ISO/IEC JTC 1/SC 27/WG 3 **N 2487**

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, Redmond April 17th – 21st, 2023

Document type	Related content	Document date	Expected action
Meeting / Minutes	Meeting: Redmond (United States) 17 Apr 2023	2023-04-25	**INFO**

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

79th Meeting, Redmond, Washington, USA

April 17th – 21st, 2023

All recommendations are approved UNANIMOUSLY unless otherwise noted.

WG Recommendation 1. Acceptance of minutes

ISO/IEC JTC 1/SC 27/WG 3 recommends accepting the minutes of ISO/IEC JTC 1/SC 27/WG 3 of the 78th virtual meeting, October 3rd – 6th 2022, in document WG 3 N2409.

WG Recommendation 2. Appointment of the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 recommends appointing Kwangwoo Lee, Mike Grimm and Graham Costa as Drafting Committee of the meeting and instructs them to prepare the draft WG recommendations document for WG 3.

WG Recommendation 3. Cancellation of Project

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

Title (and N-Nr, if any)	Justification
PWI 5896 Cybersecurity assurance of systems and system of systems (SoS)	Move to NP
PWI TS 20540 Information technology — Security techniques — Testing cryptographic modules in their operational environment	Move to Revision

WG Recommendation 4. Call for editors

ISO/IEC JTC 1/SC 27/WG 3 recommends circulating a call for editors for the following projects. Submissions should reach the WG 3 Secretariat by the due date identified below.

Project	Title	To be sent to/by
20540	Information technology — Security techniques — Testing cryptographic modules in their operational environment	WG 3 Secr/ 2023-09-15

WG Recommendation 5. Approval of Project Editors/Co-Editors

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

Project	Name (Country)
ISO/IEC 19792	Asahiko YAMADA (JP) Julien BRINGER (FR) *
ISO/IEC 19896-1	Heebong CHOI (KR)

Project	Name (Country)
	Stiepan KOVAC (LU) * John DIMARIA (CSA) * Carolyn FRENCH (CA) *
ISO/IEC 19896-3	Helge KREUTZMANN (DE) Henry TAN (SG) * Robert LEE (SG) * Carolyn FRENCH (CA) *
ISO/IEC TS 20540	Heebong CHOI (KR) Seunghwan YUN (KR) *
ISO/IEC 29128-2	Ritu-Ranjan SHRIVASTWA (FR) Carolyn FRENCH (CA) *
ISO/IEC 29128-3	Ritu-Ranjan SHRIVASTWA (FR) Carolyn FRENCH (CA) *

* Co-editor

WG Recommendation 6. Preparation of Documents

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

Document	Project No.	Title	To be sent to/by
WG 3 N2296	19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	WG 3 Secr. 2023-06-30
WG3 N2485	20540	Information technology — Security techniques — Testing cryptographic modules in their operational environment	WG 3 Secr. 2023-06-30
WG 3 N2193	29128-2	Information security, cybersecurity and privacy protection – Verification of Cryptographic Protocols – Part 2: Evaluation Methods and Activities for Cryptographic Protocols	WG 3 Secr. 2023-06-30
WG 3 N2194	29128-3	Information security, cybersecurity and privacy protection – Verification of Cryptographic Protocols – Part 3: Evaluation Methods and Activities for Protocol Implementation Verification	WG 3 Secr. 2023-06-30

WG Recommendation 7. Updating of documents

ISO/IEC JTC 1/SC 27/WG 3 recommends 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 N2478	17825	Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	SC 27 Secr. 2023-06-30	WG 3 N2477
WG 3 N2479	19790	Information technology — Security techniques — Security requirements for cryptographic modules	SC 27 Secr. 2023-06-30	WG 3 N2470
WG 3 N2480	19792	Information technology — Security techniques — Security evaluation of biometrics	WG 3 Secr. 2023-06-30	WG 3 N2475
WG 3 N2481	19896-1	IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements	WG 3 Secr. 2023-06-30	WG 3 N2458
WG 3 N2482	19896-2	IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers	WG 3 Secr. 2023-06-30	WG 3 N2459
WG 3 N2483	24462	Information security — Security techniques — Ontology building blocks for security and risk assessment *	SC 27 Secr. 2023-04-24	
WG 3 N2484	24759	Information technology — Security techniques — Test requirements for cryptographic modules	SC 27 Secr. 2023-06-30	WG 3 N2471
WG 3 N2382	--	WG 3 Roadmap	WG 3 Secr. 2023-06-30	

* Subject to approval of title change

WG Recommendation 8. Documents for Study and Comment

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

Document	**Project**	**Title**	**Comments Due date**
WG 3 N2480	19792	Information technology — Security techniques — Security evaluation of biometrics	2023-09-15
WG 3 N2481	19896-1	IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction,	2023-09-15

		concepts and general requirements	
WG 3 N2482	19896-2	IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers	2023-09-15
WG 3 N2296	19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	2023-09-15
WG3 N2485	20540	Information technology — Security techniques — Testing cryptographic modules in their operational environment	2023-09-15
WG 3 N2193	29128-2	Information security, cybersecurity and privacy protection – Verification of Cryptographic Protocols – Part 2: Evaluation Methods and Activities for Cryptographic Protocols	2023-09-15
WG 3 N2194	29128-3	Information security, cybersecurity and privacy protection – Verification of Cryptographic Protocols – Part 3: Evaluation Methods and Activities for Protocol Implementation Verification	2023-09-15
WG 3 N2382	--	WG 3 Roadmap	2023-09-15
WG 3 N2469		XML catalogue of ISO/IEC 15408 SFRs/SARs and ISO/IEC 18045 WUs	2023-06-15
WG 3 N2486		Questions on side channel attacks from expert Stiepan A. KOVAC	2023-09-15

WG Recommendation 9. New Work Item

ISO/IEC JTC 1/SC 27/WG 3 recommends the SC 27 Secretariat to submit the following NP.

