



ISO/IEC JTC 1/SC 27 N7769

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: officer's contribution

TITLE: SC 27 Presentation to ITU-T Workshop in Geneva, February 2009

SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2009-02-01

PROJECT:

STATUS: This document is being circulated for information.

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
T. Humphreys, M.-C. Kang, K. Naemura, M. Ohlin, K. Rannenber, WG-
Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 18



SC 27

ISO/IEC JTC 1/SC 27 – IT Security Techniques

Dr. Walter Fumy, Chief Scientist, Bundesdruckerei GmbH

ISO/IEC JTC 1 – Information Technology

Security Related Sub-committees



- SC 6 Telecommunications and information exchange between systems
- SC 7 Software and systems engineering
- SC 17 Cards and personal identification
- SC 25 Interconnection of information technology equipment
- SC 27 IT Security techniques
- SC 29 Coding of audio, picture, multimedia and hypermedia information
- SC 31 Automatic identification and data capture techniques
- SC 32 Data management and interchange
- SC 36 Information technology for learning, education and training
- SC 37 Biometrics

SC 27 – IT Security Techniques

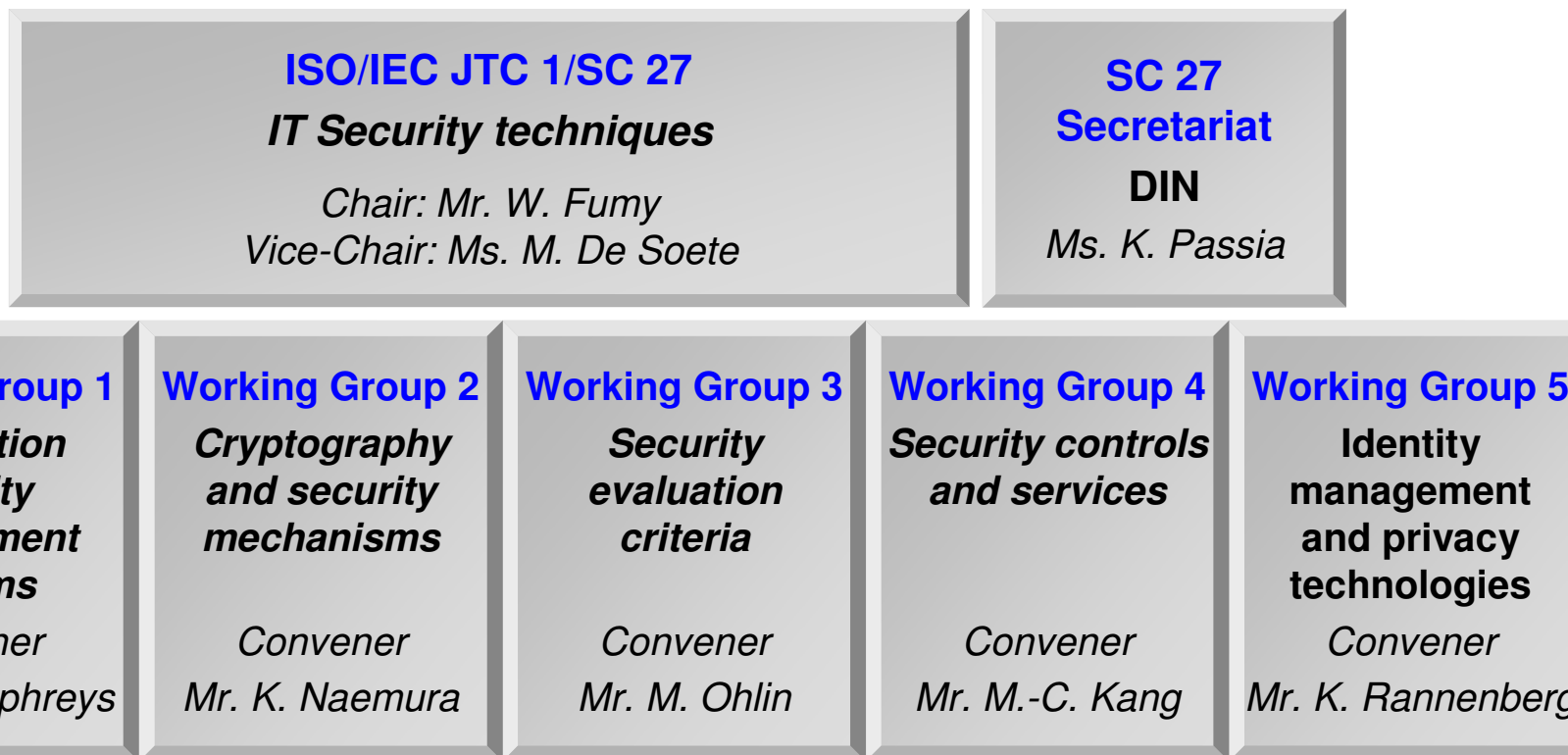
Scope



The development of standards for the protection of information and ICT. This includes **generic methods, techniques and guidelines to address both security and privacy aspects**, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

