Introduction

- Used for communication to verify
- Authentication of sender/data origin
- Integrity of the message received
- Non-repudiation private key for E & public key for D
- Identification of doc or message etc.
- For interchanging data electronically

Implementation

- Scheme has the following 3 algorithm

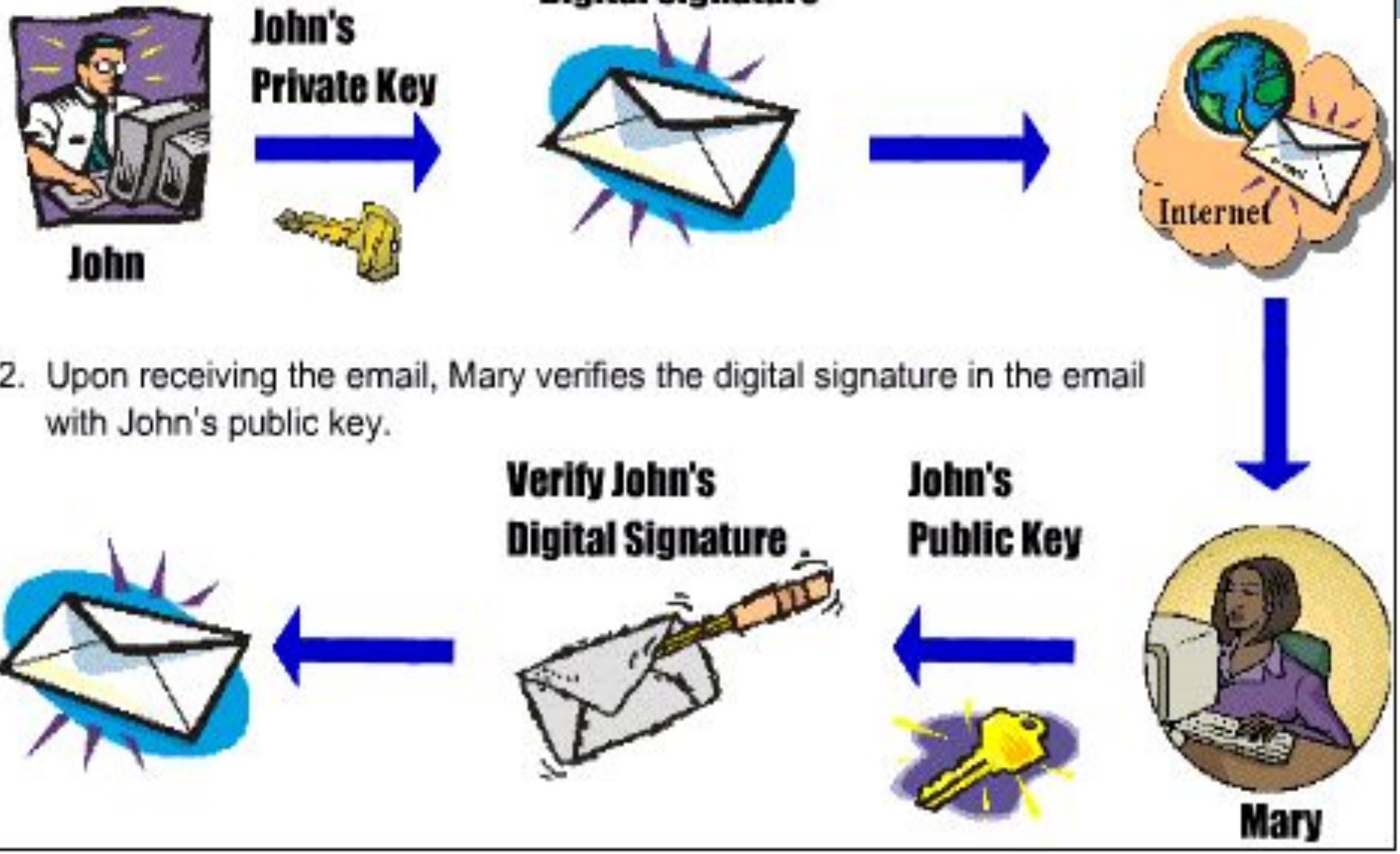
1. Key generation
2. Signing
3. Verification

