# UNIT-3

Q) Write a short note on digital signature.

A) A digital signature is a cryptographic technique used to provide authentication, integrity and non-repudiation for digital messages or documents

It acts like an electronic form of a handwritten signature but is more secure because it uses public-key cryptography

how it works:

1. Sender generates a hash of message
2. This hash is encrypted with sender's private key, creating digital signature
3. The receiver decrypts the signature using sender's public key to verify hash
4. If both hashes match, the message is verified

| Features: | Applications: |
|---|---|
| Authentication | email security |
| Integrity | software distribution |
| non-repudiation | E-commerce |
| | Digital certificates |
| | legal documents |

Scanned with OKEN Scanner

There is only ONE Language
The Language of the HEART
...Bhagwan Sri Sathya Sai Baba

Q) Steps & advantages of HMAC

OR

Q) Explain HMAC algorithm with detail.

HMAC – Hash based message authentication code

→ It is mechanism used to provide message authentication and integrity using a secret key & hash function

→ It is widely used with hashfunctions like SHA-256, SHA-1, MD5.

→ HMAC ensures that:
- message is not modified
- Sender is authenticated

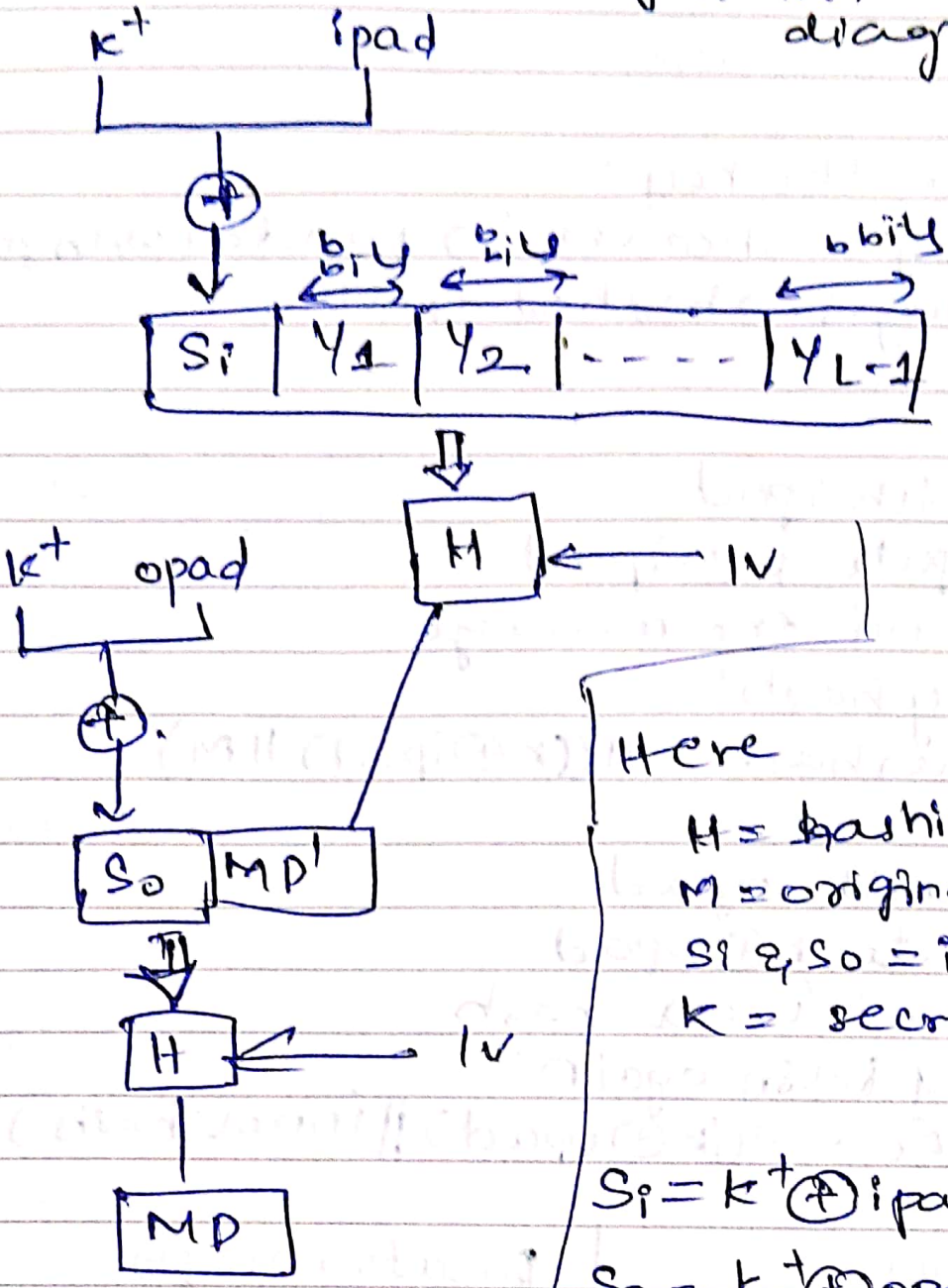
→ It combines a secret key with message using two constants:
- ipad (inner padding)
- opad (outer padding)

