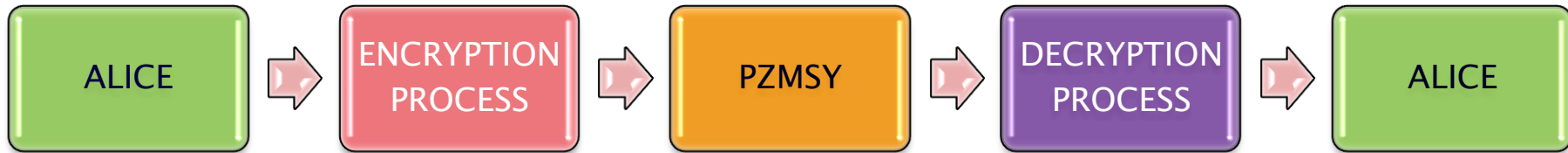


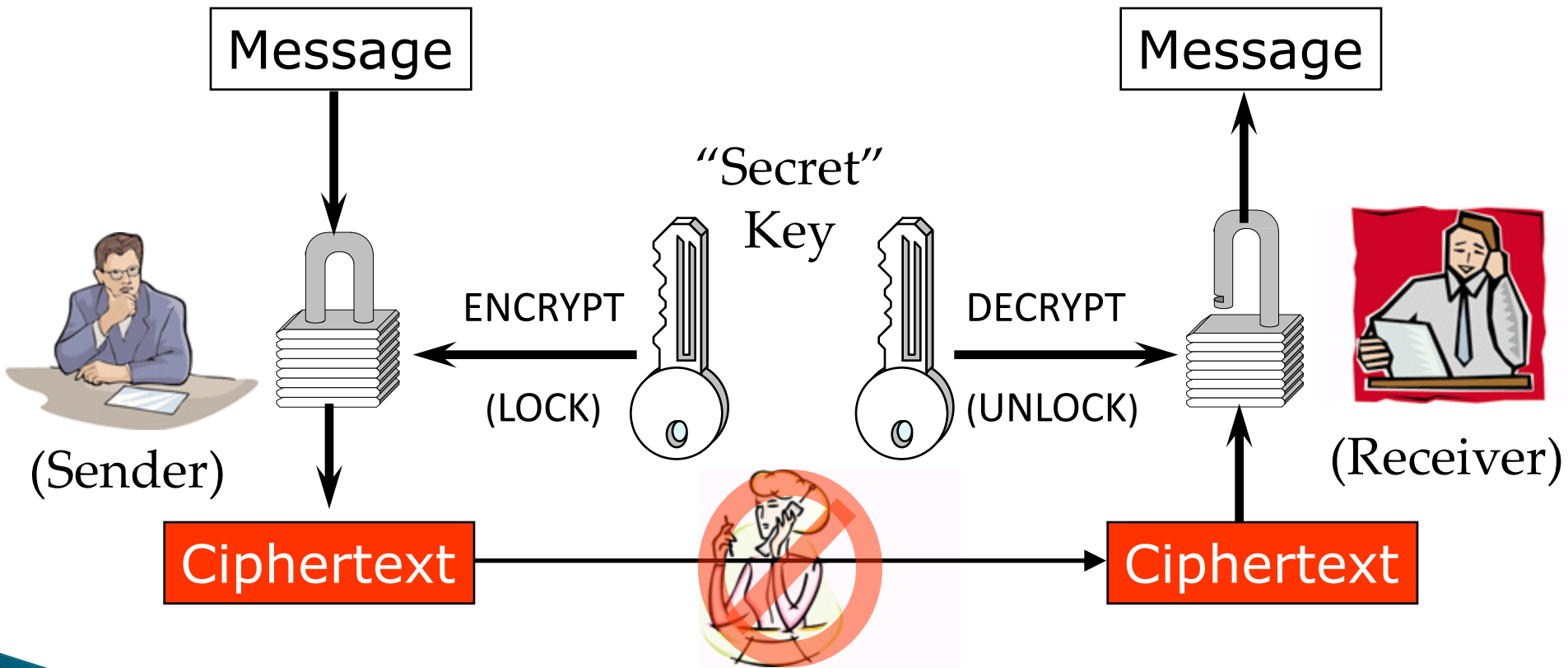
WHAT IS DIGITAL SIGNATURE



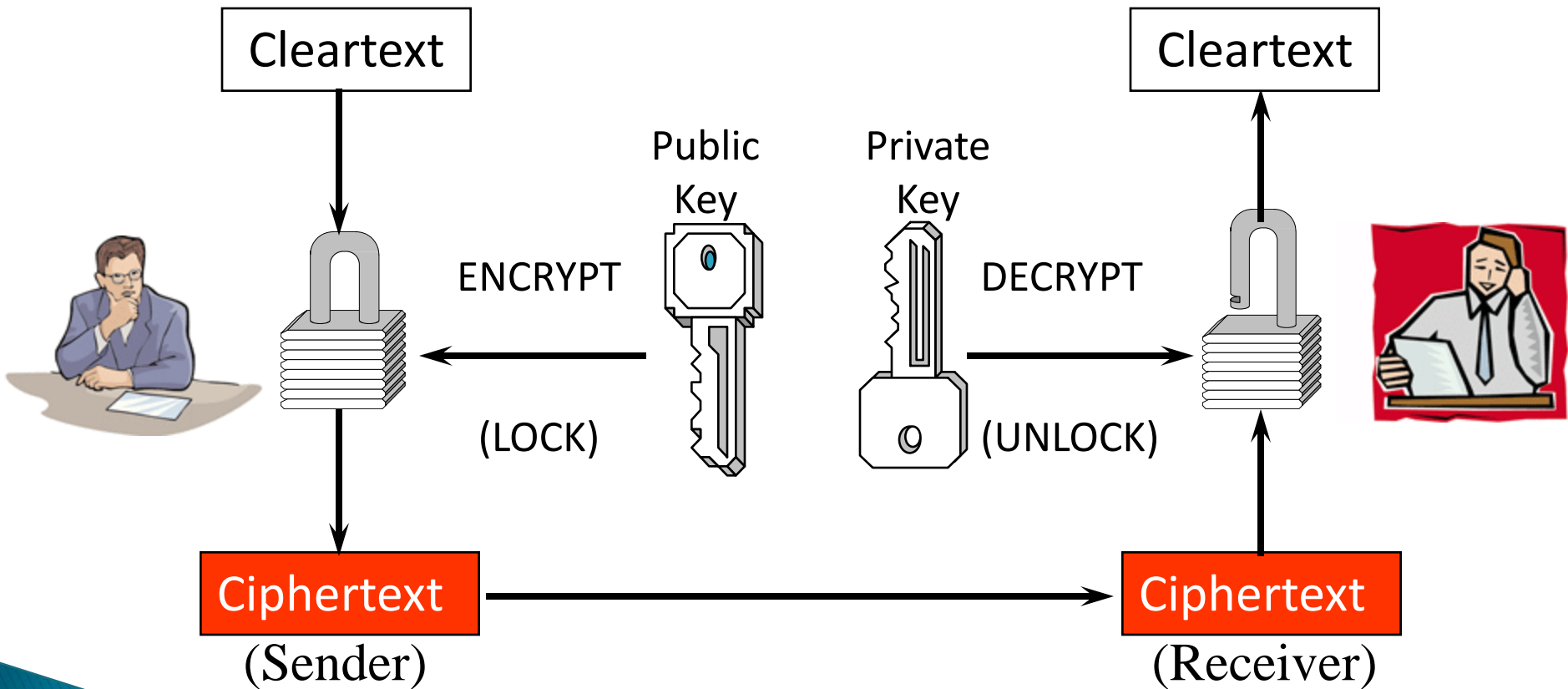
CRYPTOGRAPHY



