# Reference links

<https://medium.com/@skshukla.0336/mtls-everything-you-need-to-know-e03804b30804>

Basic concepts

### Terminologies

PKI- means public key infrastructure

Ciphered text – means unreadable text

Cipher – means algorithm which is used to transform plain text to ciphered (encrypted) text

CSR – cert signing request

Entity – here entity means server or client who wants the certificate

Important points

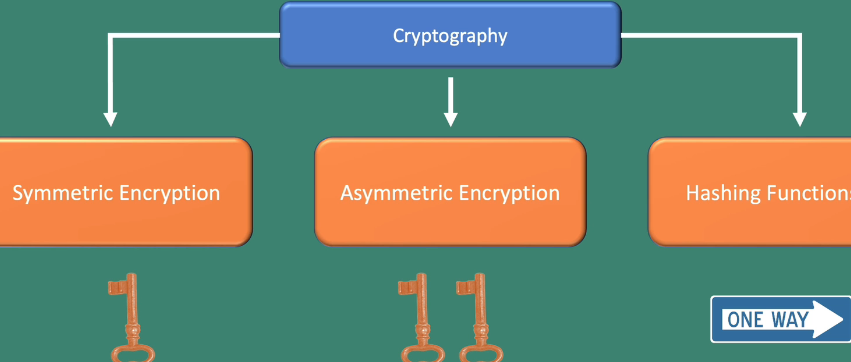
* In asymmetric encryption- Public key is used to encrypt the data, private key is used to decrypt the data
* Certificates contains the public keys (hence certificate is mandatory for authentication)

Cryptography

Method of securing data such that is trusted and viewable only by authorized parties

Military people when they send messages they will use cryptography

Cryptograhpy is a art of secure communication -ex:- encrypting, hashing



**Cryptographic keys storage**

* These keys can be stored in PKI certificate
* Or those can be stored on smart card/common access card (smart card= our daily ID card)
* These keys can be stored in a password protected file also
* Token device – hard MFA token or smart android apps

Encoding Vs. encryption vs. hashing

Encoding:- it’s a basic data representation to enable info **which doesn’t involve keeping secrets**

**In encoding security is not the primary concern**

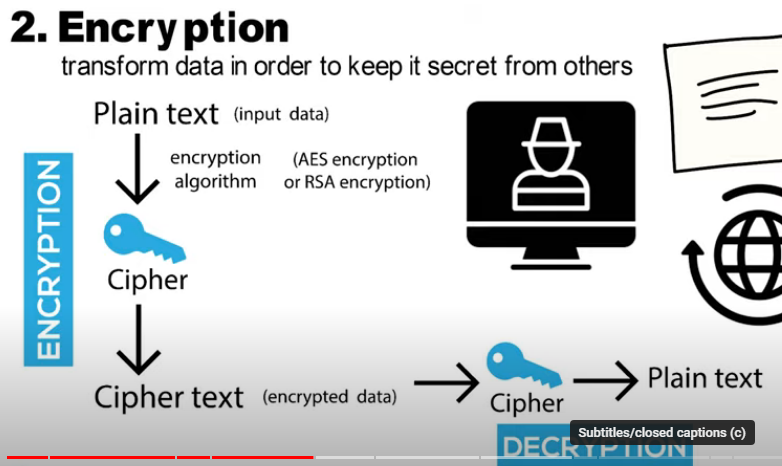
**Encrypting(like cryptography): -** here data can’t be consumed by anyone other than intended recipients

Goals of encryption- confidentialy (only intended people should understand)

It is to transform the data in order **to keep** it secret from others

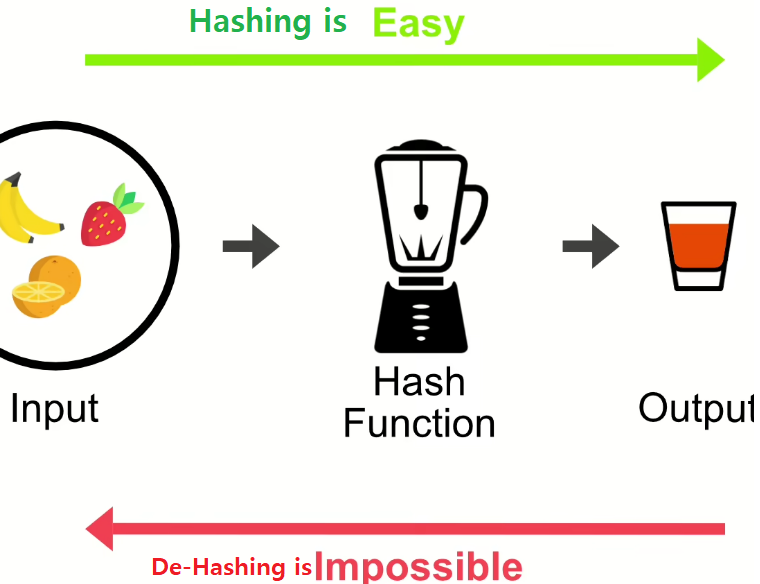
**Encryption algorithm will use a key To encrypt and decrypt** and the encrypted data is called cipher text

