

---

---

**Information technology — Security  
techniques — Digital signatures with  
appendix —**

**Part 1:  
General**

**iTeh STANDARD PREVIEW**  
*Technologies de l'information — Techniques de sécurité — Signatures  
numériques avec appendice —*  
**(standards.iteh.ai)**  
*Partie 1: Généralités*

[ISO/IEC 14888-1:2008](https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008)

[https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-  
2c0d067ebe14/iso-iec-14888-1-2008](https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008)

**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.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 14888-1:2008](https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008)

<https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

**Contents**

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols, conventions, and legend for figures</b> .....	<b>3</b>
<b>4.1 Symbols</b> .....	<b>3</b>
<b>4.2 Coding convention</b> .....	<b>4</b>
<b>4.3 Legend for figures</b> .....	<b>4</b>
<b>5 General</b> .....	<b>4</b>
<b>6 General model</b> .....	<b>5</b>
<b>7 Options for binding signature mechanism and hash-function</b> .....	<b>6</b>
<b>8 Key generation</b> .....	<b>6</b>
<b>9 Signature process</b> .....	<b>7</b>
<b>9.1 General</b> .....	<b>7</b>
<b>9.2 Computing the signature</b> .....	<b>7</b>
<b>9.3 Constructing the appendix</b> .....	<b>7</b>
<b>9.4 Constructing the signed message</b> .....	<b>7</b>
<b>10 Verification process</b> .....	<b>8</b>
<b>Annex A (informative) On hash-function identifiers</b> .....	<b>10</b>
<b>Bibliography</b> .....	<b>11</b>

## 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*

## 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.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 14888-1:2008](https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008)

<https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 14888-1:2008

<https://standards.iteh.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008>

# Information technology — Security techniques — Digital signatures with appendix —

## Part 1: General

### 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].

(standards.iteh.ai)

### 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

**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]

ITeC STANDARD PREVIEW  
(standards.itec.ai)  
ISO/IEC 14888-1:2008  
<https://standards.itec.ai/catalog/standards/sist/be592ec0-1a1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008>

**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



**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

ITeH STANDARD PREVIEW

(standards.iteh.ai)

message, the verification key and the domain parameters, and which  
 result of the signature verification: valid or invalid  
 https://standards.iteh.ai/catalog/standards/sist/1c-42b8-a69d-2c0d067ebe14/iso-iec-14888-1-2008

**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.

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

*S* second part of a signature

*X* signature key

*Y* verification key