SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A+’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

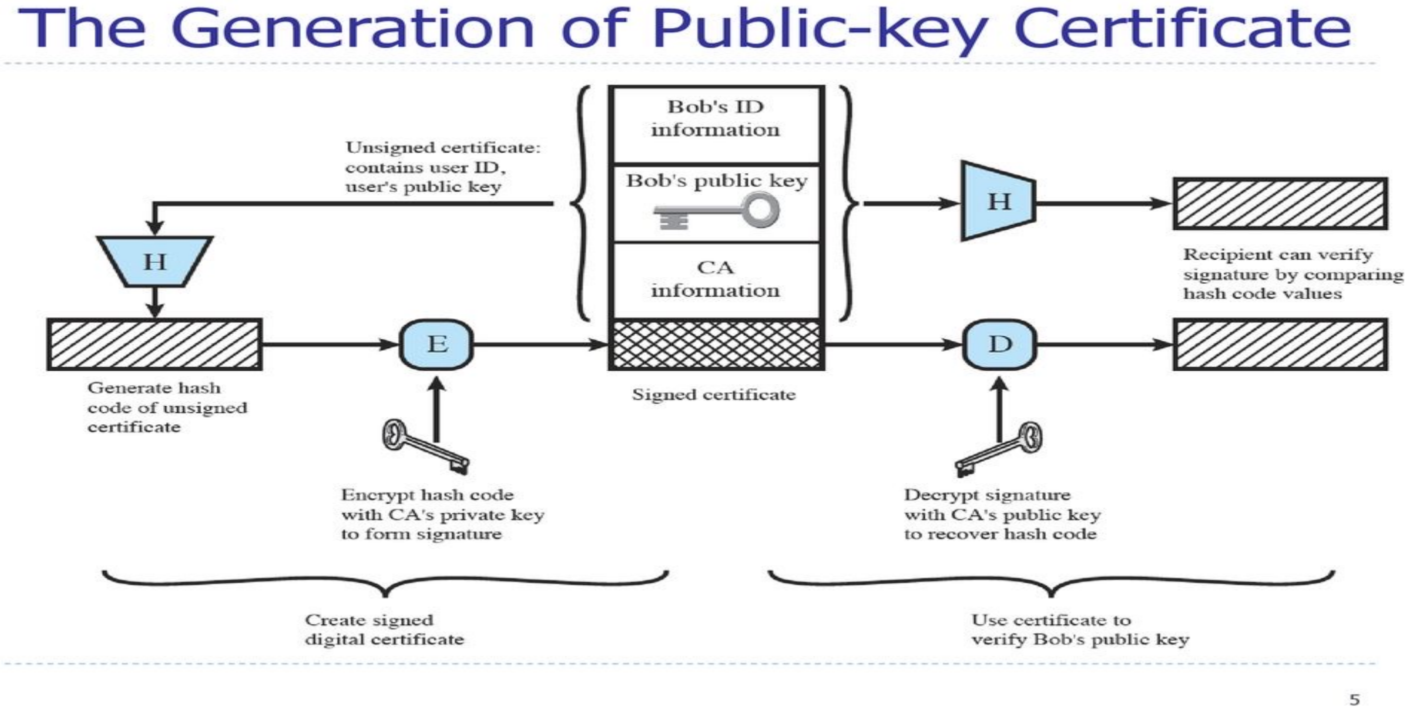
DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-4 INTERACTIVE TECHNIQUES AND TOOLS

X.509 certificate

- **X.509 certificates** are digital documents that are used to verify the identity of individuals, organizations, or devices over the internet. They are widely used in various applications like secure email, web browsing, online banking, and electronic transactions.
- An X.509 certificate contains information about the **certificate holder's identity**, such as their name, **public key**, **digital signature**, and the name of the **certificate authority (CA)** that issued the certificate. The public key is used to encrypt messages, and the digital signature is used to verify that the message was sent by the holder of the private key associated with the public key.
- In other words, an X.509 certificate acts like a **digital identity card** that enables secure communication and transaction between two parties. The **use of X.509 certificates** ensures that the communication is encrypted and authenticated, thereby providing a high level of security for online transactions.



