

Office of Controller of Certification



Rajan Raj Pant
Controller

Government of Nepal

Ministry of Environment, Science & Technology



Electronic Record

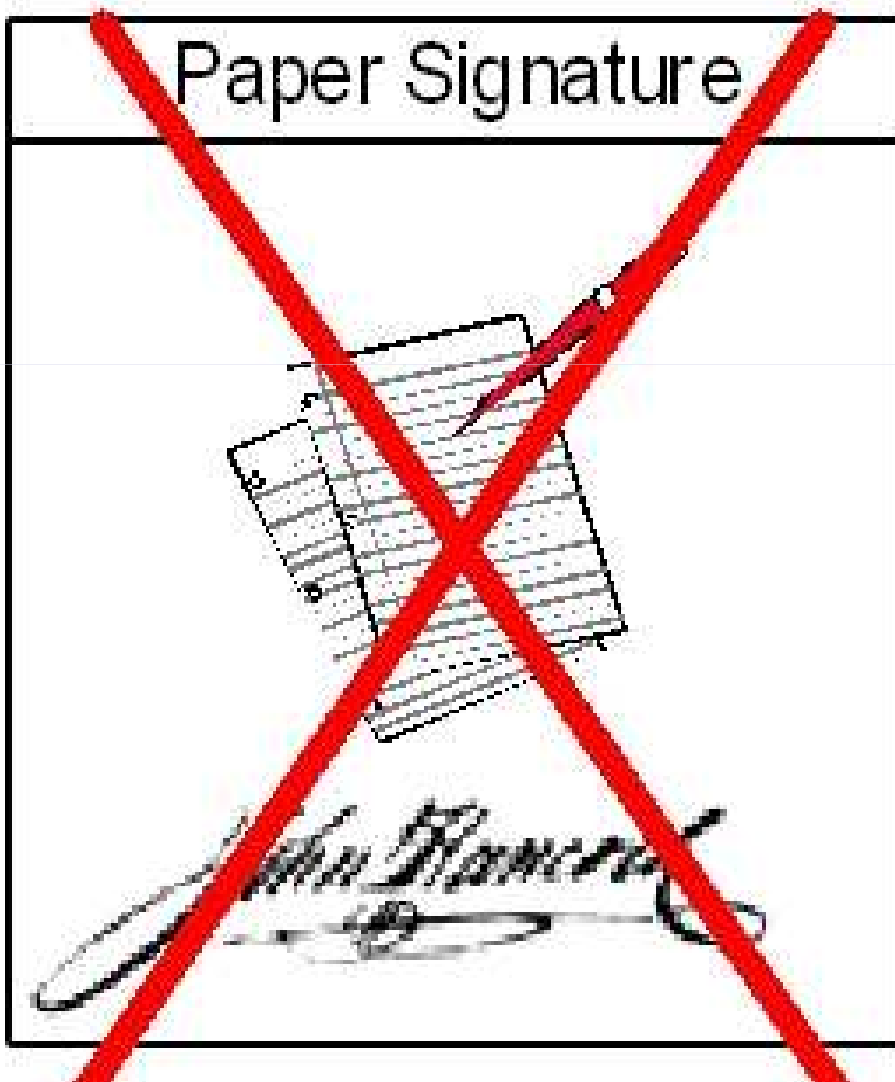
- i. Very easy to make copies
- ii. Very fast distribution
- iii. Easy archiving and retrieval
- iv. Copies are as good as original
- v. Easily modifiable
- vi. Environmental Friendly



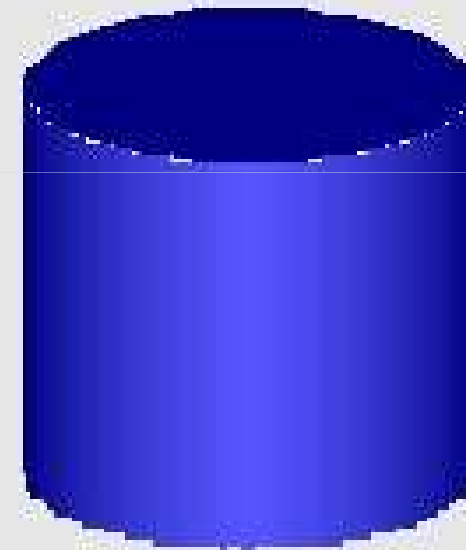
Because of IV & V together, these lack authenticity

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



The image shows two overlapping windows. The background window is the 'Cisco Systems VPN Client' with the title bar 'Cisco Systems VPN Client'. It displays 'Connecting to 16.142.12.2' and a 'User Authentication for goliath' dialog box. The dialog box contains a lock icon and the instruction 'Enter a new PIN between 4 to 8 digits'. It has fields for 'Username:' (containing 'sanjay') and 'Password:', a 'Save Password' checkbox, and 'OK' and 'Cancel' buttons. At the bottom of the main window are 'Connect' and 'Close' buttons.

The foreground window is the '50682711 - Software Token' window with a menu bar containing 'Options', 'Copy!', 'View', and 'Help'. It features a red header with a PIN display showing '14084181^{PIN}'. Below this is the 'RSA SecurID[®]' logo. A numeric keypad with digits 1-0 is visible, along with 'Enter' and 'Clear' buttons. At the bottom, it says 'Enter PIN and click Enter.'.

Smart Token



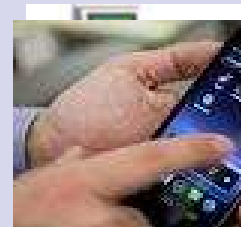
User can choose different packaging:



Reader +
Smart Card



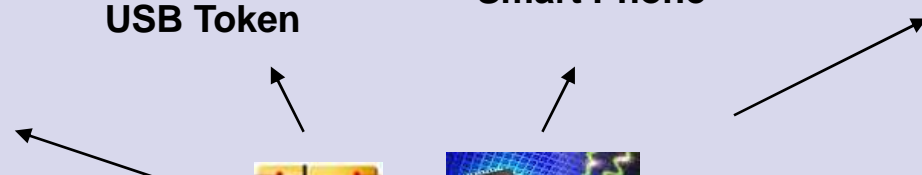
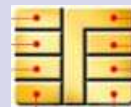
Plug-n-Play
USB Token



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

Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: digitalid.hitrust.com.hk

Issued by: www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(c)97 VeriSign

Valid from: 8/23/2001 to 8/24/2002

Buttons: Install Certificate..., Issuer Statement, OK

Show: <All>

Field	Value
Signature algorithm	sha1RSA
Issuer	VeriSign Trust Network, (c) 1998 Veri...
Valid from	Monday, 18 May, 1998 8:00:00
Valid to	Saturday, 19 May, 2018 7:59:59
Subject	VeriSign Trust Network, (c) 1998 Veri...
Public key	RSA (1024 Bits)
Thumbprint algorithm	sha1
Thumbprint	CFF3 60F5 24CB 20F1 FEAD 8900 6F...

