

Information technology — Security techniques — Digital signatures with appendix —

Part 3: Certificate-based mechanisms

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 14888-3:1998, including Technical corrigendum 1:2001, and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to iv, pages 1 to 35 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Sidelining in this document indicates the most recent changes by amendment.

Amendments issued since publication

Amd. No.	Date	Comments
13614 Tech. Corr. No. 1	14 May 2002	Indicated by a sideline

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 March 1999

© BSI 14 May 2002

ISBN 0 580 32218 1

Contents

	Page
National foreword	Inside front cover
Foreword	iii
Text of ISO/IEC 14888-3	1

INTERNATIONAL STANDARD

**ISO/IEC
14888-3**

First edition
1998-12-15

Technical corrigendum
2001-09-15

Information technology — Security techniques — Digital signatures with appendix —

Part 3: Certificate-based mechanisms

*Technologies de l'information — Techniques de sécurité — Signatures
digitales avec appendice —*

Partie 3: Mécanismes fondés sur certificat



Contents

	Page
Foreword	iii
1 Scope	1
2 Normative references	1
3 General	1
4 Definitions	2
5 Symbols and notation	2
6 Digital signature mechanisms based on discrete logarithms	3
7 Digital signature mechanisms based on factoring	8
Annex A (normative) Examples of certificate-based digital signatures with appendix based on discrete logarithms	10
Annex B (normative) Example of certificate-based digital signatures with appendix based on factoring	16
Annex C (informative) FIPS PUB 186 Generation of Primes P and Q	19
Annex D (informative) Elliptic Curve mathematical background	20
Annex E (informative) Numerical examples of certificate-based digital signatures with appendix	22
Annex F (informative) Claimed features for choosing a signature scheme	34
Annex G (informative) Patent Information	34
Bibliography	35
Figure 1 — Signature process with randomized witness	6
Figure 2 — Verification process with a randomized witness	7

Foreword

ISO (the International Organization for Standardization) and the 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. 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.

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

ISO/IEC 14888 consists of the following parts, under the general title *Information technology — Security techniques — Digital signatures with appendix*:

- *Part 1: General*;
- *Part 2: Identity-based mechanisms*;
- *Part 3: Certificate-based mechanisms*.

Further parts may follow.

Annex A and Annex B form an integral part of this part of ISO/IEC 14888. Annex C to Annex G are for information only.

1 Scope

ISO/IEC 14888 specifies digital signature mechanisms with appendix for messages of arbitrary length and is applicable for providing data origin authentication, non-repudiation, and integrity of data.

This part of ISO/IEC 14888 specifies certificate-based digital signature mechanisms with appendix. In particular, this part of ISO/IEC 14888 provides 1) a general description of certificate-based digital signature mechanisms whose security is based on the difficulty of the discrete logarithm problem in the underlying commutative group (see Clause 6), 2) a general description of certificate-based digital signature mechanisms whose security is based on the difficulty of factoring (see Clause 7), and 3) a variety of normative digital signature mechanisms with appendix using certificate-based mechanisms for messages of arbitrary length (see Annex A and Annex B).

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 14888. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 14888 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 14888-1:1998, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*.

ISO/IEC 14888-2:1998, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Identity-based mechanisms*.

ISO/IEC 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery*.

ISO/IEC 9796-2:1997, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash-function*.

ISO/IEC 10118-3:1998, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*.

ISO/IEC 10118-4:1998, *Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic*.

3 General

This part of ISO/IEC 14888 makes use of the definitions, symbols, legend for figures, and notation given in ISO/IEC 14888-1.

The verification of a digital signature requires the signing entity's verification key. It is thus essential for a verifier to be able to associate the correct verification key with the signing entity. For certificate-based mechanisms, this association must be provided by some certifying measure, for example, the verification key is retrieved from a certificate.

