International Telecommunication Union

Security Standardization in ITU-T

Herbert Bertine

Chairman ITU-T Study Group 17

hbertine@lucent.com

Cybersecurity Symposium II *29 March 2005* *Moscow, Russia*

ITU Plenipotentiary Conference 2002

Resolution PLEN/2 - Strengthening the role of ITU in information and communication network security

resolves

1 to review ITU's current activities in information and communication network security;

2 to intensify work within existing ITU study groups in order to:

a) reach a common understanding on the importance of information and communication network security by studying standards on technologies, products and services with a view to developing recommendations, as appropriate;

b) seek ways to enhance exchange of technical information in the field of information and communication network security, and promote cooperation among appropriate entities;

c) report on the result of these studies annually to the ITU Council.

ITU-T World Telecommunications Standardization Assembly (WTSA)

- **Resolution 50, Cyberscecurity**

  - Evaluate existing and evolving new Recommendations with respect to their robustness of design and potential for exploitation by malicious parties

  - Raise awareness of the need to defend against the threat of cyber attack

- **Resolution 51, Combating spam**

  - Report on international initiatives for countering spam

  - Member States to take steps within their national legal frameworks to ensure measures are taken to combat spam

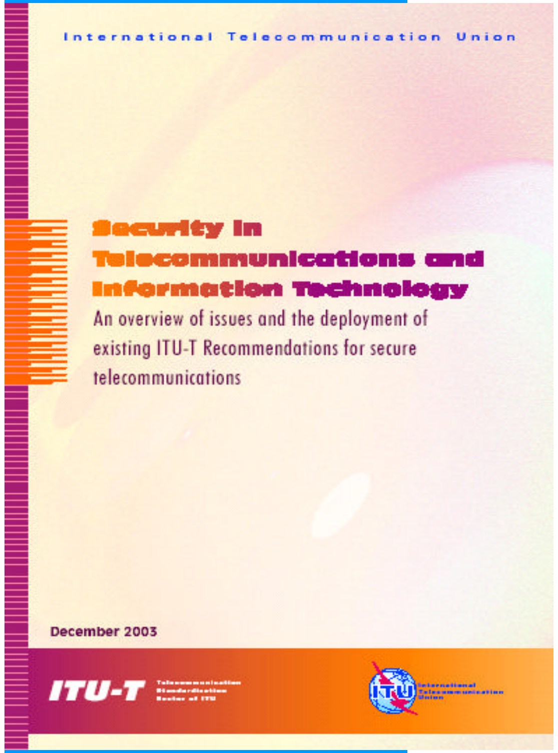
- **Resolution 52, Countering spam by technical means**

  - Study Groups, in cooperation with other relevant groups, to develop as a matter of urgency technical Recommendations on countering spam

ITU-T Study Groups

www.itu.int/ITU-T

- **SG 2** Operational aspects of service provision, networks and performance
- **SG 3** Tariff and accounting principles including related telecommunications economic and policy issues
- **SG 4** Telecommunication management
- **SG 5** Protection against electromagnetic environment effects
- **SG 6** Outside plant and related indoor installations
- **SG 9** Integrated broadband cable networks and television and sound transmission
- **SG 11** Signalling requirements and protocols
- **SG 12** Performance and quality of service
- **SG 13** Next generation networks
- **SG 15** Optical and other transport network infrastructures
- **SG 16** Multimedia terminals, systems and applications
- **SG 17** Security, languages and telecommunication software
- **SG 19** Mobile telecommunication networks
- **TSAG** Telecommunication Standardization Advisory Group



International Telecommunication Union

Security in Telecommunications and Information Technology

An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications

December 2003

ITU-T Telecommunication Standardization Sector of ITU

ITU International Telecommunication Union

ITU-T Security Manual

December 2003, October 2004

- Basic security architecture and dimensions
- Vulnerabilities, threats and risks
- Security framework requirements
- PKI and privilege management with X.509
- Applications (VoIP, IPCablecom, Fax, Network Management, e-prescriptions)
- Security terminology
- Catalog of ITU-T security-related Recommendations
- List of Study Groups and security-related Questions

www.itu.int/itudoc/itu-t/85097.pdf
www.itu.int/itudoc/itu-t/86435.pdf

ITU-T security building blocks

Security Architecture Framework

X.800 – Security architecture
X.802 – Lower layers security model
X.803 – Upper layers security model
X.810 – Security frameworks for open systems: Overview
X.811 – Security frameworks for open systems: Authentication framework
X.812 – Security frameworks for open systems: Access control framework
X.813 – Security frameworks for open systems: Non-repudiation framework
X.814 – Security frameworks for open systems: Confidentiality framework
X.815 – Security frameworks for open systems: Integrity framework
X.816 – Security frameworks for open systems: Security audit and alarms framework

Telecommunication Security

X.805 – Security architecture for systems providing end-to-end communications
X.1051 – Information security management system – Requirements for telecommunications (ISMS-T)
X.1081 – A framework for specification of security and safety aspects of telebiometrics
X.1121 – Framework of security technologies for mobile end-to-end communications
X.1122 – Guideline for implementing secure mobile systems based on PKI

Protocols

X.273 – Network layer security protocol
X.274 – Transport layer security protocol

Security in Frame Relay

X.272 – Data compression and privacy over frame relay networks

Security Techniques

X.841 – Security information objects for access control
X.842 – Guidelines for the use and management of trusted third party services
X.843 – Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

X.500 – Overview of concepts, models and services
X.501 – Models
X.509 – Public-key and attribute certificate frameworks
X.519 – Protocol specifications

