INTERNATIONAL STANDARD

ISO/IEC 20008-2

First edition
2013-11-15

Information technology — Security techniques — Anonymous digital signatures —

Part 2: Mechanisms using a group public key

Technologies de l'information — Techniques de sécurité — Signatures numériques anonymes —

Partie 2: Mécanismes utilisant une clé publique de groupe

Reference number
ISO/IEC 20008-2:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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

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.

ISO/IEC 20008-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 20008 consists of the following parts, under the general title *Information technology — Security techniques — Anonymous digital signatures*:

— *Part 1: General*

— *Part 2: Mechanisms using a group public key*

Further parts may follow.

Introduction

Anonymous digital signature mechanisms are a special type of digital signature mechanism in which, given a digital signature, an unauthorized entity cannot discover the signer's identifier yet can verify that a legitimate signer has generated a valid signature.

ISO/IEC 20008 specifies anonymous digital signature mechanisms. ISO/IEC 20008-1 specifies principles and requirements for two categories of anonymous digital signatures mechanisms: signature mechanisms using a group public key, and signature mechanisms using multiple public keys. This part of ISO/IEC 20008 specifies a number of anonymous signature mechanisms of the first category.

Anonymous signature mechanisms of the first category can have capabilities for providing more information about the signer. Some have a linking capability, where two signatures signed by the same signer are linkable. Some have an opening capability, where the signature can be opened by a special entity to reveal the identity of the signer. Some have both linking and opening capabilities.

For each mechanism, the processes of opening, linking, and/or revocation are specified.

The mechanisms specified in this part of ISO/IEC 20008 use a collision-resistant hash-function. A hash-function specified in ISO/IEC 10118 is to be used.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity, and scope of these patent rights.

The holders of these patent right have assured the ISO and IEC that they are willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

— Electronics and Telecommunications Research Institute (ETRI)

  161, Gajeong-dong, Yuseong-gu, Daejeon, Korea

— NEC Corporation

  7-1, Shiba 5-chome, Minato-Ku, Toyko 108-8001, Japan

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and/or IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Information technology — Security techniques — Anonymous digital signatures —

Part 2: Mechanisms using a group public key

1 Scope

This part of ISO/IEC 20008 specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature.

It provides

— a general description of an anonymous digital signature mechanism using a group public key, and

— a variety of mechanisms that provide such anonymous digital signatures.

For each mechanism, this part of ISO/IEC 20008 specifies

— the process for generating group member signature keys and a group public key,

— the process for producing signatures,

— the process for verifying signatures,

— the process for opening signatures (if the mechanism supports opening),

— the process for linking signatures (if the mechanism supports linking), and

— the process for revoking group members.

2 Normative references

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

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*

ISO/IEC 20008-1, *Information technology — Security techniques — Anonymous digital signatures — Part 1: General*