



ISO/IEC JTC 1/SC 27 **N 7784**

ISO/IEC JTC 1/SC 27/WG 3 **N 984**

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Meeting Report

TITLE: ISO/IEC JTC 1/SC 27/WG 3 Meeting Report - Meeting No. 38
4th to 8th May, 2009
Beijing, China

SOURCE: WG 3 Secretary (M Nash)

DATE: 2009-05-20

PROJECT:

STATUS: This document is being circulated for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P, O and L-Members
L. Rajchel, Secretariat JTC 1
K. Brannon, ITTF
W. Fumy, SC 27 Chair, M. DeSoete Vice-chair
E. Humphreys, K. Naemura, M. Bañón, M.C. Kang, K. Rannenber, WG-
Conveners
WG 3 Experts

MEDIUM: Server

NO. OF PAGES: 1+11

ISO/IEC JTC 1/SC 27/WG 3 Meeting No. 38
Beijing, China
4th to 8th May, 2009
Meeting Report

1 Opening of meeting, Monday 8th May at 1000

Delegates were welcomed by Mike Nash, WG 3 Secretary, who opened the meeting.

2 Roll call of delegates

<u>Canada</u>	Faud Khan, Alcatel-Lucent
<u>China</u>	Cui Shukun, China Standardisation Institute Li Shoupeng, China Standardisation Institute Jing Qianyuan, China Standardisation Institute Xiao Jinghua, China Standardisation Institute Bu Ning, China Information Security Certification Center Ge Li, China IWNCOMM Ma Chaobin, China Standardisation Institute
<u>Finland</u>	Jukka Valkonen (*), Helsinki University of Technology
<u>France</u>	Ludovic Merrien, Sagem Sécurité Jean-Pierre Quémard, EADS Secure Networks
<u>Germany</u>	Bertolt Krüger, SRC Security Research and Consulting GmbH Nils Tekampe, TUVIT
<u>Japan</u>	Naruki Kai, IT Promotion Agency Junichi Kondo, IT Promotion Agency Shin'ichiro Matsuo, NICT Toshio Miyachi, JPCERT Kunihiko Miyazaki, Hitachi Ltd Masao Tanabe, NTT Laboratories Masato Terada, IT Promotion Agency
<u>Korea (Rep. of)</u>	Soo-Young Chae, National Security Research Institute Sang-Yun Han, National Security Research Institute Jong-Hun Kim, Korean Information Security Agency Gang-Seok Lee, Korean Information Security Agency
<u>Spain</u>	Miguel Bañón, for Centro Criptológico Nacional Rosa Garcia, Consejería de Sanidad Paloma Llaneza, Razona Legal Tech
<u>UK</u>	Michael Nash, Gamma Secure Systems Ltd.

USA

Dan Benigni, NIST
Randall Easter, NIST
Helmut Kurth, atsec information security corp.
Mike Lai, Microsoft Corp.
Katie Moussouris, Microsoft Corp.
Fiona Pattinson, atsec information security corp.

Delegates marked (*) arrived after the start of the meeting. E-mail addresses are given in Attachment 1.

3 Adoption of the agenda and revision of meeting timetable

The draft agenda and timetable proposed in WG 3 N980rev2 were approved. A number of additional input documents were identified and added. An extra liaison issue, the International Organization of Legal Metrology, was added to the agenda as item 6.8.

4 Appointment of acting convenor and drafting committee

Mike Nash, WG 3 Secretary, reported that Mats Ohlin, the WG 3 Convenor, was ill and could not attend the meeting. Mike Nash was appointed Acting Convenor for the meeting (Resolution 2), as well as secretary (Resolution 3). He was instructed to prepare this meeting report as WG 3 N984. The following experts volunteered for the drafting committee: Miguel Bañón (Spain), Helmut Kurth (USA) and Fiona Pattinson (USA).

