Recent Developments in ISO/IEC Security Standardization

Dr. Walter Fumy

Chairman ISO/IEC JTC 1/SC 27
Chief Scientist, Bundesdruckerei GmbH, Germany

6th ETSI Security Workshop - Sophia Antipolis, January 2011
Agenda

- ISO/IEC JTC 1 – Information Technology
- JTC 1/SC 37 – Biometrics
- JTC 1/SC 17 – Cards and Personal Identification
- JTC 1/SC 27 – IT Security Techniques
  - Scope, organization, work programme
  - Recent achievements & new projects
- Conclusion
ISO/IEC JTC 1 – Information Technology

Mission & Principles

▶ JTC 1 develops, maintains, promotes and facilitates **IT standards** required by global markets meeting business and user requirements.

▶ Principles include

  ▪ business-like approach (i.e., cost effective, short development times, market-oriented results, …);
  ▪ ensuring that user needs including multicultural requirements, are fully met;
  ▪ actively promoting the use of JTC 1 products and services;
  ▪ recognizing the value of the work of other organizations and the contribution they make to international IT standardization, and complementing existing and forthcoming JTC 1 programs through other leading edge activities with the objective of providing the best standards worldwide.
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 38 Distributed application platforms and services (DAPS)
SC 37 – Biometrics

Scope

- Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems.
- Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.
- Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification.
- Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protections techniques, biometric security testing, evaluations, and evaluations methodologies.
SC 37 – Biometrics

Key Facts

- Working Groups
  - WG 1 Harmonized biometric vocabulary
  - WG 2 Biometric technical interfaces
  - WG 3 Biometric data interchange formats
  - WG 4 Biometric functional architecture and related profiles
  - WG 5 Biometric testing and reporting
  - WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics

- 28 participating countries
- 52 published standards

- Technology innovations and new customers’ needs are being addressed in a “second generation” of biometric standards such as the revision of the biometric data interchange formats, new biometric technical interface standards, performance (and conformance) testing methodology standards, and biometric sample quality standards.
SC 17 – Cards and Personal Identification

Key Facts

- Standardization in the area of:
  - Identification and related documents,
  - Cards and devices associated with their use in inter-industry applications and international interchange.

- Working Groups
  - WG 1 Physical characteristics and test methods for ID-cards
  - WG 3 Identification cards - Machine readable travel documents
  - WG 4 Integrated circuit cards with contacts
  - WG 5 Registration Management Group (RMG)
  - WG 8 Integrated circuit cards without contacts
  - WG 9 Optical memory cards and devices
  - WG 10 Motor vehicle driver license and related documents
  - WG 11 Application of biometrics to cards and personal identification

- 33 participating countries
- 84 published standards
Electronic Displays in IC Cards

New SC 17 Project

Use of security materials

Optical communication

Visible information

Personalized materials, exclusive material properties, unique spectrum of display materials

Tamperproof optical data transfer via display, dynamic security feature and watermarks

Password, PIN, address data, visa information, card and internet transaction status, 3D photo, video identification

Displays in IC cards provide security options at all levels
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.
## ISMS Family of Standards

### 27001 ISMS Requirements

<table>
<thead>
<tr>
<th>27000 ISMS Overview and Vocabulary</th>
<th>27006 Accreditation Requirements</th>
<th>27010 ISMS for Inter-sector communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>27002 (pka 17799) Code of Practice</td>
<td>27007 ISMS Auditing Guidance</td>
<td>27011 / ITU-T X.1051 Telecom Sector ISMS Requirements</td>
</tr>
<tr>
<td>27003 ISMS Implementation Guidance</td>
<td>TR 27008 ISMS Guide for auditors on ISMS controls</td>
<td>27015 Financial and Insurance Sector ISMS Requirements</td>
</tr>
<tr>
<td>27004 Information Security Mgt Measurements</td>
<td></td>
<td>TR 27016 Information Security Mgt - Organizational economics</td>
</tr>
<tr>
<td>27005 Information Security Risk Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Supporting Guidelines