Features
1) keyed hashing i- secret key & hash function
2) Inner & outer hashing
3) provides integrity & authentication
4) resistant to cryptographic attacks
5) Efficient & widely used

Scanned with OKEN Scanner

There is only ONE RELIGION
The Religion of Love.
...Bhagwan Sri Sathya Sai Baba

# HMAC algorithm diagram




Here

H = hashing function
M = original message
Si & So = input & output
K = secret key

$S_i = K^+ \oplus ipad$

$S_o = K^+ \oplus opad$

$MD' = H(S_i || M)$

$MD = H(S_o || MD')$

(or)

$MD = H(S_o || H(S_i || m))$

Scanned with OKEN Scanner

Steps:

① prepare the key:
- If key is shorter → padded with zeros
- If longer → hashed first

② XOR with ipad
- compute K ⊕ ipad
- append the message
- apply hash:
  Innerhash = H((K ⊕ ipad) || M)

③ XOR with opad
- compute K ⊕ opad
- append inner hash
- apply hash again:
  HMAC = H((K ⊕ opad) || inner hash)

| Advantages | Disadvantages |
|---|---|
| • High security | • no confidentiality |
| • Fast & efficient | • key management required |
| • Flexible | |
| • Resistant to attacks | |
| • keyed hash | |

Scanned with OKEN Scanner

9) Explain how digital signatures (DS) provide authentication with application example

→ DS is a cryptographic technique used to verify the identity of sender & ensure that message has not changed

→ It uses public key cryptography

how authentication works:-

(1) sender creates a hash (message digest) of message using such as SHA-256

(2) hash is then encrypted using sender's private key

(3) signature is attached to message & sent to receiver

(4) receiver decrypts the signature using sender's public key

(5) If decrypted digest matches the hash of received message:

- message truly came from sender → authenticated
- message was not modified → integrity

Scanned with OKEN Scanner

M → message
H → hash

All are ONE : Be alike to EVERYONE
...Bhagwan Sri Sathya Sai Baba

Sender

M → H → Digest

encrypt with sender's private key

digital signature

receiver

M → H → New digest

signature → decrypt signature using sender's public key

compare digests

If both matched → sender is authenticated

Application Example:
Secure Email (PGP / S/mime)

---

Q) Advantages of kerbos
1) Strong authentication
2) No passwords sent over n/w
3) single sign on (SSO)
4) Mutual authentication
5) Efficient & fast
6) Widely supported
7) prevent replay attack

GOD + Desire = MAN
Man - Desire = GOD

...Bhagwan Sri Sathya Sai Baba

HPL

9) What is kerberos? explain hypothetical dialogues of kerberos V4.