Hex dump:
3081 8902 8181 00A7 8801 2174 2CE7 1A03 F098
E197 3C0F 2108 F19C DB97 E99A FCC2 0406 13BE
5F52 C8CC 1E2C 1256 2CB8 0169 2CCC 991F ADB0
96AE 7904 F213 39C1 7B98 BA08 2CE8 C284 132C
AA69 E909 F4C7 A902 A442 C223 4F4A D8F0 0EA2
FB31 6CC9 E66F 9927 07F5 E6F4 4C78 9E6D EB46
86FA B986 C954 F2B2 C4AF D446 1C5A C915 30FF
0D6C F52D 0E6D CE7F 7702 0301 0001

Buttons: Edit Properties..., Copy to File..., OK

Digital Signatures



- Pair of keys for every entity

One **Public** key – known to everyone

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



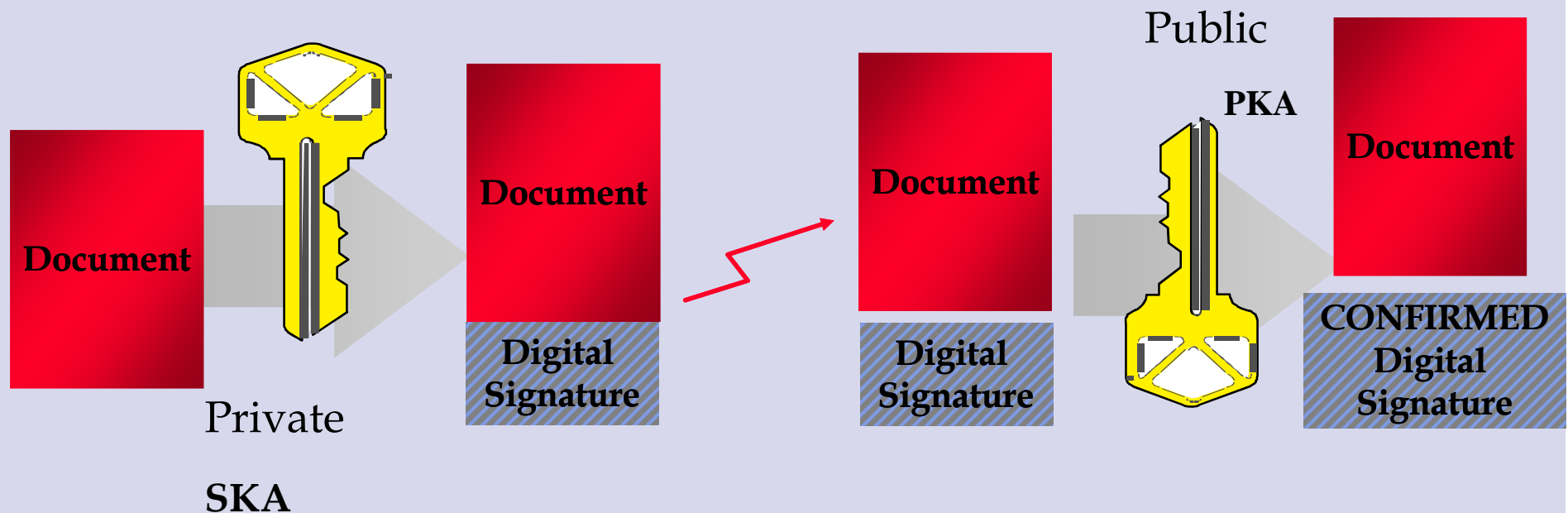
Digital Signatures

- 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.



