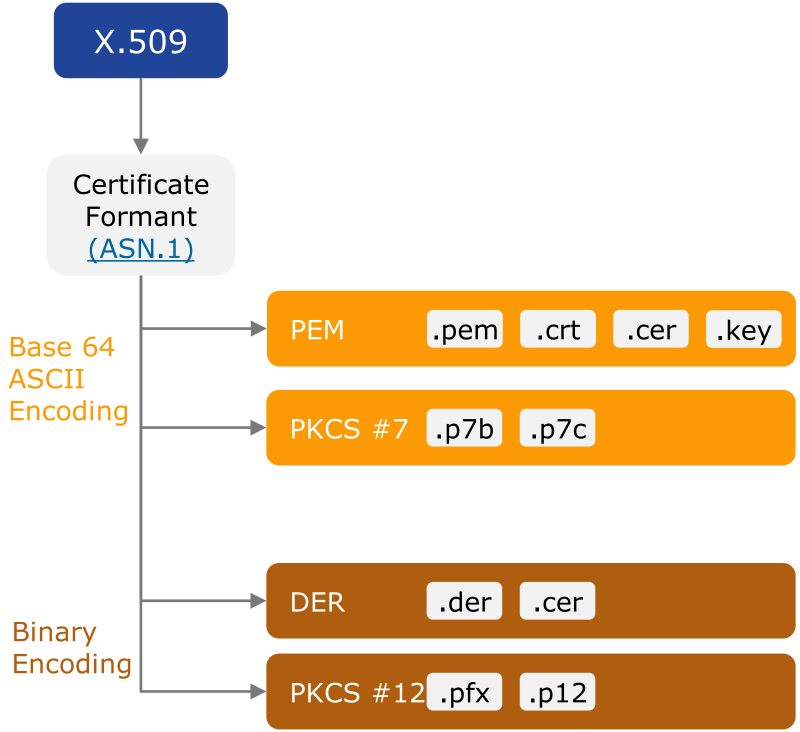
Formats

DER format (Distinguished Encoding Rule)

- This format is used for binary encoded X.509 certificates and private keys
- The certificates in this format have .der or .cer as file extensions
- Typically used in java environment.

PFX format (PKCS #12) (Personal Information Exchange)

- The certificates in this format are binary encoded. The term PFX & PKCS #12 are interchangeably used.
- In this format, end entity certificate, issue authority certificate and private keys can be saved as a single file with password protection
- The certificates in this format have .pfx or .p12 as file extensions
- This certificates are used predominantly in windows operating system.



Chain of Trust

Introduction

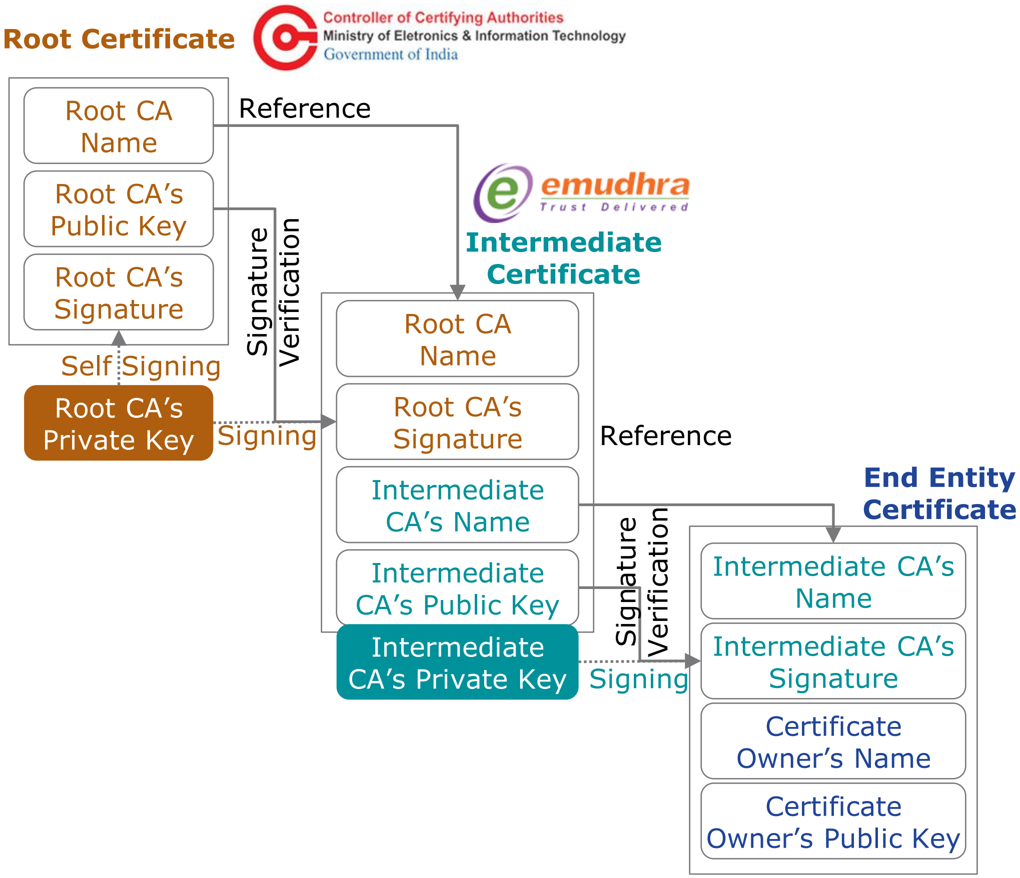
- Chain of Trust contains multiple components

- First, a **Trust Anchor**. It is also called Root Certifying Authority. They are the starting point or the source of trust in the chain

- Second, an **intermediate certifying authority** (CA). They can have sub certifying authority under intermediate CA

- Intermediate CA acts as a layer of protection between Root CA's and the end entity who receive the final certificates

- Finally, an **end entity certificate** issues to a person, server, organization or website



Root Certificate

Controller of Certifying Authorities
Ministry of Eletronics & Information Technology
Government of India

Root CA Name

Root CA's Public Key

Root CA's Signature

Self Signing

Root CA's Private Key

Signing

Signature Verification

Reference

emudhra Trust Delivered

Intermediate Certificate

Root CA Name

Root CA's Signature

Intermediate CA's Name

Intermediate CA's Public Key

Intermediate CA's Private Key

Signing

Signature Verification

Reference

End Entity Certificate

Intermediate CA's Name

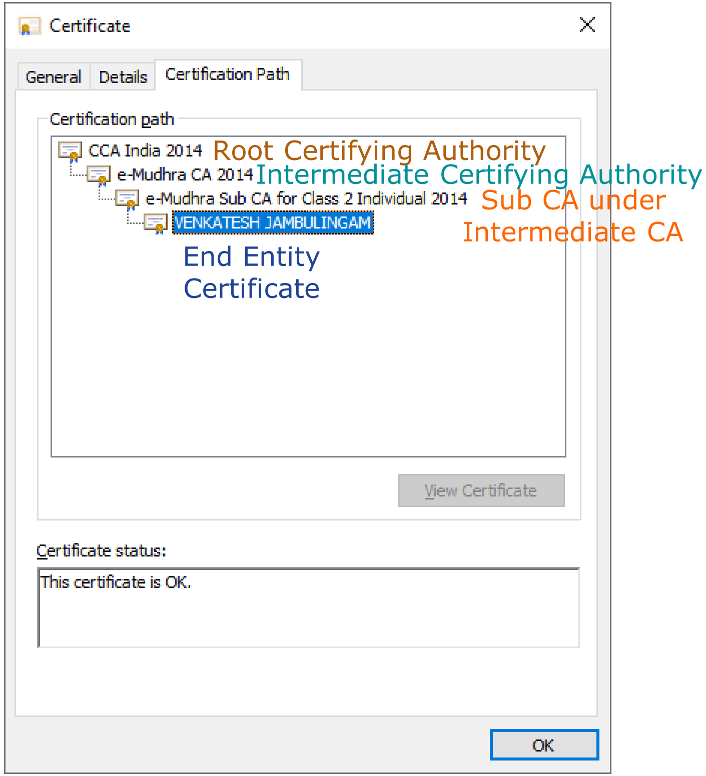
Intermediate CA's Signature

Certificate Owner's Name

Certificate Owner's Public Key

Chain of Trust

Example



Certificate

General | Details | Certification Path

Certification path

- CCA India 2014 Root Certifying Authority
  - e-Mudhra CA 2014 Intermediate Certifying Authority
    - e-Mudhra Sub CA for Class 2 Individual 2014 Sub CA under Intermediate CA
      - VENKATESH JAMBULINGAM

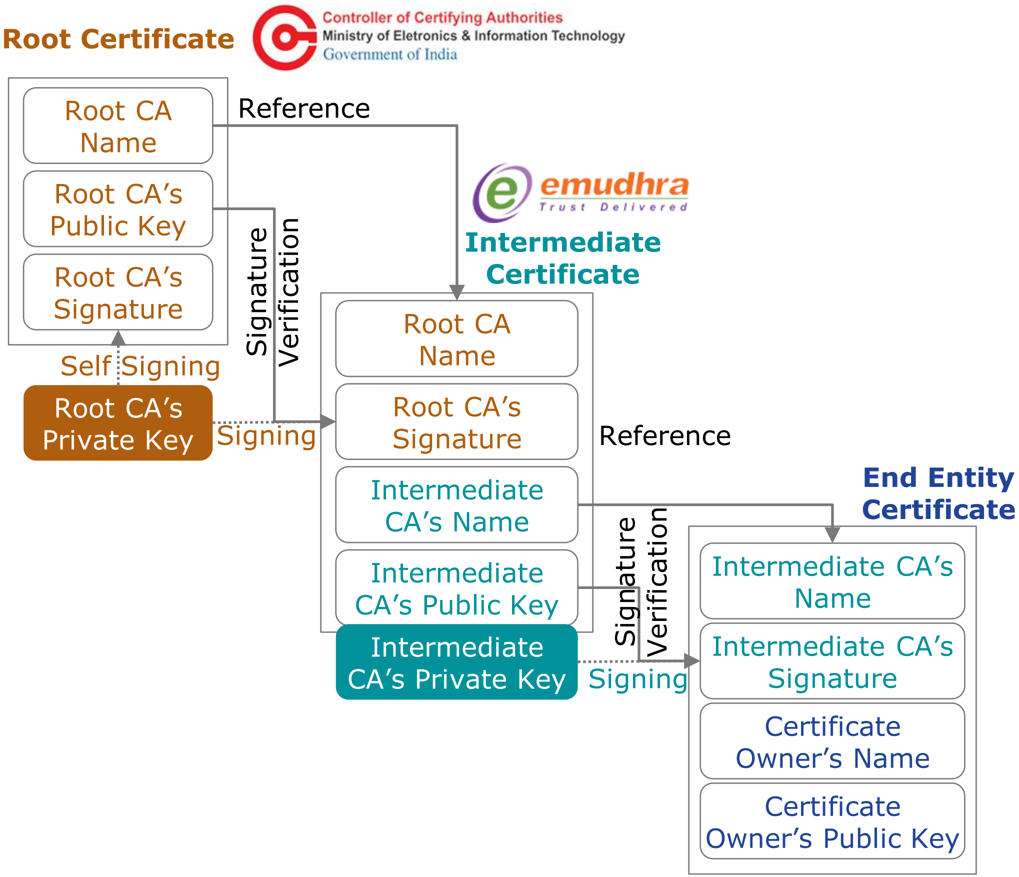
End Entity Certificate

View Certificate

Certificate status:

This certificate is OK.

OK



Root Certificate

Controller of Certifying Authorities
Ministry of Eletronics & Information Technology
Government of India

Root CA Name

Root CA's Public Key

Root CA's Signature

Self Signing

Root CA's Private Key

Reference

Signature Verification

Signing

emudhra
Trust Delivered

Intermediate Certificate

Root CA Name

Root CA's Signature

Intermediate CA's Name

Intermediate CA's Public Key

Intermediate CA's Private Key

Reference

Signature Verification

Signing

End Entity Certificate

Intermediate CA's Name

Intermediate CA's Signature

Certificate Owner's Name

Certificate Owner's Public Key

Chain of Trust

Verification Process

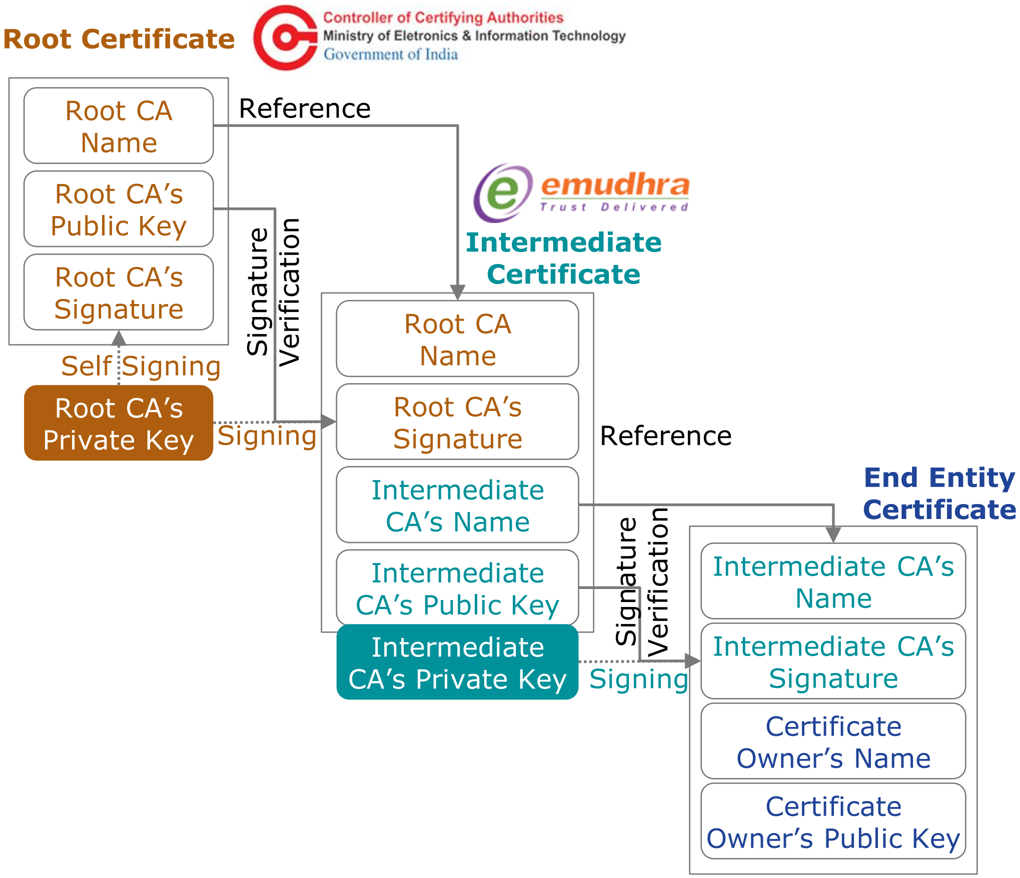
- A customer who wants to prove the identity provides the certificate. This certificate will usually contain the certificate chain until Root CA

- The entity verifying the certificate will use the issuing authority's public key to verify the certificate. This is part of the certificate chain in customer's certificate

- If the verifying entity trusts this certifying authority, the verification is completed successfully and the verification process will stop here.

- If not, this process is repeated for the issuing authority up in the certificate chain

- This process will continue until a trusted CA is found or till the Root CA



Trust Store

Certification Store

- ▸Trust store is a collection of Root CA’s that are trusted by default
- ▸This is maintained by organizations that creates operating system / browsers

Microsoft Trusted Root Certificate Program

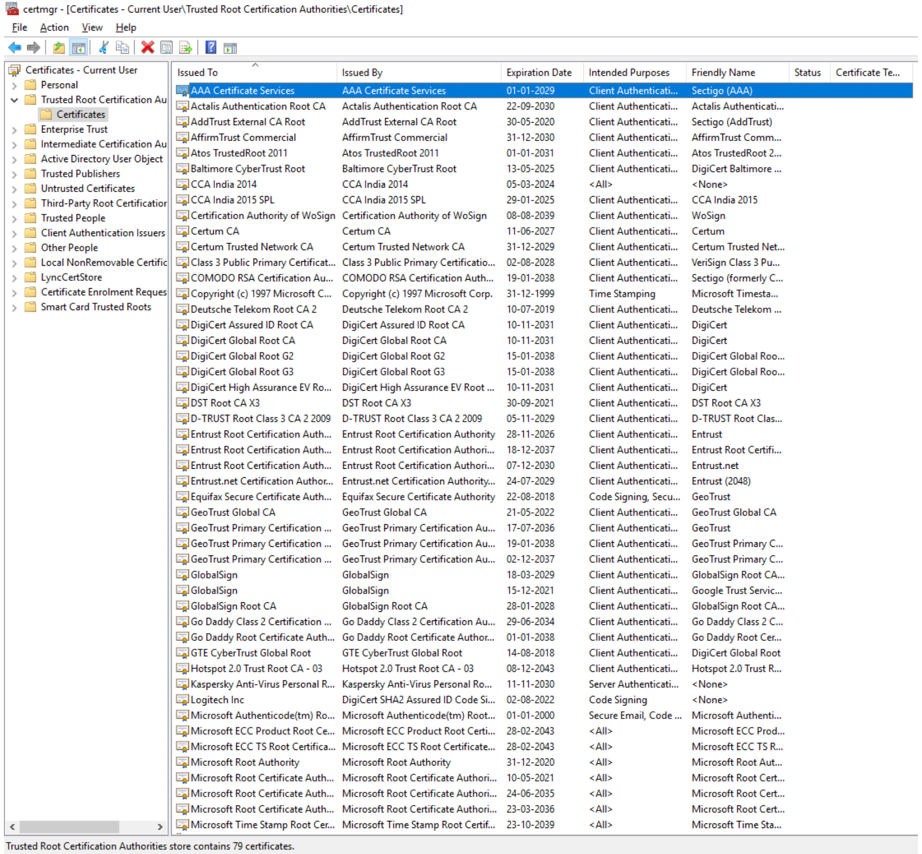
Apple Root Certificate Program

Google

Mozilla Network Security Services

Adobe Trusted Certificates List

Java Root Certificate Program



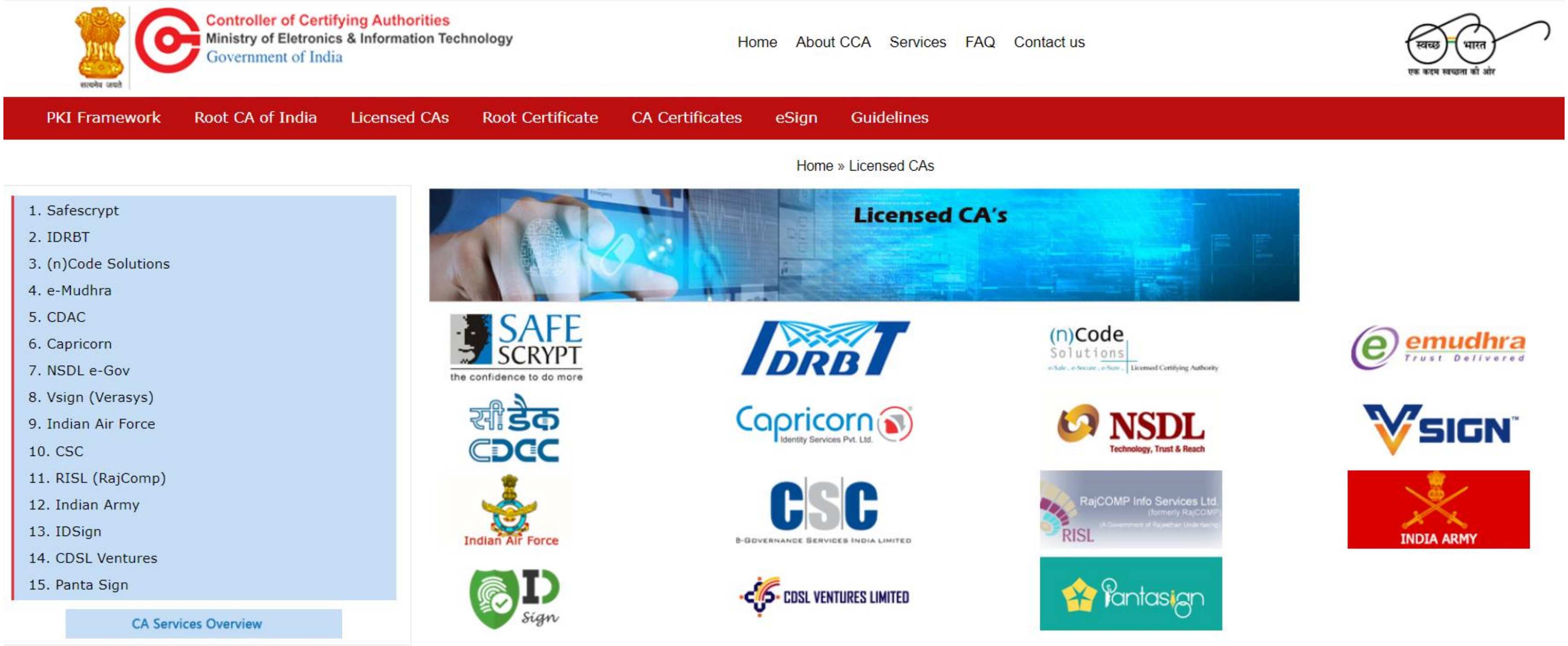
certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certific
LyncCertStore
Certificate Enrolment Reques
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
AAA Certificate Services	AAA Certificate Services	01-01-2029	Client Authenticati...	Sectigo (AAA)		
Actalis Authentication Root CA	Actalis Authentication Root CA	22-09-2030	Client Authenticati...	Actalis Authenticati...		
AddTrust External CA Root	AddTrust External CA Root	30-05-2020	Client Authenticati...	Sectigo (AddTrust)		
AffirmTrust Commercial	AffirmTrust Commercial	31-12-2030	Client Authenticati...	AffirmTrust Comm...		
Atos TrustedRoot 2011	Atos TrustedRoot 2011	01-01-2031	Client Authenticati...	Atos TrustedRoot 2...		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13-05-2025	Client Authenticati...	DigiCert Baltimore ...		
CCA India 2014	CCA India 2014	05-03-2024	<All>	<None>		
CCA India 2015 SPL	CCA India 2015 SPL	29-01-2025	Client Authenticati...	CCA India 2015		
Certification Authority of WoSign	Certification Authority of WoSign	08-08-2039	Client Authenticati...	WoSign		
Certum CA	Certum CA	11-06-2027	Client Authenticati...	Certum		
Certum Trusted Network CA	Certum Trusted Network CA	31-12-2029	Client Authenticati...	Certum Trusted Net...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02-08-2028	Client Authenticati...	VeriSign Class 3 Pu...		
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	19-01-2038	Client Authenticati...	Sectigo (formerly C...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31-12-1999	Time Stamping	Microsoft Timesta...		
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	10-07-2019	Client Authenticati...	Deutsche Telekom ...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10-11-2031	Client Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	10-11-2031	Client Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	15-01-2038	Client Authenticati...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	15-01-2038	Client Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10-11-2031	Client Authenticati...	DigiCert		
DST Root CA X3	DST Root CA X3	30-09-2021	Client Authenticati...	DST Root CA X3		
D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	05-11-2029	Client Authenticati...	D-TRUST Root Clas...		
Entrust Root Certification Auth...	Entrust Root Certification Authority	28-11-2026	Client Authenticati...	Entrust		
Entrust Root Certification Auth...	Entrust Root Certification Authori...	18-12-2037	Client Authenticati...	Entrust Root Certifi...		
Entrust Root Certification Auth...	Entrust Root Certification Authori...	07-12-2030	Client Authenticati...	Entrust.net		
Entrust.net Certification Author...	Entrust.net Certification Authority...	24-07-2029	Client Authenticati...	Entrust (2048)		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	22-08-2018	Code Signing, Secu...	GeoTrust		
GeoTrust Global CA	GeoTrust Global CA	21-05-2022	Client Authenticati...	GeoTrust Global CA		
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	17-07-2036	Client Authenticati...	GeoTrust		
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	19-01-2038	Client Authenticati...	GeoTrust Primary C...		
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	02-12-2037	Client Authenticati...	GeoTrust Primary C...		
GlobalSign	GlobalSign	18-03-2029	Client Authenticati...	GlobalSign Root CA...		
GlobalSign	GlobalSign	15-12-2021	Client Authenticati...	Google Trust Servic...		
GlobalSign Root CA	GlobalSign Root CA	28-01-2028	Client Authenticati...	GlobalSign Root CA...		
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29-06-2034	Client Authenticati...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	01-01-2038	Client Authenticati...	Go Daddy Root Cer...		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14-08-2018	Client Authenticati...	DigiCert Global Root		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08-12-2043	Client Authenticati...	Hotspot 2.0 Trust R...		
Kaspersky Anti-Virus Personal R...	Kaspersky Anti-Virus Personal Ro...	11-11-2030	Server Authenticati...	<None>		
Logitech Inc	DigiCert SHA2 Assured ID Code Si...	02-08-2022	Code Signing	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01-01-2000	Secure Email, Code ...	Microsoft Authenti...		
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	28-02-2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...	28-02-2043	<All>	Microsoft ECC TS R...		
Microsoft Root Authority	Microsoft Root Authority	31-12-2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10-05-2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	24-06-2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23-03-2036	<All>	Microsoft Root Cert...		
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	23-10-2039	<All>	Microsoft Time Sta...		

