



International
Standard

ISO/IEC 20008-3

**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

**First edition
2024-12**

[ISO/IEC 20008-3:2024](https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024)

<https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024>

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 20008-3:2024](https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024)

<https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024>



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 20008-3:2024(en)

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

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ISO/IEC 20008-3:2024](https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024)

<https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024>

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.

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.

(<https://standards.iteh.ai>)
Document Preview

<https://standards.iteh.ai>

<https://standards.iteh.ai/catalog/standards/iso/ab83492a-456c-4ca7-95b9-8c41feb29224/iso-iec-20008-3-2024>

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 20008-3:2024(en)

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.

B_{sn}	Linking base, either a special symbol \perp or an arbitrary string.
\oplus	Bitwise exclusive OR (XOR) operation.
\setminus	Set subtraction operation.
$Enc_k(m)$	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.
$Dec_k(C)$	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 \perp as output.
C	A ciphertext generated from a symmetric-key encryption function.

N	The size of the ring, i.e. the number of entities in the set consisting of the true signer and the potential signer (or signers).
π	Index of the true signer, where $1 \leq \pi \leq N$. If $\pi = N$, $\pi + 1$ is set to 1. Similarly, if $\pi = 1$, $\pi - 1$ is set to N .
$\text{lb}(x)$	The base 2 logarithm of x .
$\text{max}(X)$	The largest integer within the integer set X .
$\text{gcd}(a,b)$	The greatest common divisor of the integers a and b .
H	A hash-function taking an arbitrary string as input and giving a fixed-length bit string as output, e.g. one of the dedicated hash-functions specified in ISO/IEC 10118-3.
\parallel	$X \parallel Y$ denotes the result of the concatenation of octet strings X and Y in the order specified. In cases where the result of concatenating two or more octet strings is input to a cryptographic function as part of one of the mechanisms specified in this document, this result shall be composed so that it can be uniquely resolved into its constituent octet strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property can be achieved in a variety of different ways, depending on the application. For example, it can be guaranteed by fixing the length of each of the octet strings throughout the domain of use of the mechanism, or by encoding the sequence of concatenated octet strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 ^[9] .

5 General model and requirements

5.1 General

This clause specifies the general model and requirements for the anonymous digital signature mechanisms specified in this document. Some of the contents of this clause are taken from ISO/IEC 20008-1. In addition, specific requirements applying to mechanisms using multiple public keys are addressed.

5.2 Model

An anonymous digital signature mechanism using multiple public keys is also known as a ring signature mechanism. A ring signature mechanism involves a set of possible signers. Each possible signer has a signature key pair in the same form as in a conventional signature mechanism. These possible signers are independent of each other in the sense that it is not necessary for them to agree on being involved in the same signature process. To create a ring signature, one of them is the true signer and the others are the potential signers. The true signer chooses one or more potential signers and forms a ring of N possible signers. The true signer may select only one potential signer and, in this case, $N = 2$.

Some ring signature mechanisms have special capabilities. These mechanisms make it possible to link two signatures, trace a signature back to its true signer or apply thresholds to the signing process.

A ring signature mechanism is defined by the specification of the following processes:

- key generation process;
- signature process;
- verification process;
- linking process (if supported);
- tracing process (if supported);
- threshold signature process (if supported);

- threshold verification process (if supported).

The security properties of a general ring signature include unforgeability and anonymity. Other specific properties such as linkability, traceability and threshold are associated with ring signatures with special capabilities.

The anonymous digital signature mechanisms using multiple public keys specified in this document involve a range of types of entity. Some of these entities exist in every mechanism whereas others exist only in some mechanisms. The following list defines the role of each entity:

- True signer: an entity generating a digital signature.
- Potential signer: an entity whose public key is used in creating a digital signature, which means the public key is used in both the signature process and signature verification process, although the potential signer is not involved in these two processes.
- Verifier: an entity verifying a digital signature.
- Linker: an entity that checks whether two signatures have been generated by the same signer with a linking base. This entity exists in some of the mechanisms.
- Tracer: an entity that identifies the true signer when given as input two (message, signature) pairs which are both generated by the same signer within the same ring setting. This entity exists in some of the mechanisms.

5.3 Requirements

In order to use any of the mechanisms specified in this document, the following requirements shall be met.

- Each verifier shall have access to an authentic copy of the public key of each entity in the ring.
- A collision-resistant hash function shall be as specified in accordance with the ISO/IEC 10118 series.
- A robust random bit generator shall be as specified in accordance with ISO/IEC 18031.
- A robust prime number generator shall be as specified in accordance with ISO/IEC 18032.
- Symmetric-key encryption and decryption functions shall be as specified in accordance with ISO/IEC 18033-3, ISO/IEC 18033-4, ISO/IEC 10116, ISO/IEC 29192-2 or ISO/IEC 29192-3.
- Object identifiers described in [Annex A](#) shall be used.
- Conversion functions described in [Annex B](#) shall be used.

Numerical examples of mechanisms in this document are provide in [Annex C](#).

6 Mechanisms without special capability

6.1 General

This clause specifies three digital signature mechanisms without any special capabilities such as linking, tracing or threshold.

NOTE 1 The mechanism given in [6.2](#) is based on the scheme originally specified in Reference [\[7\]](#).

NOTE 2 The mechanism given in [6.3](#) is based on the scheme originally specified in Reference [\[1\]](#).

NOTE 3 The mechanism given in [6.4](#) is based on the scheme originally specified in Reference [\[1\]](#).

6.2 Mechanism 1

6.2.1 Symbols

The following symbols apply in the specification of this mechanism.

- b : integer
- d_i : integer in the range $[0, (p_i - 1)(q_i - 1) - 1]$
- k : l_k -bit string
- l_b : integer equal to or greater than 160
- l_k : integer equal to or greater than 256
- l_n : integer equal to or greater than 2048
- n : l_n -bit string
- $p_i, q_i, p'_i, q'_i, e_i$: prime numbers
- v, x_i, y_i : b -bit integers
- H : a hash function that outputs an l_k -bit hash-code as defined in [Annex B](#)
- Enc_k : symmetric-key encryption function that takes a secret key k and a variable-length message as input and outputs an integer in the range $[0, 2^b - 1]$
- Dec_k : symmetric-key decryption function taking a secret key k and a ciphertext as input and outputs an integer in the range $[0, 2^b - 1]$

6.2.2 Key generation process

The key generation process involves each user i ($1 \leq i \leq N$) independently performing the following steps.

- a) Choose prime numbers p'_i, q'_i with $l_n/2$ bits such that $p_i = 2p'_i + 1, q_i = 2q'_i + 1$ are prime numbers. Compute modulus $n_i = q_i p_i$.
- b) Choose a number $e_i \in [0, (p_i - 1)(q_i - 1) - 1]$ such that $\text{gcd}(e_i, (p_i - 1)(q_i - 1)) = 1$.
- c) Compute $d_i = e_i^{-1} \text{ mod } (p_i - 1)(q_i - 1)$.
- d) Output the following:
 - Public key = $vk_i = (n_i, e_i)$;
 - Private key = $sk_i = d_i$.

6.2.3 Ring signature process

In the ring signature process, a true signer first chooses a set of $N - 1$ potential signers. The true signer also chooses a random integer π satisfying $1 \leq \pi \leq N$, which denotes the index of the true signer. The true signer then signs a message using its private key and the public keys of the potential signers, without requiring their approval or assistance. In this process the potential signers are arranged in random order.