Office of Controller of Certification

Rajan Raj Pant
Controller
Government of Nepal
Ministry of Science & Technology

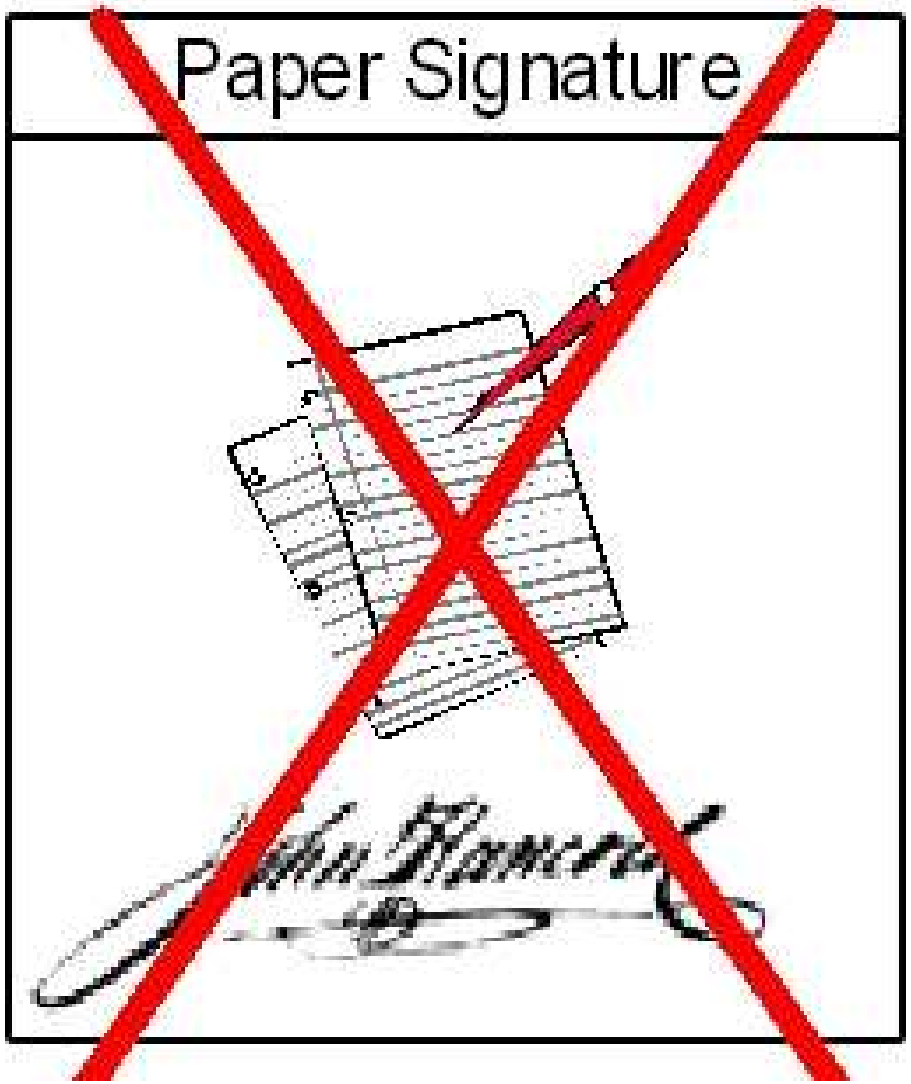
Electronic Record

i. Very easy to make copies
ii. Very fast distribution
iii. Easy archiving and retrieval
iv. Copies are as good as original
v. Easily modifiable
vi. Environmental Friendly

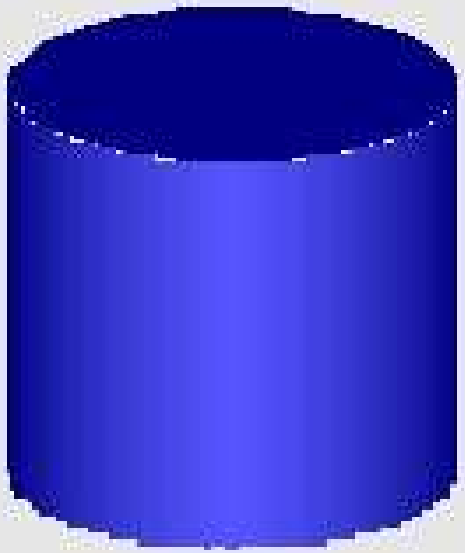
Because of IV & V together, these lack authenticity

What is a Digital Signature?

Paper Signature



Digital Signature



302C02143EBB0ABB
7815A10482802B7E
AEB5D55D9B34B467

Digital Signature

- Only electronic originals are legally binding because they can be checked using ***trusted software*** to determine if they are authentic or not
- A digital signature is produced by using the PKI method.

PIN protected Soft token

Smart Token

User can choose different packaging:

Reader + Smart Card

Plug-n-Play USB Token

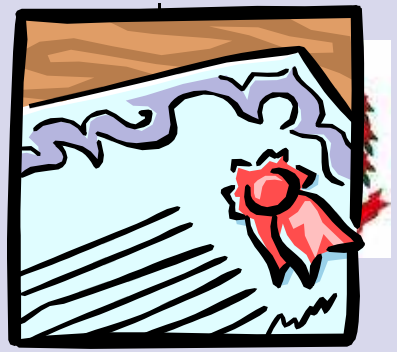
Smart Phone

Other Electronic Locks

USB Token

Smart Card

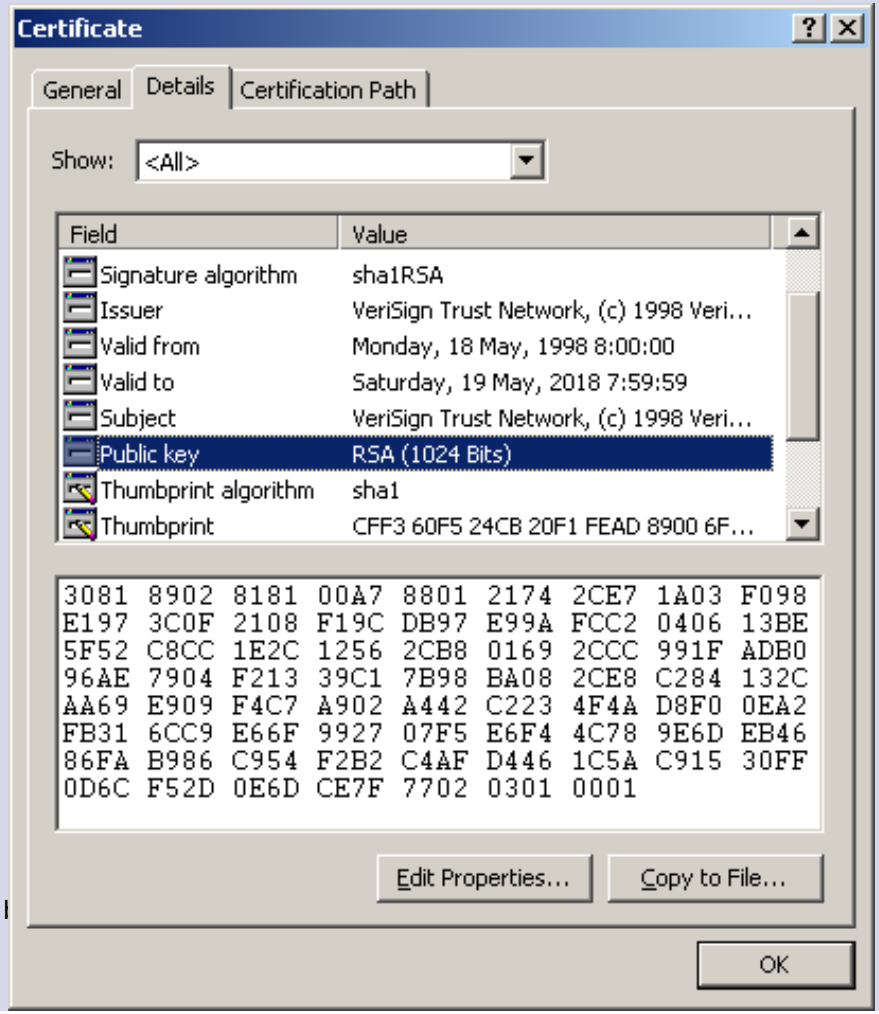
Digital Certificates



- Digital Certificate is a data with digital signature from one trusted Certification Authority (CA).
- This data contains:
  - Who owns this certificate
  - Who signed this certificate
  - The expired date
  - User name & email address

Elements of Digital Cert.

- A Digital ID typically contains the following information:
  - Your public key, Your name and email address
  - Expiration date of the public key, Name of the CA who issued your Digital ID



Digital Signatures

- Pair of keys for every entity

  One ***Public*** key – known to everyone

  One ***Private*** key – known only to the possessor

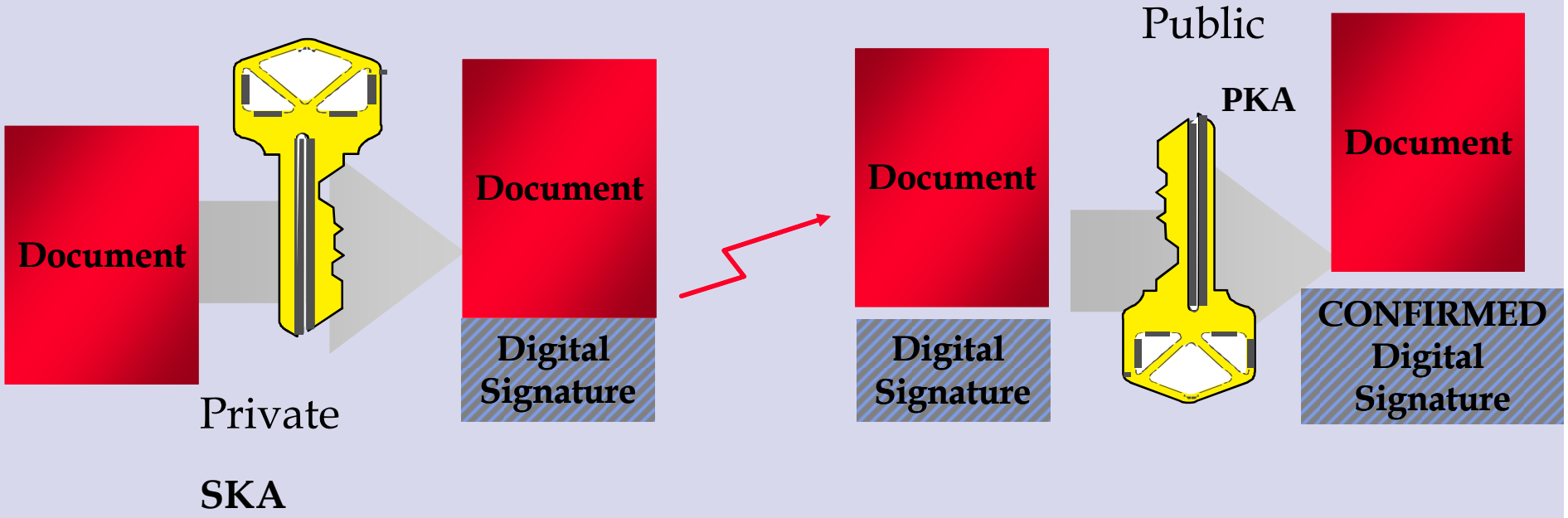
Digital Signatures

- To ***digitally sign*** an electronic document the signer uses his/her ***Private*** key.

- To ***verify*** a digital signature the verifier uses the signer's ***Public*** key.