SC 27 – IT Security Techniques *Organization*



<http://www.jtc1sc27.din.de/en>

SC 27/WG 1

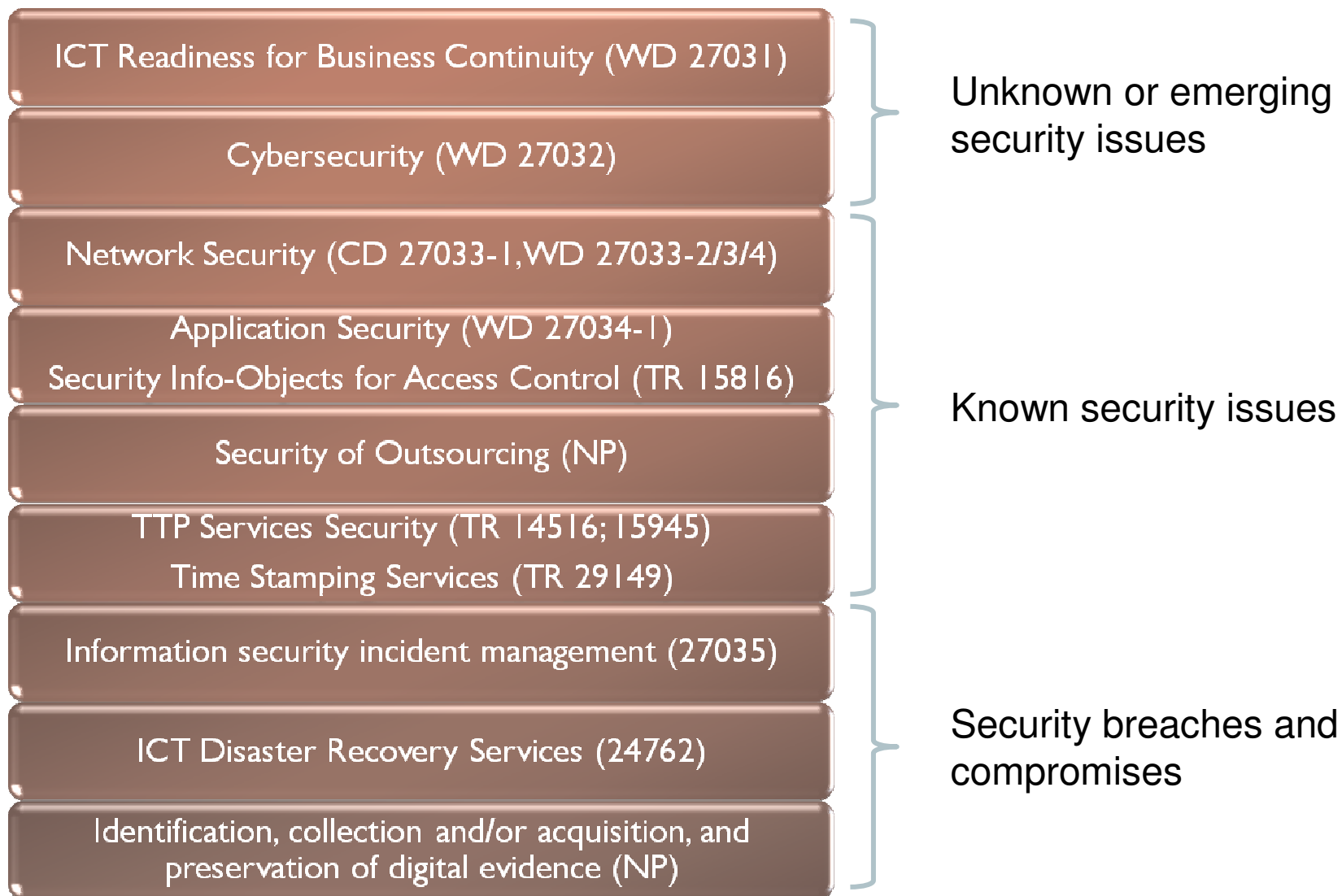
ISMS Family of Standards



27001 ISMS Requirements		
27000 ISMS Overview and Vocabulary	27006 Accreditation Requirements	27010 ISMS for Inter-sector communications
27002 (pka 17799) Code of Practice	27007 ISMS Auditing Guidance	27011 Telecom Sector ISMS Requirements
27003 ISMS Implementation Guidance	27008 ISMS Guide for auditors on ISMS controls	27012 ISMS for e-Government
27004 Information Security Mgt Measurements		27015 Financial and Insurance Sector ISMS Requirements
27005 Information Security Risk Management		
Supporting Guidelines	Accreditation Requirements and Auditing Guidelines	Sector Specific Requirements and Guidelines

