



ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"

Convenorship: UNE

Convenor: Bañón Miguel Mr



**ISO/IEC JTC 1/SC 27/WG 3 Recommendations 62nd Meeting, Virtual (via Zoom)
April 12th – 15th, 2021**

Document type	Related content	Document date	Expected action
Meeting / Other	Meeting: VIRTUAL 12 Apr 2021	2021-04-27	INFO

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

62nd Meeting, Virtual (via Zoom)

April 12th – 15th, 2021

All recommendations are approved UNANIMOUSLY unless otherwise noted.

WG Recommendation 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 61st virtual meeting, September 12th – 16th 2020, in document WG 3 N2006.

WG Recommendation 2. Appointment of the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 resolves to appoint Kwangwoo Lee and Philippe Magnabosco as Drafting Committee of the meeting and instructs them to prepare the draft WG recommendations document for WG 3.

WG Recommendation 3. Appointment of Acting Liaison Officers

ISO/IEC JTC 1/SC 27/WG 3 resolves to appoint the following acting liaison officers through the end of the meeting.

Liaison Officer	Liaison Institution
Hao Qin	to ITU-T SG 17
Martin Ward	to ETSI ISG QKD
Hao Qin	to ITU-T FG-QIT4N

WG Recommendation 4. PWI registration requests

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to register the following PWIs listed below.

Title (and N-Nr, if any)	Project Editors: Name (Country)
Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045 (WG3 N2083)	Carolina Lavatelli (FR) * Christian Noetzel (DE) * David Martin (GB) Elzbieta Andrukiewicz (PL) * Fiona Pattinson (US) * Guillaume Têtu (FR) * Heebong Choi (KR) * Hongsong SHI (CN) * Kwangwoo Lee (KR) * Nicholas Muthambi (ZA) * Philippe Magnabosco (FR) * Tony Boswell (GB) *

Revision of ISO/IEC 19792:2009 Security evaluation of biometrics (WG3 N2053)	Julien Bringer (FR) Asahiko Yamada (JP) *
Requirements for the competence of IT security conformance assessment body personnel (WG3 N2084)	Heebong Choi (KR) * Carolyn French (CA) * Fiona Pattinson (US) Randall Easter (US) *

* Co-editor

WG Recommendation 5. Cancellation of Projects

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to cancel the following projects listed below.

Title (and N-Nr, if any)	Justification
PWI 5888: Evaluation criteria for connected vehicle information security based on ISO/IEC 15408	Agreed to develop an IS.
PWI 5891: A general framework for runtime hardware security assessment	Agreed to develop a TR.
PWI 5895: Multi-party coordinated vulnerability disclosure and handling	Agreed to develop a TR.
PWI 29128-2: Verification of cryptographic protocols – Part 2: Evaluation methods and activities	Agreed to develop new parts of ISO/IEC 29128.

WG Recommendation 6. Call for contributions

ISO/IEC JTC 1/SC 27/WG 3 resolve to circulate a call for expert participation and contributions for the following projects. Submissions should reach the WG 3 Secretariat by the due date identified below.

Document	Project	Title	To be sent to/by
WG3 N2054	PWI	Cybersecurity assurance of complex systems based on ISO/IEC 15408	WG 3 Secr/ 2021-09-10
WG 3 N2055	PWI	ISO/IEC 15408 in the cloud	WG 3 Secr/ 2021-09-10
WG 3 N2083	PWI	Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045	WG 3 Secr/ 2021-09-10
WG 3 N2053	PWI	Revision of ISO/IEC 19792:2009 Security evaluation of biometrics	WG 3 Secr/ 2021-09-10
WG 3 N2084	PWI	Requirements for the competence of IT security conformance assessment body personnel	WG 3 Secr/ 2021-09-10
WG 3 N2056	23837	Call for contributions on the definition of the term “information theoretic security”	WG 3 Secr/ 2021-06-15

WG Recommendation 7. Technical Report registration

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to add the Technical Report project listed below to the SC 27 Programme of Work.

