ISO/IEC JTC 1
Information technology
Secretariat: ANSI (USA)

Document type: Business Plan

Title: SC 27 Business Plan October 2012 – September 2013

Status: This document is circulated to JTC 1 National Bodies for review and consideration at the November 2012 JTC 1 Plenary meeting in Jeju.

Date of document: 2012-10-16

Source: SC 27 Chairman and Secretariat

Expected action: ACT

Email of secretary: lrajchel@ansi.org

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1

ISO/IEC JTC 1/SC 27 N11599

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Business Plan

TITLE: SC 27 Business Plan October 2012 – September 2013

SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2012-10-10

PROJECT:

STATUS: for submission to JTC 1

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
H. Cuschieri, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
T. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 1 + 12

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787, [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-4-2652; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

Business Plan for JTC 1/SC 27 'IT Security Techniques'

Period covered: October 2012 – September 2013

Submitted by: Walter Fumy, SC 27 Chairman

1 Management Summary

1.1 Chairman's Remarks

This Business Plan has been prepared in accordance with Resolution 53 of the 24th SC 27 Plenary meeting in Stockholm, Sweden, 14th – 15th May 2012.

1.2 JTC 1/SC 27 Statement of 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 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

1.3 Project Report

1.3.1 Progress

The overall progress made over the past year again was excellent as shown by the number of documents that have been published (see section 2.2) and also by the target dates being kept in the majority of cases.

- total number of projects 176
- number of active projects 75
- number of publications: 114

SC 27 fully supports all its active projects. Details of the current status of all projects and their target dates can be found in SC 27 Standing Document SD 4, see also http://www.jtc1sc27.din.de/en .

1.3.2 New Projects and Study Periods

The following New Work Items for SC 27 have been approved over the past 12 months, all supported by substantial NB interest:

- ISO/IEC 18367: *Cryptographic algorithms and security mechanisms conformance testing*
- ISO/IEC 18370-1: *Blind digital signatures -- Part 1: General*
- ISO/IEC 18370-2: *Blind digital signatures -- Part 2: Discrete logarithm based mechanisms*
- ISO/IEC 27044: *Security information and event management (SIEM)*
- ISO/IEC 29003: *Identity proofing*
- ISO/IEC 29134: *Privacy impact assessment -- Methodology*
- ITU-T X.bhsm | ISO/IEC 17922: *Telebiometric authentication framework using biometric hardware security module*
- ISO/IEC 27018: *Code of practice for data protection controls for public cloud computing services*
- Revision of ISO/IEC 27033-1: *Network Security – Part 1: Overview and concepts*
- Revision of ISO/IEC 27035: *Information security incident management*
  – Part 1: Principles of incident management
  – Part 2: Guidelines for incident response readiness
  – Part 3: Guidelines for incident response operations
- ISO/IEC 27036-5: *Information security for supplier relationships -- Part 5: Guidelines for security of Cloud services*
- ISO/IEC 27041: *Information technology – Security techniques – Guidance on assuring suitability and adequacy of investigation methods*
- ISO/IEC 27042: *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*
- ISO/IEC 27043: *Information technology – Security techniques – Investigation principles and processes*

In addition, SC 27 has established Study Periods on the following topics:

- SC 27 study period on Cloud computing security and privacy
- SC 27 study period on Information security within Smart Grid environments
- Capability maturity framework for information security management (WG 1)
- Privacy / Personal Information Management Systems (PIMS) (WG 1/WG 5)
- Adjustment of ISO/IEC 27000 family of standards vocabulary to align with ISO/IEC 27002 revision process (WG 1)
- International certification of information security management specialists (WG 1)
- Criteria for the standardization of encryption algorithms(WG 2)
- Password-based anonymous entity authentication (WG 2)
- Lightweight hash-functions (WG 2)
- Key derivation mechanisms (WG 2)
- Security evaluation of anti-spoofing techniques for biometrics (WG 3/WG 5)
- Standards for privacy seal programs (WG 3/WG 5)
- Electronic discovery (WG 4)
- Cloud security technology standards (WG 4)
- Coordination of investigative projects (WG 4)
- Documentation of data deletion principles for personally identifiable information in organizations (WG 5)
- Privacy impact assessment (WG 5)

Furthermore, SC 27 has considered initiating activities in the following areas

- Activity monitoring

  Several SC 27 projects that may provide for the security needs of activity monitoring were identified. In addition, depending on the type of activity monitoring, there may be privacy concerns that may need to be addressed. In this regard, SC 27 will continue to monitor this development and initiate new work items as necessary.