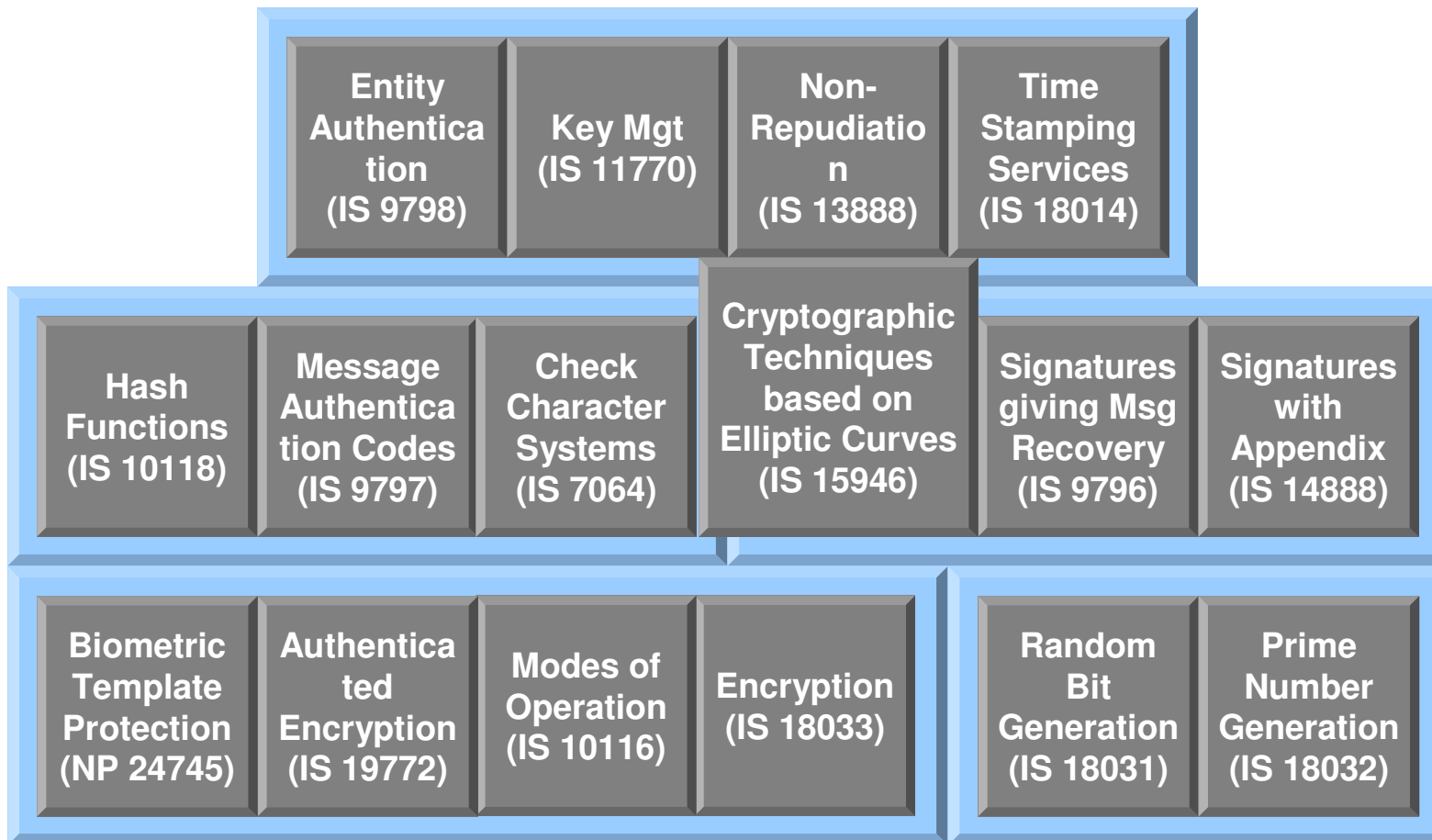
SC 27/WG 4

Security Controls and Services



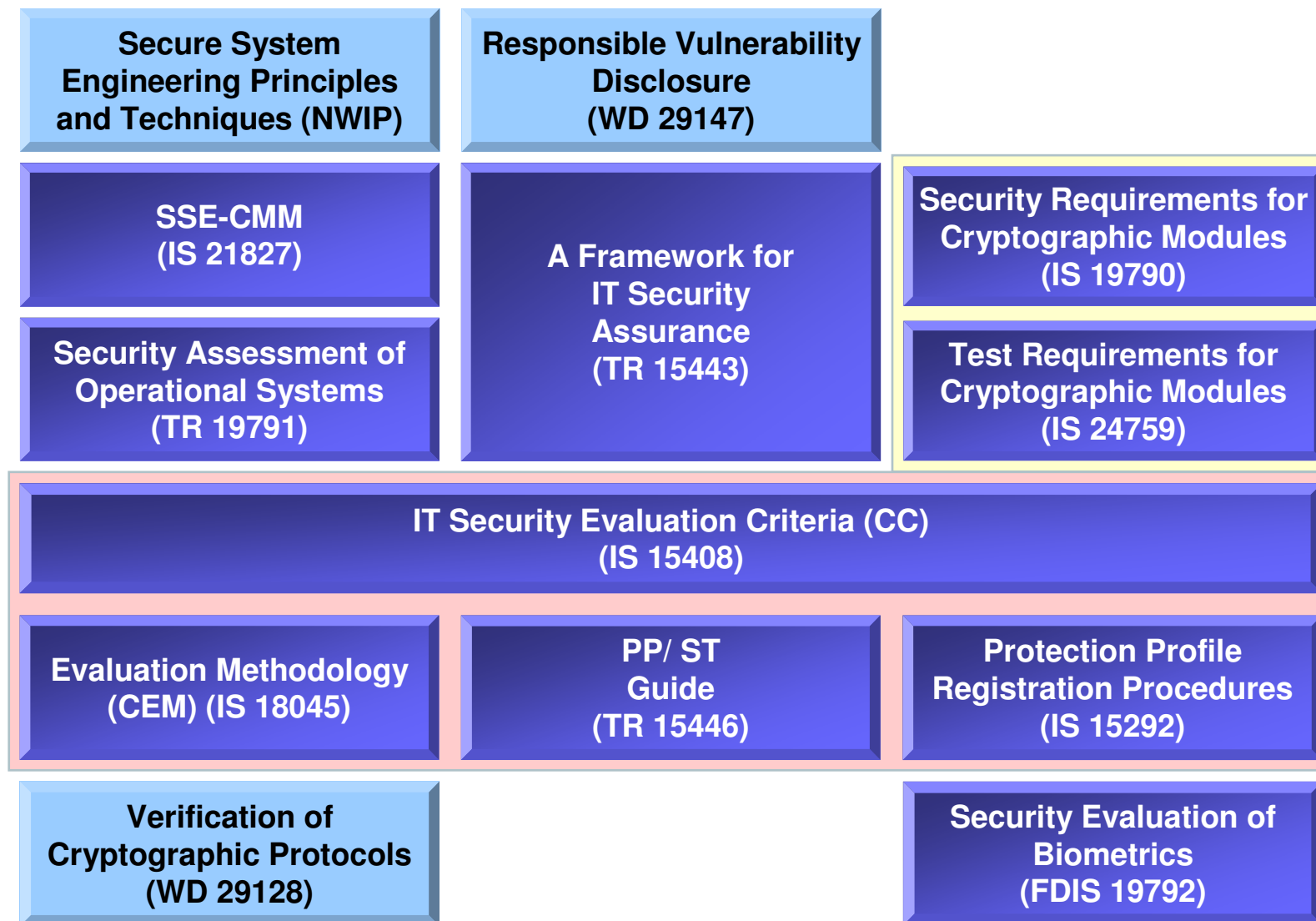
SC 27/WG 2

Cryptography and Security Mechanisms



SC 27/WG 3

Security Evaluation Criteria





SC 27/WG 5

Identity Management & Privacy Technologies

WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data. This includes:

- **Frameworks & Architectures**

- A Framework for Identity Management (ISO/IEC 24760, WD)
- Privacy Framework (ISO/IEC 29100, CD)
- Privacy Reference Architecture (ISO/IEC 29101, WD)
- A Framework for Access Management (ISO/IEC 29146, WD)

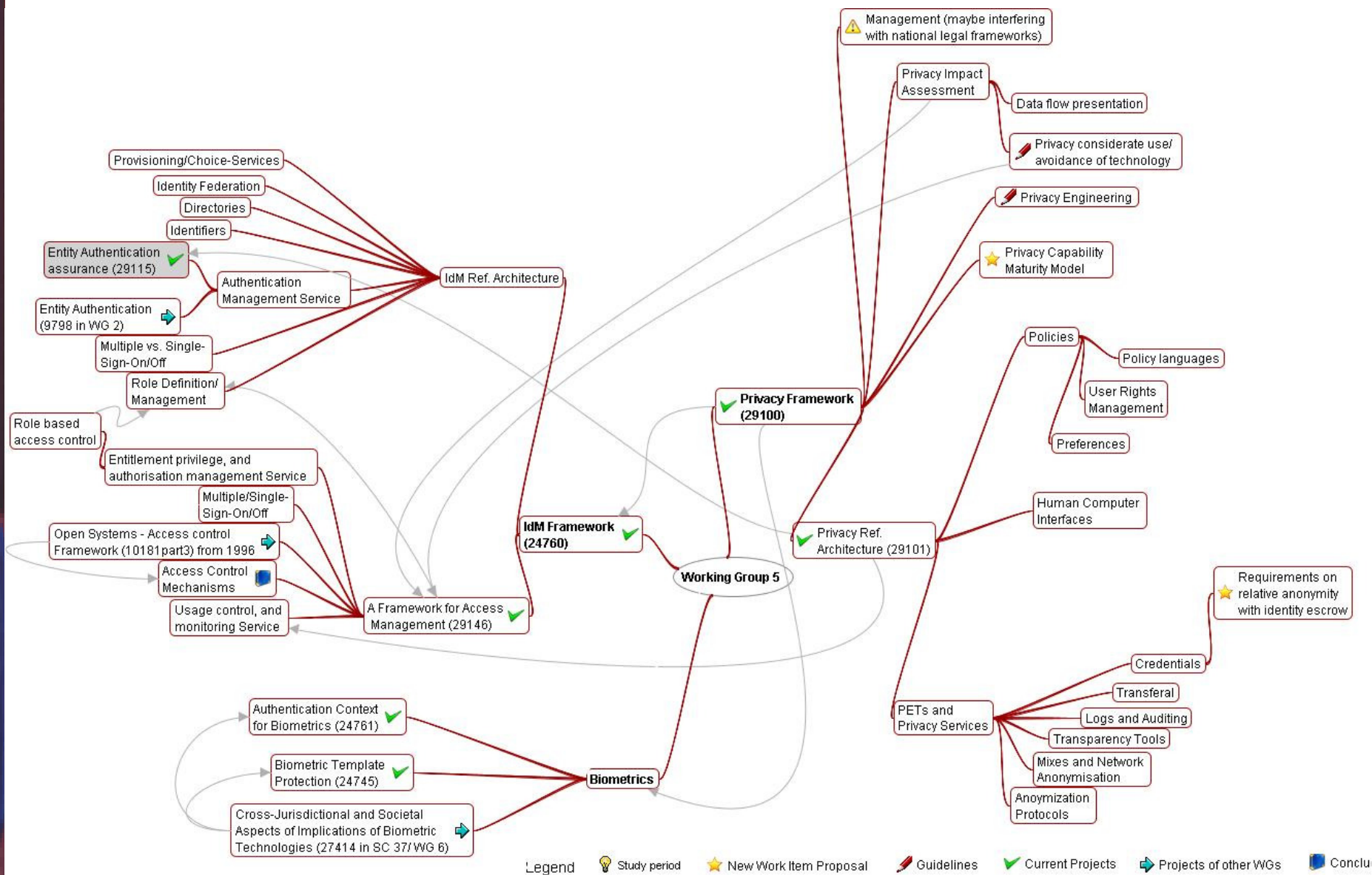
- **Protection Concepts**

- Biometric template protection (ISO/IEC 24745, WD)
- Requirements on relative anonymity with identity escrow – model for authentication and authorization using group signatures (NWIP)

