Distr.
LIMITED
E/ESCWA/ICTD/2003/WG.1/CRP.19
31 January 2003
ORIGINAL: ENGLISH

ESCWA

ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA

Western Asia Preparatory Conference for the World
Summit on the Information Society (WSIS)
Beirut, 4-6 February 2003

Ministry of
Telecommunications

infoDev

SECURITY ON THE INTERNET

UNESCO

Salah Rustom
President ITIA

UN ICT Task Force

ITU

Note: This document has been reproduced in the form in which it was received, without formal editing. The opinions expressed are those of the author and do not necessarily reflect the views of ESCWA.

03-0102

ITIA
LEBANON
IT AND INTERNET ASSOCIATION

GlobalSign The Certification Authority

Security on the Internet

Salah Rustom

President, ITIA

Western Asia Preparatory Conference for WSIS

Beirut - ESCWA [February 4-6, 2003]

Security Risks

- As you all know, the Internet is an open Network that allows all those interested to view what is being transmitted, alter its contents and claim that the mail has actually originated from a different 3rd party all together.
- Consequently, with the increased number of users the infringement of other people's privacy became a common practice and the interests of those using the Internet for commercial reasons were jeopardized.

Security Risks

- As a result, experts investigated various possibilities to secure commercial transactions and looked into other venues to safeguard the database of commercial enterprise.
- Some of the common attack methods are outlined here under for your guidance:
- Denial of Service / Session Hijacking / DNS Poisning Security Account Manager Exploit and backdoor attacks

Security Risks

- Defense Mechanism may be described as follows:
  a. Perimeter Defenses
  b. Network, Data & e-mail Defenses
  d. PKI & E-Signature
  e. Application Defenses
  g. Physical Security

Digital Certificates & PKI

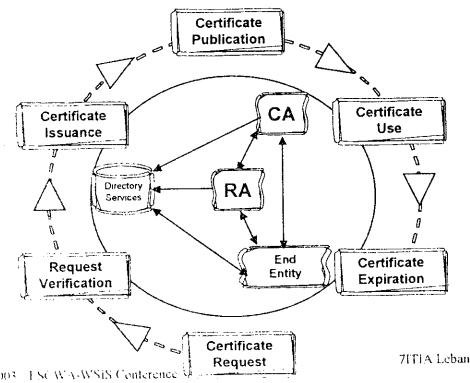
- An x.509 digital certificate allows each participant of an electronic transaction to prove his/her identity towards the other participants.
- These Certificates are used as the digital equivalent of an ID card.
- PKI is the application of an x.509-based digital certificates to establish secure messaging or transaction over networks.

Digital Certificates & PKI

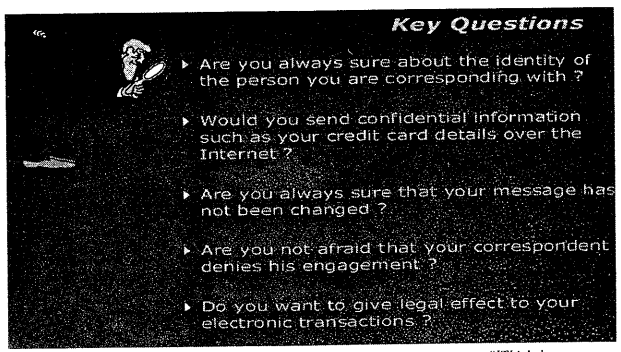
Digital Certificates are used to establish:

- Authentication of the sender's identity.
- Integrity:The inability to change contents of the e-document after its creation.
- Non-repudiation - validity after creation.
- Confidentiality: Secrecy of exchanged contents of the e-document.

