X.509 Certificate

Dhruvit Boricha- 2109802
Jagrut Gala- 2109805
Raunak Ghetla- 2109806
Hatim Sadriwala- 2109847

Overview

- What is a Digital Certificate?
- What is X.509?
- X.509 Certificate Structure
- X.509 Certificate Notation
- Obtaining A User Certificate
- Chain Authentication
- Revocation of Certificates
- Certification Path Constraints

What is a Digital Certificate?

What is a Digital Certificate?

- In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key.
- It is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).
- A digital certificate certifies the ownership of a public key by the name of the subject on the certificate.
- A digital certificate serves two purposes: it establishes the owner's identity, and it makes the owner's public key available. A digital certificate is issued by a trusted authority--a certificate authority (CA)--and it is issued only for a limited time. When its expiration date passes, the digital certificate must be replaced.

What is X.509?

What is X.509?

- In cryptography, X.509 is a standard defining the format of public key certificates.
- X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.
- They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed.
- When a certificate is signed by a trusted certificate authority(CA), or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

X.509 Certificate Structure

Structure of X.509

There are 3 versions of X.509 Certificate

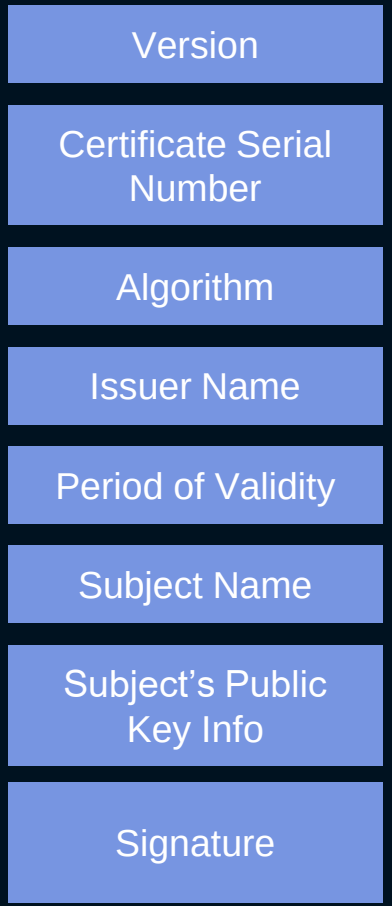
- First version was issued in 1988
- Second version was issued in 1993
- Third and the latest version was issued in 1995

Each version of X.509 has different structure,

Let’s see each one in detail.

X.509 - Version 1

- Version: Differentiates among successive versions of the certificate format
- Serial number: An integer value unique within the issuing CA that is unambiguously associated with this certificate.
- Algorithm: The algorithm used to sign the certificate together with any associated parameters.



Version 1

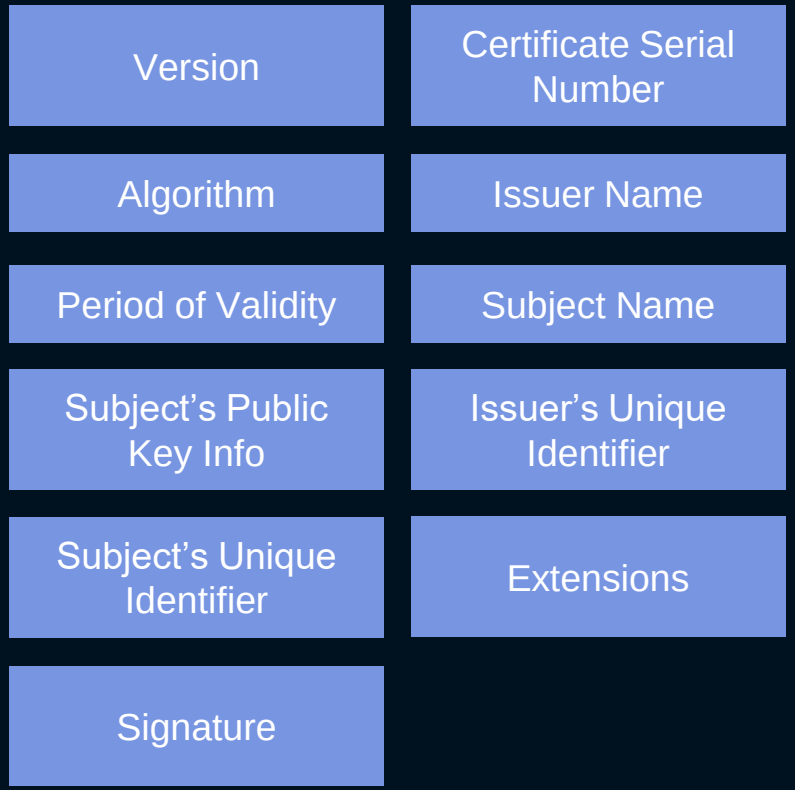
X.509 - Version 2

- Issuer name: 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.

