Building Trust and Security for IP-based Networks and Services

6-9 December 2004 – Suva, Fiji

Alexander NTOKO
Chief, E-Strategies Unit
ITU Telecommunication Development Bureau (BDT)

©1998-2004 ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit..

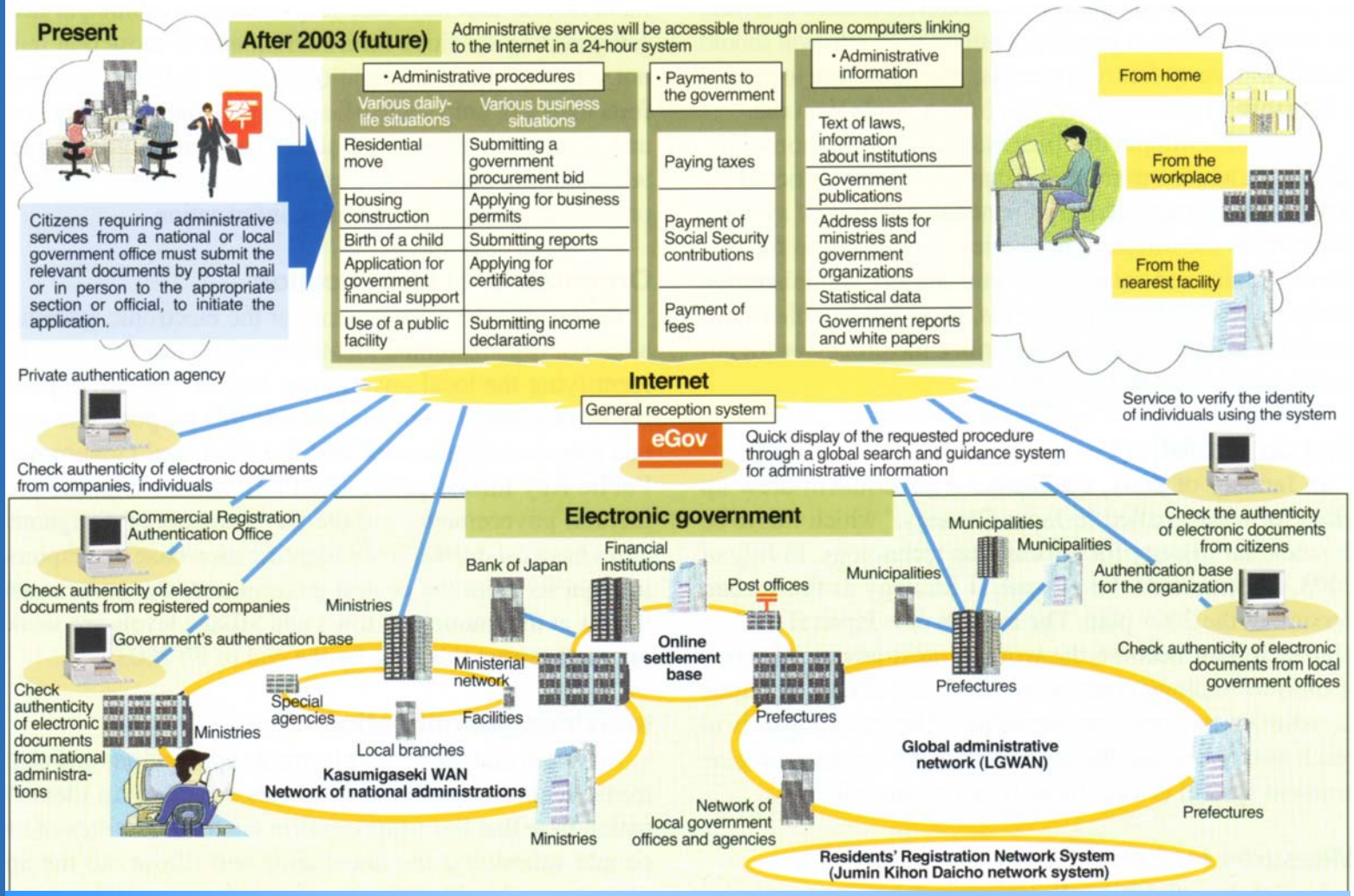
As Pacific Island States work on their national and sub-regional policies, strategies and legislation for ICTs, security and trust concerns must be addressed in these frameworks…

Agenda

1. Threats
2. Framework
3. 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: Am I dealing with the owner of the identity card?
  C: How do I know this is really a government site?

