Building Confidence in E-government Services

ITU-T Workshop on Challenges, Perspectives and Standardization Issues in E-government

Geneva, 5-6 June 2003

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

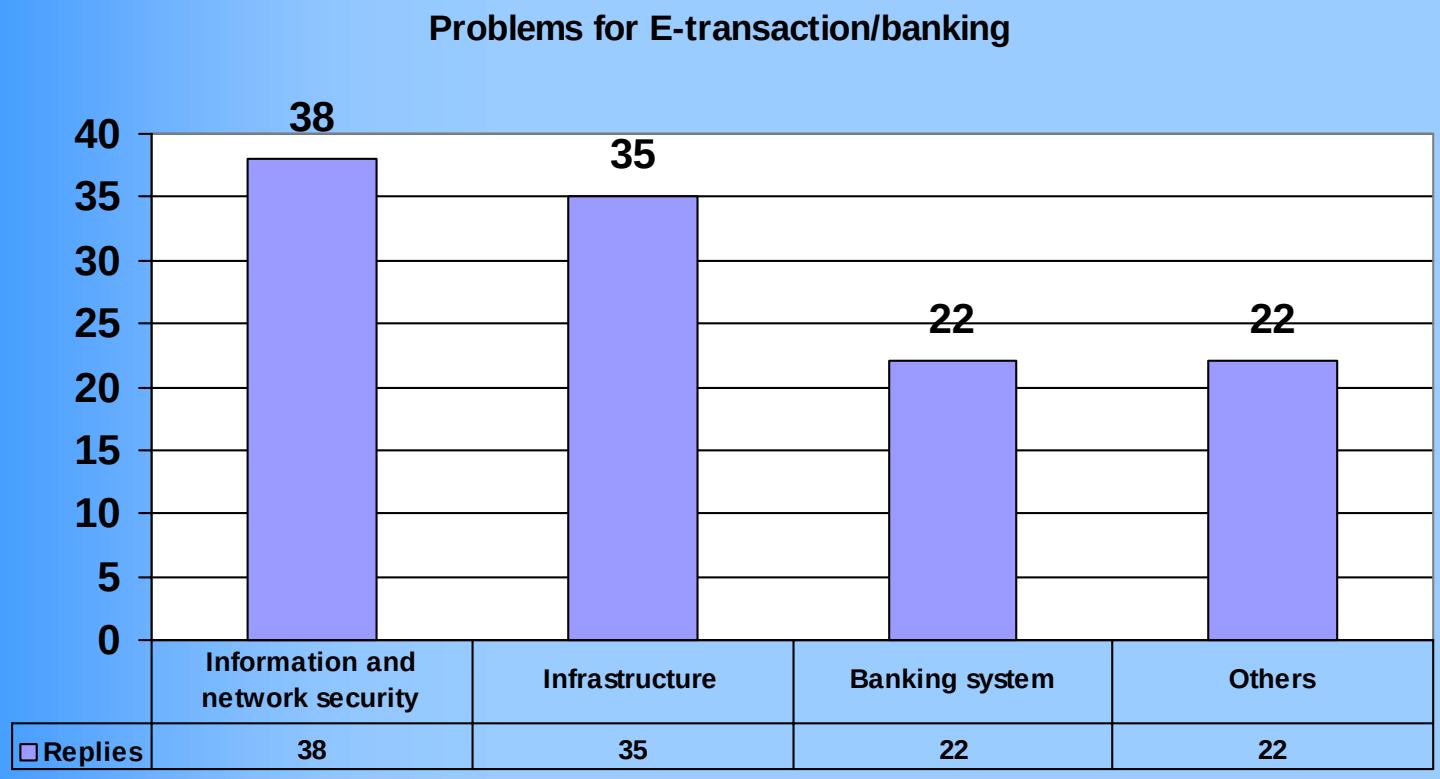
But Why?

A Holistic Approach to Building Confidence is A <u>Key</u> Driver for E-government.

