ISO/IEC JTC 1/SC 27 **N 13041**

ISO/IEC JTC 1/SC 27/WG 3 **N 1045**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Resolutions

TITLE: **Resolutions of the 47th SC 27 WG 3 meeting held in Incheon, Republic of Korea, October 21st-25th 2013**

SOURCE: 47th SC 27 WG 3 meeting

DATE: 2013-10-25

PROJECT:

STATUS: This document is being circulated for action.
This document was available at the above-mentioned meeting.

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
E. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1SC 27

NO. OF PAGES: 1+14

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

ISO/IEC JTC 1/SC 27/WG 3 Resolutions

47th Meeting in Incheon, Republic of Korea

October 21st-25th 2013

All resolutions are approved UNANIMOUSLY unless otherwise noted.

Resolution 1: Acceptance of minutes

ISO/IEC JTC 1/SC 27/WG 3 resolves to accept the minutes of ISO/IEC JTC 1/SC 27/WG 3 of the 46th meeting in Sophia Antipolis, France, April 22nd-26th 2013, in document N12497.

Resolution 2: Appointment of the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 resolves to appoint Helmut Kurth and Naruki Kai as drafting committee of the meeting, and instructs them to prepare the draft resolutions document for WG 3, to be recorded in N13041.

Resolution 3: Appointment of Acting Editor

ISO/IEC JTC 1/SC 27/WG 3 appoints the following acting editor through the end of the meeting:

Editor	Project	Title
Katie Moussouris	1.27.96 (30127)	Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis

Resolution 4: Appointment of Acting Liaison Officers

ISO/IEC JTC 1/SC 27/WG 3 appoints the following acting liaison officers through the end of the meeting:

Liaison Officer	Liaison Institution
Christian Noetzel	to SC 37
Jan-Bernhard de Meer	to ETSI TC MTS
Shin'ichiro Matsuo	to ITU-T SG 17
Naruki Kai	to SC 7

Resolution 5: Appointment of Acting Rapporteurs

ISO/IEC JTC 1/SC 27/WG 3 appoints the following acting rapporteurs through the end of the meeting:

Rapporteur	SP
Fiona Pattinson	Study Period on High-assurance evaluation under ISO/IEC 15408/18045

Rapporteur	SP
Christian Noetzel	Joint ISO/IEC JTC 1/SC 27/WG 3 and ISO/IEC JTC 1/SC 27/WG 5 Study Period on Security evaluation of anti-spoofing techniques for biometrics

Resolution 6: Appointment of Editors

ISO/IEC JTC 1/SC 27/WG 3 appoints the following editors:

Editor	Project	Title
Helmut Kurth	1.27.108 (19249)	Catalogue of architectural and design principles for secure products, systems, and applications
Julio González * Naruki Kai #	1.27.41 (19791)	Information technology – Security techniques -- Security assessment of operational systems
Katie Moussouris * Heiko Rudolph #	1.27.75.02 (20004-2)	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 – Part 2: CWE and CAPEC based software penetration testing**

* project editor # co-editor ** subject to approval of resolution P4

Resolution 7: Establishment of WG 3 Study Period

ISO/IEC JTC 1/SC 27/WG 3 requests its Secretariat to take appropriate action for the establishment of the Study Period below, and to appoint the indicated rapporteur:

Document	Study Period	Rapporteur
SC 27 N13022	Competence requirements for security evaluators, testers, and validators	Fiona Pattinson
SC 27 N13403	Operational test guideline of cryptographic module in environment	Hee Bong Choi

Resolution 8: Extension of WG 3 Study Periods

ISO/IEC JTC 1/SC 27/WG 3 requests its Secretariat to take appropriate action for the extension of the Study Periods listed below for another six month period.

Document	Study Period	Rapporteur
SC 27 N11281	Joint ISO/IEC JTC 1/SC 27/WG 3 and ISO/IEC JTC 1/SC 27/WG 5 Study Period on security evaluation of anti spoofing techniques for biometrics	Ludovic Merrien Nils Tekampe
SC 27 N12483	Study Period on High-assurance evaluation under ISO/IEC 15408/18045	Rance DeLong

Resolution 9: Appointment of Rapporteurs

ISO/IEC JTC 1/SC 27/WG 3 appoints the following rapporteurs:

Rapporteur	Title
Fiona Pattinson	Competence requirements for security evaluators, testers, and validators
Philip Statham (*)	Joint ISO/IEC JTC 1/SC 27/WG 3 and ISO/IEC JTC 1/SC 27/WG 5 Study Period on security evaluation of anti spoofing techniques for biometrics
Hee Bong Choi	Operational test guideline of cryptographic module in environment

* co-rapporteur

Resolution 10: Updating of documents

ISO/IEC JTC 1/SC 27/WG 3 requests the Project Editors / Co-Editors / Rapporteurs of the projects identified below to update the following drafts and produce Dispositions of Comments in accordance with the instructions decided at the Working Group/editing meetings, and to send these documents to the WG 3 Secretariat/Vice-Convenor by the due dates.