- Submitting confidential bids for government procurements:
  G: Is the bid from a registered company?
  B: Can my competitors see my bid?

- Transmitting sensitive government documents online.
  G: Can an unauthorized person view the document?
  G: 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?

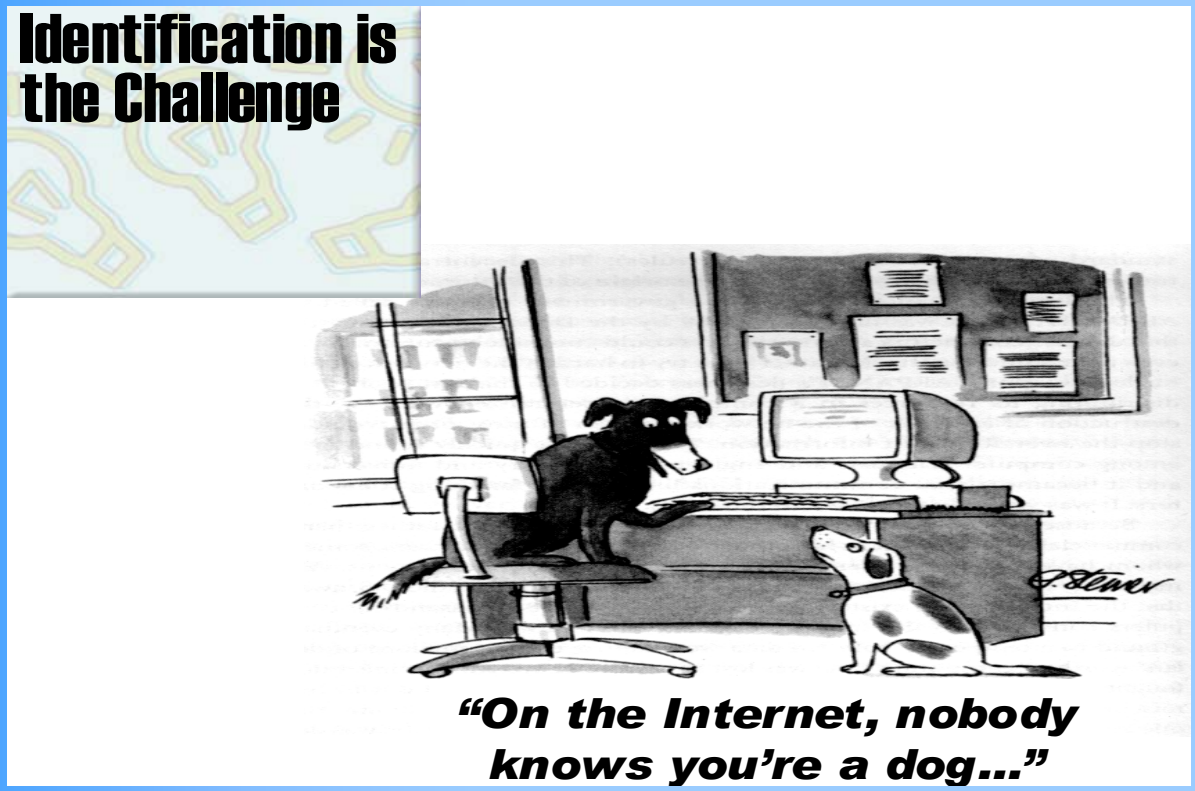
The main e-security threats…

1. Identity Interception: The observation of identities of communicating parties for misuse.
2. Data Interception: The observation of user data during a communication by an unauthorized user.
3. Manipulation: The interception and modification of information in a private communication.