…Because the challenges for DCs are not just limited to technology and access

Security plays a central role in building user confidence for e-government services

Security concerns for e-applications are quite high in the priorities of Developing Countries



Results of ITU-D Survey (March 2003) on Challenges to E-Transactions. WTDC02 IsAP Programme3 - Security

What is TRUST?

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

Its about having confidence in government services provided via Telecommunications/ICTs.

Knowing who you are dealing with remains a major concern

Identification is the Challenge

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

...but in e-government, it is important to Know if you are dealing with a dog.

What are some of the security concerns?

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.).

Let's Map some of the Security/Trust Issues to Possible Solutions…

Identity Interception: Confidentiality (Strong Encryption).

Data Interception: Confidentiality (Strong Encryption).

Manipulation: Data Integrity (Digital Signatures).

Masquerade: Authentication (Digital Certificates)

Replay: Digital Signatures + with Time Stamp.

Repudiation: Digital Signatures.

Denial of Service: Authentication and Access Control.

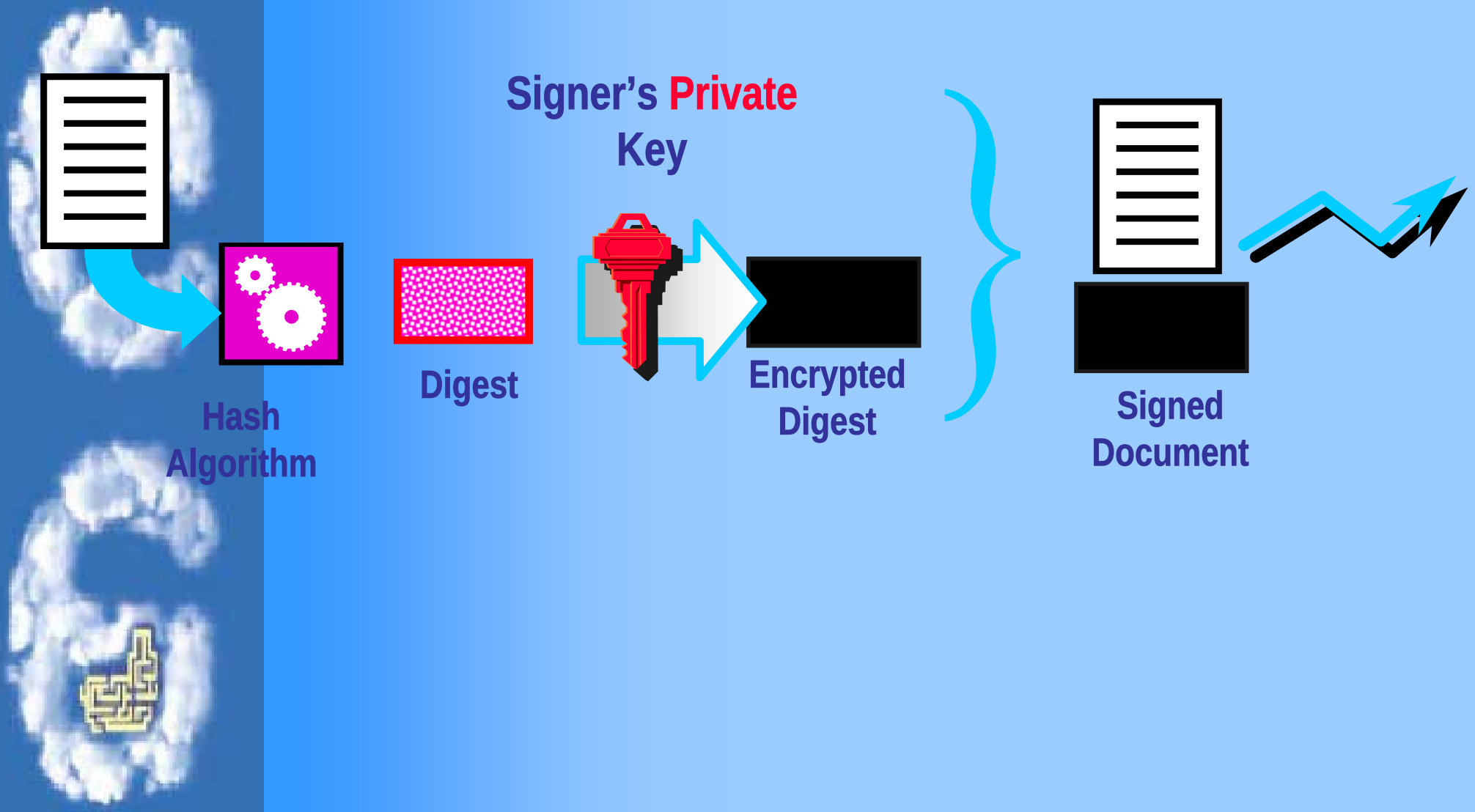
Traffic Analysis: Strong Encryption.

