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

ICS 35.040 **Ref. No. ISO/IEC 14888-3:1998/Cor.1:2001(E)**

Page 30, subclause E.5.3.3

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

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

Page 30, subclause E.5.3.3

Replace: $S =$

```
53491b7d  54b79d59  a9a16251  e6192609
3336ffb6  368ae323  386360cc  4af5ded3
8a86dd1a  9f3061f7  b66dde43  7d4aa7a1
0b533cb7  89f5c025  d74a4fea  6601fb2e
00241743  fd143a85  6836ba63  d62aa0fe
151636ea  adb8c7c9  cafb5f78  3053227c
0e76bb1b  b889ba2d  73ea27d4  05133979
5502c867  7087de5f  4917f5c8  92a2713f
5f2d0781  ad765763  b930bf8a  0fcb7def
1b38696c  0b072aeb  5f9f03d1  44c07c85
5989bc79  9765836d  20299357  b9b636bc
fb778b07  faeefbff  57d73a5e  6c35fd4e
a31cc4ae  497ea98e  3e07cc00  0368de91
6559069c  a2362bfc  1b7aff82  32c4fe35
707cc105  e0cf460f  62dc0c99  ecf31551
6bbafacc  b4de790c  f55e384a  1901f624
d351bb3f  d3443467  5f53cf13  6ac986fc
0a71fe11  772ba428  fb09967e  c9b9c8dc
```


with: $S =$

```
550d7551  f7450a88  89f613fa  ce3863a7
5182beb1  bc62b354  e6eef81b  45406e5a
033f0b43  b6ad6b60  7f9bcc1e  e9b64292
68e09323  e26c8b96  7174fef0  53c2282e
0884cec9  db5ee394  bbef7659  ff558850
95bb9e8e  fade7893  9b0bc89b  8745d44b
0414ab42  b3f68c85  401da274  9db85b3d
1be33a03  b1ea3e51  b495f474  affdbaeb
c03f89e0  1c86e90e  a4741eb4  1306ef92
eef50e26  001af511  7d145498  aea6513f
0f61c563  e7f8aeac  000d9e21  78cee3f2
4cf9e89f  2c18502e  94f2e7db  ff5a6a0a
41238836  9d6eca74  f59f7d5e  158692ed
305a5203  70fc41fd  8a415b71  b0dc1a72
78921250  f708b910  80eacb6b  055724df
e63fcc5b  44a4a735  fd6ae922  34997db4
44c674ec  975844de  8cecc29c  6ce31931
b3a123a2  9cdab580  b62e06b9  2ca6f72b
```