# Towards an Egyptian Framework for CyberSecurity

Dr. Sherif Hashem
Executive VP, ITIDA
Chairman of the CyberSecurity Committee, MCIT
shashem@itida.gov.eg

# Outline

- Egypt Building Digital Bridges
- Some aspects of CyberSecurity Threats
- Key Issues & Challenges
- The Road Ahead

# Egypt: Building Digital Bridges

- MCIT established; launches a National ICT Plan (1999): infrastructure, HRD, access, applications
- ICT Club Initiative (2000)
- Subscription-free Internet initiative (2002)
- PC for every home initiative (2002)
- Smart Village (2003)
- Egypt Information Society initiative (2003)
- Broadband initiative (2004)
- ITIDA established (2004)
- Arabic E-Content initiative (2005)
- Education Initiative (2006)
- ICT Export Strategy (2006)
- CyberSecurity Initiative (2007-9)

# Some Aspects of CyberSecurity Threats

- **40 Million Credit Card Numbers Hacked: Data Breached at Processing Center (CardSystems Solutions Inc),** *Washington Post* – 18 June`05
- **At least 45.7 million credit and debit card numbers** were stolen by hackers who broke into the wireless computer network of the **TJX Companies** of more than nine major retailers including Marshall's, T.J. Maxx, BJ's Wholesale Club, OfficeMax, Barnes and Noble and Sports Authority, over a period of several years, making it the biggest breach of personal data ever reported, according to security specialists, *Boston Globe* – 28 March`07
- Oops!!! TJX breach may be twice as big as admitted, banks say, World's biggest credit card heist now estimated at **94 million** accounts and may cost **100s of millions of USDs**, *Associated Press*, 24 Oct`07
- We've just witnessed the 1st real **"Cyberwar"** against Estonia (2007), DDOS attacks crippled its communication networks, banking systems and ATMs for several days…..

# CyberSecurity Threats (cont.)

On April 21st 2009, the Wall Street Journal reported that the:

"*Computer spies have broken into the Pentagon's $300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever .*

- *…. Similar incidents have also breached the Air Force's air-traffic-control system in recent months.*
- *…..In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft."*

**What's next ?! who's next?!**

# Challenge Question:

***"How can we establish a more secure & safe Information Society?"***

# Challenging Tasks

- ***Better security strategies & policies***
- ***Better legal framework & regulations***
- ***Better systems & processes***
- ***Better technologies & tools***
- ***Better skills***
- ***Better cooperation & networks***
- ***Better awareness***