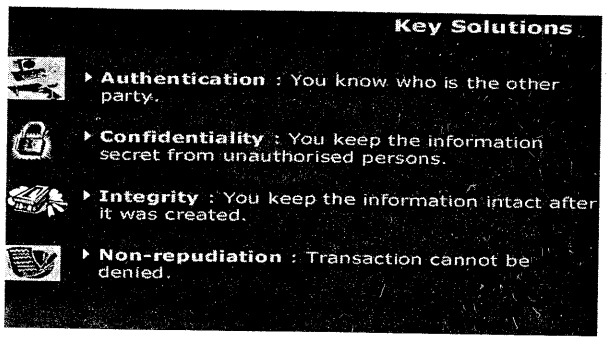
Certificate Lifecycle



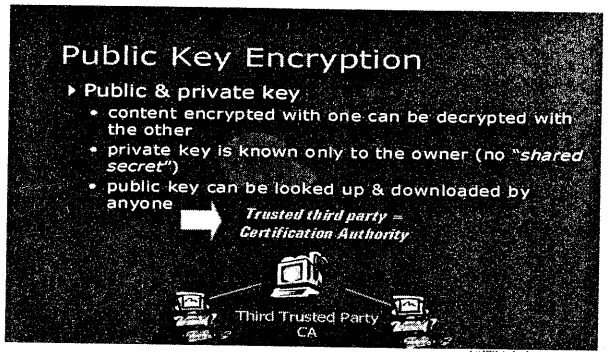
The Internet & Privacy



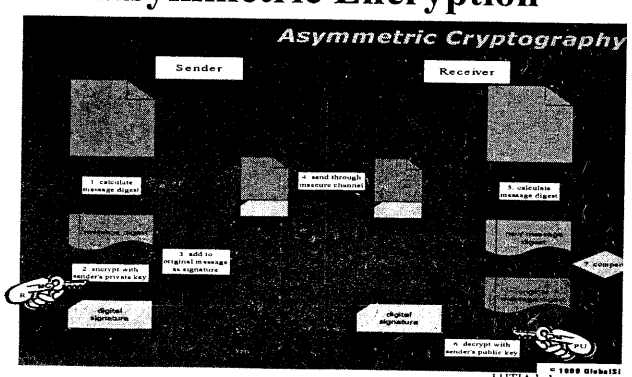
Peace of Mind & Satisfaction



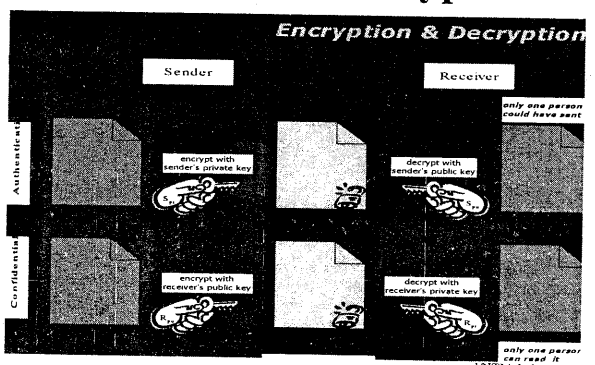
The Private / Public Keys !