The Generation of Public-key Certificate

Unsigned certificate: contains user ID, user's public key

Bob's ID information

Bob's public key

CA information

H

Generate hash code of unsigned certificate

E

Encrypt hash code with CA's private key to form signature

Signed certificate

H

Recipient can verify signature by comparing hash code values

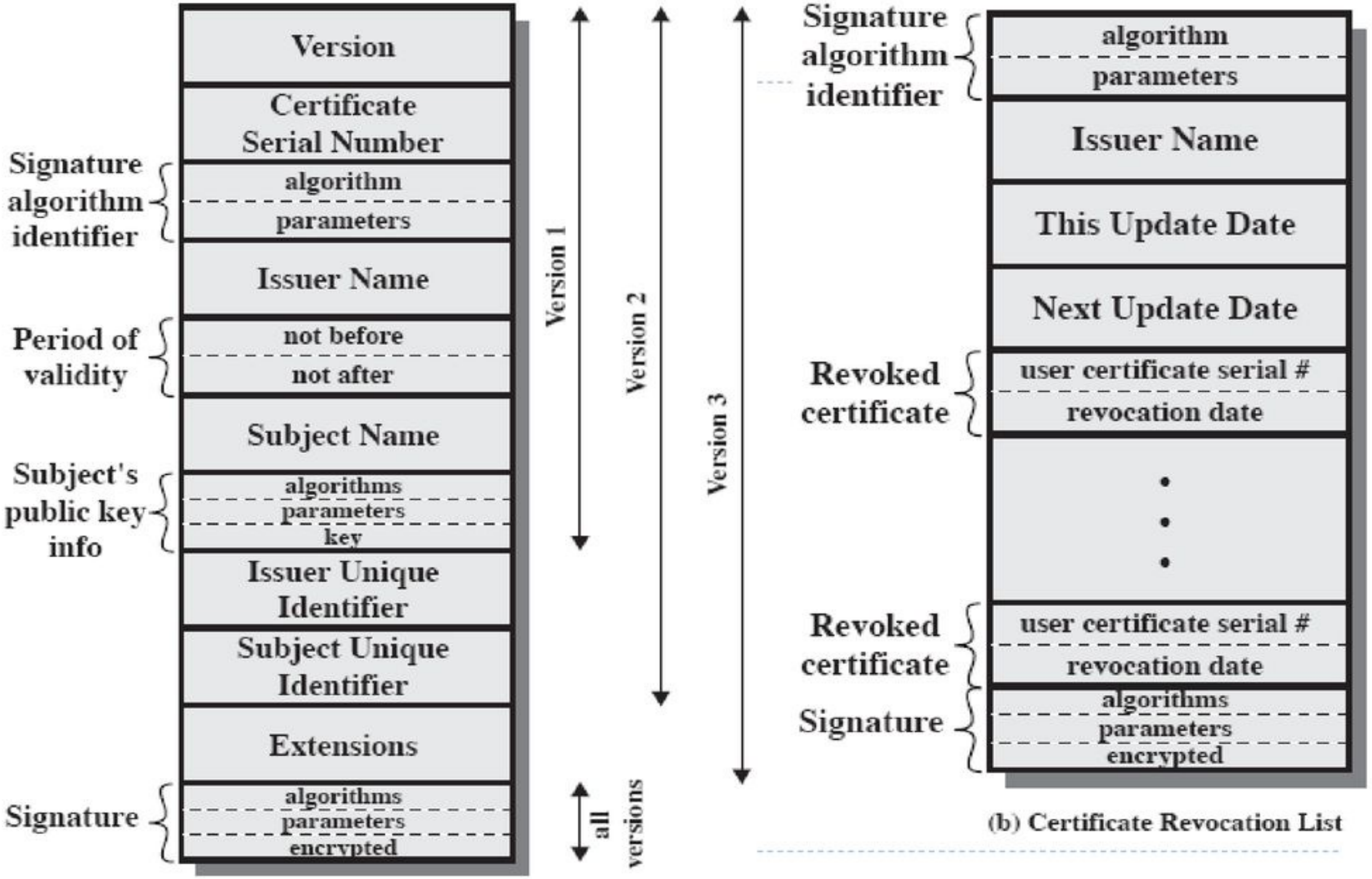
D

Decrypt signature with CA's public key to recover hash code

Create signed digital certificate

Use certificate to verify Bob's public key

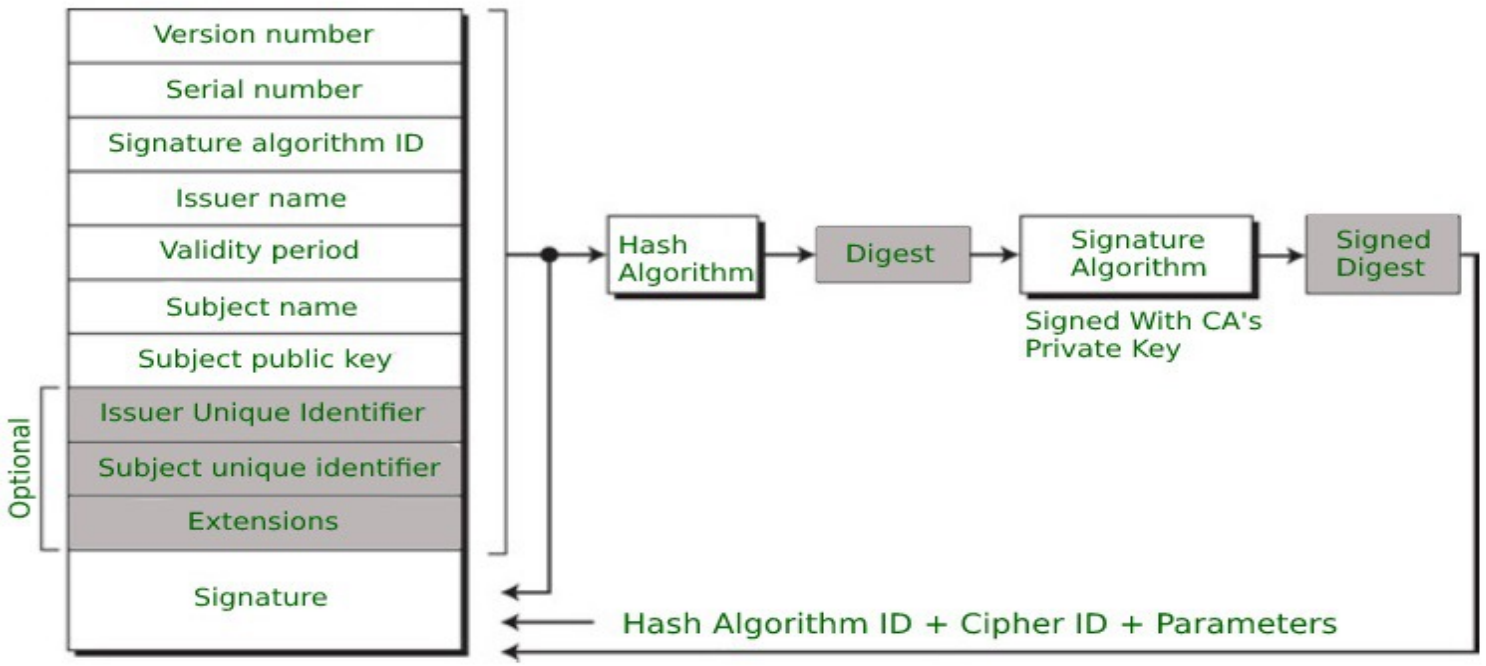
X.509 Certificates



(a) X.509 Certificate

(b) Certificate Revocation List

- **Version number:** It defines the X.509 version that concerns the certificate.
- **Serial number:** It is the unique number that the certified authority issues.
- **Signature Algorithm Identifier:** This is the algorithm that is used for signing the certificate.
- **Issuer name:** Tells about the X.500 name of the certified authority which signed and created the certificate.
- **Period of Validity:** It defines the period for which the certificate is valid.
- **Subject Name:** Tells about the name of the user to whom this certificate has been issued.
- **Subject's public key information:** It defines the subject's public key along with an identifier of the algorithm for which this key is supposed to be used.
- **Extension block:** This field contains additional standard information.
- **Signature:** This field contains the hash code of all other fields which is encrypted by the certified authority private key.


Version number
Serial number
Signature algorithm ID
Issuer name
Validity period
Subject name
Subject public key
Issuer Unique Identifier
Subject unique identifier
Extensions
Optional
Signature
Hash Algorithm
Digest
Signature Algorithm
Signed With CA's Private Key
Signed Digest
Hash Algorithm ID + Cipher ID + Parameters

Obtaining a User's 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.

