REPLACES:

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: other document

TITLE: **SC 27 Press Release — A Cautionary Note on the Use of ISO/IEC 18031:2011**

SOURCE: JTC 1 website publicly opened

DATE: 2013-12-06

PROJECT: 1.27.31 (18031)

STATUS: SC 27 press relaese entitled "A Cautionary Note on the Use of ISO/IEC 18031:2011" has recently been published on the JTC 1 website and is accessible from its public section available at www.iso.org/jtc1

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 + 1

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

A Cautionary Note on the Use of ISO/IEC 18031:2011

ISO/IEC 18031:2011 *Information Technology - Security Techniques - Random bit generation* contains a number of random bit generator mechanisms, one of which is known as the Dual_EC_DRBG. In recent months concerns have been expressed about the security of this mechanism. In particular, the concerns relate to the default application specific parameters that are provided in Annex D of this International Standard.

For example, NIST has released a supplemental bulletin giving advice about the use of the same mechanism in NIST Special Publication 800-90A,

(see http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf).

In light of these developments, ISO/IEC JTC 1/SC 27 recommends that users of this standard to take note of these security concerns. ISO/IEC JTC 1/SC 27 has initiated a dedicated Study Period to carefully review the security issues for Dual_EC_DRBG and to revise ISO/IEC 18031 as appropriate. The Study Period will further analyse if other mechanisms in this standard are affected, where similar concerns might be raised due to the specification of default parameter sets.

Updates to this statement will be published as and when further information becomes available. More information regarding progress on this topic can be found in Standing Document 12 of JTC 1/SC 27 on the *Assessment of cryptographic techniques and key lengths* (http://www.jtc1sc27.din.de/sbe/SD12).