ITU-D Mandate and Strategy and Activities in Cyber Security

Alexander NTOKO
Chief, E-Strategies Unit
ITU Telecommunication Development Bureau
When did it start? Brief History

- ITU-D activities in Cyber Security started at the launch of the ITU Electronic Commerce for Developing Countries in March 1998.

- Priority was to assist developing countries in the implementation of secure and high trust e-commerce platforms.

- Projects delivering cyber security solutions for e-commerce transactions were implemented in Burkina Faso, Brazil, Cambodia, Morocco, Peru, South Africa, Senegal, Turkey, Venezuela and Vietnam.

- Participation of industry security companies in e-commerce security and trust deployment.

- Citation in leading press/media e.g., Time Magazine, International Security Review on ITU initiatives to secure e-commerce transactions.
Then What happened?

- ITU Member States at the 2002 World Telecommunication Development Conference (WTDC) at Istanbul, adopted a new Programme – **E-Strategies and e-services/applications**.

- Extended ITU-D mandate in the domain of e-applications by including other e-applications (e.g., e-government, e-commerce, e-agriculture, e-health etc).

- Included Cyber Security and E-legislation as two of the six (6) priority domains of this new Programme.
E-strategies - What is it all about?

- Using ICTs to reduce the social divide, improve the quality of life and facilitate entry into the information society for developing countries.

- Leveraging the potentials of Internet as a low-cost channel for the delivery of online services in the Health (e-health), Business (e-business), Educational (e-education) and Government Services (e-government).

- But to move from simple online dissemination systems to the conduct of critical transactions in e-health, e-business and e-government requires security and confidence in the networks, applications and services.
What is it all about?

Cyber security not a stand-alone solution but a critical service that is a core component for the implementation of secure e-applications.
Why are we doing it? – Mandate


Two (2) out of the six (6) priority domains of IsAP Programme 3 address Security, confidence and E-legislation. Excerpts from WTDC02 IsAP Istanbul Action Plan Programme 3:

- Enhance security and build confidence in the use of public networks for e-services/applications…
- Provide assistance to Member States in developing laws and model legislation for e-services/applications, prevention of cyber crime, security, ethical issues and data privacy ...
- Identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/applications on various types of networks using relevant technologies ...
- Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of this Programme.
- It is necessary to address the security concerns in order to leverage the potentials of public networks as vehicles for delivering affordable value-added e-services/applications …
What are the synergies with WSIS AP?

WSIS Plan of Action
December 2003

- C5) Building confidence and security in the use of ICTs
  12. Confidence and security are among the main pillars of the information society.
  a) Governments in cooperation with the private sector, should prevent, detect and respond to cyber crime and misuse of ICTs...
  b) Take appropriate action on spam at national and international levels.
  c) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs...
  d) Share good practices in the field of information security and network security and encourage their use by all parties concerned.
  e) Encourage further development of secure and reliable applications to facilitate online transactions.

IsAP Programme 3
WTDC March 2002

- Enhance security and build confidence in the use of public networks for e-services/applications.
- Provide assistance to Member States in developing laws and model legislation for e-services/applications, prevention of cyber crime, security, ethical issues and data privacy.
- Identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/applications on various types of networks using relevant technologies.
- Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of this Programme.
- It is necessary to address the security concerns in order to leverage the potentials of public networks as vehicles for delivering affordable value-added e-services/applications.
What is our strategy?

Identity Management as vital component for cyber security.

E-applications should be built on secure the trusted platforms based on relevant ITU-T standards to increase their benefits to the population.

A holistic approach to cyber security addressing the needs of all sectors.

Appropriate policies and legislation taking into account the balance between enforceable legislation and technology neutrality.
Concretely, what do we do? – Deliverables

- **Implementing Projects**: Coordinating the design, development and implementation of projects on cyber security for e-commerce, e-government and e-health.

- **Formulation of National Policies**: Assisting Member States in addressing technology and policy issues on IT security for e-applications and the Internet including the development of Certificate Policy and Certification Practice Statement for PKI platforms.

