



**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.”

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

Hash-function	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
<b>Supported Security Strengths</b>	80,	80,	80,	80,	80,
	112,	112,	112,	112,	112,
	128	128,	128,	128,	128,
		192	192,	192,	192,
			256	256	256
<b>Required Minimum Entropy</b>	$\max(120, \text{Security Strength})$				
<b>Seed Length (seedlen)</b>	440	440	440	888	888

**Table C.1 – Security strength table for hash functions**

NOTE The description of the function  $\max(\dots)$  is given in 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.”

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).”

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.”