- It includes

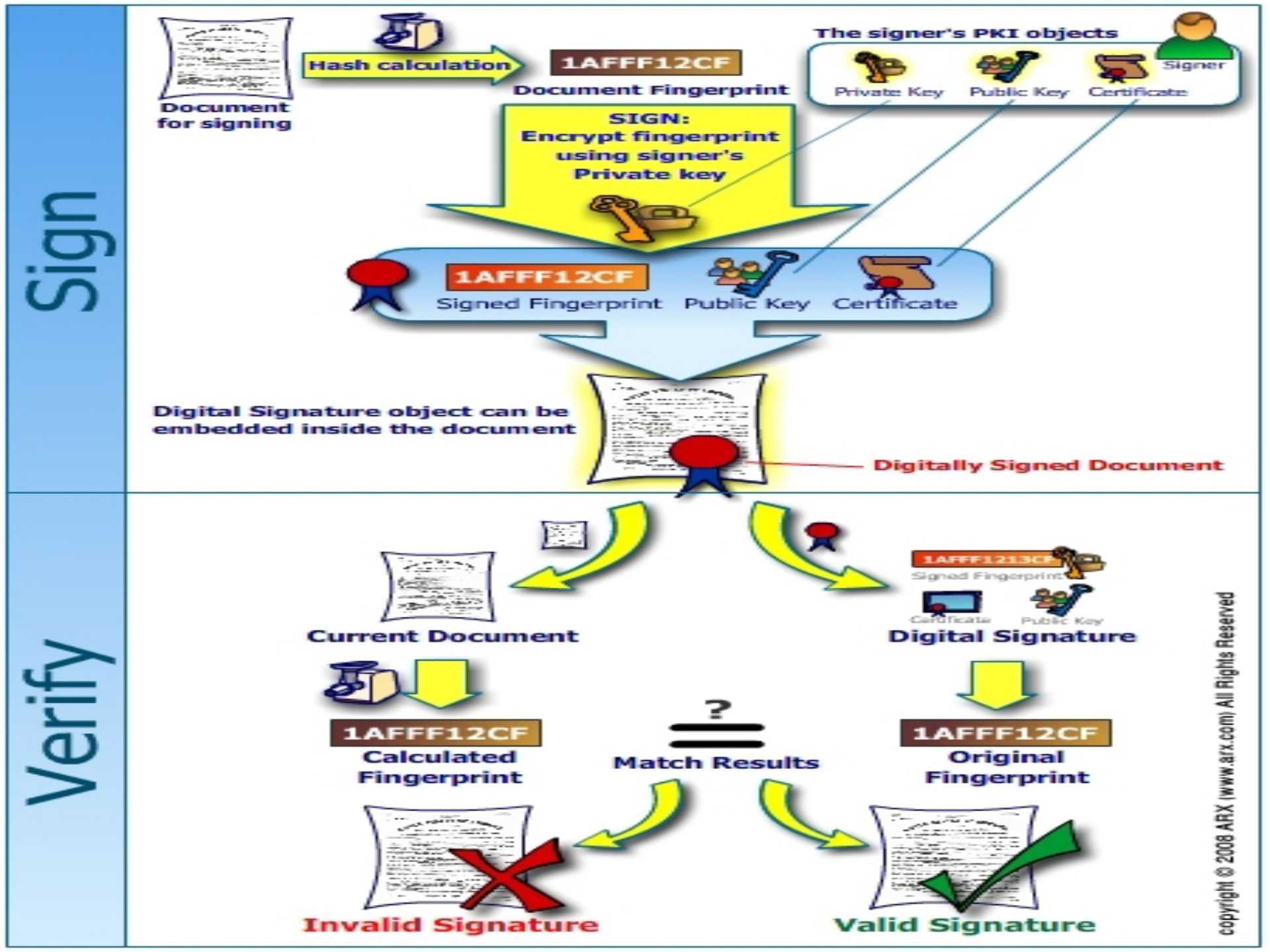
1. MAC
2. Hash values of message
3. Digital pen pad device

Digital Signature

1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.



2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.


Sign
Document for signing
Hash calculation
1AFFF12CF
Document Fingerprint
The signer's PKI objects
Private Key
Public Key
Certificate
Signer
SIGN:
Encrypt fingerprint using signer's Private key
1AFFF12CF
Signed Fingerprint
Public Key
Certificate
Digital Signature object can be embedded inside the document
Digitally Signed Document
Verify
Current Document
Signed Fingerprint
Certificate
Public Key
Digital Signature
1AFFF12CF
Calculated Fingerprint
?
Match Results
1AFFF12CF
Original Fingerprint
Invalid Signature
Valid Signature
copyright © 2008 ARX (www.arx.com) All Rights Reserved

Security (icon shown in Message)

Invalid Signature

Encrypted

Valid Signature

Unknown Signature

Signature Warning

DIGITAL SECURITY

emudhra
Trust Delivered

EMUDHRA IS A LICENSED CERTIFYING AUTHORITY (CA) WITH PAN INDIA OFFICES

TRUST KEY

eMudhra provides Trust Key Tokens – the most accepted and widely used token device in India for storing your Digital Signatures.

Your key to a **SECURE** world!

THE PROFESSIONAL'S FIRST CHOICE

LATEST TECHNOLOGY: THE ONLY TOKEN IN INDIA WHICH IS FIPS-140-2 CERTIFIED AND PLUG N PLAY (NO SEPARATE DRIVER REQUIRED).

