Cyber Security Standardization

Walter Fumy

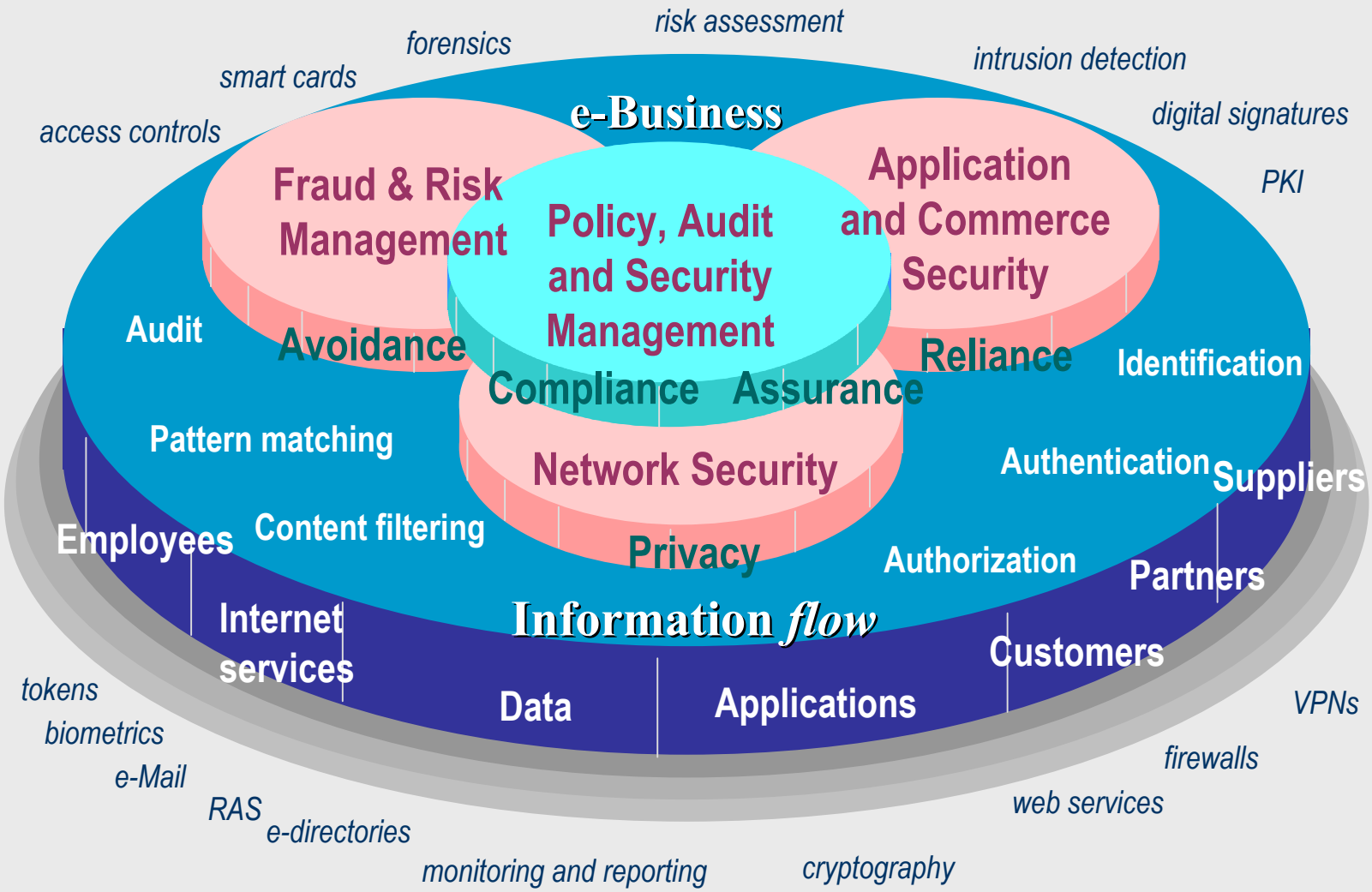
VP Security Technology, Siemens AG

Chairman ISO/IEC JTC 1/SC 27 "IT Security Techniques"

Common Sense

- "On the Internet, nobody knows you're a dog."
- "eBusiness (eGovernment, ...) will not evolve without appropriate security solutions."
- "Secure systems are 10% about security technology and 90% about organization."
- "Standards connect the world."

Security Technologies

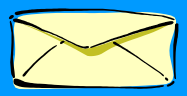


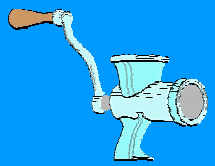
Source: Aberdeen*Group*

Agenda

- ✓ Introduction
- Cyber Security Standardization
  - Cryptographic Mechanisms
  - Security Architectures & Protocols
  - Security Management, Awareness & Education
- Cyber Security Standardization Initiatives
- Conclusion

ITU-T





Cyber Security Standardization

- **Cryptographic Mechanisms**
- **Security Architectures & Protocols**
- **Security Management, Awareness & Education**

Cryptographic Mechanisms –
Major Players

- ISO/IEC JTC 1/SC 27: Information technology - Security techniques
  - standardization of generic IT security services and techniques