4. Masquerade: Pretending to be another user to access information or to acquire additional privileges.
5. Replay: The recording and subsequent replay of a communication at some later date.
6. Repudiation: The denial by a user of having participated in part or all of a communication.
7. Denial of Service: The prevention or interruption of a communication or the delay of time-critical operations.
8. Traffic Analysis: The unauthorized analysis and observation of information (e.g. frequency, sequence, type, amount, etc.).

But 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.



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

Technology Framework for Online Trust

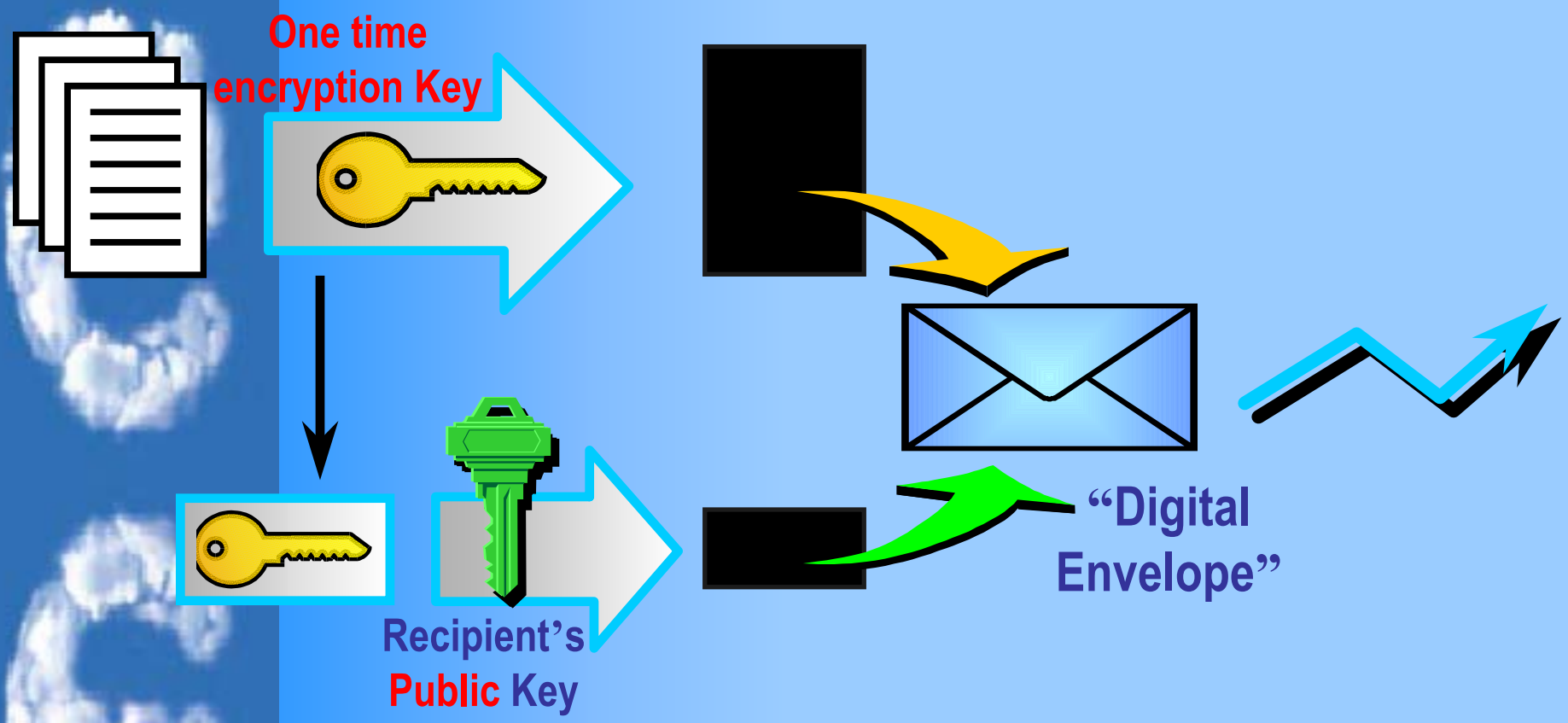
Five (5) Key Requirements – The big 5!