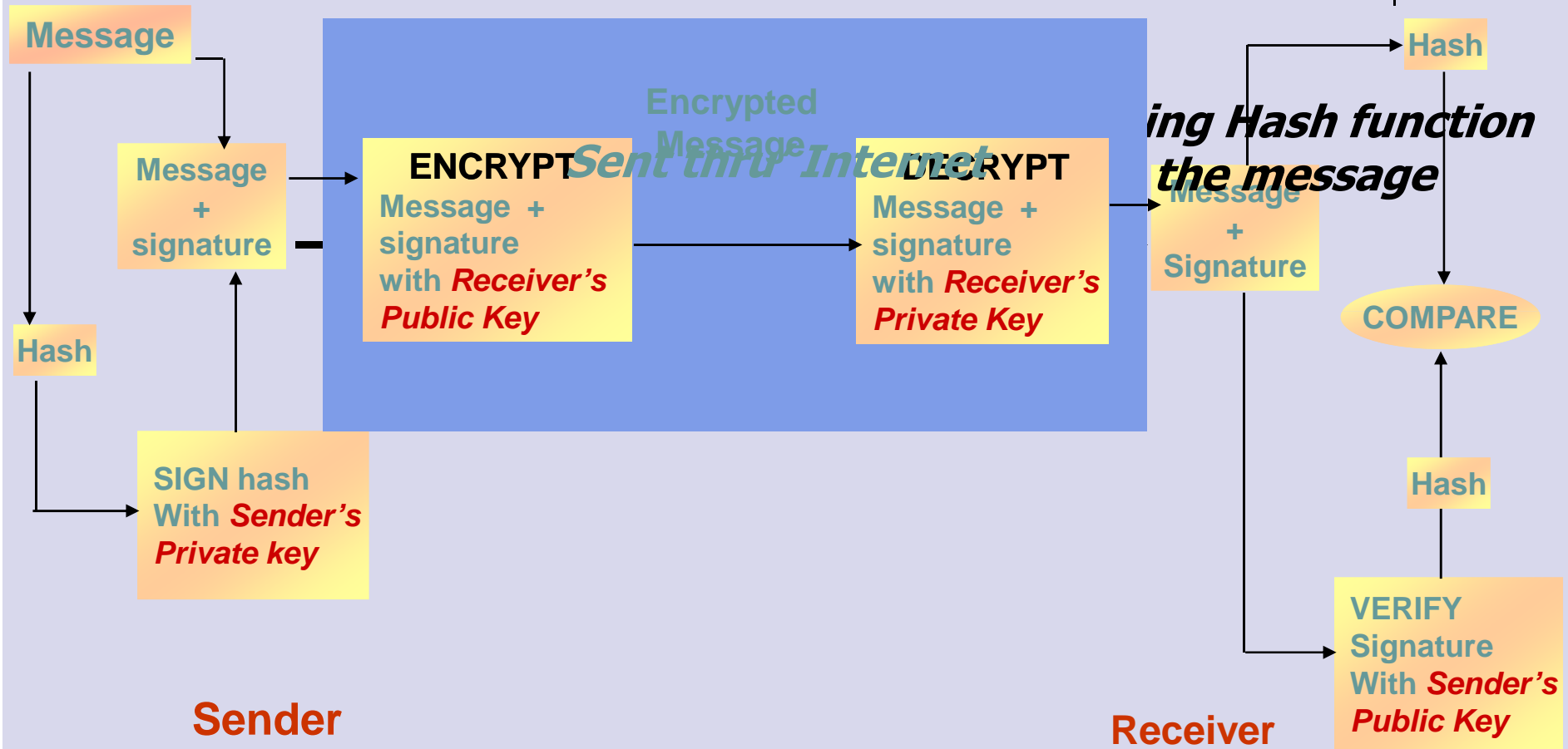
Digital Signature

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

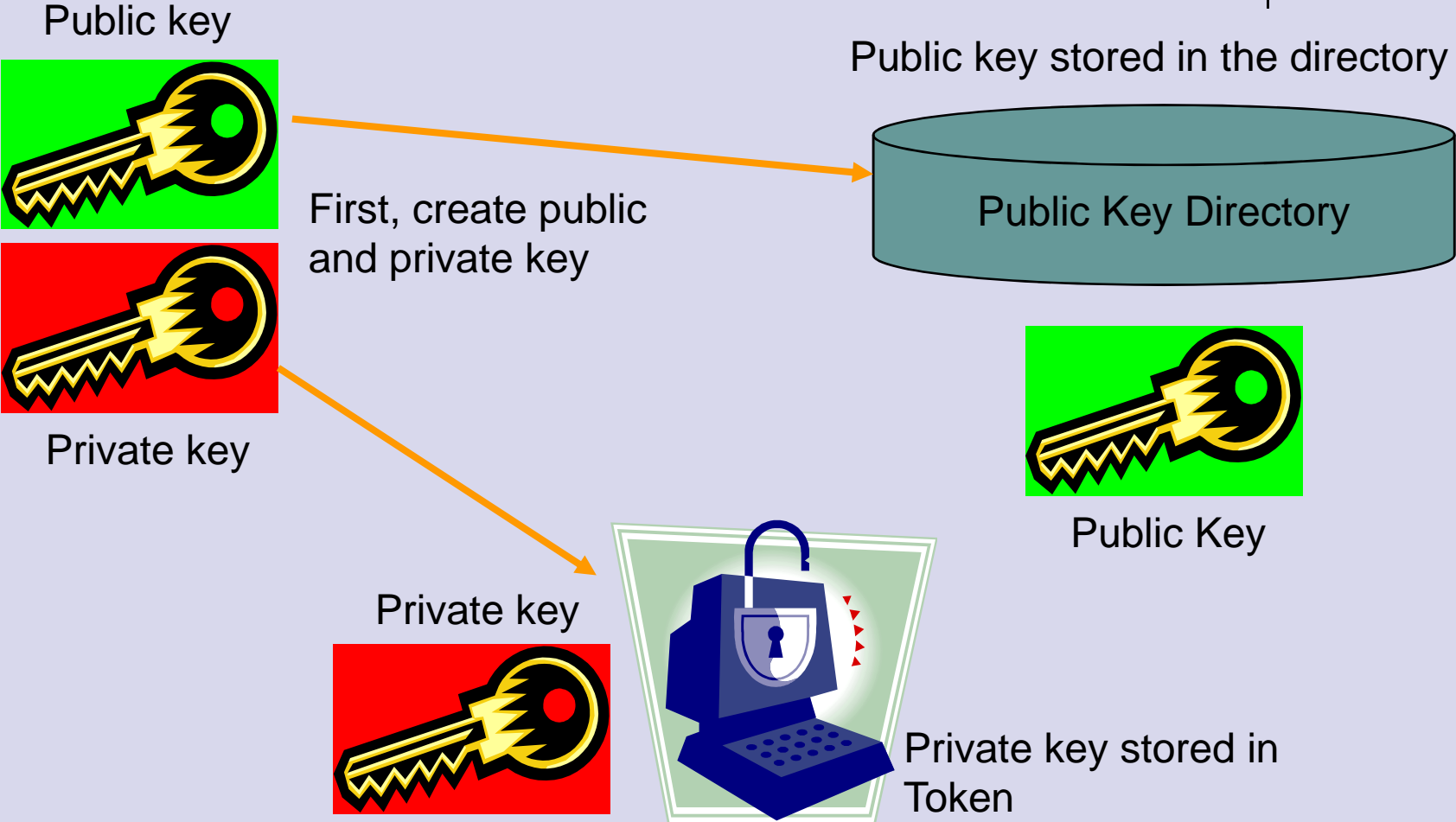


Confidential