Network Management Security

M.3010 – Principles for a telecommunications management network
M.3016 – TMN Security Overview
M.3210.1 – TMN management services for IMT-2000 security management
M.3320 – Management requirements framework for the TMN X-Interface
M.3400 – TMN management functions

Systems Management

X.733 – Alarm reporting function
X.735 – Log control function
X.736 – Security alarm reporting function
X.740 – Security audit trail function
X.741 – Objects and attributes for access control

Televisions and Cable Systems

J.91 – Technical methods for ensuring privacy in long-distance international television transmission
J.93 – Requirements for conditional access in the secondary distribution of digital television on cable television systems
J.170 – IPCablecom security specification

Multimedia Communications

H.233 – Confidentiality system for audiovisual services
H.234 – Encryption key management and authentication system for audiovisual services
H.235 – Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals
H.323 Annex J – Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
H.350.2 – Directory services architecture for H.235
H.530 – Symmetric security procedures for H.323 mobility in H.510

Facsimile

T.30 Annex G – Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
T.30 Annex H – Security in facsimile Group 3 based on the RSA algorithm
T.36 – Security capabilities for use with Group 3 facsimile terminals
T.503 – Document application profile for the interchange of Group 4 facsimile documents
T.563 – Terminal characteristics for Group 4 facsimile apparatus

Message Handling Systems (MHS)

X.400/ F.400 – Message handling system and service overview
X.402 – Overall architecture
X.411 – Message transfer system: Abstract service definition and procedures
X.413 – Message store: Abstract service definition
X.419 – Protocol specifications
X.420 – Interpersonal messaging system
X.435 – Electronic data interchange messaging system
X.440 – Voice messaging system

ITU-T Recommendations are available from the ITU website http://www.itu.int/publications/bookshop/how-to-buy.html (this site includes information on limited free access to ITU-T Recommendations)

Current important security work in ITU-T includes

Telebiometrics, Security management, Mobility security, Emergency telecommunications

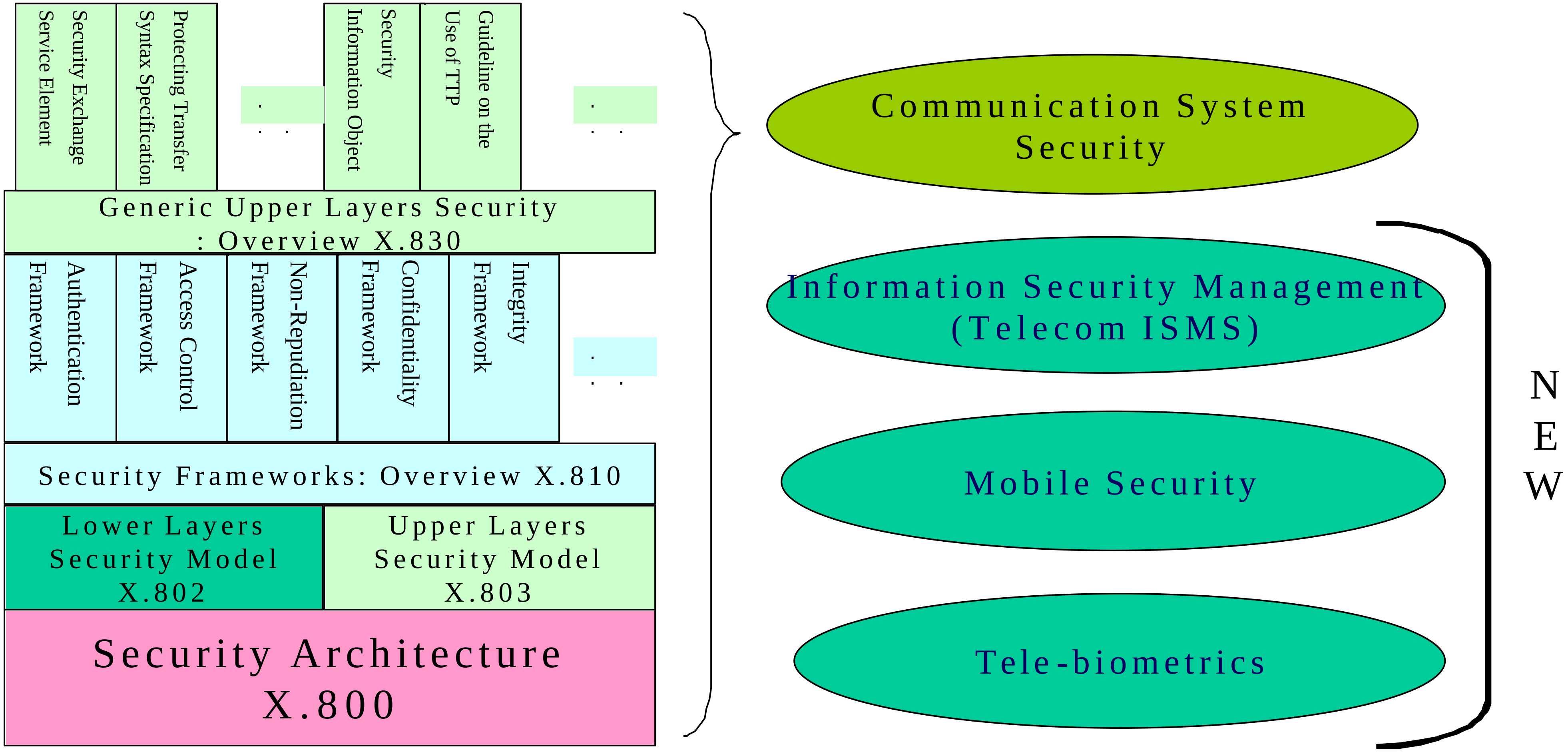
For further information on ITU-T and its Study Groups: http://www.itu.int/ITU-T