Title (and N-Nr, if any)
Cybersecurity evaluation of complex systems – Introduction and framework overview (WG3 N2461)

WG Recommendation 10. Revision of ISO/IEC TS 20540:2018

ISO/IEC JTC 1/SC 27/WG 3 recommends SC 27 to note WG3 N2464 and approve a revision of ISO/IEC 20540:2018.

- development track (18, 24, 36 months): 36 months
- project editor(s): Heebong CHOI (KR),
  Seunghwan YUN (KR) *
  * co-editor
- WG in charge: WG3
- the current scope is confirmed
- the project is starting at stage: (20.20)

Project plan (target dates):

- Circulation of first WD (20.20) (if any): 2023-06-01
- Circulation of CD (30.20) (if any): 2024-06-01
- Submission of DIS (40.00): 2025-06-01
- Publication: 2026-06-01

WG Recommendation 11. Document for DTS

ISO/IEC JTC 1/SC 27/WG 3 recommends the SC 27 Secretariat to register the following document as DTS to circulate for balloting.

Document	Project	Title
WG 3 N2483	24462	Information security — Security techniques — Ontology building blocks for security and risk assessment *

* Subject to approval of title change

WG Recommendation 12. Documents for DIS

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

Document	Project	Title
WG 3 N2479	19790	Information technology — Security techniques — Security requirements for cryptographic modules
WG 3 N2484	24759	Information technology — Security techniques — Test requirements for cryptographic modules

WG Recommendation 13. Documents for FDIS

ISO/IEC JTC 1/SC 27/WG 3 recommends the SC 27 Secretariat to register the following document as FDIS to circulate for balloting.

Document	Project	Title
WG 3 N2478	17825	Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

WG Recommendation 14. Title Changes

ISO/IEC JTC 1/SC 27/WG 3 recommends changing the title of following projects.

Project	Current Title	New Title	Justification
ISO/IEC TS 24462	Ontology for ICT Trustworthiness Assessment	Information security — Security techniques — Ontology building blocks for security and risk assessment	The editors are requesting the title change because the new title better reflects the contents of the TS and the original scope of the TS.

WG Recommendation 15. Liaison Statements

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

Document	To	Topic	Reference
WG 3 N2468	CCDB	All projects	WG3N2404、 WG3N2421
WG 3 N2466	CCUF	All projects	WG3N2439
WG 3 N2467	CMUF	19790, 24759	WG3N2436
WG 3 N2474	SC 37	19792	
WG 3 N2472	SC 28	15408, 18045	WG3N2440

WG Recommendation 16. Future meeting schedule

ISO/IEC JTC 1/SC 27/WG 3 agrees to the following meeting arrangements. Any other meetings will be notified no later than four weeks before the meeting.

Date	Meeting	Location
2023-06 (Date: TBD)	Ad-hoc editing meeting for 1st DTS 24462 Information security — Security techniques — Ontology building blocks for security and risk assessment	Zoom

WG Recommendation 17. Availability of ISO/IEC 15408 and ISO/IEC 18045 at no cost

ISO/IEC JTC 1/SC 27/WG 3, considering WG 3 N2449 "Request for freely available standards-ISO/IEC 15408" and WG 3 N2450 "Request for freely available standards-ISO/IEC 18045", recommends its Committee Manager to take appropriate action to make ISO/IEC 15408 and ISO/IEC 18045 available at no-cost from the ISO website:

https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

WG Recommendation 18. Correction of ISO/IEC 15408:2022 (multipart) and ISO/IEC 18045:2022 legal notices

ISO/IEC JTC 1/SC 27/WG 3 recommends to correct two organization names (See below the bold text for the additions) in the Legal notice section of ISO/IEC 15408:2022 (multipart) and ISO/IEC 18045:2022, as requested by the CCDB.

Spain Ministerio de Asuntos Económicos y Transformación Digital and **Centro Criptológico Nacional**

United States The National Security Agency and **the National Institute of Standards and Technology**

Resolution A Thanks to the SC 27 Committee Manager

ISO/IEC JTC 1/SC 27/WG 3 thanks Katharina Kursch, Sobhi Mahmoud, Christine Fries and Alexander Zimmermann for their efficient 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 Kwangwoo Lee, Mike Grimm and Graham Costa for drafting the recommendations.

Acclamation

Resolution C 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 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, 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
Jihoon CHO Sylvain GUILLEY You Sung KANG	24485	Information security, cybersecurity and privacy protection — Security techniques — Security properties and best practices for test and evaluation of white box cryptography
Carolyn FRENCH	29128-1	Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework

Acclamation

Resolution E Thanks to the Host

ISO/IEC JTC1/SC 27/WG 3 expresses its appreciation to the following teams, for supporting the SC 27 WG meetings in Redmond.

Microsoft - Facilities

Cheri Williams and Cheri Doyle – Eventions/Compass Group

Eventions Catering team

Robert McColley and the Allied Security team

Stewart Transportation

Eugene Muller - Building 92 Lobby Concierge

Chad Guse - Building 92 Concierge Team

AV Team Support (Erin Fuhrman, John Uchytil, Bill Lord, Greg Peck, Brianna Daniels, Bill Foreman, Brendan Saur, Cameron Beaty)

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