- **Development of E-legislation**: Providing guidance in the development of laws and model legislation for the prevention of cyber crime, security and data privacy.

- **Increased Awareness**: Building basic awareness amongst the population on the potentials of secure e-applications for the delivery of services in various sectors.
Solutions implemented in projects:
Confidentiality for Sensitive Data using 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, PKCS#11-based devices), biometrics, FIPS-140-x based Hardware Security Modules.
Hash Algorithm

- Used to determine if document has changed.
- Currently based on FIPS 180-2 approved algorithms (*SHA-1, SHA-256, SHA-384 and SHA-512*).
- Produces 160, 256, 284 or 512 bit “digests”.
- Infeasible to produce a document matching a digest
- A one bit change in the document affects about half the bits in the digest.

**Solutions implemented in projects:**

*Ensuring data integrity through FIPS-180-x Algorithms*
Signer's Private Key

Signed Document

Encrypted Digest

Hash Algorithm

Digest

Solutions implemented in projects:
Digital signatures for authentication and non-repudiation

Combines Hash Algorithms (FIPS-180-x), Key Exchange, Public Key Encryption to provide Data integrity, Non-repudiation and Certificate-based Authentication. Digital credentials are established using ITU-T X.509 V.3 Digital Certificate Standard
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)

Solutions implemented in projects:
Certificate-based authentication using ITU-T X.509 V.3
Solutions implemented in projects:
Automating identity verification and management

- PKI including Certificate Authority, Registration Authorities and related policies and procedures (CPS and CP) for identity verification and management taking into account national policies and national sovereignty issues.

© 1998-2005 ITU Telecommunication Development Bureau (BDT)
Sample operational project – Georgia
Securing communication within government networks

Challenge: Government of Georgia embarks on a project to convert paper documents (including restricted ones) into digital format to facilitate dissemination of government information to citizens. Senior officials plan to electronically sign official correspondences. How can access to these documents be controlled? How is the integrity of these official electronic correspondences ensured?

Solution: Implementation of public key infrastructure providing strong certificate-based authentication including fingerprint biometrics, data integrity using FIPS-approved digest algorithms, e-signature and data confidentiality based on both public key and symmetric encryption. Solutions built on existing infrastructure to ensure seamless integration. Funding and implementation by ITU.
**Sample operational project – Paraguay**

**Securing the transmission of sensitive documents**

**Challenge:** Clients of CONATEL needed secure IT solutions to transmit confidential data (reports) to CONATEL. To address this requirement, the solutions should ensure the integrity of data, preserve the confidential nature of the documents, ensure that both sender and receiver are certain of the identities of each other.

**Solution:** After a careful assessment of the security and trust requirements and discussions with the management and IT professionals of CONATEL, ITU/BDT assisted in the design and development of a public key infrastructure providing solutions for identity management, non-repudiation, data integrity and strong encryption. Technology components including digital signature, biometric authentication, cryptographic token interfaces were built on the existing infrastructure for a seamless integration. Funded and implemented by ITU/BDT this project has increased the efficiency in the business processes of CONATEL and provides security and trust solutions for communicating with its clients (operators and service providers).
Sample operational project – Bulgaria
Building Security and Confidence in Government Services

**Challenge:** Securing communication between government officials and providing security for IP-based interconnection of three (3) government agencies. Main cyber security challenges included providing solutions for authentication, data integrity, data confidentiality and non-repudiation.

**Solution:** Now in its third phase, Phase I provided solutions for certificate-based authentication of government officials, confidentiality in the transmission of sensitive documents and non-repudiation through e-signatures. In Phase II three government agencies were interconnected using PKI-enabled Virtual Private Networks as a cost-efficient way to use the Internet for sensitive e-government services. Project funding and coordinating the design and implementation was provided by ITU/BDT. Phases I and II are operational and Phase III is expected to be operational in Q2 2005.
Sample ongoing Project – Turkey
Building security and trust for the Health Sector

Challenge: 81 provinces, 90,000 doctors, 1200 hospitals and 70+ million inhabitants to be connected through an ICTs health platform as part of national the health transformation project. In addition to several other technological, policy, regulatory and institutional challenges, there are security and trust issues to be addressed. e.g., Transmission of sensitive medical records, authenticating doctors, patients, healthcare professionals and institutions, ensuring patient-doctor confidentiality, integrity, privacy and ownership of EPRs and protecting critical infrastructure and data.

