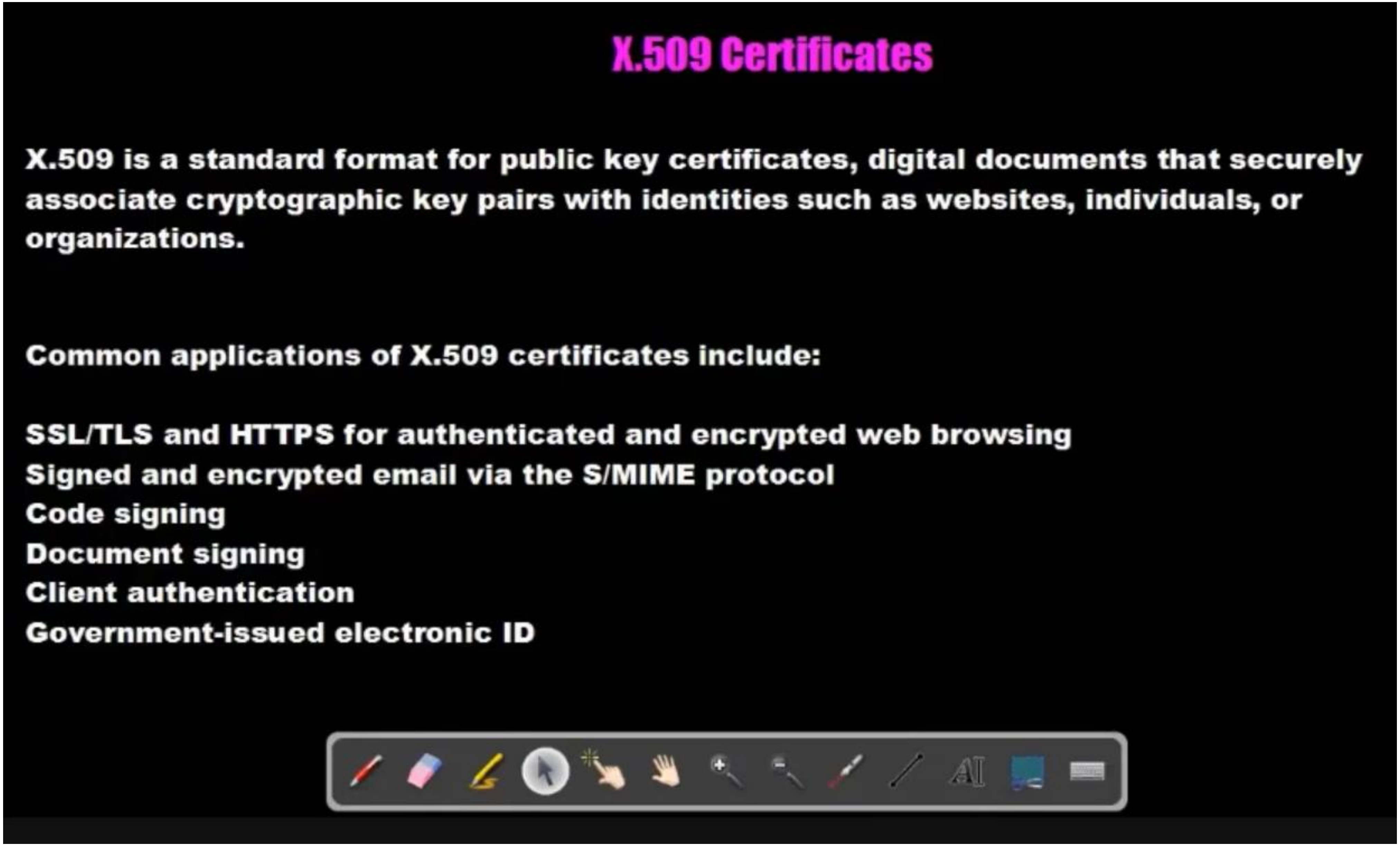
X.509 Digital Certificate

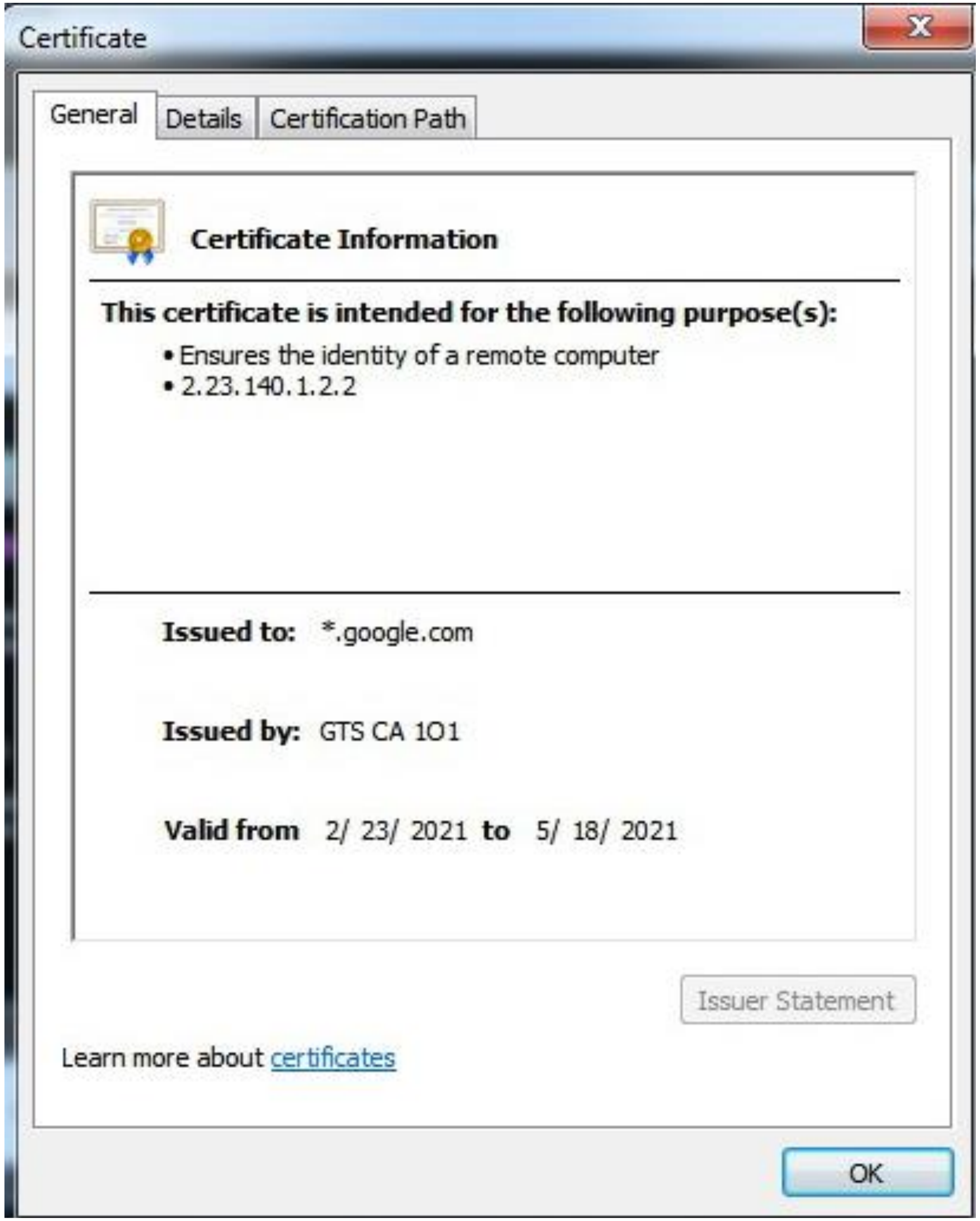


X.509 Certificates

X.509 is a standard format for public key certificates, digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations.

Common applications of X.509 certificates include:

SSL/TLS and HTTPS for authenticated and encrypted web browsing
Signed and encrypted email via the S/MIME protocol
Code signing
Document signing
Client authentication
Government-issued electronic ID



Certificate Information