…It is clear that identity verification/management plays a crucial role in addressing many of these problems…

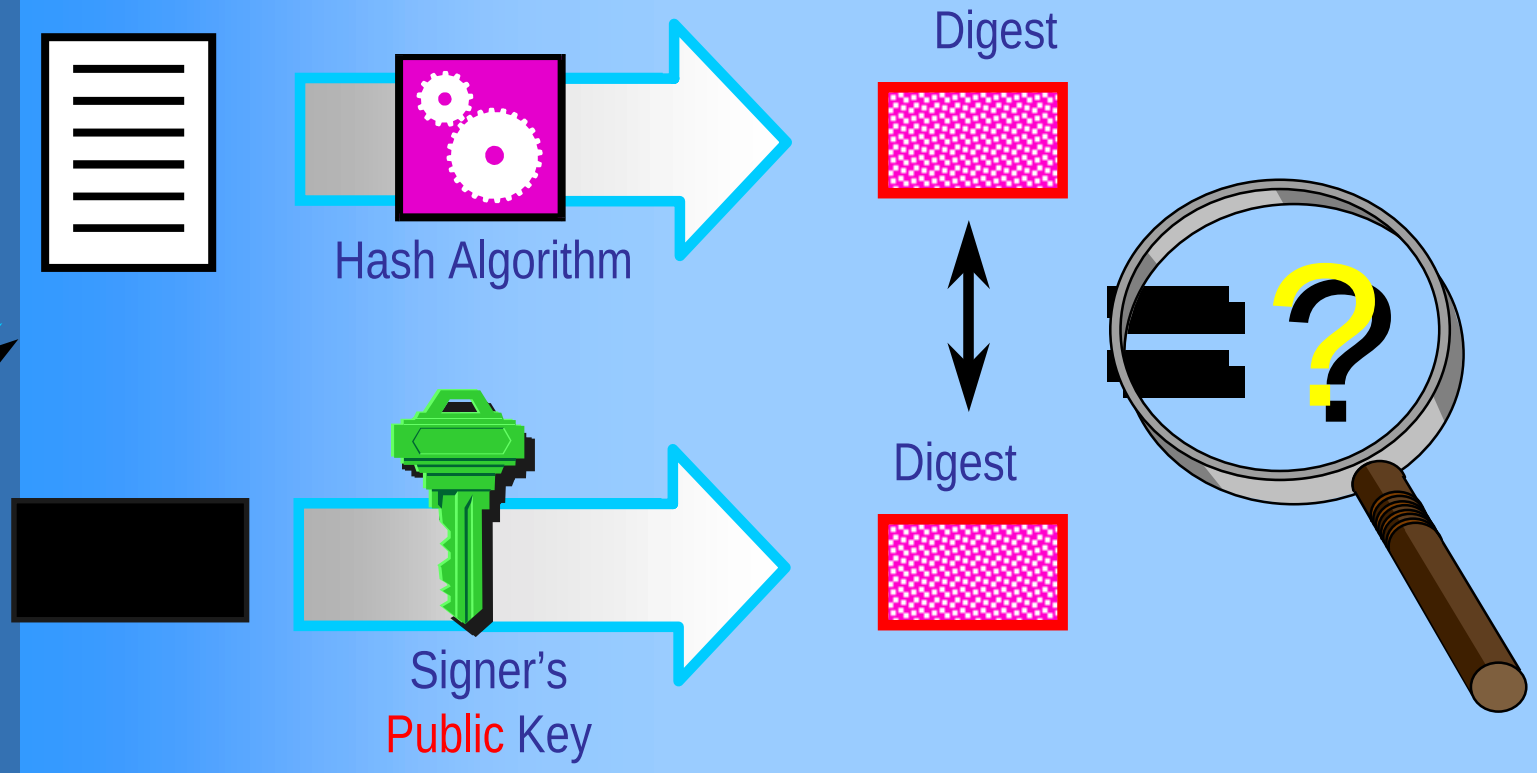
Simple Diagram of ITU-T X.509 Certificate Version 3