5 Report from WG 3 meeting in Limassol

The record of the resolutions from the meeting in Limassol (WG 3 N958) was presented and approved. The report of the meeting documented in WG 3 N959 was formally approved (Resolution 1).

6 Liaisons

6.1 Liaison with the ISSEA

Mike Nash, Acting Convenor, reported that no Liaison Statement had been received from the ISSEA. Since the ISSEA were already aware of the publication of ISO/IEC 21827:2008 (second edition), no new return Liaison Statement was considered necessary.

6.2 Liaison with the CCDB

A Liaison Statement from the CCDB was received at the start of the meeting (WG 3 N982). It was presented to the Group by Miguel Bañón, the Liaison Officer to WG 3 (see WG 3 N985). It provided latest information on the activities of the CCDB.

A return Liaison Statement to the CCDB was prepared (WG 3 N986). This thanked the CCDB for its Liaison Statement and provided details of progress on relevant WG 3 Projects.

In particular, it included a record of discussions on the future progress of IS 15408 (see WG 3 N 996).

The SC 27 Secretariat was requested to send the statement to the CCDB (Resolution P1).

6.3 Liaison with SC 37

Mike Nash, Acting Convenor, reported that SC 27 had received a Liaison Statement from SC 37 covering multiple Working Groups (SC27 N7611). There was little of direct relevance to WG 3, other than a request for update on the progress of Project 19792, Security evaluation of biometrics.

WG 3 prepared text for a combined SC 27 return Liaison Statement (see Resolution 10). This advised SC 37 that Project 19792 was currently undergoing FDIS ballot, and expressed interest in SC 37 NP 29156, Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics.

6.4 Liaison with FIRST

Mike Nash, Acting Convenor, reported that a Liaison Statement had been received from the Forum of Incident Response and Security Teams (FIRST) (SC 27 N7619), apologising that Damir Rajnovic, the Liaison Officer, could not attend the meeting, and advising that comments had been submitted on the second Working Draft for Project 29147, Responsible Vulnerability Disclosure (see SC 27 N7600).

A return Liaison Statement to FIRST was prepared (WG 3 N988), providing information on the progress of Project 29147 (see item 16).

The SC 27 Secretariat was requested to send the statement to FIRST (Resolution P1).

6.5 Liaison with ITU-T SG 17

Mike Nash, Acting Convenor, reported that SC 27 had received a Liaison Statement from ITU-T SG 17, concerning a proposed survey of security standards relevant to developing countries and countries with economies in transition (DC/CET) (see SC 27 N7435).

WG 3 prepared a contribution for use by SC 27 when replying to this Liaison Statement (WG 3 N989) (Resolution 11). WG 3 considered that relevant information was already generally available, but it would be willing to assist ITU-T SG 17 if the survey was approved.

6.6 Liaison with ECSA

Mike Nash, Acting Convenor, reported that SC 27 had received a request from the European Corporate Security Association (ECSA) to establish multiple Class C liaisons to SC 27 Working Groups, including WG 3 (see SC 27 N7436).

WG 3 noted this request, but took no further action.

6.7 Liaison with the Trusted Computing Group

Mike Nash, Acting Convenor, reported that a liaison between the Trusted Computing Group and SC 27 had been approved by SC 27, and was now with JTC 1 for default approval (see SC 27 N7425).

WG 3 expected that it would be assigned responsibility for ISO/IEC 11889, Trusted Platform Module, which was based on a Publicly Available Specification provided by the Trusted Computing Group (see item 19). If this assignment was approved by the SC 27 Plenary, WG 3 would take responsibility for this liaison.

Secretary's Note: WG 3 was indeed assigned overall responsibility for this activity by the SC 27 Plenary, with specific support on cryptographic matters to be provided by WG 2.

6.8 Liaison with the International Organization of Legal Metrology

Miguel Bañón noted that the International Organization of Legal Metrology (OIML) had requested a Category A liaison with SC 27 (see SC 27 N7358), and that part of the stated activities of the OIML was of direct relevance to WG 3 and also the CCDB.