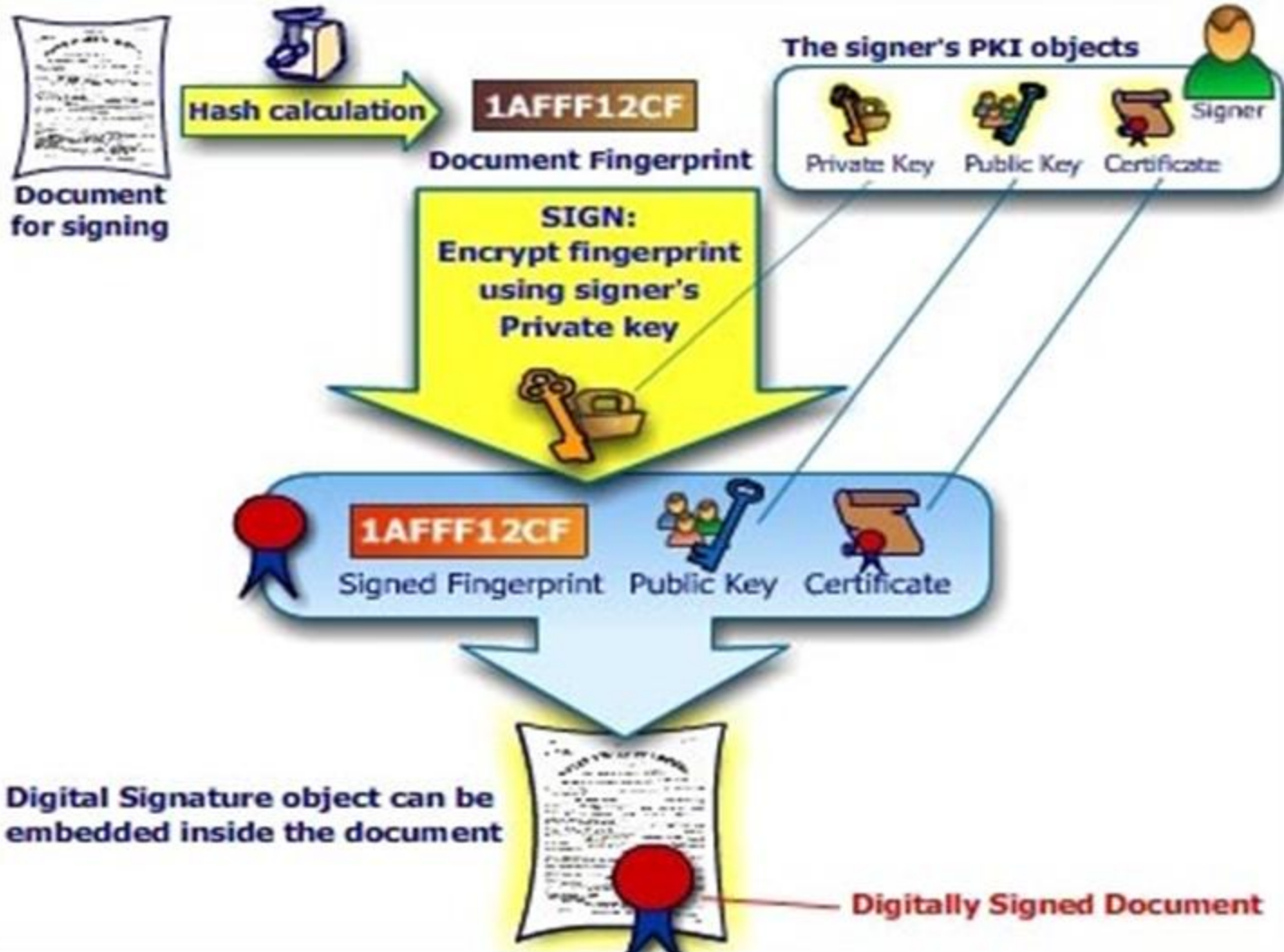
SYMMETRIC KEY CRYPTOGRAPHY




ASYMMETRIC KEY CRYPTOGRAPHY




DIGITAL SIGNATURE



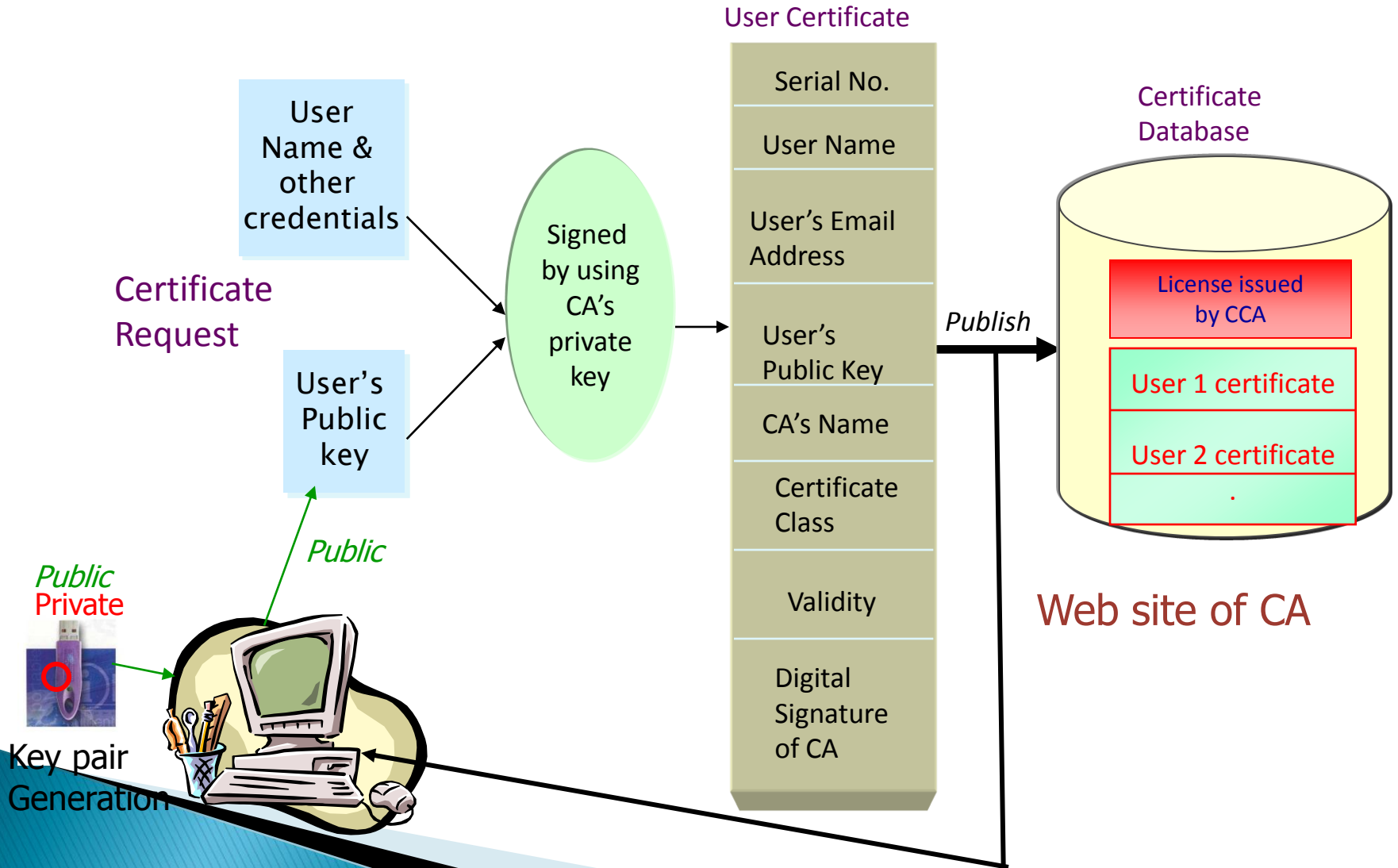
