INTERNATIONAL STANDARD ISO/IEC 14888-2:2008

TECHNICAL CORRIGENDUM 1

Published 2015-10-01

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 2: Integer factorization based mechanisms

TECHNICAL CORRIGENDUM 1: To ISO/IEC 14888-2:2008

Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice —

Partie 2: Mécanismes basés sur une factorisation entière

RECTIFICATIF TECHNIQUE 1: L'ISO/IEC 14888-2:2008

Technical Corrigendum 1 to ISO/IEC 14888-2:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques.*

ICS 35.040 **Ref. No. ISO/IEC 14888-2:2008/Cor.1:2015(E)**

© ISO/IEC 2015 – All rights reserved

Published in Switzerland

AA)

Page 33, 2nd row of Table B.1:

Change "From 750 to 1599" to "From 1024 to 1599".

BB)

Page 52, C.5:

Replace whole C.5 with the following:

C.5 GPS1 scheme

Data elements for signing/verifying – The size of each prime factor is 512 bits. The size of the modulus is 1024 bits. The private bit string consists of $|H| = 160$ bits. The base number is $g = 2$.

p_1=

EAB2E6E3 022960B7 2BE00DDD B4439E87 067B9D2C C0C6DF4F AA2E7CC9 A65E6C3D 4D95ECE7 D983B3C4 EBE812C8 99F050F4 D5D231E0 9399CAB8 6ECFB654 02C0E4EB

p_2=

D115FD6E 67944C3F 407ED927 7D1178A3 A0C01A41 DD446EAC B89CC6BC 2FC01846 5D6C4E74 EDAD1C4E 17BFFBE7 882E3E07 C25AEFF3 3BD59EB1 62AD57B2 CA9717D3

n=

BFB03784 4B667442 37043AF8 16AD20C6 E719F8C0 E18E4A35 E3BFD9B4 7BF63F05 E08CCFDD B89763A2 DBEA6889 D6D17F73 39061A58 02981F10 6461F87E 3DA25C39 154C51A9 8263AE43 8686B21D E53F2AFA A1C4CA8A 040D892C 39A33483 00D69532 E611379F 7C4B7659 95F1FAE4 FA3D33FA 60A71433 2B97422B F508B04C 0E2ACAB1

Q=

F2B65E4B 46BC211F 2A2909B5 77F9BF40 42B49595

G=

B4800C63 F665E640 028C05DB A59D5C4A B221CEB3 26EC5BD0 FB0E3961 28803C04 C40EE4A5 892FE494 86F639E5 429B68FC 1B77B412 AC08E848 AFFD6E39 56666FA7 F098F1BC 61153A9A 475E51EE 90A50F77 98C7068F 7B12A7D4 18916FCC 9B21E186 13E41F1F A106AC57 1B670979 A9FD90D9 5A237208 8C2CAD54 C13CE112 42E1F912

Coupon production – Every coupon (and every first part of signature) is a string of $|H| = 160$ bits; consequently, every random bit string consists of $2|H| + 80 = 400$ bits.

© ISO/IEC 2015 – All rights reserved

r=

DD3B 0C9E9D3C 11F8A12C EF86B279 844FEFB9 1CA37E5E 4D953477 25A6E22E 48938CAF 145B0EE1 9923E1E8 63333BC5 AB37111E

W=

132F2236 49AB1067 1D06D167 D2815583 B075A639 D045009E 52B0E888 6046EEC5 52999E94 7E95EA97 F8C39073 24B3B1CD 8C638B18 012B2FD9 C8AA4BC6 80370FF1 5395986B C6E8DB17 7422974E 0C3F783A A549EE39 61E478E4 BB34CC0E 004D6CB6 72390C78 A26642ED 78828E77 ABEC813D 40F27174 EBAA1A10 5B60FFB1 36A471FD

T=

ACAE249E 1FC4322D D96E98C3 19C9DD28 7E126180

Coupon consumption – The message is a string of 48 octets.

M=

F6D4764A 2B716EEB F31A5EC3 A2A214BF DEA62B53 C11A4D89 CA72E95C BCC15359 70786B89 0C3704E5 D7FE2D45 0771971B

As $T = h(W)$, with SHA-1 in accordance with the third hash-variant, $R = h(h(W) \| M)$ is computed.

R=

2EB8ECA4 021955AC 113BC1C6 80058F99 4EEE51FD

S=

DD3B 0C9E9D3C 11F8A12C C33A9A18 99C00B59 79876097 FE059CC1 C7EC5D77 7AB96A70 5783AC00 72C36AEB 406839A5 24E517DD

Verification – $W^* = G^R \times g^S \bmod n$.

*W**=

132F2236 49AB1067 1D06D167 D2815583 B075A639 D045009E 52B0E888 6046EEC5 52999E94 7E95EA97 F8C39073 24B3B1CD 8C638B18 012B2FD9 C8AA4BC6 80370FF1 5395986B C6E8DB17 7422974E 0C3F783A A549EE39 61E478E4 BB34CC0E 004D6CB6 72390C78 A26642ED 78828E77 ABEC813D 40F27174 EBAA1A10 5B60FFB1 36A471FD

$h(W^*)$=

ACAE249E 1FC4322D D96E98C3 19C9DD28 7E126180

*R**=

2EB8ECA4 021955AC 113BC1C6 80058F99 4EEE51FD

© ISO/IEC 2015 – All rights reserved