Mike Nash, Acting Convenor, reported that Canada had objected to the establishment of this liaison (see SC 27 N7416). Any further action was a matter for OIML.

7 IS 15408 “Evaluation Criteria for IT Security” (Revision)

7.1 Revision of IS 15408-1:2005

Fiona Pattinson, the Project Editor, reported that final text for the revision had been prepared and submitted to ITTF for FDIS ballot (SC 27 N7261). Unfortunately, the FDIS ballot had not yet started, due to processing delays within ITTF.

7.2 Future work on IS 14508

A discussion was held on the future of the IS 15408 standard. This discussion is summarised in WG 3 N996. No specific action points were identified.

It was noted that once Part 1 of the current revision of IS 15408 had been published, WG 3 should request the availability of both IS 15408 and IS 18045 for free download from the ITTF web site.

8 Project IS 15292 “Protection Profile registration procedures”

Miguel Bañón reported on behalf of Centro Criptológico Nacional that CCN had still not yet been formally appointed as the Registration Authority by ITTF. The long and unexplained delay was causing CCN some embarrassment.

Secretary's Note: The SC 27 Plenary instructed its Chairman to raise an official complaint with ITTF concerning the delay.

9 TR 15446 “Guide for the production of Protection Profiles and Security Targets” (Revision)

Mike Nash and Helmut Kurth, joint Project Editors, advised that late comments on the DTR text had been received from ITTF (see SC 27N7287) and had been taken into account whilst

preparing the final text (SC 27 N7262). A list of changes from the DTR text was available in SC 27 N7293.

The revision had now been published (see SC 27 N7427).

10 Project TR 15443 “A Framework for IT security assurance” (Revision)

10.1 Project Editor’s report

Faud Khan, the Project Editor, reported that the second call for contributions for early revision of TR 15443 contained in SC 27 N7370 had produced no responses. The call for co-editors contained in SC 27 N7373 had generated no nominations. He concluded that there was little demand or interest from National Bodies for early revision of this Technical Report.

10.2 Further Work

After discussion, WG 3 decided to request SC 27 to cancel the early revision of this Technical Report, on the grounds that no essential changes had been identified by National Bodies (Resolution P8).

11 Project IS 19790 “Security requirements for cryptographic modules”

11.1 Project Editor’s report

Randall Easter, the Project Editor, reported that no First Working Draft for the revision of this Standard had been circulated, as the parallel revision of FIPS 140 had been delayed. However, he was hopeful that a new draft for public comment of FIPS 140-3 would be available shortly, and could be circulated as an initial Working Draft for revision of ISO/IEC 19790.

11.2 Further work

WG 3 considered that alignment with the revision process for FIPS 140 remained essential. WG 3 decided to encourage NIST to submit the new draft of FIPS 140-3 to WG 3 as soon as it was available, and to propose a joint editing session to discuss FIPS 140-3 and IS 19790 comments as part of the next WG 3 meeting, in Redmond, USA.

WG 3 prepared a letter containing these proposals (WG 3 N995) and requested SC 27 to send it to NIST (Resolution P7).

12 Project FCD 19792 “Security Evaluation of Biometrics”

Nils Tekampe, the Project Editor, reported that final text had been prepared and submitted to ITTF for FDIS ballot (SC 27 N7265). However, the start of the FDIS ballot had been delayed and was still in progress, due to end on 2009-06-16 (see SC 27 N7620).

Since the ballot was still in progress, there was nothing further to discuss.

13 Project IS 21827 “Systems Security Engineering - Capability Maturity Model” (Revision)

Mike Nash, Acting Convenor, reported that the legal problems concerning the 2007 revision had finally been sorted out and the second edition published as promised during October 2008 (see SC 27 N7329).