Kerberos is a network authentication protocol designed to provide secure user authentication in distributed systems

It uses secret key cryptography & trusted authentication server to verify the identity of users & services

→ It involves a client (C)
Authentication server (AS)
Ticket Granting server (TGS)
Service server (V)

Hypothetical dialogues

(1) C → AS: "I am Alice. Get a ticket-Granting ticket (TGT)"

(2) AS → C: "Here is your TGT & session key"

(3) C → TGS: "Here is my TGT. Give me a service ticket for a file server".

(4) TGS → C: "Here is the service ticket and session key for the server"

Scanned with OKEN Scanner

(5) C → V: "Here is my service ticket and authenticator

(6) V → C: "verified! You can access the service"

Features
1) Strong authentication
2) Single sign-on
3) Mutual authentication
4) Centralized management
5) Ticket-based Access

---

Q) Requirements of a secure hash function

A secure hash function takes an i/p of arbitary length and produces a fixed length hash

(1) Deterministic
(2) Fast computation
(3) Pre-image resistance
(4) Second pre image resistance
= find $M2 \neq M1$
such that
$H(M2) = H(M1)$

Scanned with OKEN Scanner

(5) Collision Resistance:
$H(M_1) = H(M_2)$

(6) Avalanche effect

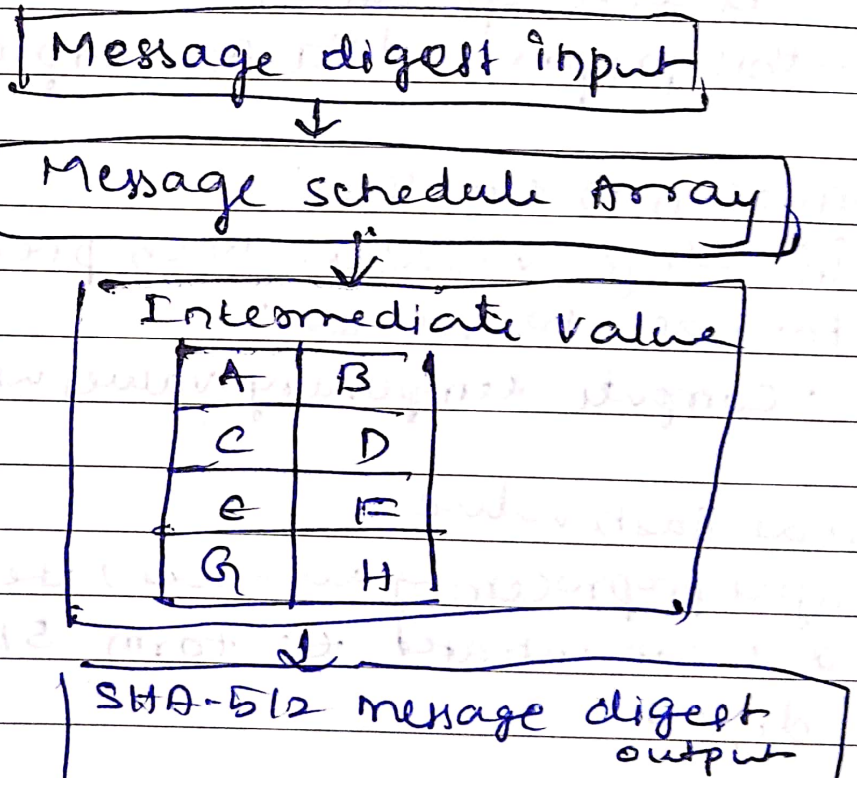
(7) Fixed O/P length

(8) Security against cryptanalysis

Q) Explain SHA-512 message digest with flowchart & intermediate steps.

SHA-512 is a cryptographic hash function that processes i/p data into fixed-512-bit digest

→ It is widely used in digital signatures, certificates and data integrity.




