



Information technology — Security techniques — Digital signatures with appendix —

Part 3: Discrete logarithm based mechanisms

TECHNICAL CORRIGENDUM 2

*Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice —
Partie 3: Mécanismes basés sur un logarithme discret*

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 to ISO/IEC 14888-3:2006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 50, F.3.4

Replace the numerical example of $h(R||M)$ with the following:

$h(R||M) = 2048680B \ 36D19516 \ CF78E869 \ BEAE7BC9 \ AB5DC543$

Page 52, F.5.1

Replace the first two sentences with the following:

“This example uses RIPEMD-160 as the hash-function h . The hash-code is simply the value of RIPEMD-160.”

Page 53, F.5.2

Replace the first two sentences with the following:

“This example uses the Secure Hash Algorithm (SHA-1) as the hash-function h . The hash-code is simply the value of SHA-1.”