Document	Project No.	Title	To be sent to/by	DoC Doc. No.
SC 27 N13044	1.27.95 (17825)	Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules	WG 3 Secr/ 2013-12-15	SC 27 N13033
SC 27 N13045	1.27.101 (18367)	Cryptographic algorithms and security mechanisms conformance testing	WG 3 Secr/ 2013-12-15	SC 27 N13034
SC 27 N13046	1.27. 75.01 (20004-1)	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045 - Part 1: Using publicly available information security resources **	WG 3 Secr/ 2013-12-15	SC 27 N 13035
SC 27 N13051	1.27. 75.02 (20004-2)	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045 - Part 2: CWE and CAPEC based software penetration testing**	WG 3 Secr/ 2013-12-15	SC 27 N13036
SC 27 N13048	1.27.51 (24759)	Test Requirements for Cryptographic Modules	WG 3 Secr/ 2013-12-15	SC 27 N13047
SC 27 N13050	1.27.87 (30104)	Physical Security Attacks, Mitigation Techniques and Security Requirements	WG 3 Secr/ 2013-12-15	SC 27 N12490

** subject to approval of resolution P4

Resolution 11: Preparation of Document

ISO/IEC JTC 1/SC 27/WG 3 requests the editors of the projects listed below to prepare 1st WD for the projects identified.

Document	Project	Title	Due date
SC 27 N13052	1.27.108 (19249)	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications	2013-12-15
SC 27 N13053	1.27.41 (19791)	Information technology – Security techniques -- Security assessment of operational systems	2013-12-15

Resolution 12: Documents for Study and Comment

ISO/IEC JTC 1/SC 27/WG 3 requests its Secretariat to circulate the following documents to National Bodies for study and comment:

Document	Project	Title	Comments Due date
SC 27 N13045	1.27.101 (18367)	Cryptographic algorithms and security mechanisms conformance testing	2014-03-15
SC 27 N13052	1.27. 108 (19249)	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications	2014-03-15
SC 27 N13053	1.27.41 (19791)	Information technology – Security techniques -- Security assessment of operational systems	2014-03-15
SC 27 N13046	1.27. 75.01 (20004-1)	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045 - Part 1: Using publicly available information security resources *	2014-03-15
SC 27 N13051	1.27. 75.02 (20004-2)	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045 - Part 2: CWE and CAPEC based software penetration testing *	2014-03-15
SC 27 N13050	1.27.87 (30104)	Physical Security Attacks, Mitigation Techniques and Security Requirements	2014-03-15

* Subject to approval of resolution P4

Resolution 13: Liaison Statements

ISO/IEC JTC 1/SC 27/WG 3 approves the following liaison statements and requests the SC 27 Secretariat to send these liaison statements to the committees/institutions concerned.

WG	Document	To	Topic	Reference
3	SC 27 N13021	CCDB	15408, 18045, 20004, 30104, 30111, 30127	N13020
3	SC 27 N13043	ETSI TC MTS	15408, 20004	N12821, N13072
3	SC 27 N13031	SC 7	15026, 29119	N12930

Resolution 14: Text for liaison statement to ISO/IEC JTC 1/SC 37 to be sent by ISO/IEC JTC 1/SC 27/WG 5:

ISO/IEC JTC 1/SC 27/WG 3 provides input of the following text to WG 5:

"**Security evaluation testing and specification**

ISO/IEC JTC 1/SC 27/WG 3 would further like to thank SC 37 for the report provided and would specifically would like to inform ISO/IEC JTC 1/SC 37 about the current activities of interest:

Study Period on Anti-Spoofing

The future of this study period has been discussed and the input of ISO/IEC JTC 1/SC 37 to avoid overlapping activities has been taken into account. However - as this is a topic of broad relevance – it has been decided to extend the study period, nevertheless. The current feedback (including the ISO/IEC JTC 1/SC 37 feedback) will be circulated among the NBs of ISO/IEC JTC 1/SC 27. Philip Statham from the UK NB volunteered to support Nils Tekampe and Ludovic Merrien as a co-rapporteur for this study period.