The goal of this part of ISO/IEC 14888 is to specify the following processes and functions within the general model described in ISO/IEC 14888-1:

- the process of generating keys
 - generating domain parameters
 - generating signature and verification keys
- the process of producing signatures
 - (optional) producing pre-signatures
 - preparing the message for signature
 - computing witnesses
 - computing the signature
- the process of verification
 - preparing message for verification
 - retrieving the witness
 - computing the verification function
 - verifying the witness

4 Definitions

For the purpose of this part of ISO/IEC 14888, the definitions of ISO/IEC 14888-1 apply. Additional definitions which are required are as follows.

4.1

finite commutative group

a finite set J with the binary operation « $*$ » such that:

- For all $a, b, c \in J$, $(a*b) * c = a * (b*c)$
- There exists $e \in J$ with $e*a = a$ for all $a \in J$
- For all $a \in J$ there exists $b \in J$ with $b*a = e$
- For all $a, b \in J$, $a*b = b*a$

4.2

order of an element in a finite commutative group

if $a^0 = e$, and $a^{n+1} = a*a^n$ (for $n \geq 0$), is defined recursively, the order of $a \in J$ is the least positive integer n such that $a^n = e$.

5 Symbols and notation

Throughout this part of ISO/IEC 14888 the following symbols and notations are used in addition to those given in ISO/IEC 14888-1.

E	a finite commutative group
$\#E$	the cardinality of E
$a b$	concatenation of b to a
Q	a divisor of $\#E$
G	an element of order Q in E
$\text{gcd}(U, N)$	the greatest common divisor of integers U and N
T_1	first part of assignment
T_2	second part of assignment
Z_N	the set of integers U with $0 \leq U < N$
Z_N^*	the set of integers U with $0 < U < N$ and $\text{gcd}(U, N) = 1$
$\lfloor a \rfloor$	the least integer equal to or greater than a

6 Digital signature mechanisms based on discrete logarithms

6.1 Key generation process

6.1.1 Generating domain parameters

For digital signature mechanisms based on discrete logarithms, the set Z of domain parameters determines the following parameters:

- a finite commutative group E
- one or more divisors Q of $\#E$
- one or more elements G of order Q in E

In the group E , multiplicative notation is used. The signature mechanism will use one element G in E . It is worthwhile to note that the particular signature mechanism chosen may place additional constraints on the choice of E , Q , and G .

6.1.2 Generation of signature key and verification key

A signature key of a signing entity is a secretly generated random or pseudo-random integer X such that $0 < X < Q$ and $\gcd(X, Q) = 1$. The corresponding public verification key Y is an element of E and is computed as

$$Y = G^X.$$

NOTE It is allowed to exclude a few integers from consideration as possible X values.

In some instances, validation of domain parameters and keys may be required. However, it is outside the scope of this standard.

6.2 Signature process

In this clause the signature process for a class of signature mechanisms is described. Within this class the signature function for the mechanism to be used is specified by a permutation (A, B, C) of (S, T_1, T_2) which determines the coefficients of the signature equation

$$AK + BX + C \equiv 0 \pmod{Q}.$$

This permutation will be specified or agreed upon when setting up the signature system.

The signature process and the formation of a signed message consists of eight stages (see Figure 1):

- producing the randomizer
- producing the pre-signature
- preparing the message for signing
- computing the witness (the first part of the signature)
- computing the assignment
- computing the second part of the signature
- constructing the appendix
- constructing the signed message

In this process, the signing entity makes use of its private signature key X , and the domain parameters E , G , and Q .

6.2.1 Producing the randomizer

The signing entity generates a secret randomizer which is an integer K with $0 < K < Q$ and satisfying $\gcd(K, Q) = 1$. The output of this stage is K , which the signing entity keeps secret.

NOTE It is allowable to exclude a few integers from consideration as possible K values.

6.2.2 Producing the pre-signature

The input to this stage is the randomizer K , with which the signing entity computes

$$\Pi = G^K.$$

in E . The output of this stage is the pre-signature, Π

6.2.3 Preparing the message for signing

The message is split into two parts which will be called data inputs M_1 and M_2 . One of these parts may be empty and the two parts need not be distinct (see ISO/IEC 14888-1 for further details.)

