5th GLOBAL FORUM ON REINVENTING GOVERNMENT:

“INNOVATION AND QUALITY IN GOVERNMENT FOR THE 21ST CENTURY”

CAPACITY BUILDING WORKSHOP:
“NEW ICT AND E-GOVERNMENT”

5-6 November 2003, Mexico City, Mexico

Building Trust and Confidence for Critical E-government Services

Alexander NTOKO
Chief, E-Strategy Unit
ITU Telecommunication Development Bureau (BDT)
1. Issues
2. Framework
3. Solutions
4. Strategies
A Transaction-based E-government Infrastructure

**But how do we get governments, businesses and citizens to conduct critical government transactions online?**
As many countries embark on the e-government bandwagon, governments, citizens and businesses are asking many questions – Can we trust these systems?

- Receiving online submissions to renew national identity cards:
  \[G: \text{Am I dealing with the owner of the identity card?}\]
  \[C: \text{How do I know this is really a government site?}\]

- Submitting confidential bids for government procurements:
  \[G: \text{Is the bid from a registered company?}\]
  \[B: \text{Can my competitors see my bid?}\]

- Transmitting sensitive government documents online.
  \[G: \text{Can an unauthorized person view the document?}\]
  \[G: \text{How can access control be ensured?}\]
• Issuing birth certificates and land certificates via the Internet:
  
  G: Can a citizen modify his or her date of birth?
  G: What if she changes the size of her land or uses this to make another land certificate?

• Conducting online elections via the Internet – e-voting:
  
  C: Can someone know whom I voted for?
  G: How do we guarantee that a citizen votes only once?
  G: Is this vote from a registered voter?
It is mostly about TRUST
Having firm integrity in something or somebody

- An entity A, can be said to trust another entity B when A makes the assumption that B will behave exactly as A expects.

Identification is the Challenge

"On the Internet, nobody knows you’re a dog..."

In addition to privacy, security and policies, knowing whom you are dealing with is vital for building trust.
Technology Framework for Online Trust

Five (5) Key Requirements – The big 5!
This list is NOT exhaustive but constitutes vital elements for trust.

- **Data Confidentiality**
  - Information accessed only by those authorized.

- **Data Integrity**
  - No information added, changed, or taken out.

- **Strong Authentication**
  - Parties are who they pretend to be.

- **Non-repudiation**
  - Originator cannot deny origin or transaction.

- **Infrastructure of trust**
  - Automating the verification of digital credentials.
1. Digital Envelope

Combines the high speed of symmetric encryption (e.g., AES Rijndael) and the key management convenience of public key encryption. Includes PSE (Smartcards, Mega-brid, USB tokens), biometrics, Hardware Security Modules etc.

One time encryption Key
Recipient’s Public Key
“Digital Envelope”
Combines Hash Algorithms (FIPS-180), Key Exchange, Public Key Encryption to provide **Data integrity**, **Non-repudiation** and Certificate-based **Authentication**. Digital credentials are established using ITU-T X.509 Digital Certificate Standard.
Technology Framework for Online Trust

3. Digital Certificate

ITU-T X.509 creates the framework for establishing digital identities – A key component for establishing security and trust for ICT applications in public networks (such as the Internet)
# Industry Solutions for Online Trust and Security

## Common e-Security Technologies

<table>
<thead>
<tr>
<th>Topology</th>
<th>Authentication</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Non-repudiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Firewalls</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Why Public Key Infrastructure (PKI)
and What Solutions do Industry Provide?

- It’s **Not** about waging a technology war (*PKI vs Non-PKI*) but combining technologies and policies for total solutions.
- Combines various industry solutions and standards – PKCS#11, PSE (Smart Cards, Tokens Megabrid), OCSP Transponders, HSMs, CA, RA and Content Validation Software.
- Enables security and trust to be built on comprehensive and interoperable solutions with appropriate policies ensuring national sovereignty and enforceable legislation.
- Most highly rated e-government countries have PKI as an important component of their e-government strategy.
Building Online Trust For E-Government

Digital Signature – Issues and Challenges

- Acceptance of Digital Signatures Across Multi-Jurisdictional PKI Domains (at the National, Regional and Global Levels).
- Adopting Policies for Generic Identity Certificates (PKI) and the relationship with Attribute Certificates (Privilege Management Infrastructures).
- Elaborating Harmonized and Technology Neutral E-Legislative Framework and Enforcement Mechanisms.
Strategy for E-Signatures and CAs

Online Trust and Security for e-Government Needs to be part of a comprehensive policy framework dealing with other e-services
What could be the Role of Governments in fostering e-government deployment and use?

- National/Regional Policies for the Management of Public IP Resources to ensure fair and equitable allocation of:
  - Internet Protocol Addresses
  - Domain Names (under ccTLDs)
- Creating an Enabling Environment for E-Applications (e.g.,):
  - Accreditation of Certification Authorities
  - Control and Enforcement Mechanisms (e.g., anti- Spam and Data privacy legislations).
  - Harmonized Regional Framework E-Legislation
- Active Role in Implementing e-government.
ITU Development Activities in E-government
Activities undertaken within the past three years.

- Projects using trust technologies (encryption, digital certificates, biometrics, smart cards/USB tokens) implemented in Bulgaria, Burkina Faso, Cambodia, Ecuador, Peru, Senegal, Turkey and Vietnam.
- Workshops/Seminars on technology policies in Africa, Asia, Arab Region, Latin America and World.
- Assistance to ASETA, Burkina Faso, Cape Verde and Mongolia to elaborate legislation for e-signatures.
- Agreement with EU for projects in 2004-2005 period.
- Policy analysis, guidelines and best practices.
- Multi-lateral and self-regulatory framework launched - World e-Trust Memorandum of Understanding.
ITU WTDC02 E-Strategies Programme
An Overview of Related Projects and Activities
For e-government to move from simple web-based systems for disseminating government information to transaction-based services for critical applications, citizens, governments and businesses must all have TRUST in the solutions.

Thank You
for your attention

For further information:
Web:  http://www.itu.int/ITU-D/e-strategy
Email: e-strategy@itu.int