***…and we need to work together*** ☺

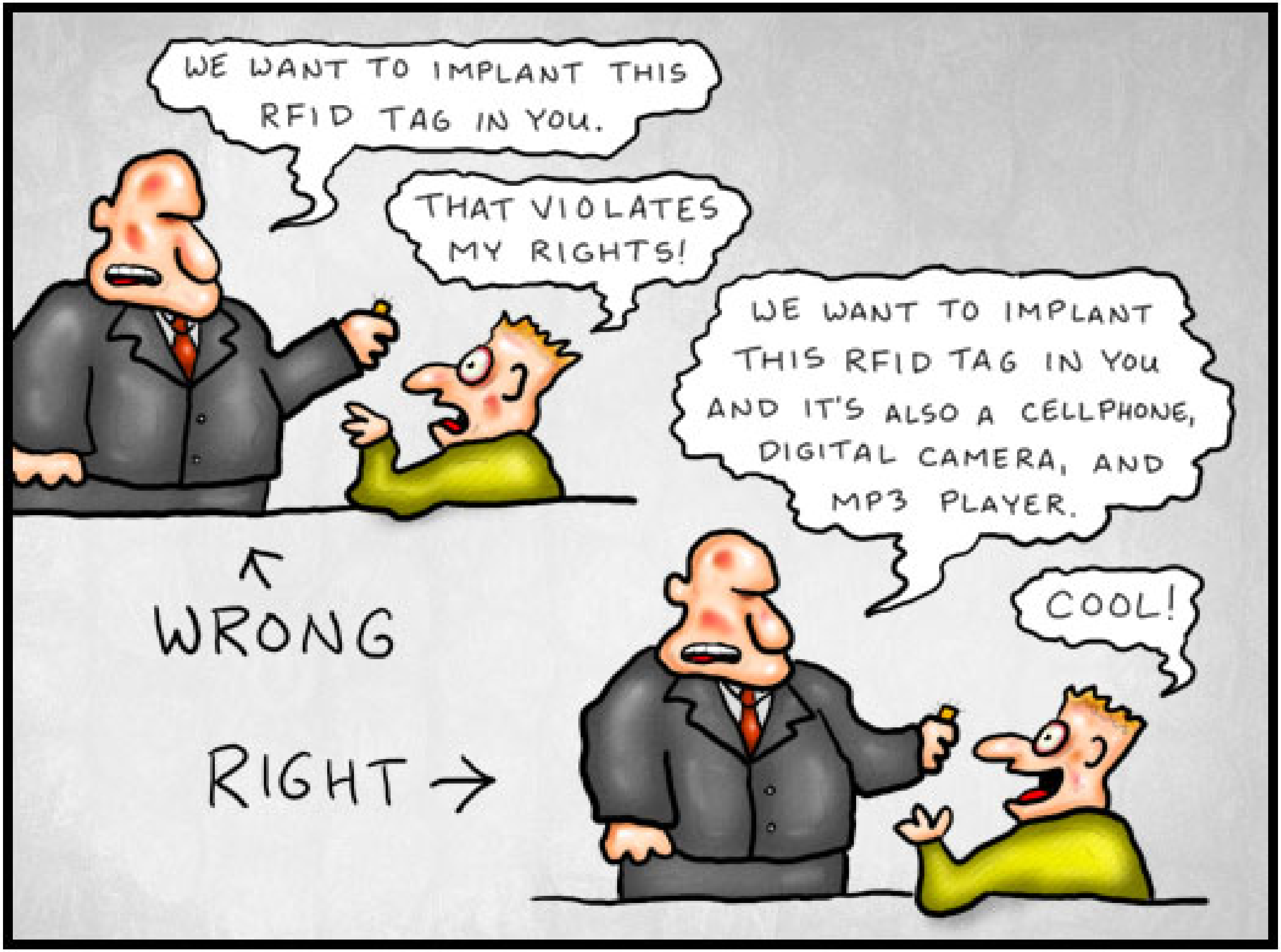
## *Better security strategies & policies:*

# Digital Identity & Privacy

- What's a digital identity?
- How can it be useful to:
  - eGovernment? Citizens? Private service providers?
- What are potential risks?
  - Complexity:
    - Digital ID projects may turn out to be fairly complex, taking longer than expected and costing a lot more than initially anticipated

      "UK Biometric Identity Cards – expected to cost £5.8-19.2B over 10 years" (IEEE Spectrum – Jan 2006)
  - Information theft:

    "Personal electronic information of 26.5 million US military veterans has been stolen ……." (May 2006)
  - Privacy vs. Security


WE WANT TO IMPLANT THIS RFID TAG IN YOU.
THAT VIOLATES MY RIGHTS!
WRONG
WE WANT TO IMPLANT THIS RFID TAG IN YOU AND IT'S ALSO A CELLPHONE, DIGITAL CAMERA, AND MP3 PLAYER.
COOL!
RIGHT

## *Better Legal Framework & Regulations:*

# Cyberlaws & ICT-related Laws & Regulations

- A comprehensive IPR Law (Law No. 82/2002)
- A comprehensive Communications Act (Law No. 10/2003)
- An E-Signature law ( Law No. 15/2004)
- Inclusion of CyberSecurity in the National Security Council and the establishment of CyberSecurity committee at MCIT (2007)

Drafts:

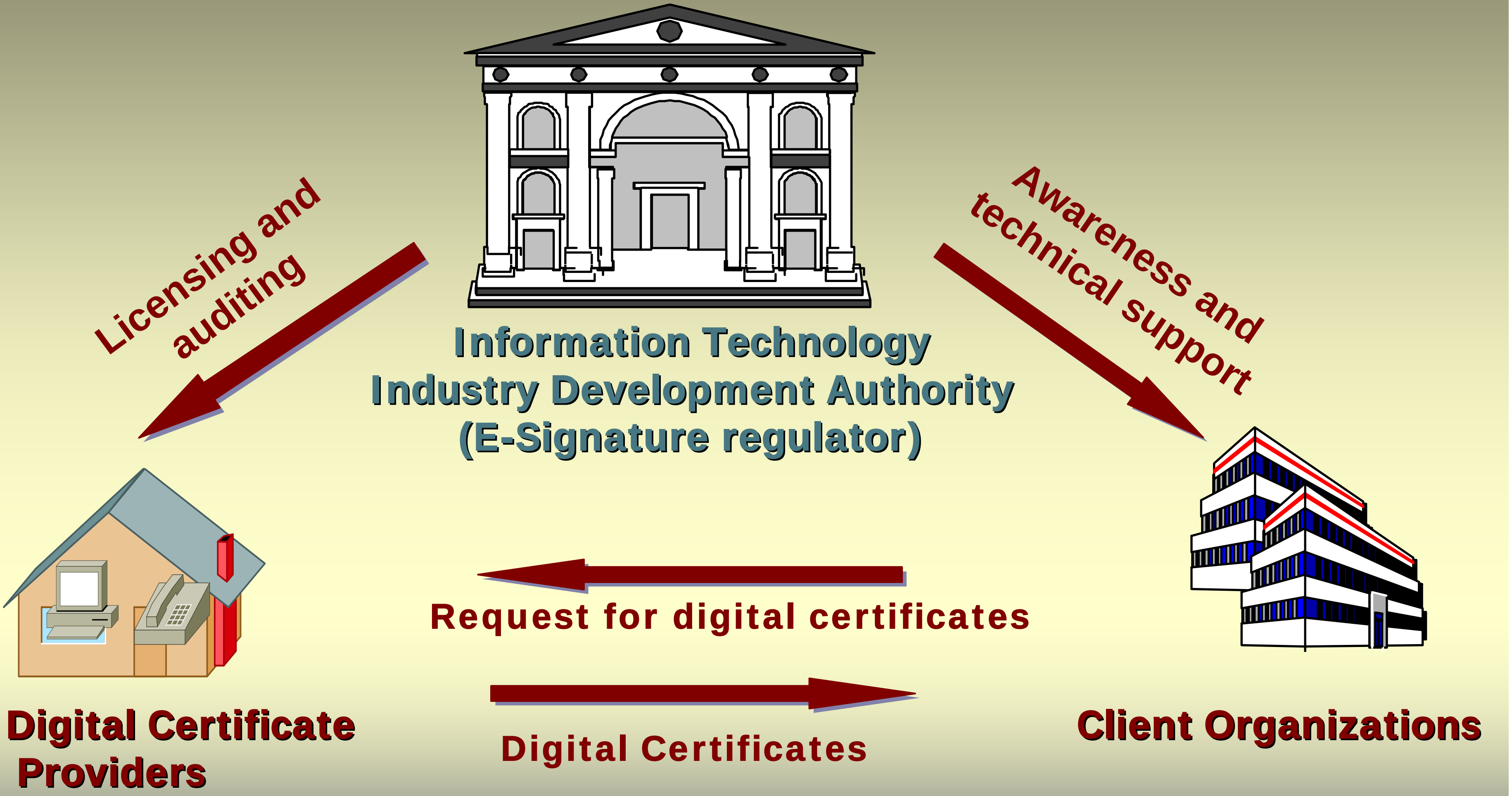
- A Data Protection, Privacy, and Cyber Security law
- A Cyber Crime law
- Access to Information Law

### *Better Legal Framework & Regulations:*

## Highlights of Egypt’s E-Signature Law (2004)

- Recognizes electronic/digital signatures and scripts
- Covers commercial, administrative, civil transactions
- Technology neutral
- Establishes a regulatory body (ITIDA)
- Empowers local CAs, while recognizing “foreign” CSPs
- Executive directives – requires the use of **Smart Cards** for storing digital certificates

# Regulating Digital Certificates



Information Technology
Industry Development Authority
(E-Signature regulator)

Licensing and auditing

Awareness and technical support

Digital Certificate Providers

Request for digital certificates

Digital Certificates

Client Organizations

*Better Technologies & Tools*

# E-Signature & PKI Tools

- Smart Cards
  - Separate plastics cards w/readers (contact & contactless)
  - Cell phone

