UN-ESCWA

UNITED NATIONS - Economic and Social Commission for Western Asia

35TH ANNIVERSARY UN-ESCWA

Implementation of e-Signature in the ESCWA Region: Status and Next Steps

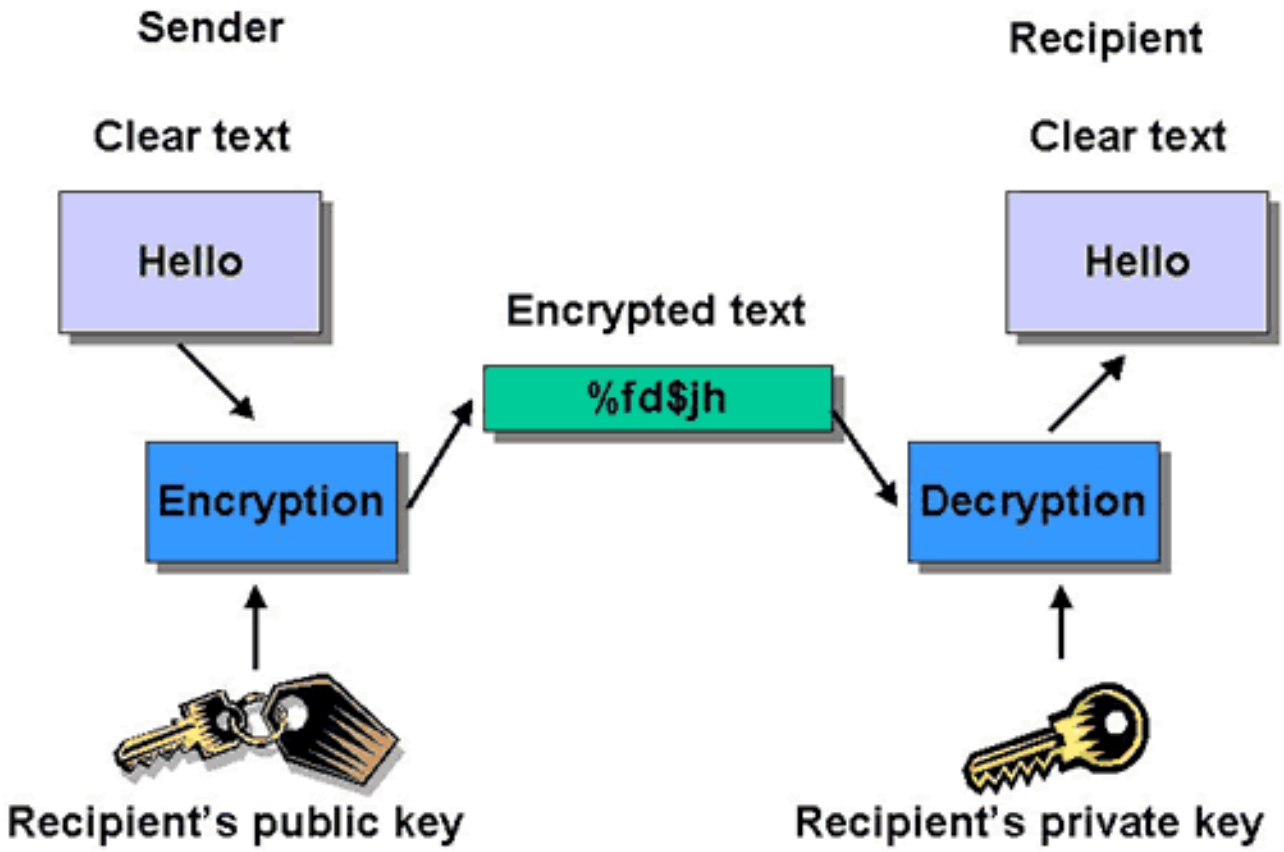
By Matthew Perkins

Understanding e-Signature

- How do we identify ourselves online?
- Electronic records of real-world authenticators
  - Credit Card numbers
  - National ID number
- Clicking the mouse
  - ‘click here to agree’
  - Software shrink-wrap agreements