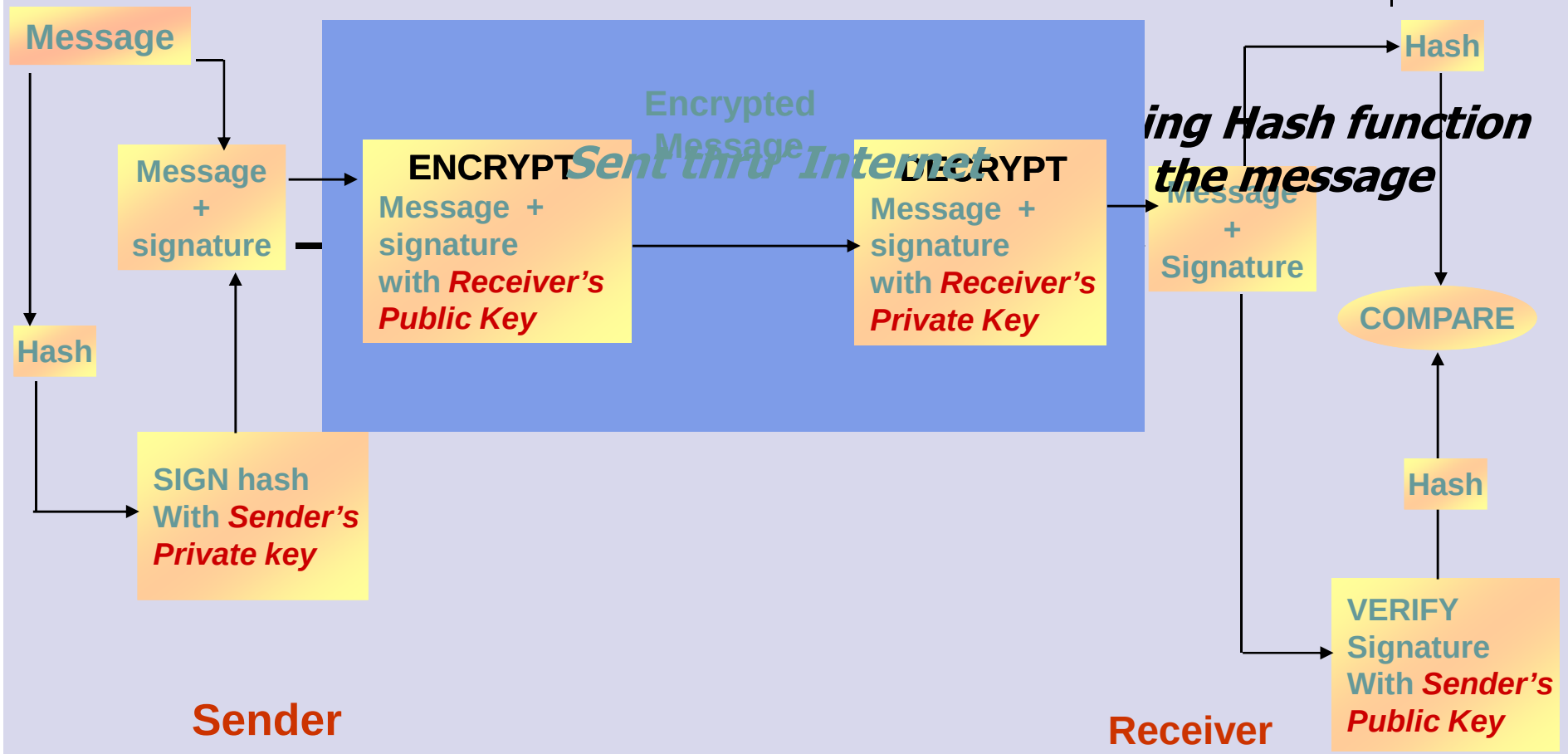
Digital Signature

- The message is encrypted with the sender's private key
- Recipient decrypts using the sender's public key