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

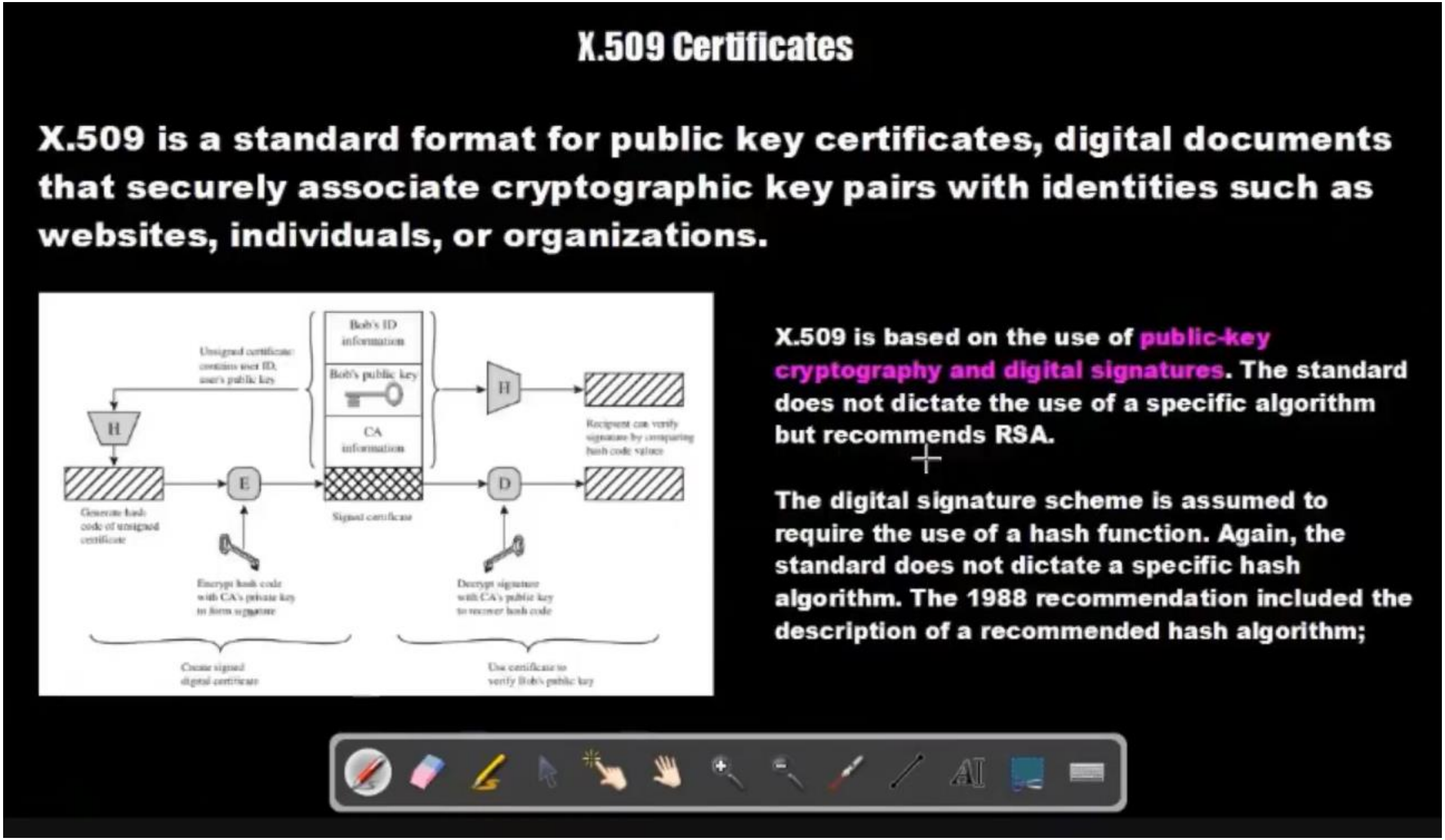
- Ensures the identity of a remote computer
- 2.23.140.1.2.2

Issued to: *.google.com

Issued by: GTS CA 1O1

Valid from 2/ 23/ 2021 **to** 5/ 18/ 2021

Learn more about certificates



X.509 Certificates

X.509 is a standard format for public key certificates, digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations.

X.509 is based on the use of public-key cryptography and digital signatures. The standard does not dictate the use of a specific algorithm but recommends RSA.