Title (and N-Nr, if any)	Project Editors: Name (Country)	SDT
Multi-party coordinated vulnerability disclosure and handling	Josh Dembling (US) Dr. Claire Vishik (GB) * Dr. Amit Elazari Bar On (IL) * Tomotaka Ito (JP) * Deana Shick (US) *	SDT 18 (18 months to publication) WD: 2021-04-11 DTR: 2021-08-01 TR: 2022-10-30
A General Framework for Runtime Hardware Security Assessment	Bowei Zhang (CN) Ao Luo (CN) * Yuto Nakano (JP) *	SDT 18 (18 months to publication) WD: 2021-04-11 DTR: 2021-08-01 TR: 2022-10-30

* Co-editor

WG Recommendation 8. Updating of documents

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the Project Editors/Co-Editors of the projects identified below to update the following drafts and send them to the SC 27 or WG 3 Secretariat by the due dates.

Document	Project No.	Title	To be sent to/by	DoC Doc. No.
WG 3 N2085	17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	WG 3 Secr. 2021-07-29	
WG 3 N2057	19790	Security requirements for cryptographic modules	WG 3 Secr. 2021-07-29	WG 3 N2040
WG 3 N2058	22216	Introductory guidance on evaluation for IT security	SC 27 Secr. 2021-07-29	WG 3 N2081
WG 3 N2060	23837-1	Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements	SC 27 Secr. 2021-07-29	WG 3 N2059
WG 3 N2061	23837-2	Security requirements, test and evaluation methods for quantum key distribution – Part 2: Test and evaluation methods	SC 27 Secr. 2021-07-29	WG 3 N2059
WG 3 N2062	24485	Security properties, test and evaluation guidance for white box cryptography	SC 27 Secr. 2021-07-29	WG 3 N2042
WG 3 N2063	24759	Test requirements for cryptographic modules	WG 3 Secr. 2021-07-29	WG 3 N2041

WG 3 N2065	29128-1 *	Verification of cryptographic protocols	SC 27 Secr. 2021-07-09	WG 3 N2064
WG 3 N2066	Technical Report	Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045	SC 27 Secr. 2021-07-29	WG 3 N2052
WG 3 N2067	Technical Report	Multi-party coordinated vulnerability disclosure and handling	SC 27 Secr. 2021-07-29	
WG 3 N2068	Technical Report	A General Framework for Runtime Hardware Security Assessment	SC 27 Secr. 2021-07-29	
WG 3 N2069	--	WG 3 Roadmap	WG 3 Secr. 2021-07-29	

* Subject to approval of WG recommendation 16

WG Recommendation 9. Documents for Study and Comment

ISO/IEC JTC 1/SC 27/WG 3 resolves to circulate the following documents to experts for study and comment.

Document	Project	Title	Comments Due date
WG 3 N2085	17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	2021-09-17
WG 3 N2057	19790	Security requirements for cryptographic modules	2021-09-17
WG 3 N2063	24759	Test requirements for cryptographic modules	2021-09-17
WG 3 N2066	Technical Report	Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045	2021-09-17
WG 3 N2069	--	WG 3 Roadmap	2021-09-17

WG Recommendation 10. New Work Item

ISO/IEC JTC 1/SC 27/WG 3 resolves to invite the SC 27 Secretariat to submit the following NP with the ballot period indicated.

Title (and N-Nr, if any)	Ballot Period
Information security, cybersecurity and privacy protection — Security requirements and evaluation activities for connected vehicle devices (WG 3 N2070)	12 weeks
Information technology — Security techniques — Verification of cryptographic protocols — Part 2: Evaluation Methods and Activities for Cryptographic Protocols (WG 3 N2071)	12 weeks
Information technology — Security techniques — Verification of cryptographic protocols — Part 3: Evaluation Methods and Activities for Protocol Implementation Verification (WG 3 N2072)	12 weeks

WG Recommendation 11. Technical Corrigendum of ISO/IEC 19790:2012

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to approve the initiation of a Technical Corrigendum for ISO/IEC 19790:2021. Justification is included in WG 3 N2073.

WG Recommendation 12. Technical Corrigendum of ISO/IEC 24759:2017

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to approve the initiation of a Technical Corrigendum for ISO/IEC 24759:2017. Justification is included in WG 3 N2074.