ITU-T Study Group 17

www.itu.int/ITU-T/studygroups/com17

- Lead Study Group for Telecommunication Security
  www.itu.int/ITU-T/studygroups/com17/tel-security.html
  - Coordination/prioritization of security efforts
  - Development of core security Recommendations
- Led ITU-T Workshop on Security 13-14 May 2002
  www.itu.int/ITU-T/worksem/security
  - Security requirements and telecommunication reliability
  - Hot topics on IP-based network security
  - Security management
  - Biometric authentication
- Another ITU-T Workshop on Security being planned
- Initiated the ITU-T Security Project
  - Provide vision and direction for future work
  - Reflect situation of current work

Study Group 17 Security Focus 2001-2004



Security Exchange Service Element

Protecting Transfer Syntax Specification

. . .

Security Information Object

Guideline on the Use of TTP

. . .

Generic Upper Layers Security : Overview X.830

Authentication Framework

Access Control Framework

Non-Repudiation Framework

Confidentiality Framework

Integrity Framework

. . .

Security Frameworks: Overview X.810

Lower Layers Security Model X.802

Upper Layers Security Model X.803

Security Architecture X.800

Communication System Security

Information Security Management (Telecom ISMS)

Mobile Security

Tele-biometrics

NEW

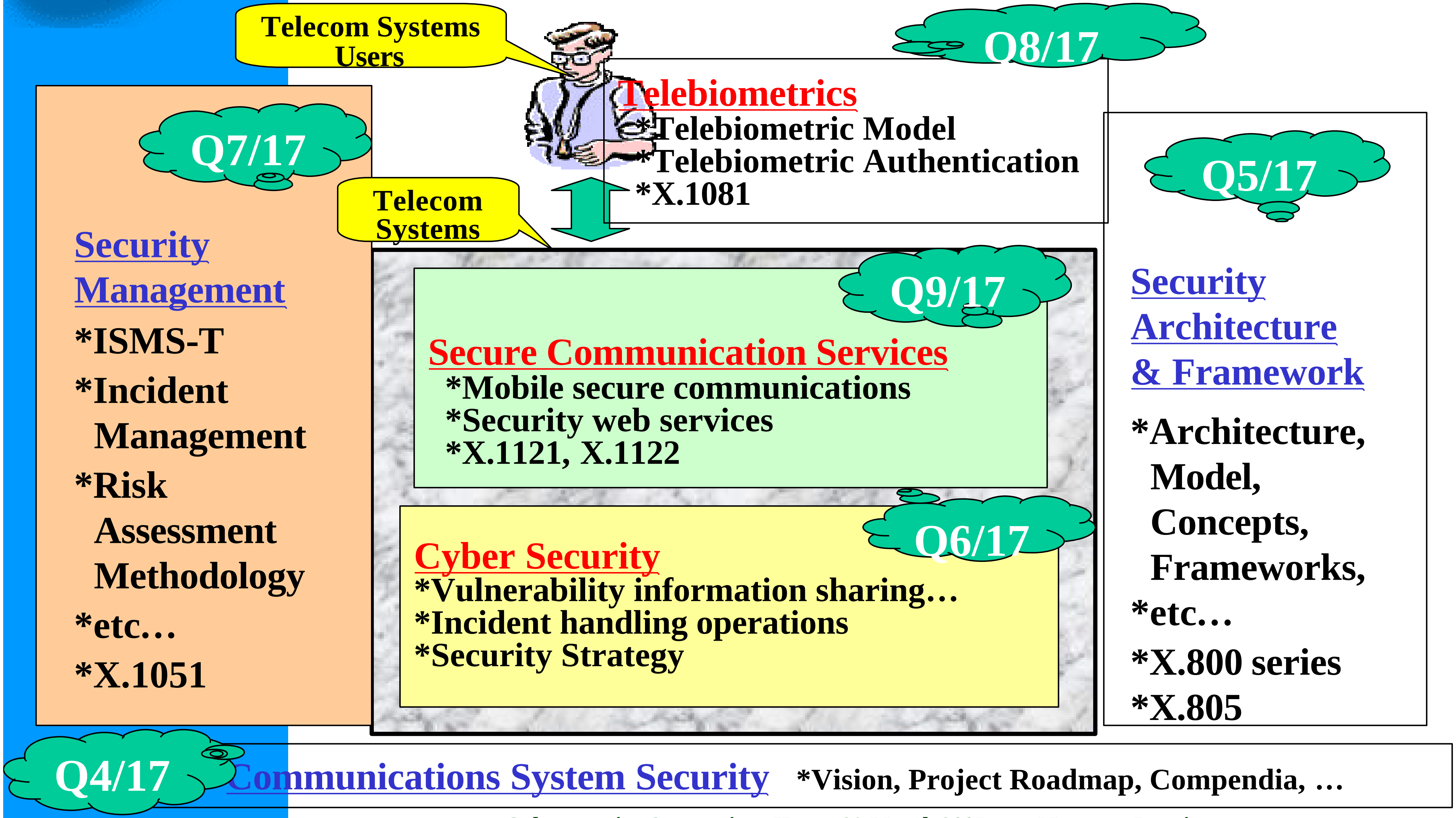
Existing Recommendations in X.800-series

