

Draft Technical Corrigendum			
ISO/IEC 19790:2006/DCOR1			
Date: 2007-10-05		Ref. number: ISO/IEC JTC 1/SC27 N6288	
Supersedes document		None	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: 2007-xx-xx Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.		
ISO/IEC 19790:2006/DCOR1			
Title: Information technology -- Security techniques – Security requirements for cryptographic modules			
Draft Technical Corrigendum 1			
Project: 19790/DCOR1			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
Defect Report Proposal	35 th SC 27/WG 3 meeting, Oct. 2007, Resolution xx (Nxxxx)	Defect Report (SC27 N6043)	Text f. 19790:2006/DCOR1 (N6288)
DTC Consideration			
In accordance with resolution xx (see SC 27 Nxxxx) of the 35 th SC 27/WG 3 meeting held in Lucerne, Switzerland, October 2007, the attached document is hereby submitted for a 3-month DCOR letter ballot closing by 2008-xx-xx			
Medium: Livelink-server			
No. of pages: 1 + 2			

G5 Defect Report

DEFECT REPORT

The submitter of a defect report shall complete the items in Part 2 and shall send the form to the Convener or the Secretariat of the WG with which the relevant editor's group is associated.

The WG Convener or Secretariat shall complete the items in Part 1 and circulate the defect report for review and response by the appropriate defect editing group.

The defect editor shall complete Part 4 and submit the completed report to the Convener or the Secretariat of the WG.

PART 1 - TO BE COMPLETED BY WG SECRETARIAT
DEFECT REPORT NUMBER: 19790:2006/DR4
WG SECRETARIAT:
DATE CIRCULATED BY WG SECRETARIAT:
DEADLINE ON RESPONSE FROM EDITOR:

PART 2 - TO BE COMPLETED BY SUBMITTER
SUBMITTER: National Body of Japan
FOR REVIEW BY: ISO/IEC JTC 1/SC27
DEFECT REPORT CONCERNING ISO/IEC 19790: 2006-03-01
QUALIFIER Missing sub clause
REFERENCES IN DOCUMENT clause 7.8.2
NATURE OF DEFECT The software/firmware load test should be included in the conditional self test. This test was included in 1st WD 19790, however this was deleted during the drafting process of 2nd WD 19790 by mistake.
SOLUTION PROPOSED BY THE SUBMITTER 7.8.2.2 Software/firmware load test. If software or firmware components can be externally loaded into a cryptographic module, then the following software/firmware load tests shall be performed: <ol style="list-style-type: none">1. An Approved authentication technique (e.g., an Approved message authentication code, digital signature algorithm, or HMAC) shall be applied to all validated software and firmware components when the components are externally loaded into a cryptographic module. The software/firmware load test is not required for any software and firmware components excluded from the security requirements of this international standard (refer to clause 7.1).2. The calculated result shall be compared with a previously generated result. If the calculated result does not equal the previously generated result, the software/firmware load test shall fail.

PART 3 - EDITOR'S RESPONSE

As indicated, the software/firmware load test is not included in published ISO/IEC 19790. This text was inadvertently dropped during the drafting of the early working document. This item is accepted as a technical defect and will proceed to resolution in this manner. The proposed text is accepted as follows:

7.8.2.5 Software/firmware load test

If software or firmware components can be externally loaded into a cryptographic module, then the following software/firmware load tests shall be performed:

1. An Approved authentication technique (e.g., an Approved message authentication code, digital signature algorithm, or HMAC) shall be applied to all validated software and firmware components when the components are externally loaded into a cryptographic module. The software/firmware load test is not required for any software and firmware components excluded from the security requirements of this international standard (refer to clause 7.1).
2. The calculated result shall be compared with a previously generated result. If the calculated result does not equal the previously generated result, the software/firmware load test shall fail.