

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



ESCWA



Ministry of
Telecommunications



infoDev



UNESCO



UN ICT Task Force



ITU

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

UN ECONOMIC AND SOCIAL COMMISSION
FOR WESTERN ASIA

07-05-2003

LIBRARY & DOCUMENTATION SECTION

SECURITY ON THE INTERNET

Salah Rustom
President ITIA

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



GlobalSign The Certification Authority

Security on the Internet

Salah Rustom
President, ITIA



Western Asia Preparatory Conference for WSIS

Beirut - ESCWA [February 4-6, 2003]

1

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.

FEB 04-06/2003 - ESCWA-WSIS Conference

2ITIA Lebanon

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 Poisoning
Security Account Manager Exploit and backdoor attacks

FEB 04-06/2003 - ESCWA-WSIS Conference

3ITIA Lebanon

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

FEB 04-06/2003 - ESCWA-WSIS Conference

4ITIA Lebanon

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.

FEB 04-06/2003 - ESCWA-WSIS Conference

51TIA Lebanon

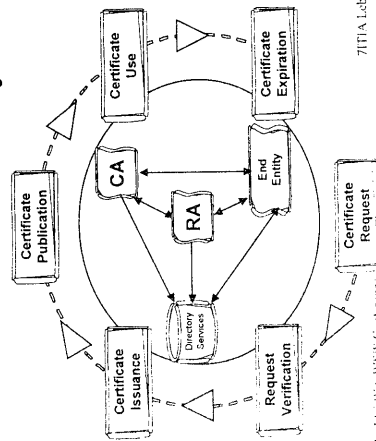
Digital Certificates & PKI

- 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.

FEB 04-06/2003 - ESCWA-WSIS Conference

61TIA Lebanon

Certificate Lifecycle



FEB 04-06/2003 - ESCWA-WSIS Conference

71TIA Lebanon

The Internet & Privacy

Key Questions

- ▶ Are you always sure about the identity of the person you are corresponding with ?
- ▶ Would you send confidential information such as your credit card details over the Internet ?
- ▶ Are you always sure that your message has not been changed ?
- ▶ Are you not afraid that your correspondent denies his engagement ?
- ▶ Do you want to give legal effect to your electronic transactions ?

FEB 04-06/2003 - ESCWA-WSIS Conference

81TIA Lebanon

Peace of Mind & Satisfaction

Key Solutions

- ▶ **Authentication** : You know who is the other party.
- ▶ **Confidentiality** : You keep the information secret from unauthorised persons.
- ▶ **Integrity** : You keep the information intact after it was created.
- ▶ **Non-repudiation** : Transaction cannot be denied.



FEB 04-06/2003 - ESCWA-WSSIS Conference

9/11/14 Lebanon

The Private / Public Keys !

Public Key Encryption

- ▶ **Public & private key**
 - content encrypted with one can be decrypted with the other
 - private key is known only to the owner (no "shared secret")
 - public key can be looked up & downloaded by anyone