- Context aware computing

  Context-aware computing was found to be not that different from general IT. This also holds for the privacy aspects of context-aware computing as these are not fundamentally different from IT security related issues of privacy in general. Consequently, context-aware computing was presumed not mature enough to justify a new technology area in standardization. However, any standardization work in the field of context-aware computing bearing relation to IT security and in particular to privacy related aspects should be considered within the scope of ISO/IEC JTC 1/SC 27.

- Green-by-ICT

  The list of prospective standardization topics in the area of Green–by-ICT addresses several areas of current and potentially future SC 27 projects, e.g., ISO/IEC 27010 (Information Security Management Guidelines for Inter-sector and Inter-organizational Communications), ISO/IEC 27033 (Network Security), and the Study Period on Security for Smart Grid. Any work in the field of Green-by-ICT standardization bearing relation to ICT security, and in particular security related aspects within JTC 1/WG 7 should be considered in liaison to and/or within the scope of ISO/IEC JTC 1/SC 27. SC 27 is open for discussion of any contributions.

- Smart Grid

In view of market demands, SC 27 has started work looking at Smart Grid Security.

1.4 Co-operation and Competition

SC 27 enjoys an extremely large number of fruitful and valuable liaisons with many organizations within ISO/IEC JTC 1 including WG 6, WG 7, SC 6, SC 7, SC 17, SC 25, SC 31, SC 36, SC 37 and SC 38, within ISO including TC 46, TC 68, TC 176, TC 215, TC 251, PC 259, TC 262, ISO/CASCO, TMB/JTCG MSS, TMB/SAG, within IEC including IEC/TC 57, IEC/TC 65, and to external organizations including ABC4Trust, ARTICLE 29 Data Protection Working Party, CCDB, CEN/TC 377, CEN/CENLEC/ETSI/SGCG Smart Grid Coordination Group, CSA, ECRYPT II, ENISA, EPC, ETSI, FIDIS, FIRST, ICDPPC, INLAC, INTERPOL, ISACA, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, PICOS, PrimeLife, TAS3, TCG and VISA.

Currently SC 27 maintains 25 internal and 29 external liaisons. A complete list is available at www.jtc1sc27.din.de/sbe/members .

Selected aspects related to these liaisons are highlighted below.

1.4.1 SC 37 'Biometrics'

Strong synergy exists between biometrics and IT security. The potential contribution of SC 27 to biometrics standards is evident. In particular, the areas of template protection techniques, algorithm security, and security evaluation are fields where SC 27 has the necessary experience to complement the mandate of SC 37. Therefore, SC 27 maintains close collaboration with SC 37 'Biometrics'.

1.4.2 TC 68/SC 2 'Financial Services - Security'

TC 68/SC 2 and SC 27 coordinate on IT security standards of mutual interest by sharing expertise and content, in order to avoid overlap in standards development. SC 27 is looking forward to further coordinate with the recently established new TC 68/SC 2 Management Team.

1.4.3 ITU-T Q3/SG17 and ITU-T FG Cloud Computing

ITU-T Q3/SG17 and SC 27 collaborate on several projects in order to progress common or twin text documents and to publish common standards. These projects include

- Recommendation ITU-T X.841 I ISO/IEC 15816: *Security information objects for access control*
- Recommendation ITU-T X.842 I ISO/IEC TR 14516: *Guidelines on the use and management of Trusted Third Party services*
- Recommendation ITU-T X.843 I ISO/IEC 15945: *Specification of TTP services to support the application of digital signatures*
- Recommendation ITU-T X.1051 I ISO/IEC 27011: *Information security management guidelines for telecommunications* Recommendation ITU-T X.1054 I ISO/IEC 27014: *Governance of information security*
- Recommendation ITU-T X.1254 I ISO/IEC 29115: *Entity authentication assurance*
- Draft Recommendation ITU-T X.bhsm I ISO/IEC 17922: *Telebiometric authentication framework using biometric hardware security module*

.

