INTERNATIONAL STANDARD ISO/IEC 18031:2005
TECHNICAL CORRIGENDUM 1

Published 2009-02-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Random bit generation

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Génération de bits aléatoires

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 18031:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 52, C.2.1.1

Replace the third paragraph from the bottom of the page with the following:

"The length of the *seed* (*seedlen*) shall be at least the maximum of the hash output block size (*outlen*) and the security strength."

ICS 35.040 **Ref. No. ISO/IEC 18031:2005/Cor.1:2009(E)**

Page 53, C.2.1.1

Replace Table C.1 and its title with the following:

Hash-function	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Supported Security Strengths	80, 112, 128	80, 112, 128, 192	80, 112, 128, 192, 256	80, 112, 128, 192, 256	80, 112, 128, 192, 256
Required Minimum Entropy	**max**(120, Security Strength)				
Seed Length (*seedlen*)	440	440	440	888	888

Table C.1 – Security strength table for hash functions

NOTE The description of the function **max**(…) is given in C.2.1.2.1.

Page 54, C.2.1.2.1

Add the following variable and its corresponding description below *max_no_of_states* in the list of variables used in the description of **Hash_DRBG (...)**:

"*max_request_length* The maximum number of pseudorandom bits that may be requested during a single request. This value is implementation dependent."

Page 59, C.2.1.2.4

Replace step 3 of the **Hash_DRBG (…)** function with the following statement:

"3. If (*requested_no_of_bits* > *max_request_length*), then **Return** (Failure message)."

Page 59, C.2.1.2.4

Replace steps 6 to 6.3 of the **Hash_DRBG (...)** function with the following statements:

"6. If ((*reseed_counter* ⩾ *reseed_interval*) OR (*prediction_resistance_request_flag* = *provide_prediction_resistance*)) then:

6.1 If reseeding is not available, then **Return** (Failure message).

6.2 *status* = **Reseed_Hash_DRBG_Instantiation** (*state_pointer*, *additional_input*).

6.3 If (*status* ≠ "Success"), then **Return** (*status*, Null).

6.4 *additional_input* = *Null*."