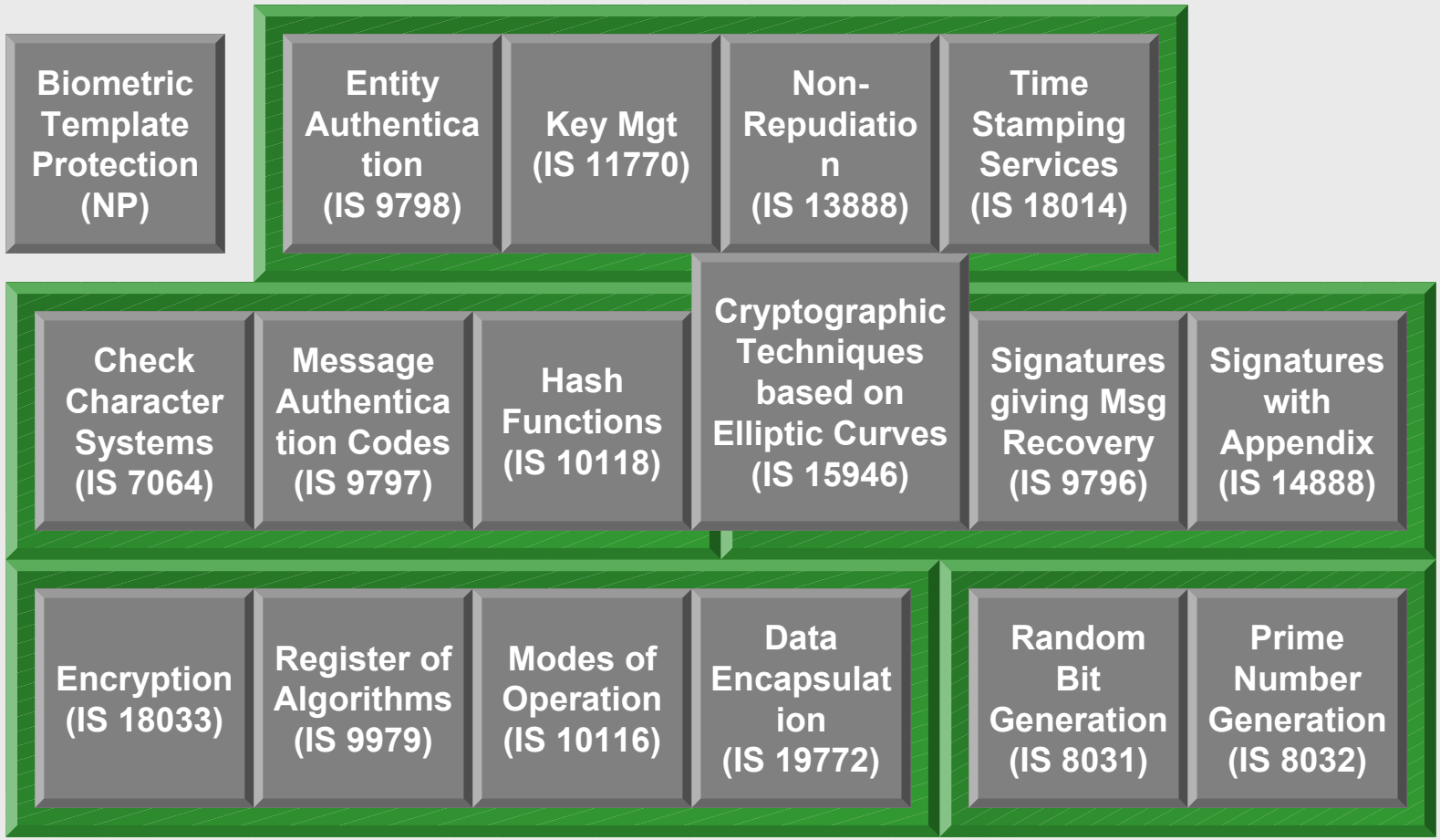
- ETSI SAGE: Security Experts Group
  - creates reports (containing confidential specifications) in the area of cryptographic algorithms and protocols specific to public/private telecommunications networks

- IEEE P1363: Standard Specifications for Public-Key Cryptography

- NIST: National Institute of Standards and Technology
  - issues standards and guidelines as Federal Information Processing Standards (FIPS) for use by the US government

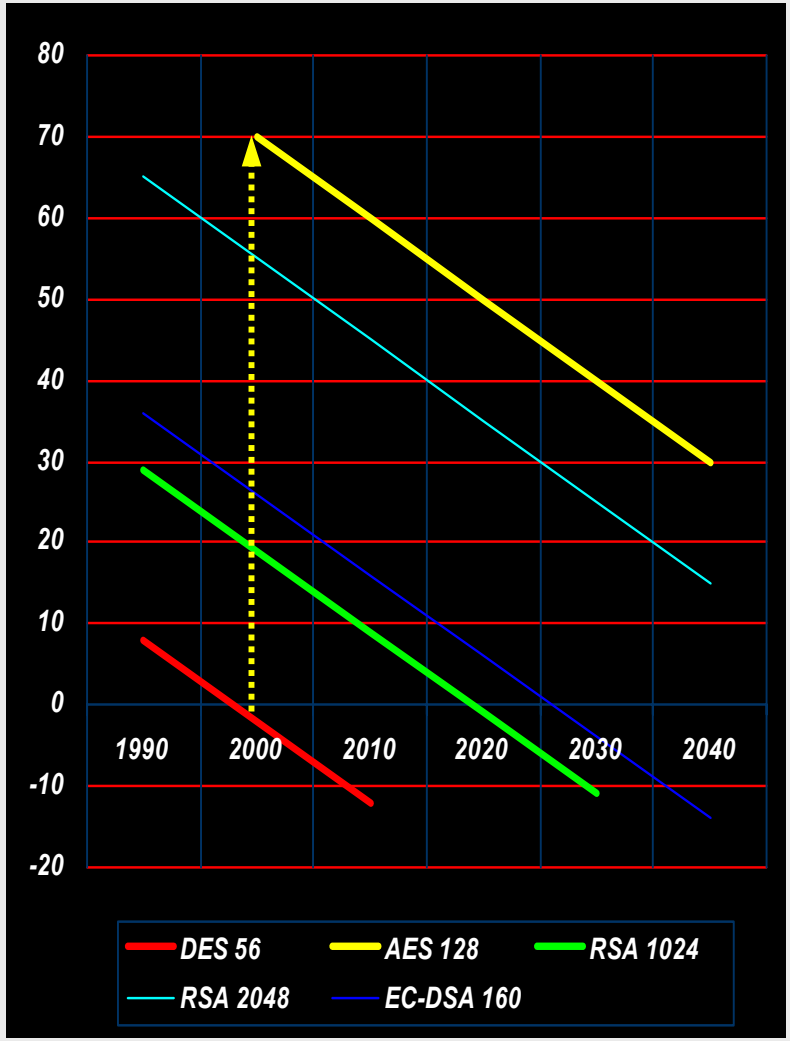
- ANSI X9F: Data & Information Security
  - standards for the financial services industry