1.4.4 The Common Criteria Development Board (CCDB)

The CCDB and SC 27/WG 3 have had a long-standing technical liaison on projects related to IT Security Evaluation Criteria. Thus, Working Group 3 has been working in close co-operation with the CCDB on the development of the Common Criteria, which has been simultaneously published as ISO/IEC 15408. The co-operation has been extended to also involve the work on 18045 “Evaluation methodology for IT security”. This close cooperation allows NBs not represented in the CCDB to review, comment and contribute to the project. Both the ISO/IEC 15408 and ISO/IEC 18045 are currently fully aligned with their CCDB counterparts. Recently the WG has been contributing to the CCDB exploratory work on future development of Common Criteria.

A number of SC 27/WG 3 projects complement the application of ISO/IEC 15408, such as ISO/IEC TR 20004 *Refining Software Vulnerability Analysis under ISO/IEC 15408 and ISO/IEC 18045*, or ISO/IEC 17825 *Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules*. This extended coverage increases the collaboration with the CCDB.

1.4.5 The Trusted Computing Group (TCG)

ISO/IEC 11889: *Trusted Platform Module* is the main area of common interest, as the TCG with PAS submitter status, is interested in its further maintenance. The TCG has submitted their draft specifications of the TPM 2.0, and they have been subject to comment and discussion by SC 27/WG 3 NBs, experts and TCG liaison officers. In view of various aspects of this cooperation, SC 27 has requested its Chairman to communicate to the next JTC 1 Plenary meeting the need to further refine and improve the PAS maintenance process. Furthermore, ISO/IEC JTC 1/SC 27 requests JTC 1 to remove assignment of projects from the SC 27 Programme of Work, for which the maintenance remains with the PAS submitter.

2 Period Review

2.1 Market Requirements

Up until the 1970s, the use of security techniques to protect information and communications was largely restricted to some specific areas of application - such as the financial industry - and governments. With the advent of the Internet and the prospect of performing business on-line, IT security has been in the forefront of information and communications technology (ICT) have emerged high on the management agenda, have been the subject of new legislation and has made its way into many news headlines. E.g., organizations deploying (remote) electronic services (e.g., e-business, e-government) need to ensure control over who gets into applications and what users are allowed once they are in. User identification, authentication and authorization management technologies address these issues. Electronic signatures provide data integrity and non-repudiation and thus help to accelerate the growth in secure electronic business and subsequently to eliminate paper-based transactions.

At the same time, users need confidence in the effectiveness of the implemented security; an area where security evaluation and resulting assurance play an important part – here we have the Common Criteria (ISO/IEC 15408) for the security evaluation of products and systems and ISO/IEC 27001 for the third party certification of an organization’s information security management system (ISMS) – similar to the model for ISO 9001 (Quality), ISO 14001 (Environment) and ISO 22000 (Food safety management).

In addition, users ask more and more about protection of the privacy of their information and data. The relation between IT security and privacy is close, complex, and delicate. This can especially be seen in the area of Identity Management, e.g. relating to the issue, who controls and is entitled to use which very personal data about whom. SC 27 addresses the technological challenges resulting from this issue in its new Working Group 5 “Identity

Management and Privacy Technologies", e.g. by ISO/IEC 24760 "A Framework for Identity Management" and ISO/IEC 29100 "Privacy Framework".

Standardized security techniques are becoming mandatory requirements for e- and m-commerce, health-care, telecoms, automotive and many other application areas in both the commercial and government sectors. SC 27 addresses those market needs and provides a center of expertise for the standardization of security techniques.

The near future sees many market opportunities for SC 27 to expand the deployment of its standards as well as collaborating with other standards bodies on new projects and ideas. SC 27 as a centre of excellence on information security and IT security has always been at the forefront of security standardization. It has the right blend of skills and resources to deliver security standards to market requirements as borne out by its past track record. As applications of security technologies have broadened during the last years, so have both the membership of SC 27 and its programme of work.

