

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

Convenorship: UNE

Convenor: Bañón Miguel Mr



WG3_LIAISON_STATEMENT_TO_CCUF_Redmond_April_2023_V0.1

Document type	Related content	Document date	Expected action
Project / Other	Meeting: Redmond (United States) 17 Apr 2023	2023-04-20	INFO

Description

This document was presented and approved at the 2022 April WG 3 meeting. It is being circulated for information.

LIAISON STATEMENT

FROM: ISO/IEC JTC 1/SC 27/WG 3
TO: The CCUF

Appreciation

ISO/IEC JTC 1/SC 27/WG 3 thanks the CCUF for their liaison statement circulated as ISO/IEC JTC 1/SC 27/WG 3 N2439 dated 14th April, 2023. The WG 3 thanks to the CCUF for the updates of organization status, scope of interest, and the dates of its forthcoming meetings. These are noted and WG 3 requests that the CCUF continue to include information about their future meetings in their future liaison statements.

Preliminary work item: “Investigation of the feasibility and implementation of changes to ISO/IEC 15408 and ISO/IEC 18045”

The aim of project “PWI 19562: *Investigation of the feasibility and implementation of changes to ISO/IEC 15408 and ISO/IEC 18045*” was to cover any work needed to gain consensus within SC 27 / WG 3 for both the contents and the implementation of the changes. It provides the overall coordination and project management needed to ensure a coherent set of changes and smooth, successful set of revision to the ISO/IEC 15408 and ISO/IEC 18045.

SC 27/WG 3 thanks the CCUF contribution to PWI 19562 that was circulated as ISO/IEC JTC 1/SC 27/WG3 N2448 dated 14 April, 2023. Overall, WG 3 received 42 comments (13 editorial comments and 29 technical comments) and additional contribution during the conversion of the ISO/IEC 15408-2:2022 and ISO/IEC 15408-3:2022 to asciidoc files. This conversion effort has identified some mistakes in the current version. WG 3 has aligned that these contributions will be considered as an input of next ISO/IEC 15408 and ISO/IEC 18045 revision and/or future changes.

In addition, the draft XML versions of the catalogue - type parts of ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC18045 have been produced by WG 3 Convenor, together with equivalent versions in Microsoft Word format. These will be supplied via liaison and comments/corrections are welcomed. Some omissions from the standards were identified during the production of XML files and these will be included in the work on PWI 19562.

WG 3 also requested that the committee manager make ISO/IEC 15408 and ISO/IEC 18045 available at no-cost from the ISO website as agreed. An SC27 meeting in June 2023 will consider widening the applicability of the approach (e.g., other related documents/standards such as the work on patch management) and to longer term outputs (e.g., to subsequent versions). In addition, the request for correction of names in Legal notice Sections of ISO/IEC 15408:2022 (all parts) and ISO/IEC 18045:2022 has been passed to the relevant ISO editors for action.

WG 3 will contribute to discuss the future roadmap of the revision of ISO/IEC 15408 and ISO/IEC 18045. In addition, WG 3 would welcome inputs from the CCUF at any point and, in particular, any suggestions arising from their use of the updated standards.

Notice of publication

The followings have been published and is now available through the National Standard Bodies, ISO and IEC.

- ISO/IEC TR 24485: “*Information security, cybersecurity and privacy protection — Security techniques — Security properties and best practices for test and evaluation of white box cryptography*”

- ISO/IEC 29128-1: "*Information security, cybersecurity and privacy protection —Verification of cryptographic protocols – Part1: Framework*"

Current status on specific projects: cryptographic modules

The ISO/IEC 19790:2012 ("*Security requirements for cryptographic modules*") is currently under revision. It specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication system. ISO 19790 defines four security levels for cryptographic module to provide for a wide spectrum of data sensitivity and diversity of application environments. ISO/IEC 19790 specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

The ISO/IEC 24759:2017 ("*Test requirements for cryptographic modules*") is also currently under revision, in parallel to ISO/IEC 19790. It specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories. It also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790.

Summary of the ISO 19790 and 24759 experts editing sessions

The total comments on 19790 is 301 and the total comments on 24759 is 151. Due to the number of comments received, the editing team did not review comments individually during the editing sessions with the WG3 Experts. The comments marked by the editing team as "for discussion" prior to the WG3 meetings in Redmond or requested by an expert were discussed.

The editing team grouped the comments into the following topic: Exiting degraded mode, Manufacturer SSPs, Error state for all of module vs subset of module, Maintenance Role zeroization, Introduction of tamper indicators, Definition of Operational Environment, Load Test, Audit mechanism service, Interconnection protection, Physical security at level 4, SSPs used in Approved functions, Attestation, EFT and EFP requirements (requested by an expert).

The editing team prepared slides for the topics they marked for discussion and presented options to address the group of related comments under the same topic. Experts at the editing sessions provided their feedback. The best effort is demonstrated to seek consensus. The next step of these two standards is to advance to DIS stage.

General

We look forward to continuing the rewarding relationship with the CCUF and encourage the CCUF to provide any CCUF work items that the working group may consider for review. Please note that the latest status of all WG 3 projects, the relevant document numbers, and the schedule for updates and comments are all to be found in the WG 3 recommendations document that is attached to this liaison statement. Documents of interest to the CCUF are made available through the liaison channel with SC 27/WG 3.

Future meetings

WG 3 includes information regarding its future meetings and would like to inform the CCUF of the following events planned for remaining 2023.

- 16-20 October 2023, The 80th ISO/IEC JTC 1/SC 27/WG 3 meeting, Virtual

Attachments

ISO/IEC JTC 1/SC 27/WG 3 Recommendations, 79th Meeting

Regards,

Liaison Officer from SC 27/WG 3 to the CCUF
Kwangwoo Lee