Version 2

X.509 - Version 3

- 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.



Version 3

X.509 - Version 3 (Continued)

- Subject Unique Identifier: An optional-bit string field used to identify uniquely the subject.
- Extensions: A set of one or more extension fields. Extensions were added in version 3.
- Signature: It contains the hash code of the other fields encrypted with the CA's private key.

X.509 Certificate Notation

X.509 Notation

Notation for Certificate: **CA <<A>> = CA {V, SN, AI, CA, UCA, A, UA, Ap, TA}**

CA <<A>> = the certificate of user A issued by certification authority CA.

V = version of the certificate.

SN = serial number of the certificate.

AI = identifier of the algorithm used to sign the certificate.

CA = name of certificate authority.

UCA = optional unique identifier of the CA.

A = name of user A.

UA = optional unique identifier of the user A.

Ap = public key of user A.

TA = period of validity of the certificate.

Obtaining A User Certificate

Obtaining A User Certificate

User certificates generated by a Certificate Authority(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 CA can modify the certificate without this being detected.
- Since certificates are *unforgeable*, they can be placed in a directory without the need for the directory to make special efforts to protect them.

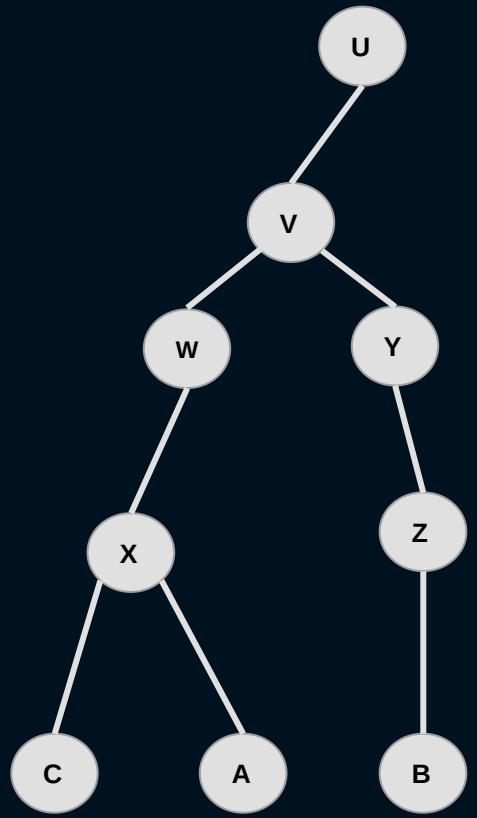
Obtaining A User Certificate (Continued)

- All users under the same CA have a common trust of that CA.
- Hence users A and B under the same CA can communicate with each other with assurance that messages will be secure from eavesdropping and that messages signed with user's private key are unforgeable.
- However with many users, it may be more practical for there to be a number of CAs, each of which securely provides its public key to some fraction of the users. This is where chain authentication plays its role in authenticating users.

Chain Authentication

Chain Authentication

- In this example, user A is trying to communicate with user B. But to communicate with B, A has to authenticate himself. The Problem here is that A and B are under different Certificate Authorities X and Z respectively.
- For authentication, A needs B's certificate. But A and B cannot exchange certificate directly.
- But X and A have exchanged certificate. Then X and W have exchanged certificate. Then W and V have exchanged certificates, and so on until we reach B.
- Certificate Exchange Path: X << W>> W << V>> V <<Y>> Y <<Z>> Z <<B>> ➔ X<<B>>
- This path shows A that B is authenticated by certificate authority Z.



Revocation of Certificates

Revocation of Certificates

Referring slide 10 that each certificate includes a period of validity, much like a credit card. Typically, a new certificate is issued just before the expiration of the old one. In addition, it may be desirable on occasion to revoke a certificate before it expires, for one of the following reasons:

- The user's private key is assumed to be compromised.
- The user is no longer certified by this CA. Reasons for this include that the subject's name has changed, the certificate is superseded, or the certificate was not issued in conformance with the CA's policies.
- The CA's certificate is assumed to be compromised.

Certification Path Constraints

Certification Path Constraints

These extensions allow constraint specifications to be included in certificates issued for CAs by other CAs. The constraints may restrict the types of certificates that can be issued by the subject CA or that may occur subsequently in a certification chain. The extension fields in this area include:

- Basic Constraints: Indicates if the subject may act as a CA. If so, a certification path length constraint may be specified.
- Name Constraints: Indicates a name space within which all subject names in subsequent certificates in a certification path must be located.
- Policy Constraints: Specifies constraints that may require explicit certificate policy identification or inhibit policy mapping for the remainder of the certification path.

Conclusion

Conclusion

- Digital Certificates are better and more secure way of authentication than passwords.
- X.509 is widely accepted digital certificate.
- X.509 is a standard format for Public Key Certificates. X.509 standard, which defines the format of public key infrastructure (PKI) certificates.
- It is used to verify identity and manage security in internet communication.

Thank You