The digital signature scheme is assumed to require the use of a hash function. Again, the standard does not dictate a specific hash algorithm. The 1988 recommendation included the description of a recommended hash algorithm;

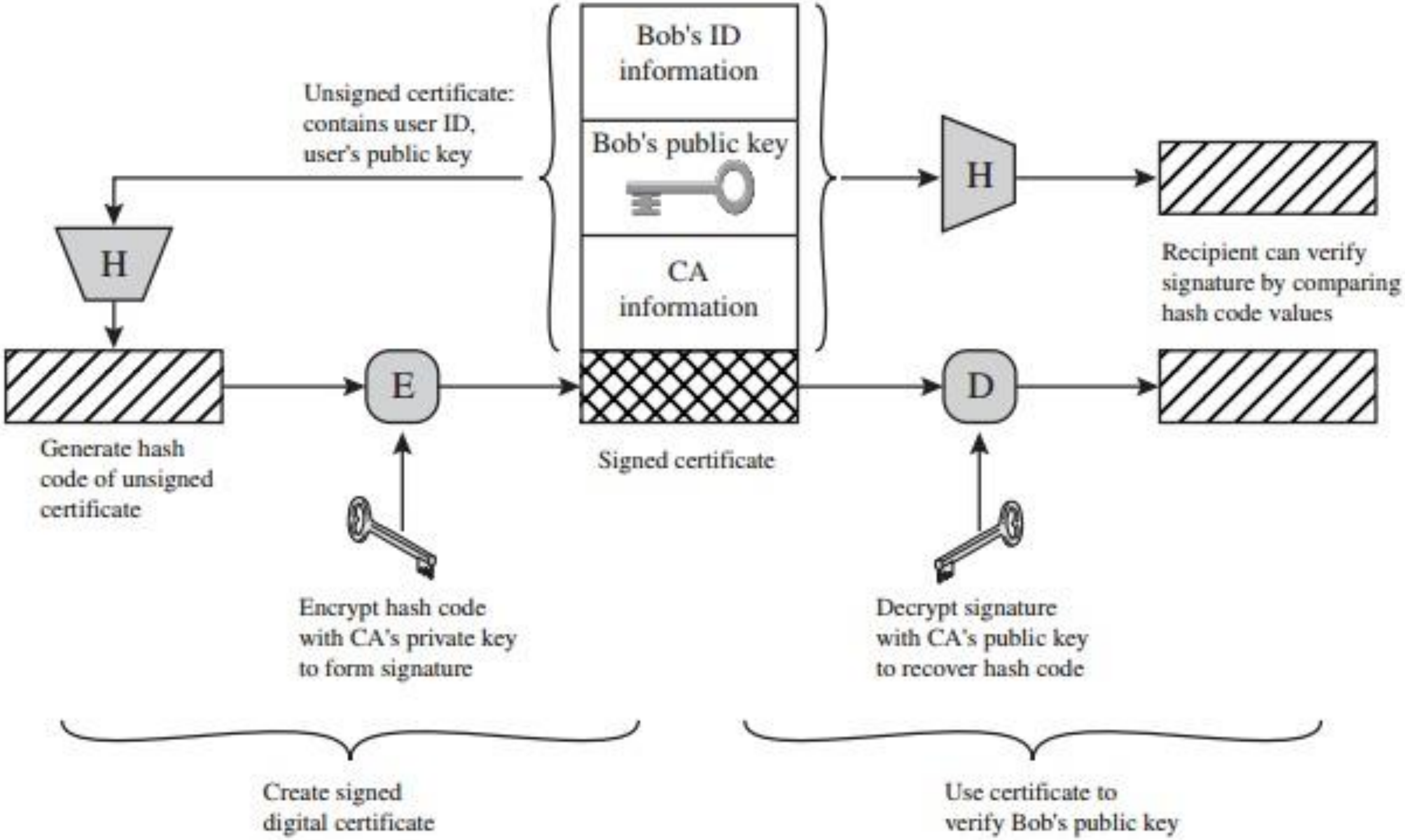
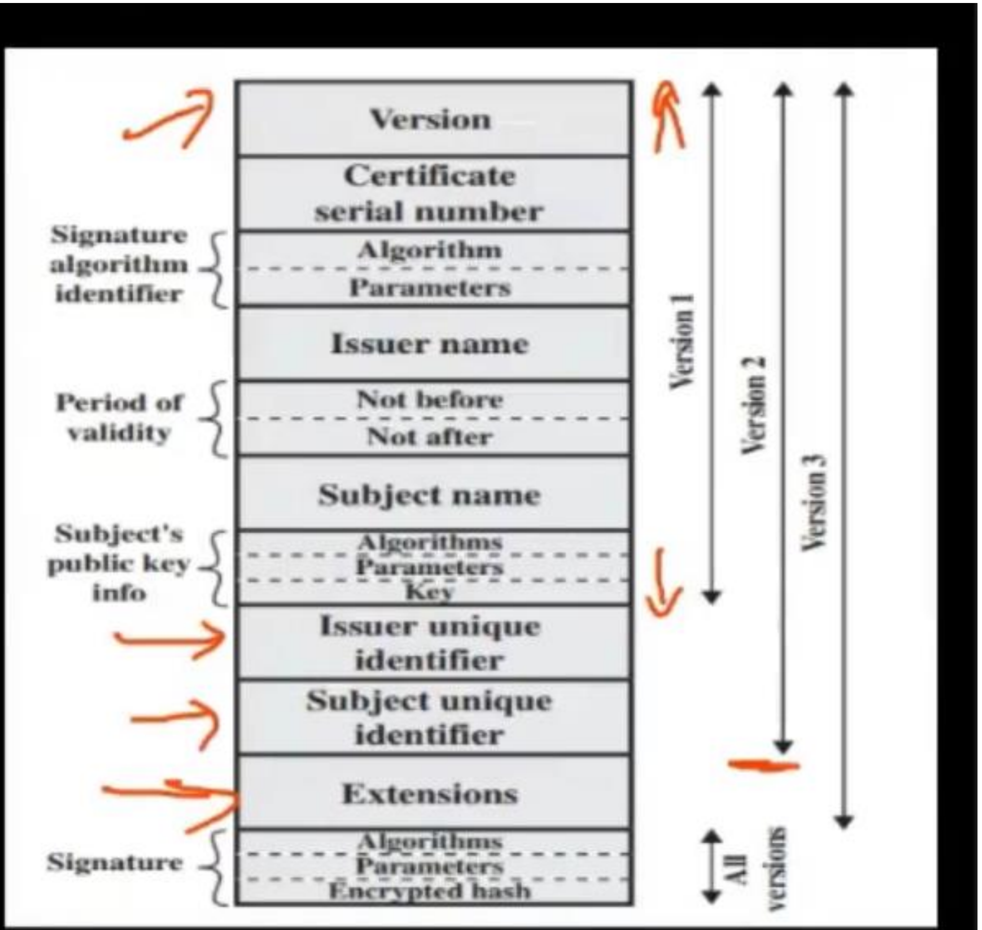