A rapidly emerging and critical area of standardization to address corporate needs around the world is that of governance whether in the form of IT governance or information security governance (ISG). SC 27 is embarking on a programme of work into ISG in collaboration with other groups in JTC 1 dealing with other governance issues such as IT governance. Protecting corporate information assets cannot be solved by IT security solutions and technologies alone. Hence resolving strategic issues concerning the protection of corporate information assets and to support the organization's corporate governance relies on effective information security governance. ISO/IEC 27014 Governance of information security will define a framework, establish objectives, principles, and processes, and show how it can be used to evaluate, direct, and monitor an information security management system. SC 27 is also working closely with JTC 1/SC 7 in the development of ISO/IEC 30121, Governance of digital forensic risk framework.

Furthermore, the so-called "Internet of things" is gaining more and more attention. Technologies such as RFID pose new challenges with respect to security and privacy, and in view of specific constraints, require dedicated solutions, such as lightweight cryptographic techniques, authentication, etc.

For seamless security across devices and applications, ISO/IEC 11889 Trusted Platform Module has been specified and included into the SC 27 work programme.

More and more, organizations are recognizing the importance of addressing security within systems and software engineering processes, as well as within the supply chain.

Apart from the need for guidelines and standards enabling or contributing to the implementation and assurance of security, a need exists for guidelines and standards addressing incident management, specific activities in handling potential digital evidence, and common investigation processes across various investigation scenarios.

2.2 Achievements

2.2.1 Publications

Since October 2011, the following International Standards and Technical Reports have been published:

- ISO/IEC 9797-3: *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-function*

  Publication date: 2011-11-15 – 25 pages

ISO/IEC 9797-3:2011 specifies Message Authentication Code (MAC) algorithms that use a secret key and a universal hash-function with an n-bit result to calculate an m-bit MAC based on the block ciphers specified in ISO/IEC 18033-3 and the stream ciphers specified in ISO/IEC 18033-4.

- ISO/IEC 11770-5: *Information technology -- Security techniques -- Key management -- Part 5: Group key management*

  Publication date: 2011-12-15 – 22 pages

  ISO/IEC 11770-5:2011 specifies key establishment mechanisms for multiple entities to provide procedures for handling cryptographic keying material used in symmetric or asymmetric cryptographic algorithms according to the security policy in force. It defines the symmetric key based key establishment mechanisms for multiple entities with a key distribution center (KDC), and defines symmetric key establishment mechanisms based on general tree based structure with both individual rekeying and batched rekeying. It also defines key establishment mechanisms based on key chain with both unlimited forward key chain and limited forward key chain.

- ISO/IEC 18031: Information technology -- Security techniques -- Random bit generation

  Publication date: 2011-11-15 – 142 pages

  ISO/IEC 18031:2011 specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model and establishes the security requirements for both non-deterministic and deterministic random bit generators. Techniques for statistical testing of random bit generators for the purposes of independent verification or validation, and detailed designs for such generators, are outside the scope of ISO/IEC 18031

- ISO/IEC 18033-4: Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers

  Publication date: 2011-12-15 – 92 pages

  ISO/IEC 18033-4 specifies stream cipher algorithms. It describes five dedicated keystream generators and two output functions to combine a keystream with plaintext.

- ISO/IEC 19790: *Information technology — Security techniques — Security requirements for cryptographic modules (2nd ed)*

  Publication date: 2012-08-15 – 71 pages

  ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module protecting sensitive information in computer and telecommunication systems. The standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location).

- ISO/IEC TR 20004: Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

  Publication date: 2012-08-15 – 17 pages

  ISO/IEC TR 20004:2012 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045:2008 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation. The Technical Report leverages the Common Weakness Enumeration (CWE) and the Common Attack Pattern Enumeration and Classification (CAPEC) to support the method of scoping and implementing ISO/IEC 18045:2008(E) vulnerability analysis activities. It does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

- ISO/IEC 24760-1: *A framework for identity management – Part 1: Terminology and concepts*

  Publication date: 2012-12-15 – 20 pages

  ISO/IEC 24760-1:2011 defines terms for identity management, and specifies core concepts of identity and identity management and their relationships. The standard is applicable to any information system that processes identity information. A bibliography of documents describing various aspects of identity information management is provided.

- ISO/IEC 27006: *Requirements for bodies providing audit and certification of information security management systems* (2nd edition)

  Publication date: 2011-11-15 – 37 pages

  ISO/IEC 27006:2011 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in this standard need to be demonstrated in terms of competence and reliability by anybody providing ISMS certification, and the guidance contained in ISO/IEC 27006:2011 provides additional interpretation of these requirements for anybody providing ISMS certification.

