INTERNATIONAL STANDARD

ISO/IEC 14888-1

Second edition
2008-04-15

Information technology — Security techniques — Digital signatures with appendix —

Part 1: **General**

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

Partie 1: Généralités

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

Reference number
ISO/IEC 14888-1:2008(E)

© ISO/IEC 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

© ISO/IEC 2008 – All rights reserved

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.

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

This second edition cancels and replaces the first edition (ISO/IEC 14888-1:1998), which has been technically revised.

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: Integer factorization based mechanisms*

— *Part 3: Discrete logarithm based mechanisms*

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

© ISO/IEC 2008 – All rights reserved

Introduction

Digital signature mechanisms are asymmetric cryptographic techniques which can be used to provide entity authentication, data origin authentication, data integrity and non-repudiation services. There are two types of digital signature mechanisms:

- When the verification process needs the message as part of the input, the mechanism is called a "signature mechanism with appendix". A hash-function is used in the calculation of the appendix.
- When the verification process reveals all or part of the message, the mechanism is called a "signature mechanism giving message recovery". A hash-function is also used in the generation and verification of these signatures.

Signature mechanisms with appendix are specified in ISO/IEC 14888. Signature mechanisms giving message recovery are specified in ISO/IEC 9796. Hash-functions are specified in ISO/IEC 10118.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

1 Scope

ISO/IEC 14888 specifies several digital signature mechanisms with appendix for messages of arbitrary length.

This part of ISO/IEC 14888 contains general principles and requirements for digital signatures with appendix. It also contains definitions and symbols which are used in all parts of ISO/IEC 14888.

Various means are available to obtain a reliable copy of the public verification key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC 14888. For further information, see ISO/IEC 9594-8 [4], ISO/IEC 11770-3 [3] and ISO/IEC 15945 [5].

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

None.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
appendix
string of bits formed by the signature and an optional text field

3.2
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

NOTE Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1]

3.3
data element
integer, bit string, set of integers or set of bit strings

© ISO/IEC 2008 – All rights reserved

3.4
domain
set of entities operating under a single security policy

EXAMPLES public key certificates created by a single authority or by a set of authorities using the same security policy

3.5
domain parameter
data element which is common to and known by or accessible to all entities within the domain

3.6
hash-code
string of bits which is the output of a hash-function

[ISO/IEC 10118-1]

3.7
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output

NOTE 1 Computational feasibility depends on the specific security requirements and environment.

NOTE 2 This definition of hash-function is referred to as one-way hash-function.

[ISO/IEC 10118-1]

3.8
identification data
sequence of data elements, including the distinguishing identifier for an entity, assigned to an entity and used to identify it

NOTE The identification data may additionally contain data elements such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters.

3.9
key pair
pair consisting of a signature key and a verification key, i.e.,

— a set of data elements that shall be totally or partially kept secret, to be used only by the signer;

— a set of data elements that can be totally made public, to be used by any verifier

3.10
message
string of bits of any length

3.11
parameter
integer, bit string or hash-function

3.12
signature
one or more data elements resulting from the signature process

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

© ISO/IEC 2008 – All rights reserved

3.13
signature key
set of private data elements specific to an entity and usable only by this entity in the signature process

NOTE Sometimes called a private signature key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3.

3.14
signature process
process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

3.15
signed message
set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

NOTE In the context of this part of ISO/IEC 14888, the entire message is included in the signed message and no part of the message is recovered from the signature.

3.16
verification key
set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process

NOTE Sometimes called a public verification key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3.

3.17
verification process
process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid

4 Symbols, conventions, and legend for figures

4.1 Symbols

Throughout all parts of ISO/IEC 14888 the following symbols are used.

H hash-code

K randomizer

M message

R first part of a signature

NOTE First part of a signature R is alternatively called a witness.