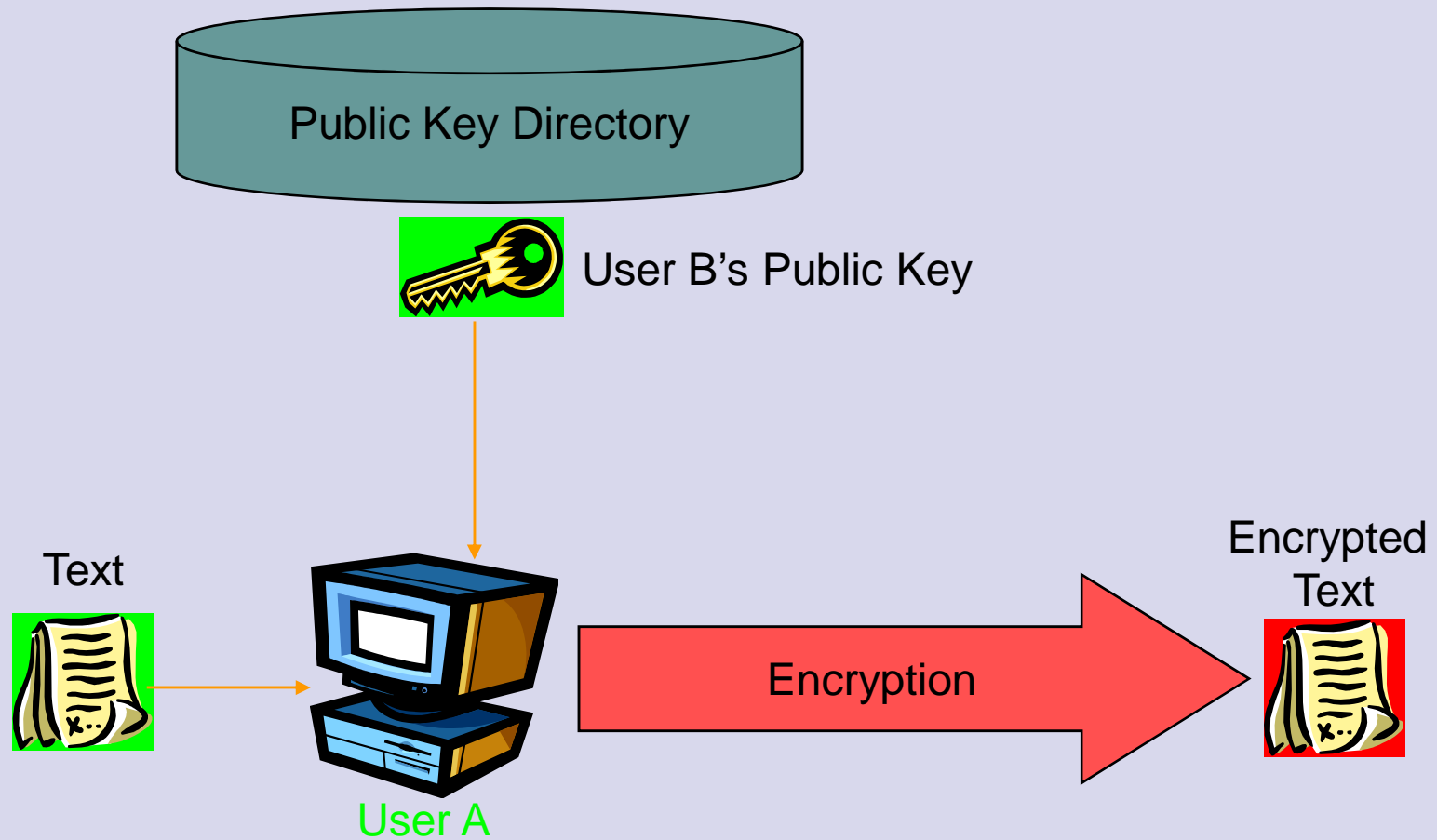
Signed Messages



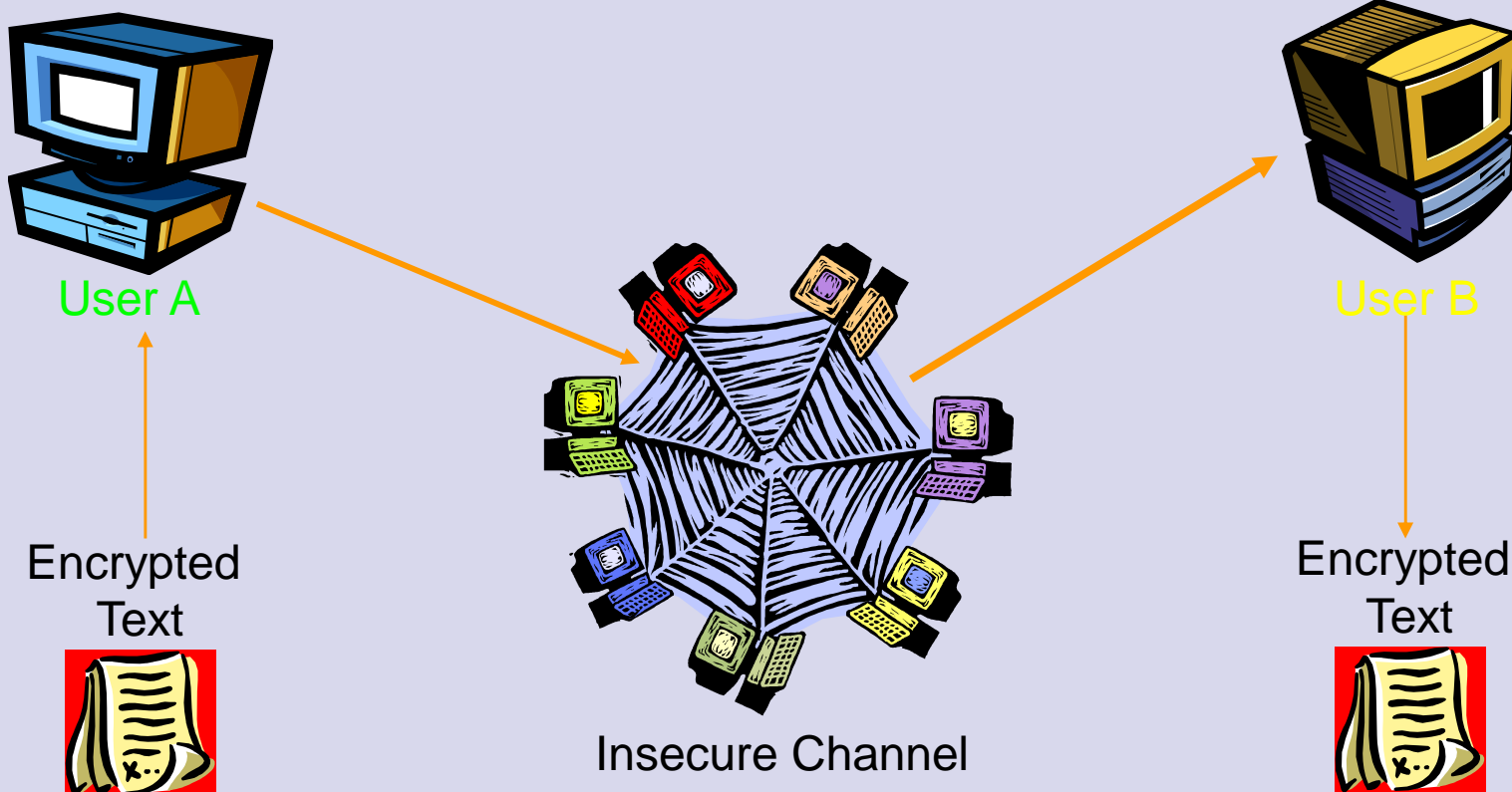
Public-Private Encryption



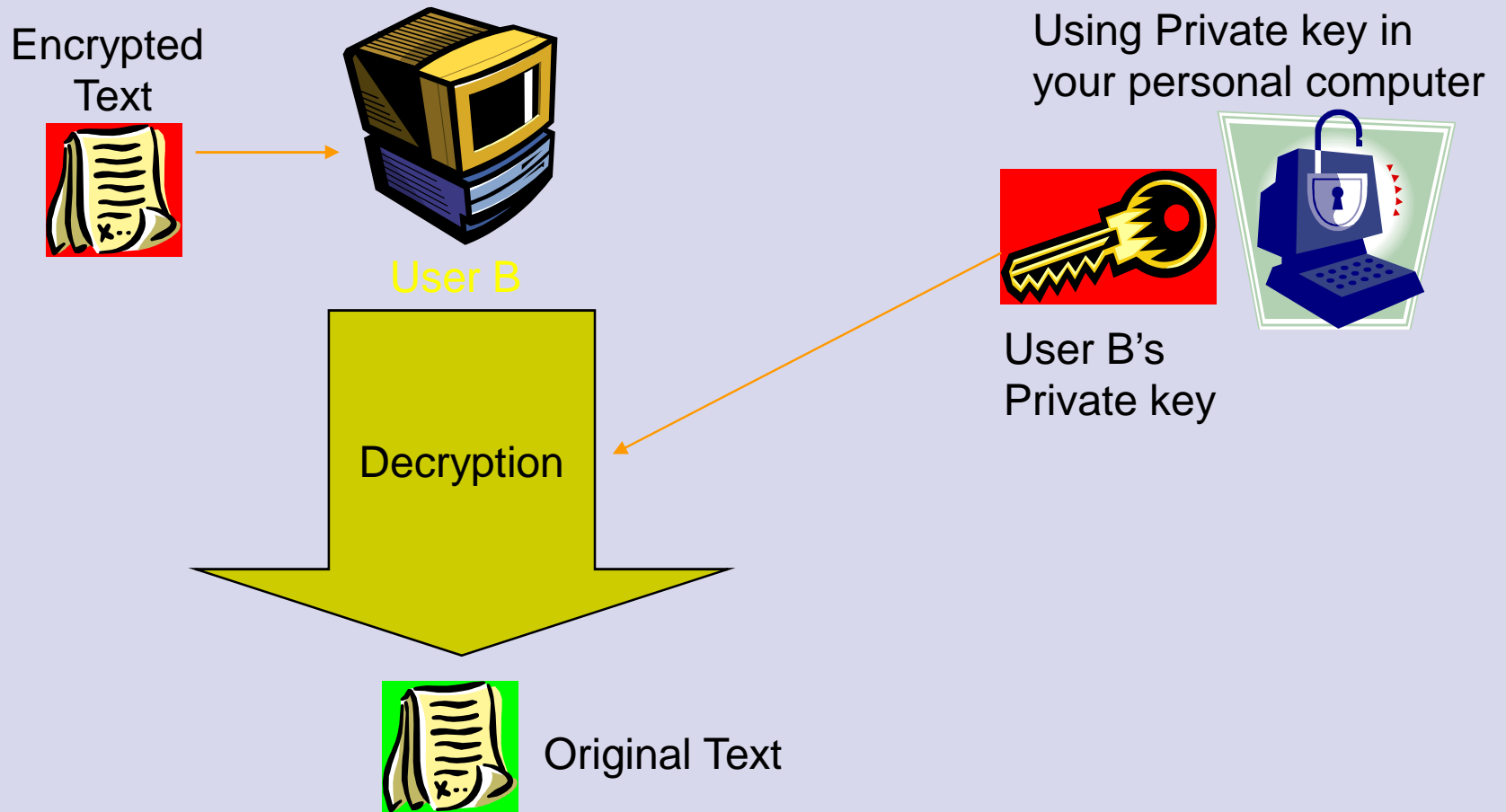