14 Project PDTR 19791 “Security assessment of operational systems” (Revision)

14.1 Project Editor’s report

Mike Nash, the Project Editor, advised that a PDTR ballot had been completed. The results of the ballot were contained in SC 27 N7386. 17 approval votes had been received, one with comments, 10 abstentions, one with comments, and one disapproval vote. The disapproval vote was on the grounds that the Technical Report was considered unnecessary.

14.2 Comments and contributions

All comments were considered and addressed at the meeting. The disposition of comments is recorded in WG 3 N991. WG 3 considered that there was sufficient consensus on technical content to proceed immediately to DTR ballot.

14.3 Further Work

The Project Editor was instructed to act upon the agreed disposition of comments, prepare a new version of the document as SC 27 N7792, and to send it to the SC 27 Secretariat by 2009-06-06 (Resolution 4). SC 27 was requested to progress the new draft to DTR and circulate it for balloting (Resolution P3).

15 Project WD 29128 “Verification of cryptographic protocols”

15.1 Project Editor’s report

Kunihiko Miyazaki, the Project Editor, reported that a Third Working Draft had been circulated for National Body comment. Comments had been received from three National Bodies, and were contained in SC 27 N7598.

15.2 Comments and contributions

All National Body comments were considered and addressed at the meeting. The disposition of comments is recorded in WG 3 N993. In addition, a joint breakout session was held with WG 2 to discuss relevant issues. WG 3 considered that the document was now sufficiently mature to progress to CD ballot.

15.3 Further Work

The Project Editor was instructed to prepare a First Committee Draft as SC 27 N7794, and to send it to the SC 27 Secretariat by 2009-07-06 (Resolution 4). SC 27 was requested to register this draft as a Committee Draft and circulate it for balloting (Resolution P2).

16 Project WD 29147 “Responsible Vulnerability Disclosure”

16.1 Project Editor’s report

Faud Khan, the Project Editor, reported that a Second Working Draft had been circulated for National Body comment. Comments had been received from six National Bodies, and were contained in SC 27 N7599. In addition, liaison comments had been received from FIRST (SC 27 N7600). As advised within the FIRST Liaison Statement (SC 27 N7619), these were duplicated within the UK National Body comments so that they could be presented at the meeting. However, they appeared as Belgian comments.

16.2 Comments and contributions

All National Body comments and contributions, including the FIRST liaison comments, were considered and addressed at the meeting. The disposition of comments is recorded in WG 3 N999.

16.3 Further work

The Project Editor was instructed to prepare a Third Working Draft as SC 27 N7901, and to send it to the SC 27 Secretariat by 2009-07-06 (Resolution 4). SC 27 was requested to distribute this Working Draft for National Body review and comment (Resolution P4).

FIRST was asked in its return Liaison Statement not to duplicate comments unnecessarily (see WG 3 N988).

17 Project NP 29193 Secure-System Engineering Principles and Techniques

17.1 Project Editor’s Report

Fiona Pattinson, the Rapporteur for the Study Period, reported that the New Work Item Proposal had been balloted by National Bodies. The results were contained within SC 27 N7393. 21 members had approved the addition of the new work item to the work programme, with six abstentions and two no votes. Comments had been submitted by three National Bodies. The proposal had therefore been accepted, and the Project assigned number 29193.

17.2 Appointment of Project Editor

Fiona Pattinson, the Rapporteur for the Study Period, stated that she wished to withdraw her nomination as Project Editor as proposed at the Limassol meeting (see WG 3 N958, Resolution P1). She noted that although no other nominations had been received in response to the call for editors for this New Project (SC 27 N7372), Anne Coat had been nominated by the French National Body in response to Question 4 of the NWIP (see SC 27 N7393). Thus an alternative candidate existed. However, Anne Coat had not been able to attend the Beijing Meeting. She was therefore willing to proceed as Acting Editor until a transfer of responsibility to Anne Coat could be completed.

WG 3 appointed Fiona Pattinson as Acting Editor for the Project, with duration until its next meeting in Autumn 2009 (Resolution 9).