Solution (First Phase): Secure health information system enabling citizens, medical institutions, health insurance and health care professionals participating in Phase I to use information technologies to store, access and disseminate sensitive health data national wide. Funding is provided by Government of Turkey. Launched at WSIS I, ITU is providing expertise for the coordination and implementation.
Other Ongoing projects for 2005: Barbados, Cameroon, Jamaica, Zambia and Rwanda

Enabling secure transaction-based e-government services such as renewing national IDs online, obtaining land certificates, securing the transmission of documents between government officials and agencies, providing online payment for government services and interconnecting government agencies using PKI-enabled Virtual Private Networks. Solutions include e-signatures, data confidentiality and integrity, government run/operated CA, fingerprint biometrics. Implementation by ITU and funding by host governments, EU and ITU.

© 1998-2005 ITU Telecommunication Development Bureau (BDT)
Technology strategy for PKI-based e-business security and trust model for developing countries

- Asymmetrical Trust Model and technology strategy based on Public Key Infrastructure (PKI), Privilege Management Infrastructure and related PMI and PKI-enabled applications.

Original article published in June 2000 edition of World Market Series Business Briefings and referenced in several media in various languages.
Legislative Framework for e-applications
Including data privacy and data protection and

- Assisted ASETA (Bolivia, Colombia, Ecuador, Peru and Venezuela) to develop a harmonized legal framework for the delivery of services based on digital certification, e-signature and e-commerce, data privacy and consumer protection for e-transactions.
Provided assistance to individual states including Burkina Faso, Cape Verde, Mauritania, Mongolia and Tanzania) to elaborate national legislation on e-applications addressing e-signatures, digital certification and data privacy issues.
Sub-regional seminar for Caribbean countries in St. Lucia to discuss sub-regional strategies for e-legislation.

Workshops and seminars addressing technology strategies for cyber security for e-applications in Azerbaijan, Cameroon, Chile, Mongolia, Pakistan, Paraguay, Romania, Seychelles, Syria and Uzbekistan.
Regional Policies and Strategies

- Bringing together Member States to address regional policies and strategies for ICTs (e-applications, Internet and e-Security at the ITU Regional E-government and IP symposium for Arab Region leading to the Dubai Declaration

... Invite ITU to provide more support to Arab countries in accordance to the requirements of each country in the e-government applications and Internet Protocol (electronic certification, information and network security, legal aspect and e-business arbitrage) ... Point 6 – Dubai Declaration of 25 November 2005

© 1998-2005 ITU Telecommunication Development Bureau (BDT)
Increasing Awareness on cyber security technologies through Workshops and Seminars

More than 500 participants from 128 countries including 50 security expert from leading IT security companies met at ITU HQ to launch a technology strategy for building trust and security for e-business transactions. For the first time, delegates from many developing countries could had the opportunity to see an operational public key infrastructure, participate in live demonstrations and better understand some of the technology issues, challenges and solutions in place.

African delegate participating in live demonstration of a public key infrastructure

Delegates at Workshop
Ongoing activities for 2005

1. **PKI Projects:** Barbados, Cameroon, Jamaica, Rwanda, Turkey and Zambia. New request for ITU assistance from Seychelles.

2. **Seminars and Workshops:** Cyber Security Seminar for CEE, CIS and Baltic States, Cyber Security Seminar for Latin America, ITU WSIS Thematic Meeting on Cyber Security in Geneva in collaboration with ITU/SG/SPU and ITU-T.

Scope of Activities for the entire Programme
Including other priority domains