



ISO/IEC JTC 1/SC 27 **N7403**

ISO/IEC JTC 1/SC 27/WG 3 **N981**

REPLACES:

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: call for contributions

TITLE: Call for contributions to WG 3 Study Period on Tamper protection requirements and evaluation

SOURCE: Rapporteur (Miguel Bañón)

DATE: 2009-02-13

PROJECTS: **WG 3 Study Period**

STATUS: As per resolution 11 (see SC27 N7088) of its 37th meeting held in Limassol, Cyprus (Oct. 2008), and in accordance to the SC 27/WG 3 Road Map (see SC27 N5690), SC 27/WG 3 has agreed to initiate a Study Period in the area of Tamper Protection Requirements and Evaluation and to launch a call for contributions to this study period. Some background information regarding the Study Period and intention of this request for contributions are provided in the attachment

The National Bodies and Liaison Organizations of JTC 1/SC 27 are invited to send their contributions to the above-mentioned Study Period directly to the SC27 Secretariat as soon as possible but no later than **2009-04-20**.

ACTION: **COM**

DUE DATE: **2009-04-20**

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. Rannenber, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1+1

Secretariat ISO/IEC JTC 1/SC 27 –

DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany

Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de

[HTTP://www.jtc1sc27.din.de/en](http://www.jtc1sc27.din.de/en)

ISO/IEC JTC 1/SC 27 N7403

WG 3 STUDY PERIOD ON TAMPER PROTECTION REQUIREMENTS AND EVALUATION

Background

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 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 the 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 concerning tamper protection requirements and evaluation has been initiated by ISO/IEC JTC1 SC 27/WG 3. Potential outcomes for the Study Period might include an NWI for a Standard to address this topic area.

The NB's of SC 27 are kindly asked to provide input to this Study Period. Specifically the following issues may be addressed:

- the current treatment to 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;
- the need to provide extensions to existing standards related to the security requirements specification and evaluation criteria to address the relationship between IT and underlying hardware, including security properties and mechanisms, which encompass tamper protection;
- the need to harmonize the tamper protection requirements and evaluation with existing standards (namely ISO/IEC 15408, ISO/IEC 19790), if applicable.