- **Guidance on Context and Assessment**

- Authentication Context for Biometrics (ISO/IEC 24761, FDIS)
- Entity Authentication Assurance (ISO/IEC 29115, WD)
- Privacy Capability Maturity Model (NWIP)

Identity Management & Privacy Technologies Roadmap



ISO/IEC PAS 11889

Trusted Platform Module



- The Trusted Computing Group (TCG) submitted the TPM 1.2 specification to JTC 1 for PAS Transposition
- ⇒ ISO/IEC PAS DIS 11889
 - Trusted Platform Module - Part 1: Overview
 - Trusted Platform Module - Part 2: Design principles
 - Trusted Platform Module - Part 3: Structures
 - Trusted Platform Module - Part 4: Commands
- ⇒ 6 month NB ballot closed 2008-07-24
- ⇒ Ballot resolution meeting 2008-10-11, Limassol, Cyprus
- ⇒ Final text for ISO/IEC 11889 submitted for publication

SC 27 – IT Security Techniques

Approved New Projects



- NP 27008: *Guidance for auditors on ISMS controls.*
- NP 27010: *Information security management for inter-sector communications.*
- NP 27012: *Information security management guidelines for e-government services.*
- NP 27035: *Information security incident management.*
- NP 29128: *Verification of cryptographic protocols.*
- NP 29146: *A framework for access management.*
- NP 29147: *Responsible vulnerability disclosure.*
- NP 29149: *Best practice on the provision of time-stamping services.*
- NP 29150: *Signcryption.*

SC 27 – IT Security Techniques

Proposed New Projects – Approval Pending



- NP 27013: Guidance for the integrated implementation of 20000-1 with 27001 (collaborative with JTC 1/SC7).
- NP 27014: Information security governance framework.
- NP 27015: *Information security management systems (ISMS) for the financial and insurance services sector.*
- *Guidelines for the security of outsourcing.*
- *Guidelines for identification, collection, and/or acquisition and preservation of digital evidence.*
- Requirements on relative anonymity with identity escrow - *Model for authentication and authorization using group signatures.*
- Privacy Capability Maturity Model.
- *Secure System Engineering principles and techniques.*
- Lightweight cryptography.

SC 27 – IT Security Techniques

Achievements & New Projects



Summary

Between November 2007 and October 2008

- 14 International Standards and Technical Reports have been published (total number of pages: 1331)
- 2 International Standards are awaiting publication