Cryptographic Techniques –
SC 27 Standards



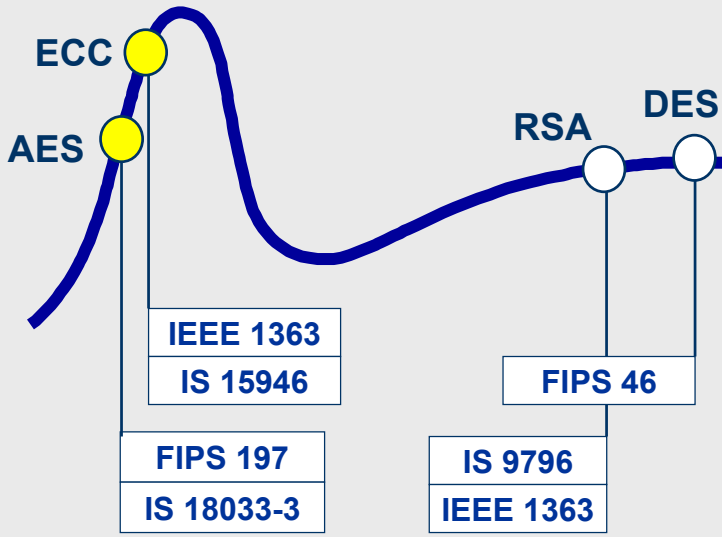
Lifetime of Cryptographic Algorithms

- Moore's law & steady growth of the Internet
  - Chip complexity doubles every 18 months
  - Internet computing power doubles every 12 months
  - ➔ Power of attack doubles every 12 months
- Steady loss of cryptographic strength
  - Symmetric ciphers „lose" 1 bit of security per year
  - Hash functions and Elliptic Curve based schemes „lose" 2 bits of security per year
  - RSA schemes „lose" about 50 bits of security per year
- Additional algorithmic improvements
  - in particular for asymmetric schemes



Conclusion
Cryptographic Mechanisms

- Well established technology
- Unanticipated advances in algorithms may occur
- Major trends include
  - increasing block and key lengths
  - increasing size of hash codes
  - signature schemes allowing for message recovery
  - randomized signatures



- New generation of mechanisms
  - DES ➔ AES
  - RSA ➔ ECC (?)
  - SHA-1 ➔ SHA-256, -384, -512
- Many techniques have been (or are being) standardized

- In addition, techniques are approved at a national level

ITU-T

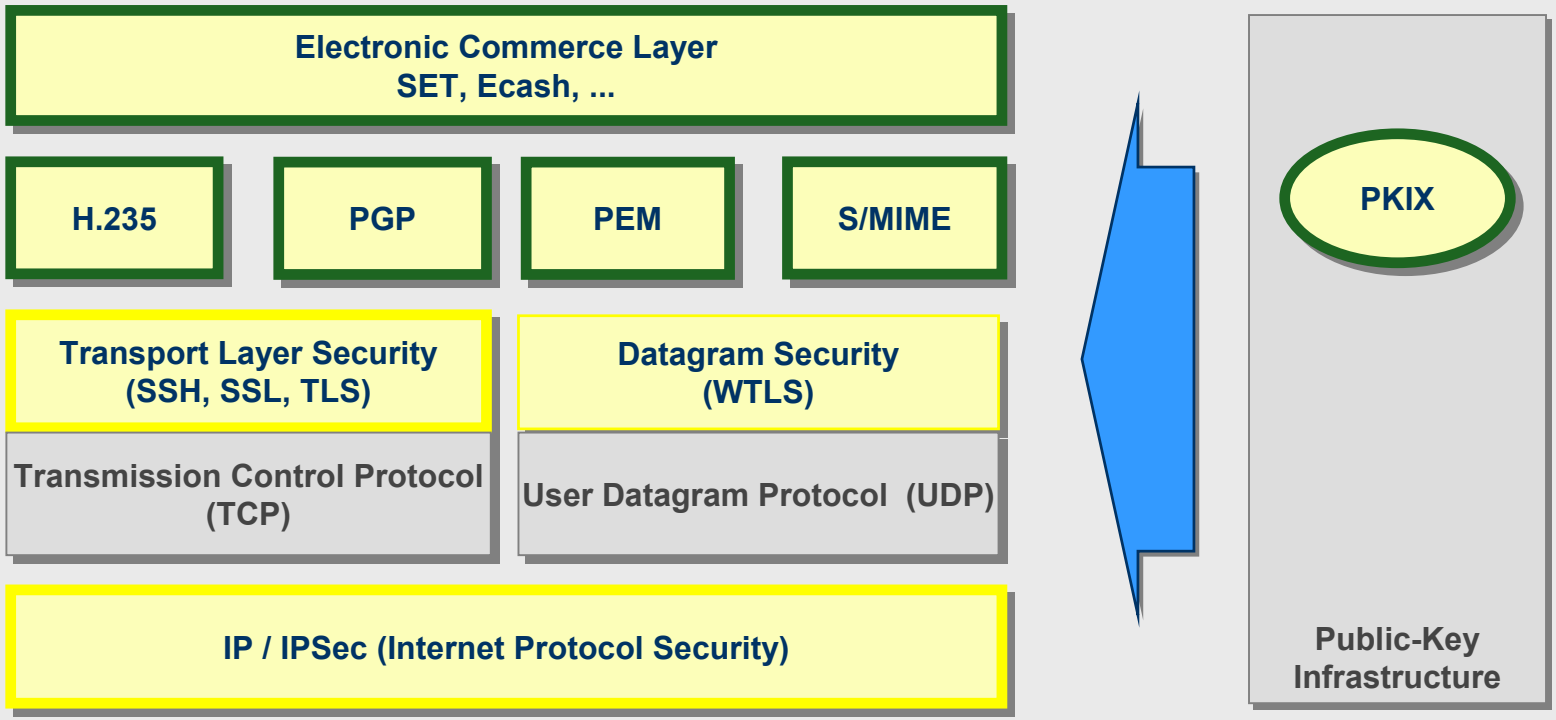
Cyber Security Standardization

- Cryptographic Mechanisms
- **Security Architectures & Protocols**
- Security Management, Awareness & Education

Security Protocols & Services – Major Players

- IETF: Internet Engineering Task Force
  - IP Security Protocol, Transport Layer Security, Public-Key Infrastructure (X.509), S/MIME Mail Security,...
- ITU-T: International Telecommunication Union
  - X.509 (Public-key certificates), H.235 (Security and encryption for H-Series multimedia terminals), X.841, X.842, X.843, ...
- ETSI
  - GSM, 3GPP, TETRA, TIPHON, SPAN, TISPAN, ...
- IEEE 802.11: Wireless LANs
  - 802.11i, 802.1X, ...