Confidential

Signed Messages



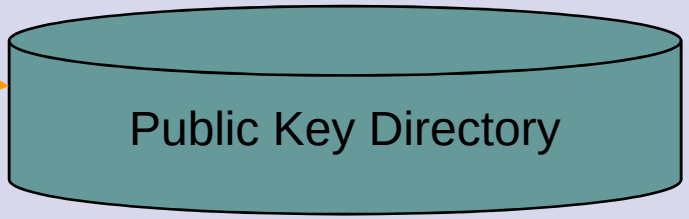
Public-Private Encryption

Public key

Private key

First, create public and private key

Public key stored in the directory

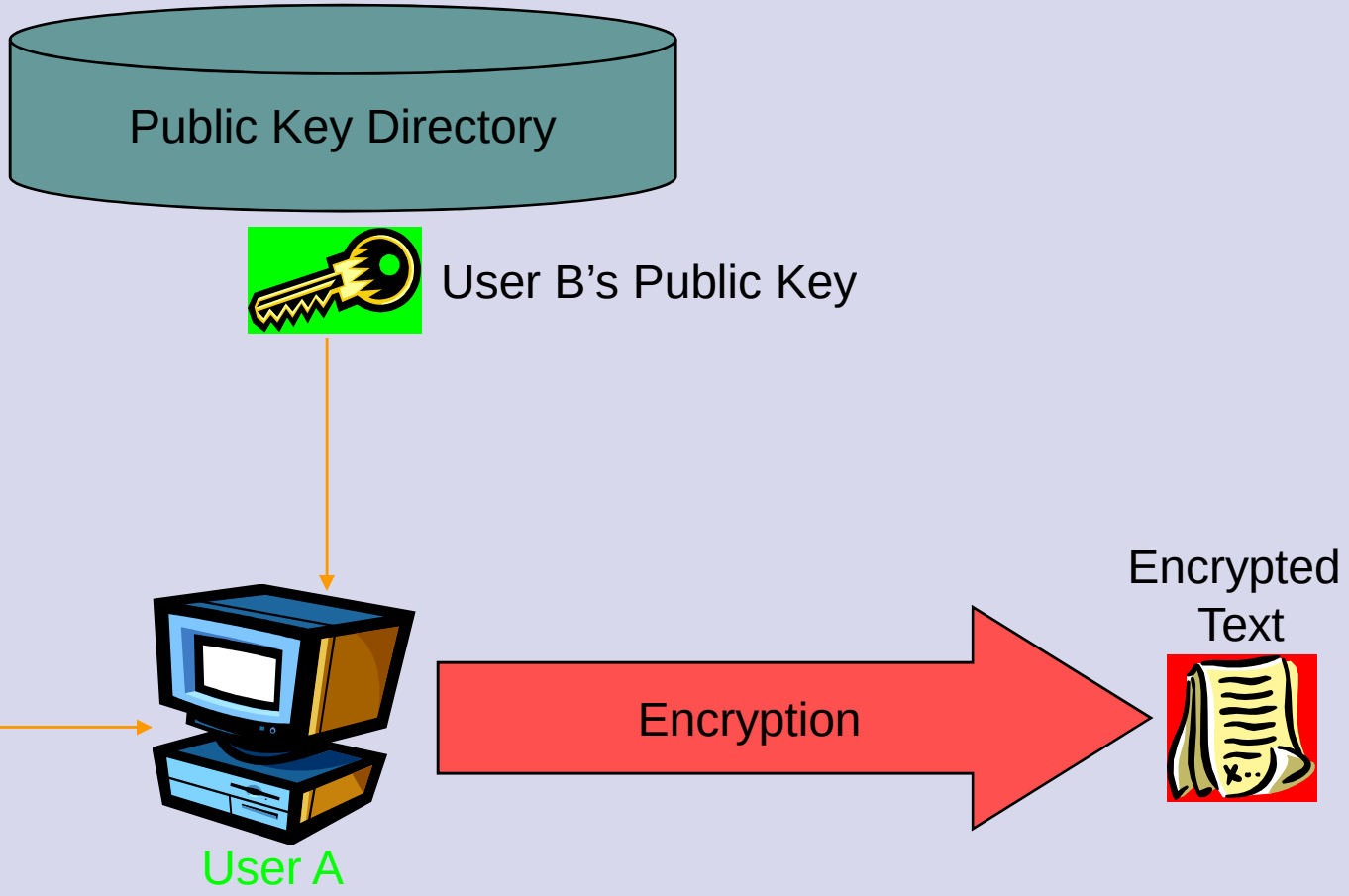


Public Key

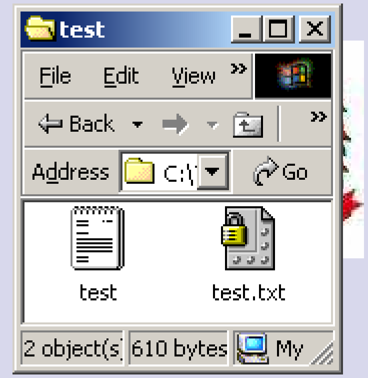
Private key

Private key stored in Token

Message Encryption
(User A sends message to User B)