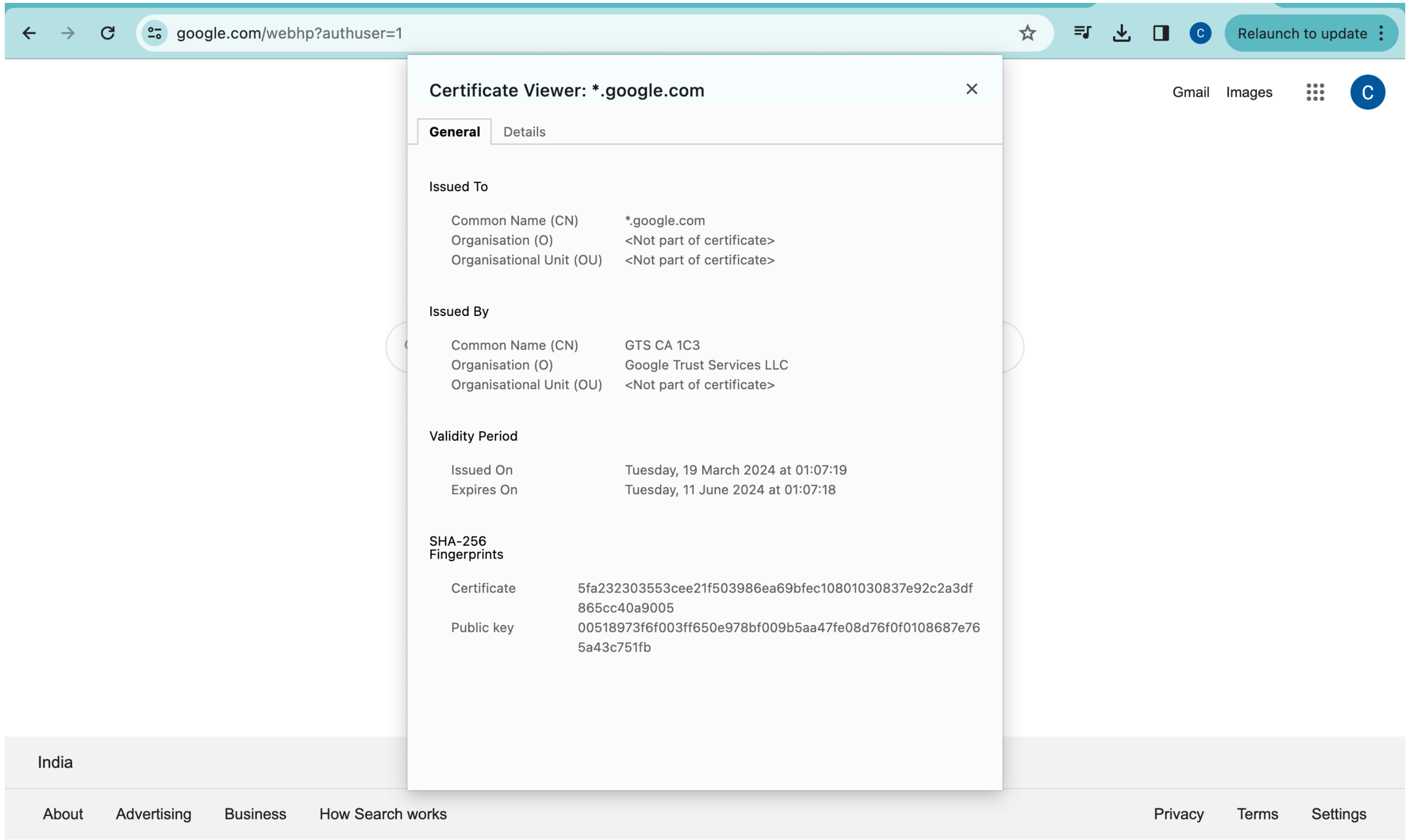
Certificate Revocation

Certificates have a period of validity and may need to revoke before expiry, for the following reasons

1. user's private key is compromised
2. User is no longer certified by this CA
3. CA's certificate is compromised

X.509 Version 3

- **Authority key identifier**: Identifies the public key to be used to verify the signature on this certificate or CRL.
- **Subject key identifier**: Identifies the public key being certified. Useful for subject key pair updating.
- **Key usage:** Indicates a restriction imposed as to the purposes for which, and the policies under which, the certified public key may be used.
- **Private-key usage period:** Indicates the period of use of the private key corresponding to the public key.
- **Certificate policies:** Certificates may be used in environments where multiple policies apply.
- **Policy mappings:** Used only in certificates for CAs issued by other CAs.



Certificate Viewer: *.google.com

General | Details

Issued To

Common Name (CN)	*.google.com
Organisation (O)	<Not part of certificate>
Organisational Unit (OU)	<Not part of certificate>

Issued By

Common Name (CN)	GTS CA 1C3
Organisation (O)	Google Trust Services LLC
Organisational Unit (OU)	<Not part of certificate>

Validity Period

Issued On	Tuesday, 19 March 2024 at 01:07:19
Expires On	Tuesday, 11 June 2024 at 01:07:18

SHA-256 Fingerprints

Certificate	5fa232303553cee21f503986ea69bfec10801030837e92c2a3df865cc40a9005
Public key	00518973f6f003ff650e978bf009b5aa47fe08d76f0f0108687e765a43c751fb