$\overline{R}$ recomputed first part of a signature

S second part of a signature

X signature key

Y verification key

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

© ISO/IEC 2008 – All rights reserved

Z set of domain parameters

Σ signature

$A \bmod N$ the unique integer B from 0 to $N - 1$ so that N divides $A - B$

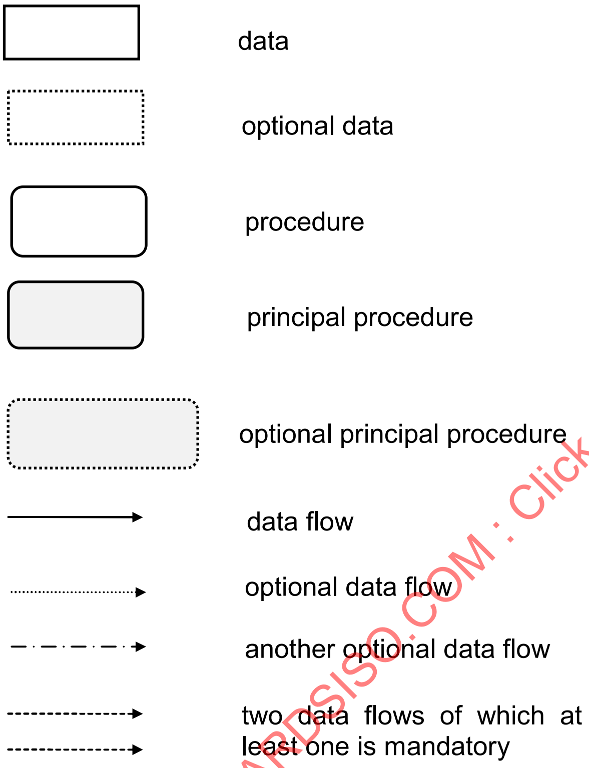
$A \equiv B \pmod{N}$ Integer A is congruent to integer B modulo N, i.e. $(A - B) \bmod N = 0$.

4.2 Coding convention

All integers in all parts of ISO/IEC 14888 are written with the most significant digit (or bit, or byte) in the leftmost position.

4.3 Legend for figures

The following legend for figures is used in all parts of ISO/IEC 14888.


data
optional data
procedure
principal procedure
optional principal procedure
data flow
optional data flow
another optional data flow
two data flows of which at least one is mandatory

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

5 General

The mechanisms specified in ISO/IEC 14888 are based upon asymmetric cryptographic techniques. Every asymmetric digital signature mechanism involves three basic operations.

— A process for generating pairs of keys, where each pair consists of a signature key and the corresponding verification key.

— A process using the signature key called the signature process.

- When, for a given message and signature key, the probability of obtaining the same signature twice is negligible, the operation is probabilistic.

© ISO/IEC 2008 – All rights reserved

- When, for a given message and signature key, all the signatures are identical, the operation is deterministic.

— A process using the verification key called the verification process.

The verification of a digital signature requires the signer's verification key. It is thus essential for a verifier to be able to associate the correct verification key with the signer, or more precisely, with (parts of) the signer's identification data. If this association is somehow inherent in the verification key itself, the scheme is said to be "identity-based". If not, the association between the correct verification key with the signer's identification data shall be provided by a certificate for the verification key. The scheme is then said to be "certificate-based".

6 General model

A digital signature mechanism with appendix is defined by the specification of the following processes:

— key generation process;

— signature process;

— verification process.

In the signature process, the signer computes a digital signature for a given message. The signature, together with an optional text field, forms the appendix, which is appended to the message to form the signed message.

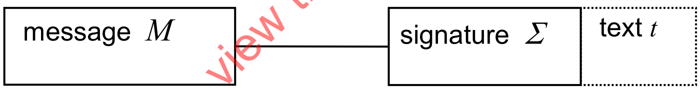


Figure 1 — Signed message

Depending on the application, there are different ways of forming the appendix and associating it with 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. The optional text field can be used for transmitting the signer's identification data or an authenticated copy of the signer's verification key to the verifier. In some cases the signer's identification data may need to be part of the message M, so that it is protected by the signature.