WD 30107

ISO/IEC 30107 is a project of great interest for ISO/IEC JTC 1/SC 27, as it contains various aspects falling into the core responsibility of ISO/IEC JTC 1/SC 27. It would therefore propose a deeper cooperation regarding this project, such as a more direct communication between interested experts, potentially also apart from the meeting schedule of both SCs. This would be the basis for a better understanding of each others' positions and be a fruitful basis for comments to generated by

SC 27 for this standard, which could also improve the further development of the standard. It could e.g. be organized in form of regular telephone-conferences or web-meetings, that take place in between SC37 and SC27 meetings.

Template protection

ISO/IEC JTC 1/SC 27 would like to invite the editors of the new standard on performance testing for biometric template protection schemes to a close liaison interaction with ISO/IEC JTC 1/SC 27. As outlined in the call for contributions to this standard the editors are planning to include aspects of security and privacy into this standard. Based on this information and based on the fact that the underlying standard ISO/IEC 24745 has been developed in ISO/IEC JTC 1/SC 27 a cooperation between both SCs should be beneficial for the development of this standard.

ISO/IEC JTC 1/SC 27 would like to suggest that the editors of the standard consider the relevant standards of ISO/IEC JTC 1/SC 27 WG 3 and WG 5 when in the context of security and privacy.

Specifically ISO/IEC 15408 (Common Criteria) and its concept of Protection Profiles may be a valuable starting point for considerations around the security of template protection schemes."

Resolution 15: Text for liaison statement to IEC/TC65/WG10 to be sent by ISO/IEC JTC 1/SC 27/WG 1

ISO/IEC JTC 1/SC 27/WG 3 provides input of the following text to WG 1:

"**Security evaluation testing and specification**

ISO/IEC JTC 1/SC 27/WG 3 thanks IEC TC 65/WG 10 for its recent Liaison Statement, distributed as SC 27 document N13102, and for the Disposition of Comments on 1st CD IEC 62443-2-4, 65/523B/CD, distributed as SC 27 document N12748.

SC 27/WG 3 notes that a CDV ballot for IEC 62443-2-4 is scheduled for December 2013, and requests that the balloted text is sent to the SC 27 Secretariat at that time for distribution to WG 3 for liaison comments.

There are no specific SC 27/WG 3 Projects that WG 3 wishes to bring to the attention of IEC TC 65/WG 10 at this time."

Resolution 16: Text for liaison statement to ISA 99 to be sent by ISO/IEC JTC 1/SC 27/WG 1

ISO/IEC JTC 1/SC 27/WG 3 provides input of the following text to WG 1:

"**Security evaluation testing and specification**

ISO/IEC JTC 1/SC 27/WG 3 thanks ISA 99 for its recent Liaison Statement, distributed as SC 27 document N13191.

ISO/IEC JTC 1/SC 27/WG 3 would like to retain its liaison relationship with ISA 99. SC 27/WG 3 volunteers to distribute new drafts of any parts of ISA 62443 that are related to information security test and evaluation to its members for review and comment.

There are no specific SC 27/WG 3 Projects that WG 3 wishes to bring to the attention of ISA 99 at this time."

Resolution 17: Text for liaison statement to the Open Group to be sent by ISO/IEC JTC 1/SC 27/WG 4

ISO/IEC JTC 1/SC 27/WG 3 provides input of the following text to WG 4:

"**Security evaluation testing and specification**

ISO/IEC JTC 1/SC 27/WG 3 thank The Open Group for the updates of the dates and location of its forthcoming meeting schedule. This is noted and WG 3 request that The Open Group continue to include information about their future meetings in their future liaison statements.

WG 3 thank The Open Group for updating WG 3 on the activities of The Open Group Trusted Technology Forum (OTTF)™, and the Real Time Embedded Systems Forum.

WG 3 look forward to a rewarding relationship with The Open Group and encourage the Open Group to provide any Open Group work items that WG 3 may consider for review or comment as attachments to the next liaison statement.

The Open Group Trusted Technology Forum (OTTF)™
ISO/IEC JTC 1/SC 27/WG 3 thanks The Open Group for the updates on progress with the O-TTPS and the associated accreditation program.