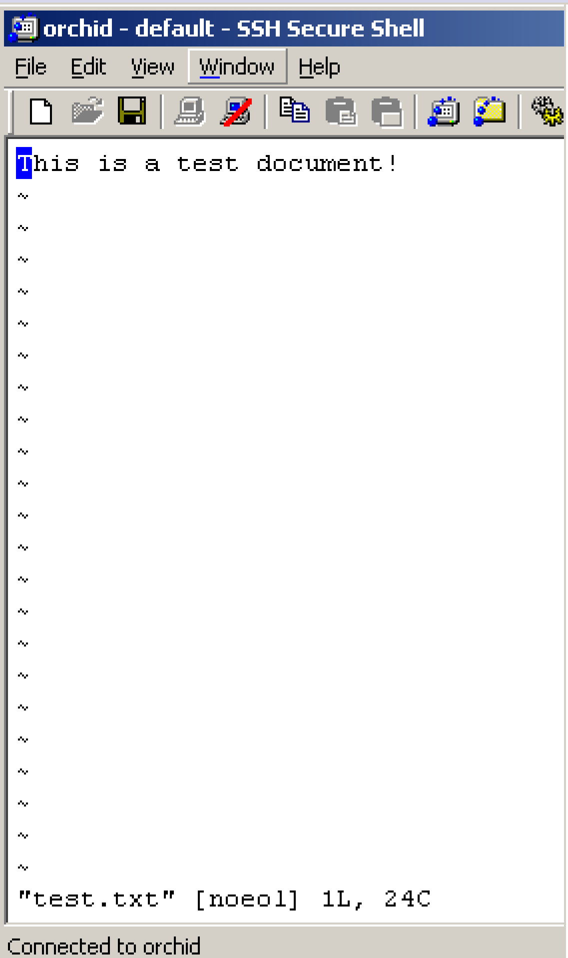


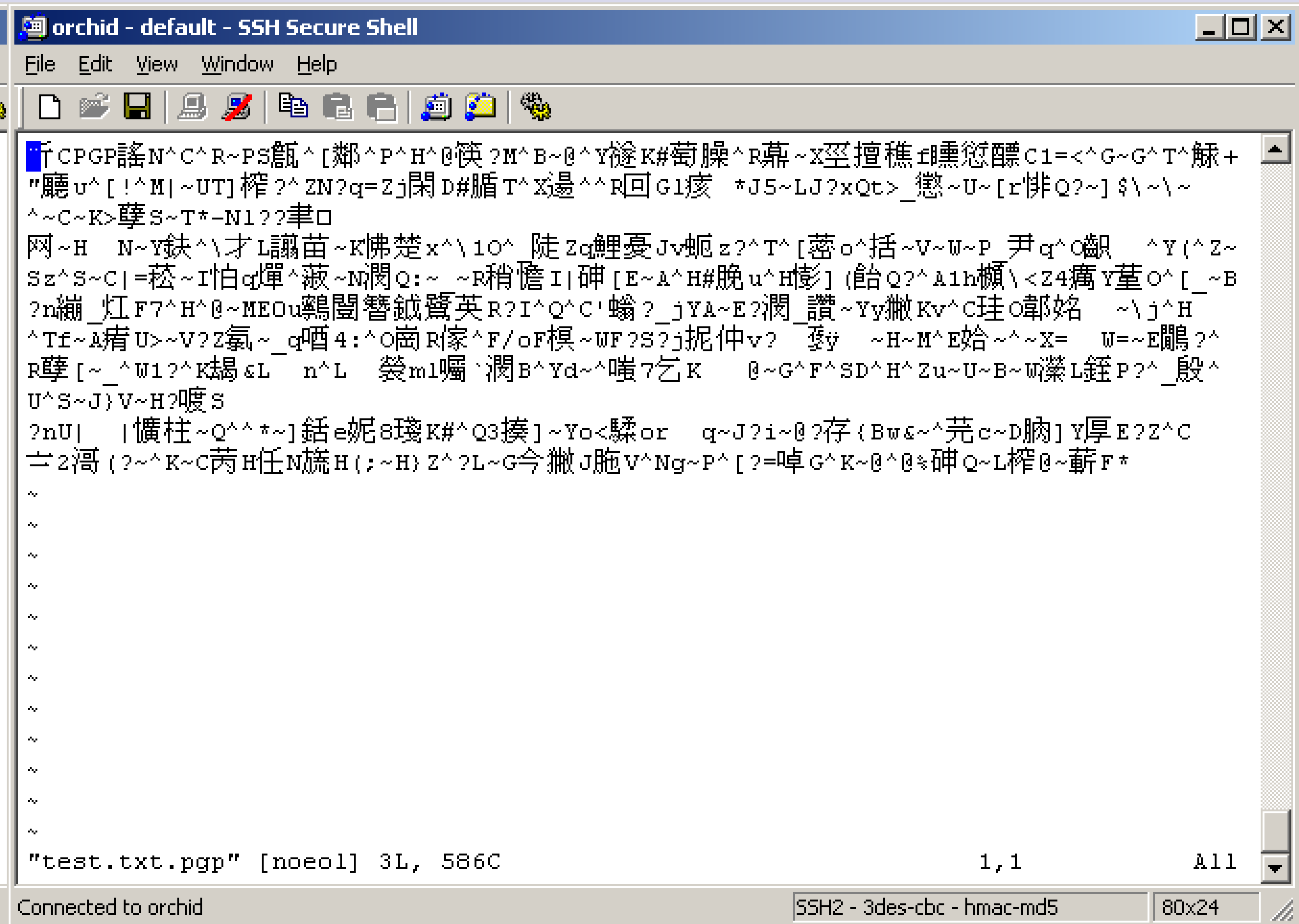
Message Encryption



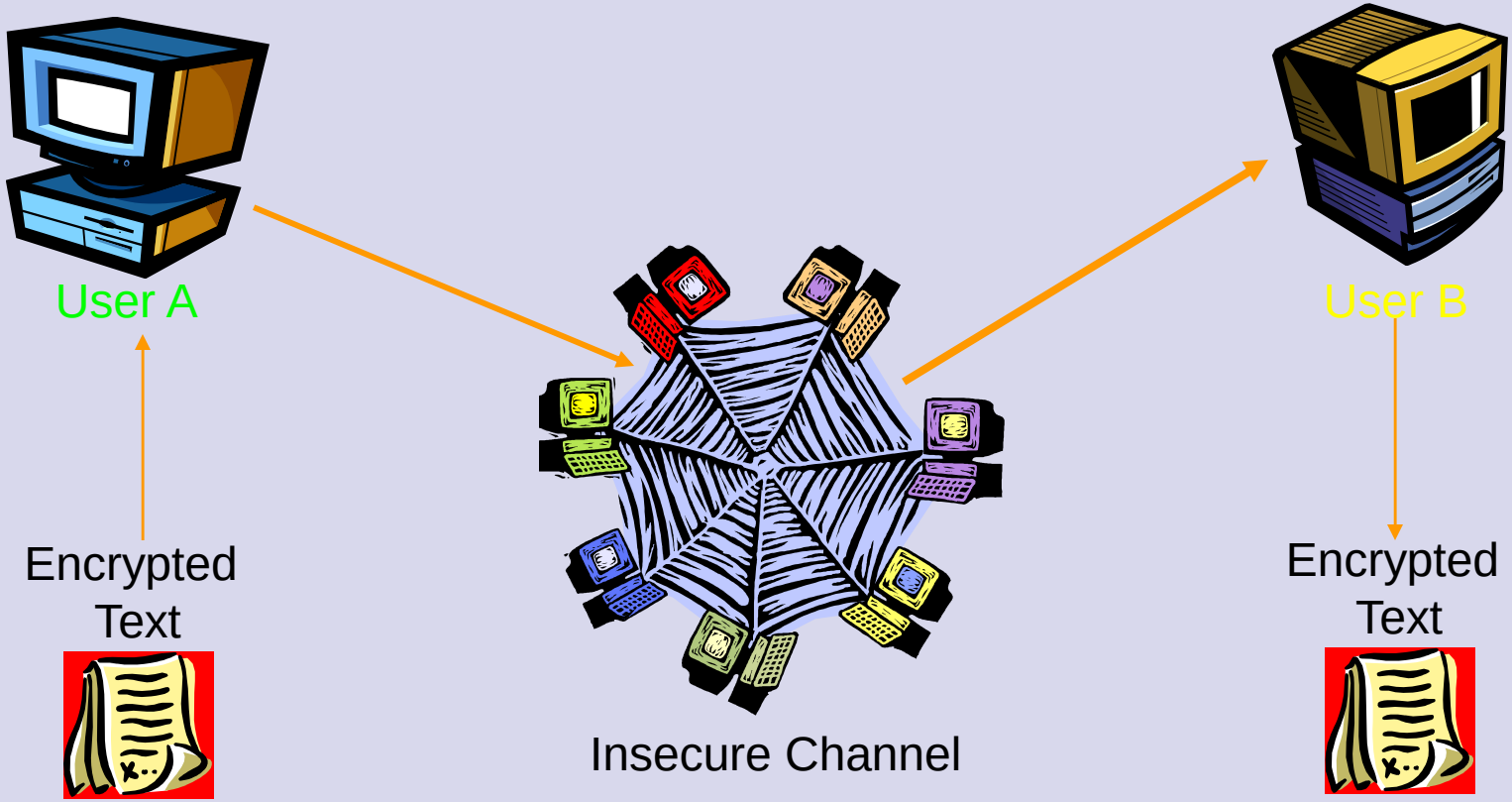
Original Message

Encrypted Message



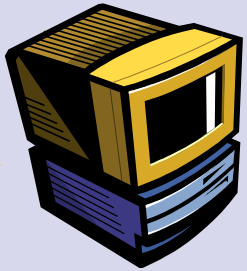


Transfer Encrypted Data



Decryption with your Private key

Encrypted Text



User B

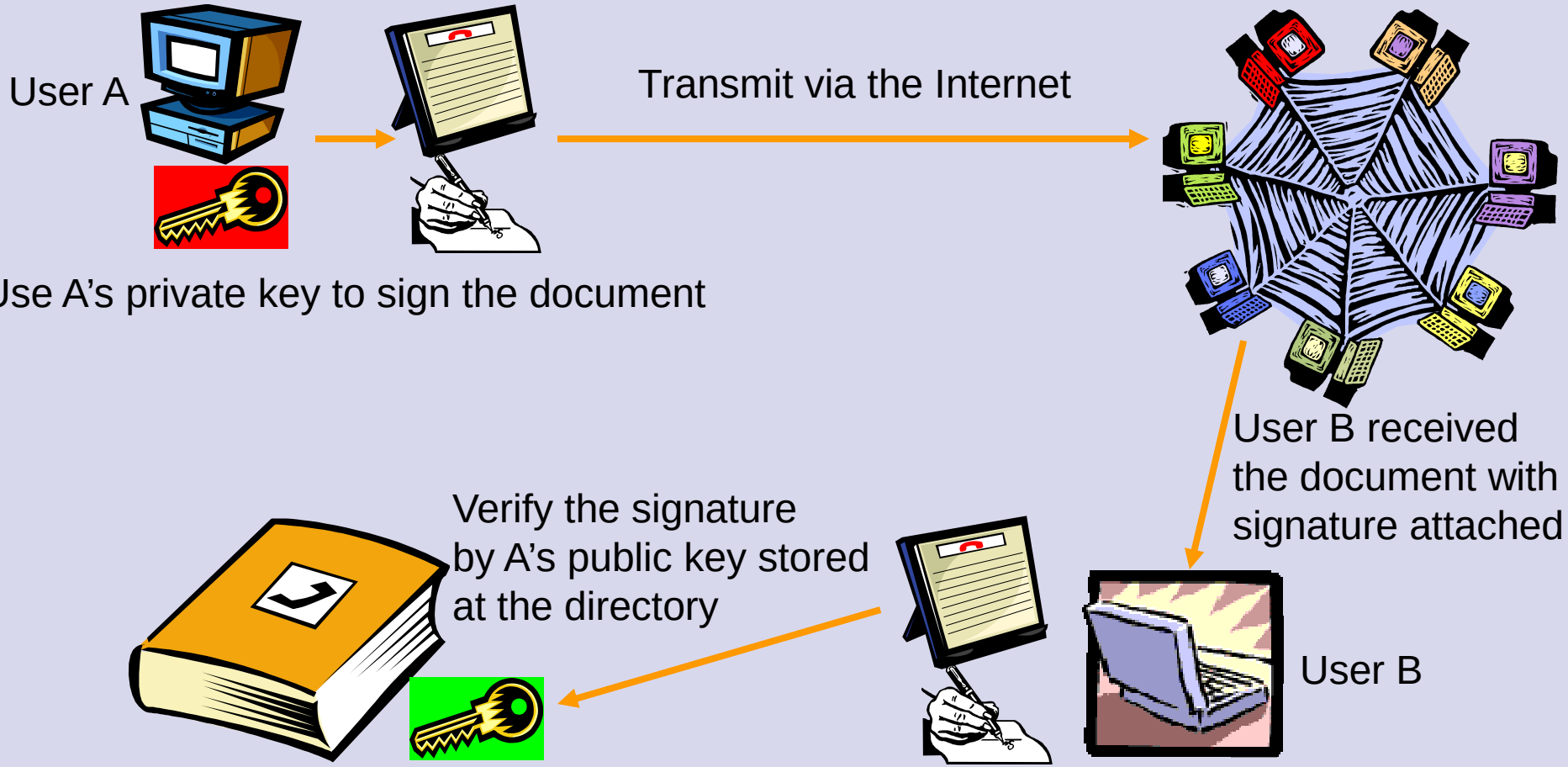
Using Private key in your personal computer

User B's Private key

Decryption

Original Text

