Date / /
Page

X.509 Authentication Service:

> It is a digital certificate that is built on top of a widely trusted standard known as ITU or International Telecommunication Union.

> It is a certificate-based authentication security framework that can be used for providing secure transaction processing & private information.

> These are primarily used for handling the security and identity in computer networking and internet-based communications.

Working:

> The core of the X.509 authentication service is the public key certificate connected to each user.

> This certificate is created by a trusted authority and stored in a directory, making it easy for others to find and use.

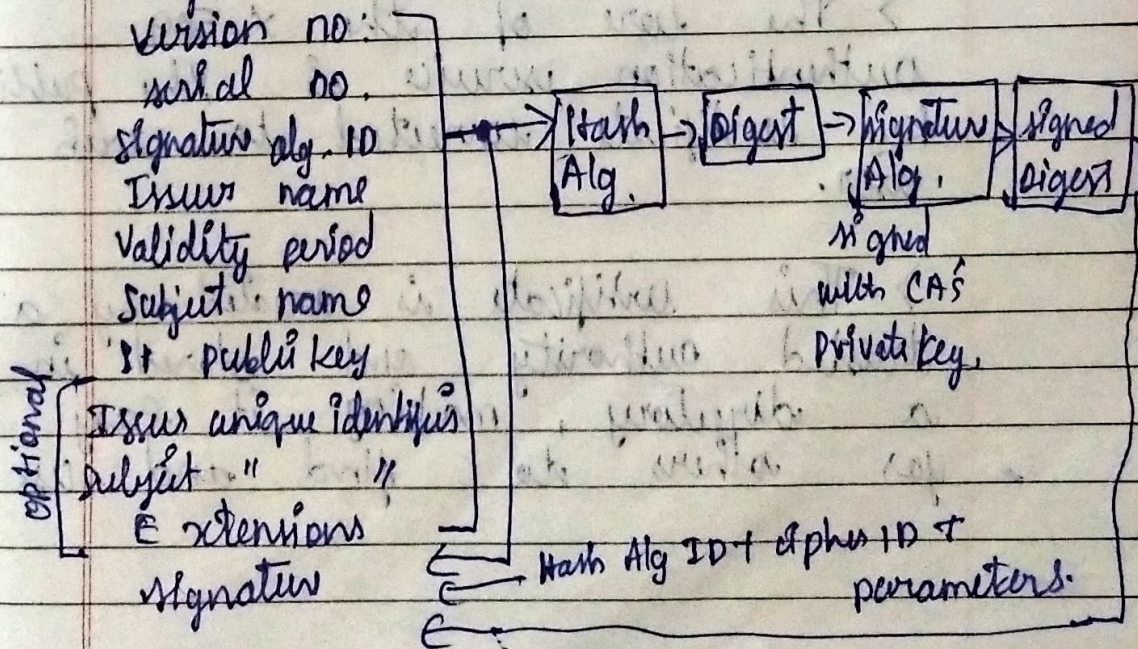
Date / /
Page

> X.509 is based on a structure called ASN.1 and the certificate uses a pair of keys to secure msg by encrypting & decrypting.

> once an X.509 certificate is it provided to a user by the admin like an ID card for the certificate (making it much safer than regular passwords since it's harder to steal or lose.

> The certificate is then shown as proof of identity whenever the user needs to access a resource that requires authentication.

Diagram:



Date / /
Page

(1) Version no: It defines the X.509 version that concerns the certificate.
(2) serial no: It is the unique no. that the certified authority issues.
(3) signature Alg. Identifier: This is the Alg. that is used for signing the certificate.
(4) Issuer name: Tells about the X.500 name of the certified authority which signed & created the certificate.
(5) period of validity: It defines the period for which the certificate is valid.
(6) subject Name: Tells about the name of the user to whom this certificate has been issued.
(7) subject public key Information: It defines the subjects public key along with an identifier of the Alg. for which this key is supposed to be used.
(8) Extension block: This field contains additional standard information.
(9) signature: This field contains the hash code of all other fields which is encrypted by the certified authority private key.

Applications:

* Digital signature
* Web server security
* Email certificates
* code signing.
* Digital identities
* Secure shell protocol (SSH) keys.