WHAT IS DIGITAL SIGNATURE
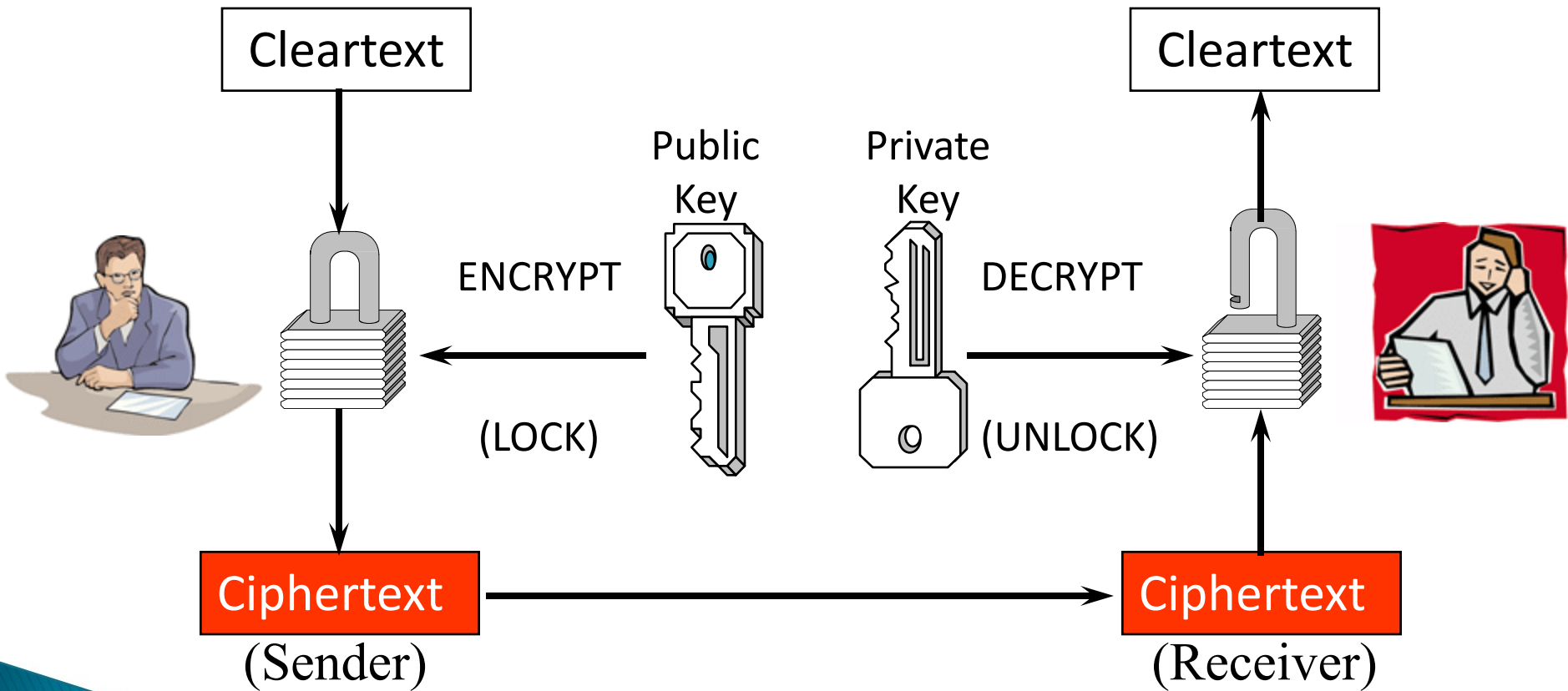
CRYPTOGRAPHY