Bob's ID information
Bob's public key
CA information
Unsigned certificate: contains user ID, user's public key
H
H
Recipient can verify signature by comparing hash code values
E
D
Generate hash code of unsigned certificate
Signed certificate
Encrypt hash code with CA's private key to form signature
Decrypt signature with CA's public key to recover hash code
Create signed digital certificate
Use certificate to verify Bob's public key

Figure 14.13 Public-Key Certificate Use

The heart of the X.509 scheme is the public-key certificate associated with each user. These user certificates are assumed to be created by some trusted certification authority (CA) and placed in the directory by the CA or by the user. T

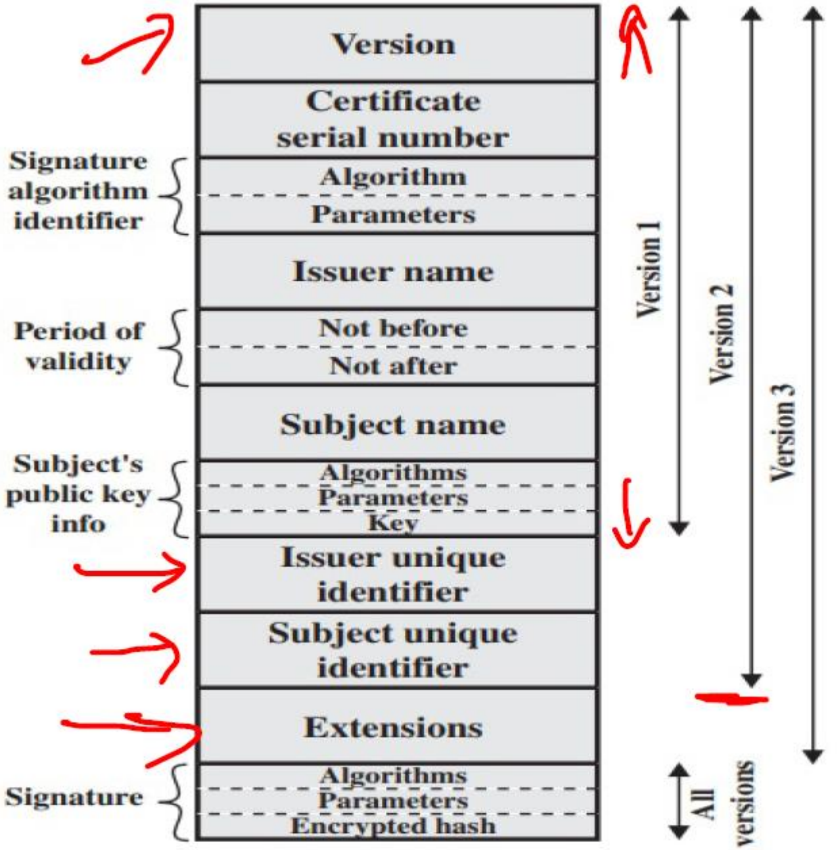
Version: Differentiates among successive versions of the certificate format; the default is version 1. If the issuer unique identifier or subject unique identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.

Ver:2 , Ver:3



Version: Differentiates among successive versions of the certificate format; the default is version 1. If the issuer unique identifier or subject unique identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.

