International Standard

ISO/IEC 20008-3

First edition
2024-12

Information security — Anonymous digital signatures —

Part 3: Mechanisms using multiple public keys

Sécurité de l'information — Signatures numériques anonymes —

Partie 3: Mécanismes utilisant plusieurs clés publiques

Reference number
ISO/IEC 20008-3:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Symbols and abbreviated terms **2**
5 General model and requirements **3**
5.1 General 3
5.2 Model 3
5.3 Requirements 4
6 Mechanisms without special 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 Ring signature process 5
6.2.4 Ring signature verification process 6
6.3 Mechanism 2 6
6.3.1 Symbols 6
6.3.2 Key generation process 7
6.3.3 Ring signature process 7
6.3.4 Ring signature verification process 7
6.4 Mechanism 3 8
6.4.1 Symbols 8
6.4.2 Key generation process 8
6.4.3 Ring signature process 8
6.4.4 Ring signature verification process 8
7 Mechanisms with linking capability **9**
7.1 General 9
7.2 Mechanism 1 9
7.2.1 Symbols 9
7.2.2 Key generation process 10
7.2.3 Ring signature process 10
7.2.4 Ring signature verification process 10
7.2.5 Ring signature linking process 11
7.2.6 Event-linkable type 11
8 Mechanisms with tracing capability **11**
8.1 General 11
8.2 Mechanism 1 11
8.2.1 Symbols 11
8.2.2 Key generation process 11
8.2.3 Ring signature process 12
8.2.4 Ring signature verification process 12
8.2.5 Ring signature tracing process 13
9 Mechanisms with threshold capability **13**
9.1 General 13
9.2 Mechanism 1 13
9.2.1 Symbols 13
9.2.2 Key generation process 13
9.2.3 Ring signature process 13
9.2.4 Ring signature verification process 14

© ISO/IEC 2024 – All rights reserved

9.3 Mechanism 2 14
9.3.1 Symbols 14
9.3.2 Key generation process 14
9.3.3 Ring signature process 15
9.3.4 Ring signature verification process 15
Annex A (normative) **Object identifiers** **16**
Annex B (normative) **Conversion functions** **17**
Annex C (informative) **Numerical examples of mechanisms in this document** **18**
Bibliography **23**

© ISO/IEC 2024 – 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 20008 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Introduction

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

The ISO/IEC 20008 series specifies anonymous digital signature mechanisms. ISO/IEC 20008-1 specifies principles and requirements for two categories of anonymous digital signatures mechanisms:

1) signature mechanisms using a group public key;

2) signature mechanisms using multiple public keys.

This document specifies a number of anonymous signature mechanisms in the second category.

Anonymous signature mechanisms in the second category allow a signer to form a group spontaneously by combining the public keys of the relevant users with the signer’s own public key. The verifier can confirm that a signature is generated by one of the users within this group but cannot find out who the actual signer is. Unlike the first category described in ISO/IEC 20008 series, mechanisms in the second category do not require a group manager, and the private key and public key are generated individually by each user.

Some mechanisms described in this document are unlinkable, where no one can determine whether two signatures are generated by the same signer or not. Some mechanisms have a linking capability, making it possible to be determined whether two signatures were generated by the same signer under certain conditions. Some mechanisms have a tracing capability, where, given two (message, signature) pairs generated by the same signer within the same ring setting, the true signer can be identified. Some mechanisms have a threshold setting, where the verifier can confirm a signature is generated by subsets (of specified size) of group users, but cannot determine which users were involved.

© ISO/IEC 2024 – All rights reserved

Information security — Anonymous digital signatures —

Part 3:
Mechanisms using multiple public keys

1 Scope

This document specifies anonymous digital signature mechanisms in which a verifier uses multiple public keys to verify a digital signature.

This document provides:

— a general description of an anonymous digital signature mechanism using multiple public keys;

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

For each mechanism, this document specifies the process for:

— generating the private key and public key of each user;

— producing signatures;

— verifying signatures;

— linking signatures (if the mechanism supports linking);

— tracing signatures (if the mechanism supports tracing);

— producing signatures with threshold capability (if the mechanism supports a threshold capability);

— verifying signatures with threshold capability (if the mechanism supports a threshold capability).

This document does not define the implementation of a public key infrastructure (PKI) and the means for distinct entities to exchange, extract and verify their respective public key certificates.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118-1, *Information technology — Security techniques — Hash-functions — Part 1: General*

ISO/IEC 10118-2, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*

ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 10118-4, *Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic*

ISO/IEC 18033-2:2006, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

© ISO/IEC 2024 – All rights reserved

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 18033-4, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*

ISO/IEC 18033-5:2015, *Information technology — Security techniques — Encryption algorithms — Part 5: Identity-based ciphers*

ISO/IEC 29192-2, *Information security — Lightweight cryptography — Part 2: Block ciphers*

ISO/IEC 29192-3, *Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers*

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

ISO/IEC 18032, *Information security — Prime number generation*

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

ISO/IEC 20008-2:2013, *Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key*

RFC 9380, *Hashing to Elliptic Curves, Internet Research Task Force (IRTF)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20008-1, ISO/IEC 18033-4 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
symmetric encryption system
encryption system based on symmetric cryptographic techniques

[SOURCE: ISO/IEC 18033-1:2021, 3.29, modified — the admitted terms “symmetric encipherment system” and “symmetric cipher” were removed.]

4 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply.

Bsn	Linking base, either a special symbol ⊥ or an arbitrary string.
$\oplus$	Bitwise exclusive OR (XOR) operation.
$\setminus$	Set subtraction operation.
$\mathrm{Enc}_k(m)$	A symmetric-key encryption function taking a secret key k and a variable-length message m as input and giving a ciphertext c as output, e.g. the encryption function for one of the symmetric encryption systems specified in ISO/IEC 18033-3, ISO/IEC 18033-4, ISO/IEC 10116, ISO/IEC 29192-2 or ISO/IEC 29192-3.
$\mathrm{Dec}_k(C)$	A symmetric-key decryption function taking a secret key k and a ciphertext C as input and giving a message m or a decryption failure symbol ⊥ as output.
C	A ciphertext generated from a symmetric-key encryption function.

© ISO/IEC 2024 – All rights reserved