Trusted Root Certification Authorities store contains 79 certificates.

Licensed Certifying Authorities in India



1. Safescrypt
2. IDRBT
3. (n)Code Solutions
4. e-Mudhra
5. CDAC
6. Capricorn
7. NSDL e-Gov
8. Vsign (Verasys)
9. Indian Air Force
10. CSC
11. RISL (RajComp)
12. Indian Army
13. IDSign
14. CDSL Ventures
15. Panta Sign

Public Key Infrastructure (PKI)

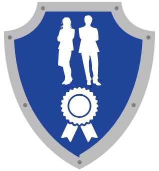
Capabilities

- Public Key Infrastructure provides Trust Services
- To put it simply, it helps you to trust the actions / output of a person, computer or an organization
- The purpose of the trust services are based on the following capabilities

Authentication	Creates a way to identify the users/devices	**We know whom we are communicating with**
Confidentiality	Ensures creation of a secure way to send/receive data	**We know the information is secure**
Integrity	Ensures the data/information was not modified during the transmission	**We know what we are talking about**
Non-Repudiation	Prevents an organization / individual’s ability to deny not sending/receiving electronic communications & transactions	**We cannot deny the information we sent**

Trust Services

Trust Services



Digital Signature Certificate

Transport Layer Security Certificate

Code Signing Certificate

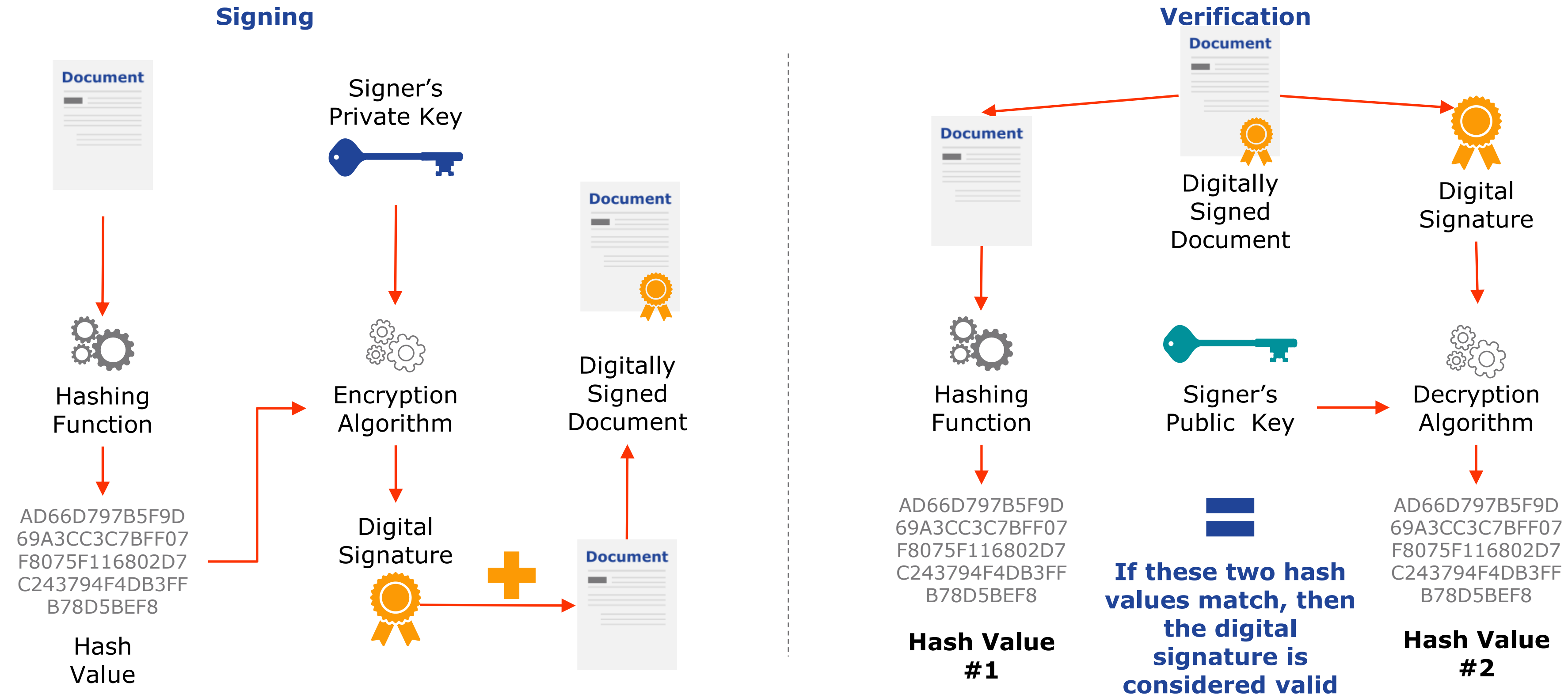
Time Stamping

Email Encryption Certificate

Digital Signature Certificate

Digital Signature

Signing/Verification Process



Signing

Document

Signer's Private Key

Hashing Function

Encryption Algorithm

Digitally Signed Document

AD66D797B5F9D
69A3CC3C7BFF07
F8075F116802D7
C243794F4DB3FF
B78D5BEF8

Hash Value

Digital Signature

Document

Verification

Document

Digitally Signed Document

Digital Signature

Document

Hashing Function

Signer's Public Key

Decryption Algorithm

AD66D797B5F9D
69A3CC3C7BFF07
F8075F116802D7
C243794F4DB3FF
B78D5BEF8

Hash Value #1

If these two hash values match, then the digital signature is considered valid

AD66D797B5F9D
69A3CC3C7BFF07
F8075F116802D7
C243794F4DB3FF
B78D5BEF8

Hash Value #2

Digital Signature

Certificate Classes

Certificate Class	Assurance Level	Applicability
Class 1 Certificate	▸ Class 1 certificates are issued for both business personnel and private individuals use. ▸ These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases	▸ This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise ▸ Risk / consequences are not considered to be of major significance.
Class 2 Certificate	▸ Class 2 certificates are issued for both business personnel and private individuals use. ▸ These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	▸ This level is relevant to environments where risks and consequences of data compromise are moderate. ▸ It includes transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial
Class 3 Certificate	▸ Class 3 certificates are issued to individuals as well as organizations. ▸ As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	▸ This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. ▸ This may include very high value transactions or high levels of fraud risk.

Certificate Based Authentication

Introduction

- Certificate based authentication is a method of authentication where a digital certificate is used to identify a user, device or machine.
- Authentication is usually done before giving access to any resource, network or application
- With respect to human identity, this method is used in combination with other traditional methods like passwords, Biometrics or OTP
- The unique capability of this authentication method is, unlike solutions that work only for humans (password, OTP or biometrics), this can be used as a single authentication solution for all type of identities.

Certificate based authentication works based on 4 questions. If any one of the questions fail, the authentication would also fail and the user will be denied access

1. Is the certificate issues by a trusted CA?
Is the intermediate CA and Root CA are trusted?

2. What is the expiry status of the certificate?
What is the issue & expiry date of the certificate

3. Is the certificate status revoked?
Is this certificate revoked for any reason?

4. Did the user provide proof of ownership?
Were the user able to prove having private keys associated with this certificate?

Employees & Contractors

Programs & Applications

APIs/Services

Desktops, Laptops,
Printers, Scanners

Servers & Network Devices

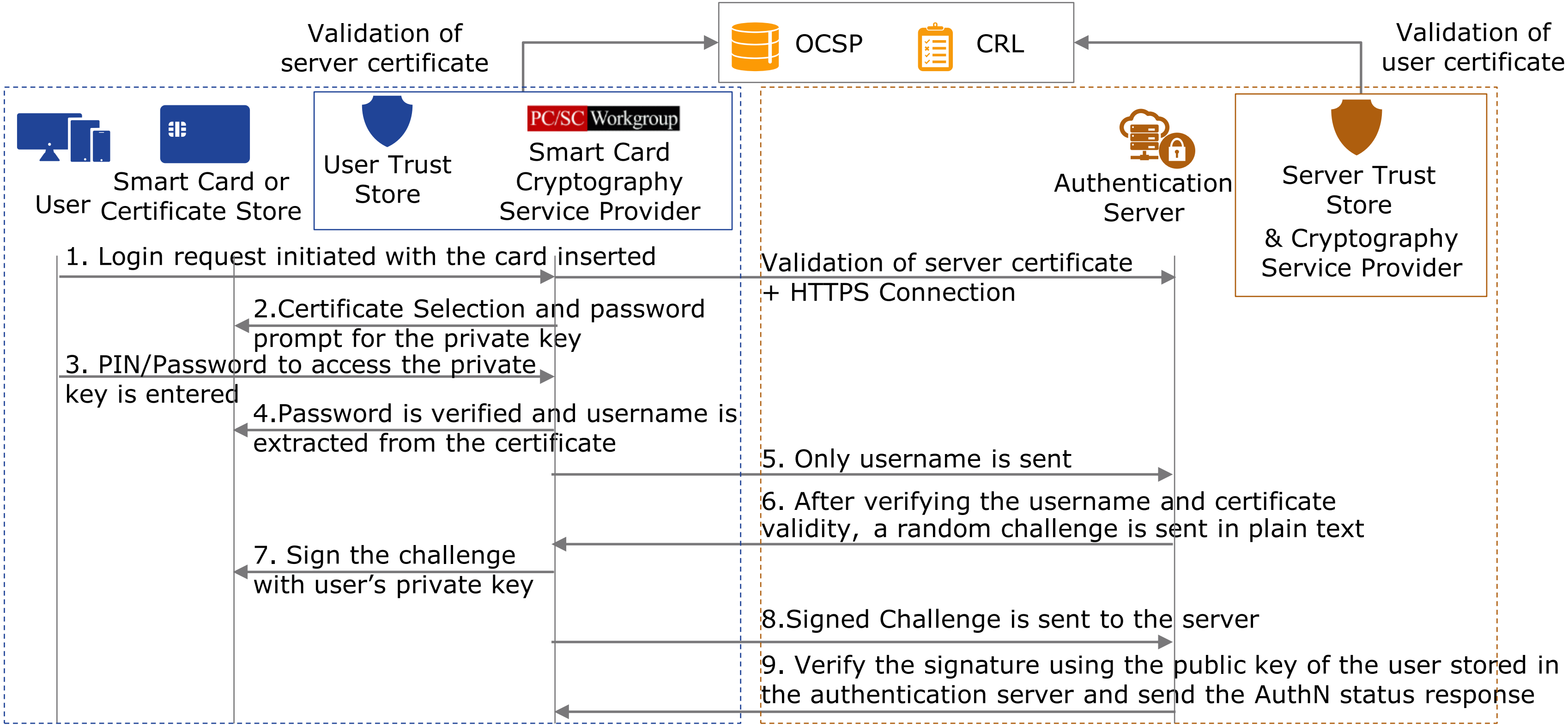
Consumer

Smart Car

Smart Devices

Certificate Based Authentication

Processes involved in request/response



Validation of server certificate

OCSP

CRL

Validation of user certificate

User

Smart Card or Certificate Store

User Trust Store

PC/SC Workgroup

Smart Card Cryptography Service Provider

Authentication Server

Server Trust Store & Cryptography Service Provider

1. Login request initiated with the card inserted

Validation of server certificate + HTTPS Connection

2.Certificate Selection and password prompt for the private key

3. PIN/Password to access the private key is entered

4.Password is verified and username is extracted from the certificate

5. Only username is sent

6. After verifying the username and certificate validity, a random challenge is sent in plain text

7. Sign the challenge with user’s private key

8.Signed Challenge is sent to the server

9. Verify the signature using the public key of the user stored in the authentication server and send the AuthN status response

Smart Card

- Smart card logon & authentication is a type of certificate based authentication
- Smart card is a small computer without screen or a keyboard. It integrates a microprocessor, memory and some applications
- Smard cards contain an integrated circuit and are compliant with ISO/IEC 7810 ID-1, 7816 & 14443
- Smart cards have the ability to perform cryptographic processing like encryption, decryption, digital signature, hashing and key pair creation within the card itself
- Smart cards offer a secure storage space for storing highly sensitive information like private keys, digital certificates, account numbers, passwords
- Private keys are always stored securely
- Only public key and digital certificates are exposed

Smart Cards Logon & Authentication Use Cases

National Identity

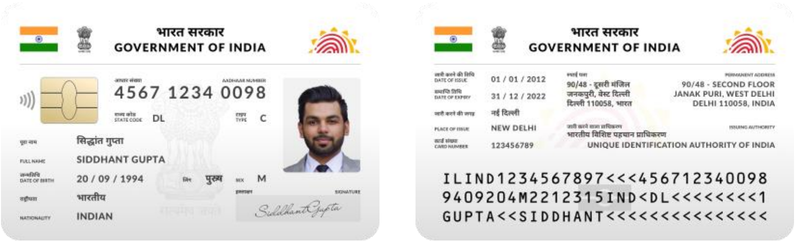
- National Identification Card
- E-Passport
- Driving License
- Voter ID Card
- Health Insurance Card
- Digital Signature

Organization/University Identity

- Secure login & authentication (computer, application, email)
- Storage of digital certificates, credentials, and passwords
- Encryption of sensitive data
- Secure storage of Biometric Data
- Building, conference room and parking facility access
- Attendance and Time Logging