Sender Verification

- PKI Encryption



Non-repudiation

- Confirms the nature of the document as well as the nature of the signature

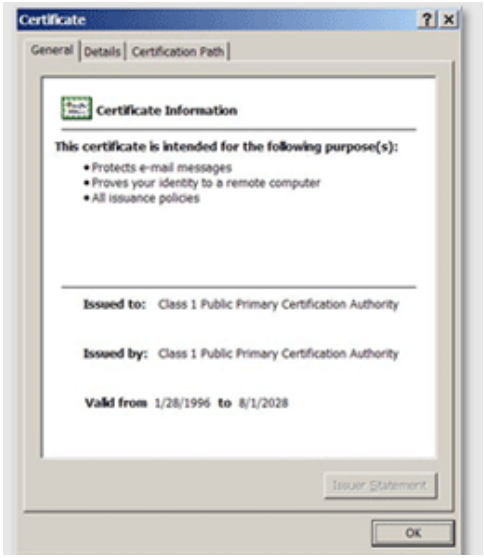
  "A service that provides proof of the integrity and origin of data.

  An authentication that with high assurance can be asserted to be genuine."

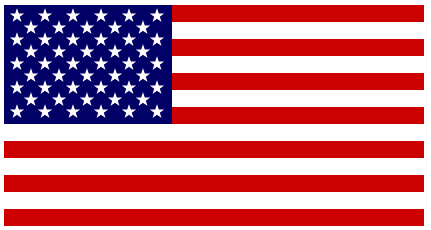
Electronic/Analog Signatures

UN-ESCWA

- Paper Signature
  - Can be forged
  - Document can be altered
- Digital Signature
  - Attachment
- e-Signature
  - Non-repudiation
  - Non-alteration



E-Signature Legal Standards



- US Definition:
- “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

E-Signature Legal Standards

- UN Definition:

"(*a*) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;"

E-Signature Legal Standards

"3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

- (*a*) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
- (*b*) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
- (*c*) Any alteration to the electronic signature, made after the time of signing, is detectable; and
- (*d*) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable."

e-Signature Adoption

Country or territory	e-transaction law	e-signature law	Management of PKI
Bahrain	✓	✓	×
Egypt	✓	✓	✓
Iraq	×	×	×
Jordan	✓	✓	×
Kuwait	×	×	×
Lebanon	×	×	×
Oman	✓	✓	×
estinePal	×	×	×
Qatar	×	×	×
Saudi Arabia	✓	✓	✓
The Sudan	✓	✓	×
Syrian Arab Republic	×	✓	×
United Arab Emirates	✓	✓	×
Yemen	×	×	×

Source: Compiled by ESCWA.