Generally everyone can see the data which is in transmission so we should **encrypt the data before transmitting over wire/ wirelessly**



## Hashing and De hashing

Hashing is a one way cryptography and it is irreversible



Once u hash u cant reverse that, ex:- Hash 256, once passwords are hashed u can’t un hash that

Passwords hashed can’t be de-hashed/reversed/decrypted

### Symmetric vs. asymmetric encryption

Symmetric encryption:- With same key we will encrypt and decrypt (in real time both sender and receiver should use same key for encryption and decryp)

Symmetric encryption Algorithms are – AES (Advanced encryption algorithm), DES, 3DES, Blowfish, RC4, ChaCha20

Asymmetric encryption:

This is mostly used in real time

|  |  |
| --- | --- |
| - | * we will encrypt with public key before sending (public key cant decrypt the encrytped one) * we can only decrypt with private key after receiving   Everybody will have access to public key & only intended user will have private key  Asymmetric encryption algorithms are 🡪 RSA (Max key size = 4096 Bits) |

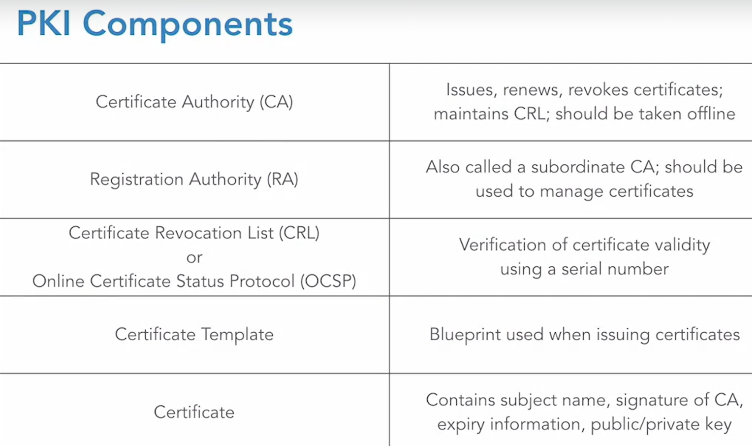
SSL TLS network security

|  |  |
| --- | --- |
| and this symmetric key will be encrypted and send server decrypts with its own private key and it will get the symmetric key |  |

AES 128 bit

AES(Advanced encryption standard) 128 bit means =block size is 128, algorithm will encrypt into 128 bits (1 block) sets

# **Pki components**



Pki = public key infrastructure = collection of digital security certificates

Certificate will contain the public keys , private keys can also be stored in separate file

**Certificate Request**

A Client or Server in order to acquire a valid certificate first need to create a **CSR** (Certificate Request) file which they need to submit to the **Certificate Authority** which can sign and issue a valid certificate

## 2.2 Certificate Authority (CA)

|  |  |
| --- | --- |
| Simple, authority means power, here certificate Authority means the power to issue the certificate,  So certificate authority is the one who will Issue the Certificates to the Entities (Servers, Clients, Websites)  CA sometime may include a physical visit by them to the business premises and then issue the public certificate  And certificate authority is the one who can confirm whether it’s the same Website which it claims it is.  A Certificate Authority is a trusted organization who confirm the authenticity of a website (Server). Their primarily responsibilities are, |  |
| CA can even Issues,renew,revoke the certificate and it maintains CRL (certificate revocation list )  Registration authority is the one who is a subordinate to CA – he also can do whatever CA can do  CA will issue cert only for limited period of time – after that either they have to renew/ they should revoke old cert and issue a new cert  CA will revoke the old cert based on the serial num of old cert  Few of the Certificate Authorities are [VeriSign](https://www.verisign.com/), [DigiCert](https://www.digicert.com/) |  |

.