Commercial Application

- Banking (Debit/Credit Cards) and Payment Services
- Secure B2B & B2C ecommerce transactions
- Loyalty Management & Discount Services
- Travel Ticketing / Event Ticketing
- Parking Fees & Toll Collection
- Secure Mobile SIM & authentication



भारत सरकार
GOVERNMENT OF INDIA

AADHAAR NUMBER 4567 1234 0098

STATE CODE DL

TYPE C

सिद्धांत गुप्ता

FULL NAME SIDDHANT GUPTA

DATE OF BIRTH 20 / 09 / 1994

पुरुष

SEX M

SIGNATURE Siddhant Gupta

भारतीय

NATIONALITY INDIAN

भारत सरकार
GOVERNMENT OF INDIA

DATE OF ISSUE 01 / 01 / 2012

DATE OF EXPIRY 31 / 12 / 2022

नई दिल्ली

PLACE OF ISSUE NEW DELHI

CARD NUMBER 123456789

90/48 - दूसरी मंजिल
जनकपुरी, वेस्ट दिल्ली
दिल्ली 110058, भारत

PERMANENT ADDRESS
90/48 - SECOND FLOOR
JANAK PURI, WEST DELHI
DELHI 110058, INDIA

भारतीय विशिष्ट पहचान प्राधिकरण

ISSUING AUTHORITY
UNIQUE IDENTIFICATION AUTHORITY OF INDIA

```
ILIND1234567897<<<456712340098
9409204M2212315IND<DL<<<<<<<<<1
GUPTA<<SIDDHANT<<<<<<<<<<<<<<<<
```

Sample Aadhaar National ID Card
Image Created by: Mr. Siddhant Gupta

Transport Layer Security Certificates

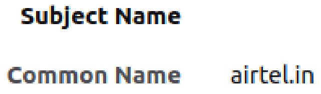
CYBER VATTAM

TLS Certificate Types

Based on Validation Method

Domain validation

- Provides minimum level of assurance. These certificates are easy to obtain and verify only the ownership of a domain name
- The websites with this type of certificates are displayed with a secure pad lock. It will not contain the domain's owner name or the organizations name
- While it is secure, there is no way for the users to verify if the website actually belongs to the business that they are interested in

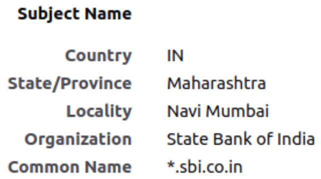


Subject Name

Common Name	airtel.in

Organization Validation

- This is the most common level of assurance used
- The websites with this type of certificates are displayed with a secure pad lock and business / organization's name
- As these certificates offer high level of assurance, they are issued by CA's after a strong vetting/verification process
- This type of certificate is used by businesses dealing with sensitive customer data

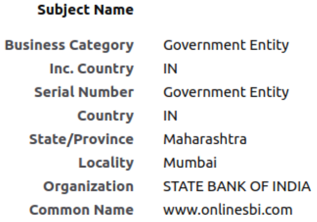


Subject Name

Country	IN
State/Province	Maharashtra
Locality	Navi Mumbai
Organization	State Bank of India
Common Name	*.sbi.co.in

Extended Validation

- Provides highest level of assurance and are very difficult to obtain
- Organizations requesting this type of certificate are subject to extreme verification process. CA's check for the registration, default location/operations of the company and the industry in which they operate
- These certificates include the organization name, country code, type of business and is displayed with green pad lock



Subject Name

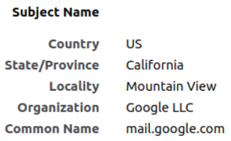
Business Category	Government Entity
Inc. Country	IN
Serial Number	Government Entity
Country	IN
State/Province	Maharashtra
Locality	Mumbai
Organization	STATE BANK OF INDIA
Common Name	www.onlinesbi.com

TLS Certificate Types

Based on Domain Type

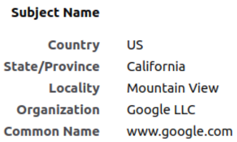
Single Domain Certificates

- Protects the single domain mentioned in the certificate
- Can be issued to a domain or a subdomain



Subject Name

Country	US
State/Province	California
Locality	Mountain View
Organization	Google LLC
Common Name	mail.google.com

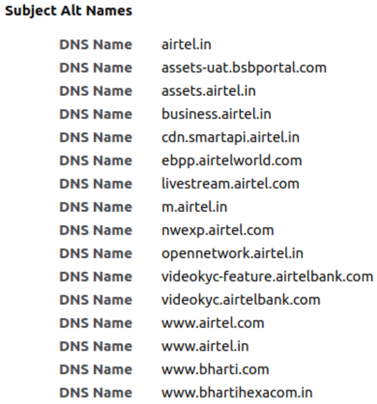


Subject Name

Country	US
State/Province	California
Locality	Mountain View
Organization	Google LLC
Common Name	www.google.com

Multi-Domain Certificates

- Also known as Subject Alternative Name Certificates / Unified Communications Certificates
- Certain Server environments won't allow installation of multiple certificates. This type of certificate is a simple solution to solve such problems.
- Can be obtained for all validation types
- Upto 250 domains could be added in a single certificate
- Before the certificate could be activated, domain validation for all domains mentioned in the certificate should have been successful



Subject Alt Names

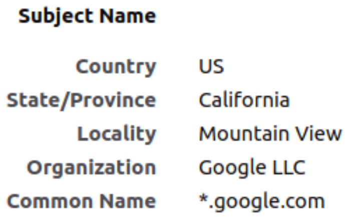
DNS Name	airtel.in
DNS Name	assets-uat.bsbportal.com
DNS Name	assets.airtel.in
DNS Name	business.airtel.in
DNS Name	cdn.smartapi.airtel.in
DNS Name	ebpp.airtelworld.com
DNS Name	livestream.airtel.com
DNS Name	m.airtel.in
DNS Name	nwexp.airtel.com
DNS Name	opennetwork.airtel.in
DNS Name	videokyc-feature.airtelbank.com
DNS Name	videokyc.airtelbank.com
DNS Name	www.airtel.com
DNS Name	www.airtel.in
DNS Name	www.bharti.com
DNS Name	www.bhartihexacom.in

TLS Certificate Types

Based on Domain Type

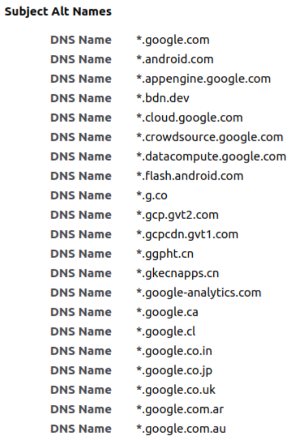
Wildcard Certificates

- This type of certificate is very popular among organizations having multiple sub domains ending in single domain name.
- While issuing the certificate, asterik (*) is used along with the main domain name in the format "*.domainname.com"
- "*" means it is a wildcard. This certificate will protect all domains & sub domains ending with "domainname.com"
- This type of certificate is issued by organization validation & extended validation types only



Subject Name

Country	US
State/Province	California
Locality	Mountain View
Organization	Google LLC
Common Name	*.google.com



Subject Alt Names

DNS Name	*.google.com
DNS Name	*.android.com
DNS Name	*.appengine.google.com
DNS Name	*.bdn.dev
DNS Name	*.cloud.google.com
DNS Name	*.crowdsource.google.com
DNS Name	*.datacompute.google.com
DNS Name	*.flash.android.com
DNS Name	*.g.co
DNS Name	*.gcp.gvt2.com
DNS Name	*.gcpcdn.gvt1.com
DNS Name	*.ggpht.cn
DNS Name	*.gkecnapps.cn
DNS Name	*.google-analytics.com
DNS Name	*.google.ca
DNS Name	*.google.cl
DNS Name	*.google.co.in
DNS Name	*.google.co.jp
DNS Name	*.google.co.uk
DNS Name	*.google.com.ar
DNS Name	*.google.com.au

