



ISO/IEC JTC 1/SC 27 **N6167**

ISO/IEC JTC 1/SC 27/WG 3 **N 907**

REPLACES:

ISO/IEC JTC 1/SC 27

Information technology – Security techniques

Secretariat: DIN, Germany

**DOC. TYPE:** Dispositions of comments

**TITLE:** Disposition of comments on Defect Report to ISO/IEC 19790:2006-03-01 -- Information technology -- Security techniques -- Security requirements for cryptographic modules

**SOURCE:** Project editor Randall Easter, co-editors Jean-Pierre Quémard and Hans von Sommerfeld

**DATE:** 2007-10-05

**PROJECT:** 19790

**STATUS:** Output document of the editing session for Defect Report to ISO/IEC 19790:2006-03-01 (SC 27 N 6043) held during the 35<sup>th</sup> SC 27/WG 3 meeting Lucerne, Switzerland, October 1 – 5, 2007.

**ACTION:** FYI

**DUE DATE:**

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

**MEDIUM:** Livelink-server

**NO. OF PAGES:** 1 + 5

## 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.

<b>PART 1 - TO BE COMPLETED BY WG SECRETARIAT</b>
DEFECT REPORT NUMBER: 19790:2006/DR1
WG SECRETARIAT:
DATE CIRCULATED BY WG SECRETARIAT:
DEADLINE ON RESPONSE FROM EDITOR:

<b>PART 2 - TO BE COMPLETED BY SUBMITTER</b>
SUBMITTER: <a href="#">National Body of Japan</a>
FOR REVIEW BY: <a href="#">ISO/IEC JTC 1/SC27</a>
DEFECT REPORT CONCERNING <a href="#">ISO/IEC 19790: 2006-03-01</a>
QUALIFIER <a href="#">Inconsistency</a>
REFERENCES IN DOCUMENT <a href="#">Clause 3 (Terms and definitions)</a>
NATURE OF DEFECT <a href="#">The contents of clause 3 in WD 24759 (Terms and definitions) were the copy of ISO/IEC 19790.</a> <a href="#">However some of the definitions have been revised so that these two are not identical now.</a>
SOLUTION PROPOSED BY THE SUBMITTER <a href="#">Replace the clause 3 of ISO/IEC 19790 with the clause 3 of the latest 24759.</a>

<b>PART 3 - EDITOR'S RESPONSE</b>
Following an ITTF comment, the terms and definitions found in ISO/IEC 24759 will be removed and replaced with the following text: "For the purposes of this document, the terms and definitions given in ISO/IEC 19790 and the following apply." No change required.

## 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.

<b>PART 1 - TO BE COMPLETED BY WG SECRETARIAT</b>
DEFECT REPORT NUMBER:19790:2006/DR2
WG SECRETARIAT:
DATE CIRCULATED BY WG SECRETARIAT:
DEADLINE ON RESPONSE FROM EDITOR:

<b>PART 2 - TO BE COMPLETED BY SUBMITTER</b>
SUBMITTER: <a href="#">National Body of Japan</a>
FOR REVIEW BY: <a href="#">ISO/IEC JTC 1/SC27</a>
DEFECT REPORT CONCERNING <a href="#">ISO/IEC 19790: 2006-03-01</a>
QUALIFIER <a href="#">clarification required</a>
REFERENCES IN DOCUMENT <a href="#">clause 7.5.2.2</a>
NATURE OF DEFECT <a href="#">The explanation of the voltage range shown below (4th paragraph of clause 7.5.2.2) is difficult to understand.</a> <a href="#">The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs to the smallest positive voltage (with respect to ground) that that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs, including reversing the polarity of the voltages.</a>
SOLUTION PROPOSED BY THE SUBMITTER <a href="#">The voltage range tested shall be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all CSPs and shall be gradually increasing from a voltage within the normal operating voltage range to a higher voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all CSPs, including reversing the polarity of the voltages.</a>

<b>PART 3 - EDITOR'S RESPONSE</b>
This topic was addressed, discussed, revised and accepted as currently written. RE: ISO/IEC N4238, 22 Oct 2004. Additional clarification will be added to 24759. No change required.