- ISO/IEC 27007: *Guidelines for information security management systems guidelines auditing*

  Publication date: 2011-11-15 – 27 pages

  ISO/IEC 27007:2011 provides guidance on managing an information security management system (ISMS) audit programme, on conducting the audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. The standard is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

- ISO/IEC TR 27008: *Guidelines for auditors on information security controls*.

  Publication date: 2011-10-15 – 36 pages

  ISO/IEC TR 27008:2011 provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organization's established information security standards. The standard is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations conducting information security reviews and technical compliance checks. It is not intended for management systems audits.

- ISO/IEC 27010: *Information security management for inter-sector and inter-organisational communications*

  Publication date: 2012-04-01 – 34 pages

  ISO/IEC 27010:2012 provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. The standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications. ISO/IEC 27010:2012 is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organization's or nation state's critical infrastructure.

- ISO/IEC 27013: *Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

Publication date: 2012-10-15 – 38 pages

- ISO/IEC 27032: *Guidelines for cybersecurity*

  Publication date: 2012-07-15 – 50 pages

  ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular information security, network security, internet security, and critical information infrastructure protection (CIIP). The standard covers the baseline security practices for stakeholders in the Cyberspace and provides an overview of Cybersecurity, an explanation of the relationship between Cybersecurity and other types of security, a definition of stakeholders and a description of their roles in Cybersecurity, guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

- ISO/IEC 27033-2: *Network security — Part 2: Guidelines for the design and implementation of network security*

  Publication date: 2012-08-01 – 21 pages

  ISO/IEC 27033-2:2012 gives guidelines for organizations to plan, design, implement and document network security. This standard cancels and replaces ISO/IEC 18028-2:2006.

- ISO/IEC 27034-1: *Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts*

  Publication date: 2011-11-15 – 67 pages

  ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications. The standard presents an overview of application security, and introduces definitions, concepts, principles and processes involved in application security. ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.

- ISO/IEC 27037: *Guidelines for identification, collection, acquisition and preservation of digital evidence*

  Publication date: 2012-10-15 – 38 pages

- ISO/IEC 29100: Privacy framework

  Publication date: 2011-12-15 – 21 pages

  ISO/IEC 29100:2011 provides a privacy framework which specifies a common privacy terminology, defines the actors and their roles in processing personally identifiable information (PII), describes privacy safeguarding considerations, and provides references to known privacy principles for information technology. ISO/IEC 29100 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

- ISO/IEC 29128: *Information technology -- Security techniques -- Verification of cryptographic protocols*

  Publication date: 2011-12-07 – 50 pages

  ISO/IEC 29128:2011 establishes a technical base for the security proof of the specification of cryptographic protocols. It specifies design evaluation criteria for these protocols, as well as methods to be applied in a verification process for such protocols. It also provides definitions of different protocol assurance levels consistent with evaluation assurance components in ISO/IEC 15408.

- ISO/IEC TR 29149: *Best practices for the provision and use of time-stamping services*

  Publication date: 2012-03-15 – 21 pages

  ISO/IEC TR 29149:2012 explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness, data integrity, and non-repudiation services in conjunction with other mechanisms. It defines how time-stamp requesters should use time-stamp token generation services, how TSAs (time-stamping authorities) should provide a service of guaranteed quality, and how TSAs should deserve trust based on good practices.

- ISO/IEC 29150: Information technology -- Security techniques -- Signcryption

  Publication date: 2011-12-15 – 53 pages

  ISO/IEC 29150:2011 specifies four mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to have their own public and private key pairs. The methods specified have been designed to maximize the level of security and provide efficient processing of data. All the mechanisms defined have mathematical "proofs of security", i.e. rigorous arguments supporting their security claims.

- ISO/IEC 29192-1: *Lightweight cryptography -- Part 1: General*

  Publication date: 2012-06-01 – 13 pages

  ISO/IEC 29192-1:2012 provides terms and definitions that apply in subsequent parts of ISO/IEC 29192. The standard sets the security requirements, classification requirements and implementation requirements for mechanisms that are proposed for inclusion in subsequent parts of ISO/IEC 29192.