- 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

Digital Signatures are central to the Solution



Verifying the Digital Signature for Authentication and Data Integrity



Integrity: One bit change in the content changes the digest

What Solutions do Digital Signatures provide?

Guarantees:

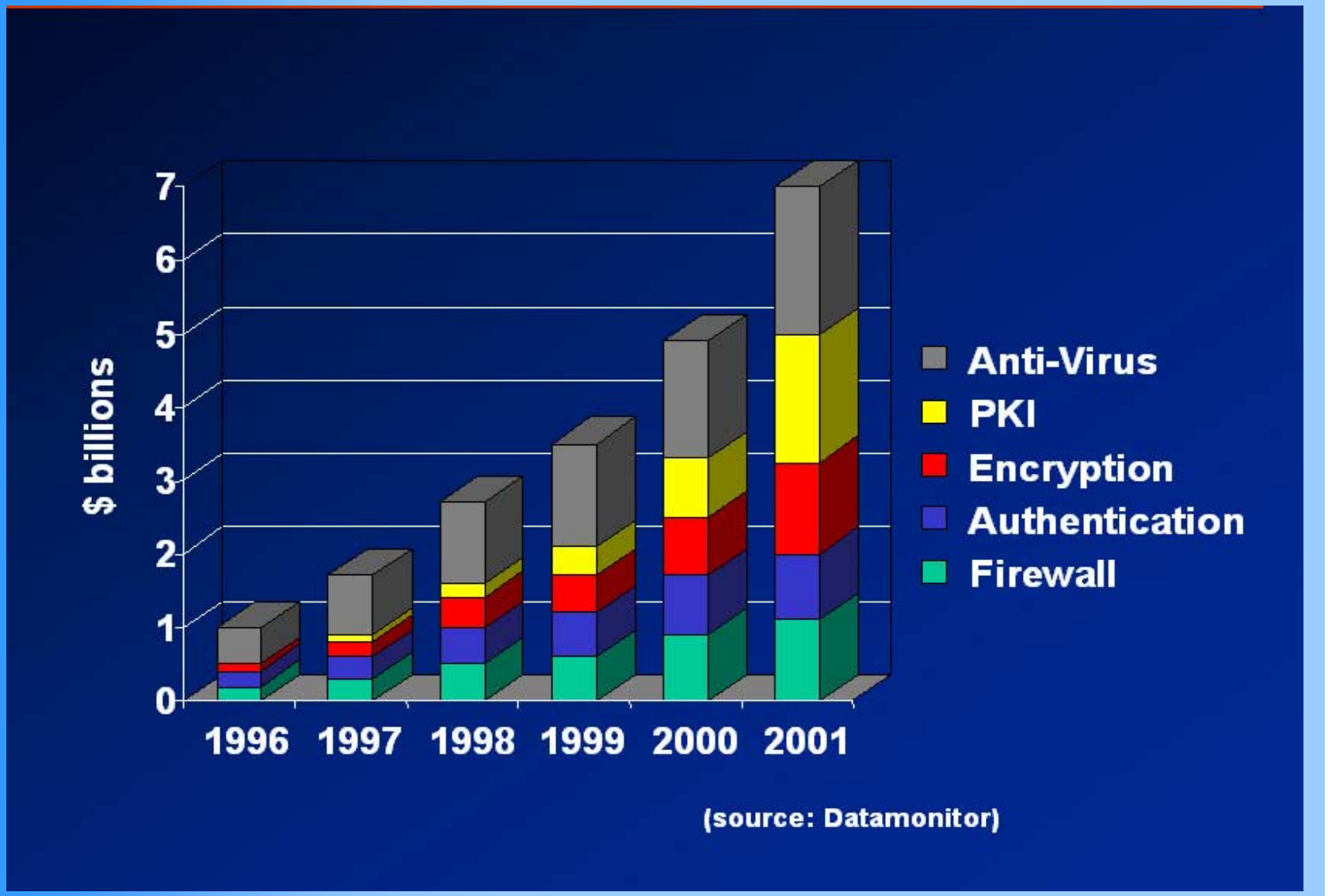
- **Integrity of document**
  One bit change in document changes the digest
- **Authentication of sender**
  Signer's public key decrypts digest sent and decrypted digest matches computed digest
- **Non-repudiation**
  Only signer's private key can encrypt digest that is decrypted by his/her public key and matches the computed digest. Non-repudiation prevents reneging on an agreement by denying a transaction.