This list is NOT exhaustive and 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.

Technology Framework for Online Trust

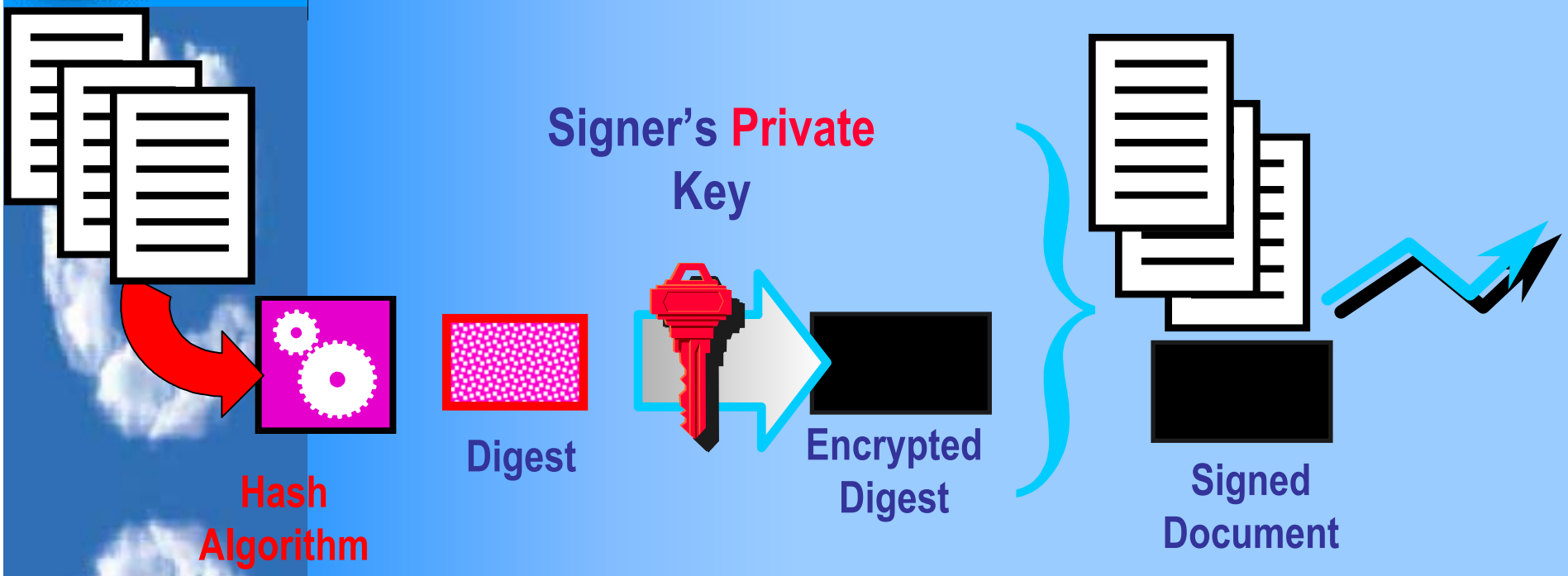
1. Digital Envelope



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

Technology Framework for Online Trust

2. Digital Signature



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

Simple Diagram of ITU-T X.509 Certificate Version 3

- Certificate version, serial number and signature algorithm
- Certificate Authority Name
- Certificate holder information (Name, Organisation, Address etc.)
- Public Key of certificate holder
- X.509 V3 Certificate Extensions
- Digital Signature of Certificate Authority