17.3 Comments and contributions

All National Body comments on the New Work Item Proposal were considered and addressed at the meeting. The disposition of comments is recorded in WG 3 N997.

17.4 Further work

The Acting Editor was instructed to prepare a First Working Draft as SC 27 N7902, and to send it to the SC 27 Secretariat by 2009-07-06 (Resolution 5). SC 27 was requested to distribute this Working Draft for National Body review and comment (Resolution P4).

SC 27 was requested to note the withdrawal of Fiona Pattinson as Project Editor (Resolution P5) and appoint Anne Coat as her replacement (Resolution P6).

18 WG Study Period on Tamper Protection Requirements and Evaluation

18.1 Rapporteur's Report

Miguel Bañón, the Rapporteur for the Study Period, made a presentation (WG 3 N990) reporting that a call for contributions had been circulated (SC 27 N7403), and two responses received from National Bodies (SC 27 N7604). He concluded that there was consensus that the development of a Technical Report covering tamper protection requirements and evaluation was feasible, and would facilitate good practice in industry. A full report on the Study Period was prepared (WG 3 N998).

18.2 Further work

WG 3 resolved to extend the Study Period for a further six months, in order to seek further contributions from National Bodies and identify potential editors (Resolution 8).

19 BRM Report IS 11889 Trusted Platform Module

Mike Nash, Acting Convenor, reported that a Ballot Resolution Meeting had been held in Limassol following the Working Group Meetings, chaired by the WG 3 Convenor, Mats Ohlin. A report on the meeting was available (SC 27 N7317), together with dispositions of comments on the four parts balloted as a fast track Publicly Available Specification (SC 27 N7318 to N7321). The published text was available as SC 27 N7331 to N7334.

It was likely that maintenance of this International Standard would be assigned to WG 3 by the SC 27 Plenary.

Secretary's Note: WG 3 was indeed assigned overall responsibility for this activity by the SC 27 Plenary, with specific support on cryptographic matters to be provided by WG 2.

20 Road Map for WG 3

Mike Nash, Acting Convenor, reported that, once again, there had been no Expert or National Body comments on the draft WG 3 Road Map (WG 3 N869). It was decided to defer further discussion of the Road Map until the next meeting of WG 3, when updated management guidelines would be available.

21 WG 3 Revision of Target Dates and List of Editors

New target and actual dates for Projects 15408-1, 19790, 29147 and 29193 are recorded in WG 3 N983 (Resolution 7).

22 WG 3 Meeting Calendar

The next WG meeting was confirmed as 2009-11-02 to 2009-11-06 in Redmond, USA. The following meeting will be held in Malaysia, date and venue to be decided (Resolution 6).

Secretary's Note: The SC 27 Plenary confirmed that the following meeting would be held in Melaka, Malaysia, 2010-04-19 to 2010-04-23.

23 Updates of SC 27 Standing Documents

Project Editors were once again requested to check SC 27 Standing Documents SD6 and SD7 for any changes that might be necessary (Resolution 7).

24 Resolutions and Recommendations to SC 27 Plenary

The resolutions approved by WG 3 in Beijing China are recorded in WG 3 N983.

The SC 27 Secretariat, the Drafting Committee, the WG 3 Secretary, Acting Convenor, experts and editors, as well as the meeting hosts and sponsors were thanked for their efforts and support (Resolutions A-F). In particular, the editors Michael Nash, Helmut Kurth and John Hopkinson were thanked for their efforts in successfully getting documents through the standardisation process.

WG 3 and the experts and National Bodies that it represents expressed their warmest thanks to the WG 3 Convenor, Mats Ohlin, for his respected management of the WG programme of work (Resolution G).

25 New WG 3 convenor

Mike Nash, Acting Convenor, reported that a call for nominations for a new WG 3 Convenor had been circulated to National Bodies (SC 27 N7388). Two candidates, Miguel Bañón and Helmut Kurth, had been nominated (see SC 27 N7464). A decision would be made by the SC 27 Plenary following the Working Group meeting.