Licensed Certifying Authority (Govt. of India)

(n)Code Solutions

SAFE SCRYPT
the confidence to do more

IDRBT

emudhra
Trust Delivered

IFS INDIA IFS INDIA IFS INDIA IFS INDIA

MTNL TRUSTLINE
WE CERTIFY DIGITAL SIGNS

TATA
TATA CONSULTANCY SERVICES

IFS INDIA IFS INDIA IFS INDIA IFS INDIA

digital signature certificate for

e-tendering

e-ticketing

e-procure

e-trademark

e-bidding

efile with smiles
Save Trees, Save Environment

MCA21
Service Transformation

TDS
Centralised Processing Cell

itr / mca e-filing

e-tds form 16 /16a signing

doc / mail signing

Keep Your DIGITAL SIGNATURE Key Securely

Do Not Share It with Any One

- The owner of the digital signature key is legally responsible for digital signatures created by that key.
- Use of strong password to access the digital signature key lowers the risk of compromise.
- In the case of digital signature key being lost or stolen, contact the Certifying Authority (CA) immediately and get the Digital Signature Certificate revoked.
- For details please visit website http://cca.gov.in

CONTROLLER OF CERTIFYING AUTHORITIES

CONTROLLER OF CERTIFYING AUTHORITIES
6, CGO Complex, Electronics Niketan
Lodhi Road, New Delhi - 110003
E-mail : info@cca.gov.in Website : http://cca.gov.in

Ministry of Communications & Information Technology
Government of India

Digital Signature Standard

- Digital Signature Algorithm
- In 1991, NIST proposed DSA to be used in DSS (FIPS PUB 186)
- Adopted as a standard in 94
- In 96, minor revision was issued
- In 2000, standard was expanded further
- SHA-1
- DSA v/s RSA

1. Free & license
2. DS & DS + Encryption
3. Strength Of Algorithm

- Computer Security Resource Center NIST(csrc.nist.gov)
- Federal Information Processing standard

RSA Digital Signature

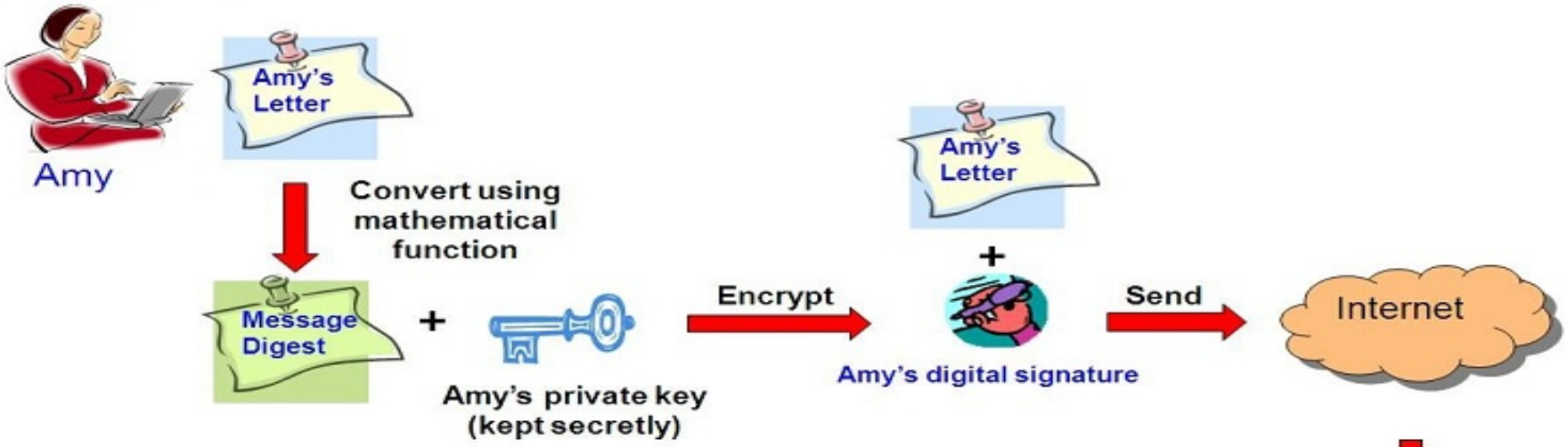
1. MD Calculation
2. Signing(i.e:-DS Creation)
3. Transmission Of Original Message & DS together
4. Receiver calculates its own MD
5. De-sign digital signature(i.e:-retrieves sender's MD)
6. Verification(Note:-Same Hash Algo should be used)

a) MD1=MD2

b) MD1≠MD2

Digital Signature

1. Amy converts her letter into a message digest by using a mathematical function. She then creates her digital signature by encrypting the message digest using her private key. Her letter, together with her digital signature are sent to Ben via email.



2. Ben, upon receiving the email, verifies Amy's digital signature using Amy's public key to decrypt the message digest by comparing the other one converted from the letter using the same mathematical function.