Scanned with OKEN Scanner

# Steps in SHA-512

- **Preprocessing:**
  - convert input message into binary
  - append a single 1 bit, followed by 0s until the length = 896 (mod 1024)
  - Append a 128 bit representation of original message length
- **parsing:**
  - divide padded message into 1024 bit blocks
  - Each block is further split into sixteen 64-bit words
- **Message schedule:**
  - expand 16 words into 80 words using bitwise operations
  - this prepares data for compression function
- **compression function:**
  - initialize variables with predefined constants
  - For each 80 rounds:
    - Compute temporary values using logical functions
- **Final Hash value:**
  after preprocessing all blocks, the eight variables are concatenated to form 512 bit digest

Scanned with OKEN Scanner

...Bhagwan Sri Sathya Sai Baba

## Intermediate Eg:

i/p = "hello world"

1) Binary conversion → ASCII to binary

2) Padding → append 1 + 0s + 128 bit length

3) Block Division → 1024 bit block created

4) Message schedule → 16 words expanded to 80 words

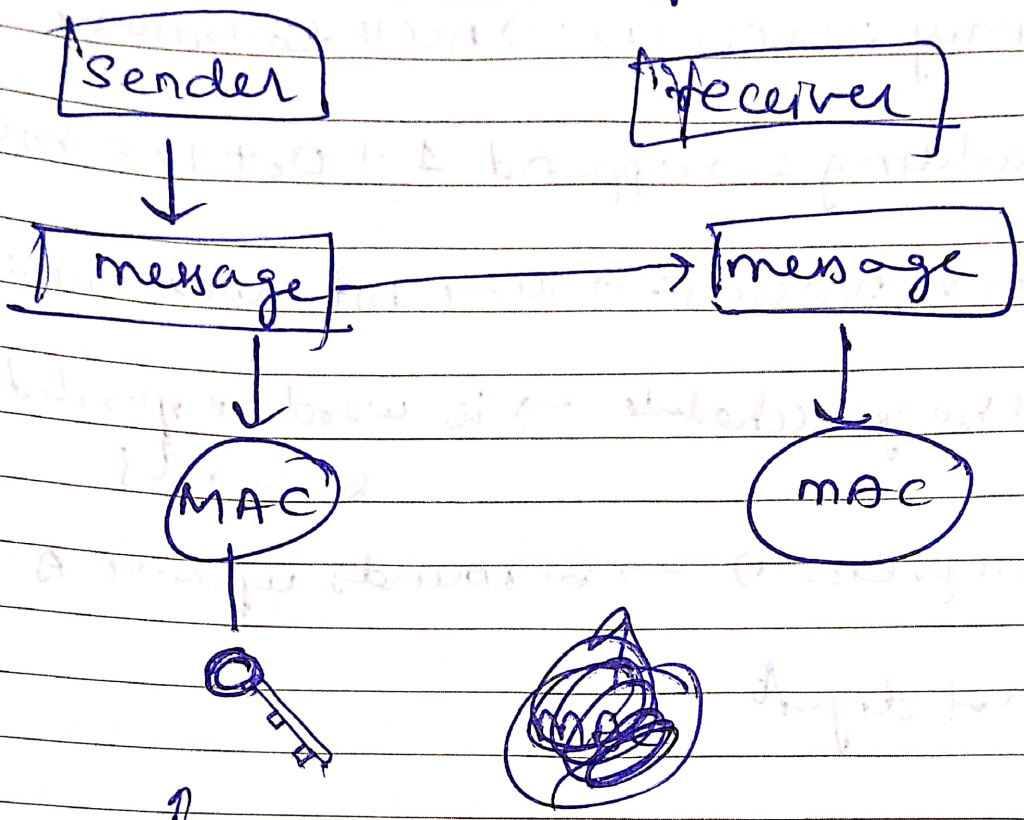
5) compression → 80 rounds update A-H

6) Final digest

Why fear when I am here.
I shall Guide You and Guard You
...Bhagwan Sri Sathya Sai Baba

Q) Basic uses of MAC with diagram

Message authentication codes (MACs) are used to verify the integrity & authenticity of message using a shared secret key.




