ISO/IEC JTC 1/SC 27 **N14020**

SC 27/WG 2 SD5

REPLACES:N13232

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: standing document

TITLE: **SC 27/WG 2 Standing Document 5 -- Process for inclusion and deletion of Cryptographic Mechanisms**

SOURCE: Editor (Riaal Domingues), Co-editor (Atsuko Miyaji)

DATE: 2014-04-14

PROJECT: WG 2 SD5

STATUS: **This document is circulated for information.**

PLEASE NOTE: **This document is also freely accessible from the public SC 27 web site at: http://www.jtc1sc27.din.de/sbe/wg2sd5**

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E.J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 1 + 2

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1SC 27.din.de/en

Title: SC 27/WG 2 Standing Document 5 — Process for inclusion and deletion of Cryptographic Mechanisms

Source:WG2

1. Background

If a new cryptographic technique is to be added to a WG2 standard, there is a need to apply a defined process with qualification criteria before the new cryptographic technique is adopted.

Similarly if a standardized cryptographic technique is discovered to have a significant weakness, or a cryptographic technique is no longer believed to be in use anymore, then there is a need to apply a defined process for the deprecation of the cryptographic technique.

This standing document addresses both situations.

2. Introduction Process

The following are the steps to be followed for the introduction of a new cryptographic technique:

a) Proposal: Proposals for addition of a cryptographic mechanism to an International Standard shall be made by a National Body in SC27, or Liaison organisation to SC27. The proposal shall be in writing and shall be circulated for consideration at the next meeting of the working group responsible for the standard at least two months before the meeting.

b) Contents of the proposal: The proposal shall contain a full description of the cryptographic technique to be standardized, as well as all relevant parameters and numerical examples. The proposal shall contain the motivation for adding the cryptographic technique to the standard, and shall also demonstrate that the cryptographic technique meets the minimum criteria set out in the relevant appendix of the proposed standard, if applicable. In a case where the security parameters of the cryptographic technique are quite unusual or are not generally accepted, e.g. specific curve parameters, an analysis that is dedicated to the security of the parameters shall be provided.

c) Study period: After the working group has determined at a meeting that sufficient documentation has been provided, it shall start a study period to consider the standardization of the proposed cryptographic technique. This study period shall have a duration of at least six months. No decision shall be reached on whether to proceed to the next stage of adoption of the proposed cryptographic technique until the end of the study period.

d) Adoption: After all the results of the study period have been made available to all the National Bodies involved in the maintenance of the relevant International Standard at the WG 2 meeting, and a decision can be made to include a particular mechanism(s), the decision shall be recorded in the WG 2 resolutions.

e) Automatic termination: If a cryptographic technique is broken (as defined in the relevant appendix of the standard) during the process of standardization (i.e. during a stage of the standardization process), then the cryptographic technique shall be deleted from the draft.

f) Security analysis information: Upon adoption of new mechanisms, WG2 SD4 shall be updated with appropriate security analysis of the mechanisms. Appropriate text shall be added to the standard to refer the reader to WG2 SD4 for a security analysis of the mechanism.

3. Deprecation Process

The following are the steps to be followed for the deprecation of an existing, standardized cryptographic technique. One of two scenarios may lead to this process being initiated. A compromise of the standardized

cryptographic technique could occur, i.e. an attack against the cryptographic technique is discovered that can lead to a practical attack against a real world system earlier than predicted. Alternatively, a National Body could collect and present evidence that a particular standardized cryptographic technique, while still secure, is no longer used in practice or has never been implemented and used. As a result, standardization is no longer required.

a) SC 27/WG2 confirms the fact of the compromise or ageing of the cryptographic technique and records this in WG2 SD4.

b) WG2 shall determine the severity of the compromise or aging of the cryptographic technique from a). Based on this determination, the decision will be made as to whether adding guidance for the usage of the cryptographic technique is sufficient, or whether the cryptographic technique must be removed from the standard.

    1) When WG2 concludes that additional guidance is needed on the use of the cryptographic technique, appropriate guidance text shall be added to the standard by the process of corrigendum or amendment, as well as recorded in SC 27/SD 12 on the Assessment of encryption algorithms and key lengths or SC 27WG 2 SD4 on Analysis and status of cryptographic algorithms (whichever is appropriate), so that the information is available to users of the standard as soon as possible.

    2) When WG2 concludes that the cryptographic technique should be deleted, this shall be addressed by the process of corrigendum or amendment. In this process, the applicable risks shall be recorded in SC 27/SD 12 on the Assessment of encryption algorithms and key lengths, or SC 27WG 2 SD4 on Analysis and status of cryptographic algorithms (whichever is appropriate).

c) When a cryptographic technique has been deleted by this process, the standard is shall be revised at the next periodical review.

d) If an alternative cryptographic technique is needed by industry, then WG2 shall conduct an early revision of the affected standard.