WG 3 note that The OTTF is working with various groups to harmonize their work including considering whether to put the standard forward as a PAS Submission in the area of secure methodologies for technology development including supply chain security. WG 3 notes that there are several mechanisms, other than the PAS process, for progressing such contributions. If The Open Group decide to move forward with such a work item, WG 3 suggests that The Open Group work with JTC 1 to determine the most expedient mechanism for achieving its goals in collaboration with WG 3.

The Open Group Real Time Embedded Systems Forum
ISO/IEC JTC 1/SC 27/WG 3 would like to bring to the attention of The Open Group the ongoing WG 3 Study Period for High Assurance under ISO/IEC 15408 and ISO/IEC 18045.

The report on the Study period, prepared by the rapporteur and presented at the Songdo meeting, is attached. WG 3 brings to the attention of The Open Group that this study period has been extended by a further 6 months. WG 3 invites The Open Group to submit its contributions to the Study Period, as an attachment to the next liaison statement to WG 3, so that they may be circulated appropriately for review by ISO/IEC JTC 1/SC 27 and the rapporteur before the next meeting.

Please note that the latest status of WG 3 projects, relevant document numbers and the schedule for updates and comments are all to be found in the WG 3 resolutions document that is attached to this liaison statement.

ISO/IEC JTC 1/SC 27/WG 3 welcomes comments from The Open Group on any of its work items. The Open Group are invited to submit any comments in regard to ongoing work items as an attachment to the next liaison statement to WG 3.

Working Group Future meetings

SC 27 plans its next Working Group meetings in:

- Hong Kong, on 7-11 April, 2014
- Mexico City, Mexico, on 20-24 October, 2014
- Sarawak, Malaysia, on 04-08 May, 2015
- Jaipur, India, on 26-30 October, 2015

Attachments
- WG 3 resolutions (N13041)
- WG 3 Study Period report for High Assurance under ISO/IEC 15408 and ISO/IEC 18045 (N13038)”

Resolution 18: Text for liaison statement to ITU-T SG 17 to be sent by ISO/IEC JTC 1/SC 27/SWG-T

ISO/IEC JTC 1/SC 27/WG 3 provides input of the following text to SWG-T:

"**Security evaluation testing and specification**

SC 27/WG 3 thanks ITU-T SG17 for their Liaison Report (SC 27 N12741 and SC 27 N12744).

For verification of cryptographic protocols, ISO/IEC 29128 was published in November 2011. This standard defines process and protocol assurance level.

In ISO/IEC JTC1 SC27, this standard has been applied to following projects.

- ISO/IEC 11770-2 and 11770-3 (Key management)
  Defect report was provided according to verifications with align to ISO/IEC 29128. As a result of the defect report, ISO/IEC SC27/WG2 discuss the treatment of the report in the Incheon meeting. ISO/IEC SC27/WG2 had determined that it will organize study period on the security features of key management protocol.

- ISO/IEC 25185 (Entity authentication protocol from ISO/IEC SC17)
  ISO/IEC SC27 was requested to evaluate lightweight authentication protocols for smartcards from ISO/IEC SC27 and then conducted evaluation with align to ISO/IEC 29128. As a result of the verification, several problems in protocol description were found and gave comments to ISO/IEC SC17. As a result of this comment, this standard currently stays in 2nd DIS stage to fix these problems.

- ISO/IEC 9798-2, 9798-3 and 9798-4 (Entity authentication)
  Verifications were conducted to align to ISO/IEC 29128. Several vulnerable variants of protocols were found. Corrigenda have been published to fix these vulnerabilities.

Following process for reviews are planned in ISO/IEC JTC1 SC27/WG3 for ISO/IEC 29128.

- 1st pre-review: 2014
- Systematic review: 2016

ISO/IEC JTC1 SC27/WG3 would also like to inform ITU-T SG17 of our next meetings as follows:

- Hong Kong, on 7-11 April, 2014
- Mexico City, Mexico, on 20-24 October, 2014
- Sarawak, Malaysia, on 04-08 May, 2015
- Jaipur, India, on 26-30 October, 2015

ISO/IEC JTC1 SC27/WG3 asks ITU-T SG17 to continuously report further progress in the correspondence group to ISO/IEC JTC1 SC27/WG3 through the established liaison."

