INTERNATIONAL STANDARD

ISO/IEC 20008-2

First edition
2013-11-15

Corrected version
2017-11

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)

© ISO/IEC 2013



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols (and abbreviated terms) **2**
5 General model and requirements **3**
6 Mechanisms with linking capability **4**
6.1 General 4
6.2 Mechanism 1 5
6.2.1 Symbols 5
6.2.2 Key generation process 5
6.2.3 Signature process 8
6.2.4 Verification process 9
6.2.5 Linking process 10
6.2.6 Revocation process 10
6.3 Mechanism 2 10
6.3.1 Symbols 10
6.3.2 Key generation process 11
6.3.3 Signature process 13
6.3.4 Verification process 14
6.3.5 Linking process 15
6.3.6 Revocation process 15
6.4 Mechanism 3 16
6.4.1 Symbols 16
6.4.2 Key generation process 16
6.4.3 Signature process 17
6.4.4 Verification process 18
6.4.5 Linking process 19
6.4.6 Revocation process 19
6.5 Mechanism 4 20
6.5.1 Symbols 20
6.5.2 Key generation process 20
6.5.3 Signature process 22
6.5.4 Verification process 22
6.5.5 Linking process 23
6.5.6 Revocation process 23
7 Mechanisms with opening capability **23**
7.1 General 23
7.2 Mechanism 5 23
7.2.1 Symbols 23
7.2.2 Key generation process 24
7.2.3 Signature process 25
7.2.4 Verification process 26
7.2.5 Opening process 26
7.2.6 Revocation process 26
7.3 Mechanism 6 27
7.3.1 Symbols 27
7.3.2 Key generation process 27
7.3.3 Signature process 28
7.3.4 Verification process 29
7.3.5 Opening process 29

© ISO/IEC 2013 – All rights reserved

7.3.6 Revocation process 29
8 Mechanisms with both opening and linking capabilities 29
8.1 General 29
8.2 Mechanism 7 30
8.2.1 Symbols 30
8.2.2 Key generation process 30
8.2.3 Signature process 32
8.2.4 Verification process 32
8.2.5 Opening process 33
8.2.6 Evidence evaluation process 33
8.2.7 Linking process 33
8.2.8 Revocation process 34
Annex A (normative) **Object identifiers 35**
Annex B (normative) **Special hash-functions 37**
Annex C (informative) **Security guidelines for the anonymous signature mechanisms 39**
Annex D (informative) **Comparison of revocation mechanisms 42**
Annex E (informative) **Numerical examples 45**
Annex F (informative) **Proof of correct generation in Mechanism 5 ..... 80**
Bibliography 84

 © ISO/IEC 2013 – 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.

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.

This corrected version of ISO/IEC 20008-2:2013 incorporates the following correction:

— in 6.5.4, step g) has been corrected and step h) has been added consequently.

© ISO/IEC 2013 – All rights reserved

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.

© ISO/IEC 2013 – All rights reserved

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20008-1 and the following apply.

© ISO/IEC 2013 – All rights reserved

3.1
assistant signer
entity that can help a principal signer to create anonymous signatures, but that cannot generate anonymous signatures unaided

3.2
member-list
list that includes the identities of group members together with their corresponding group membership credentials

3.3
principal signer
entity which is in possession of a group member signature key and which can create anonymous signatures using this key

3.4
secret seed value
secret data known to a group member and used for deriving group member private keys

3.5
security parameters
variables that determine the security strength of a mechanism

4 Symbols (and abbreviated terms)

For the purposes of this part of ISO/IEC 20008, the following symbols and abbreviations apply.

bsn	Linking base, either a special symbol $\perp$ or an arbitrary string.
e	A bilinear map function $e: G_1 \times G_2 \rightarrow G_T$ such that for all $P \in G_1$, $Q \in G_2$, and all positive integers a, b, the equation $e([a]P, [b]Q) = e(P, Q)^{ab}$ holds. This function is also called a pairing function.
gcd(*a*, *b*)	The greatest common divisor of the integers *a* and *b*.
G_1	An additive cyclic group of order *p* over an elliptic curve.
G_2	An additive cyclic group of order *p* over an elliptic curve.
G_T	A multiplicative cyclic group of order *p*.
H	A cryptographic hash-function.
m	Message to be signed.
n	An RSA modulus where $n = pq$.
O_E	The elliptic curve point at infinity.
p	A prime number.
P_1	Generator of G_1.
P_2	Generator of G_2.
q	A prime number.
Q_1+Q_2	The elliptic curve sum of points Q_1 and Q_2.
QR(*n*)	The group of quadratic residues modulo *n*.

© ISO/IEC 2013 – All rights reserved