How do different Technologies Address the main Security Challenges for E-government?

Common e-Security Technologies

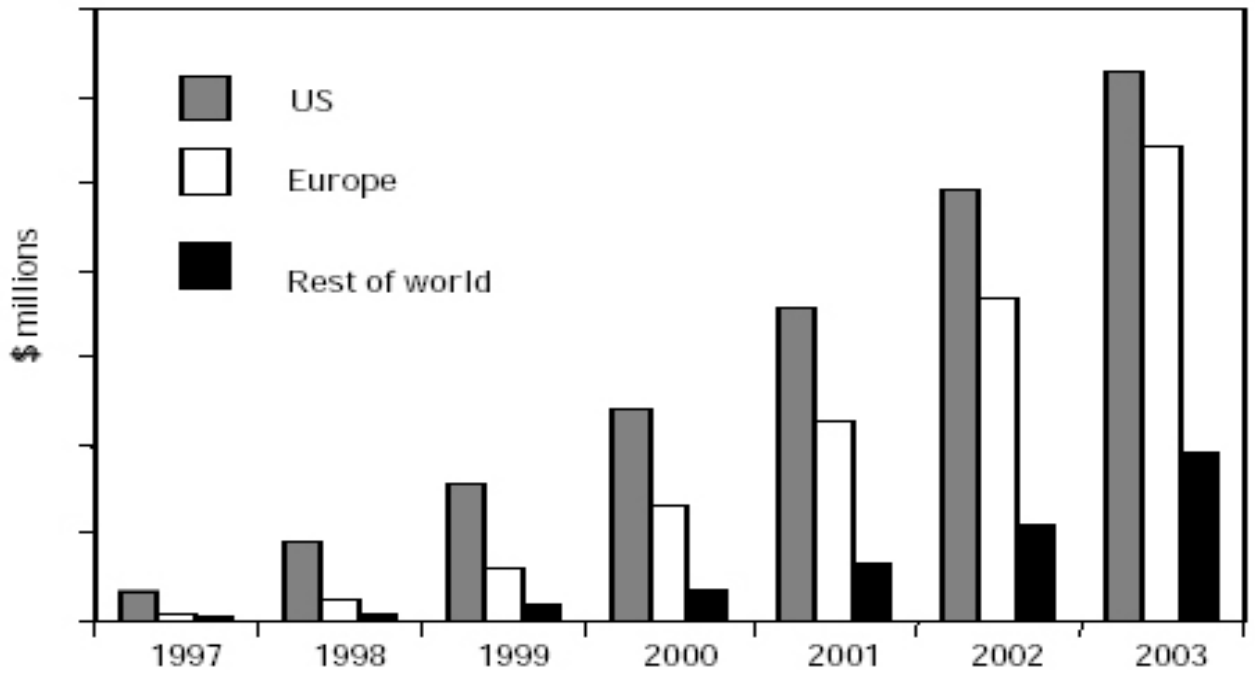
	Authentication	Confidentiality	Integrity	Non-repudiation
Anti-virus			✓	
Firewalls	✓	✓		
Access Control	✓	✓		
Encryption		✓		
Public Key Infrastructure	✓	✓	✓	✓