6.2.4 Computing the witness (the first part of the signature)

The variables to this stage are the pre-signature Π from 6.2.2 and M_1 from 6.2.3. The values of these variables are taken as inputs to the witness function. The output of the witness function is witness R .

6.2.5 Computing the assignment

The inputs to the assignment function are the first part of the signature, which is the witness R from 6.2.4, and M_2 from 6.2.3. The output of the assignment function is assignment $T = (T_1, T_2)$ where T_1 and T_2 are integers such that

$$0 < |T_1| < Q, 0 < |T_2| < Q.$$

6.2.6 Computing the second part of the signature

The inputs to this stage are randomizer K from 6.2.1, the signature key X , assignment $T = (T_1, T_2)$ from 6.2.5, the permutation (A, B, C) of (S, T_1 , T_2) and domain parameter Q as specified in 6.1.1. The signing entity forms the signature equation

$$(AK + BX + C) \equiv 0 \pmod{Q}.$$

and solves the signature equation for S , the second part of the signature, where $0 < S < Q$. The pair (R, S) will be called the signature, Σ .

6.2.7 Constructing the appendix

The appendix is constructed from the signature and an optional text field, *text*, as $((R, S), \text{text})$. The text field could include a certificate which cryptographically ties the public verification key to the identification data of the signing entity.

NOTE As indicated in ISO/IEC 14888-1, depending on the application, there are different ways of forming the appendix and appending it to the message. The general requirement is that the verifier is able to relate the correct signature to the message. For successful verification, it is also essential that prior to the verification process, the verifier is able to associate the correct verification key with the signature.

6.2.8 Constructing the signed message

The signed message is obtained by the concatenation of message M and appendix

$$M || ((R, S), \text{text}).$$

6.3 Verification process

The verification process consists of four stages (see Figure 2).

- Preparing message for verification
- Retrieving the witness
- Computing the verification function
 - retrieving the assignment
 - recomputing the pre-signature
 - recomputing the witness
- Verifying the witness

In this process, the verifier makes use of the signer's verification key Y and the domain parameters: finite group E , element G in E and its order Q .

6.3.1 Preparing message for verification

The verifier retrieves M from the signed message and divides the message into two parts M_1 and M_2 .

6.3.2 Retrieving the witness

The verifier retrieves the signature (R, S) from the appendix, and divides it into witness R and the second part of the signature S .

6.3.3 *Computing the verification function*

6.3.3.1 *Retrieving the assignment*

This stage is identical to 6.2.5. The inputs to the assignment function consist of the witness R from 6.3.2 and M_2 from 6.3.1. The assignment $T = (T_1, T_2)$ is recomputed as the output from the assignment function.

6.3.3.2 *Recomputing the pre-signature*

The inputs to this stage are the set Z of domain parameters, the verification key Y , the assignment $T = (T_1, T_2)$ from 6.3.3.1 and the second part of the signature S from 6.3.2. The verifier assigns to the coefficients (A, B, C) the values (S, T_1, T_2) according to the order specified by the signature function, and computes the element $\bar{\Pi}$ in E as

$$\bar{\Pi} = Y^m G^n.$$

where $m = -A^{-1} B \bmod Q$ and $n = -A^{-1} C \bmod Q$.

6.3.3.3 *Recomputing the witness*

The computations at this stage are the same as in 6.2.4. The verifier executes the witness function. The inputs are $\bar{\Pi}$ from 6.3.3.2 and M_1 from 6.3.1.

The output is the recomputed witness $\bar{R}$.

6.3.4 *Verifying the witness*

The signature is verified if the recomputed witness $\bar{R}$ from 6.3.3.3 is equal to R from 6.3.2. Additional checks may be required (see A.1.2.4.6 for other example checks.)