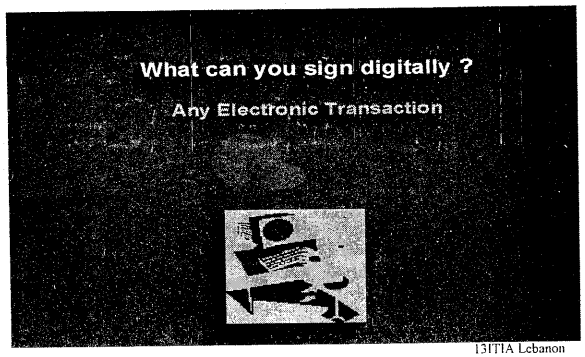
Asymmetric Encryption



Encryption & Decryption



E-Signature & Applicability

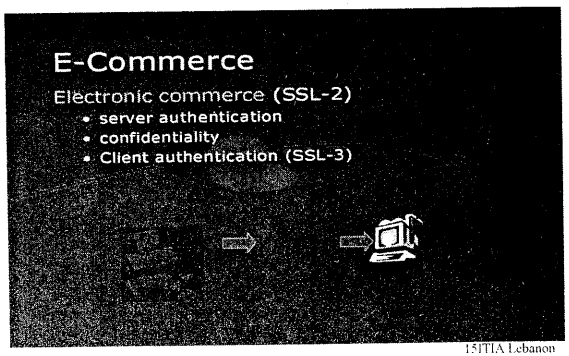


Secure E-mail

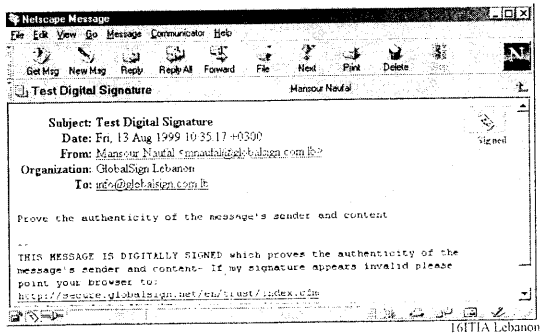
Secure email communication (S/MIME)

- digital signatures
  - authenticity of the sender
  - authenticity of the content
- confidentiality
- non-repudiation
- integrity

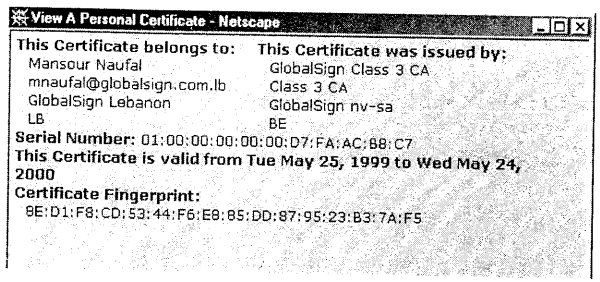
Server Authentication e-Banking



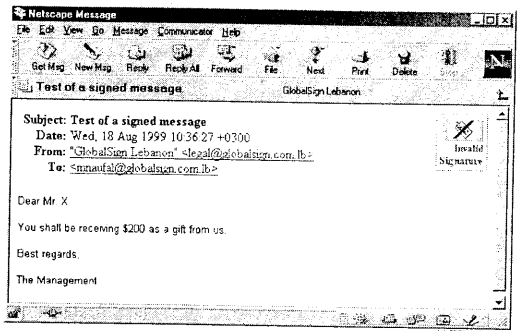
Non Repudiation



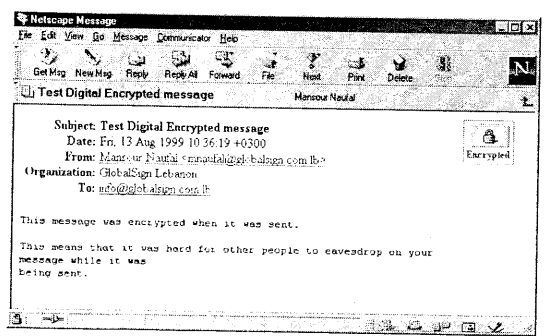
Digital ID



Signed Message - Integrity



Confidentiality & Encryption



Certification Practice Statement

This document describes in detail the practices and procedures used for the management of certificates.

Contents of CPS:

Properties of certificates

Financial stability, records & accreditation.

Relationship between the CA & the user on one hand and between the CA & the Government on the other and vice versa.

In Brief

- **Independent mail boxes will most certainly allow us to receive a positive impulse, and the Internet rate of growth will multiply.**
- **Should we aim for a paperless community we must aide and encourage the application of digital IDs on all our mail.**
- **Do not worry about time wasted - Investing is not a waste! It is solid human pre-occupation.**
- **To enhance the Internet, we should not only speak of its colossal benefits, but should do something about it. Let us be the good example!**

WSIS Conference Members

♥ Thank you for hearing me out!

Dr Salah A. Rustum
Chairman GlobalSign Lebanon &
President IT & Internet Association [ITIA]
http://itialebanon.org
http://www.globalsign.com.lb
Khorafi Bldg/Clemenceau Street
RL-2021 6404 Beirut