Multi-Domain Wildcard Certificates

- This type of certificate is used by organizations with complex network infrastructure
- Depending on the issuer, the certificate can protect upto 250 domains
- Common Name should be a full qualified domain name (www.domainname.com)
- Subject Alternative names can be FQDN (www1.domainname.com) or wildcard domain (*.domainname.com) or a mixture of both

Code Signing Certificates

Code Signing

Introduction

- Code signing is the process of digitally signing the software (executables, binaries, scripts, source code) to identify the publisher of the software
- Code signing assures that the software has not been modified or tampered with after signing the software. Hash Values are used for this purpose.
- The security of this system of identifying & authenticating the publisher depends on the security of the private keys that was used for signing
- The integrity of this entire system is dependent on software publishers securing their private keys with high confidentiality
- It is recommended to store the private keys in secure, tamper resistant cryptographic hardware devices. These devices are called Hardware Security Module(HSM)

Standard Code Signing Certificates

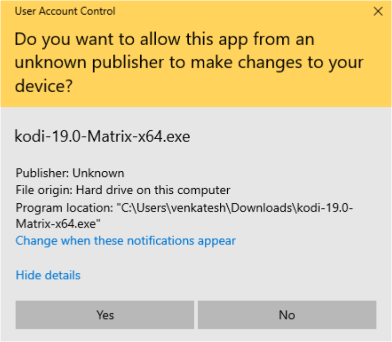
Extended Validated Code Signing Certificates

Code Signing

Certificate Types

Standard Code Signing Certificates

- ▶For software signed with this type of certificate, the Microsoft SmartScreen will keep displaying alerts until the software publisher builds a reputation by having a large number of downloads and with minimal error report for the software.
- ▶Does not provide the assurance to trust the software itself. It verifies that the software was signed using a specific private key belonging to the publisher using PKI
- ▶The public key or the digital certificate used to verify the signature should have been issued by CA connected to a trusted Root CA. This can be verified from the chain of trust



User Account Control

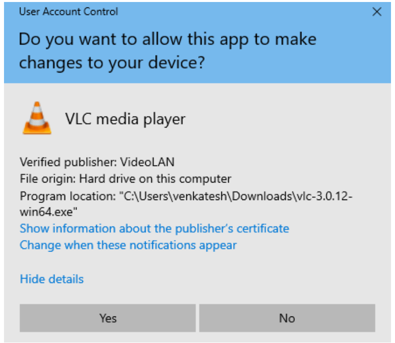
Do you want to allow this app from an unknown publisher to make changes to your device?

kodi-19.0-Matrix-x64.exe

Publisher: Unknown
File origin: Hard drive on this computer
Program location: "C:\Users\venkatesh\Downloads\kodi-19.0-Matrix-x64.exe"

Extended Validated Code Signing Certificates

- ▶EV code signing certificates are issued after stringent verification of the software publisher
- ▶By signing the software with EV code signing certificate, a software publisher with no prior reputation in Microsoft SmartScreen can immediately build reputation.
- ▶Does not provide the assurance to trust the software itself. It verifies that the software was signed using a specific private key belonging to the publisher using PKI



User Account Control

Do you want to allow this app to make changes to your device?

VLC media player

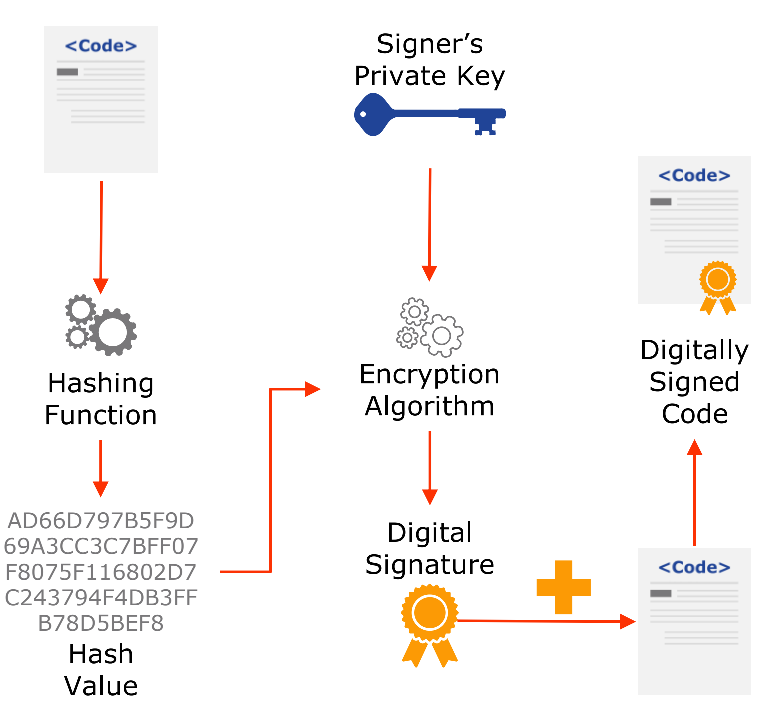
Verified publisher: VideoLAN
File origin: Hard drive on this computer
Program location: "C:\Users\venkatesh\Downloads\vlc-3.0.12-win64.exe"

×
Show information about the publisher's certificate
Change when these notifications appear
Hide details
Yes
No

Code Signing

Process for Signing/Verification

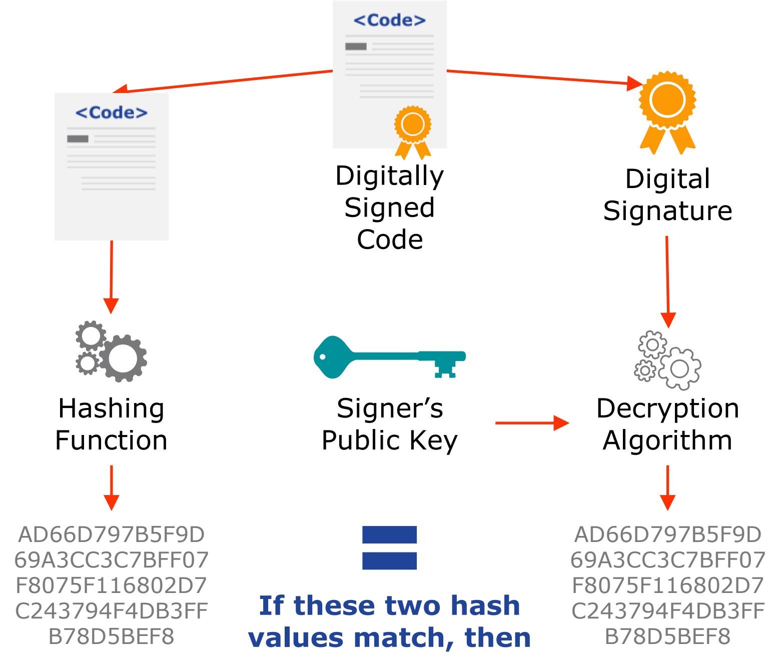
Signing



AD66D797B5F9D
69A3CC3C7BFF07
F8075F116802D7
C243794F4DB3FF
B78D5BEF8

Hash Value

Verification



AD66D797B5F9D
69A3CC3C7BFF07
F8075F116802D7
C243794F4DB3FF
B78D5BEF8

Hash Value #1

AD66D797B5F9D
69A3CC3C7BFF07
F8075F116802D7
C243794F4DB3FF
B78D5BEF8

Hash Value #2

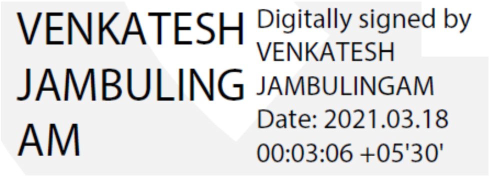
If these two hash values match, then the digital signature is considered valid