Growing Demand for Security and Trust



Reflected in growth projections for PKI

HOW WILL PKI UPTAKE VARY BY REGION AND LINE OF BUSINESS ?

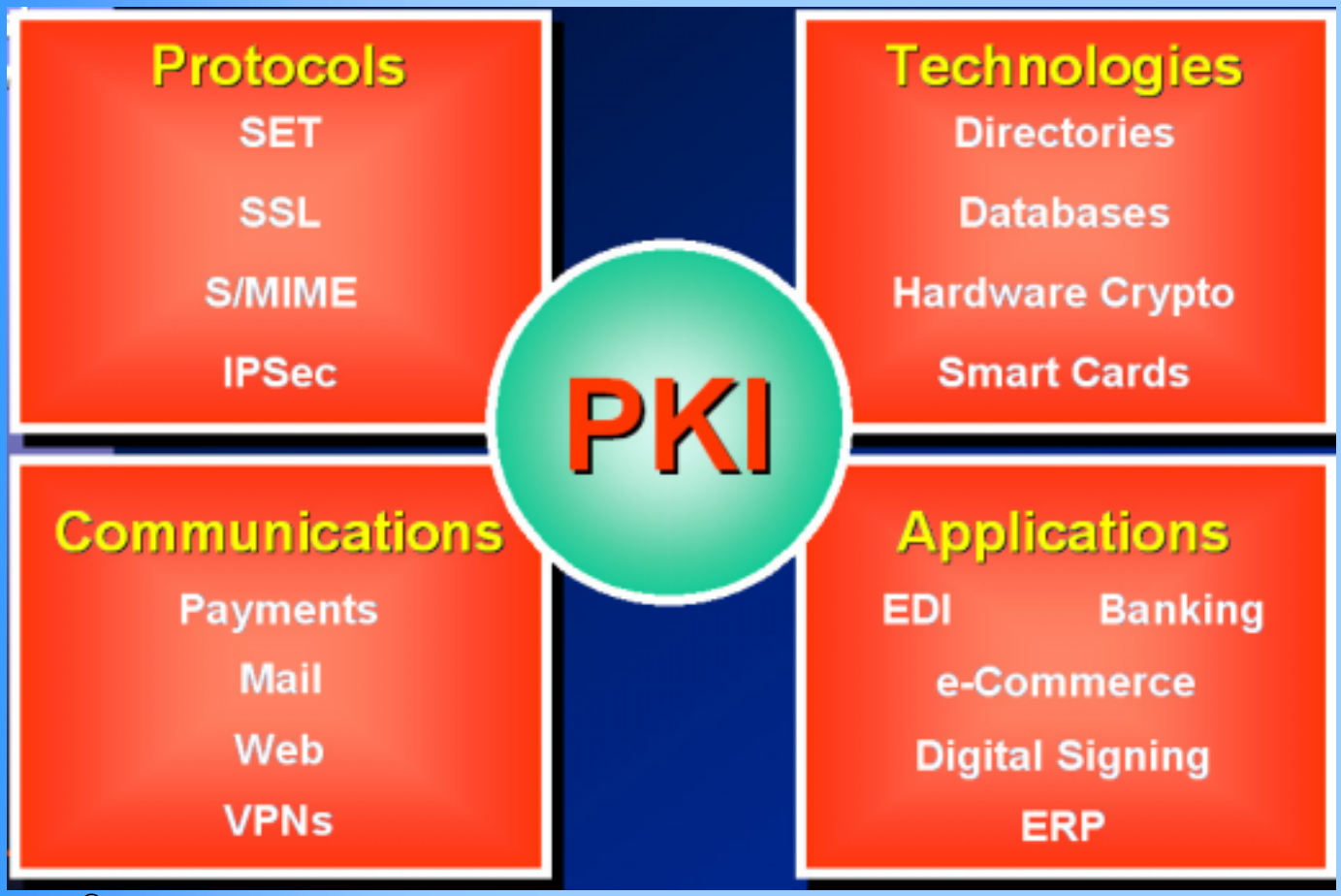


PKI product revenues to 2003

Source: Datamonitor.

But Why PKI?

- It's Not about Waging a Technology War.
- The Issue is about Providing Solutions.



PKI Addresses Many Security and Trust Issues for Building Confidence in E-government:

- 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
- Infrastructure of trust
  - Automating the checking of identities
- Mechanism to prevent Replay
  - Digital signature combined with Time Stamp

But To Assist DCs we must Learn from the Experiences of Industrialized Countries:

1. ***What are the issues facing industrialized countries with PKIs?***
2. ***Can developing countries avoid these pitfalls?***

Some PKI Challenges faced by Industrialized Countries?

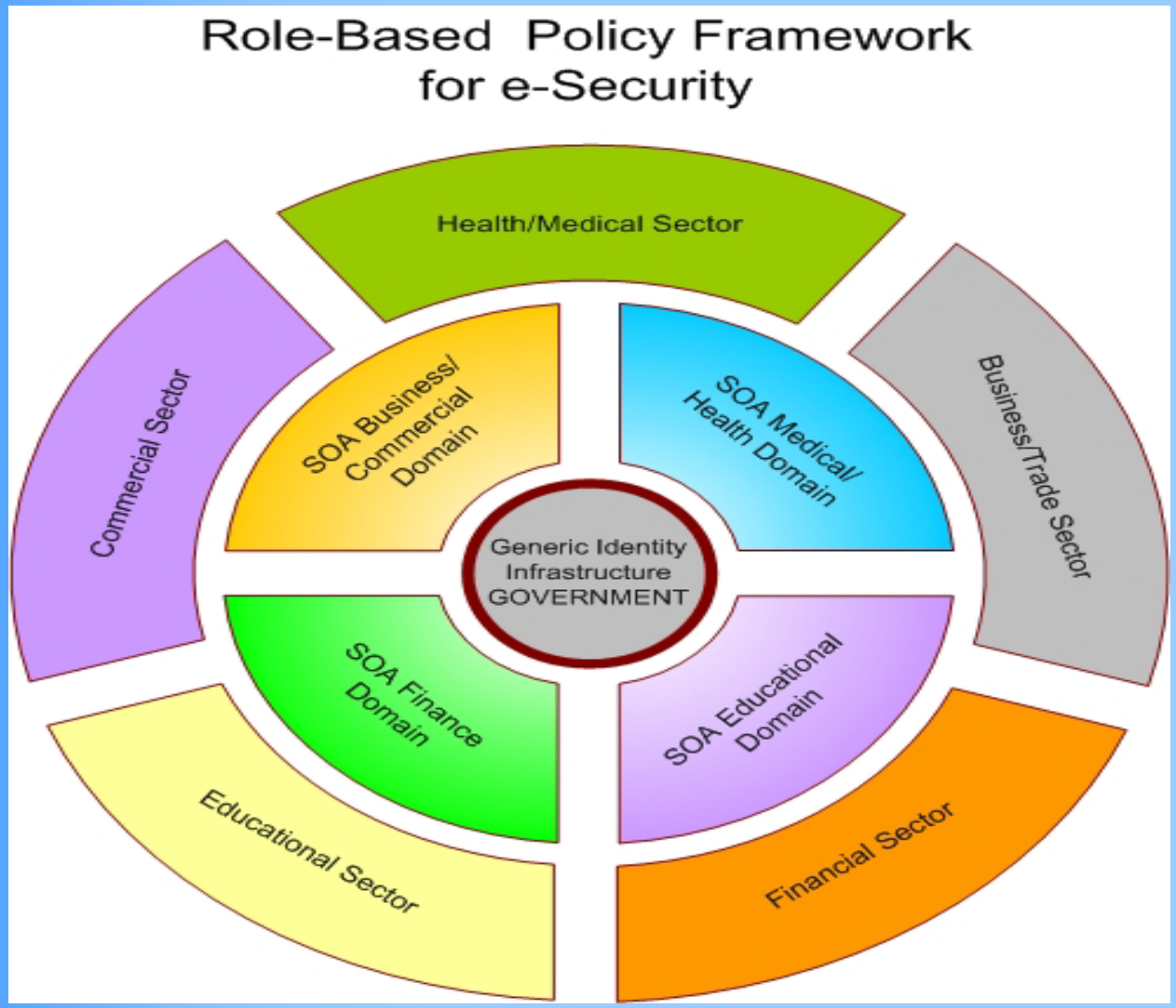
1. Technology-Level *Non* Interoperability Between Different PKI Vendors.
2. Different Approaches to Address CA-CA Interoperability Challenges.
3. Sector-Specific Strategies for Identity Certificates Leading to Non-interoperability of Digital Signatures Across PKI Domains (e.g., for Health, Finance and Business).
4. Recognition of Certificates across Geographical Boundaries. *National Identities or National Passports?*