Message Encryption (User A sends message to User B)



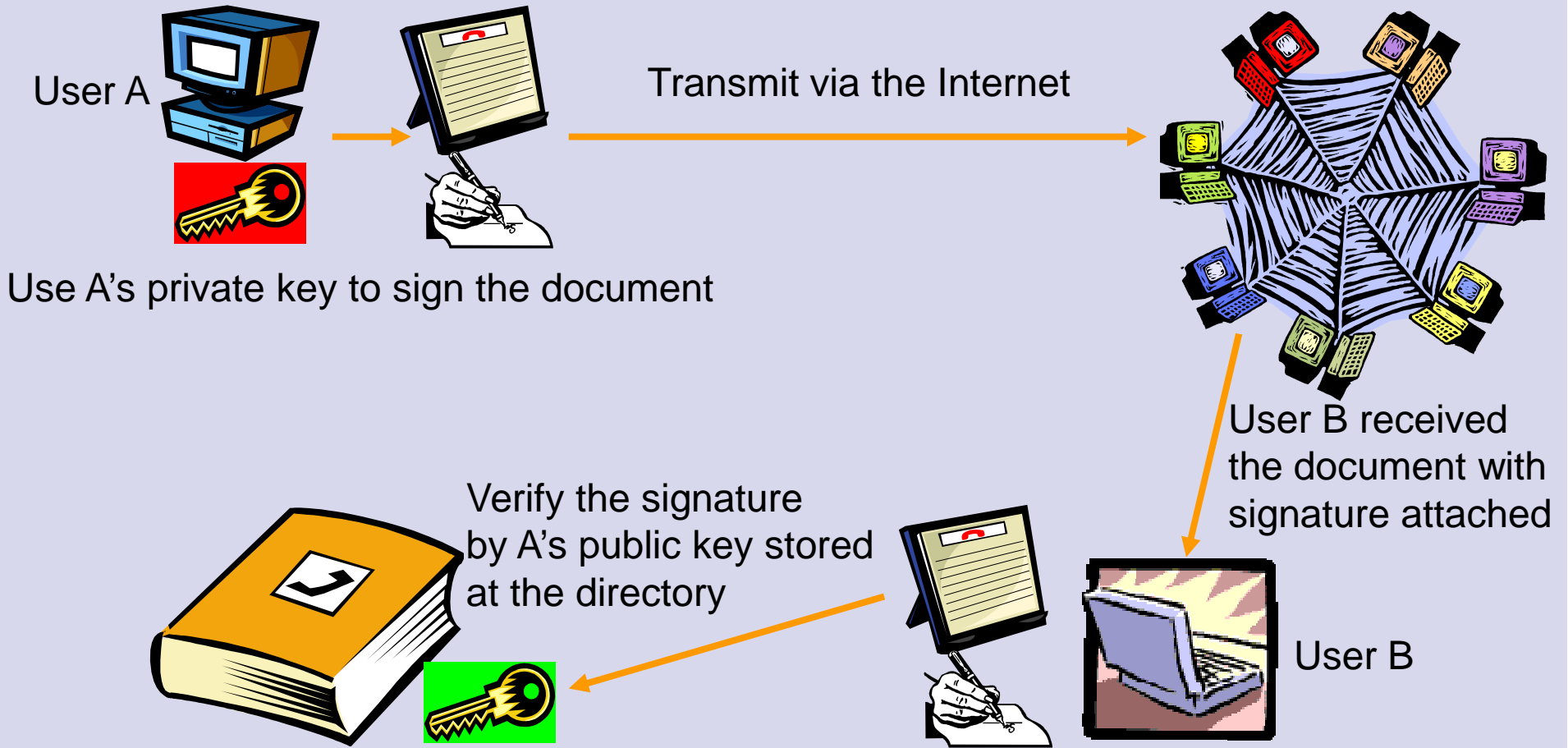
Transfer Encrypted Data



Decryption with your Private key



How digital Signature works?