Basic use of MAC

1) message integrity
2) " authentication
3) secure communication
4) digital transaction
5) software updates

Scanned with OKEN Scanner

## How MAC works

1) Sender side

- i/p : message + secret key
- uses a MAC algorithm to generate a MAC value
- sends both message & MAC to receiver

2) Receiver side

- receives the message & MAC
- recomputes MAC using same algorithm & secret key
- compares the received MAC with computed one
- If they match, the message is authenticated.

## Common MAC algorithms:

1) HMAC — hash based using SHA or MD5

2) CMAC — cipher based MAC using block cipher

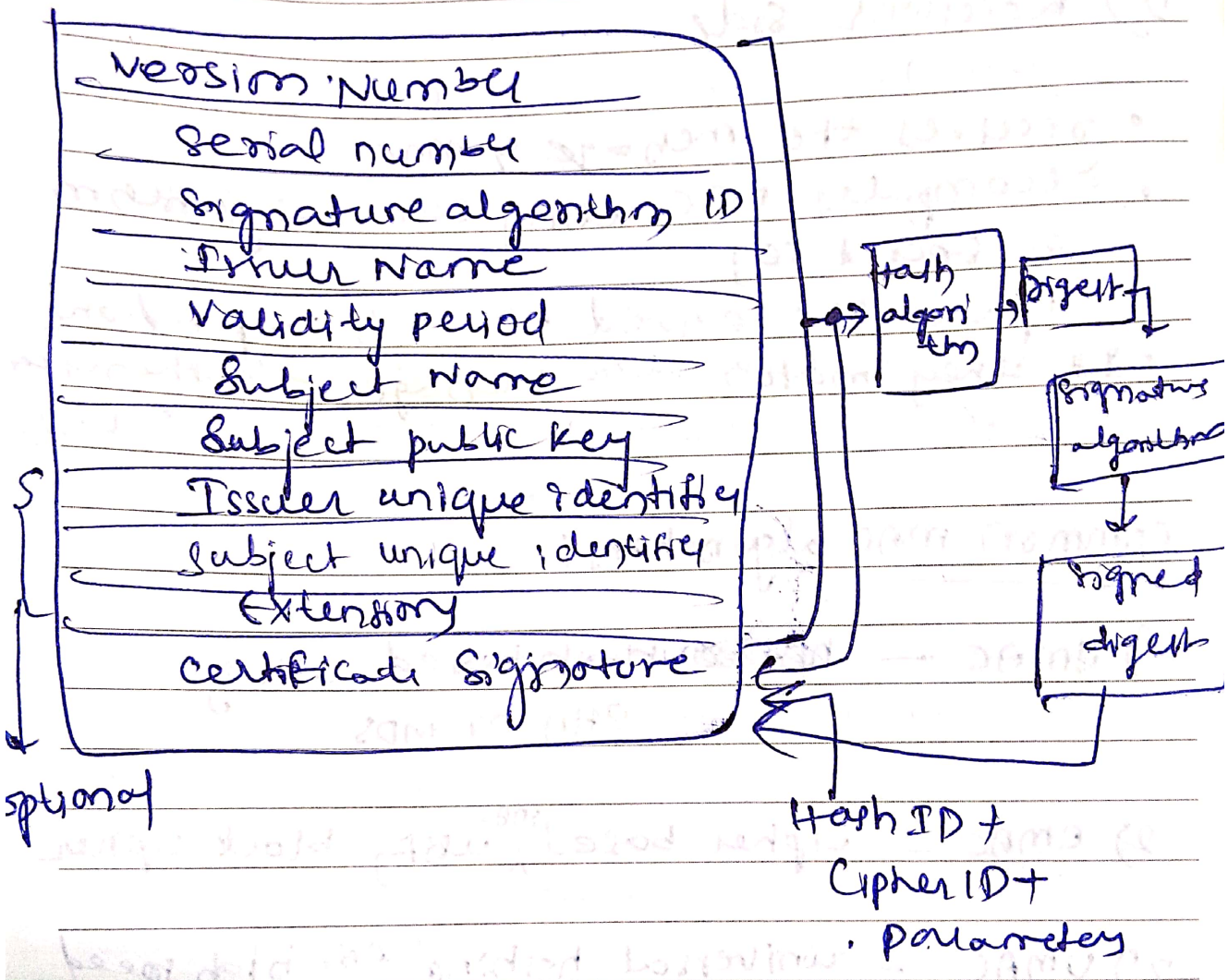
3) UMAC — universal hashing for high speed MAC

Scanned with OKEN Scanner

Q) Describe general form of X.509 certificate.