Internet Security Protocols



- Security services provided by security protocols depend on the layer of integration:
  - Security protocols can only protect the payload and/or header information available at this layer
  - Header information of lower layers is not protected

Conclusion
Security Architectures & Protocols

- IPSec and TLS are well-established security protocols
  - transition from DES to AES (at moderate speed)
- WEP is a weak security protocol
  - Confidentiality, data integrity & access control are not preserved when using WEP
  - VPN and other solutions can be used on top of WEP
  - 802.11i (RSN) overcomes the vulnerabilities of WEP
  - WPA serves as intermediate solution
- Definition of NGN security architecture at the beginning (ETSI TISPAN)
- Trend from security as an add-on to integrated security solutions

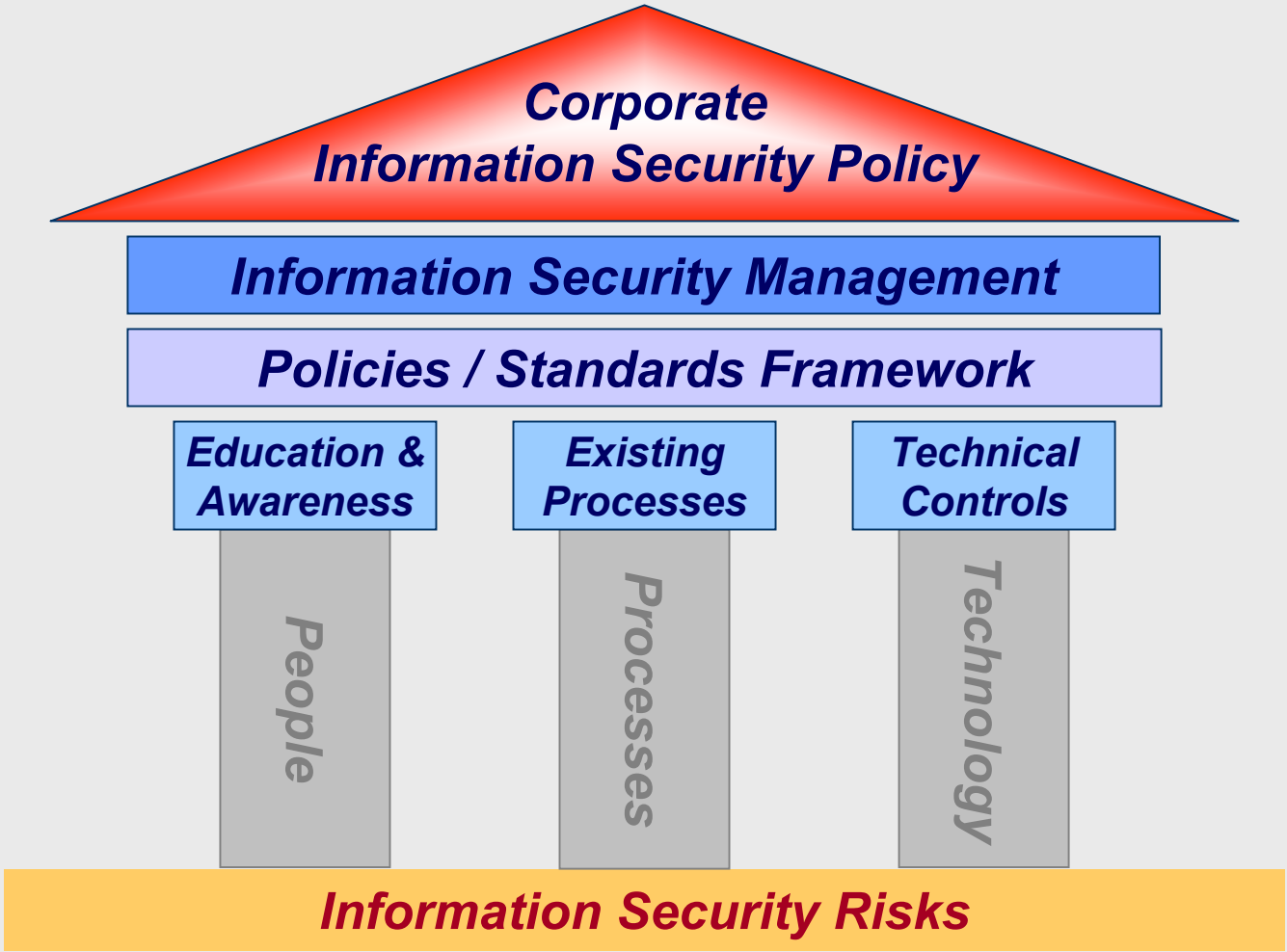
ITU-T

Cyber Security Standardization

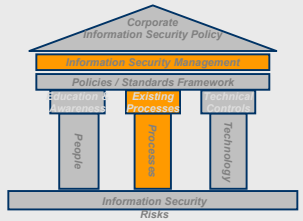
- Cryptographic Mechanisms
- Security Architectures & Protocols
- **Security Management, Awareness & Education**

Information Security Management System

Key Principles



Best Practice ISMS Model
(PDCA: Plan-Do-Check-Act)



Policies, Standards & Procedures

ISMS Processes

ISMS Operational Management

- Audit & Review
- Business Continuity Mgmt.
- Change Management
- Education & Awareness
- Incident Management
- Monitoring & Reporting
- Risk Analysis & Risk Mgmt.
- Security Operations Mgmt.

Management System Framework

managing & protecting people, business processes & applications, procedures, information, communications, networks, ...

