X-509
CERTIFICATE
&
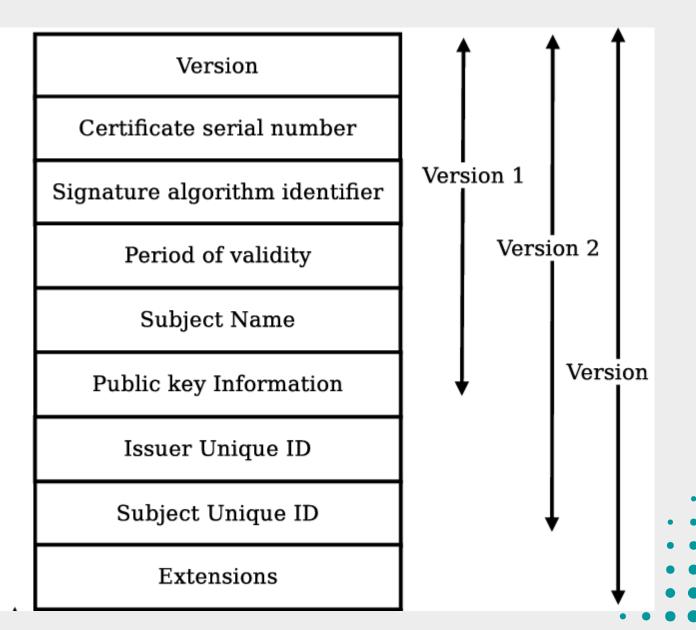## PUBLIC KEY
INFRASTRUCTURE

X-509 certificate

X.509

* X-509 AUTHENTICATION SERVICE:

-digital certificate accepted internationally

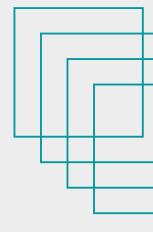-does not generate any keys.

-but provides a way to access public keys.
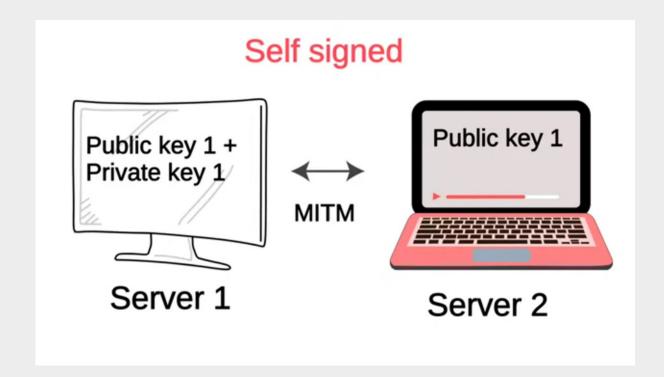
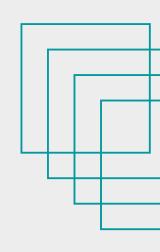There are Several elements in X509 certificate

it has (3) Versions
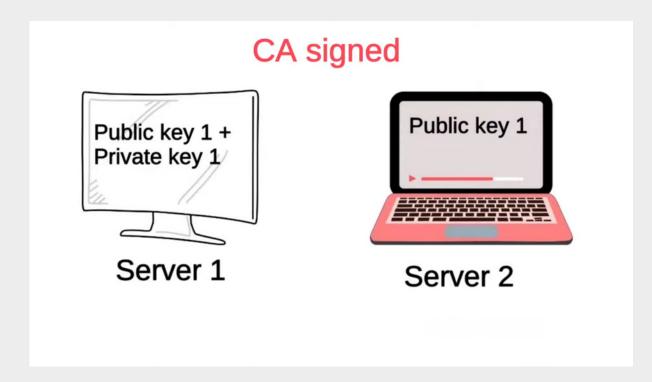
Version
Certificate serial number
Signature algorithm identifier
Period of validity
Subject Name
Public key Information
Issuer Unique ID
Subject Unique ID
Extensions

Version 1

Version 2

Version

Self signed

Public key 1 + Private key 1

Server 1

MITM

Public key 1

Server 2

CA signed

Server 1 — Public key 1 + Private key 1

Server 2 — Public key 1

Public
key
infrastructure

Components of PKI

PUBLIC KEY INFRASTRUCTURE

1. CERTIFICATE MANAGEMENT SYSTEM

2. DIGITAL CERTIFICATES

3. VALIDATION AUTHORITY

4. CERTIFICATION AUTHORITY

5. REGISTRATION AUTHORITY

6. END USER

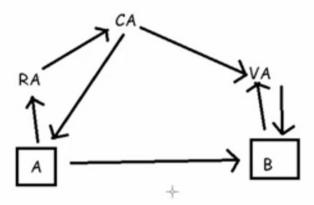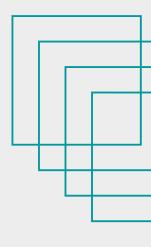# PUBLIC KEY INFRASTRUCTURE

Components of PKI:
1. Certificate Management System
2. Digital Certificates
3. Validation Authority
4. Certification Authority
5. Registration Authority
6. End User

Thank You