Current work items

ITU-T SG 17 Security Focus 2001-2004

- **Public Key and Attribute Certificate Frameworks** (X.509) Revision 2005
  - Ongoing enhancements as a result of more complex uses
- **Security Architecture** (X.805) New 2003
  - For end-to-end communications
- **Security Management System** (X.1051) New 2004
  - For risk assessment, identification of assets and implementation characteristics
- **Mobile Security** (X.1121 and X.1122) New 2004
  - For mobile end-to-end data communications
- **Telebiometric Multimodal Model** (X.1081) New 2004
  - A framework for the specification of security and safety aspects of telebiometrics

Study Group 17 Security Questions 2005-2008



Telecom Systems Users

Q8/17

Telebiometrics

*Telebiometric Model

*Telebiometric Authentication

*X.1081

Q7/17

Security Management

*ISMS-T

*Incident Management

*Risk Assessment Methodology

*etc…

*X.1051

Telecom Systems

Q9/17

Secure Communication Services

*Mobile secure communications

*Security web services

*X.1121, X.1122

Q6/17

Cyber Security

*Vulnerability information sharing…

*Incident handling operations

*Security Strategy

Q5/17

Security Architecture & Framework

*Architecture, Model, Concepts, Frameworks,

*etc…

*X.800 series

*X.805

Q4/17

Communications System Security *Vision, Project Roadmap, Compendia, …

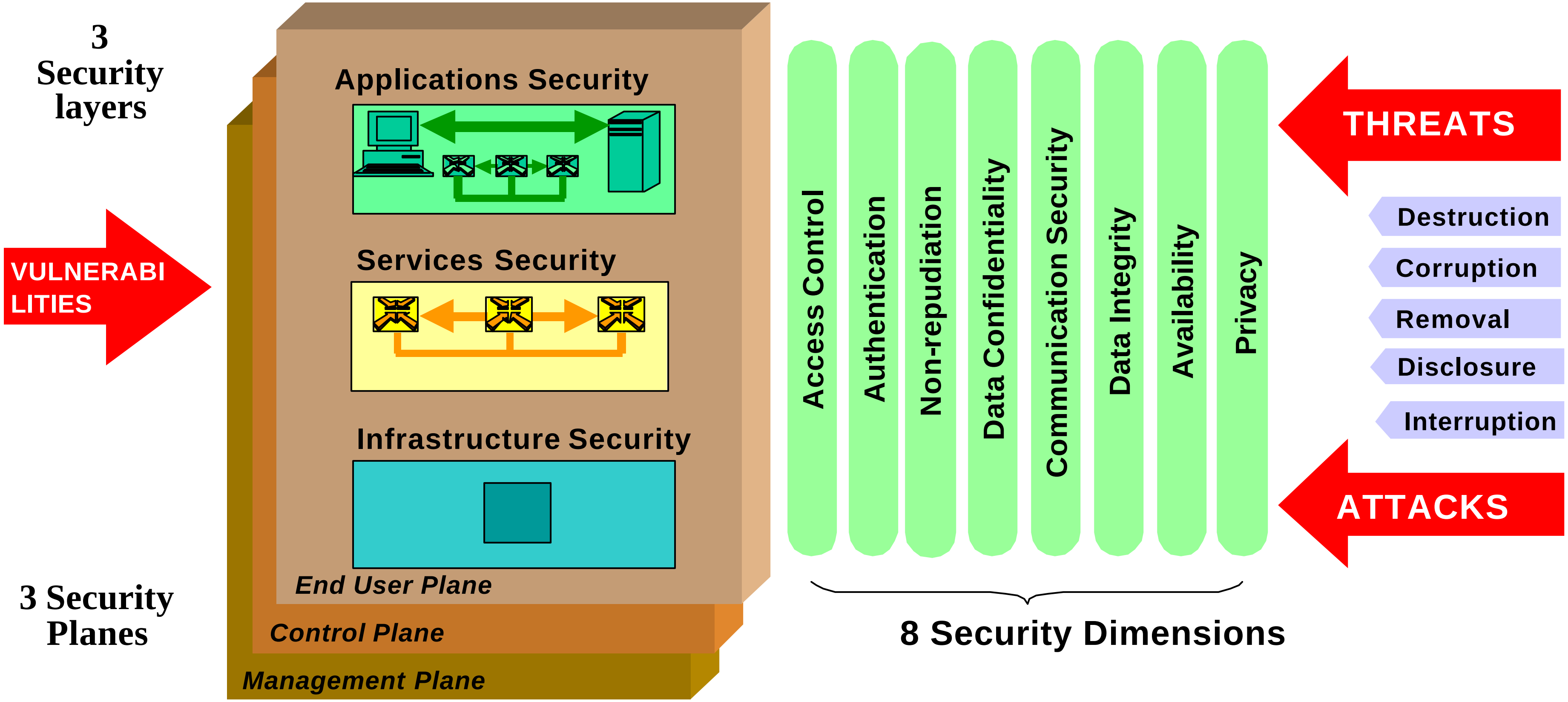
Concluding Observations

- Security is everybody's business
- Security needs to be designed in upfront
- Security must be an ongoing effort
- Systematically addressing vulnerabilities (intrinsic properties of networks/systems) is key so that protection can be provided independent of what the threats (which are constantly changing and may be unknown) may be – X.805 is helpful here

Thank You!

