INTERNATIONAL STANDARD ISO/IEC 10118-2:2000
TECHNICAL CORRIGENDUM 2

Published 2007-02-15

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 — Hash-functions —

Part 2: Hash-functions using an *n*-bit block cipher

TECHNICAL CORRIGENDUM 2

Technologies de l'information — Techniques de sécurité — Fonctions de brouillage —

Partie 2: Fonctions de brouillage utilisant un chiffrement par blocs de n *bits*

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 to ISO/IEC 10118-2:2000 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. Corrigendum 2 cancels and replaces ISO/IEC 10118-2:2000/Cor.1:2006.

Page iii, Contents

Delete the entries for Annex A and Annex B.

Page iv, Foreword

Delete the last sentence.

Page 1, Clause 2

In the first reference, replace “ISO/IEC 10116:1997” with “ISO/IEC 10116:2006”.

ICS 35.040 **Ref. No. ISO/IEC 10118-2:2000/Cor.2:2007(E)**

© ISO/IEC 2007 – All rights reserved

Published in Switzerland

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Page 2, Subclause 6.4

Delete “(see annex A for guidance)” at the end of the first paragraph.

Page 4, Subclause 7.4

Delete “(see annex A)” at the end of the first paragraph.

Pages 11–18

Delete Annexes A and B.

Page 19, Bibliography

Delete bibliography items [1], [2], [3], [6], [7] and [8] and associated cross-references.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale