

**African Information Society Initiative**  
*Africa's digital agenda*


**ECA Regional Perspective on e-Security**

---

**EAC Workshop on Information Security**  
 Kampala, Uganda 27-28 April 2006

United Nations Economic Commission for Africa

[www.uneca.org/aisi](http://www.uneca.org/aisi)

---

---

---



---

---

---

---

---

**Introduction: AISI and e-Security**

Security is vital for trust and confidence in the Information Society and must be considered at all layers. This includes:

- Information Security Management;
- Standards of Information Security;
- Threats and Attacks to Information;
- Education and Curriculum for Information Security;
- Social and Ethical Aspects of Information Security;
- Information Security Services;
- Applications of Information Security;
- Infrastructure for Information Security;
- Legislation for Information Security;
- Modeling and Analysis for Information Security; and
- Tools for Information Security.

[www.uneca.org/aisi](http://www.uneca.org/aisi)

---

---

---


---

---

---

---

---




**within the AISI framework, the Security concern is addressed :**

- In formulating the National and Regional ICT policies and Strategies
- In designing the legal frameworks for the Information Society

[www.uneca.org/aisi](http://www.uneca.org/aisi)

---

---

---

---

---

---

---

---



## International Framework

**- Resolution adopted by the UN General Assembly**

[on the report of the Second Committee  
(A/58/481/Add.2)]

**58/199. Creation of a global culture of cyber security and the protection of critical information infrastructures**

**- WSIS Plan of Action**

**C5. Building confidence and security in the use of ICTs**

**Confidence and security are among the main pillars of the Information Society**

[www.uneca.org/faisi](http://www.uneca.org/faisi) 

---

---

---

---

---

---

---

---



a) Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.

b) Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

c) Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.

[www.uneca.org/faisi](http://www.uneca.org/faisi) 

---

---

---

---

---

---

---

---



e) Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication.


f) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.

g) Share good practices in the field of information security and network security and encourage their use by all parties concerned.

h) Invite interested countries to set up focal points for real-time incident handling and response, and develop a cooperative network between these focal points for sharing information and technologies on incident response.

i) Encourage further development of secure and reliable applications to facilitate online transactions.

j) Encourage interested countries to contribute activities to build confidence and security in the United Nations activities to build confidence and security

[www.uneca.org/faisi](http://www.uneca.org/faisi) 

---

---

---

---

---

---

---

---

ECA Survey on the implementation of WSIS Plan of Action

| ICT Security Issue   | Addressed in the country ICT policies and plans | Existence of Legislation to enforce this issue |
|--|---|--|
| Information security and network security issues   | 58%   | 8%   |
| Education and raising awareness on security and use of ICTs  | 58%   | 17%  |
| Prevention, detection and response to cyber-crime and misuse of ICTs   | 50%   | 0%   |
| Effective investigation and prosecution of misuse of ICTs  | 33%   | 0%   |
| Government to actively promote user education and awareness about online privacy and the means of protecting privacy | 33%   | 0%   |

www.uneca.org/aisi

---

---

---

---

---

---

---

---

---

---

### Building Trust in Cyberspace

- Data and communications privacy
- e-commerce/e-Government frameworks
- Intellectual property
- Consumer protection
- Cyber security
  - Network reliability
  - Cyber crime

www.uneca.org/aisi

---

---

---

---

---

---

---

---

---

---

### Security - A Shared Responsibility

- Cyber security is shared responsibility of government, service providers, software and hardware makers, and users (large and small).
- Cyber security strategy has many components:
  - industry standards and best practices
  - information sharing
  - awareness, education
  - R&D
  - obligations under civil law
  - criminal law

www.uneca.org/aisi

---

---

---

---

---


---

---

---


---

---



## IT Security Guidelines - Models

- OECD Guidelines for Security of Info. Systems and Networks
- APEC Strategy and Statement on the Security of Info and Communications Infrastructure
- EU
- E-Japan Priority Policy Program (cyber security incorporated)
- Australia E-Security National Agenda
- US National Strategy to Secure Cyberspace & eGovernment Act (cyber security included)

[www.uneca.org/faai](http://www.uneca.org/faai) 

---

---

---

---

---

---

---

---



## e-Security in Africa

### 1) Legal Framework

- Countries with laws on electronic signatures: Mauritius, Tunisia, Cap Verde, South Africa, Egypt.
- Pays with Draft laws on electronic signatures : Algeria, Burkina Faso, Cameroon, Morocco, Senegal,...

