INTERNATIONAL STANDARD

ISO/IEC 14888-3

Second edition
2006-11-15

AMENDMENT 2
2012-07-01

Information technology — Security techniques — Digital signatures with appendix —

Part 3:
Discrete logarithm based mechanisms

AMENDMENT 2: Optimizing hash inputs

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

Partie 3: Mécanismes basés sur un logarithme discret

AMENDEMENT 2: Optimisation des entrées pour la fonction de hachage

Reference number
ISO/IEC 14888-3:2006/Amd.2:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 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*.

It introduces an optimization for the Schnorr Elliptic Curve Digital Signature Algorithms specified in ISO/IEC 14888-3:2006/Amd.1:2010. Whereas this optimization is described in an informative (only) note of ISO/IEC 14888-3:2006/Amd.1:2010, Amendment 2 makes the optimization a normative option. It also corrects various errata in Annexes E and F and updates the date of a reference in the Bibliography.

Information technology — Security techniques — Digital signatures with appendix —

Part 3: Discrete logarithm based mechanisms

AMENDMENT 2: Optimizing hash inputs

Subclause 6.9.1, Introduction to EC-SDSA

Replace the text in 6.9.1 with the following:

EC-SDSA (Elliptic Curve Schnorr Digital Signature Algorithm) is a signature mechanism with verification key $Y = [X]G$; that is, the parameter D is equal to 1. The message is prepared such that M_2 is empty and $M_1 = M$ the message to be signed. The witness R is computed as a hash-code of the message M and a random pre-signature $\Pi = [K]G$, by one of two methods, either

normal $R = h(FE2BS(\Pi_X) \,||\, FE2BS(\Pi_Y) \,||\, M)$

or

optimized $R = h(FE2BS(\Pi_X) \,||\, M)$.

The first method generates the witness by hashing the concatenation of the x-coordinate of Π, the y-coordinate of Π and the message M. The second method omits the y-coordinate from the hash calculation and thereby improves performance.

The second method is an optimized variant of EC-SDSA (see [40]).

Subclause 6.9.4.4, Computing the witness

Replace the text in 6.9.4.4 with the following:

The signing entity computes $R = h(FE2BS(\Pi_X)||FE2BS(\Pi_Y)||M)$.

For the optimized variant of EC-SDSA, the signing entity instead computes $R = h(FE2BS(\Pi_X)||M)$.

Annex A, ASN.1 Module

Add the following entries at the appropriate places in the OID assignments section.

```
id-dswa-dl-EC-SDSA-opt OID ::= { id-dswa-dl ec-sdsa-opt(13) }


    dswa-dl EC-SDSA-opt


dswa-dl-EC-SDSA-opt ALGORITHM ::= {
   OID id-dswa-dl-EC-SDSA-opt PARMS HashFunctions
}
```

F.11.2.3, Per message data

Append the following text to F.11.2.3:

For the optimized variant of EC-SDSA,

$R = h(FE2BS(\Pi_X) \,||\, M) =$

```
D7FB8135 D8EA45E8 FB3C9059 F146E263 0EF4BD51 C4006A92
EDB4C8B0 849963FB
```

F.11.2.4, Signature

Append the following text to F.11.2.4:

For the optimized variant of EC-SDSA,

$R =$

```
D7FB8135 D8EA45E8 FB3C9059 F146E263 0EF4BD51 C4006A92
EDB4C8B0 849963FB
```

$S =$

```
B46D1525 379E02E2 32D97928 265B7254 EA2ED978 13454388
C1A08F62 DCCD70B3
```

F.11.2.5, Verification

Append the following text to F.11.2.5:

For the optimized variant of EC-SDSA,

$R' = h(FE2BS(\Pi'_X) \,||\, M) =$

```
D7FB8135 D8EA45E8 FB3C9059 F146E263 0EF4BD51 C4006A92
EDB4C8B0 849963FB
```

F.11.3.3, Per message data

Append the following text to clause F.11.3.3:

For the optimized variant of EC-SDSA,

$R = h(FE2BS(\Pi_X) \,||\, M) =$

```
27D2F5B9 62A3ACF6 390A4718 EA540DA7 9612A60E AA15BEBB
00B9E166 5783F7C7 91CCAC42 2CEE815A 9C5DA367 8AC8D1F0
```

F.11.3.4, Signature

Append the following text to F.11.3.4:

For the optimized variant of EC-SDSA,

$R =$

```
27D2F5B9 62A3ACF6 390A4718 EA540DA7 9612A60E AA15BEBB
00B9E166 5783F7C7 91CCAC42 2CEE815A 9C5DA367 8AC8D1F0
```

$S =$

```
22CC89CE B9E6BE84 15CC14B3 99BC66E6 F3A21E5B A38E09A6
DE8DE670 A145C0E4 74D5CC88 BE8878F0 123CC662 25A1BA12
```

F.11.3.5, Verification

Append the following text to F.11.3.5:

For the optimized variant of EC-SDSA,

$R' = h(FE2BS(\Pi'_X) \| M) =$
```
27D2F5B9 62A3ACF6 390A4718 EA540DA7 9612A60E AA15BEBB
00B9E166 5783F7C7 91CCAC42 2CEE815A 9C5DA367 8AC8D1F0
```

Annex E

To provide a description of the reduced Tate pairing, which is used in examples of Annex F, insert the following clause at the end of Annex E:

E.4 The reduced Tate pairing

Let $l > 2$ be prime, and let P and Q be points on E with $[l]\ P = O$, the pairing $< P, Q >$ can be computed in the following steps:

- choose some random point T on E, then
- compute $<P, Q> = (d(P, Q - T) / d(P, -T))^{(p^k - 1) / l}$.

If during the computation of the pairing, a division by zero is attempted, then the computation should be restarted with a new point T.

NOTE 1 – More detailed information of pairing implementation can be found in [2, 14].

NOTE 2 – The reduced Tate pairing is used in numerical examples of clauses F.7 and F.8.

F.2.2, Signature key and verification key

To correct a one-digit error in the value of Y, in the last line of the formula for Y change "`48CDF8DE`" to "`48CBF8DE`".

F.3, Pointcheval-Vaudenay mechanism

To identify which hash-function is used in the example of F.3, insert the following at the beginning of F.3:

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

F.5.2.1, Parameters

To correct a one-digit error in the value of G_Y, in the formula of G_Y change "`631011EC`" to "`631011ED`".

F.5.3, Example 2: Field F_{P^m}, 32-bit P and m = 5

To correct a minor typographical error in the title of F.5.3, change "Example 2" to "Example 3".

F.7.2.1, Parameters

To correct the polynomial cited in F.7.2.1, change "$Y^2 = X^3 + 1$" to "$Y^2 = X^3 + X$".

F.8.1.1, Parameters

To correct a multiple-digit error in the value of q in F.8.1.1, in the formula of q change

```
80000000 00000000 00FFFFFF FFFFFFFF FFFFFFFF
```

to

```
80000000 000FFFFF FFFFFFFF FFFFFFFF FFFFFFFF.
```

Bibliography

Update reference [3] (ISO/IEC 11770-3) by changing "1999" to "2008".