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)

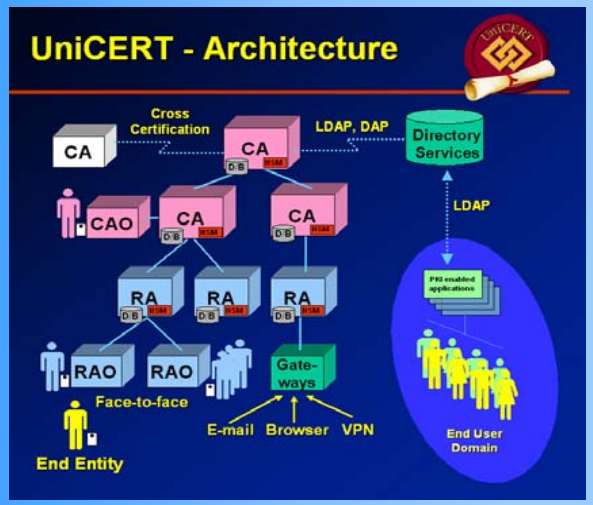
Industry Solutions for Online Trust and Security

Common e-Security Technologies

	Authentication	Confidentiality	Integrity	Non-repudiation
Anti-virus			✓	
Firewalls	✓	✓		
Access Control	✓	✓		
Encryption		✓		
Public Key Infrastructure	✓	✓	✓	✓

Public Key Infrastructure (PKI) and Industry Solutions for Trust

- 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, 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.

Cross Certification

- A CA issues a certificate to another CA. This is applied to Strict Hierarchy (Root CAs)
- Establishment of Trust Relationship between CAs (Chain of Trust).
- Could result in Trust Cascades (A>B and B>C should not imply A>C).
- Trust relationship could be Mutual (Horizontal Trust relationship) or Unilateral (Vertical Trust relationship – Root CAs).

Bridge Certificate Authority

- A CA acts as a bridge between CAs in different PKI domains.
- Each CA establishes a Trust Relationship with the Bridge CA.
- The absence of direct relationships between CAs avoids overheads related to the establishment of direct trust relationships between co-operating CAs.

Cross Recognition

- No trust relationship on cross certification between CAs.
- Requires a mutually trusted and recognized third party.
- CA-CA Interoperability is achieved through the licensing or auditing by a mutually agreed authority.

Accreditation Certificate

- A combination of cross-certification and cross recognition.
- Involves the creation of an accreditation CA.
- Public Key of each CA is signed by accreditation CA.
- Used in Australia in the Gatekeeper Accreditation CA.
- Requires high level government structure and control to create hierarchy (e.g., government-wide PKI).

Certificate Policy – Plays an important role in the implementation of some of these initiatives

- Certificate Policy (CP) – A Named set of rules that indicate the applicability of a certificate to a particular community and/or class of applications of common security requirements.

ITU-T X509: CA-CA Policy Interoperability

Policy Mappings Extension

Allows a certification authority to indicate that certain policies in its own domain can be considered equivalent to certain other policies in the subject certification authority's domain.