- ISO/IEC 29192-2: *Lightweight cryptography -- Part 2: Block ciphers*

  Publication date: 2012-01-15 – 41 pages

  ISO/IEC 29192-2:2012 specifies two block ciphers suitable for lightweight cryptography. PRESENT which is a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits, and CLEFIA, which is a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits.

- ISO/IEC 29192-3 *Lightweight cryptography -- Part 3: Stream ciphers*

  Publication date: 2012-10-01 – 28 pages

In addition, a substantial number of Amendments and Technical Corrigenda have been published over the past 12 months.

2.2.2 Documents awaiting Publication

The following International Standards or Technical Reports developed by SC 27 have been finalized and are awaiting publication:

- ISO/IEC DTR 15443-1: *Security assurance framework -- Part 1: Introduction and concepts* (2nd ed)
- ISO/IEC DTR 15443-2: Security assurance framework -- *Part 2: Analysis* (2nd ed)
- ISO/IEC DIS 27000: *Information security management systems – Overview and vocabulary*
- ITU-T X.1054 | ISO/IEC FDIS 27014: *Governance of information security*
- ITU-T X.1254 | ISO/IEC FDIS 29115: *Entity authentication assurance framework*

- ISO/IEC DIS 29147: *Vulnerability disclosure*
- ISO/IEC DIS 29191: *Requirements for partially anonymous, partially unlinkable authentication*
- ISO/IEC FDIS 29192-4 *Lightweight cryptography -- Part 3: Mechanisms using asymmetric techniques*

2.3 Resources

The last SC 27 Plenary meeting took place May 14-15, 2012 in Stockholm, Sweden and was attended by 65 delegates from 27 of the current 49 P-members.

The five SC 27 Working Groups held meetings May 7-11, 2011 in Stockholm, Sweden and October 10–14, 2011 in Nairobi, Kenya. In average, these WG meetings were attended by more than 270 delegates in total with many delegates attending several Working Groups.

The next Working Group meetings are scheduled for October 22-26, 2012 in Rome, Italy and for April 22-26, 2013 in Sophia Antipolis, France. The next SC 27 Plenary meeting is planned to take place April 29-30, 2013 in Sophia Antipolis, France.

Overall, the resources and expertise prove to be sufficient to meet the many challenges SC 27 is facing. For selected projects, SC 27 resources are complemented by resources from appropriate SC 27 liaison organizations.

The 6-month meeting cycle of SC 27 is a good end efficient tradition, as it allows holding meetings at about the same time every year and does not charge too much on delegates' budgets.

In order to further improve the efficiency of SC 27 and its WGs, to increase the quality of deliverables, to define the right balance between WG autonomy and coordination at SC 27 level, and to make optimal use of the relevant ISO processes and tools available, SC 27 resolved to establish an ad hoc group on SC 27 "modus operandi" under the lead of the SC 27 Vice-Chair.

3 Focus Next Work Period

3.1 Deliverables

Deliverables expected from the next work period (October 2012 - September 2013) include

- ISO/IEC 11770-3: *Key management -- Part 3: Mechanisms using asymmetric techniques* (3rd ed)
- ISO/IEC DTR 15443-1: *Security assurance framework -- Part 1: Introduction and concepts* (2nd ed)
- ISO/IEC DTR 15443-2: Security assurance framework -- *Part 2: Analysis* (2nd ed)
- ISO/IEC 27000: *Information security management systems – Overview and vocabulary*
- ISO/IEC TR 27016: *Information security management -- Organizational economics*
- ISO/IEC TS 27018: *Physical security attacks , mitigation techniques and security requirements*
- ITU-T X.1054 | ISO/IEC 27014: *Governance of information security*
- ITU-T X.1254 | ISO/IEC 29115: *Entity authentication assurance framework*

- ISO/IEC 29147: *Vulnerability disclosure*
- ISO/IEC 29101: *Privacy architecture framework*
- ISO/IEC 29191: *Requirements for partially anonymous, partially unlinkable authentication*
- ISO/IEC 29192-4 *Lightweight cryptography -- Part 3: Mechanisms using asymmetric techniques*
- ISO/IEC TR 29193: *Secure system engineering principles and techniques*
- ISO/IEC TS 30104: *Physical security attacks , mitigation techniques and security requirements*
- ISO/IEC 30111: *Vulnerability handling processes*

3.2 Strategies

SC 27's Area of Work is the standardization of generic methods and techniques for IT security. Among its 'users' are other standardization groups that adopt these where appropriate, in whole or in part, and provide detailed, sector-specific guidance for selected options. An important means to ensure the timely development of market-oriented methods and techniques for IT security is the cooperation with such users, such as SC 7, SC 37, TC 68/SC 2 and ITU-T.