Additional Details on Recently Approved Study Group 17 Security Recommendations

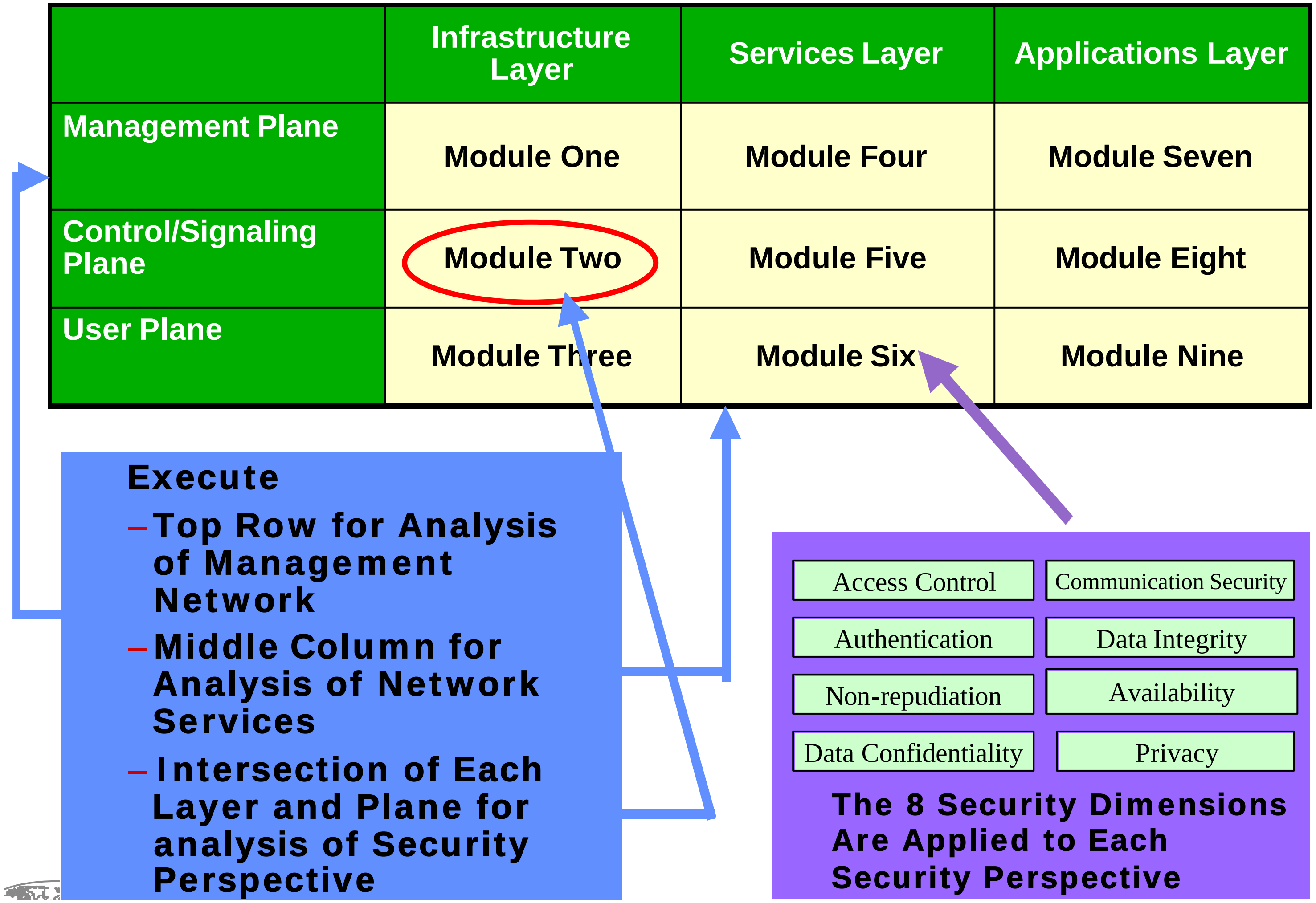
X.805: Security Architecture for End-to-End Communications



- Vulnerabilities can exist in each Layer, Plane and Dimension
- 72 Security Perspectives (3 Layers ✖ 3 Planes ✖ 8 Dimensions)

X.805

ITU-T X.805 Approach



	Infrastructure Layer	Services Layer	Applications Layer
Management Plane	Module One	Module Four	Module Seven
Control/Signaling Plane	Module Two	Module Five	Module Eight
User Plane	Module Three	Module Six	Module Nine

Execute

- Top Row for Analysis of Management Network
- Middle Column for Analysis of Network Services
- Intersection of Each Layer and Plane for analysis of Security Perspective

Access Control	Communication Security
Authentication	Data Integrity
Non-repudiation	Availability
Data Confidentiality	Privacy

The 8 Security Dimensions Are Applied to Each Security Perspective

ITU-T X.805

Provides A Holistic Approach:

- Comprehensive, End-to-End Network View of Security
- Applies to Any Network Technology
  - Wireless, Wireline, Optical Networks
  - Voice, Data, Video, Converged Networks
- Applies to Any Scope of Network Function
  - Service Provider Networks
  - Enterprise Networks
  - Government Networks
  - Management/Operations, Administrative Networks
  - Data Center Networks
- Can Map to Existing Standards
- Completes the Missing Piece of the Security Puzzle of what to do next

Security Management

- Information security management system – Requirements for telecommunications (ISMS-T)

