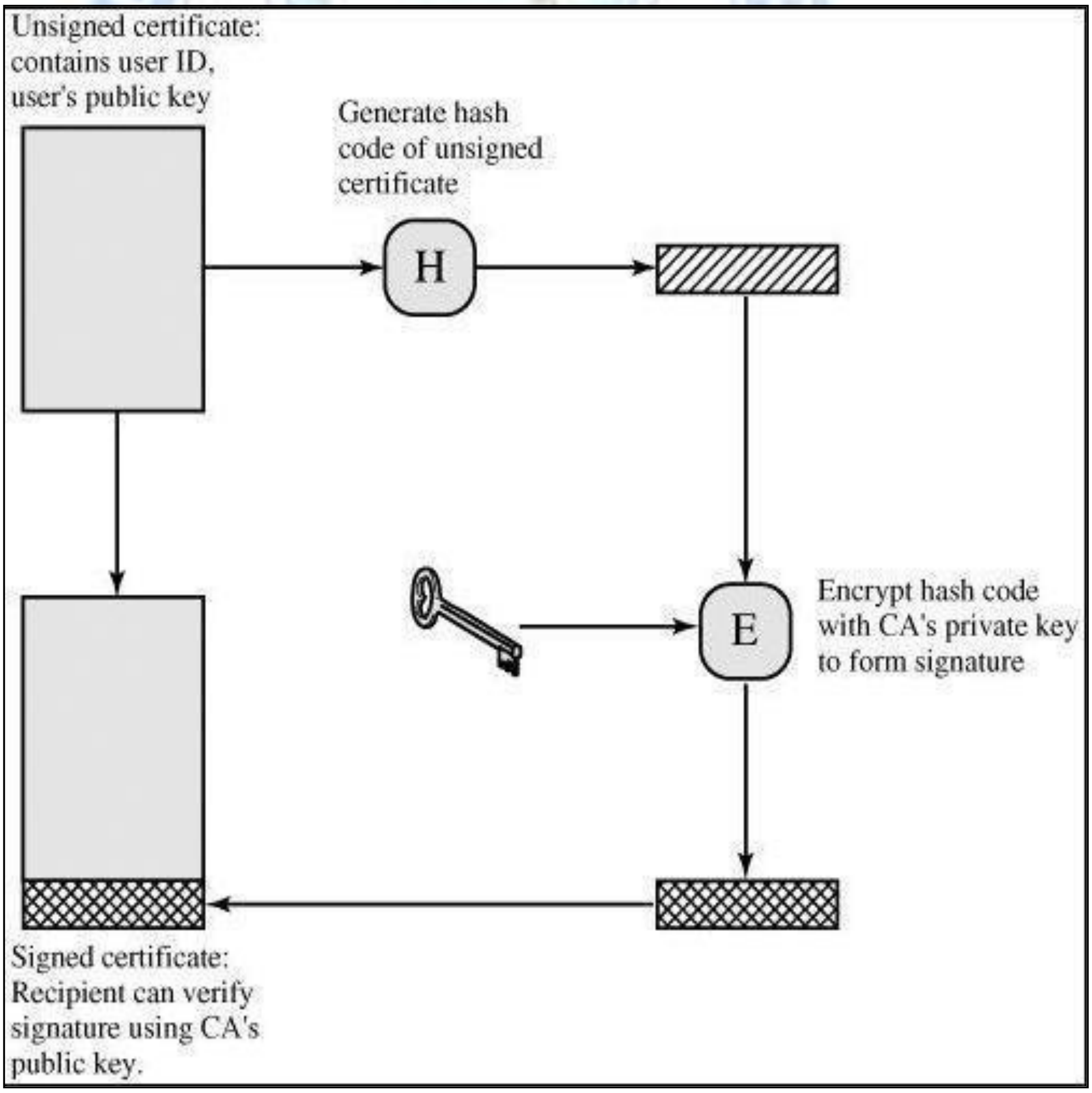
2.2 X.509 AUTHENTICATION SERVICE

ITU-T Recommendation X.509 is part of the X.500 series of recommendations that define a directory service. X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates of the type.

Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. X.509 certificate format is used in S/MIME, IP Security, and SSL/TLS and SET.

X.509 is based on the use of public-key cryptography and digital signature algorithms. Figure illustrates the generation of public key.


Unsigned certificate: contains user ID, user's public key
Generate hash code of unsigned certificate
H
E
Encrypt hash code with CA's private key to form signature
Signed certificate: Recipient can verify signature using CA's public key.

Certificates

Figure shows the general format of a certificate, which includes the following elements:

Version:
Differentiates among successive versions of the certificate format; the default is version

Serial number: An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.

Signature algorithm identifier: The algorithm used to sign the certificate,
together with any associated parameters

Issuer name: X.500 name of the CA that created and signed this certificate.

Period of validity: Consists of two dates: the first and last on which the certificate is valid.

Subject name: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.