- Smart Tokens
  - USB tokens
  - w/pens, mouse, …

*Better Technologies & Tools*

# R&D Project: Smart Token for E-Business

- Financed by ITIDA (research grant)
- Encourage consortia from R&D centers, academia and private sector companies
- Technical know how and technology transfer
- Developing an Egyptian e-signature tool
- Grant of 1M LE awarded in Sept 2006
- Scope: smart token for e-signature with and w/o a biometric feature (finger print)

*Better Technologies & Tools :*

# Plans for Egypt’s PKI Cards!

- **Citizens’ Government cards** ***(Multi-purpose dual-interface PKI + Biometric Smart Card):***
  - E-signature digital certificates (Law 15/2004& its executive directives),
  - National ID, Passport information, Driver’s license,
  - Social security information,
  - Tax record,
  - National health insurance, etc.
- ***Financial Services Cards:***
  - Banks (e.g. CIB)
  - Stock market (MCSD)
  - Egypt Post

Arab Republic of Egypt

Ministry of telecommunications and
information technology

# The Egyptian CyberSecurity Committee

***Better systems & processes:***

# Pre-existing Services In Egypt

- At MCIT
  - **Security Audits or Assessments.**

    Periodically prepare penetration testing reports for Affiliated organizations
  - **Network monitoring and analysis**
  - **Incident handling**
  - **Announcement/awareness:**

    Critical errors investigated and communicated to relevant parties

***Better security strategies & policies:***

# Critical Information Infrastructure Protection (CIIP)

- Protection of Critical Telecom Infrastructure:
  - Voice backbones (fixed and mobile)
  - Internet and data backbones
  - International gateways

- Development of security guidelines and standards for operators of national critical telecom infrastructure

- Procedure for crisis handling and service continuity

# Launching: Computer Emergency Response Team (CERT) – Apr09

- Create Core CERT
- Assessment and penetration testing for CII networks
- Incident handling
- Awareness and security alerts portal
- International coordination
- Capacity building and training

# Complementary Functions

- Extend the legal/regulatory framework: cybersecurity/cybercrime/privacy & data protection
- Establish digital forensic lab
- Enhance digital identity management schemes (PKI, etc.)

# Key Issues & Challenges

- **Supportive legal and regulatory environment:**
  - Comprehensive Cyberlaws: e-signature, e-contracting / e-commerce, privacy & data protection, cybersecurity & cybercrime,
  - Establishment of a CERTs, credit bureau, etc.
- **Common technical standards and interoperability specifications for smart cards and their deployment in various applications** (e.g. PKI and e-signature).
- **Standardization, coordination, and cooperation across Government and across sectors:**
  - Telecommunication, banking, transport, healthcare, financial, etc.

# Key Issues & Challenges (Cont.)

- **New infrastructure to be established:**
  - Public Key Infrastructure, Root CA, Gov CA, etc.
  - Cards manufacturing and personalization
  - Issuance and processing centers,
  - Service and distribution centers.

- **Access terminals:**
  - Card readers, POSs, and ATMs,
  - Communication networks, etc.

- **Cost-benefit analysis & business re-engineering:**
  - Front office & back office,
  - 24/7 service availability,
  - 24/7 customer services,
  - Service quality.

# Key Issues & Challenges (Cont.)

- **Deployment models**
  - Who funds, who builds, who operates, and who regulates the infrastructure?
- **Finding the “right” skills and HRD:**
  - Outsourcing vs. In-sourcing?
  - Training & certification (loop :)
- **Awareness (at ALL levels)**
  - Top management, executives, support staff
  - Service providers, end users, general public
- **Privacy vs. Security**
  - Finding the “right” balance.

# The Road Ahead

- Privacy & Data Protection/Cyber Security Law
- Strengthen the e-security framework & culture; empower our Computer Emergency Response Teams CERT(s)
- Protect e-initiatives, e-services & e-projects
- Enhance and develop cybersecurity skills
- Awareness campaigns, workshops & seminars

# Finally

By addressing these issues and challenges,
one can figure out:

How to have
a safer information society?

Thank You…..