



ISO/IEC JTC 1/SC 27 **N 7798**

ISO/IEC JTC 1/SC 27/WG 3 **N 998**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: other

TITLE: **Report on WG 3 Study Period on tamper protection requirements and evaluation**

SOURCE: Rapporteur (Miguel Bañón)

DATE: 2009-05-08

PROJECT: WG 3 Study Period

STATUS: This document was made available at the 38th SC 27/WG 3 meeting held in Beijing, China, 4th – 8th May 2009. It is circulated within SC 27 for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenberg,
WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 1

Report of ISO/IEC JTC 1/SC 27/WG 3 Study Period on tamper protection requirements and evaluation.

Anti-tampering measures have their application in areas of the IT security field (protection of hardware resources, transport devices for passwords and cryptographic keys, biometric sensor devices etc), and as such are already present in the architectural aspects of ISO/IEC 15408 assurance components (ADV_ARC), and are of relevance to ISO/IEC 19790.

The exclusion from the existing security evaluation criteria of hardware countermeasures has created a grey area, in some cases clarified by the application of technology specific supporting documents, as is the case in the evaluation of smart cards. In these cases, the hardware-based supporting countermeasures that provide anti-tamper functionality are being specified and addressed as part of the device security evaluation.

The application of security requirements and evaluation using ISO/IEC 15408 is broadening, for example to provide coverage to different regulations and sector specific approval schemes based on similar devices (e.g. passports, id-cards), and also based on different devices (e.g. tachographs, pin-entry devices, points of interaction in payment systems, etc.), all of them having a deep dependency of their provided security in the hardware-based anti-tamper measures.

A study period on tamper protection requirements and evaluation was initiated at the 37th WG 3 meeting in Limassol, as the topic had been identified of interest to be explored in the WG 3 roadmap, and sufficient interest and appropriateness was detected.

This potential new project would have to address the current treatment of hardware based anti-tamper mechanisms in the security evaluation of IT, and how security assurance can be stated for products where the security environment requires the support of such mechanisms, so to harmonize the tamper protection requirements and evaluation with existing SC 27 standards (namely ISO/IEC 15408, ISO/IEC 19790).

The call for contributions was launched in SC 27 N7403, and responses were provided by AU and UK, that are detailed in SC 27 N7604. These were the subject of review and discussion during the Beijing meeting.

Based on the discussion during the Beijing meeting, there was consensus that the development of a Technical Report covering tamper protection requirements and evaluation is feasible, and would facilitate good practice in industry, in particular to complement existing evaluation standards, provided that the required resources are available.

It was also noted that the concurrent development of such a Technical Report with the ongoing review of IS 19790 would facilitate their coordination and compatibility.

It was decided that ensuring now the appropriate scope and availability of resources will expedite the project once started. To this end, as per Resolution 8 (SC 27 N7783), ISO/IEC JTC 1 SC 27/WG 3 has agreed to extend the Study Period in the area of tamper protection requirements and evaluation, and to request the SC 27 Secretariat to circulate a call to National Bodies for contributions and to identify possible editors for a future NWI.