



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

Convenorship: UNE

Convenor: Bañón Miguel Mr



## ToR for PWI Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045

Document type	Related content	Document date	Expected action
Project / Other	Meeting: <a href="#">VIRTUAL 12 Apr 2021</a>	2021-04-27	<b>COMMENT/REPLY</b> by 2021-09-10

### Description

This document was presented and approved at the 2021 April WG 3 meeting. It is being circulated for calling for contributions.

# Preliminary Work item: Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045

15 April 2021

## Motivation

During the recent revision of ISO/IEC 15408 and ISO/IEC 18045 the editors identified a number of aspects (highlighted in bold below) that could benefit from further consideration. A discussion with experts, of these and other items, was held during the WG3 meeting on 12 April 2021 and several topics were noted as to be addressed (in the priority order proposed by the editors):

1. **Simplification:** improve the comprehension and the use of the standard:
  - a. The repetitive/duplicative nature of the documents<sup>1</sup> makes it very hard to maintain their consistency when updating (especially when using a word processor for editing rather than a more structured document production system),
  - b. improvements to the readability and usability of the standard could be made by simplifying concepts and explanations without reducing its value, or making fundamental changes.
2. **Streamlining:** The documents could also be streamlined so that they are more readily applied by specification-based as well as attack-based approaches to evaluations (as described in ISO/IEC TR 22216) supporting both types of use without undesired side effects.
3. **Clarification:** Clearer presentation of requirements separating them from parts of text containing guidelines, explanations and examples, specifically for Part 1. Additionally, work on a unified terminology for all parts, possibly creating a separate part following the advice from ISO Editors, and using results from the Study Period that took place in 2019 on Concepts and Terminology in support to ISO/IEC 15408/18045.
4. Some changes proposed during the initial study period were found to be impractical to implement in the time available and were deferred for later consideration,
5. There are already other SC27 standards making use/proposing the use of at least some parts of ISO/IEC15408 and ISO/IEC18045 - e.g. ongoing work on cloud services, QKD, patch management, verification of cryptographic protocols, etc. - consideration should be given as to how best to take account of those, whether that be through adding further requirements/activities to the standards, or by providing a framework that adapts to the differing needs via supporting documents (placing these, which have been used for many years by the smartcard community for example, on a more formal footing).

## The Proposal

The group of experts proposes to identify and study the various issues raised and assess the feasibility and level of effort involved in addressing these. A roadmap (in the form of a technical report) would be the key output from the study.

---

<sup>1</sup>There are good reasons why the documents are necessarily repetitive/duplicative: - many requirements are hierarchical and are repeated so that an evaluator can see all the requirements needed in one place, requirements are used/described in different ways the most obvious example being that the definition of each assurance component in ISO/IEC15408-3 then needs to be repeated in ISO/IEC1 8045 when describing the evaluator actions to assess whether the component requirement has been met. However ensuring consistency could be much easier and more reliable if a more structured approach were taken (e.g. with important definitions and text defined once and then included automatically wherever used). Possible ways to do this are to use XML and XSLT scripts (as was done in a previous version of the standards) or some other database/scripting approach.

## Call for contributions

The call for contributions has the following aims:

- Without reducing its value, or making fundamental changes, what could be done to make the standard simpler/easier to use? (whether by updating content, layout, format, etc.)
- Can the standard be better structured to reflect significant differences in the use of the standard between different technology areas/evaluation/certification approaches?
- For SC27 and other experts developing documents related to ISO/IEC 15408 /18045/Standards, Technical specifications, Technical reports (e.g. QKD, Patch management, Cloud services, etc.); are there any structural/content changes in ISO/IEC 15408/18045 that would ease/improve implementation?
- For users of the standards and resultant outputs, eg Certifying Schemes, recognition arrangement owners, policy/procurement organisations, developers, and Protection Profile/Security Target authors, are there any structural/content changes in ISO/IEC 15408/18045 that would ease/improve implementation?

Contributions would be welcomed from all sources but particularly from the CCDB and EUCC/ENISA (via respective liaisons) regarding scheme/recognition/general implementation aspects, and from the CCUF regarding general implementation aspects and linkages to wider uses of CC.

Contributions would also be welcomed from other stakeholders such as SDOs.

**NOTE:** Contributions that include examples of implementation detail would be particularly welcome.

## Terms of Reference/process

The ‘rapporteurs’ group will analyse the contributions, including those made previously, together with the simplification, streamlining, and clarification items seen as essential foundations by the editors, and assess the likely effort involved in each. This will result in a draft roadmap for discussion within WG3 (possibly including further consultation with CCDB/CCUF etc.) which would be published as a technical report. The report would be updated appropriately as the ecosystem of users gains practical experience in using the new revisions of ISO/IEC 15408 and ISO/IEC 18045, and as the use of the standards by the security evaluation community evolves.