A digital signature mechanism shall satisfy the following requirements:

— Given only the verification key and not the signature key it is computationally infeasible to produce any message and a valid signature for this message.

— The signatures produced by a signer can neither be used for producing any new message and a valid signature for this message nor for recovering the signature key.

— It is computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE Computational feasibility depends on the specific security requirements and environment.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

7 Options for binding signature mechanism and hash-function

Use of the signature schemes specified in this standard requires the selection of a collision-resistant hash-function. There shall be a binding between the signature mechanism and the hash-function in use. Without such a binding, an adversary might claim the use of a weak hash-function (and not the actual one) and thereby forge the signature.

There are various ways to accomplish this binding. The following options are listed in order of increasing risk.

a) Require a particular hash-function when using a particular signature mechanism. The verification process shall exclusively use that particular hash-function;

b) Allow a set of hash-functions and explicitly indicate the hash-function in use in the certificate domain parameters. Inside the certificate domain, the verification process shall exclusively use the hash-function indicated in the certificate. Outside the certificate domain, there is a risk arising from certification authorities (CAs) that may not adhere to the user's policy. If, for example, an external CA creates a certificate permitting other hash-functions, then signature forgery problems may arise. In such a case a misled verifier may be in dispute with the CA that produced the other certificate;

c) Allow a set of hash-functions and indicate the hash-function in use by some other method, e.g., an indication in the message or a bilateral agreement. The verification process shall exclusively use the hash-function indicated by the other method. However, there is a risk that an adversary may forge a signature using another hash-function.

NOTE The 'other method' referred to in item c) immediately above could be in the form of a hash-function identifier which explicitly indicates in a signature in the form of hash-token, a concatenation of a hash-code and a hash-function identifier. If the hash-function identifier is included in this way then an attacker cannot fraudulently reuse an existing signature with a different message, even when the verifier could be persuaded to accept signatures created using a hash-function sufficiently weak that pre-images can be found. However, as discussed in detail in [1] (see also Annex A), using the weak hash-function, an attacker can still find a valid signed message by randomly generating signatures containing the identifier of the weak hash-function.

The user of a digital signature mechanism should conduct a risk assessment considering the costs and benefits of the various alternative means of accomplishing the required binding. This assessment should include an assessment of the cost associated with the possibility of a bogus signature being produced.

8 Key generation

The key generation process of a digital signature mechanism consists of the following two procedures:

- generating domain parameters,
- generating signature key and verification key.

The first procedure is executed once when the domain is set up. The second procedure is executed for each signer within the domain and the outputs are the signature key X and the verification key Y. For a specific set of domain parameters, a value of X, which is different with overwhelming probability from values used previously, shall be used.

NOTE Validation of domain parameters and keys may be required. However, it is outside the scope of this standard.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

© ISO/IEC 2008 – All rights reserved

9 Signature process

9.1 General

The following data elements are required for the signature process:

- domain parameters Z;
- signature key X;
- message M;
- hash-function identifier *hid* (optional);
- other text t (optional).

The hash-function identifier can be used for binding the signature mechanism and the hash-function, see Clause 7.

The signature process of a digital signature mechanism with appendix consists of the following procedures:

- computing signature;
- constructing appendix;
- constructing signed message.

9.2 Computing the signature

The inputs to this procedure are the message M, the signature key X and the domain parameter Z. The output of this step is the signature Σ consisting of the first part of signature R and, depending upon the mechanism, the second part of signature S, see Figure 2.

9.3 Constructing the appendix

The appendix is constructed from the signature and an optional text field, *text*, as (Σ, t). The text field could include a certificate that cryptographically ties the verification key to the identification data of the signer.

NOTE 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.

9.4 Constructing the signed message

The signed message consists of message M and the appendix, i.e., M, (Σ, t).