Resolution 19: Documents for First CD

ISO/IEC JTC 1/SC 27/WG 3 requests SC 27 Secretariat to register and circulate the following documents as first CD for balloting:

Document	Project	Title
SC 27 N13044	1.27.95 (17825)	Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules

Resolution 20: WG 3 meetings – Update of SD1

ISO/IEC JTC 1/SC 27/WG 3 agrees to the updated meeting table:

From	Until	Meeting	Place
2014-04-07	2014-04-11	SC 27 WG 3	Hong Kong
2014-10-20	2014-10-24	SC 27 WG 3	Mexico City, Mexico
2015-05-04	2015-05-08	SC 27 WG 3	Sarawak, Malaysia
2015-10-26	2015-10-30	SC 27 WG 3	Jaipur, India

ISO/IEC JTC 1/SC 27/WG 3 requests its Convenor to submit to the SC 27 Secretariat the following P resolutions for approval by the SC 27 plenary.

Resolution P1: Appointment of Liaison Officer

ISO/IEC JTC 1/SC 27 appoints the following Liaison Officer.

Name	From	To	Subject
Jan-Bernhard de Meer	WG 3	ETSI TC MTS	15408, 20004

Resolution P2: Proposal for New Work Item

ISO/IEC JTC 1/SC 27 requests its Secretariat to circulate the following document for New Work Item Proposal balloting:

Document	Title
SC 27 N13026	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

Resolution P3: Cancellation of Project

ISO/IEC JTC 1/SC 27 requests its Secretariat to take appropriate action for the cancellation of the following project.

Justification	Project	Title
SC 27 N13027	1.27.96 (30127)	Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis

Resolution P4: Sub-division of Project

ISO/IEC JTC 1/SC 27 requests its Secretariat to take the appropriate action for the further sub-division of the following project:

Project	Title	Justification
1.27.75 (20004)	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045	SC 27 N13402

Resolution P5: Documents for Publication

ISO/IEC JTC 1/SC 27 requests its Secretariat to take the appropriate action for the publication of the following documents:

Document	Project	Title
SC 27 N13048	1.27.51 (24759)	Test Requirements for Cryptographic Modules
SC 27 N12761	1.27.16.1 (15408-1)	Information technology – Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
SC 27 N12762	1.27.36 (18045)	Information technology – Security techniques -- Methodology for IT security evaluation

Resolution P6: Update of SD4

ISO/IEC JTC 1/SC 27 approves to update the following target dates in SD 4 and ask SC27 Secretariat to send those changes to JTC1 for endorsement letter ballot.

PROJECT	TITLE	TARGET DATES			
		WD/ WD/	CD/ PDTR/	FDIS/ DTR/	IS/ TR/
1.27.108 (19249)	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications	13-12	15-10	16-05	16-10
1.27.41 (19791)	Information technology – Security techniques -- Security assessment of operational systems	13-12	15-10	16-05	16-10

Resolution A Thanks to the SC 27 secretariat

ISO/IEC JTC 1/SC 27/WG 3 thanks Krystyna Passia for her efficient administrative support before and during the meeting.

Acclamation

Resolution B Thanks to the drafting committee

ISO/IEC JTC 1/SC 27/WG 3 thanks the members of the drafting committee Helmut Kurth and Naruki Kai for drafting the resolutions.

Acclamation

Resolution C Thanks to WG 3 Secretariat and Vice Convenor

The WG 3 Convener and experts thank its secretary and Vice Convenor, Naruki Kai, for his efforts and assistance in developing the WG 3 Meeting Report and during the meeting.

Acclamation

Resolution D Thanks to the Experts, Rapporteurs and Editors

ISO/IEC JTC 1/SC 27 WG 3 thanks all the SC 27 WG 3 experts, rapporteurs, editors, and acting editors and acting rapporteurs for their efforts and continued support in progressing the many SC 27 WG 3 projects.

Acclamation

Resolution E Thanks to Hosts and Sponsors

ISO/IEC JTC1/SC 27/WG 3 wishes to thank the meeting host organization and support staff from the Korean Agency for Technology and Standards (KATS). In particular WG 3 would like to thank: In-Soo Park, Kyung-Soo Chae, Seung-Joo Nam from KATS (NB-Korea). WG 3 also wishes to thank the Korean Standards Association (KSA) for performing a wonderful job as organizer of the meetings. WG 3 also wishes to thank the sponsors: Microsoft, Electronics and Telecommunications Research and Institute (ETRI), Incheon Development & Tourism Corporation (IDTC). WG 3 also wishes to thank all the individuals who contributed to a very entertaining social event at the Songdo Conference, in Incheon, Republic of South Korea.

Acclamation

Resolution F Thanks to the Convenor

ISO/IEC JTC 1/SC 27 WG 3 thanks Miguel Bañón for his excellent work as WG 3 Convener.

Acclamation