WG Recommendation 13. Confirmation of ISO/IEC 19792:2009

ISO/IEC JTC 1/SC 27/WG 3 notes the comments and ballot results from the Systematic Review of ISO/IEC 19792:2009 in N21579 and resolves to confirm this Standard for an additional five years.

WG Recommendation 14. Confirmation of ISO/IEC TS 19247:2017

ISO/IEC JTC 1/SC 27/WG 3 notes the comments and ballot results from the Systematic Review of ISO/IEC TS 19247:2017 in N21587 and resolves to confirm this Technical Specification for an additional five years.

WG Recommendation 15. Scope Change of ISO/IEC 29128

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to change the scope of ISO/IEC 29128 from:

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

to:

“This document establishes a framework for the verification of cryptographic protocol specifications according to academic and industry best practices.”

Justification:

“The original scope of ISO/IEC 29128:2011 included technical content related to security proofs for the verification of protocol specifications, as well as the evaluation methods for protocol specifications under the framework of ISO/IEC 15408. During the revision of 29128, it was suggested by the editors and agreed within WG3 to move the evaluation framework related to 15408 to a second part to the standard. Therefore, the scope of the first part has been narrowed to the verification of cryptographic protocols using proofs generated by automated tools”

WG Recommendation 16. Number change

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 to change the following project number.

Current project number	New project number	Justification	Remark
ISO/IEC 29128	ISO/IEC 29128-1	This project is to become a multipart standard.	Subject to approval of NWIP 29128-2 and 29128-3 in WG 3 Recommendation 10

WG Recommendation 17. Document for 1st DTR

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following document as 1st DTR to circulate for balloting.

Document	Project	Title
WG 3 N2067	Technical Report	Multi-party coordinated vulnerability disclosure and handling
WG 3 N2068	Technical Report	A General Framework for Runtime Hardware Security Assessment

WG Recommendation 18. Document for further CD

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to circulate the following document for balloting.

Document	Project	Title
WG 3 N2060	23837-1	Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements
WG 3 N2061	23837-2	Security requirements, test and evaluation methods for quantum key distribution – Part 2: Test and evaluation methods

WG Recommendation 19. Document for 1st DIS

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following document as 1st DIS to circulate for balloting.

Document	Project	Title
WG 3 N2065	29128-1 *	Verification of cryptographic protocols

*) Subject to approval of WG recommendation 16

WG Recommendation 20. Documents for publication

ISO/IEC JTC 1/SC 27 resolves to request the SC 27 Secretariat to publish the following documents:

Document	Project	Title
WG 3 N2058	22216	Introductory guidance on evaluation for IT security
WG 3 N2062	24485	Security properties, test and evaluation guidance for white box cryptography

WG Recommendation 21. Extension of Project Duration

ISO/IEC JTC 1/SC 27/WG 3 resolves to approve to extend the total project duration for the following project by 9 months.

Project	Current Limit Dates	Proposed Limit Dates	Justification
23837-1	DIS: 2021-07-24 IS: 2022-07-24	DIS: 2022-04-24 IS: 2023-04-24	WG 3 N2010
23837-2	DIS: 2021-07-24 IS: 2022-07-24	DIS: 2022-04-24 IS: 2023-04-24	WG 3 N2011

WG Recommendation 22. Acknowledgement of new Liaison Officer

ISO/IEC JTC 1/SC 27/WG 3 resolves to acknowledge the following new liaison officer.

Organization	Liaison Officer
Common Criteria Development Board (CCDB)	From the CCDB to ISO/IEC JTC 1/SC 27/WG 3 Elzbieta Andrukiewicz (PL)

WG Recommendation 23. Approval of external Liaison

ISO/IEC JTC 1/SC 27/WG 3 resolves to approve the request from the following external organization as well as the appointment of the below mentioned expert as Liaison Officer:

Organization	Cat (A, B or C)	Document (N-Nr.)	Liaison Officer
Cryptographic Module Users Forum (CMUF)	C	WG 3 N2002	Yi Mao