Some Possible Approaches to Build Confidence in e-government for Developing Countries?

- **Generic Identity Certificates**
  - Public Key Infrastructure (PKI) for Generic Identity Certificates (digital ID cards).
  - Comprehensive Certificate Policies for CA-CA Interoperability.
- **Attribute or Privilege Certificates**
  - Establishment of Privilege Management Infrastructures (PMI) for Sector Specific Needs.
  - Establishment of Frame work for Relationship between AA and CAs
- **Technology Level Interoperability**
  - CA-CA and CA-RA Interoperability

Build Trust Where is Exists!

Generic Identity Framework for All Sectors



…But DCs still face many challenges: …Just to list a few of them…

- Low Level of Awareness on Security/Trust Technologies and their role as a key driver for e-government.
- Human and Financial Resources to Establish PKI.
- Appropriate Business Models for Sustainability and Investments in PKI.
- Standards and/or Profiles to ensure for Multi-Vendor Interoperability.
- Policy-Level Interoperability for PKI Domains and Jurisdictions.
- Dealing with Liabilities, Risks, Insurance, Legal and Policy Framework for PKI Services.

How is ITU-D Assisting DCs in e-government?

- ITU-D Istanbul Action Plan (IsAP)
  - Policies: Assistance in Addressing National/Regional e-applications Policies
  - Projects: Projects on E-government Infrastructure and Applications/Services.
  - Training: Building Human Capacity and Awareness on e-Security and E-government.
  - Environment: Assistance in Legal Issues for E-Applications and Conducive Environment.
  - Guidelines: ITU-D Study Group Questions to Provide guidelines on E-Applications (including e-government).

Conclusion – Is there Any Hope for e-government services in Developing Countries?

- Telecommunications and ICTs can enhance government services by creating efficiencies and reaching the population in remote areas.
- E-government can stimulate the development of ICTs and telecommunication infrastructure in DCs.
- But for this to happen, decision-makers and users must have confidence in the use of this new channel for the delivery of government services.

Thank You

for Your Attention

For further information

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

Email: e-strategy@itu.int