3.2.1 Challenges

The time needed to develop market driven standards is not always consistent with the market requirements and timeframe for these standards. Ways and means to continually improve the timely development and delivery of standards while guaranteeing the adequate quality are reviewed on a regular basis.

For some specific standards, such as cryptographic algorithms, cryptographic parameter generation, etc., internal SC 27 resources are not sufficient to conduct appropriate security evaluation and to ensure the desired quality. In these cases, SC 27 needs to ensure to establish the necessary cooperation with external initiatives in this area, such as ECRYPT II.

3.2.2 Opportunities

Standardized security techniques are becoming mandatory requirements for e- and m-commerce, e-government, health-care, and many other application areas. The use of security techniques and in particular of identification, authentication and electronic signatures constitutes a core element in e-business, e-government and other on-line activities. Over the last years, SC 27's work programme has included the basic techniques required for these activities. The existing portfolio of SC 27 work items and standards can be used to define a security framework, e.g., for governance, the telecom sector, healthcare sector or for the financial sector.

Growing awareness, concerns and opportunities with regard to privacy in society offer another area of opportunity for SC 27.

3.2.3 Marketing Initiatives and Joint Standardization Events

SC 27 has established the position of a PR officer and produces and distributes a number of press releases each year. These aim at promoting the standards that SC 27 develops and publishes. The press releases are targeted at users, implementers and management in industry and commerce. The distribution channels include international user groups and associations interested in security standards, security journals, publications and news

letters, the SC 27 Web site as well standards development bodies (within ISO/IEC, ITU-T, CEN, ETSI and other bodies such as IETF and IEEE).

SC 27 has continued to promote its standards work to the wider user community through articles and press releases in conjunction with the ISO publishing. Experts working in all SC 27 have been contributing papers, presentations and talks in many conferences, seminars and workshops at events around the world.

SC 27/SD11 provides a very accessible overview of the work of SC 27. This includes a number of the SC 27 articles that have been published by ISO in the publications ISO Focus, ISO Journal and ISO Management System. SD11 is freely available to everyone and is downloadable via the SC 27 Web site http://www.jtc1sc27.din.de/en

On the occasion of its 20th birthday, the "SC 27 Platinum Book – Twenty Years of ISO/IEC JTC 1/SC 27 Information Security Standardization" has been produced. Included in this book are many articles written by experts working in SC 27 as well as by current and past officers of SC 27. The book further contains statements by SC 27 liaison organizations as well as by some National Bodies. An electronic version is available from the SC 27 Web Site.

In July of this year SC 27 contributed to the planned JTC 1 'glossy' publication. The title of the SC 27 article for this JTC 1 publication is "SC 27 - International Centre of Expertise on Information Security".

SC 27 has also been invited to take part and give a presentation at the joint Chinese/US symposium on Cyber-Security in October 2011.

Tutorial and press material on SC 27, its projects, and its standardization roadmaps are available from http://www.jtc1sc27.din.de/en

3.3 Work Programme Priorities

Priority tasks for Working Group 1 include keeping the WG 1 Roadmap up-to-date, and to ensure effective and timely progression of:

- Revisions of ISO/IEC 27000 *Information security management systems - Overview and vocabulary*, ISO/IEC 27001 *Information security management systems - Requirements*, ISO/IEC 27002 *Code of practice for information security management*, ISO/IEC 27004 *Information security management measurements*, ISO/IEC 27006 *International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems* (in alignment with the systematic revision of ISOIEC 17021).
- Development of ISO/IEC 27016 *Information security management - Organizational economics* and ISO/IEC 27017 *Cloud computing security and privacy -- Security controls*
- Recently started work looking at Smart Grid Security and the Certification of Security Personal (in keeping with accreditation standard ISO 17024).