- 9 New Projects have been approved
- 9 Proposed Projects are awaiting approval

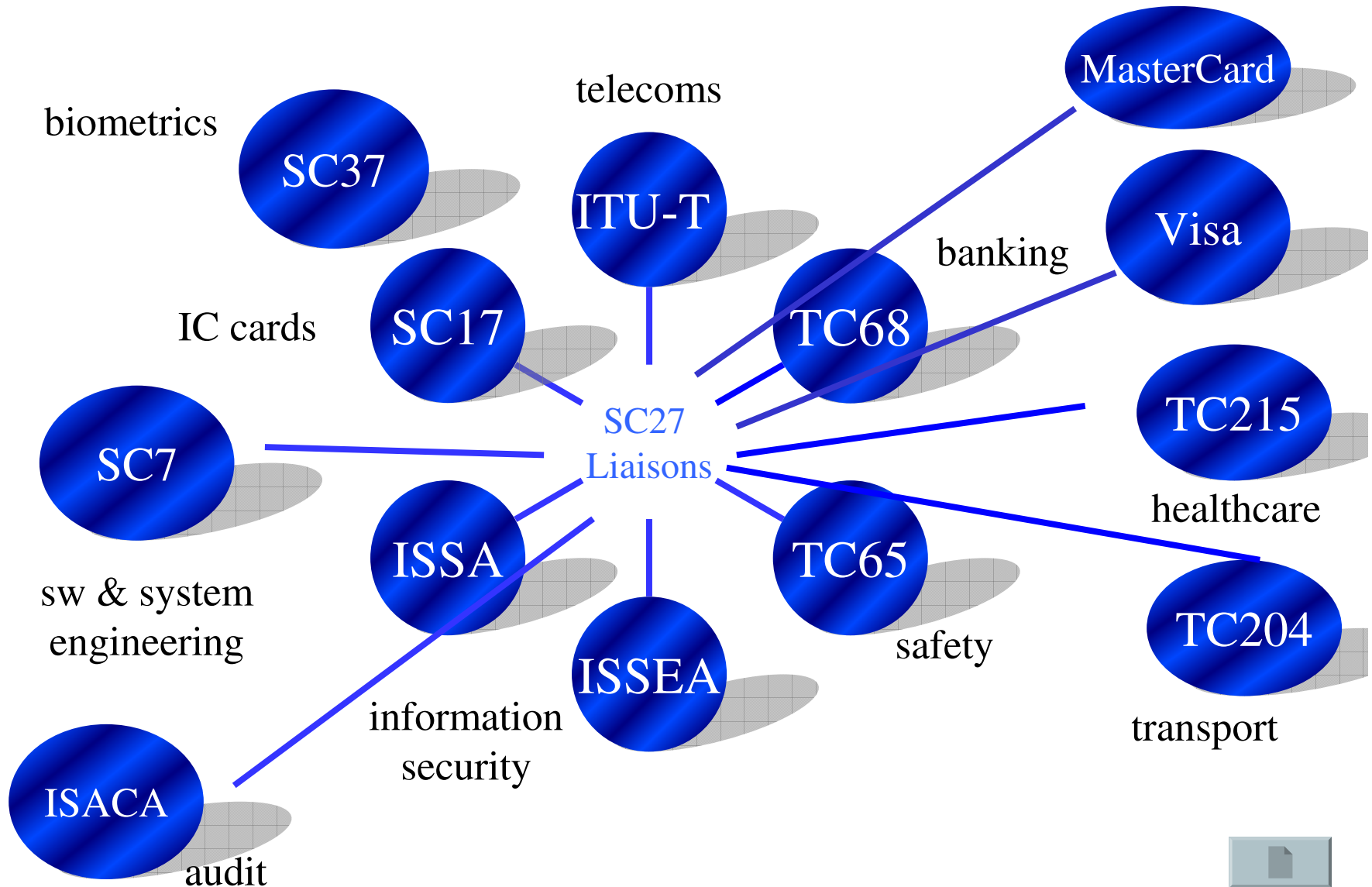
Average # of ISO standards published in 2007

- 2.04 per SC
- 0.48 per WG

Average # of pages published in 2007

- 106 per SC
- 25 per WG

Selected Liaisons





Conclusion

- The good news about (security) standards is ...
... there are so many to choose from :-)
 - Given the limited availability of resources for the development of security standards, we must avoid duplication of effort and make use of effective cooperation and collaboration.
 - Given the vast number of activities in the area of security standards, we must bring together information about existing standards, standards under development, and key organizations that are working on these standards.
- ⇒ [ICT Security Standards Roadmap](#)

SD 11: Information and ICT Security Standards – An invitation to the past, present, and future work of SC27



- Provides an high-level overview of the work of SC27.
- Includes a number of the SC27 articles that have been published by ISO in the publications ISO Focus, ISO Journal and ISO Management System.
- Freely available
⇒ <http://www.jtc1sc27.din.de/sce/sd11>
- Version 2.0, September 2008 (100 pages).



More Information & Contact

- <http://www.jtc1sc27.din.de/en>
- SC 27 Secretariat: *Krystyna.Passia@din.de*
- SC 27 Chairman: *Walter.Fumy@bdr.de*
- SC 27 Vice Chair: *Marijke.DeSoete@pandora.be*

RSA CONFERENCE JAPAN 2008 4月24日(木)	
Convention Hall F	
14:05 ▼	C5-2 ITセキュリティの国際標準化
14:55	Walter Fumy Siemens AG
15:10 ▼	C5-3 情報セキュリティのマネージメント、 ガバナンス、コンプライアンス
16:00	Edward Humphreys XISSEC
16:30 ▼	C5-4 移りゆく世界の中で変化する安全なアイデンティティー「アイデンティティ登録とプライバシー保護」ISO/IEC JTC 1/SC27 WG 50取り組み
17:20	Kai Rannenberg Goethe University Frankfurt
17:35 ▼	C5-5 サイバーセキュリティにおける セキュリティ標準の役割
18:25	Meng-Chow Kang Microsoft China (Beijing) Ltd. ISO/IEC JTC 1/SC 27