



ISO/IEC JTC 1/SC 27 **N 6650**

ISO/IEC JTC 1/SC 27/WG 3 **N 945**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Dispositions of comments

TITLE: Dispositions of comments on ISO/IEC 19790:2006/DCOR 1
Information technology – Security techniques – Security requirements
of cryptographic modules

SOURCE: 36th SC 27/WG 3 meeting

DATE: 2008-04-16

PROJECT: 19790

STATUS: Output document of the editing session for ISO/IEC
19790:2006/DCOR 1 held during the 36th SC 27/WG 3 meeting
Kyoto, Japan, April 14 – 18, 2008.

This document was available at the above-mentioned meeting. It is
being circulated 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. Rannenber,
WG-Conveners, R. Easter, Project editor, J.-P. Quémard, Co-editor

MEDIUM: Server

NO. OF PAGES: 1 + 1

Attachment 1 to SC 27 N6650

Resolution of comments on ISO/IEC 19790:2006/DCOR 1

Date: 2008-04-16	Document: SC 27 N6650
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
SG	7.8.2.5	Para 2	te	Besides checking the calculated result, additional check shall be conducted to ensure that only newer version is allowed to load. The purpose is to prevent loading older version with known exploitation.	To add in additional check on the software/firmware version. Fail the load test if attempting to load an older version.	Not Accepted: This new requirement can be addressed in the next revision of 19790.