Review & Audit

Events

- Security incidents
- Suspected weaknesses
- Malfunctions
- Audit observations
- Testing findings
- Spot check findings

'Evidential' documentation

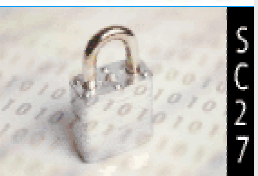
Recording and analysis

Report(s) into Forum(s)

Review and update ISMS

Hierarchical Security Management Model
(SC 27 View)

Terminology		ISO Guide 73	SC 27 SD 6 Updated and harmonized	
Overall Guide		Information Security Management Principles		
Principles		Information Security Mgt Framework	MICTS-1: Models and concepts	
Element Standards	Information Security Mgt System (NP)	Code of Practice for ISM (IS 17799 / ITU-T X.???)	MICTS-2: Risk management	ISM Metrics & Measurements (NP)
Application Guides and Supplements	ISO 19011 Auditing	Financial ISMS Guide (TC 68)	T-ISMS: Telecom ISMS Guide (ITU-T X.1051)	Healthcare ISMS Guide (TC 215)
Toolbox of Techniques	Info Security Incident Management (TR 18044)	IT Intrusion Detection Framework (TR 15947)	IT Network Security (IS 18028 / ITU-T X.???)	Guidelines for TTP Services (IS 14516 / ITU-T X.842)

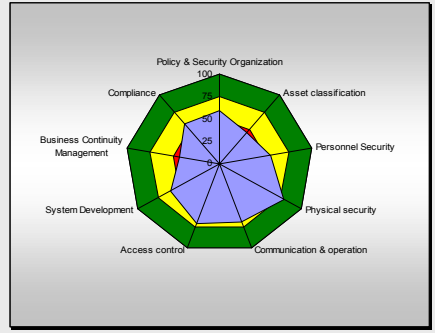


ISO/IEC 17799: Code of practice for information security management, 2000

- Guide for managing risk and development of a management system for
  - managing people, business processes & applications, procedures, information, communications, networks, operations, legal 3rd party services, compliance, contractual obligations, physical assets, etc.
- Developing information security assurance
  - organisational assurance, business partner and third party supplier assurance …
- based on BS 7799-1
- 2nd edition expected for 2005

- ISO 17799 Control Areas
  - Security Policy
  - Security Organization
  - Asset Control & Classification
  - Personnel Security
  - Physical & Environmental Security
  - Communications & Operations Management
  - Access Control
  - Systems Development & Maintenance
  - Business Continuity Management
  - Compliance

Example Scorecard
GAP Analysis IT Security



1 Information security policy	Middle	54 %	**6 Communications and operations management**	High	76 %	**8 System developement and maintenance**	Middle	71 %
1.1 Documentation of the security policy		54	6.1 Operational procedures and responsibilities		78	8.1 Security requirements of systems		75
2 Security organization	Middle	61 %	6.2 Systemplanning and acceptance		87	8.2 Security in application systems		65
2.1 Information security infrastructure		56	6.3 Protection against malicious software		82	8.3 Cryptographic controls	48	
2.2 Security of third party access		69	6.4 Housekeeping		80	8.4 Security of system files		95
2.3 Outsourcing		83	6.5 Network management		81	8.5 Security in development and support processes		81
3 Asset classification and control	Low	45 %	6.6 Media handling and security		56	**9 Business Continuity Management**	Middle	56 %
3.1 Accountability for assets		73	6.7 Exchange of information and software	50		9.1 Aspects of business continuity		56
3.2 Information classification	14		**7 Access control**	Middle	70 %	**10 Compliance**	Middle	57 %
4 Personnel security	Middle	54 %	7.1 Business requirements for access control		60	10.1 Compliance with legal requirements		63
4.1 Security in job definition and resourcing		62	7.2 User access management		78	10.2 Review of security policy and technical compliance	47	
4.2 User training	30		7.3 User responsibilities		65	10.3 System audit consideration	50	
4.3 Responding to security incidents and malfunctions		63	7.4 Network access control		74			
5 Physical and environmental security	High	78 %	7.5 Operating system access control		64			
5.1 Secure areas		85	7.6 Application access control		80	**Average InfoSec Status**	**66**	%
5.2 Equipment / site security		77	7.7 Monitoring system access and use		73			
5.3 General controls	47		7.8 Mobile computing and teleworking		60			

Standards –
Awareness, Training & Education

- National Colloquium for Information Systems Security Education
  - created in 1997 to provide a forum for dialogue among leading figures in government, industry, and academia
  - annual conference in June
  - www.ncisse.org

- NSA - National Information Assurance Education and Training Program (NIETP)
  - CNSS (Committee on National Security Systems) training & education standards
    - NSTISSI-4011 - INFOSEC Professionals
    - NSTISSI-4012 - Designated Approving Authority
    - NSTISSI-4013 - System Administrators in Information Systems Security
    - NSTISSI-4014 - Information Systems Security Officers (ISSO)
    - NSTISSI-4015 - System Certifiers
  - www.nsa.gov

Standards –
Awareness, Training & Education

- NIST – National Institute of Standards and Technology
  - Computer Security Division/Computer Security Resource Center
    - SP 800-16: *"IT Security Training Requirements, A Role- and Performance-Based Model"*
    - SP 800-50: *"Building an IT Security Awareness and Training Program"*
  - http://csrc.nist.gov

Conclusion

Security Management, Awareness & Education

- Need to continuously review policies, measures, and procedures to help assure that they meet the evolving challenges posed by threats to IT systems and networks
- Today, there is no internationally recognized Information Security Management System (ISMS) standard
  - there are a number of ISMS standards at a national or regional level, including
    - BS 7799-2: Information security management systems - Specification with guidance for use (UK)
    - IT Baseline Protection Manual (Germany)
  - there are international standards that cover certain elements of an ISMS
    - process guidelines (e.g., IS 13335, IS 21827)
    - procedural guidelines (e.g., TR 18044)
    - catalogues of controls (e.g., IS 17799)

ITU-T

Cyber Security Standardization Initiatives

Example:
Cyber Security Standard for Electricity Sector

- developed by North American Electric Reliability Council (NERC)
- NERC Critical Infrastructure Protection Advisory Group (CIPAG) initiated “Urgent Action Standard Authorization Request” to establish a NERC Cyber Security Standard

