



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

Convenorship: UNE

Convenor: **Bañón Miguel Mr**



WG 3 Recommendations, Virtual (via Zoom) September 12th – 16th, 2020

Document type	Related content	Document date	Expected action
Meeting / Other	Meeting: VIRTUAL Sep 2020	2020-09-24	INFO

Description

This document was available at the 2020 September WG 3 meeting. It is being circulated for information.

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

61st Meeting, Virtual (via Zoom)

September 12th – 16th, 2020

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 60th virtual meeting, April 20th – 24th 2020, in document WG 3 N1892.

WG Recommendation 2. Appointment of the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 resolves to appoint Kwangwoo Lee, Philippe Magnabosco and Junning Yao 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 Yousung Kang	to ITU-T SG 17
Martin Ward	to ETSI ISG QKD
Jiajun Ma	to ITU-T FG-QIT4N

WG Recommendation 4. Appointment of Project Editors/Co-Editors

ISO/IEC JTC 1/SC 27/WG 3 recommends SC 27 to appoint the experts listed below as Editor/Co-Editors.

Project	Name (Country)
17825	Sylvain Guilley (FR) Randall Easter (US) * Jean-Pierre Quémard(FR) * Jiazhe CHEN(CN) *
19790	Carolyn French (CA) Heebong Choi (KR) * Jean-Pierre Quémard (FR) * Randall Easter (US) *
24759	Heebong Choi (KR) Carolyn French (CA) *

	Jean-Pierre Quémard (FR) * Randall Easter (US) *
--	---

* Co-editor

WG Recommendation 5. Termination of WG Study Periods

ISO/IEC JTC 1/SC 27/WG 3 resolves to terminate the Study Periods listed below.

Document	Title	Rapporteur
WG 3 N1843	Evaluation criteria for connected vehicle information security based on ISO/IEC 15408	Di Tang Dietmar Bremser # Christian Noetzel # Claire Vishik # Yi Zhang # Gaëtan Pradel #
WG 3 N1844	Hardware monitoring technology for hardware security assessment	Bowei Zhang Ao Luo # Yuto Nakano #
WG 3 N1845	Creation of a patch management extension for ISO/IEC 15408 and ISO/IEC 18045	Javier Tallón Sebastian Fritsch #
WG 3 N1846	Multi-party coordinated vulnerability disclosure and handling	Josh Dembling Claire Vishik # Amit Elazari Bar On # Tomotaka Ito #
WG 3 N1847	Update of ISO/IEC 17825:2016	Sylvain Guilley Jean-Pierre Quémard # Randall Easter # Jiazhe Chen #
WG 3 N1848	Update of ISO/IEC 19790:2012 and ISO/IEC 24759:2017	Heebong Choi Jean-Pierre Quémard # Randall Easter # Carolyn French #
WG 3 N1842	Framework for cybersecurity assurance and relation with ISO/IEC 15408	Ricardo Villalón Antonio Kung #

co-rapporteur

WG Recommendation 6. 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)
Evaluation criteria for connected vehicle information security based on ISO/IEC 15408 (WG3 N1930)	Di Tang (CN) Xiaoxin Gong (CN) *

	Naruki Kai (JP) *
A general framework for runtime hardware security assessment (WG3 N1937)	Bowei Zhang (CN) Ao Luo (CN) * Yuto Nakano (JP) *
Multi-party coordinated vulnerability disclosure and handling (WG3 N1950)	Josh Dembling (US) Claire Vishik (GB) * Amit Elazari Bar On (IL) * Tomotaka Ito (JP) *
Cybersecurity assurance of complex systems based on ISO/IEC 15408 (WG3 N1924, WG3 N1925)	Ricardo Villalón (CR) Antonio Kung (FR) *
ISO/IEC 15408 in the cloud (WG 3 N1934)	Tyrone Stodart (GB)
Verification of cryptographic protocols – Part 2: Evaluation methods and activities (WG 3 N1952)	Carolyn French (CA) Ritu-Ranjan Shrivastwa (FR) *