---

---

---

---

---

---

---

---



## 2) PKI Development in Africa

South Africa (Private Sector : Thawte, SACA,...),

- Tunisia (ANCE)
- Egypt (ITIDA)
- Mauritius (ICT authority CCA)
- Efforts are underway for the creation on African PKI Forum

[www.uneca.org/faai](http://www.uneca.org/faai) 

---

---

---

---

---

---

---

---



## Common Themes on e-Security

- Public-Private Partnerships
- Public Awareness
- Best Practices, Guidelines, International Standards
- Information Sharing
- Training and Education
- Respect for Privacy
- Vulnerability Assessment, Warning and Response
- Regional and International Cooperation/Cross Border recognition

[www.uneca.org/faasi](http://www.uneca.org/faasi) 

---

---

---


---

---

---

---

---



## eGovernment: a key pillar of eStrategies

*Policy Measures*

eGovernment

eHealth

eLearning


*Benchmarking*

eBusiness

Broadband (wired, wireless), multi-platform (PC, TV, mobile, ...)

Security

*Working Groups*      *Good Practices*

[www.uneca.org/faasi](http://www.uneca.org/faasi) 

---

---

---

---

---

---

---

---



## New Business Model for eGov

The new business model for eGovernment has an array of business processes that extend outward from the organization and encompass the various partners, citizens and other governments.

It is precisely these business processes that extend outward from the organization that require a sound eSecurity strategy at all points of the extended chain.

[www.uneca.org/faasi](http://www.uneca.org/faasi) 

---

---

---

---

---

---

---

---

**eSecurity in the New Business Model**

eSecurity at the Business Process and Inter-transactional level is about:

- authentication and non-repudiation
- encryption
- data integrity
- business practices and transaction integrity
- on-line privacy, and
- confidentiality

[www.uneca.org/faisi](http://www.uneca.org/faisi)

---

---

---

---

---

---

---

---

eSecurity at the Policy and Governance level is about:

- digital and transactional security policies
- security standards and protocols
- prevention, detection and response practices
- risk and vulnerabilities assessment management
- PKI implementation and management

[www.uneca.org/faisi](http://www.uneca.org/faisi)

---

---

---

---

---

---

---

---

**Top Concerns**

- Lack of publicly stated National Information Security Policy.
- Lack of trained & qualified manpower.
- Non existent or weak institutions.
- Lack of Assurance framework (standardization, Accreditation and Certification)
- Lack of awareness & culture of cyber security

[www.uneca.org/faisi](http://www.uneca.org/faisi)

---

---

---


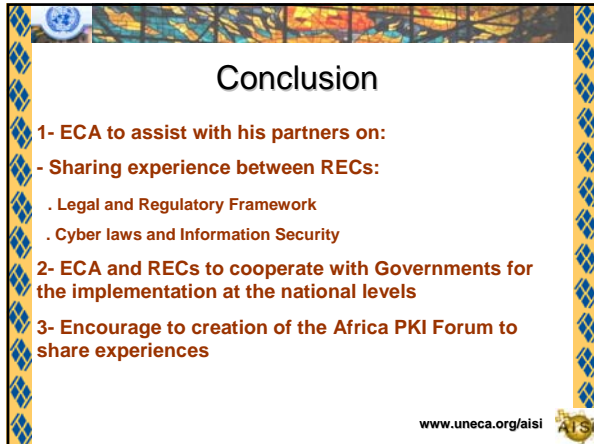
---

---

---

---

---


## Conclusion

**1- ECA to assist with his partners on:**

- **Sharing experience between RECs:**
  - . Legal and Regulatory Framework
  - . Cyber laws and Information Security

**2- ECA and RECs to cooperate with Governments for the implementation at the national levels**

**3- Encourage to creation of the Africa PKI Forum to share experiences**

[www.uneca.org/aisi](http://www.uneca.org/aisi) 

---

---

---

---

---

---

---

---

## Thank you

*for additional information*

<http://www.uneca.org/aisi>

Development Information Services Division  
Tel: + 251 1 51 14 08 - Fax: + 251 1 51 05 12



 **United Nations**  
**Economic Commission for Africa**  
*Accelerating a Continent's Development*

[www.uneca.org/aisi](http://www.uneca.org/aisi) 

---

---

---

---

---

---

---

---