→ X.509 certificate is a digital certificate used to authenticate the identity of an entity in a network

→ Commonly used in SSL/TLS, digital signature & PKI




Scanned with OKEN Scanner

HPL

9) Key management & Distribution: Symmetric & Asymmetric methods

Key management is the process of generating, distribution, storing, using and replacing cryptographic key securely.

depends on confidentiality & integrity of keys.

1) Symmetric key management

Both sender & receiver share same key for encryption & decryption

key distribution problem: the shared key must be transmitted securely otherwise attackers can intercept it

method.

1) manual key distribution
2) automatic " "

| Advantage | Disadvantage |
|---|---|
| • Fast encryption/decryption<br>• less computational overhead | • compromise of one key affect both<br>• challenging in large n/w |

Scanned with OKEN Scanner

## 2) Asymmetric key management

Uses a key pair; a public key & private key
- public key → encryption
- private key → decryption

Methods:
1) PKI (public key infrastructure):
   - ensures secure key distribution & verification
   - certificates issued by certificate Authority (CA) bind public key to user identity.

2) Diffie-Hellman key exchange
   - allows two parties to agree on shared secret key over insecure channel
   - no prior secret key is needed

Advantages
- provides authentication & non-repudiation
- solves key distribution problem

Disadvantages
- slower than symmetric
- require more computational resources

Public Key Infrastructure and X.509 authentication services.

Here's a **clear, exam-friendly answer** on **Public Key Infrastructure (PKI) and X.509 Authentication Services** suitable for 10 marks:

---

## ⭐ Public Key Infrastructure (PKI)

**PKI** is a framework that provides **secure communication, authentication, and key management** in a network using **public-key cryptography**.

It ensures that entities can:

- Verify identities (**authentication**)
- Exchange keys securely (**confidentiality**)
- Sign messages digitally (**integrity and non-repudiation**)

---

### Components of PKI

1. **Certificate Authority (CA)**
   - Trusted third party that **issues, verifies, and revokes digital certificates.**

+ Ask anything

ChatGPT can make mistakes. Check important info. See Cookie Preferences.



Scanned with OKEN Scanner

Upgrade for free ×

- Sign messages digitally (integrity and non-repudiation)

## Components of PKI

1. Certificate Authority (CA)
   - Trusted third party that issues, verifies, and revokes digital certificates.
2. Registration Authority (RA)
   - Verifies user identity before certificate issuance.
3. Digital Certificates
   - Bind a public key to an identity (person, server, organization).
   - Example: X.509 certificate.
4. Certificate Repository
   - Stores issued certificates and Certificate Revocation Lists (CRLs).
5. Key Management System
   - Handles key generation, distribution, storage, renewal, and revocation.

## ⭐ X.509 Authentication Services

X.509 is the standard for digital certificates in PKI. It provides authentication services by binding

Scanned with OKEN Scanner

Upgrade for free ×
Share

# X.509 Authentication Services

**X.509** is the standard for **digital certificates** in PKI. It provides authentication services by binding public keys to entities.

## Authentication Process Using X.509

1. **Certificate Issuance**
   - CA verifies identity of entity and issues an **X.509 certificate** containing:
     - Version, Serial Number
     - Signature Algorithm
     - Issuer Name
     - Validity Period
     - Subject Name
     - Subject Public Key Info
     - Extensions & CA Signature
2. **Certificate Verification**
   - The receiver verifies:
     - Certificate signature using **CA's public key**
     - Validity period
     - Revocation status via CRL
3. **Authentication Outcome**
   - Ensures the public key belongs to the claimed entity

+ Ask anything

ChatGPT can make mistakes. Check important info. See Cookie Preferences.