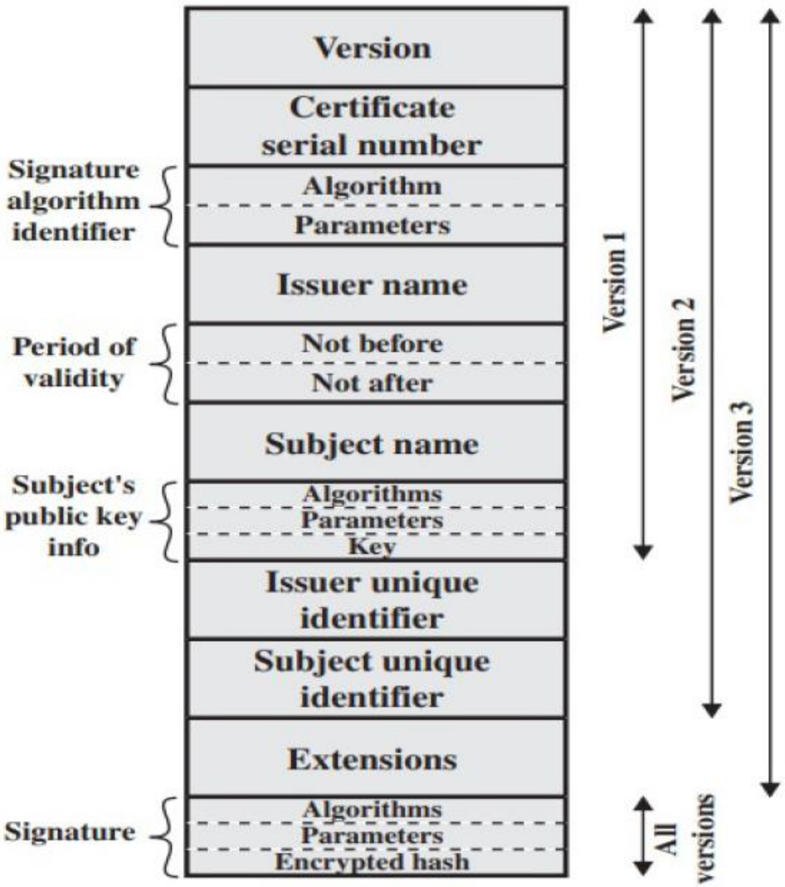
Ver:2 , Ver:3



1234 ⇔ Comodo

→ Verisign 1234

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



Version

Certificate serial number

Signature algorithm identifier: Algorithm, Parameters

Issuer name

Period of validity: Not before, Not after

Subject name

Subject's public key info: Algorithms, Parameters, Key

Issuer unique identifier

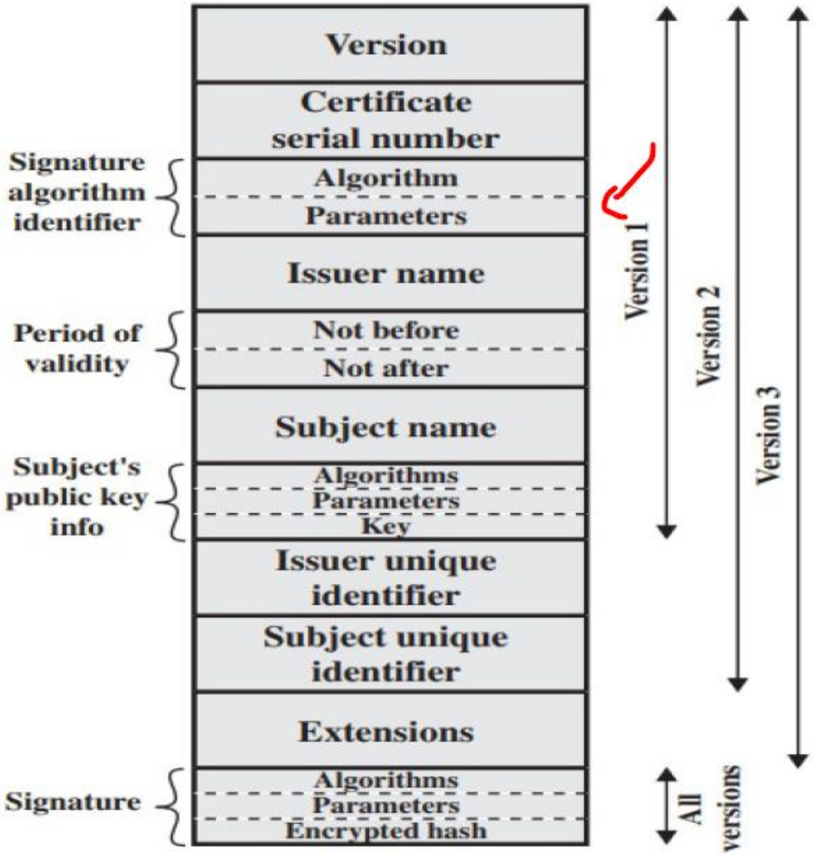
Subject unique identifier

Extensions

Signature: Algorithms, Parameters, Encrypted hash

Signature algorithm identifier: The algorithm used to sign the certificate together with any associated parameters. Because this information is repeated in the signature field at the end of the certificate, this field has little, if any, utility.