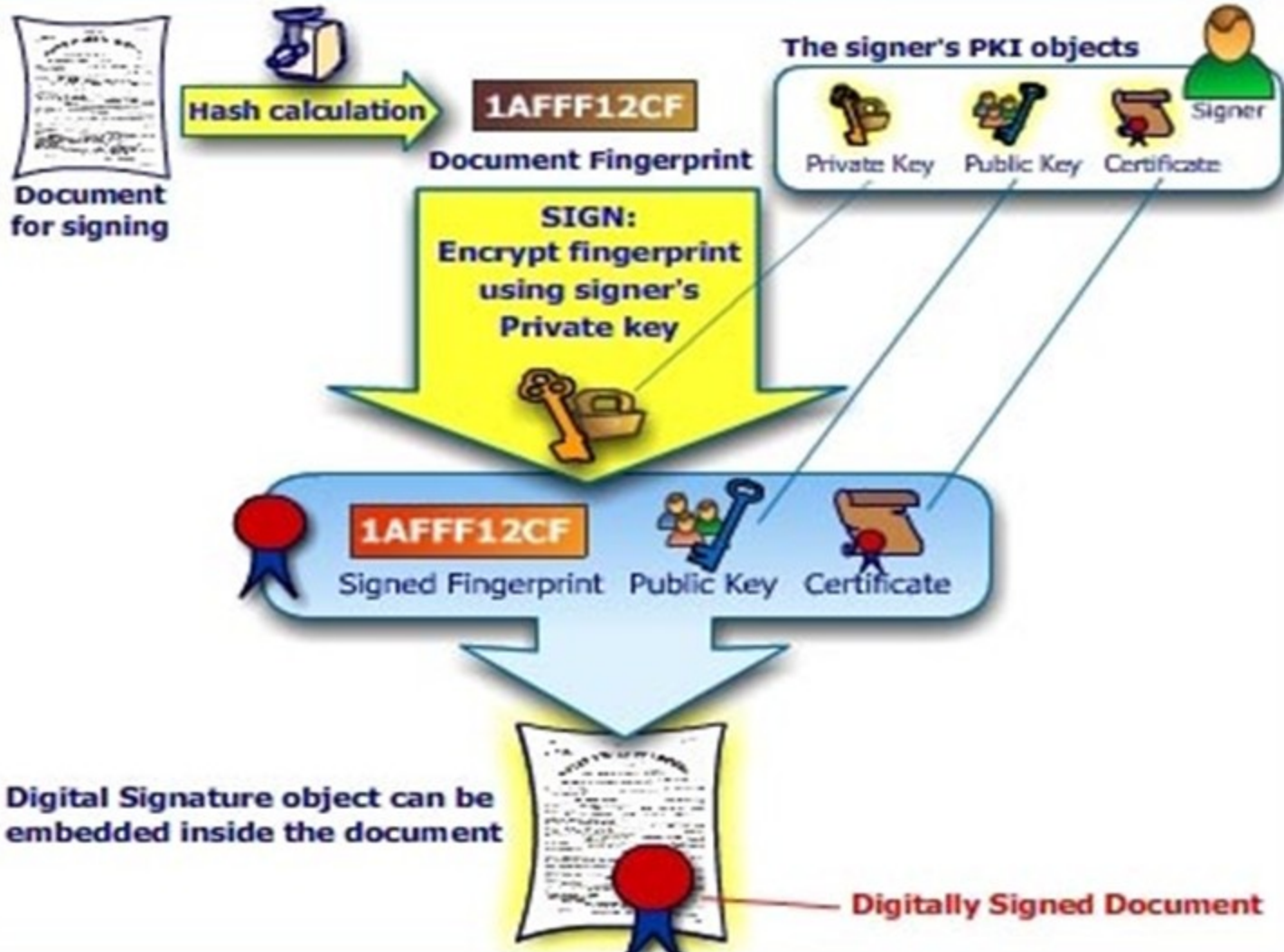
ALICE → ENCRYPTION PROCESS → PZMSY → DECRYPTION PROCESS → ALICE