ENG
IN

Scanned with OKEN Scanner

- CA verifies identity of entity and issues an **X.509 certificate containing:**
  - Version, Serial Number
  - Signature Algorithm
  - Issuer Name
  - Validity Period
  - Subject Name
  - Subject Public Key Info
  - Extensions & CA Signature

2. **Certificate Verification**
   - The receiver verifies:
     - Certificate signature using **CA's public key**
     - Validity period
     - Revocation status via CRL
3. **Authentication Outcome**
   - Ensures **the public key belongs to the claimed entity**
   - Provides **integrity and trust** in secure communications

## PKI + X.509 Workflow Diagran ↓

pascal

+ Ask anything

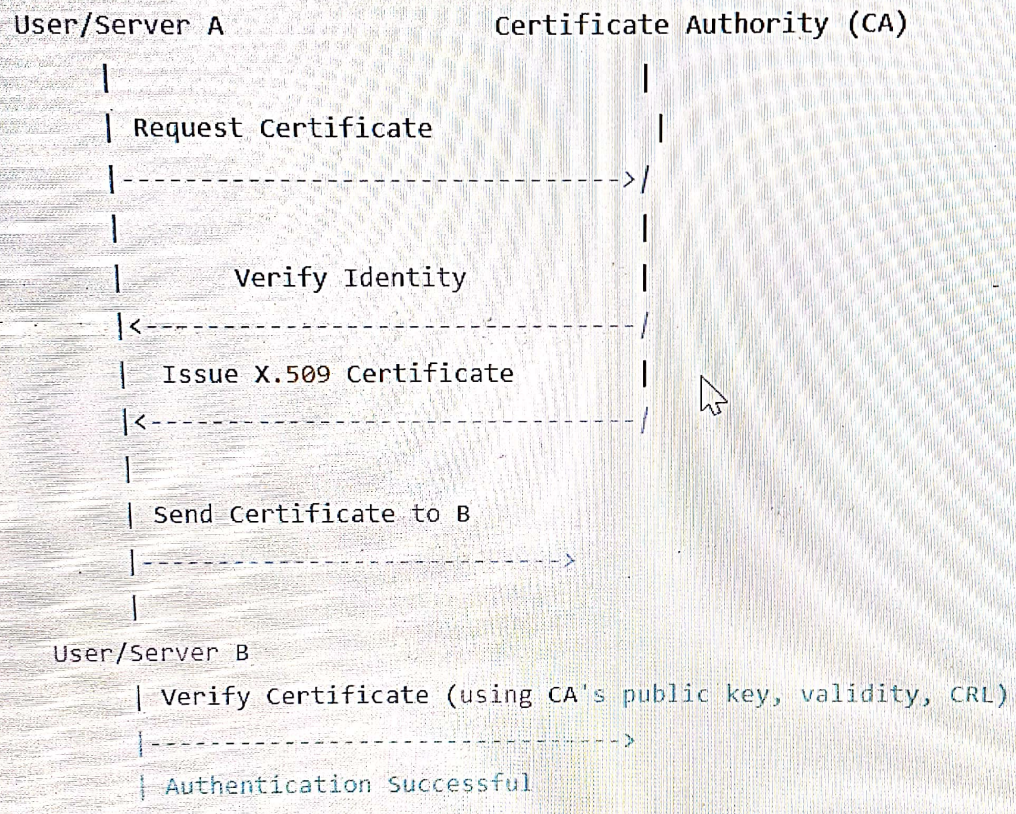
ChatGPT can make mistakes. Check important info. See Cookie Preferences.

Scanned with OKEN Scanner

Upgrade for free ×

# PKI + X.509 Workflow Diagram

pgsql




## Short 5-Mark Summary

Ask anything

ChatGPT can make mistakes. Check important info. See Cookie Preferences.

Scanned with OKEN Scanner