ITU-T X.509: Preventing Trust Cascades

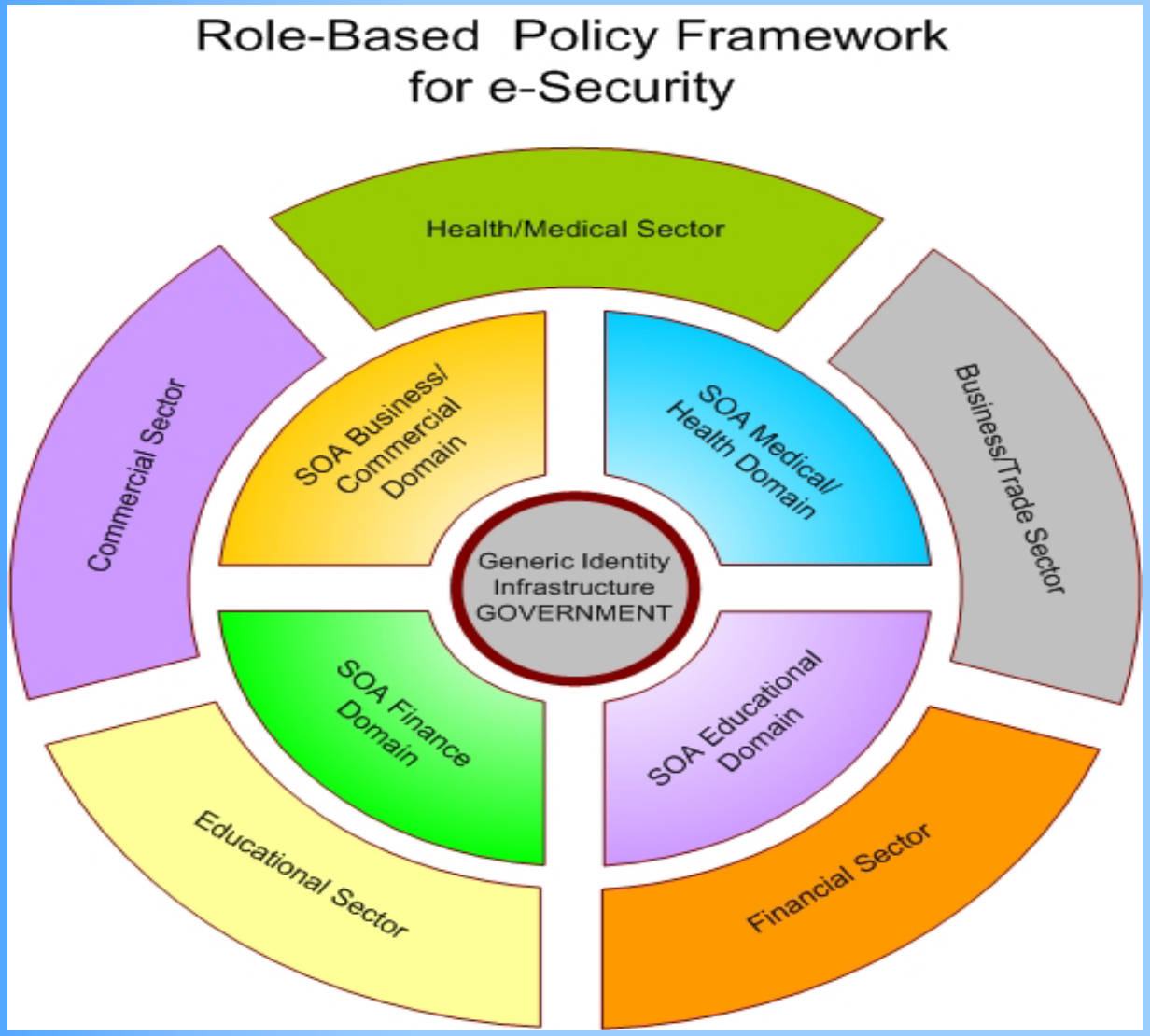
Policy Constraints extension

Ability for a certification authority to require that explicit certificate policy indications be present in all subsequent certificates in a certification path.

Ability for a certification authority to disable policy mapping by subsequent certification authorities in a certification path.

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 (Spam, Spim, Phishing and Data privacy legislations).
  - Harmonized Regional Framework E-Legislation
- Active Role in Implementing e-government.

CONCLUSION

For ICT applications to deliver services aimed at reducing the social divide, enhancing basic services in health, educational, commercial and government sectors, citizens, governments and businesses must all have **TRUST** in the technologies and the solutions.

Thank You

for your attention

For further information:

Web: http://www.itu.int/ITU-D/e-strategy

Email: e-strategy@itu.int