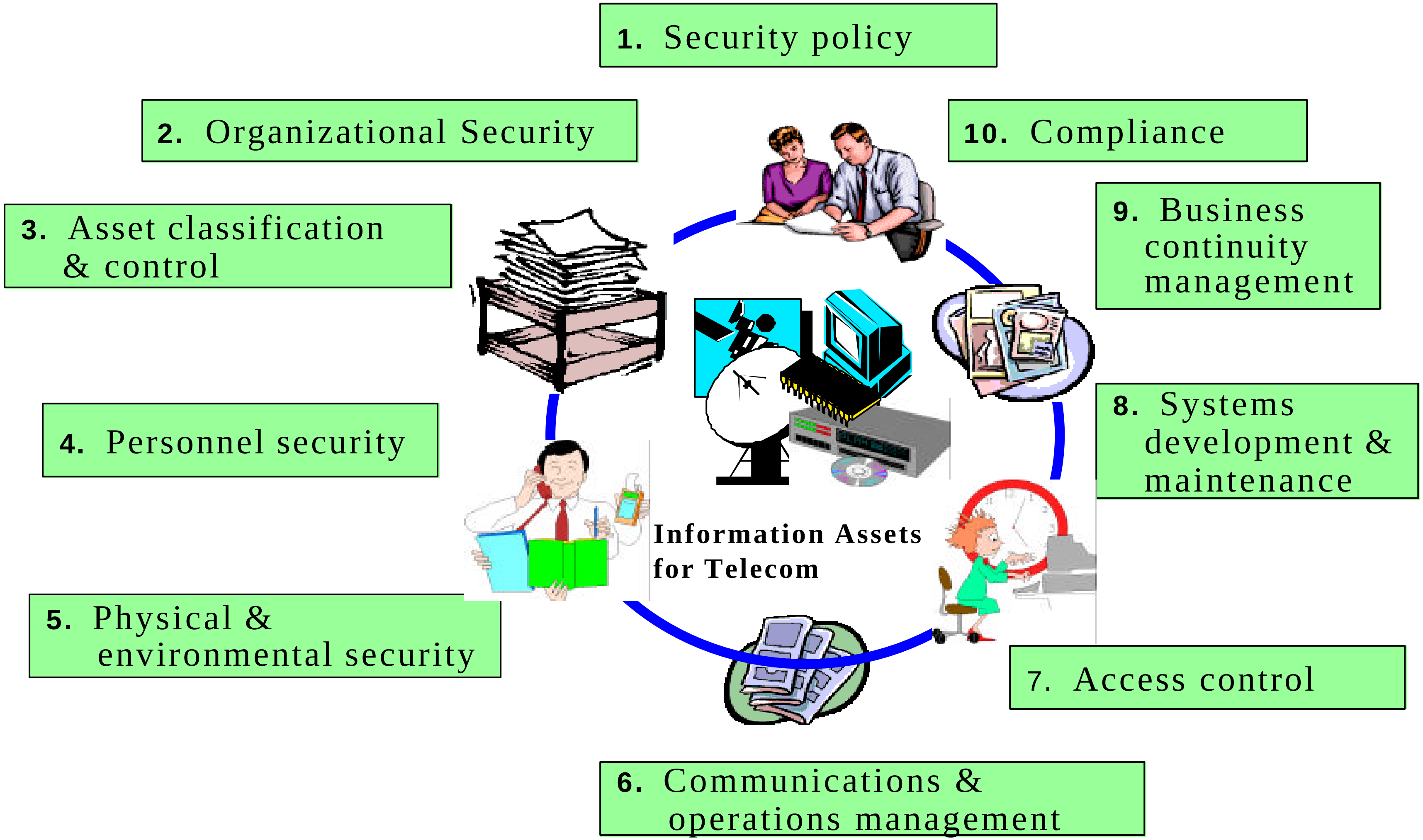
  - specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the telecommunication's overall business risks.

  - leverages ISO/IEC 17799:2000, Information technology, Code of practice for information security management

  - based on BS 7799-2:2002, Information Security Management Systems — Specifications with Guidance for use

X.1051

Information Security Management Domains defined in ISO/IEC 17799



1. Security policy
2. Organizational Security
3. Asset classification & control
4. Personnel security
5. Physical & environmental security
6. Communications & operations management
7. Access control
8. Systems development & maintenance
9. Business continuity management
10. Compliance
Information Assets for Telecom

