INTERNATIONAL STANDARD

ISO/IEC 14888-2

First edition
1999-12-15

Information technology — Security techniques — Digital signatures with appendix —

Part 2:
Identity-based mechanisms

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

Partie 2: Mécanismes basés sur des identités

This document is a preview generated by EVS

Reference number
ISO/IEC 14888-2:1999(E)

This document is a preview generated by EVS

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 14888-2 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.

Annexes A and B of this part of ISO/IEC 14888 are for information only.

© ISO/IEC 1999

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 the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Information technology — Security techniques — Digital signatures with appendix —

Part 2:
Identity-based mechanisms

This document is a preview generated by EVS

1 Scope

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

This part of ISO/IEC 14888 specifies the general structure and the fundamental procedures which constitute the signature and verification processes of an identity-based digital signature mechanism with appendix for messages of arbitrary length.

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 9796: 1991, *Information technology - Security techniques - Digital signature scheme giving message recovery*.

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

3 General

The verification of a digital signature requires the signing entity's verification key. It is therefore 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 digital signature scheme is said to be “identity-based.”

The key generation process of the identity-based mechanism defined in this part of ISO/IEC 14888 involves a trusted third party. The trusted third party has a secret parameter, the key generation exponent, which it uses to derive the signature keys of other entities. The secrecy of the signature keys depends unconditionally on the secrecy of the key generation exponent.

In the verification of an identity-based signature, two parameters are needed. The first one, the domain verification exponent, is common to all entities, while the second one, the signing entity's verification key, is specific to each entity. In the identity-based mechanism defined in this part of ISO/IEC 14888, an entity's verification key is derived directly from the entity's identification data, using a public function.

The identity-based signature mechanism with appendix is an example of a randomized mechanism, as described in ISO/IEC 14888-1. The descriptions of the signature and verification processes follow the general procedures specified in Clause 10 of ISO/IEC 14888-1. In particular, this part makes use of the general requirements, definitions and symbols given in ISO/IEC 14888-1.

The identity-based digital signature mechanism with appendix is defined by the specification of the following processes:

- key generation process;
- signature process; and
- verification process.

4 Definitions

For the purposes of this part of ISO/IEC 14888, the following definitions apply.

4.1
domain modulus
a domain parameter, which is a positive integer resulting from the product of two distinct primes which are known only to the trusted third party

4.2
domain verification exponent
a domain parameter which is a positive integer