Secretary's Note: SC 27 subsequently appointed Miguel Bañón as the new WG 3 Convenor.

26 Any other business

Mike Nash, Acting Convenor, advised WG 3 Project Editors to read the excellent guide to the attributes, skills, roles and responsibilities required of Project Editors prepared by the

Brazilian National Body (SC 27 N7489rev1). He also noted the Australian proposal to the SC 27 Plenary in SC 27 N7465 to significantly tighten the submission criteria for New Work Item Proposals.

Finally, Mike Nash repeated the SC 27 Marketing Officer's plea for information relating to articles – published, in development or planned – concerning the standards development work of SC 27.

27 Closure of meeting

The meeting of WG 3 closed on 2009-05-07 at approximately 1830. Output documents were made available between 0900 and 1000 on 2009-05-08.

Attachment 1

Attendees at the 38th WG 3 Meeting, Beijing, China.

<i>Name</i>	<i>NB</i>	<i>Organisation</i>	<i>E-mail</i>
Faud Khan	Canada	Alcatel-Lucent	faud.khan@alcatel-lucent.com
Cui Shukun	China	China Standardisation Inst	cskun-ok@126.com
Li Shoupeng	China	China Standardisation Inst	lisp@itsec.gov.cn
Jing Qianyuan	China	China Standardisation Inst	qiankun3344@yahoo.com.cn
Xiao Jinghua	China	China Standardisation Inst	
Bu Ning	China	China Info Sec Cert Center	buning@isccc.gov.cn
Ge Li	China	China IWNCOMM	geli@iwncomm.com
Ma Chaobin	China	China Standardisation Inst	machb2000@163.com
Jukka Valkonen	Finland	Helsinki Uni Technology	jukka.valkonen@tkk.fi
Ludovic Merrien	France	Sagem Sécurité	ludovic.merrien@sagem.com
Jean-Pierre Quémar	France	EADS Secure Networks	jean-pierre.quepard@eads.com
Bertolt Krüger	Germany	SRC	bertolt.krueger@src-gmbh.de
Nils Tekampe	Germany	TUVIT	n.tekampe@tuvit.de
Naruki Kai	Japan	IT Promotion Agency	n-kai@ipa.go.jp
Junichi Kondo	Japan	IT Promotion Agency	j-kondou@ipa.go.jp
Shin'ichiro Matsuo	Japan	NICT	smatsuo@nict.go.jp
Toshio Miyachi	Japan	JPCERT	toshio.miyachi@jpcert.or.jp
Kunihiko Miyazaki	Japan	Hitachi Ltd	kunihiko.miyazaki.zt@hitachi.com
Masao Tanabe	Japan	NTT Laboratories	tanabe.masao@lab.ntt.co.jp
Masato Terada	Japan	IT Promotion Agency	m-terada@ipa.go.jp
Soo-Young Chae	Korea	NSRI	sychae@ensec.re.kr
Sang-Yun Han	Korea	NSRI	syhan@ensec.re.kr
Jong-Hun Kim	Korea	KISA	uandi@kisa.or.kr
Gang-Seok Lee	Korea	KISA	5363@kisa.or.kr
Miguel Bañón	Spain	for CCN	miguel@bagnon.com
Rosa Garcia	Spain	Consejeria de Sanidad	rosa.garciaontoso@salud.madrid.org
Paloma Llana	Spain	Razona Legal Tech	pllana@razonalegaltech.com
Michael Nash	UK	Gamma Secure Systems	mnash@gammassl.co.uk
Dan Benigni	USA	NIST	dbenigni@nist.gov
Randall Easter	USA	NIST	randall.easter@nist.gov
Helmut Kurth	USA	atsec information security	helmut@atsec.com
Mike Lai	USA	Microsoft Corp	mikelai@microsoft.com
Katie Moussouris	USA	Microsoft Corp	katiemo@microsoft.com
Fiona Pattinson	USA	atsec information security	fiona@atsec.com