* Co-editor

WG Recommendation 7. 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
WG 3 N1930	PWI	Evaluation criteria for connected vehicle information security based on ISO/IEC 15408	WG 3 Secr/ 2021-03-01
WG 3 N1937	PWI	A general framework for runtime hardware security assessment	WG 3 Secr/ 2021-03-01
WG 3 N1950 WG 3 N1953	PWI	Multi-party coordinated vulnerability disclosure and handling	WG 3 Secr/ 2021-03-01
WG3 N1924 WG3 N1925	PWI	Cybersecurity assurance of complex systems based on ISO/IEC 15408	WG 3 Secr/ 2021-03-01
WG 3 N1934	PWI	ISO/IEC 15408 in the cloud	WG 3 Secr/ 2021-03-01
WG 3 N1952	PWI	Verification of cryptographic protocols – Part 2: Evaluation methods and activities	WG 3 Secr/ 2021-03-01

WG Recommendation 8. 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
--------------------------	------------------------------------	-----

Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045 (WG 3 N1852, WG 3 N1932)	Javier Tallón (ES) Sebastian Fritsch (DE) *	SDT 18 (18 months to publication) WD: 2021-01-18 DTR: 2021-10-30 TR: 2022-04-01
---	--	--

* Co-editor

WG Recommendation 9. Preparation of Documents

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the Project Editors/Co-Editors to prepare a 1st WD for the projects listed below.

Document	Project	Title	To be sent/by
WG 3 N1953	Technical Report	Multi-party coordinated vulnerability disclosure and handling	WG 3 Secr/ 2021-02-01
WG 3 N1954	Technical Report	Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045	SC 27 Secr/ 2021-01-18
WG 3 N1955	17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	WG 3 Secr/ 2021-01-18
WG 3 N1956	19790	Security requirements for cryptographic modules	WG 3 Secr/ 2021-01-18
WG 3 N1957	24759	Test requirements for cryptographic modules	WG 3 Secr/ 2021-01-18

WG Recommendation 10. 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 N1958	15408-1	Evaluation criteria for IT security – Part 1: Vocabulary, introduction and general model #	SC 27 Secr. 2021-01-18	WG 3 N1945
WG 3 N1959	15408-2	Evaluation criteria for IT security – Part 2: Security functional components	SC 27 Secr. 2021-01-18	WG 3 N1945
WG 3 N1960	15408-3	Evaluation criteria for IT security – Part 3: Security assurance components	SC 27 Secr. 2021-01-18	WG 3 N1945
WG 3 N1961	15408-4	Evaluation criteria for IT security – Part 4: Framework	SC 27 Secr.	WG 3

		for the specification of evaluation methods and activities	2021-01-18	N1945
WG 3 N1962	15408-5	Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements	SC 27 Secr. 2021-01-18	WG 3 N1945
WG 3 N1963	18045	Methodology for IT security evaluation	SC 27 Secr. 2021-01-18	WG 3 N1945
WG 3 N1964	19989-1	Criteria and methodology for security evaluation of biometric systems – Part 1: Framework	SC 27 Secr. 2021-01-18	
WG 3 N1965	19989-2	Criteria and methodology for security evaluation of biometric systems – Part 2: Biometric recognition performance	SC 27 Secr. 2021-01-18	
WG 3 N1966	19989-3	Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection	SC 27 Secr. 2021-01-18	
WG 3 N1967	20897-2	Physically unclonable functions — Part 2: Test and evaluation methods	SC 27 Secr. 2021-01-08	WG 3 N1939
WG 3 N1968	22216	Introductory guidance on evaluation for IT security	SC 27 Secr. 2021-01-18	SC 27 N20032
WG 3 N1969	23532-1	Requirements for the competence of IT security testing and evaluation laboratories – Part 1: Evaluation for ISO/IEC 15408#	SC 27 Secr. 2021-01-18	WG 3 N1977
WG 3 N1970	23532-2	Requirements for the competence of IT security testing and evaluation laboratories – Part 2: Testing for ISO/IEC 19790	SC 27 Secr. 2021-01-18	WG 3 N1922
WG 3 N1971	23837-1	Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements	SC 27 Secr. 2021-01-18	WG 3 N1935
WG 3 N1972	23837-2	Security requirements, test and evaluation methods for quantum key distribution – Part 2: Test and evaluation methods	SC 27 Secr. 2021-01-18	WG 3 N1935
WG 3 N1973	24485	Security properties, test and evaluation guidance for white	SC 27 Secr.	SC 27 N20573

		box cryptography	2021-01-18	
WG 3 N1974	29128	Verification of cryptographic protocols	SC 27 Secr. 2021-01-18	WG 3 N1943
WG 3 N1975	--	WG 3 Roadmap	SC 27 Secr. 2021-01-18	

WG Recommendation 11. 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 N1955	17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	2021-03-01
WG 3 N1956	19790	Security requirements for cryptographic modules	2021-03-01
WG 3 N1957	24759	Test requirements for cryptographic modules	2021-03-01
WG 3 N1954	Technical Report	Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045	2021-03-01
WG 3 N1975	--	WG 3 Roadmap	2021-03-01

WG Recommendation 12. Initiation of revision

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to initiate revision of the following documents.

