



ISO/IEC JTC 1/SC 27 **N6496**

ISO/IEC JTC 1/SC 27/WG 3 **N 928**

REPLACES:

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Meeting Report

TITLE: Meeting Report – 15408-2 Drafting Meeting Madrid, 26th to 27th February, 2008
Madrid, Spain

SOURCE: 15408-2 Project Editor (M Nash)

DATE: 2008-02-27

PROJECT: **15408**

STATUS: This document is being circulated for information.

ACTION: FYI

DUE DATE: -

DISTRIBUTION: P, O and L-Members
W. Fumy, SC 27 Chair, M. DeSoete Vice-chair
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenber, WG-Conveners
WG 3 Experts

MEDIUM: Livelink-server

NO. OF PAGES: 1+3

**15408-2 Drafting Meeting
Madrid, Spain
26th to 27th February, 2008
Meeting Report**

1 Objective of Meeting

The current privacy components within ISO/IEC 15408-2 are essentially unchanged from ISO/IEC 15408 2:1999. However, since this time the need for precise specification of functional components has been demonstrated by practical evaluation experience. In addition, WG 3 has received proposals for new and revised privacy components (see SC 27 N5965 and N3992). This generated the need to call this drafting meeting to discuss these issues.

2 Opening of meeting

The meeting opened at 13:00 on Tuesday 26th February.

Mats Ohlin was appointed chairman of the meeting so that the Project Editor could participate freely in the technical discussions. The Project Editor, Mike Nash, agreed to produce this record of the meeting.

3 Roll call of delegates

<u>Germany</u>	Bertolt Krüger, SRC Security Research and Consulting GmbH Miriam Serowy, Bundesamt für Sicherheit in der Informationstechnik
<u>Spain</u>	Miguel Bañón, for Centro Criptológico Nacional
<u>Sweden</u>	Mats Ohlin, FMV
<u>UK</u>	Michael Nash, Gamma Secure Systems Ltd. (Project Editor)
<u>USA</u>	Helmut Kurth, atsec information security corp.

4 Presentation of contributions

Three working papers had been received in advance of the meeting (see WG 3 N923, N925 and N926). In addition a contribution was received from Spain at the meeting (WG 3 N927).

The Project Editor, Mike Nash, reported that WG 3 had been unable to support the introduction of the privacy functional components in SC 27 N5965 into ISO/IEC 15408-2 because, in the opinion of WG 3 experts, they represented the absence of functionality and thus were not evaluable. However, the security concerns represented by the proposed components were valid. Thus a major objective of the meeting was to consider and document possible extensions to the evaluation criteria that would enable such requirements to be

handled by IS 15408 in a suitable way in the future. The contributions received indicated that this was possible, although it required significant additions to the current criteria.

All four papers were then presented by their authors.

5 Discussion

The meeting concluded that a genuine problem existed with the existing criteria, although its scope and impact were wider than just Part 2. Furthermore, the actual deficiency concerned evaluation of architectural properties of a TOE and was not limited purely to privacy requirements. In fact, it applied also to information flow requirements and other similar properties.

The meeting concluded that there were several problems with the privacy components as currently defined:

1. The current specification of the components is in several areas imprecise or not evaluatable; in particular, assignment options are too open.
2. The technical objective of some components (e.g. distribution of trust) is not clear.
3. Some components cannot be evaluated effectively using current ISO/IEC 15408 assurance components and methodology because they rely on proving architectural properties concerning the TOE. This is a defect in the evaluation model of ISO/IEC 15408, not in the privacy requirements or their specification.

The meeting concluded that all these issues needed to be addressed. The problems with specification of the privacy components were really editorial and had no wider impact on other areas of the criteria.

However, the issue of evaluation of architectural properties was a major weakness in the criteria as currently specified. Given the current invitation for proposals to make improvements to the criteria, it was important that this issue was addressed.

6 Further actions

It was agreed to perform four tasks following this meeting:

1. The formal definition of a series of questions on the privacy criteria concerning problems of meaning and specification, as identified in the Nash paper (WG 3 N923).
2. Preparation of answers to the questions from task 1, sufficient to enable the privacy criteria to be reworded unambiguously and in an evaluatable form.
3. The specification of the architectural analysis problem identified in the German, US and Spanish papers, using information flow as a practical example.

4. A specification of a possible solution to the problem specified in task 3, which has sufficient detail to convince other competent experts that it is viable and complete. The solution should also address the problems identified within Part 1 concerning vulnerability analysis and SFRs.

Tasks 3 and 4 may be satisfied in one document.

Offers were received:

- from Mike Nash to perform task 1;
- from Kai Rannenberg to perform task 2;
- from Helmut Kurth to perform tasks 3 and 4, with participation from Bertolt Krüger and Miguel Bañón.

The leader for each task agreed to prepare a status report on their task for presentation at the Kyoto WG 3 Meeting.

The Part 2 Editor, Mike Nash, was instructed to organise an editing session on this topic during the Kyoto WG 3 Meeting to report progress achieved, discuss the technical issues identified, and receive direction on future progress from the WG.

7 Closure of meeting

Mats Ohlin thanked all attendees for their participation in the meeting, and thanked Miguel Bañón of Epoche y Espri for hosting the meeting and other arrangements.

The meeting closed at 13:00 on Wednesday 27th February.