## 2.3 Certificate

|  |  |
| --- | --- |
| Why cert- these cert are used to secure network traffic /encrypting the data transfer  Cert can be issued to users, smartphoness, apps,  Since CA issues the certificates the CA can verify whether it’s valid certificate or not or whether it is signed by them or not  This cer is same like an id card that contains (to whom this id card is issued), who issued id card, till when its valid, employee num  Every cert contains this infor🡪 cert serial num,subject name (to whom this cert is issued-web site url for whom this cert is issued), sign of issuing CA(who issued this cert), expiry info, public / private key, cert usage details (for which pur this cert has been issued )   * Here this public key is used to encrypt the data (so that this encrypted data will be transmitted ) * Every certificate will have 1 serial number (CA before issuing a cert it will assign a num to that cert) to uniquely identify a cert (like PAN to each individual) so that later if that cert is expired it will block that cert with based on that cert id * with this num only we will identify whether the cert had been already revoked or not & this serial num is used to revoke the cert * It contain cert usage details – to know for what purpose this cert had been issued   CA will sign every cert with its private key, | above is the cert issued to canara bank |
| how to check if cert is valid or not:- by using its cert serial number  The Online Certificate Status Protocol (OCSP) is an Internet protocol used to check the revocation status of digital certificates, such as those used for SSL/TLS connections. It's an alternative to Certificate Revocation Lists (CRLs) and allows clients to query a CA's OCSP server to determine if a certificate is valid or revoked.  With this OCSP we can query if that cert is valid or revoked |  |
| renewal vs re issuance  generally when u are using venafi cert management portal ,when the old cert is expired, u don’t need to re-issue a new certificate, (re-issuance is needed only when private key is lost )  we just need to renew the old certificate   * Every Cert will have expiry date, Once the cert are expired browsers will detect that we are using expired cert, it will result in loss of belief | |

## 2.3 SSL vs TLS

SSL, Stands for, Server Socket Layer however TLS, Stand for, Transport Layer Security. SSL is just the older name.

SSL and TLS are security protocols that are used to secure the network communication (Data in transit must be encrypted using any ssl certificate / key algorithm)

SSL is almost old and deprecated

TLS= more updated version of SSL, but both will do same thing of encrypting the data transfer

SSL (Secure socket layer) is standard technology for securing an internet connection by **encrypting the data** that is being sent between website and browser

It prevents hackers from seeing or stealing any information transferred

TLS (Transport layer security) is a protocol that helps secure communication over computer network, **TLS is also used to encrypt the communication** between web app and server

So data is always encrypted during transit

Both functionalities are same, but internal working implementations are different, like SSL uses different hashing function and TLS uses different hashing function

SSL uses hashing function such as MD5, SDH-1 but these are old sometimes different for diff inputs result hash is same

Hi=110

Bye=110

Whereas TLS uses SHA-256 algorithm, diff inputs always gives diff hash values

|  |  |
| --- | --- |
| SSL | TLS |
| Uses data encryption standards DES, RC4 | Uses AES standard |

We cant call as SSL/ TLS certificate – we should call as PKI cert,

## 2.4 Public/Private keys

* **Public Key** is used to Encrypt the data. (Think of certificates. No harm passing the public key, certificate, to anyone publicly)
* **Private Key** is used to Decrypt the data, encrypted by Public key.
* Private Key is like a password which should never cross the boundary of a system who has generated it. Consider it very secure. Think of it a system password which you don’t even share with your manager or any other person in authority.

## 2.5 MTLS (Mutual TLS)/ 2 way authn

Mutual means both, so MTLS means both client and server will mutually verify others identity /other certificates,

Like client will verify server certificate and server will verify client certificate with the help of CA who can check the certificate

So in postman when u are hitting an MTLS URL u need to attach certificate

Because both server and client needs to verify others certificate

**How Client will validate server certificate???**

Simple client will go and ask the certificate authority (the one who issued the certificate) saying whether it had issued that certificate to that website or not

Generally in one way communication,

1. Client will verify the servers certificate to confirm whether its talking to right client or not
2. And server accepts all clients, whereas in MTLS server will also validate the client certificate

Whereas in MTLS, not only client, whereas server also will verify the client authenticity

1. While making a call to the server, Client uses its ***Certificate*** and ***Client*** ***Key*** for the communication which is validated at the Server side to ensure the identity of client. Server consults Trust Store whether it’s a valid client to be given access or not. Please note, ***Client*** ***Key*** does not travel over network, it’s a private key and used to decrypt the data over the TCP tunnel.

## 2.6 key store and trust store

Key store contains our key and certificate

What is Trust store – trust store is used to trust only some websites

Importing other party appln to trust store

Assume if our appln want to allow 1dstr application, then we should import the 1dstr app certificate (we need to import the certificate that has been issued to 1dstr) into our server,