INTERNATIONAL STANDARD

ISO/IEC 14888-1

First edition
1998-12-15

Corrected and reprinted
1999-12-15

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

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

Partie 1: Généralités

Reference number
ISO/IEC 14888-1:1998(E)

Contents

Page

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. 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 14888-1 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*

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 named a “signature mechanism with appendix”. A hash-function is involved in the calculation of the appendix. ISO/IEC 10118 specifies hash-functions for use in digital signatures with appendix.

— When the verification process reveals the message together with its specific redundancy (sometimes called the shadow of the message), the mechanism is named a “signature mechanism giving message recovery”. Redundancy schemes designed for use as part of such a signature scheme are specified in the multipart standard ISO/IEC 9796.

These two types are not mutually exclusive. Specifically, any digital signature mechanism giving message recovery, for example, the mechanism specified in ISO/IEC 9796, can be used for provision of digital signatures with appendix. In this case, the signature is generated by application of the signature process to a hash-token of the message.

1 Scope

ISO/IEC 1488 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 common to all parts of ISO/IEC 14888.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 1488. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, 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 normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

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 10118-1:1994, *Information technology — Security techniques — Hash functions — Part 1: General.*

ISO/IEC 11770-3:1999, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.*

3 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 of 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.

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

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, or more precisely, with (parts of) the signing entity•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 signing entity’s identification data shall be provided by another means. Whatever the nature of such means, the scheme is then said to be “certificate-based”.

The procedures of validation and management of verification keys in a certificate-based scheme is outside the scope of ISO/IEC 14888. Mechanisms for distribution of public verification keys are provided in ISO/IEC 11770-3.

4 Terms and definitions

For the purposes of ISO/IEC 14888, the following terms and definitions apply.

4.1
appendix
a string of bits formed by the signature and an optional text field

4.2
assignment
a data item which is a function of the witness and possibly of a part of the message, and forms part of the input to the signature function

4.3
collision resistant hash-function
[ISO/IEC 10118-1] a 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.

4.4
deterministic
independent of a randomizer, not randomized

4.5
digital signature
see signature

4.6
domain parameter
a data item which is common to and known by or accessible to all entities within the domain

4.7
hash-code
the string of bits which is the output of a hash-function

4.8
hash-function
[ISO/IEC 10118-1] a 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 Computational feasibility depends on the specific security requirements and environment.

4.9
hash-token
a concatenation of a hash-code and an optional control field, called hash-function identifier, which can be used to identify the hash-function and the padding method

4.10
identification data
a sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it

NOTE The identification data may additionally contain data items 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.

4.11
message
a string of bits of any length

4.12
pre-signature
a value computed in the signature process which is a function of the randomizer but which is independent of the message

4.13
randomized
dependent on a randomizer

4.14
randomizer
a secret data item produced by the signing entity in the pre-signature production process, and not predictable by other entities

4.15
signature
[ISO/IEC 9796] the string of bits resulting from the signature process

NOTE This string of bits may have internal structure specific to the signature mechanism.

4.16
signature equation
an equation defining the signature function

4.17
signature function
a function in the signature process which is determined by the signature key and the domain parameters. A signature function takes the assignment and possibly the randomizer as inputs and gives the second part of the signature as output

4.18
signature key
a secret data item specific to an entity and usable only by this entity in the signature process

4.19
signature process
a process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

4.20
signed message
a set of data items 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.

4.21
verification function
a function in the verification process which is determined by the verification key and which gives a recomputed value of the witness as output

4.22
verification key
a data item which is mathematically related to an entity's signature key and which is used by the verifier in the verification process

4.23
verification process
a 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

4.24
witness
a data item which provides evidence to the verifier

5 Symbols, conventions, and legend for figures

5.1 Symbols

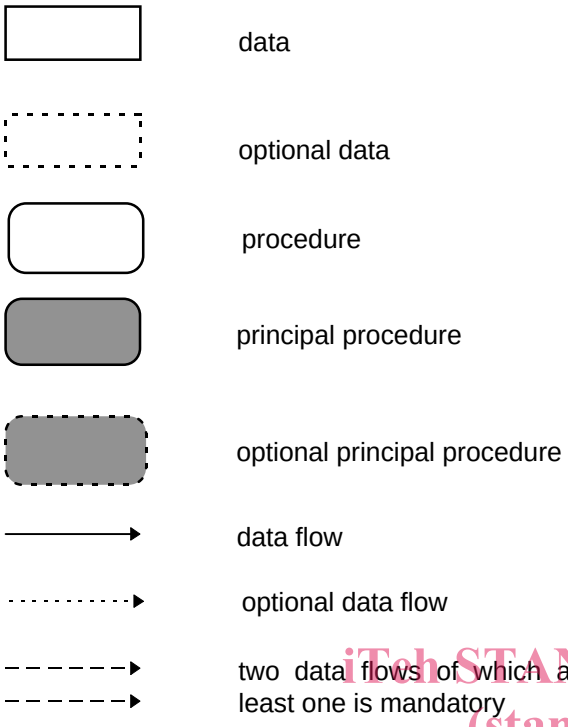
Throughout all parts of ISO/IEC 14888 the following symbols are used.

H	Hash-token
$\overline{H}$	Recomputed hash-token
K	Randomizer
M	Message
M_1, M_2	Parts of the prepared message
R	First part of a signature
$\overline{R}$	Recomputed first part of a signature
S	Second part of a signature
T	Assignment
X	Signature key
Y	Verification key
Z	Set of one or more domain parameters
Π	Pre-signature
$\overline{\Pi}$	Recomputed pre-signature
Σ	Signature
$A \bmod N$	The remainder obtained when integer A is divided by integer N
$A \equiv B \pmod N$	Integer A is congruent to integer B modulo N, i.e., $(A - B) \bmod N = 0$.

5.2 Coding convention

All integers are written with the most significant digit (or bit, or byte) in the leftmost position.

5.3 Legend for figures



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 signing entity computes its digital signature for a given message. The signature, together with an optional text field, form the appendix, which is appended to the message to form the signed message.

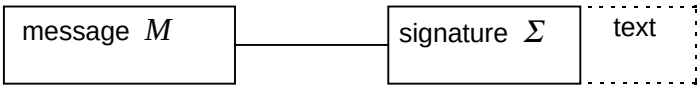


Figure 1 — Signed message

Depending on the application, there are different ways of forming the appendix and associating it 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. 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 gets protected by the signature.