<table>
<thead>
<tr>
<th>Accreditation Requirements and Auditing Guidelines</th>
<th>Sector Specific Requirements and Guidelines</th>
</tr>
</thead>
</table>

SC 27/WG 4
Security Controls and Services

- ICT Readiness for Business Continuity (WD 27031)
- Cybersecurity (WD 27032)
- Network Security (CD 27033-1, WD 27033-2/3/4)
  - Application Security (WD 27034-1)
  - Security Info-Objects for Access Control (TR 15816)
- Security of Outsourcing (NP)
- TTP Services Security (TR 14516; 15945)
  - Time Stamping Services (TR 29149)
- Information security incident management (27035)
- ICT Disaster Recovery Services (24762)
- Identification, collection and/or acquisition, and preservation of digital evidence (NP)

Unknown or emerging security issues

Known security issues

Security breaches and compromises
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, FCD/WD/WD)
  - Privacy framework (ISO/IEC 29100, FCD)
  - Privacy reference architecture (ISO/IEC 29101, CD)
  - Entity authentication assurance framework (ISO/IEC 29115 / ITU-T Xeaa, CD)
  - A framework for access management (ISO/IEC 29146, WD)

- **Protection Concepts**
  - Biometric information protection (ISO/IEC 24745, FDIS)
  - Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, CD)

- **Guidance on Context and Assessment**
  - Authentication context for biometrics (ISO/IEC 24761, 2009)
  - Privacy capability assessment framework (ISO/IEC 29190, WD)
Summary

between November 2009 and October 2010

▶ 11 International Standards and Technical Reports
   have been published (total number of publications: 98)

▶ 13 new projects have been approved
   (total number of projects: 160)

▶ 5 additional O-members (total 18)
   (total number of P-members: 41)

▶ 9 additional liaisons

5 liaisons terminated
   (total number of liaisons: 54)
Approved New Projects

- ISO/IEC 20004 – Software development and evaluation under ISO/IEC 15408
- ISO/IEC 20008 – Anonymous digital signatures (2 Parts)
- ISO/IEC 20009 – Anonymous entity authentication (2 Parts)
- ISO/IEC TR 27016 – Information security management – Organizational economics
- ISO/IEC 27038 – Specification for digital redaction
- ISO/IEC 30104 – Physical security attacks, mitigation techniques and security requirements
Platinum Book

available from
http://www.jtc1sc27.din.de/sbe/sc27berlin

Next SC 27 meetings
- Apr 11-19, 2011 Singapore (WGs and Plenary)
- Oct 10-14, 2011 Nairobi, Kenya (WGs)
- May 7-15, 2012 Sweden (WGs and Plenary)
Machine Readable Travel Documents

Major Contributions from JTC 1 Subcommittees

- ICAO TAG-MRTD

  - ISO/IEC JTC 1/SC 17
    Cards and Personal Identification
    - ISO/IEC 7816
    - ISO/IEC 10373
    - ISO/IEC 14443

  - ISO/IEC JTC 1/SC 27
    IT Security Techniques
    - ISO/IEC 9796-2
    - ISO/IEC 9797
    - ISO/IEC 11770-2

  - ISO/IEC JTC 1/SC 37
    Biometrics
    - ISO/IEC 19785
    - ISO/IEC 19794

Dr. Walter Fumy  I  6th ETSI Security Workshop, Sophia Antipolis, January 2011
Conclusion

- “The good thing about standards is ... there are so many to choose from”
- Well established security techniques available
- Trend from security as an add-on to integrated security solutions (“built in, not bolt on”)
- Security as a market differentiator
- New generation of cryptographic techniques, with lightweight cryptography still in its infancy
- Be aware of implementation level attacks, cryptography is typically bypassed, not penetrated
Thank You!

Walter.Fumy@bdr.de