RSA, Schnorr, Elgamal

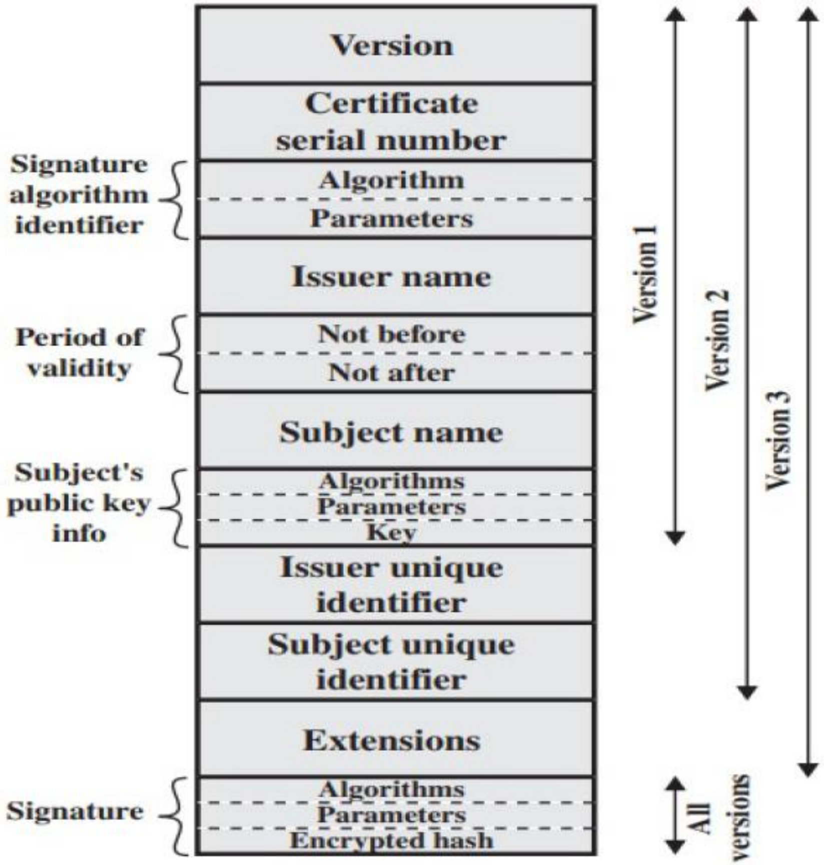


X.509

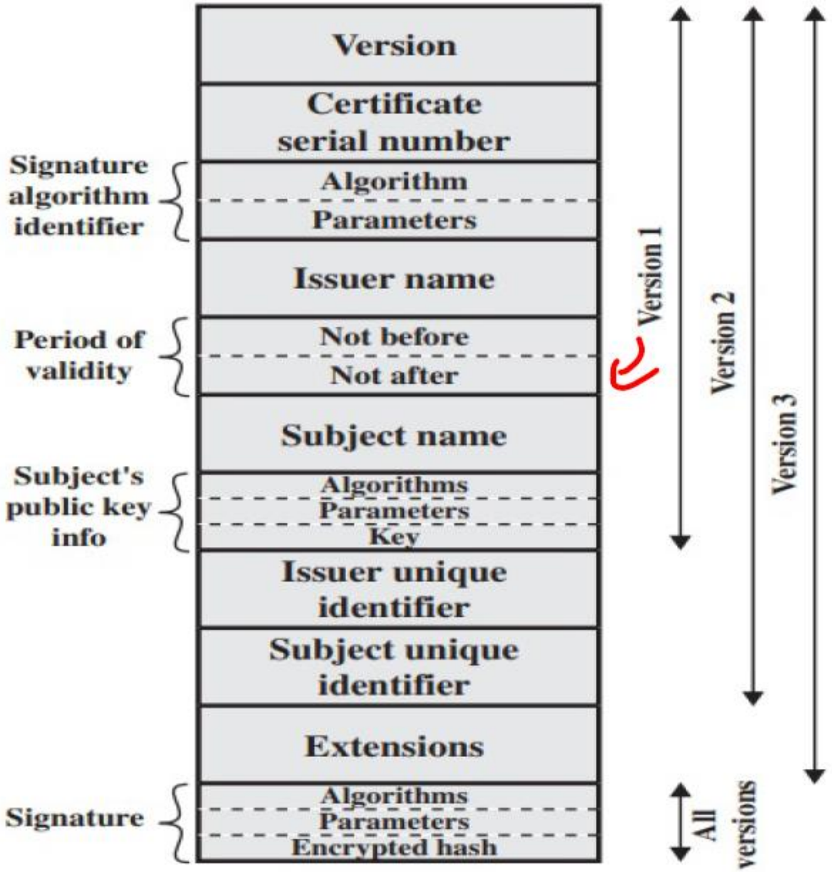
Issuer name: **X.500 name of the CA that created and signed this certificate.**

Let's Encrypt

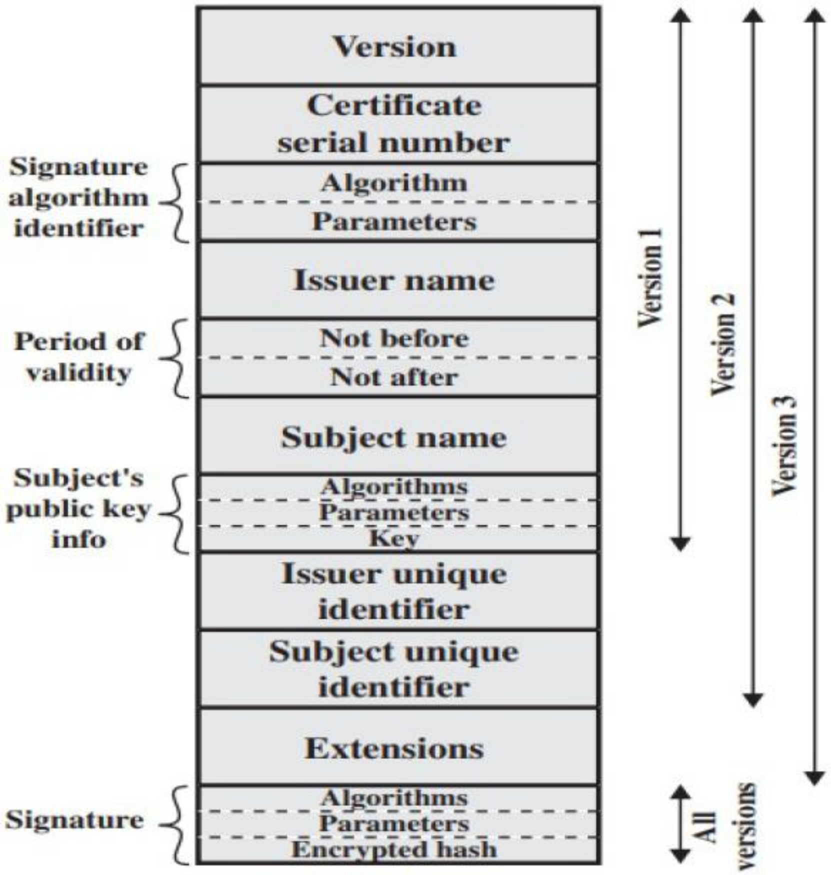
Comodo



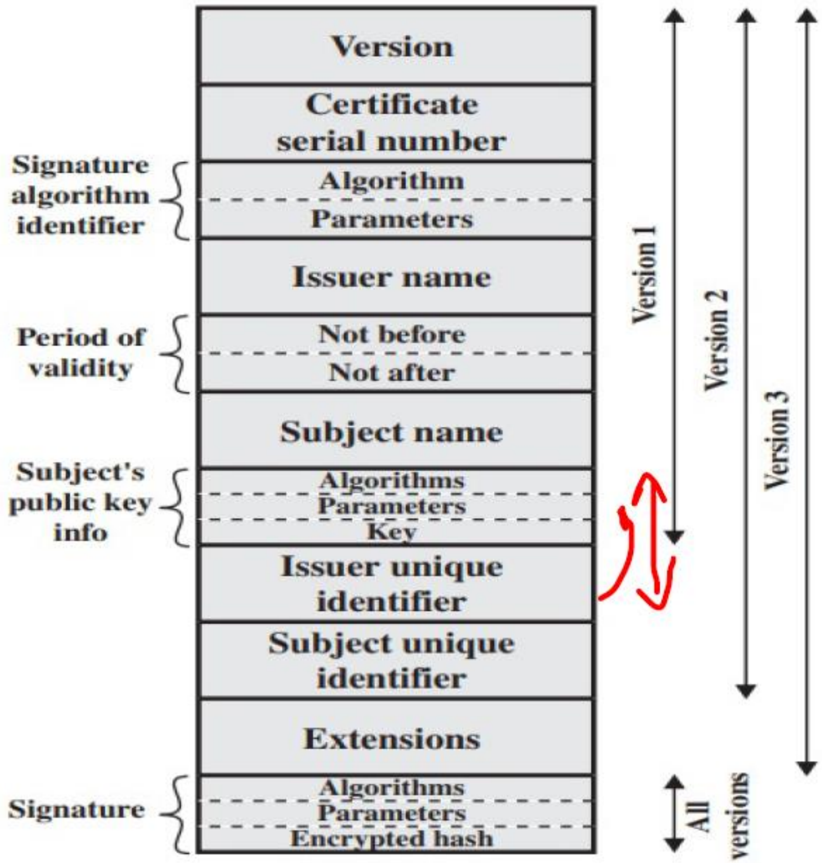
Period of validity **Consists of two dates: the first and last on which the certificate is valid.**



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.