Project	Title	Justification
17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	WG 3 N1948
19790	Security requirements for cryptographic modules	WG 3 N1941
24759	Test requirements for cryptographic modules	WG 3 N1941

WG Recommendation 13. Title Change

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to change the title of the following projects.

Project	Current title	New title	Justification
15408-1	Evaluation criteria for IT security – Part 1: Introduction and general model	Evaluation criteria for IT security – Part 1: Vocabulary, introduction and general model	The current title is not precise enough and is changed according to ISO/IEC Directives, Part 2:2018.

23532-1	Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Testing and evaluation for ISO/IEC 15408	Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408	The current title is not precise, and the requested modification reflects the content in a much suitable manner.
---------	---	---	--

WG Recommendation 14. Document for 1st CD

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

Document	Project	Title
WG 3 N1971	23837-1	Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements
WG 3 N1972	23837-2	Security requirements, test and evaluation methods for quantum key distribution – Part 2: Test and evaluation methods

WG Recommendation 15. 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 N1968	22216	Introductory guidance on evaluation for IT security

WG Recommendation 16. Document for further DTR

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 N1973	24485	Security properties, test and evaluation guidance for white box cryptography

WG Recommendation 17. 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 N1974	29128	Verification of cryptographic protocols

WG Recommendation 18. 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 N1967	20897-2	Physically unclonable functions – Part 2: Test and evaluation methods

WG Recommendation 19. Document for 1st FDIS

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

Document	Project	Title
WG 3 N1958	15408-1	Evaluation criteria for IT security – Part 1: Vocabulary, introduction and general model #
WG 3 N1959	15408-2	Evaluation criteria for IT security – Part 2: Security functional components
WG 3 N1960	15408-3	Evaluation criteria for IT security – Part 3: Security assurance components
WG 3 N1961	15408-4	Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities
WG 3 N1962	15408-5	Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements
WG 3 N1963	18045	Methodology for IT security evaluation

Subject to approval of WG Recommendation 13

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 N1964	19989-1	Criteria and methodology for security evaluation of biometric systems – Part 1: Framework
WG 3 N1965	19989-2	Criteria and methodology for security evaluation of biometric systems – Part 2: Biometric recognition performance
WG 3 N1966	19989-3	Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection
WG 3 N1969	23532-1	Requirements for the competence of IT security testing and evaluation laboratories – Part 1: Evaluation for ISO/IEC 15408 #
WG 3 N1970	23532-2	Requirements for the competence of IT security testing and evaluation laboratories – Part 2: Testing for ISO/IEC 19790

Subject to approval of WG Recommendation 13

WG Recommendation 21. 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 N1947	CCDB	All projects	WG 3 N1960
WG 3 N1951	CCUF	All projects	WG 3 N1901
WG 3 N1931 WG 3 N1949	ITU-T SG 17	20897 23837	SC 27 N21181 SC 27 N21182
WG 3 N1940	ITU-T FG-QIT4N	23837	WG 3 N1890
WG 3 N1942	ETSI ISG QKD	23837	WG 3 N1779

Resolution A Very special thanks to Krystyna Passia

ISO/IEC JTC 1/SC 27/WG 3 gives a big thanks to the SC 27 Committee Manager Krystyna Passia for her efficient and professional work and support during the meeting. It also expresses its appreciation for the superb work she has provided to SC 27 and WG 3 since 1996.

WG3 wishes her all the best for her retirement. All her friends and colleagues in WG3 will dearly miss her.

High Volume Acclamation

Resolution B Thanks to the SC 27 Committee Manager

ISO/IEC JTC 1/SC 27/WG 3 thanks Krystyna Passia and Sobhi Mahmoud for their 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, Kwangwoo Lee and Junning Yao for drafting the recommendations.

Acclamation

Resolution D 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 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.

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 Convenor.

Acclamation