ISO/IEC JTC 1 N 9910

2009-11-17

ISO/IEC JTC 1
Information Technology

Document Type: Other document (defined)

Document Title: Revised SC 27 chair's presentation

Document Source: SC 27 Chairman

Reference:

Document Status: This document is forwarded to JTC 1 National Bodies for information.

Action ID:

Due Date:

No. of Pages: 8

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1 SC 27

Walter Fumy, SC Chair
Krystyna Passia, SC Secretariat

2009 JTC 1 Plenary, Tel Aviv

What Is New?

Between November 2008 and October 2009

- 13 International Standards and Technical Reports have been published (total number of pages: 1019)
- 9 New Projects have been approved (total number of projects: 123)
- 4 additional P-members (+10%) (total number of P-members: 42)
- 11 additional liaisons (+28%) (total number of liaisons: **50**)

Approved New Projects

- NP 27013: *Guidance for the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001.*
- NP 27014: *Information security governance framework.*
- NP 27015: *Information security management system for financial and insurance services sector.*
- NP 27036: *Guidelines for security of outsourcing.*
- NP 27037: *Guidelines for identification, collection and/or acquisition and preservation of digital evidence.*
- NP 29190: *Privacy capability maturity model.*
- NP 29191: *Requirements on relative anonymity with identity escrow.*
- NP 29192: *Lightweight cryptography.*
- NP 29193: *Secure system engineering principles and techniques.*

Membership of SC 27

Brazil	Belgium	France	Netherlands	Sweden	~~Israel~~	
Canada	Denmark	Germany	Norway	Switzerland	China	
USA	Finland	Italy	Spain	UK	Japan	
founding P-Members (18 in 1990)						
						Morocco
						Côte-d'Ivoire
					Venezuela	Ireland
Russian Federation	Poland	South Africa	Kenya	Sri Lanka	Kazakhstan	Slovakia
Korea	Ukraine	Malaysia	Austria	New Zealand	Cyprus	Algeria
Australia	Czech Republic	India	Luxembourg	Singapore	Uruguay	Romania
1994	*1996-1999*	*2001*	*2002*	*2003-2005*	*2006-2007*	*2008-2009*
additional P-Members (total: 42)						

+ 13 O-members [www.jtc1sc27.din.de/sbe/members]

Liaisons within ISO/IEC JTC 1

- JTC 1 Ad Hoc on Vocabulary
- new JTC 1/WG 6 Corporate Governance of IT
- SC 6 Telecommunications and information exchange between systems
- SC 7 Software engineering
- SC 17/WG 3 Machine readable travel documents
- SC 17/WG 4 Integrated circuit cards with contacts
- SC 17/WG 11 Application of Biometrics to Cards and Personal Identification
- SC 22 Programming languages, their environments and system software interfaces
- SC 25 Interconnection of IT Equipment
- new SC 31/WG 4 (Automatic Identification and Data Capture Techniques)
- SC 36 Information technology for learning, education, and training
- SC 37 Biometrics

Liaisons within ISO / IEC

- ISO/CASCO
- ISO/JTCG Joint Technical Coordination Group on MSS
- new ISO/PC 246 Anti-counterfeiting tools
- new ISO/TC 46/SC 11 Information and documentation - Archives/records management **
- ISO/TC 68/SC 2 Financial services -- Security management and general banking operations
- new ISO/TC 204 Intelligent transport systems - WG 1 Architecture
- ISO/TC 215 Health Informatics - WG 4 Security & WG 5 Health cards
- ISO/TC 223 Societal Security
- ISO/TMB WG RM
- new IEC/TC 65 Industrial-process measurement, control and automation - WG 10 Security for industrial process measurement and control - Network and system security ***

** subject to SC 27 approval
*** subject to IEC/TC 65 approval

External CAT A Liaisons

- new ENISA (European Network and Information Security Agency) *
- European Payment Council / Security of Payment Task Force (EPC/SPTF)
- ITU Development Sector (ITU-D)
- ITU-T Study Group 13 (ITU-T SG 13)
- ITU-T Study Group 17 (ITU-T SG 17)
- MasterCard
- VISA Europe