➔ NERC Urgent Action Standard 1200: *Cyber Security*

  - approved June 2003
  - in effect for one year with possible one-year extension
    - NERC Board of Trustees approved one-year extension, effective August 13, 2004
  - to be replaced with permanent standard via ANSI Standard Authorization process
  - compliance with this standard will be evaluated in the first quarter of 2005

ANSI
Homeland Security Standards Panel (HSSP)

- Formation of ANSI-HSSP announced February, 2003
- Facilitate the development and enhancement of homeland security standards
- Serve as private/public sector forum for standards issues that cut cross-sector
  - Co-chairs provided by industry and government
- A forum for information sharing on HS standards issues
- Does not itself develop standards

- http://www.ansi.org/hssp

ISO Technical Management Board
Advisory Group on Security

The ISO/TMB Advisory Group will

- conduct a review of existing ISO deliverables related to the field of security, including the subjects of:
  - Private sector emergency preparedness and business continuity
  - Identification techniques, including biometrics
  - Emergency communications
  - Risk assessment
  - Cyber security
  - ...
- assess the needs of all relevant stakeholders for international security standards
- assess relevant standards developed by other organizations
- recommend actions to be taken by the ISO Council and/or ISO/TMB on subjects within the field of security that may benefit from the development of International Standards and that ISO would have the capability to provide
- submit a final report to the ISO/TMB and ISO Council by 31 December 2004

ENISA –
European Network & Information Security Agency

- Objectives
  - to facilitate the application of European Community measures relating to network and information security
  - to help ensure the interoperability of security functions in networks and information systems
  - to enhance the capability of the Community and the Member States to respond to network and information security problems
- established in March 2004
- situated on Greek island
- www.enisa.eu.int
- Conference on Network & Information Security
  - e-Security in Europe: Today's status and The Next Step
  - Amsterdam 27, 28 October 2004

Conclusion

- “The good thing about standards is ...
  there are so many to choose from”

- A substantial number of cyber security standards is available or available or currently under development
- There are initiatives at both national and international levels to to identify gaps and to recommend actions

- Improved collaboration and harmonization between standards organizations needed

Annex

ISO/IEC JTC 1/SC 27
IT Security Techniques

SC 27 - "IT Security Techniques"

- Standardization of generic IT security services and techniques, including
  - identification of generic requirements for IT system security services,
  - development of security techniques and mechanisms (cryptographic and non-cryptographic),
  - development of security guidelines,
  - development of management support documentation and standards,
  - development of criteria for IT security evaluation and certification of IT systems, components, and products.

ISO/IEC JTC 1/SC 27: Information technology - Security techniques *Chair: Mr. W. Fumy* *Vice-Chair: Ms. M. De Soete*	***SC 27 Secretariat DIN*** *Ms. K. Passia*

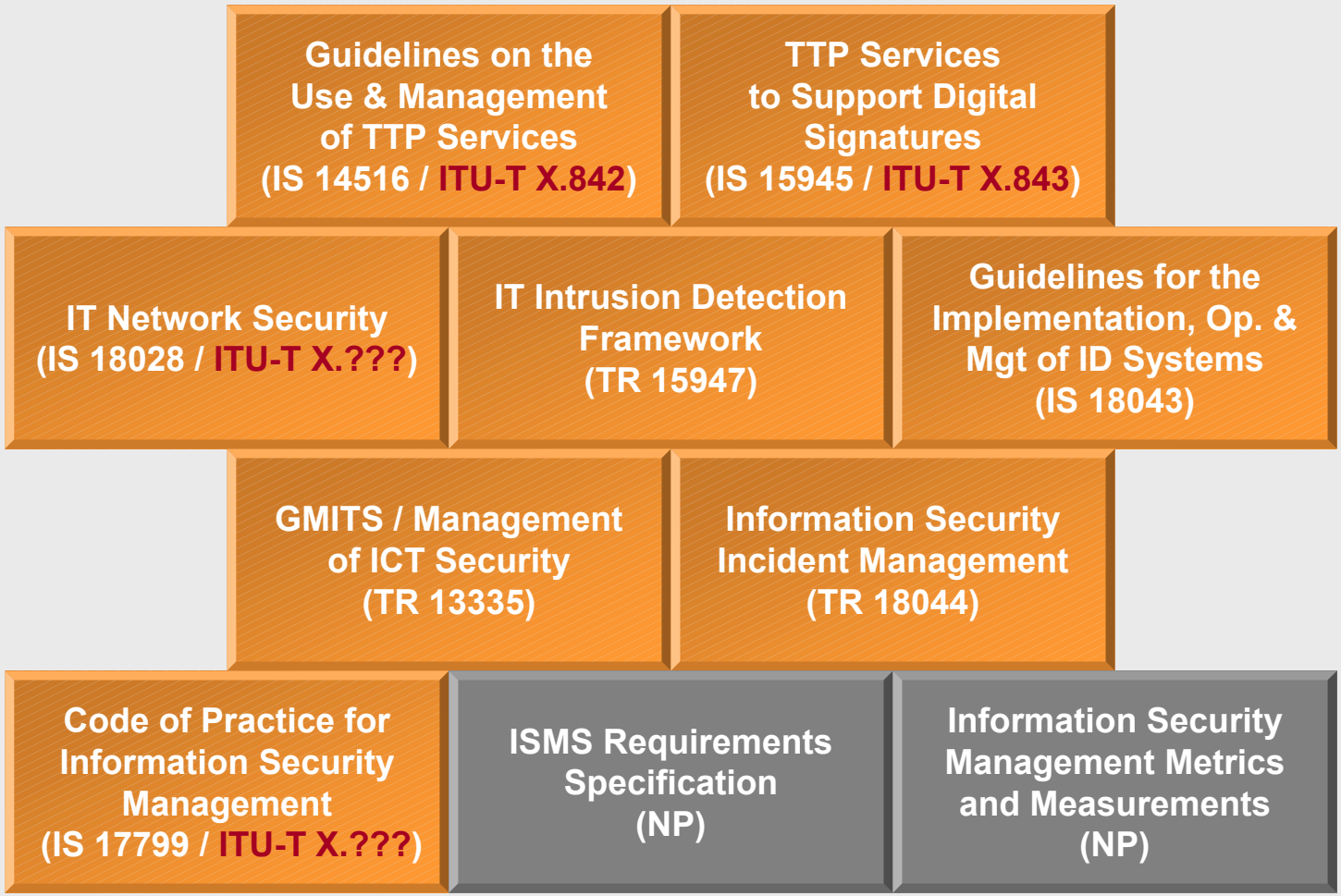
Working Group 1 Requirements, services, guidelines *Convener* *Mr. T. Humphreys*	***Working Group 2 Security techniques and mechanisms*** *Convener* *Mr. K. Naemura*	***Working Group 3 Security evaluation criteria*** *Convener* *Mr. M. Ohlin*

