



INTERNATIONAL STANDARD ISO/IEC 14888-3:1998  
TECHNICAL CORRIGENDUM 1

Published 2001-09-15

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

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