DIGITAL CERTIFICATE

- 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
- 

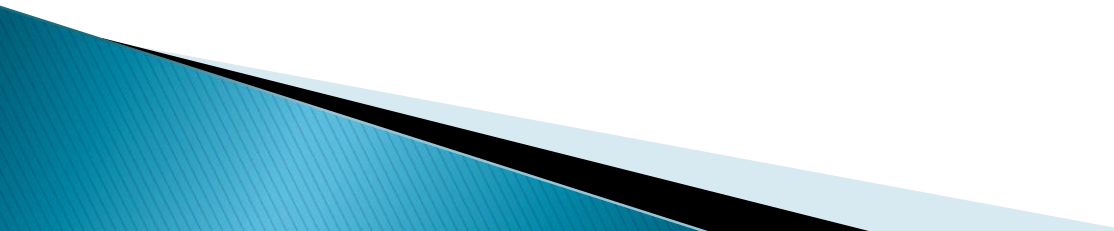
CERTIFYING AUTHORITY

- ▶ 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



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

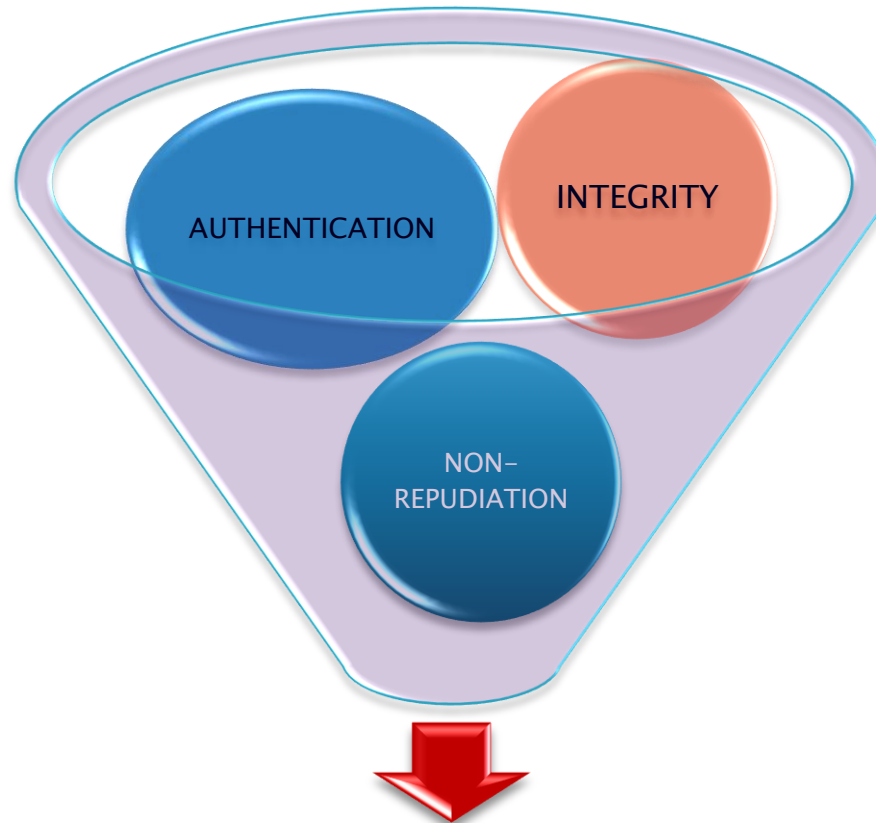


Hardware tokens



Smart card

WHY DIGITAL SIGNATURE



DIGITAL SIGNATURE

Paper signatures v/s Digital Signatures



v/s



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