INTERNATIONAL STANDARD ISO/IEC 18031:2011
TECHNICAL CORRIGENDUM 1

Published 2014-10-01

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 18031:2011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*

ICS 35.040 **Ref. No. ISO/IEC 18031:2011/Cor.1:2014(E)**

Published in Switzerland

Information technology — Security techniques — Random bit generation

Technical Corrigendum 1 to ISO/IEC 18031:2011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

A) Pages 46-50, Annex B.2

Delete the whole of annex B.2.

B) Page 76, Annex C.4.1

On line 3 of C.4.1, delete the sentence 'C.4.2 specifies a DRBG based on elliptic curves'.

C) Pages 76-85, Annex C.4.2

Delete the whole of annex C.4.2.

D) Pages 107-119, Annex D.1

Delete the whole of annex D.1.