How digital Signature works?



What are digital signatures used for? Or its Advantages

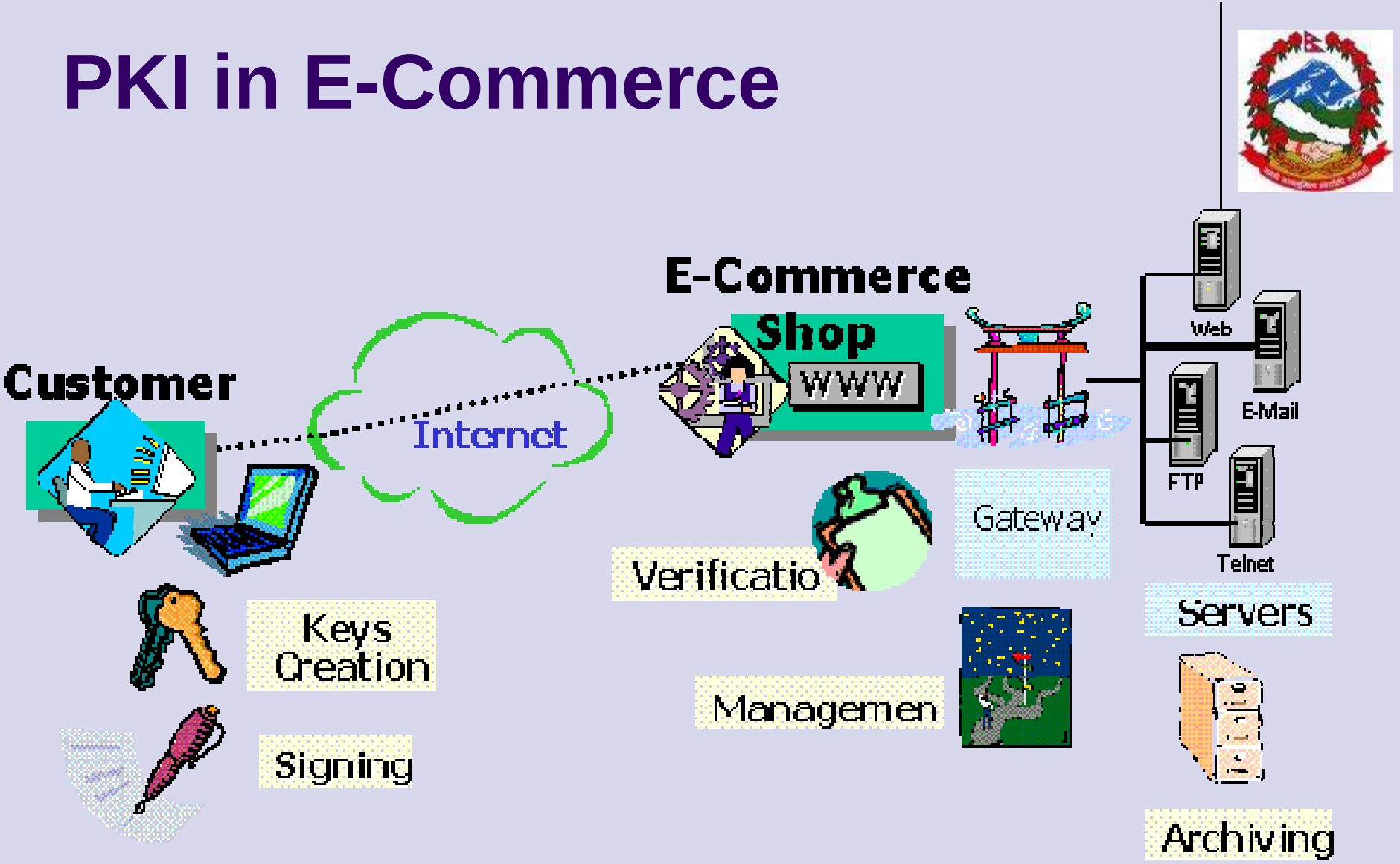
- Identification & Authentication
- Data Integrity
- Non-Repudiation
- Security

- **Imposter prevention:** By using digital signatures you are actually eliminating the possibility of committing fraud by an imposter signing the document. Since the digital signature cannot be altered, this makes forging the signature impossible.