## 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.

<b>PART 1 - TO BE COMPLETED BY WG SECRETARIAT</b>
DEFECT REPORT NUMBER: 19790:2006/DR3
WG SECRETARIAT:
DATE CIRCULATED BY WG SECRETARIAT:
DEADLINE ON RESPONSE FROM EDITOR:

<b>PART 2 - TO BE COMPLETED BY SUBMITTER</b>
SUBMITTER: <a href="#">National Body of Japan</a>
FOR REVIEW BY: <a href="#">ISO/IEC JTC 1/SC27</a>
DEFECT REPORT CONCERNING <a href="#">ISO/IEC 19790: 2006-03-01</a>
QUALIFIER <a href="#">inconsistency</a>
REFERENCES IN DOCUMENT <a href="#">clause 7.7.1</a>
NATURE OF DEFECT <a href="#">According to the definition of 'approved', ISO/IEC 19790 accepts ISO/IEC approved RBG or the approval authority approved RBG as an approved security function. However there is the sentence that "RBG and its mode of operation shall be compliant with ISO/IEC 18031" in this clause. This does not allow the vendor to implement approved RBG that is approved by approval authority.</a>
SOLUTION PROPOSED BY THE SUBMITTER <a href="#">The functional requirements for RBG shall be compliant with ISO/IEC 18031.</a>

<b>PART 3 - EDITOR'S RESPONSE</b>
This topic was addressed, discussed, revised and accepted as currently written. No change required.

## 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.

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

<b>PART 2 - TO BE COMPLETED BY SUBMITTER</b>
SUBMITTER: <a href="#">National Body of Japan</a>
FOR REVIEW BY: <a href="#">ISO/IEC JTC 1/SC27</a>
DEFECT REPORT CONCERNING <a href="#">ISO/IEC 19790: 2006-03-01</a>
QUALIFIER <a href="#">Missing sub clause</a>
REFERENCES IN DOCUMENT <a href="#">clause 7.8.2</a>
NATURE OF DEFECT <a href="#">The software/firmware load test should be included in the conditional self test. This test was included in 1<sup>st</sup> WD 19790, however this was deleted during the drafting process of 2<sup>nd</sup> WD 19790 by mistake.</a>
SOLUTION PROPOSED BY THE SUBMITTER <a href="#">7.8.2.2 Software/firmware load test.</a> <a href="#">If software or firmware components can be externally loaded into a cryptographic module, then the following software/firmware load tests shall be performed:</a> <ol style="list-style-type: none"><li><a href="#">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).</a></li><li><a href="#">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.</a></li></ol>

<b>PART 3 - EDITOR'S RESPONSE</b>
<a href="#">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.</a>

## 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.

<b>PART 1 - TO BE COMPLETED BY WG SECRETARIAT</b>
DEFECT REPORT NUMBER: 19790:2006/DR5
WG SECRETARIAT:
DATE CIRCULATED BY WG SECRETARIAT:
DEADLINE ON RESPONSE FROM EDITOR:

<b>PART 2 - TO BE COMPLETED BY SUBMITTER</b>
SUBMITTER: <a href="#">National Body of Japan</a>
FOR REVIEW BY: <a href="#">ISO/IEC JTC 1/SC27</a>
DEFECT REPORT CONCERNING <a href="#">ISO/IEC 19790: 2006-03-01</a>
QUALIFIER <a href="#">Misleading description</a>
REFERENCES IN DOCUMENT <a href="#">clause 7.8.2.1</a>
NATURE OF DEFECT <a href="#">The purposes of generation of key pair are limited to key transport or generation and verification of digital signatures. However it should not be limited. Users may generate asymmetric key pairs for other purposes.</a>
SOLUTION PROPOSED BY THE SUBMITTER <a href="#">If a cryptographic module generates asymmetric keys to be used for the approved functions, the pair-wise consistency of the keys shall be verified using a known answer test.</a>

<b>PART 3 - EDITOR'S RESPONSE</b>
The use of asymmetric keys for other purposes is not allowed by ISO/IEC 19790. ISO/IEC 7.8.2.1 addresses the requirement of a pair-wise consistency check only for the allowed purposes of transport or signatures. No change required.