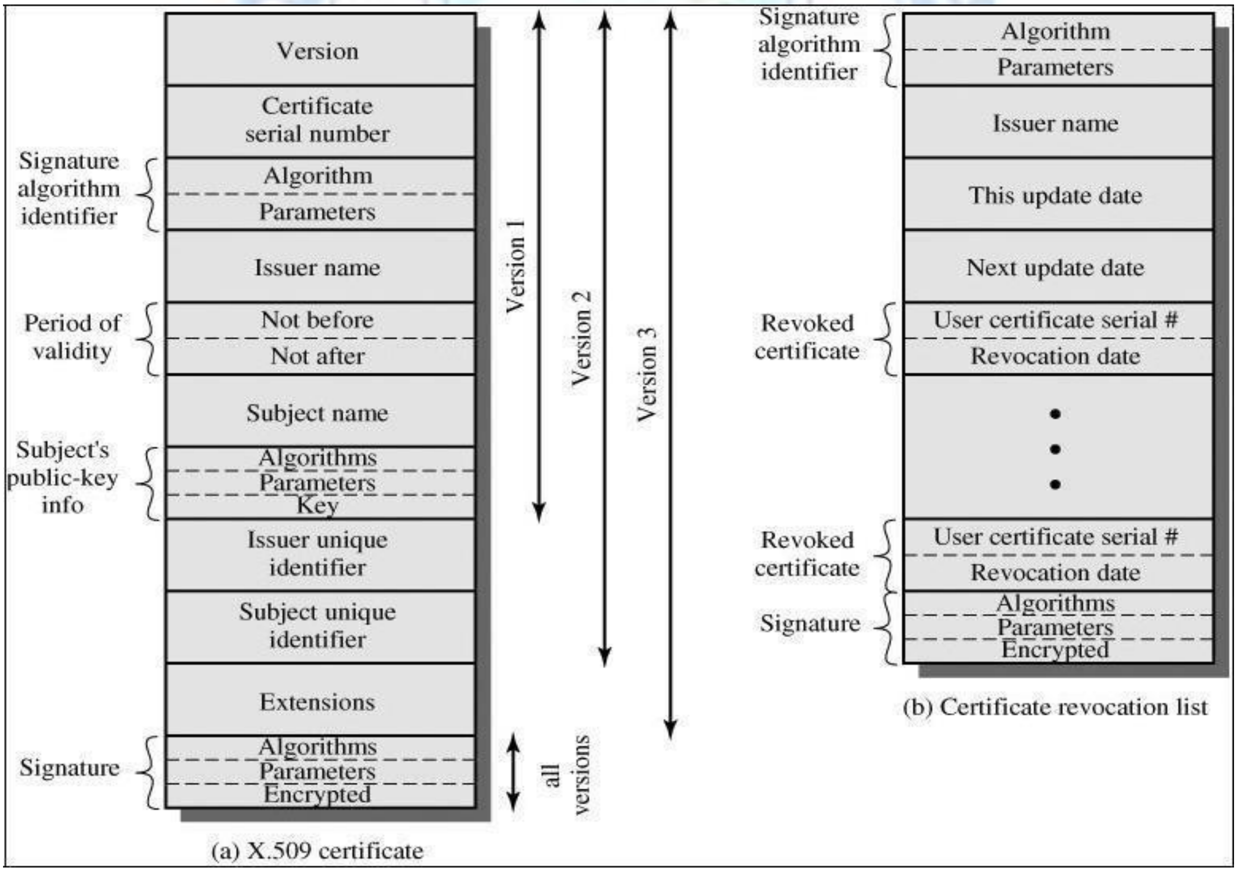
Subject's public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.

Issuer unique identifier: An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.

Subject unique identifier: An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.

Extensions: A set of one or more extension fields.

Signature: This field includes the signature algorithm identifier.



(a) X.509 certificate

(b) Certificate revocation list

The standard uses the following notation to define a certificate:

CA<<A>> = CA {V, SN, AI, CA, T_A, A, Ap}

The CA signs the certificate with its private key. If the corresponding public key is known to a user, then that user can verify that a certificate signed by the CA is valid.

Obtaining a Certificate

- User certificates generated by a CA have the following characteristics:
- Any user with access to the public key of the CA can verify the user public key that was certified.
- No party other than the certification authority can modify the certificate without this being detected. Because certificates are unforgeable, they can be placed in a directory without the need for the directory to make special efforts to protect them.

Certificate Revocation

Certificates have a period of validity.

May need to revoke before expiry, eg:

- User's private key is compromised
- User is no longer certified by this CA
- CA's certificate is compromised

CA maintain a list consisting of all revoked but not expired certificates issued by that CA, including both those issued to users and to other CAs. Each certificate revocation list (CRL) posted to the directory is signed by the issuer. When a user receives a certificate in a message, the user must determine whether the certificate has been revoked. The user could check the directory each time a certificate is received.