ISMS

Information Security Management System

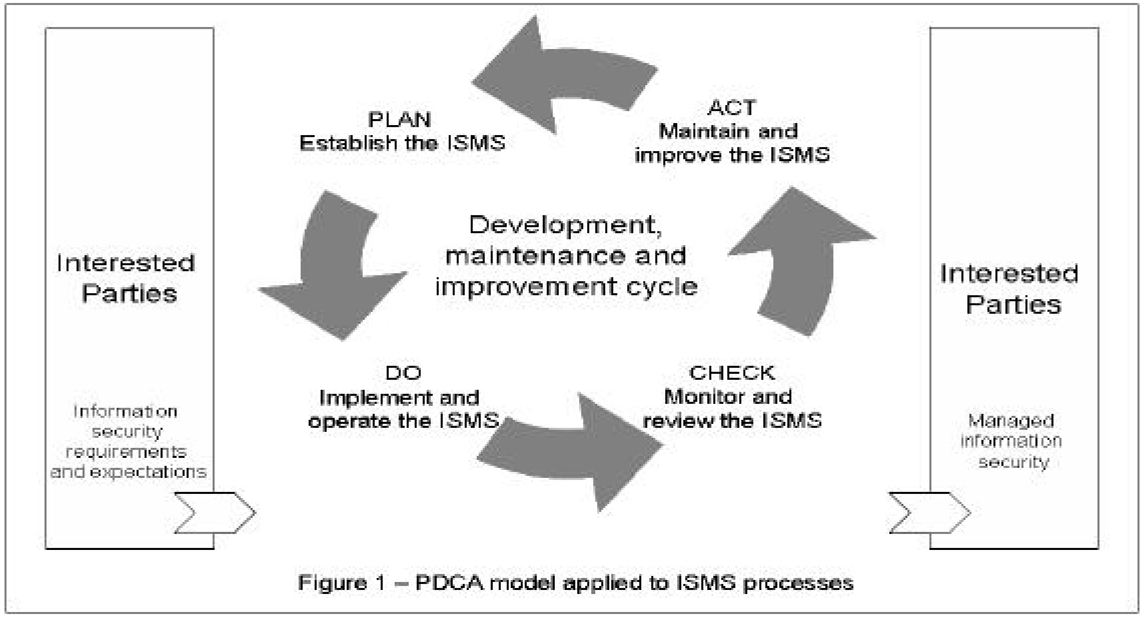

Interested Parties
Information security requirements and expectations
PLAN
Establish the ISMS
ACT
Maintain and improve the ISMS
Development, maintenance and improvement cycle
DO
Implement and operate the ISMS
CHECK
Monitor and review the ISMS
Interested Parties
Managed information security

Figure 1 – PDCA model applied to ISMS processes

- Organizational security
- Asset management
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance

X.1051

Mobile Security

Multi-part standard

X.1121

- Framework of security technologies for mobile end-to-end data communications

  - describes security threats, security requirements, and security functions for mobile end-to-end data communication

  - from the perspectives of the mobile user and application service provider (ASP)

X.1122

- Guideline for implementing secure mobile systems based on PKI

  - describes considerations of implementing secure mobile systems based on PKI, as a particular security technology

- Security Policy (under development)

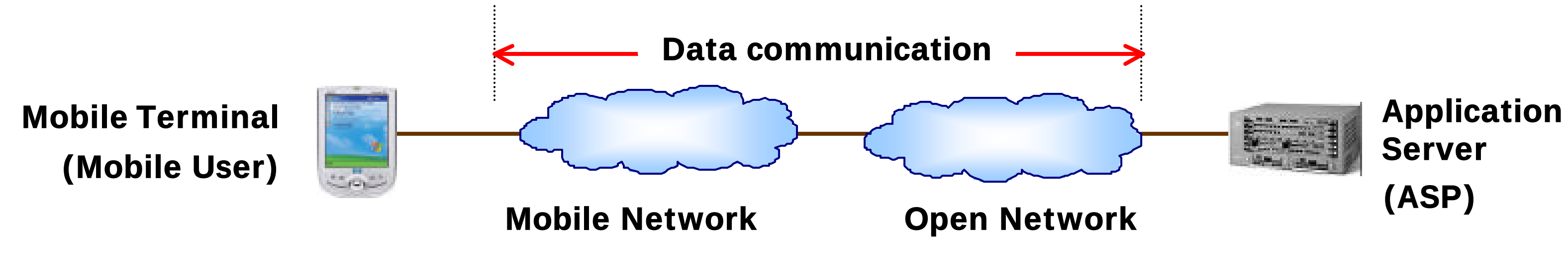
  - different quality of security service needs to satisfy various requirements of security services of both user and ASP