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

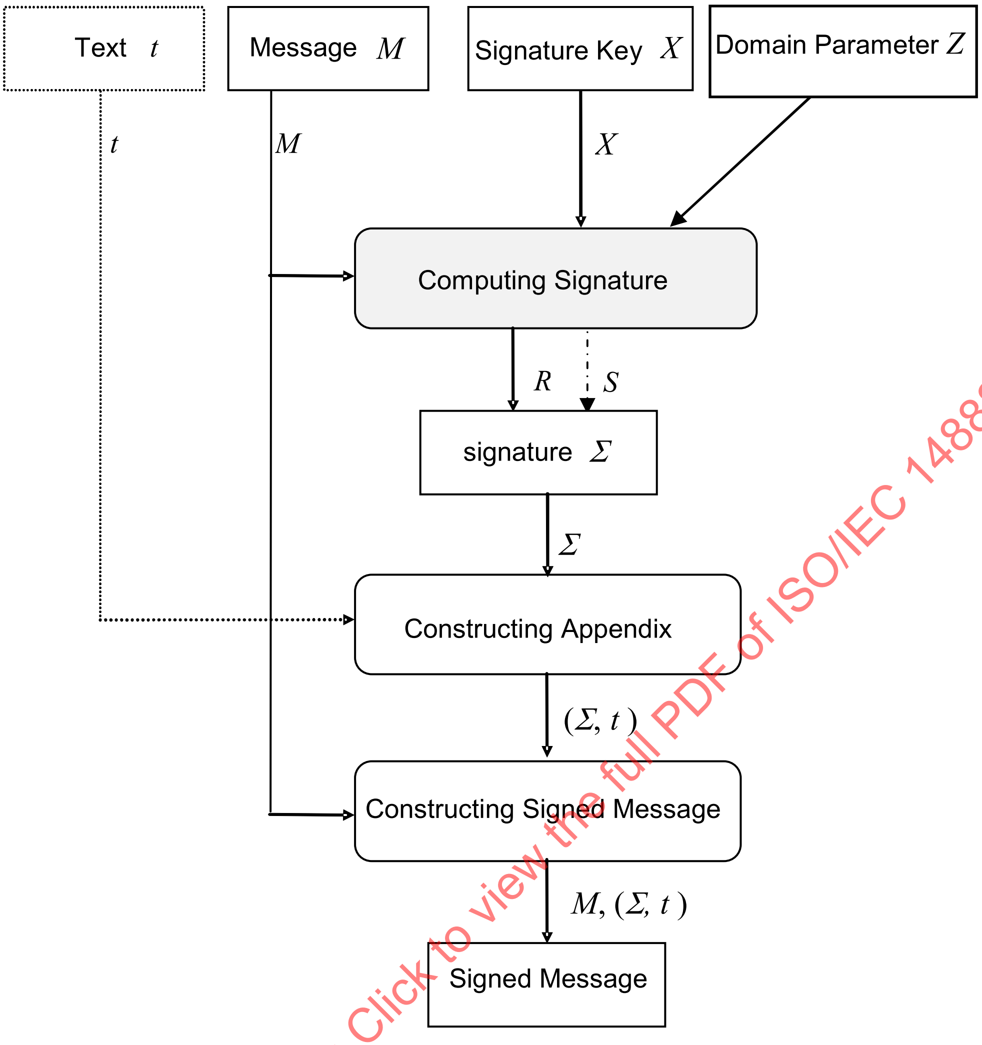


Figure 2 — Signature process

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 14888-1:2008

10 Verification process

The following data elements are required for the verification process:

— domain parameters Z;

— verification key Y;

— message M;

— signature Σ;

— identification data Id (optional);

— identifiers of the hash-functions in use hid, if not uniquely determined by other means (see Clause 7);

— other text t (optional).

© ISO/IEC 2008 – All rights reserved