Membership of SC 27

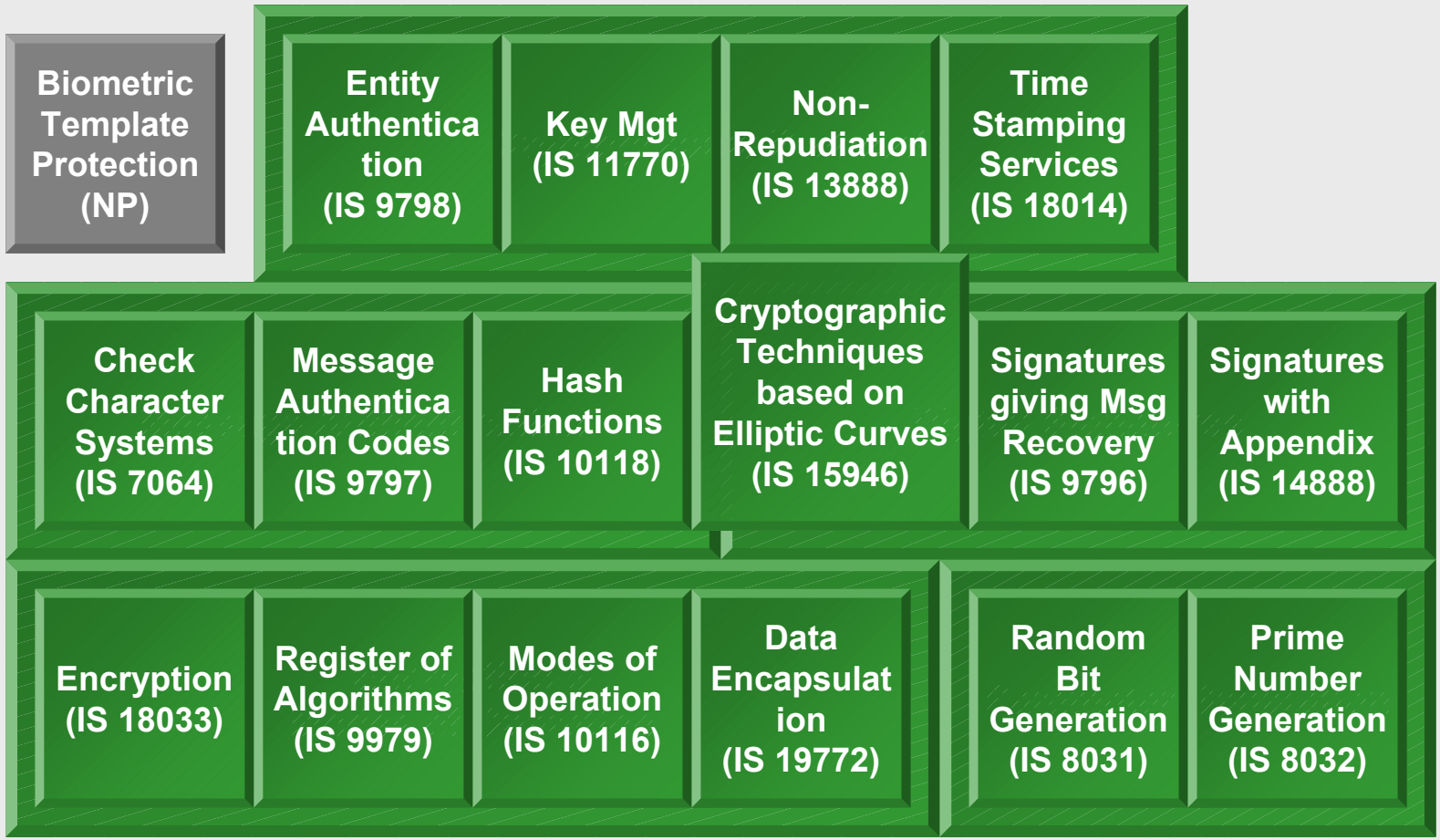
- Participating Membership
  - Obligation to take an active part in the work (e.g., to attend meetings, to vote)
  - One Member Body per country (e.g., ANSI, IBN, BSI, DIN)
  - Power of vote
- P-members of SC 27 (total 31)
  - South Africa, Kenya
  - Brazil, Canada, USA
  - Australia, China, India, Japan, Korea, Malaysia, **New Zealand, Singapore**
  - **Austria**, Belgium, Czech Republic, Denmark, Finland, France, Germany, Italy, Luxembourg, Netherlands, Norway, Poland, Russian Federation, Spain, Sweden, Switzerland, UK, Ukraine
- Observing Membership
  - Option to take an active part in the work (e.g., to attend meetings, to make contributions, to receive documents)
  - No power of vote
- O-members of SC 27 (total 11)
  - Argentina
  - Indonesia
  - Estonia, Hungary, Ireland, Israel, **Lithuania**, Serbia and Montenegro, Romania, Slovakia, **Turkey**

***) new SC 27 members**

Security Guidelines –
SC 27 Standards



Cryptographic Techniques –
SC 27 Standards



Security Evaluation –
SC 27 Standards

ITU-T

JTC1 ISO IEC Information Technology Standards

SC 27

- Methodology for IT Security Evaluation (IS 18045)
- Systems Security Engineering – Capability Maturity Model (IS 21827)
- Framework for IT Security Assurance (TR 15443)
- Security Assessment of Operational Systems (TR 19791)
- Framework for Security Evaluation & Testing of Biometric Technology (TR 19792)
- Protection Profile Registration Procedures (IS 15292)
- Guide on the Production of Protection Profiles & Security Targets (TR 15446)
- Evaluation Criteria for IT Security ("Common Criteria") (IS 15408)
- Security Requirements for Cryptographic Modules (TR 19790)

