



ISO/IEC JTC 1/SC 27 **N 7795**

ISO/IEC JTC 1/SC 27/WG 3 **N 995**

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: output letter

TITLE: Letter to NIST on FIPS 140-3 and early revision of IS 19790

SOURCE: 38th SC 27/WG 3 meeting

DATE: 2009-05-04

PROJECT: 19790

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. Rannenber, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Cita Furlani,

The International Standards Organization (ISO) published ISO/IEC 19790, *Security requirements for cryptographic modules*, in March 2006. This document was based on the US Federal Information Processing Standard (FIPS) 140-2. Following this development, ISO published ISO/IEC 24759, *Test requirements for cryptographic modules* in July 2008 which was based on the US FIPS 140-2 *Derived Test Requirements*.

We understand the FIPS 140-3, which is a revision of FIPS 140-2, is under development at NIST based on the Federal Register Notice published January 2005. Therefore ISO/IEC JTC1 SC27 WG3 proposed and agreed to an early revision of ISO/IEC 19790 after its initial publication. The US National Body (NB) submitted the early revision as a new work item (NWI) to SC27 WG3 in the fall of 2007 and this NWI was adopted. Editors (US, France and Japan) were nominated in the fall of 2008 for this effort. SC27 WG3 then asked for NB contribution to start the task with the understanding that the US NB would submit a pre-draft of 2nd draft of FIPS 140-3. Unfortunately the US NB was unable to submit FIPS 140-3, a draft or a pre-draft for the fall 2008 meeting and consideration by WG3 experts. However the US NB suggested that a pre-draft of FIPS 140-3 could be provided to WG3 early spring 2009 for working group review and comment. Again the US NB was unable to deliver. It is understood that there were reorganizational changes in the NIST Computer Security Division and work was continuing on US NIST resolution of comments received on the 1st public draft of FIPS 140-3 which was published July 2007.

Based on the 1st draft of FIPS 140-3, ISO and national bodies are very interested in contributing ideas and feedback on the FIPS 140-3 development and later development of an international standard based on the US FIPS. We would like to suggest and encourage NIST and SC27 WG3 cooperation in the development effort by providing expert feedback and comment. We understand there may be significant changes in the proposed 2nd draft different from the published 1st draft. We hope early involvement and mutual cooperation in the 2nd draft development would not only benefit NIST with expert comments, but also facilitate the adoption of the FIPS 140-3 standard with little revision in the ISO arena.

For example, we have received information that NIST may be ready to release the 2nd draft of FIPS 140-3 in the summer 2009 time period. If this document could also be submitted by the US NB to ISO/IEC JTC1 SC27 WG3 for review and comment by July 6th, 2009, then there would be two forums for the solicitation of comment. The comments received, both by the NIST public posting, and the ISO/IEC JTC1 SC27 WG3 NB review could be reviewed and resolutions generated in close cooperation or joint consolidation. This is one of the ideas we would wish to discuss. We suggest as well holding a joint editing session with your designated editor at our next ISO SC27 WG3 meeting to be in Redmond US on 02-06th November 2009.

We hope you take this under your consideration and look forward to your response.

Thank you.