



Information technology — Security techniques — Digital signatures with appendix —

Part 3: Certificate-based mechanisms

TECHNICAL CORRIGENDUM 1

*Technologies de l'information — Techniques de sécurité — Signatures digitales avec appendice —
Partie 3: Mécanismes fondés sur certificat*

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to International Standard ISO/IEC 14888-3:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 2, clause 5

Replace: $[a]$ the greatest integer equal to or less than a

with: $\lceil a \rceil$ the least integer equal to or greater than a

Page 15, subclause B.2.3.4

Replace: $S = K + ((2^{2n}H - U)/PQ \lfloor V \bmod P \rfloor PQ \bmod N$

with: $S = K + ((2^{2n}H - U)/PQ \lceil V \bmod P \rceil PQ \bmod N$