Time Stamping

Time Stamping

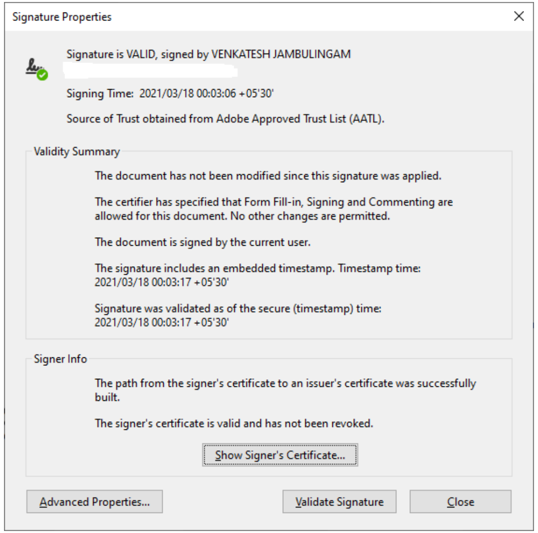
Introduction

- Time stamping is the process of secure recording the creation/modification time of a document. The output of this process is called a Trusted Time Stamp
- Here secure means ensuring that after the document is timestamped, the document cannot be modified including the owner of the document
- Adding a trusted time stamp with digital signature or code signing increases the integrity of the system and provides a secure record of date & time of the transaction
- A Trusted Time Stamping authority is used to securely document the date & time of the transaction, digital signature or Code Signing.
- A digital signature without the timestamp will expire when the underlying digital certificate used to sign expires. If timestamped, the signature will be valid even after the expiry of the underlying certificate.
- Entities receiving a timestamped document / software can verify when it was signed and it has not been modified since signing the document.
- You can timestamp a document separately or while digitally signing the document.



VENKATESH JAMBULING AM

Digitally signed by VENKATESH JAMBULINGAM
Date: 2021.03.18
00:03:06 +05'30'



Signature Properties

Signature is VALID, signed by VENKATESH JAMBULINGAM

Signing Time: 2021/03/18 00:03:06 +05'30'

Source of Trust obtained from Adobe Approved Trust List (AATL).

Validity Summary

The document has not been modified since this signature was applied.

The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.

The document is signed by the current user.

The signature includes an embedded timestamp. Timestamp time: 2021/03/18 00:03:17 +05'30'

Signature was validated as of the secure (timestamp) time: 2021/03/18 00:03:17 +05'30'

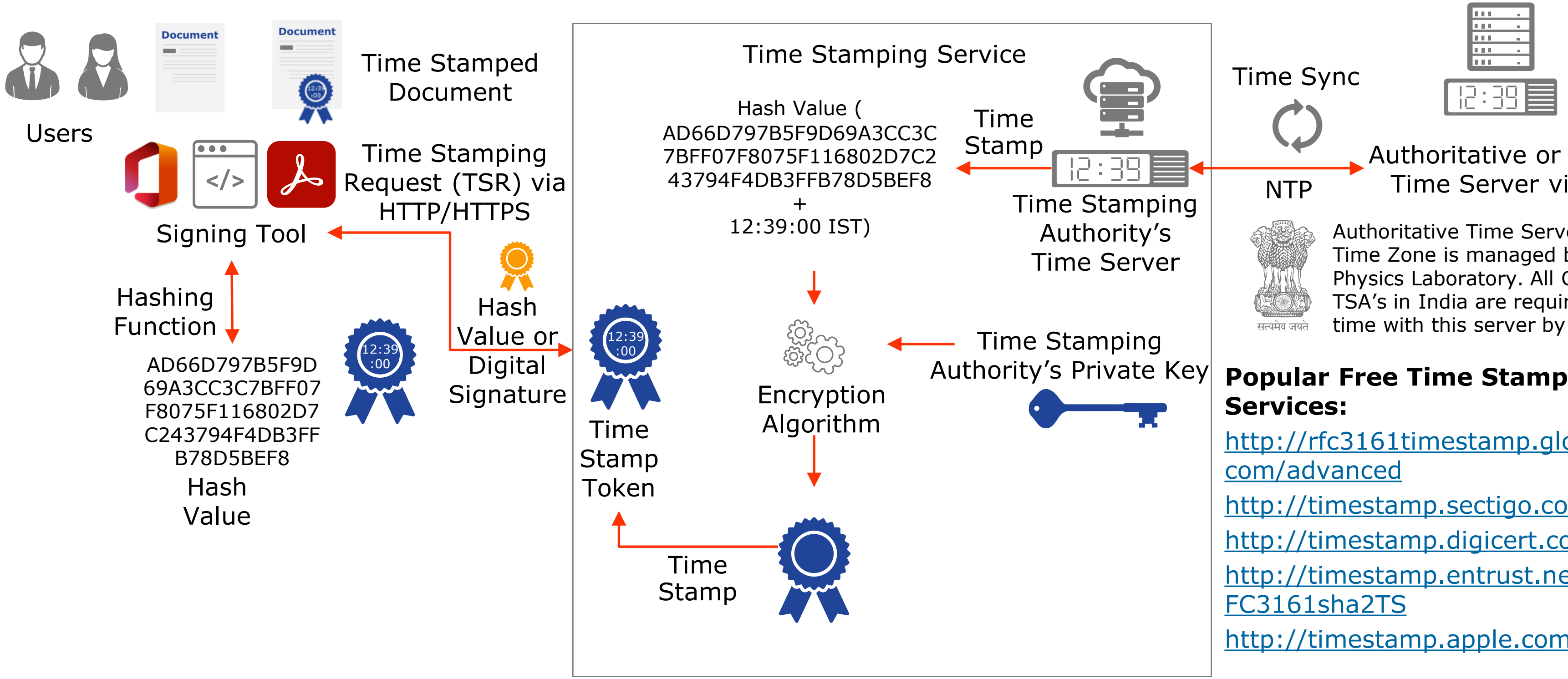
Signer Info

The path from the signer's certificate to an issuer's certificate was successfully built.

The signer's certificate is valid and has not been revoked.

Time Stamping

Process



Users
Document
Document
Time Stamped Document
Time Stamping Request (TSR) via HTTP/HTTPS
Signing Tool
Hashing Function
AD66D797B5F9D69A3CC3C7BFF07F8075F116802D7C243794F4DB3FFB78D5BEF8
Hash Value
12:39 :00
Hash Value or Digital Signature
Time Stamping Service
Hash Value (AD66D797B5F9D69A3CC3C7BFF07F8075F116802D7C243794F4DB3FFB78D5BEF8 + 12:39:00 IST)
Time Stamp
12:39
Time Stamping Authority's Time Server
Encryption Algorithm
Time Stamping Authority's Private Key
12:39 :00
Time Stamp Token
Time Stamp
Time Sync
NTP
12:39
Authoritative or Trusted Time Server via NTP

Authoritative Time Server for IST Time Zone is managed by National Physics Laboratory. All CA's & TSA's in India are required to sync time with this server by CCA

Popular Free Time Stamping Services:

http://rfc3161timestamp.globalsign.com/advanced

http://timestamp.sectigo.com

http://timestamp.digicert.com

http://timestamp.entrust.net/TSS/RFC3161sha2TS

http://timestamp.apple.com/ts01

Email Encryption Certificates

CYBER VATTAM

Email Encryption Certificates

S/MIME (Secure/Multipurpose Internet Mail Extensions) Certificates

Email Validation

For this type of certificate, only email address and the website domains are validated.

Individual Validation

For this type of certificate, identity of each individual is validated.

This certificate will contain the email address and the owner name as well

To obtain this type of certificate, a government issued id for the individual is needed and the email address should also be validated.

Organization Validation

The purpose of this validation is to verify the existence and operations of a given specific organization before issuing the certificate.

Getting OV S/MIME certificate is very similar to getting OV TLS certificate

Thank you

CYBER VATTAM

About me

Venkatesh Jambulingam
Cloud Security Expert

Email:
cybervattam@gmail.com
cybervattam@outlook.com

Follow me on