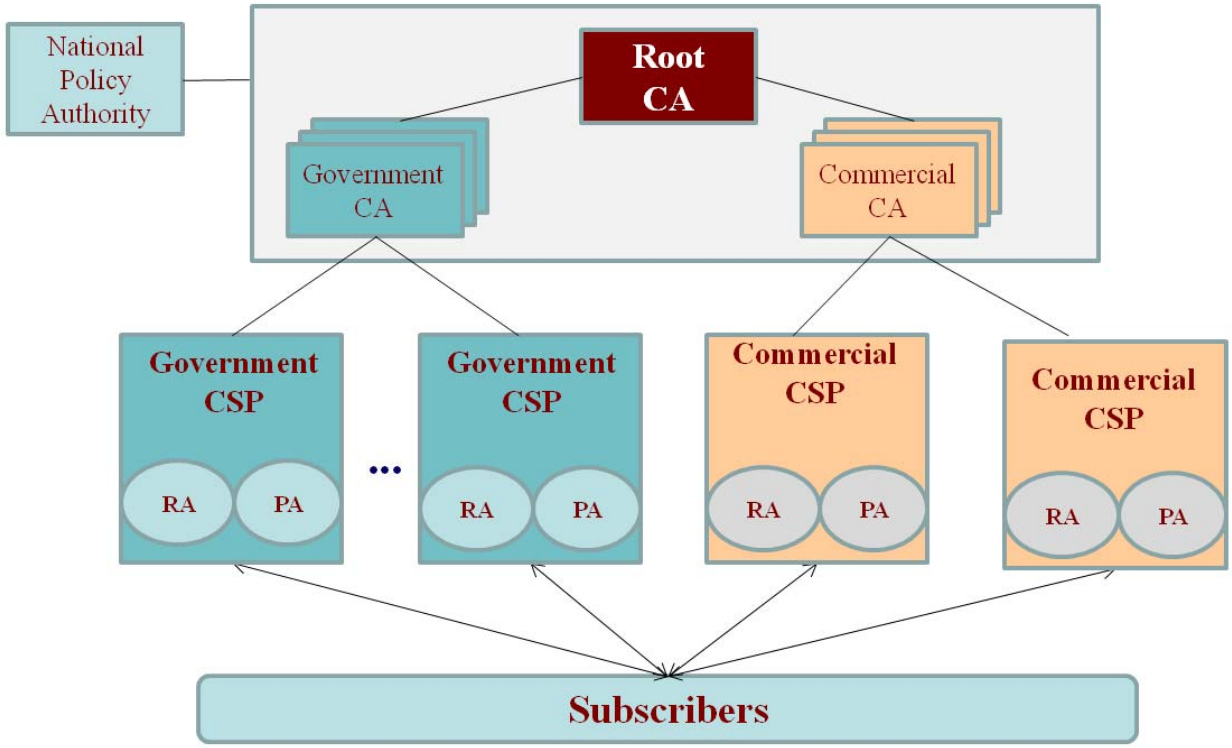
Current Status

- Recommendations from cyber legislation
- Certification authenticators
- Arabic Support
- Does it matter who or where the certifying authority is?

Saudi PKI Example

- National Center for Digital Certification
- “E-Government is the driver for successful PKI deployment”
- Individual level certifications – 3 years.
- Level 1 CA – 10 Years
- Root CA – 20 Years

Saudi PKI Example



Egyptian Example

- e-Signature law passed in 2004:
- "The e-signature is the pillar in e-transactions for all governmental, commercial or administrative sectors. The law marks a key achievement across the IT industry in Egypt and raises the country's competitiveness as a key provider of ground-breaking IT services."

Egyptian Example

- e-Signature law implemented 2005
- ITIDA
- PKI infrastructure went live on 28 September 2009, making Egyptian Root CA services available for the first time.

Bahrain Example

- National e-ID cards
- Digital Signature:
  - The United Arab Emirates became a pioneer in the region for creating a “rule of law” governing electronic transactions when it enacted the Law of Electronic Transactions and Commerce No.2/2002 (Law No. 2) in 2002.

Bahrain Example

- EIDA Rollout
  - e-Identity includes:
    - ID number
    - Name
    - PKI implementation
    - Rolling out to residents as well a citizens

German Example

"De-mail -- a play on the country-code abbreviation for Deutschland (Germany) and the word e-mail -- is a government-backed service in which all messages will be encrypted and digitally signed so they cannot be intercepted or modified in transit. Businesses and individuals wanting to send or receive De-mail messages will have to prove their real-world identity and associate that with a new De-mail address from a government-approved service provider."

Next Steps

- Steps:
- Importance of adoption of standards
- Harmonization of approach
- Goals:
- Facilitate e-transactions
  - Government processes, e-commerce transactions
  - B2b, b2c

Summary

- Many methods of facilitating e-transactions
- Linking to real-world systems
- Digital systems
- Differing legal definitions
- Harmonized standards necessary
- Health of e-transactions not correlated to use of encrypted e-signatures?

Thank you