What are digital signatures used for? Or its Advantages



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

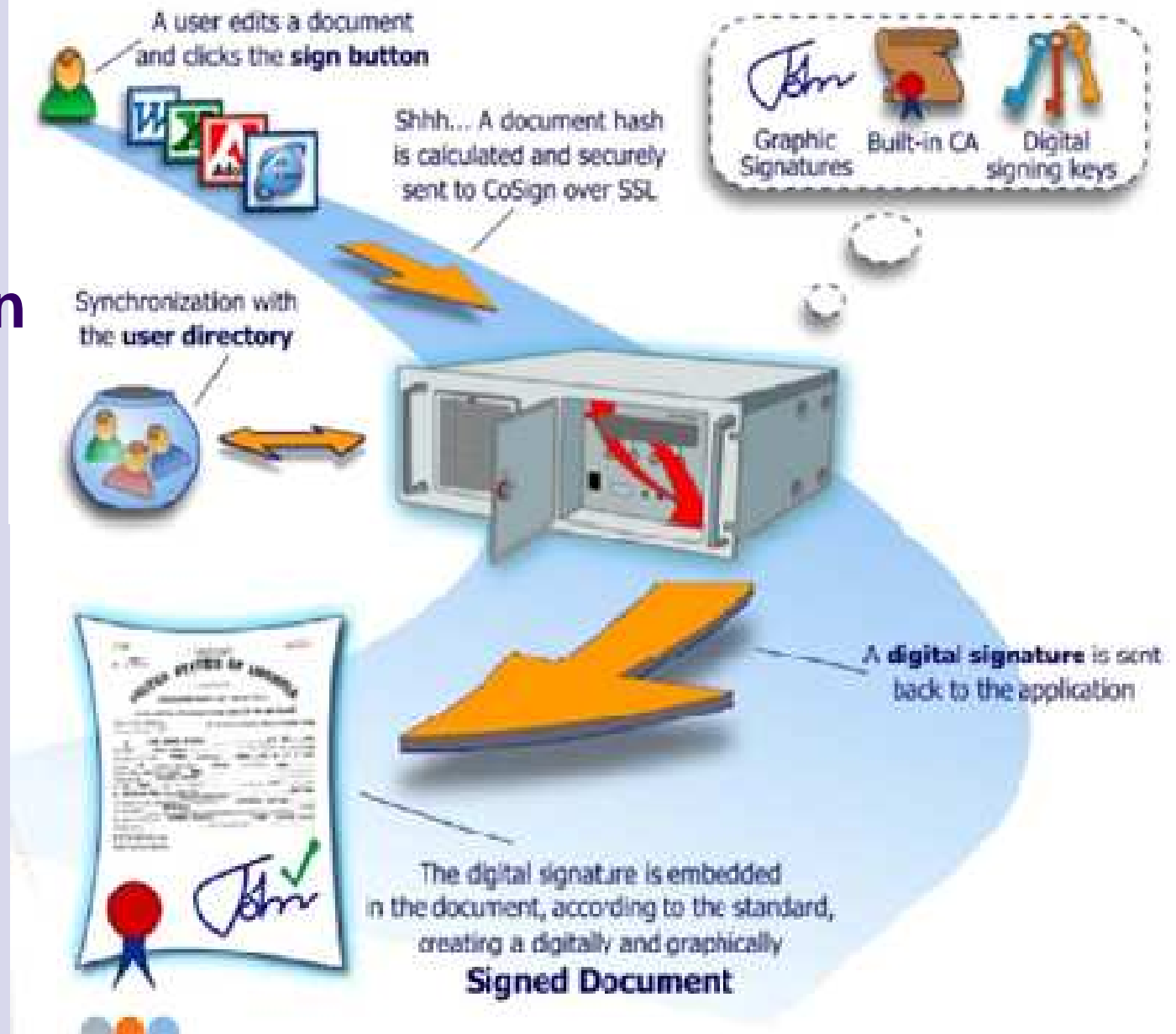


- **Imposter prevention:** By using digital signatures you are actually eliminating the possibility of committing fraud by an imposter signing the document. Since the digital signature cannot be altered, this makes forging the signature impossible.

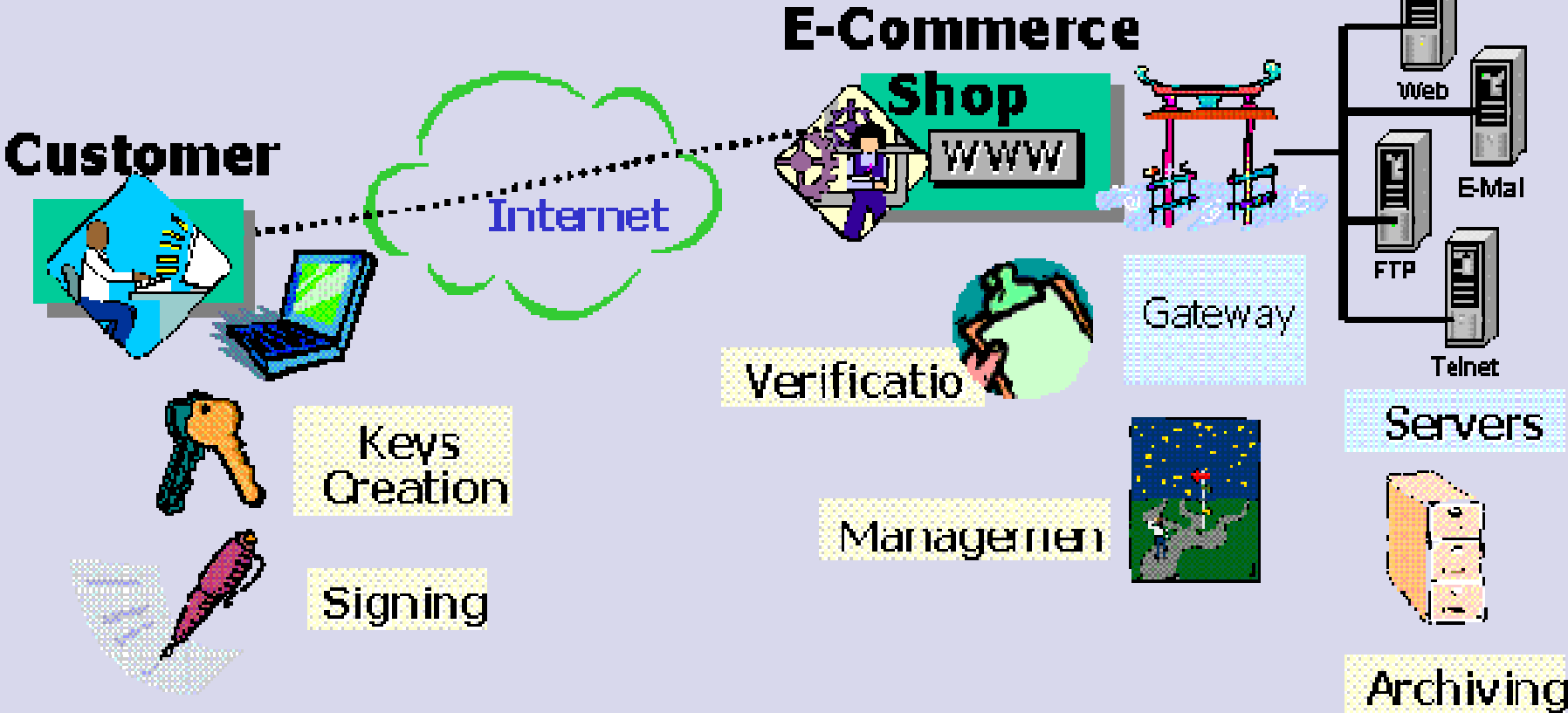


- **Legal requirements:** Using a digital signature satisfies some type of legal requirement for the document in question. A digital signature takes care of any formal legal aspect of executing the document.