* subject to JTC 1 endorsement

External CAT C Liaisons

- ASIS International
- CEN Workshop on Cyber Identity
- Common Criteria Development Board (CCDB)
- Forum of Incident Response and Security Teams (FIRST)
- Future of Identity in the Information Society (FIDIS)
- European Network of Excellence for Cryptology (ECRYPT)
- new Information Security Forum (ISF)
- new Information Systems Audit and Control Association/IT Governance Institute (ISACA / ITGI)
- International Conference of Data Protection and Privacy Commissioners
- International Systems Security Association (ISSA)
- International Systems Security Engineering Association (ISSEA) STOP
- Liberty Alliance
- Network and Information Security Steering Group (CEN/NISSG)
- Privacy and Identity Management for Community Services (PICOS)
- Privacy and Identity Management in Europe for Life (PrimeLife)
- The Open Group
- The World Lottery Association (WLA)
- new Trusted Computing Group (TCG)
- new TAS3 (Trusted Architecture for Securely Shared Services)*

* subject to JTC 1 endorsement

User Engagement

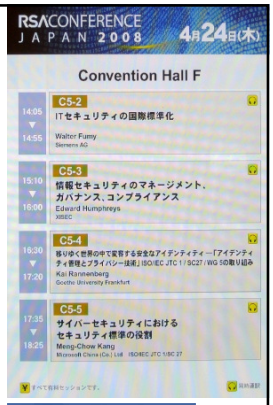
- Direct and indirect (via liaison)
- Applications of security techniques have broadened during the last years, and so have membership of SC 27 and its programme of work
- Challenges of growth
  - declining efficiency
  - increasing overhead
  - ⇨ *"… review all liaison relationships and provide a statistical report about the level of activity and communications during the past two years in order to identify liaisons that need appropriate action"*
    [2009 SC 27 Plenary, Beijing, Resolution 37].

Resources – *Delegates 2008 & 2009*

	Kyoto Japan *April 2008*	Limassol Cyprus *Oct 2008*	Beijing China *April 2009*	Redmond USA *Nov 2009*
Plenary	60		55	
WG 1	85	90	70	
WG 2	50	45	45	
WG 3	46	35	35	
WG 4	65	55	35	
WG 5	60	55	55	
WGs total	~ 180	~ 190	~ 170	~ 200e

Outreach

- Several press releases each year.
- SC 27 management and experts frequently present the work of SC 27 at conferences and workshops around the world. Examples include
  - RSA Conference Japan, Tokyo, 2008
  - Information Security Standardization International Forum, Beijing, 2009
- Since 2005, thirteen articles have been published in the ISO publications: ISO Focus, ISO Journal, and ISO Management Systems.
- SD 11 provides an accessible overview of the work of SC27.
  - Includes a number of SC 27 articles from ISO publications.
  - Freely available at http://www.jtc1sc27.din.de/sce/sd11



Challenges, Issues and Needs

- Challenges of growth
  - …
  - Educating new experts, editors, liaison organizations, …
  - Increasing demands for SC Management, Secretariat, meeting hosts
- Active vs. passive participation
  - Meeting the quorum requirements (a typical Plenary has 24 of 42 P-members present)
- Consistency across standards portfolio
  - Coordination, co-operation
  - Fighting the NIH* syndrome

*) not invented here

Next Work Period

- Again 10+ deliverables expected
- Next SC 27 meetings
  - Nov 2-6, 2009 — Redmond, USA (WGs)
  - Apr 19-27, 2010 — Melaka, Malaysia (WGs & Plenary)
  - **Oct 4-8, 2010** — **Berlin, Germany (WGs)**

TMB Privacy Steering Committee

TMB Resolution 146/2009

- Based on the final report and recommendations of the TMB Privacy Task Force, the Technical Management Board decided to create a Privacy Steering Committee (PSC) that shall report to the TMB with a view to:
  - implementing the three Privacy Task Force recommendations, and
  - assessing the feasibility of implementing the additional recommendations.
- The TMB assigned Secretariat of the Privacy Steering Committee to SC 27.
- Central Secretariat to issue to TMB members a call for the nomination of experts, PSC Secretariat to invite other committees and working groups within ISO that have worked on privacy-related standards to join the PSC.
- Privacy Steering Committee to provide the following to the TMB for approval at its June 2010 meeting:
  - an outline of its proposed workplan and related timeframes, and
  - a list of the members of the Privacy Steering Committee.

Privacy Task Force Recommendations

1. ISO should lead an effort to engage the broader standards community now working on privacy to intensify their interaction. An important first step could be the holding of a conference between all involved committees with the aim to prepare a **global inventory** of privacy-related standards work and develop some form of **overarching roadmap** which defines a strategic vision for the standards development work in this area.

2. Establish a **common terminology document** in the area of privacy and privacy principles.

3. Establish a **"live" inventory** (document and/or dedicated webpage) that would encourage sharing of information for ongoing privacy related work. Maintenance should be assigned to ISO or to a specific ISO TC (e.g., JTC1/SC 27/WG5).