WG Recommendation 24. Liaison Statements

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

Document	To	Topic	Reference
WG 3 N2082	CCDB	All projects	WG 3 N2005
WG 3 N2075	CCUF	All projects	WG 3 N2026
WG 3 N2076	ITU-T SG 17	23837	
WG 3 N2077	ITU-T FG-QIT4N	23837	SC 27 N21410 SC 27 N21411 SC 27 N21546
WG 3 N2078	ETSI ISG QKD	23837	WG 3 N2013
WG 3 N2079	ISO TC22/SC32/WG11	PWI 5888	
WG 3 N2080	SC 37	19989 19792	SC 27 N21574 SC 27 N21589

WG Recommendation 25. Request to the WG 3 convenor

ISO/IEC JTC 1/SC 27/WG 3 resolves to ask the WG 3 convenor to raise the following request at the SC 27 Plenary to be held on 16th April 2021.

“The WG3 experts considered the points made in the liaison statements from the CCDB and CCUF. The experts fully supported those points and asked the convenor to raise the concerns, through the SC27 plenary, in order to expedite the discussions and swiftly reach a suitable conclusion. The group has expended a great deal of time in the development, editing, and review of the ISO/IEC 15408 and 18045 standards and are very keen to ensure that these can continue to be used as widely as possible.”

WG Recommendation 26. Call for contribution for SC 27 Periodical Magazine articles

ISO/IEC JTC 1/SC 27/WG 3 resolves to issue a call for contribution for SC 27 Periodical Magazine articles (See detail in WG 3 N2051). Articles should be submitted to WG 3 management team (miguel@bagnon.com and n-kai@ipa.go.jp) by 7th May 2021.

WG Recommendation 27. Call for contribution for ISO/IEC 19790 virtual conference

ISO/IEC JTC 1/SC 27/WG 3 resolves to issue a call for contribution for the ISO/IEC 19790 virtual conference (See detail in WG 3 N2051).

Those experts who can volunteer for the ISO/IEC 19790 conference program committee should inform to WG 3 management team (miguel@bagnon.com and n-kai@ipa.go.jp) by 23th April 2021. The following experts already volunteered during the meeting:

- Yi Mao
- Jean Pierre Quemard
- Heebong Choi

Proposals for the ISO/IEC 19790 conference should be submitted to WG 3 management team (miguel@bagnon.com and n-kai@ipa.go.jp) by 30th April 2021.

Resolution A Thanks to the liaison officer from the CCDB to ISO/IEC JTC 1/SC 27/WG 3

ISO/IEC JTC 1/SC 27/WG 3 thanks to the liaison officer David Martin for his efficient and professional work and support for efficient liaison channel from the CCDB to ISO/IEC JTC 1/SC 27/WG 3. ISO/IEC JTC 1/SC 27/WG 3 also thanks him for his continuing support for liaison channel from ISO/IEC JTC 1/SC 27/WG 3 to the CCDB.

Acclamation

Resolution B Thanks to the SC 27 Committee Manager

ISO/IEC JTC 1/SC 27/WG 3 thanks Sobhi Mahmoud for his efficient and unfailing support before and during the meeting.

Acclamation

Resolution C Thanks to the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 thanks the members of the drafting committee Philippe Magnabosco and Kwangwoo Lee for drafting the recommendations.

Acclamation

Resolution D Thanks to WG 3 Secretariat and Convenor support

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

Acclamation

Resolution E 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, acting editors and acting rapporteurs for their efforts and continued support in progressing the many SC 27 WG 3 projects.

ISO/IEC JTC 1/SC 27 WG 3 especially thanks the following editors for their efforts in getting the following documents through the standardisation process.

Editor	Project	Title
Yamada Asahiko Christian Noetzel	19989-1	Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework
Julien Bringer Yamada Asahiko	19989-2	Information security — Criteria and methodology for security evaluation of biometric systems — Part 2: Biometric recognition performance
Yamada Asahiko Julien Bringer	19989-3	Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection
Sylvain Guilley	20897-1	Information security, cybersecurity and privacy

Soshi Hamaguchi Yousung Kang		protection — Physically unclonable functions — Part 1: Security requirements
---------------------------------	--	---

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