SYMMETRIC KEY CRYPTOGRAPHY

Message

Message

"Secret" Key

ENCRYPT

DECRYPT

(LOCK)

(UNLOCK)

(Sender)

(Receiver)

Ciphertext

Ciphertext
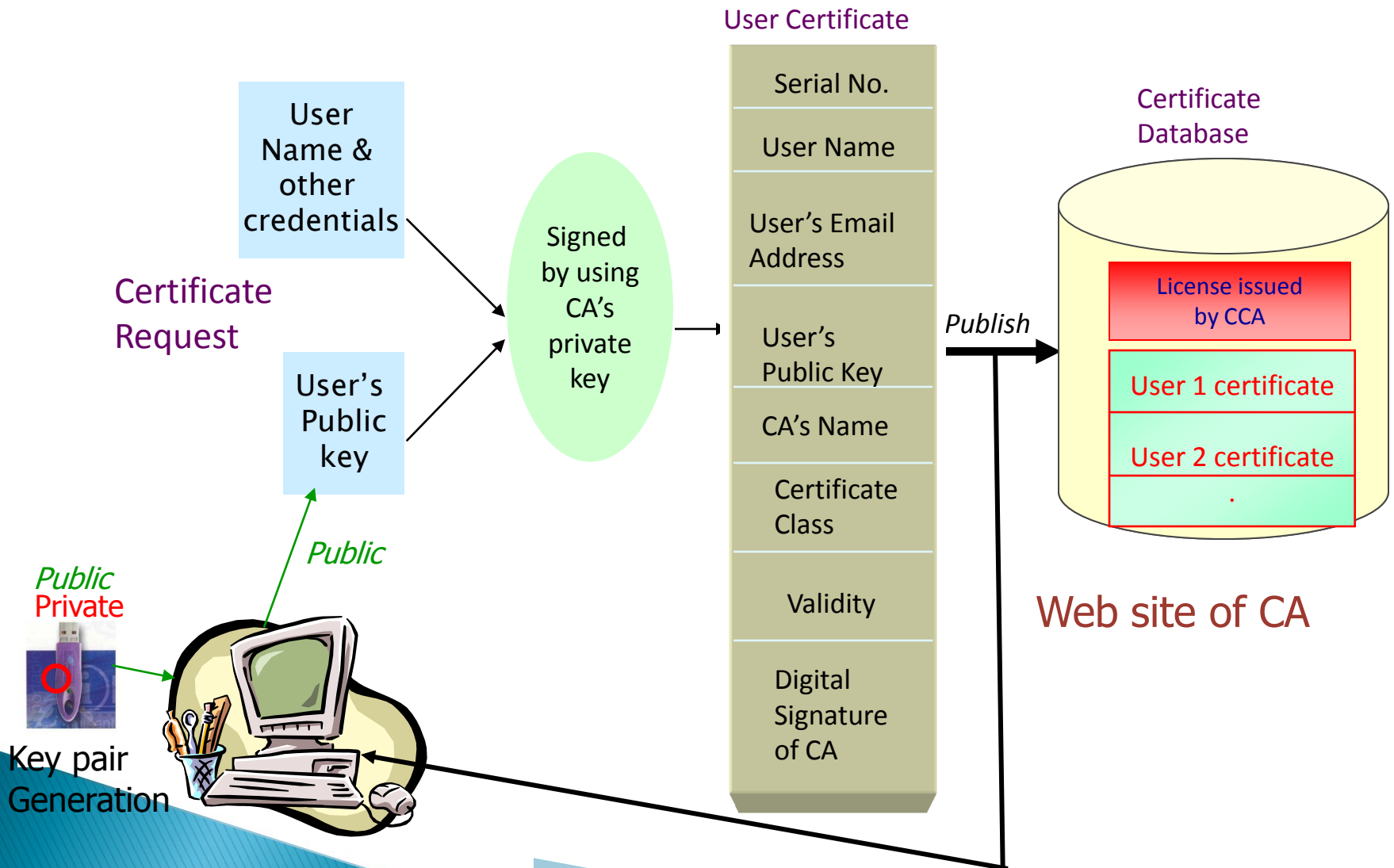
DIGITAL SIGNATURE

DIGITAL CERTIFICATE

- Digital Identity that establishes your credentials when doing business or other transactions on the Web