New Projects

- IS 9798: Entity authentication mechanisms
  - Part 6: Entity authentication based on manual data transfer
- IS 11770: Key management
  - Part 4: Key establishment mechanisms based on weak secrets

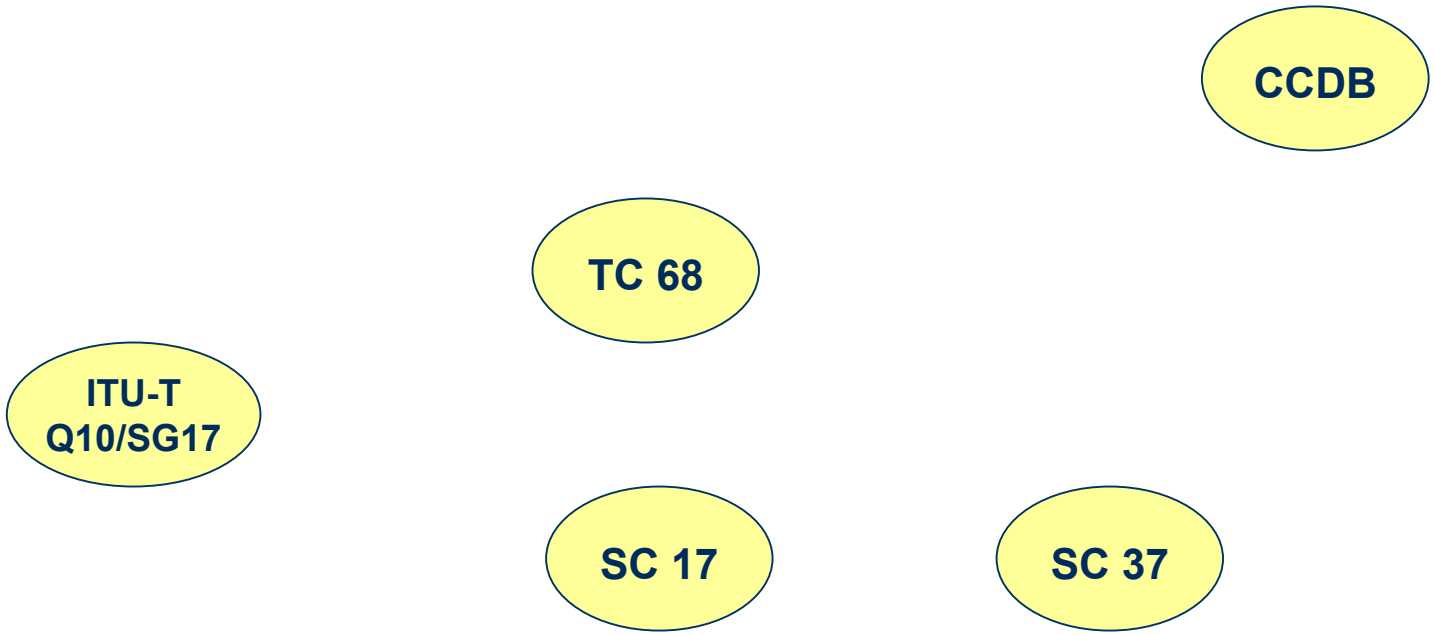
- IS 19790: Security requirements for cryptographic modules
- TR 19791: Security assessment of operational systems
- IS 19792: A framework for security evaluation and testing of biometric technology

- 2nd edition of IS 15408: Evaluation criteria for IT Security, 1999
  - next ICC conference: 28.9. - 30.9.2004, Berlin
  - www.commoncriteriaportal.org (under construction)

NP & PAS Ballots

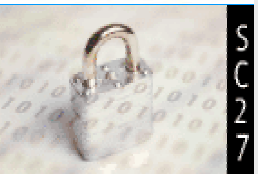
- NP Ballots
  - Information Security Management System (ISMS)
  - Information security management metrics and measurements
  - Biometric template protection
  - ISO/IEC 18043: Selection, deployment and operation of intrusion detection systems (IDS) *[formerly TR]*
- PAS Ballot
  - DIS 20886: International Security, Trust, and Privacy Alliance - Privacy Framework *[ballot ends 2004-12-11]*

Selected Collaboration



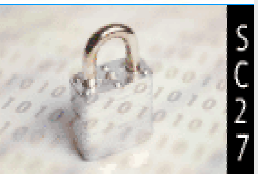
SC 27 Collaboration
ITU-T SG 17/Q.10

- ITU-T Study Group 17 has been designated the Lead Study Group for Communication Systems Security (CSS)
  - within SG 17 the Rapporteur for Q.10/17 has been identified as the coordinator for CSS activities
- Close collaboration between SC 27 and Q.10/17 in order to progress common or twin text documents and to publish common standards:
    - ISO/IEC 15816: Security information objects for access control (= ITU-T X.841)
    - ISO/IEC 14516: Guidelines on the use and management of Trusted Third Party services (= ITU-T X.842)
    - ISO/IEC 15945: Specification of TTP services to support the application of digital signatures (= ITU-T X.843)
    - ISO/IEC 18028: IT Network Security (= ITU-T X.???)
    - ISO/IEC 17799: Code of Practice for Information Security Management (= ITU-T X.???)



Summary

- SC 27 is responsible for
  - > 60 projects, including 26 active projects
- Between 1990 and today, SC 27 has published
  - 32 ISO/IEC International Standards (IS)
  - 13 revised editions of International Standards
  - 6 ISO/IEC Technical Reports (TR)
- More Information & Contact
  - SC 27 web-page: scope, organization, work items, etc. http://www.ni.din.de/sc27
  - Catalogue of SC 27 Projects & Standards http://www.ni.din.de/sc27/doc7.html
  - SC 27 Secretariat: Krystyna.Passia@din.de
  - SC 27 Chairman: Walter.Fumy@siemens.com



Any Questions ?