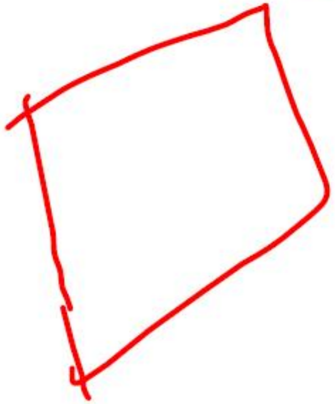


Subject’s public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.



CD1234 VR1234

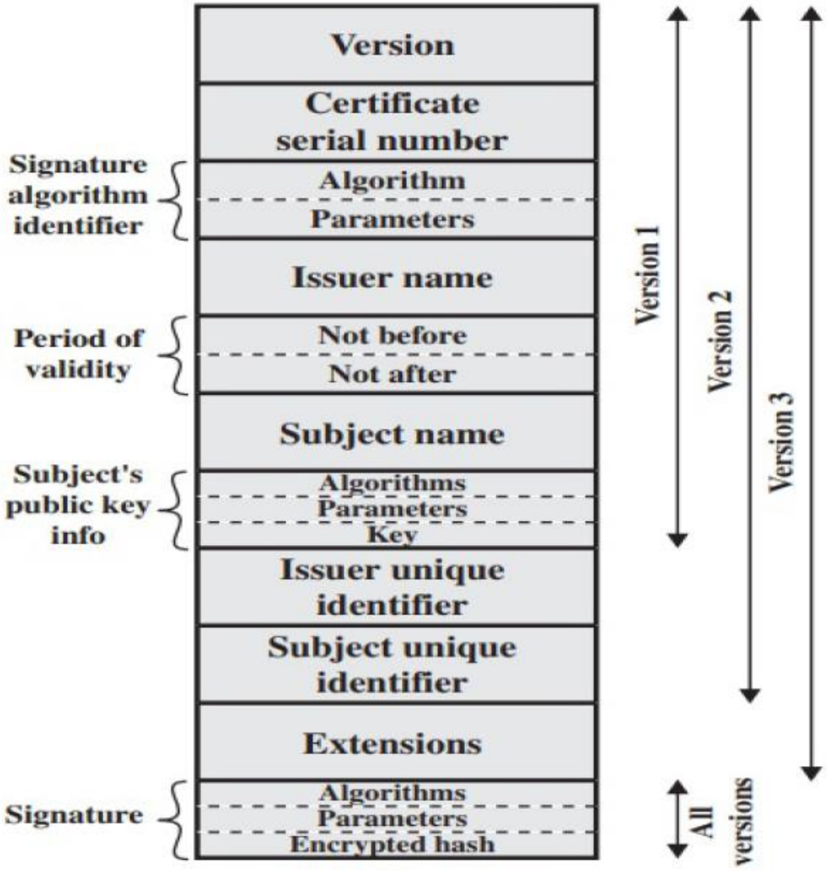
Issuer unique identifier: **An optional-bit string field used to identify uniquely the issuing CA.**