- Issued by a Certifying Authority (CA)

- Contains your name, serial number, expiration dates, public key, signature of CA

CERTIFYING AUTHORITY

- Trusted Third Party
- An organization which issues public key certificates
- Assures the identity of the parties to whom it issues certificates
- Maintains online access to the public key certificates issued

PUBLIC KEY CERTIFICATION

Certificate Request

User Name & other credentials

User's Public key

Signed by using CA's private key

User Certificate

Serial No.
User Name
User's Email Address
User's Public Key
CA's Name
Certificate Class
Validity
Digital Signature of CA

Publish

Certificate Database

License issued by CCA

User 1 certificate

User 2 certificate

.

Web site of CA

Public

Public
Private

Key pair Generation

DIGITAL SIGNATURE STANDARDS

- Uses secure hash algorithm
- Condenses message to 160 bit
- Key size 512-1024 bits
- Proposed by NIST in 1991
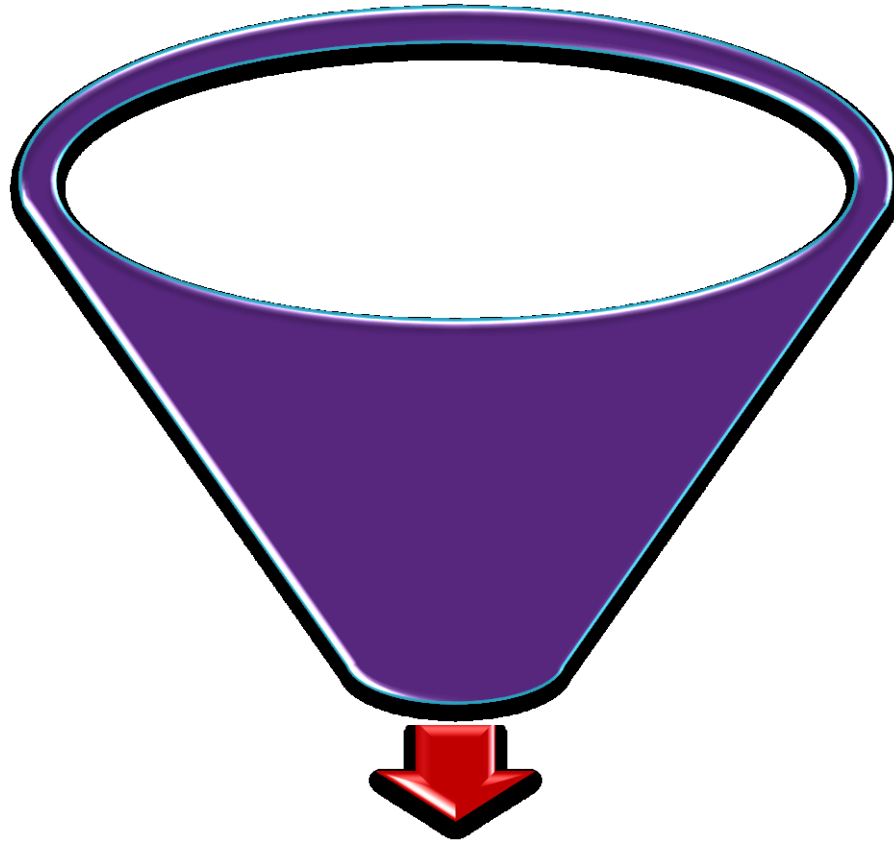- Adopted

PRIVATE KEY PROTECTION

Soft Token

Smart card

Hardware tokens

WHY DIGITAL SIGNATURE

DIGITAL SIGNATURE

Paper signatures v/s Digital Signatures

Parameter	Paper	Electronic
Authenticity	May be forged	Can not be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	a. Any computer user b. Error free

V/s

THANKYOU