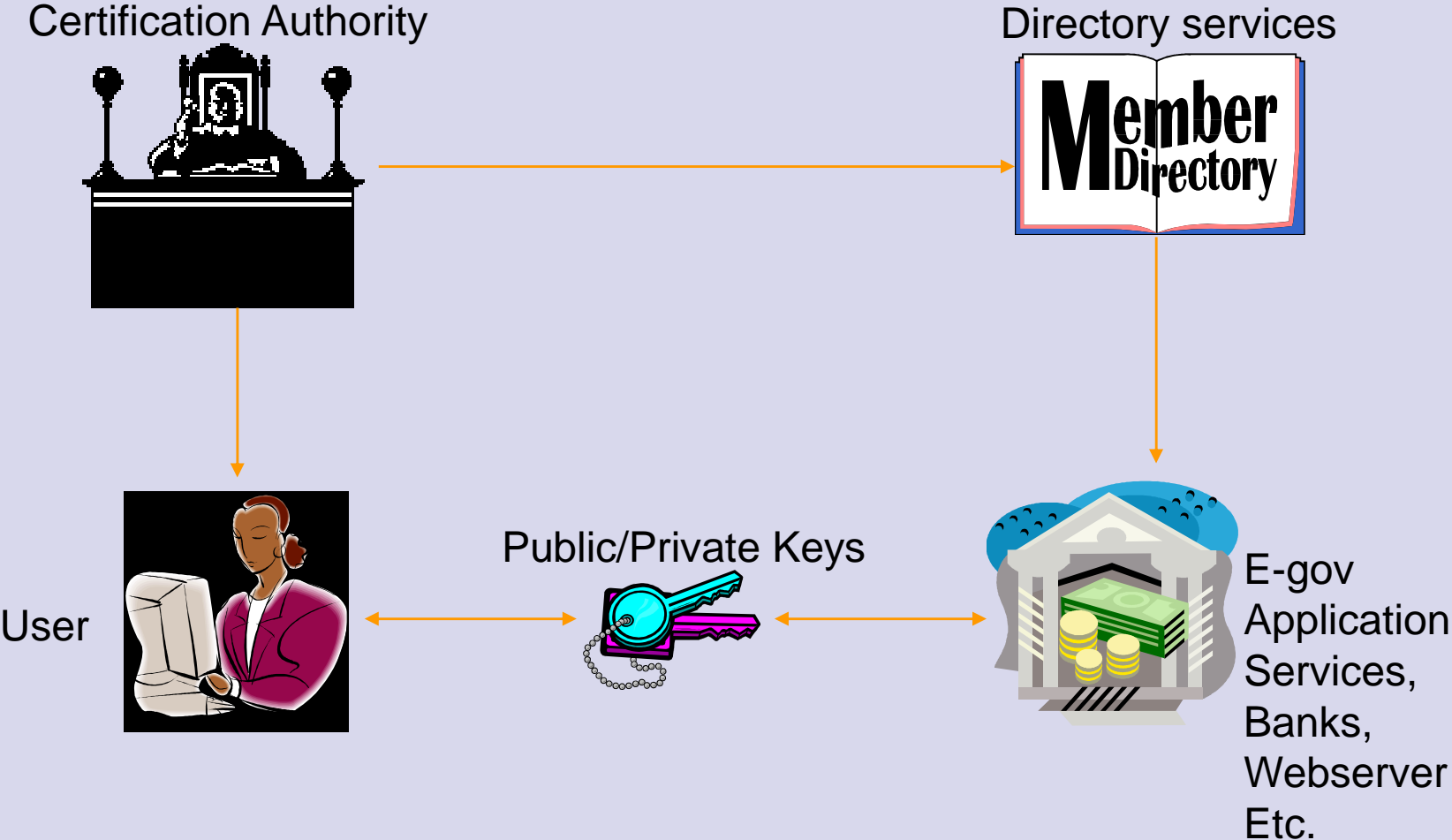
PKI in Authentication



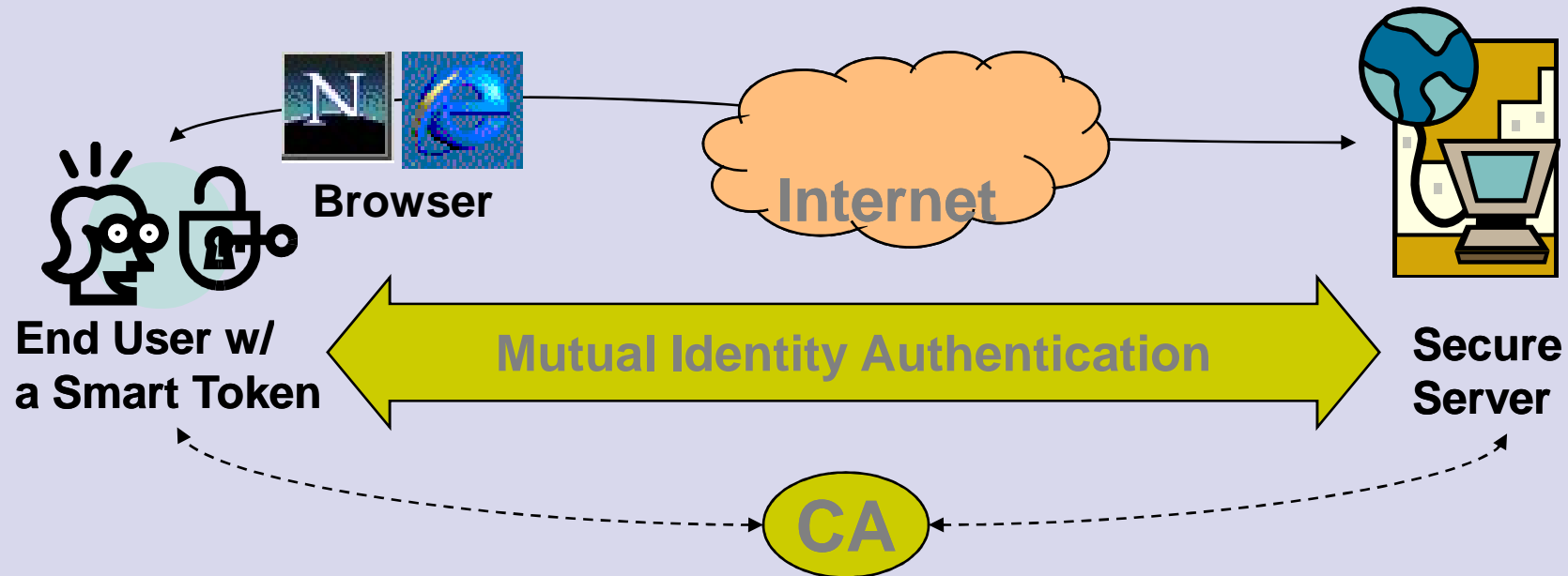
PKI in E-Commerce



PKI Structure



Banking Solution Overview



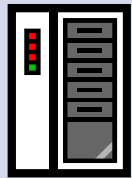
The Client-side includes:

- Smart token

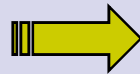
The Server-side includes:

- 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)

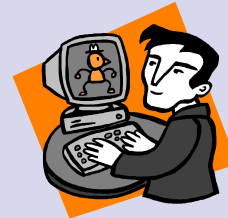
Deployment Overview



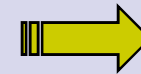
Web site and backend server setup



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



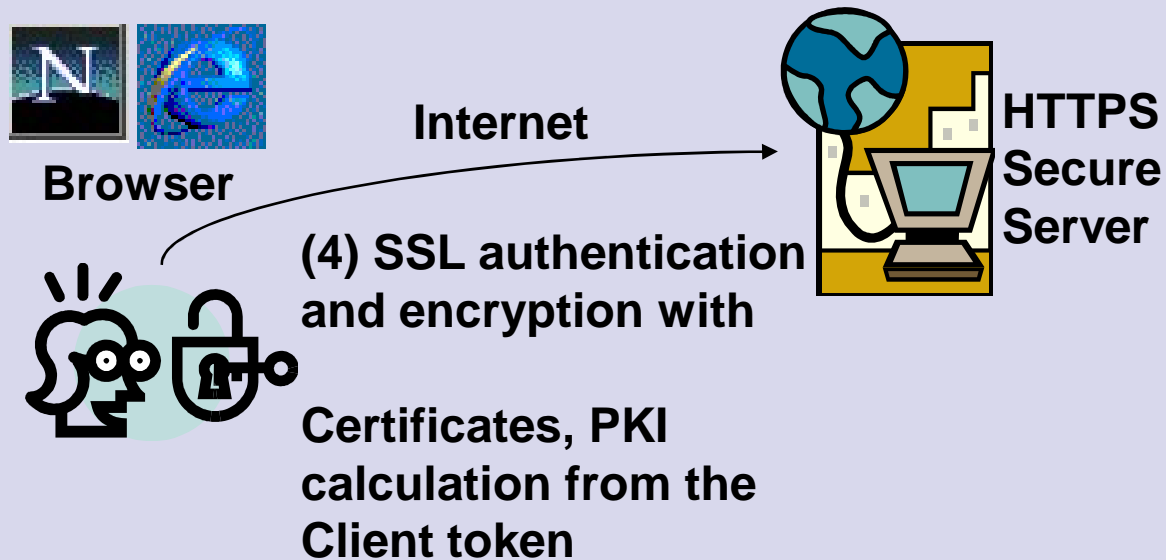
(Future) Web-based self-service for certificate renewal, token loss, damage, etc.



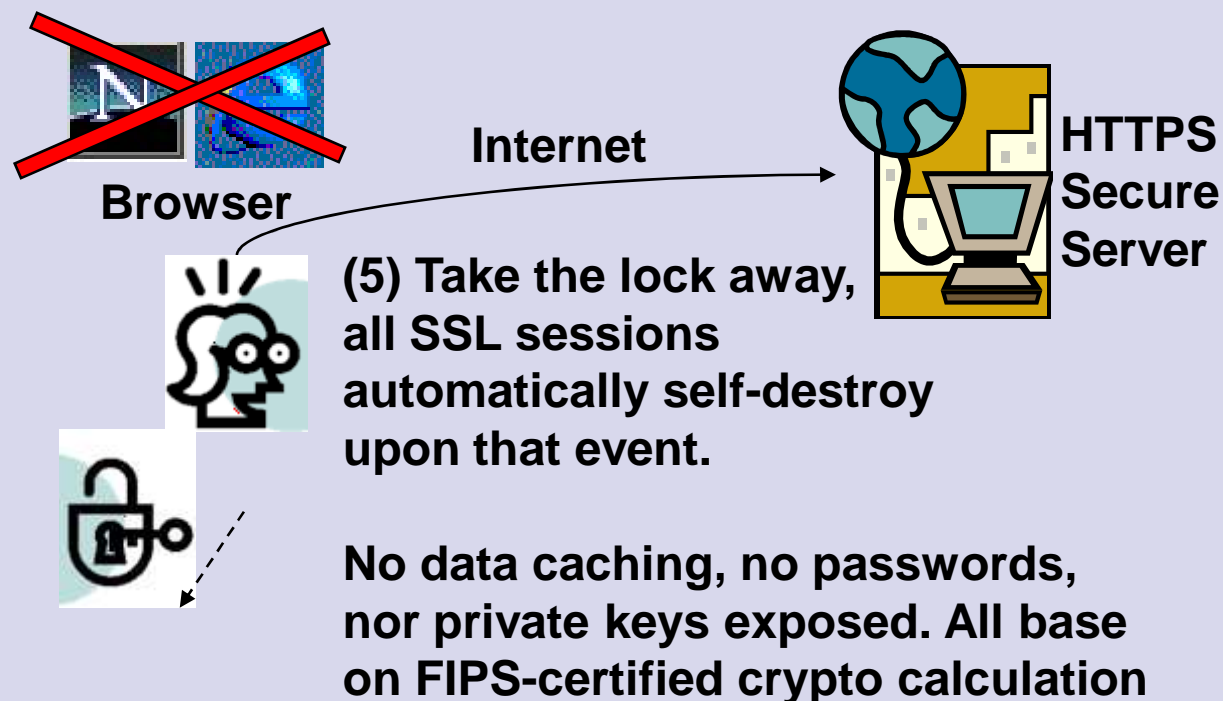
- **Security**
- **Convenience**
- **Simplicity**
- **New revenue**
- **Sharper company image**
- **Customer loyalty**
- **E-Commerce**



Server-Side Authentication



Clean Sign-off, No Traces Left



Summary

Details

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](#)

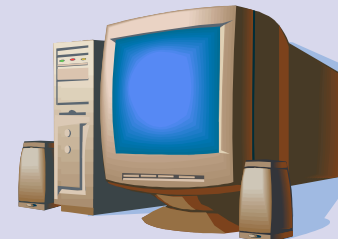


Implication

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

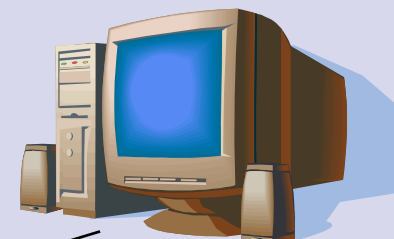


Root CA
Controller Office
National
Repository



OCSP
VM

Government
Issuing CA



CM
CRL



24/7 Help
Desk



CA

Customer



RA

Govt. Dept.

Internet with Secured VPN



Thank you