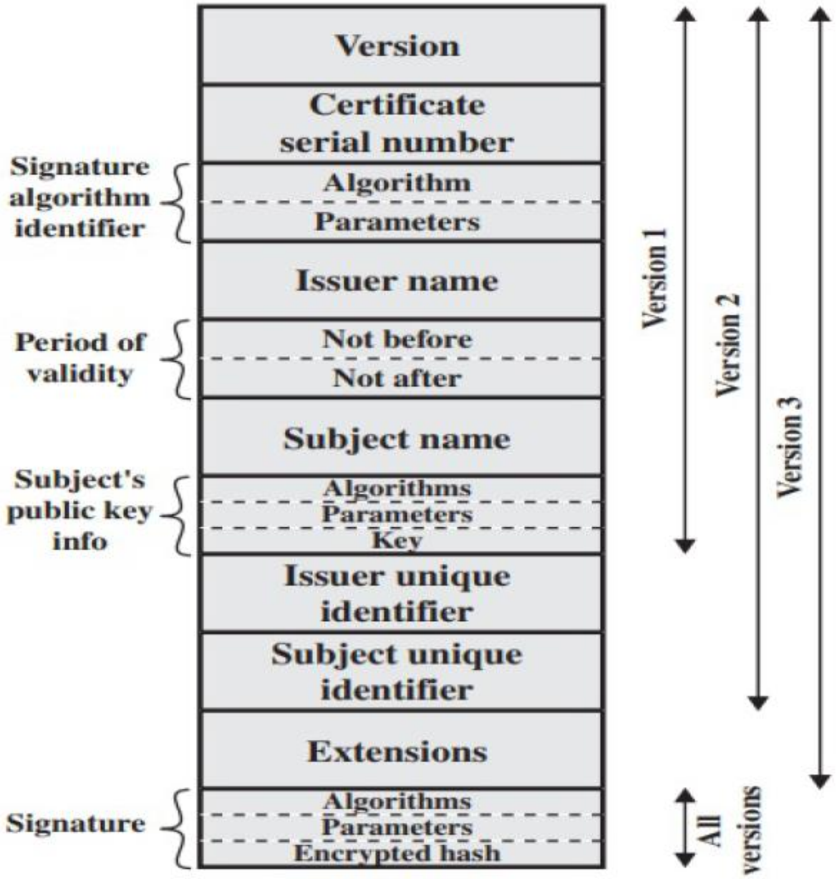
Comodo

Verisign

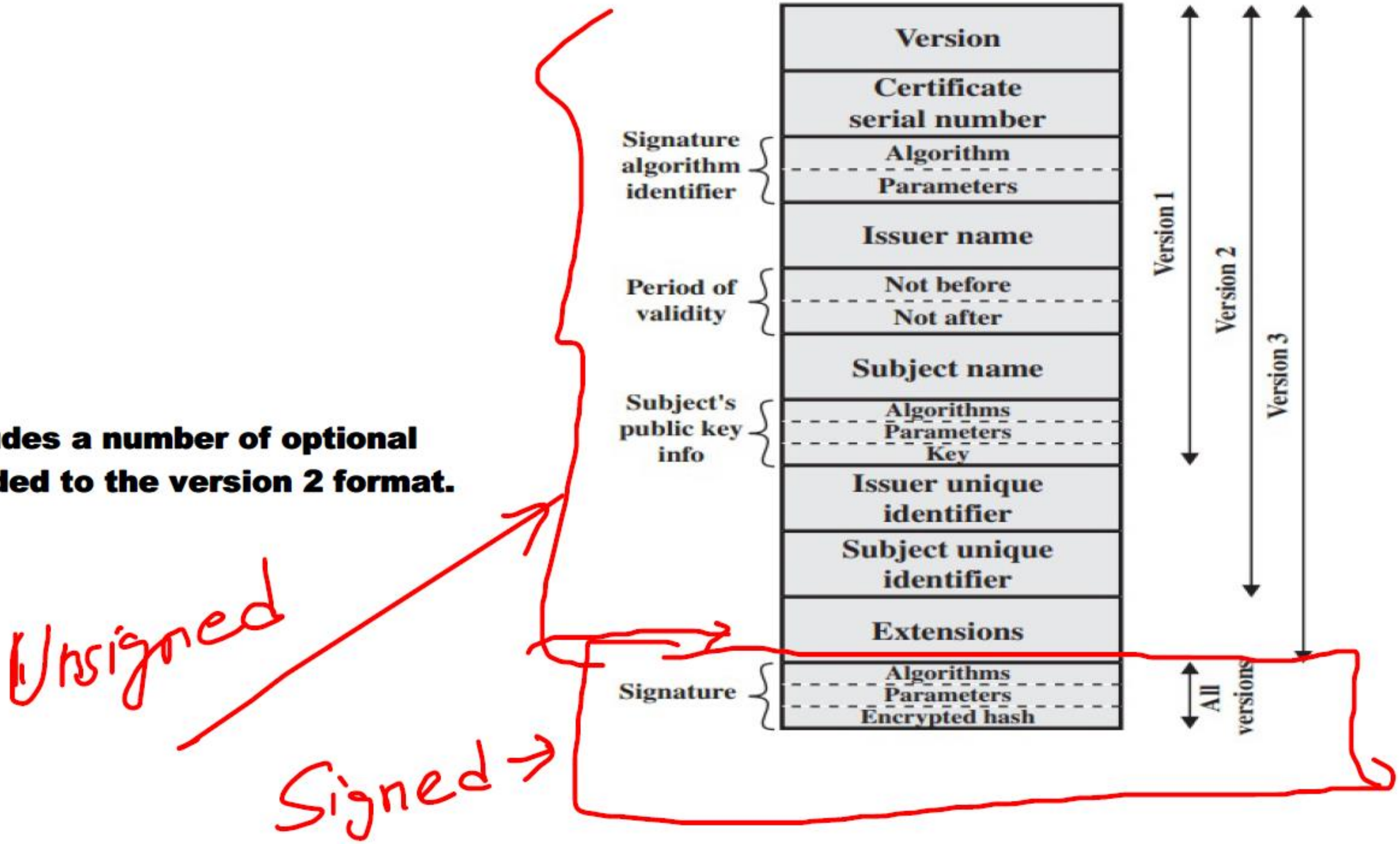
Chassis



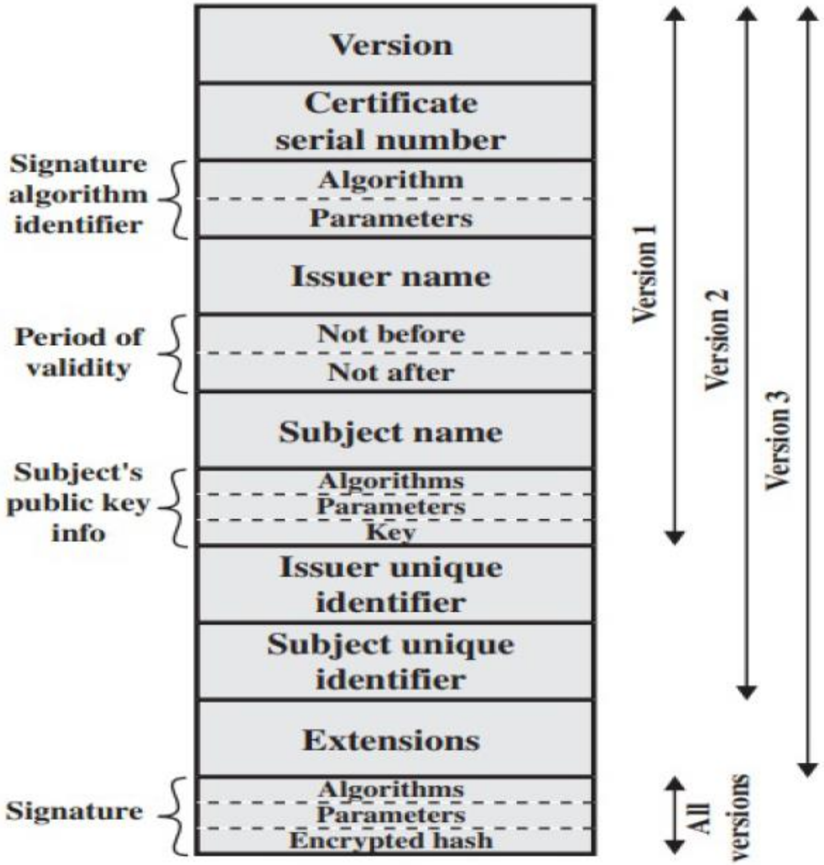
Subject unique identifier: An optional-bit string field used to identify uniquely the subject.



Extensions **Version 3 includes a number of optional extensions that may be added to the version 2 format.**



Signature: **Covers all of the other fields of the certificate; it contains the hash code of the other fields encrypted with the CA's private key. This field includes the signature algorithm identifier**


Version
Certificate serial number
Signature algorithm identifier
Algorithm
Parameters
Issuer name
Period of validity
Not before
Not after
Subject name
Subject's public key info
Algorithms
Parameters
Key
Issuer unique identifier
Subject unique identifier
Extensions
Signature
Algorithms
Parameters
Encrypted hash
Version 1
Version 2
Version 3
All versions