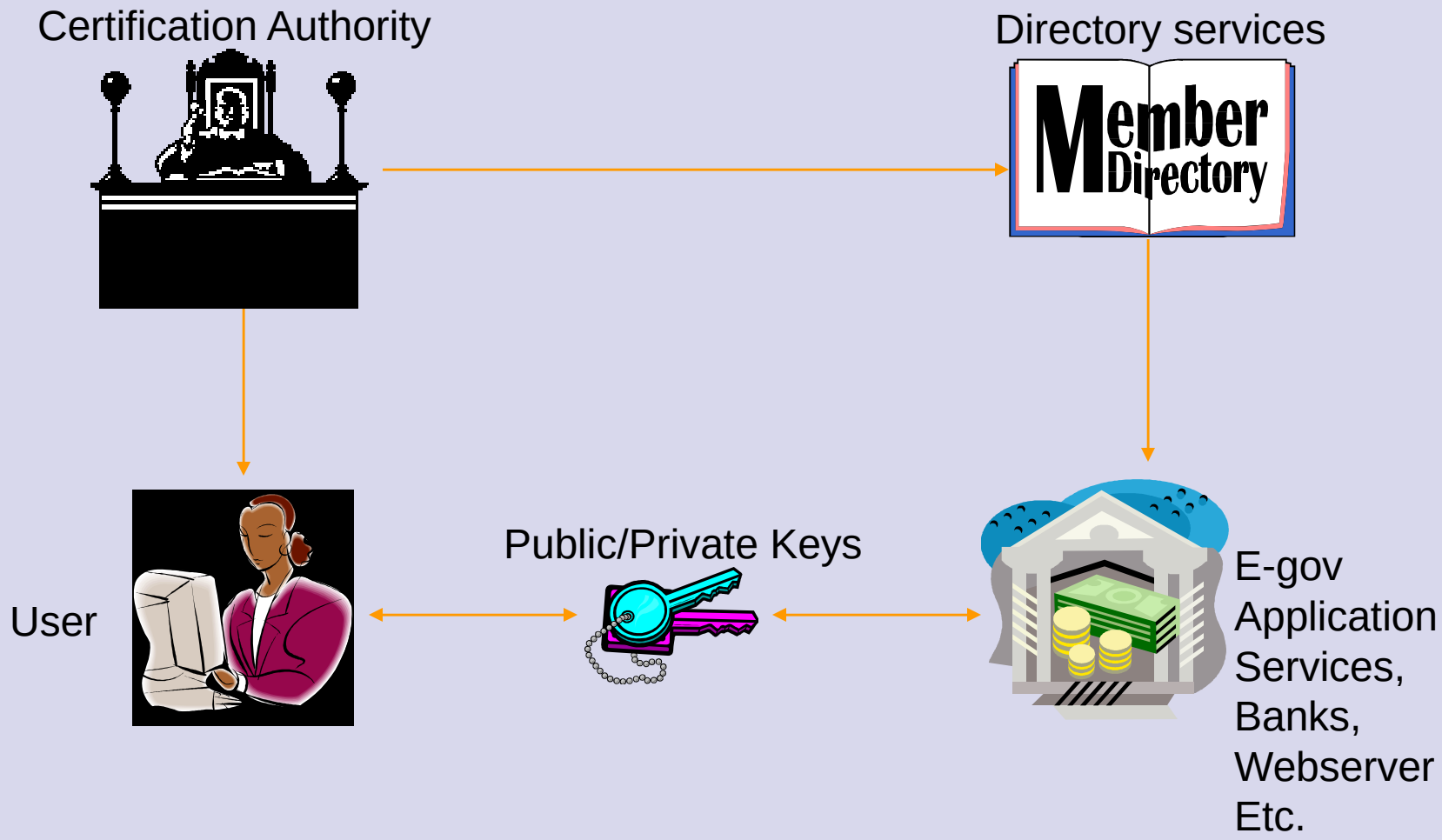
- **Legal requirements:** Using a digital signature satisfies some type of legal requirement for the document in question. A digital signature takes care of any formal legal aspect of executing the document.

PKI in Authentication

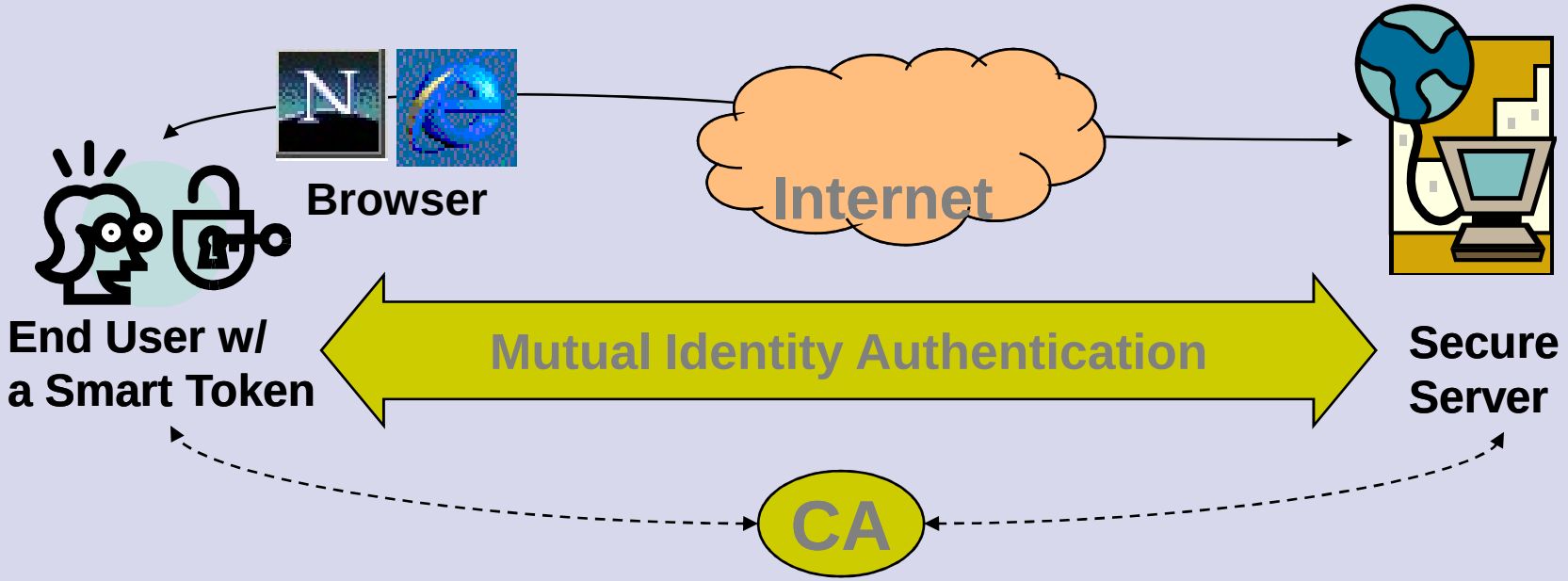
PKI in E-Commerce



PKI Structure



Banking Solution Overview



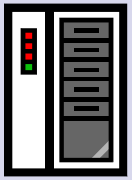
The Client-side includes:

- Smart token

The Server-side includes:

- Backend user database integration - issuance, admin , self-service
- Front-end (Web site) integration – replace password login / logout pages with token pages
- Certificate & certificate authority – Private (free) or public (annual fee)

Deployment Overview

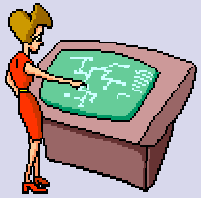


Web site and backend server setup

Token issuance to online users

User installs Token package

Secure online transactions

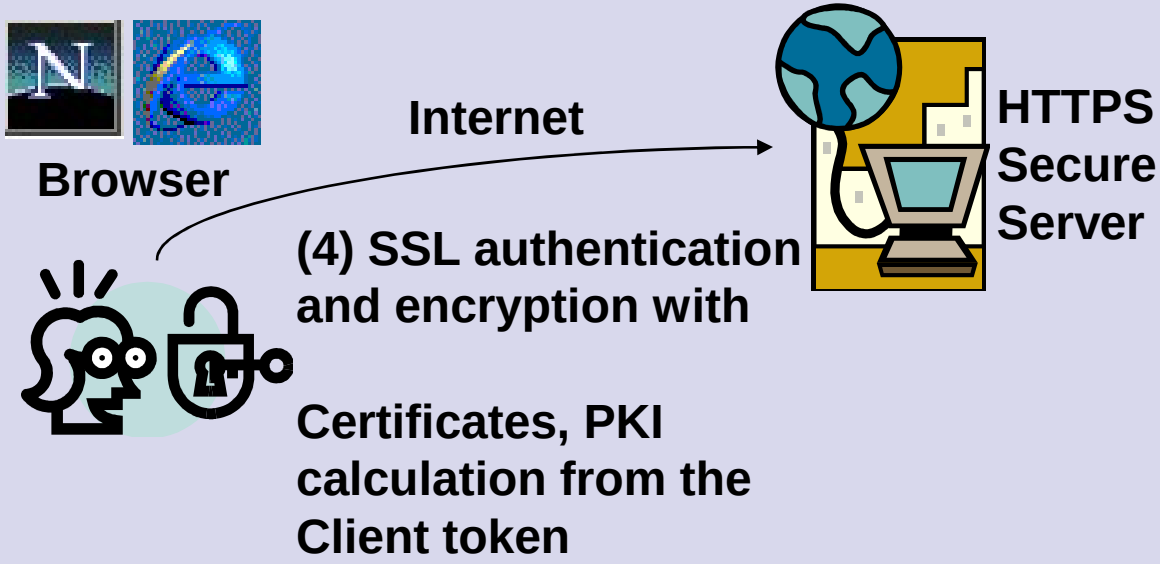


Self-service kiosk, or admin station in some branch offices for security sensitive work

(Future) Web-based self-service for certificate renewal, token loss, damage, etc.

- **Security**
- **Convenience**
- **Simplicity**
- **New revenue**
- **Sharper company image**
- **Customer loyalty**
- **E-Commerce**

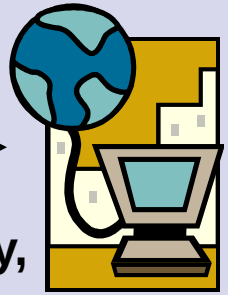
Server-Side Authentication



Clean Sign-off, No Traces Left

Browser

Internet



HTTPS Secure Server

(5) Take the lock away, all SSL sessions automatically self-destroy upon that event.

No data caching, no passwords, nor private keys exposed. All base on FIPS-certified crypto calculation

Plan of Subdivision or Consolidation

return

Remember to save and print copies for your records.

Open current Plan of Subdivision or Consolidation , (Surveyor's Plan Version: 3, Number of Pages: 1, 60 KB PDF, new window)
Digitally signed by: Adam Ronaldo (Suburban Surveyors - Never Never Land)
21/01/2008 11:15 am

Submitted: 21/01/2008
Supplied by: Adam Ronaldo

Get Acrobat PDF Reader

Description: The restriction has been amended to accord with the condition in the permit to ensure compliance with Clause 54 of the Test Council Planning Scheme

Previous Versions:

- Plan of Subdivision or Consolidation **SPEAR Version: 1** Submitted: 21/01/2008 (Number of pages:1, Surveyor's Plan Version: 1, Number of Pages: 1, 60 KB PDF, new window).
- Plan of Subdivision or Consolidation **SPEAR Version: 2** Submitted: 21/01/2008 (Number of pages:1, Surveyor's Plan Version: 2, Number of Pages: 1, 60 KB PDF, new window). easements added to accord with the engineering design minor changes to the S 14 boundaries

Accessibility: If you are unable to view the PDF Click Here

return

Implication

- NID
- Passport
- PIS
- Driving License
- E-payment
- Internet and Mobile Banking
- E-Procurement
- E-governance Applications
- Any type of online Transaction

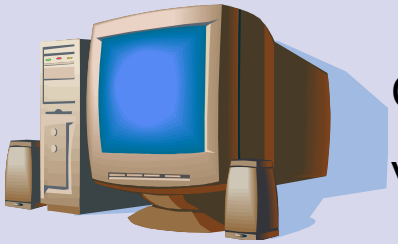
Root CA

Controller Office

National Repository

OCSP

VM



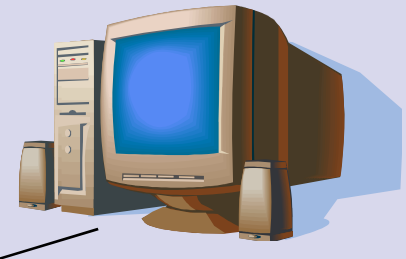
24/7 Help Desk

Government

Issuing CA

CM

CRL



CA

RA

Customer

Govt. Dept.

Internet with Secured VPN

Thank you