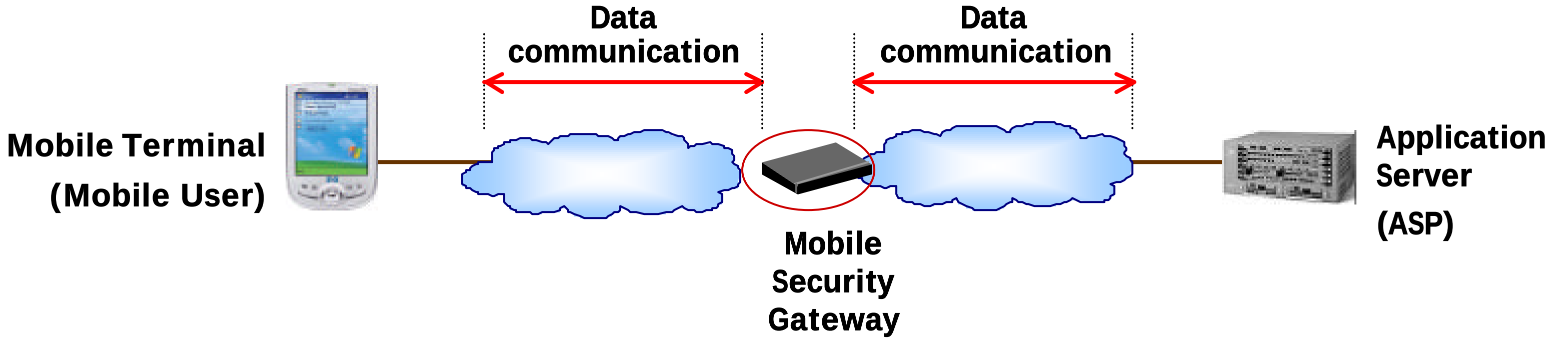
General Communication Framework

Gateway Framework

X.1121

Security framework for mobile end-to-end data communications

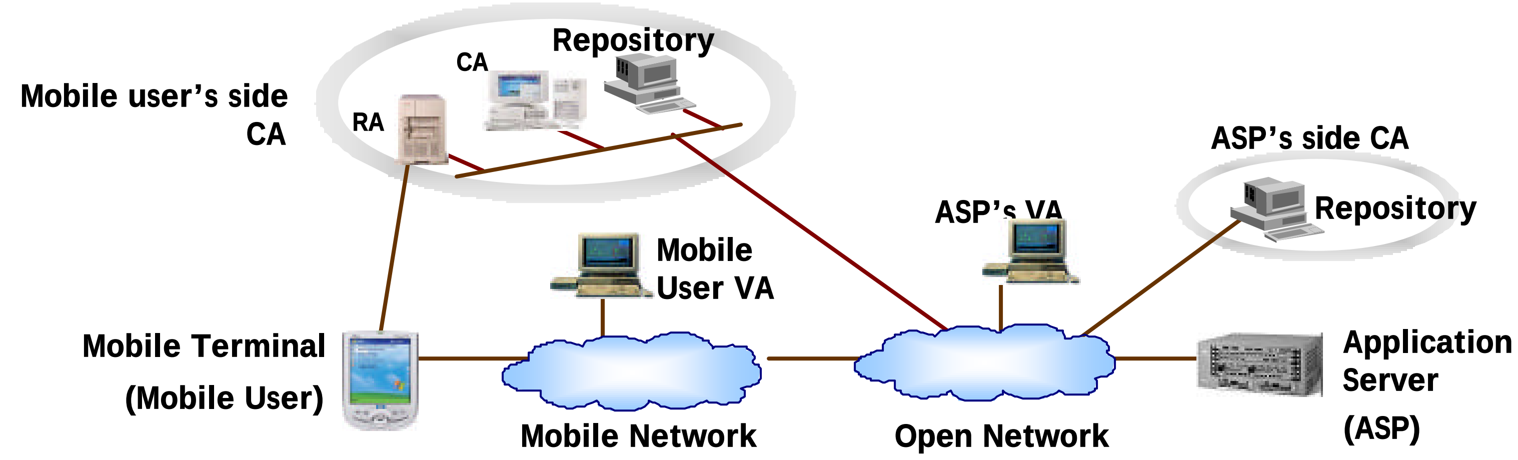




- Security threats
- Relationship of security threats and models
- Security requirements
- Relationship of security requirements and threats
- Security functions for satisfying requirements

Secure mobile systems based on PKI

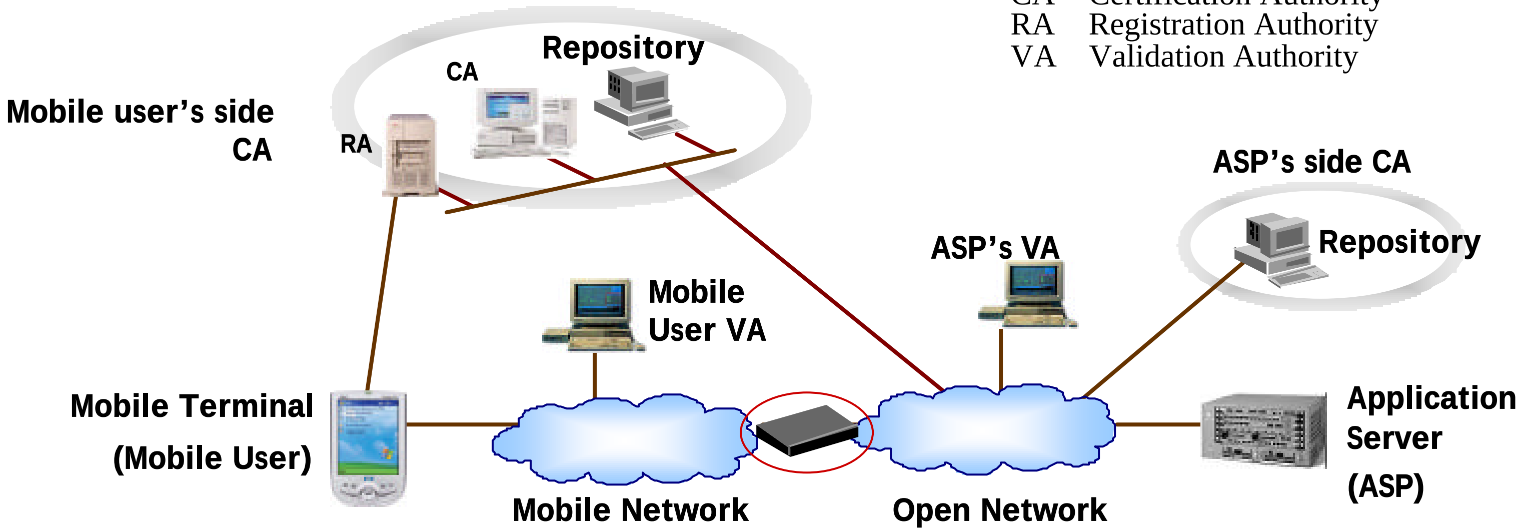
General Model



ASP	Application Service Provider
CA	Certification Authority
RA	Registration Authority
VA	Validation Authority

Gateway Model

X.1122



Telebiometrics

- A model for security and public safety in telebiometrics that can -
  - assist with the derivation of safe limits for the operation of telecommunications systems and biometric devices
  - provide a framework for developing a taxonomy of biometric devices; and
  - facilitate the development of authentication mechanisms, based on both static (for example finger-prints) and dynamic (for example gait, or signature pressure variation) attributes of a human being.
- A taxonomy is provided of the interactions that can occur where the human body meets devices capturing biometric parameters or impacting on the body.

X.1081

Telebiometric Multimodal Model: A Three Layer Model

- the scientific layer
  - 5 disciplines: physics, chemistry, biology, culturology, psychology
- the sensory layer – 3 overlapping classifications of interactions
  - video (sight), audio (sound), chemo (smell, taste), tango (touch); radio (radiation) - each with an *out* (emitted) and *in* (received) state
  - behavioral, perceptual, conceptual
  - postural, gestural, facial, verbal, demeanoral, not-a-sign
- the metric layer
  - 7 SI base units (m, kg, s, A, K, mol, cd)

X.1081