In addition, WG 1's role in the cooperation with ITU-T is of strategic importance with regard to the ISO/IEC 27000 ISMS family of standards, and more recently in regard to the soon to be published ITU-T and SC27 joint standard on information security governance.

For Working Group 2, priorities for the next work period include the successful completion of the WG 2 projects mentioned in section 3.1, as well as the development of standards by recently established project:

- ISO/IEC 29192-4 *Lightweight cryptography*
  - Part 4: Mechanisms using asymmetric techniques

WG 2 has also started working in the standardization of cryptographic mechanisms in support of WG 5's work in the area of anonymity and other aspects of privacy which are:

- ISO/IEC 18370 *Blind digital signatures*
  - Part 1: General
  - Part 2: Discrete logarithm based mechanisms.

In addition, WG 2's roles in the cooperation with TC 68 Banking and Related Financial Services are of strategic importance.

Priority for Working Group 3 is to ensure that the main security evaluation and testing standards progress and are complemented with appropriate guidance and technical reports on specific fields of application. In addition, with the recently approved update of the WG 3 terms of reference, a more clear position has been drawn in respect to the security functional and assurance specification of specific devices, like cryptographic modules or trusted platform modules, where WG 3 is working to produce an useful and coherent set of standards, both for the specification of such devices, and also for their conformance testing. While progressing in methods to evaluate and improve assurance of these foundation product types and mechanisms, WG 3 is now looking forward to developing standards in the area of the evaluation of systems, of increasing demand and in immediate need for assurance. Beyond the development of the already identified projects and roadmap, there are different sectorial and national initiatives to develop specific standards that are mostly based or derived on WG3 projects. An effort will be made to improve coordination with these initiatives to avoid a proliferation of similar standards.

Priorities for Working Group 4 for the next work period include the successful completion of the WG 4 projects listed in section 3.1, and to ensure that work on the following projects progresses to as planned:

- ISO/IEC 24762, *Guidelines for information and communications technology disaster recovery services*
- ISO/IEC 27033, *Network security, Parts 1, 4, 5 and 6;*
- ISO/IEC 27034, *Application security Parts 2, 5 and 6;*
- ISO/IEC 27035 *(all parts), Information security incident management;*
- ISO/IEC 27036 *(all parts), Information security for supplier relationships;*
- ISO/IEC 27038, *Specification for digital redaction;*
- ISO/IEC 27039, *Selection, deployment and operations of intrusion detection and prevention systems (IDPS);*
- ISO/IEC 27040, *Storage security;*
- ISO/IEC 27041, *Guidance on assuring suitability and adequacy of investigation methods;*
- ISO/IEC 27042, *Guidelines for the analysis and interpretation of digital evidence;*
- ISO/IEC 27043, *Investigation principles and processes;*
- ISO/IEC 27044, *Security information and event management;* and
- ISO/IEC 30121, *Governance of digital forensic risk framework.*

Priorities for Working Group 5 are to finalize foundational frameworks and architectures (projects ISO/IEC 24760 *A framework for identity management,* and ISO/IEC *29101 Privacy architecture*), as well as a joint project with ITU-T: X.1524 I ISO/IEC 29115 *Entity authentication assurance framework* and to develop standards according to its standards

development roadmap, that is being used to identify, promote, and prioritize future work on supporting technologies, models, and methodologies. Examples are ISO/IEC 29191 *Requirements for partially anonymous, partially unlinkable authentication*, ISO/IEC 29146 *A framework for access management,* and ISO/IEC 29190 *Privacy capability assessment model.* Additionally, Working Group 5 has started new projects in the area of Telebiometric authentication (ITU-T X.bhsm | ISO/IEC 17922), Cloud Computing (ISO/IEC 27018), Privacy Impact Assessment (ISO/IEC 29134), and Identity Proofing (ISO/IEC 29003). Moreover, there are Study Periods on Privacy Impact Assessment, Privacy / Personal Information Management Systems, security evaluation of anti-spoofing techniques for biometrics, Privacy Seal programs, and the documentation of data deletion principles for personally identifiable information in organisations. These projects and initiatives are also addressing the recommendations from the ISO/TMB Privacy Steering Committee.