Trusted third party =
Certification Authority

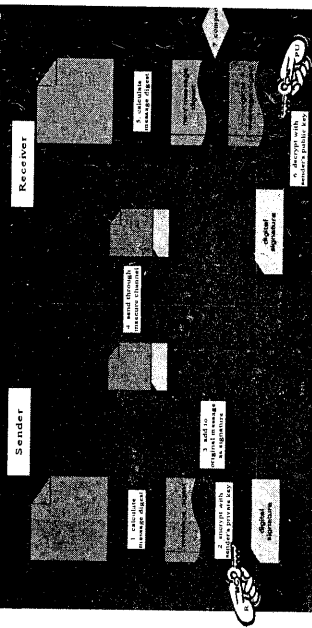


FEB 04-06/2003 - ESCWA-WSSIS Conference

11/11/14 Lebanon

Asymmetric Encryption

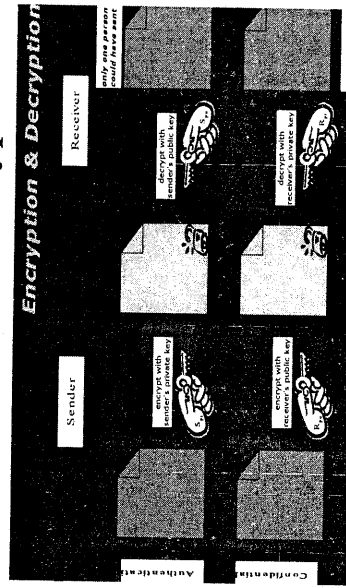
Asymmetric Cryptography



FEB 04-06/2003 - ESCWA-WSSIS Conference

11/11/14 Lebanon

Encryption & Decryption



FEB 04-06/2003 - ESCWA-WSSIS Conference

11/11/14 Lebanon

E-Signature & Applicability

What can you sign digitally?
Any Electronic Transaction



13THIA Lebanon

FEB 04-06/2003 - ESCWA-WSSIS Conference

Secure E-mail

Secure email communication (S/MIME)

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



14THIA Lebanon

FEB 04-06/2003 - ESCWA-WSSIS Conference

Server Authentication e-Banking

E-Commerce

Electronic commerce (SSL-2)

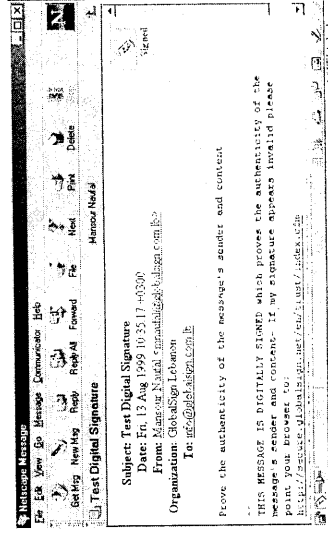
- server authentication
- confidentiality
- Client authentication (SSL-3)



13THIA Lebanon

FEB 04-06/2003 - ESCWA-WSSIS Conference

Non Repudiation



14THIA Lebanon

FEB 04-06/2003 - ESCWA-WSSIS Conference

Digital ID

View A Personal Certificate - Netscape

This Certificate belongs to: **This Certificate was issued by:**
Mansour Naoufal
GlobalSign, Class 3 CA
Class 3 CA
GlobalSign nv-sa
LB
BE
GlobalSign nv-sa

Serial Number: 01:00:00:00:00:00:07:FA:AC:68:C7
This Certificate is valid from Tue May 25, 1999 to Wed May 24, 2000

Certificate Fingerprint:
8E:D1:F8:CD:53:44:F6:E8:85:DD:87:95:23:B3:7A:1F:5

FEB 04-06/2003 - ESCWA-WSIS Conference

17TITA Lebanon

Signed Message - Integrity

Netscape Message

Subject: Test of a signed message
Date: Wed, 18 Aug 1999 10:58:27 +0300
From: 'Simaufal@globalign.com.lb' <simaufal@globalign.com.lb>
To: 'Simaufal@globalign.com.lb' <simaufal@globalign.com.lb>

Dear Mr. X

You shall be receiving \$200 as a gift from us.

Best regards,
The Management

FEB 04-06/2003 - ESCWA-WSIS Conference

17TITA Lebanon

Confidentiality & Encryption

Netscape Message

Subject: Test Digital Encrypted message
Date: Fri, 13 Aug 1999 10:36:19 +0300
From: Mansour Naoufal - simaufal@globalign.com.lb
Organization: GlobalSign Lebanon
To: simaufal@globalign.com.lb

This message was encrypted when it was sent.
This means that it was hard for other people to eavesdrop on your message while it was being sent.

FEB 04-06/2003 - ESCWA-WSIS Conference

17TITA Lebanon

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.

FEB 04-06/2003 - ESCWA-WSIS Conference

20TITA Lebanon

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!

FEB 04-06/2103 - ESCWA-WSIS Conference

21/ITIA Lebanon

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

FEB 04-06/2103 - ESCWA-WSIS Conference

22/ITIA Lebanon