INTERNATIONAL STANDARD

ISO/IEC 18370-2

First edition
2016-07-01

Information technology — Security techniques — Blind digital signatures —

Part 2: Discrete logarithm based mechanisms

Technologie de l'information — Techniques de sécurité — Signatures numériques en aveugle —

Partie 2: Mécanismes fondés sur le logarithme discret

Reference number
ISO/IEC 18370-2:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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 **3**

5 General requirements **4**

6 Blind signature mechanisms **4**
6.1 General 4
6.2 Mechanism 1 4
6.2.1 Security parameters 4
6.2.2 Key generation process 5
6.2.3 Blind signature process 5
6.2.4 Verification process 6

7 Blind signature mechanisms with partial disclosure **6**
7.1 General 6
7.2 Mechanism 2 6
7.2.1 Security parameters 6
7.2.2 Key generation process 6
7.2.3 Blind signature process with partial disclosure 7
7.2.4 Verification process 8
7.3 Mechanism 3 8
7.3.1 Symbols 8
7.3.2 Key generation process 8
7.3.3 Blind signature process with partial disclosure 9
7.3.4 Verification process 9

8 Blind signature mechanisms with selective disclosure **10**
8.1 General 10
8.2 Mechanism 4 10
8.2.1 Security parameters 10
8.2.2 Key generation process 10
8.2.3 Blind signature process with selective disclosure 10
8.2.4 Presentation process 12
8.2.5 Verification process 12

9 Traceable blind signature mechanisms **13**
9.1 General 13
9.2 Mechanism 5 13
9.2.1 Symbols 13
9.2.2 Key generation process 13
9.2.3 Traceable blind signature process 14
9.2.4 Verification process 16
9.2.5 Requestor tracing process 16
9.2.6 Signature tracing process 17
9.2.7 Requestor tracing evidence evaluation process 17
9.2.8 Signature tracing evidence evaluation process 17

Annex A (normative) **Object identifiers** **19**

Annex B (normative) **Conversion functions** **20**

Annex C (normative) **Group description** **21**

Annex D (informative) **Special hash-functions** **22**

© ISO/IEC 2016 – All rights reserved

Annex E (informative) **Security considerations and comparison of blind signature mechanisms** ..**24**
Annex F (informative) **Numerical examples** ..**26**
Bibliography ..**78**

© ISO/IEC 2016 – 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.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18370 consists of the following parts, under the general title *Information technology — Security techniques — Blind digital signatures*:

— *Part 1: General*

— *Part 2: Discrete logarithm based mechanisms*

Further parts may follow.

© ISO/IEC 2016 – All rights reserved

Introduction

Blind digital signature mechanisms are a special type of digital signature mechanism, as specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888, which allow a user (a requestor) to obtain a signature from a signer of the user's choice, without giving the signer any information about the message that is signed or the resulting signature.

In some mechanisms, the signer does not completely lose control over the signed message since the signer can include explicit information in the resulting signature under an agreement with the requestor. These types of blind signatures are called blind signatures with partial disclosure.

Other mechanisms allow a requestor to receive a blind signature on a message not known to the signer but the choice of the message is restricted and needs to conform to certain rules. Such mechanisms are called blind signature mechanisms with selective disclosure.

Depending on the mechanism, it may be possible for an authorized entity to trace a signature to the requestor who requested it. Such an entity can either identify a signature that resulted from a given signature request (signature tracing), or link a signature to the receiver who requested it (requestor tracing). Blind signature mechanisms with tracing features are called traceable blind signature mechanisms.

ISO/IEC 18370 specifies blind digital signature mechanisms, as well as three variants: blind digital signature mechanisms with partial disclosure, blind digital signature mechanisms with selective disclosure and traceable blind digital signature mechanisms. ISO/IEC 18370-1 specifies principles and requirements for these mechanisms. This part of ISO/IEC 18370 specifies several specific instances of these mechanisms.

The security of blind digital signature mechanisms and their variants depends on computational problems believed to be intractable, i.e. problems for which, given current knowledge, finding a solution is computationally infeasible, such as the integer factorization problem or the discrete logarithm problem in an appropriate group. The mechanisms specified in this part of ISO/IEC 18370 are based on the latter problem.

ISO/IEC 18370 does not specify mechanisms for key management or for certification of public keys. A variety of means are available for obtaining a reliable copy of the public verification key, e.g. a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC 18370. For further information, see ISO/IEC 9594-8, ISO/IEC 11770-3 and ISO/IEC 15945.

This part of ISO/IEC 18370 specifies mechanisms that use a collision resistant hash-function to hash the message to be blindly signed. ISO/IEC 10118 specifies hash-functions.

The generation of key pairs requires random bits and prime numbers. The generation of signatures requires random bits. Techniques for producing random bits and prime numbers are outside the scope of ISO/IEC 18370. For further information, see ISO/IEC 18031 and ISO/IEC 18032.

© ISO/IEC 2016 – All rights reserved

Information technology — Security techniques — Blind digital signatures —

Part 2: Discrete logarithm based mechanisms

1 Scope

This part of ISO/IEC 18370 specifies blind digital signature mechanisms, together with mechanisms for three variants of blind digital signatures. The variants are blind digital signature mechanisms with partial disclosure, blind digital signature mechanisms with selective disclosure and traceable blind digital signature mechanisms. The security of all the mechanisms in this part of ISO/IEC 18370 is based on the discrete logarithm problem.

For each mechanism, this part of ISO/IEC 18370 specifies the following:

— the process for generating the keys of the entities involved in these mechanisms;

— the process for producing blind signatures;

— the process for verifying signatures.

This part of ISO/IEC 18370 specifies another process specific to blind signature mechanisms with selective disclosure, namely, the following:

— the presentation process.

Furthermore, this part of ISO/IEC 18370 specifies other processes specific to traceable blind signature mechanisms, namely, the following:

a) the process for tracing requestors;

b) the process for tracing signatures;

c) the requestor tracing evidence evaluation process (optional);

d) the signature tracing evidence evaluation process (optional).

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18370-1 and the following apply.

3.1
abelian group
group $(G, *)$ such that $a * b = b * a$ for every a and b in G

© ISO/IEC 2016 – All rights reserved

3.2
cyclic group
group G of n elements that contains an element a in G, called the generator, of order n

[SOURCE: ISO/IEC 14888-3:2006, 3.2]

3.3
elliptic curve over a finite field
set E of points $P = (x, y)$, where x and y are elements of the *finite field* (3.6), that satisfy a certain equation, together with an extra point referred to as the point at infinity

Note 1 to entry: In this part of ISO/IEC 18370, only finite fields containing exactly q elements for a prime $q > 3$ are considered. In this case, the equation that every point $P = (x, y)$ of E (other than the point at infinity) should satisfy is of the form $y^2 = x^3 + ax + b$. The finite field elements a and b should satisfy $4a^3 + 27b^2 \neq 0_F$ (where 0_F is the additive identity element of the finite field).

Note 2 to entry: The set of points E, together with an appropriately defined operation, forms a *finite commutative group* (3.5), where the point at infinity is the identity element.

3.4
field
set of elements S and a pair of operations (+,*) defined on S, such that: i) $a * (b + c) = a * b + a * c$ for every a, b and c in S, ii) S together with + forms an *abelian group* (3.1) (with identity element 0), and iii) S excluding 0 together with * forms an abelian group

3.5
finite commutative group
abelian group (3.1) $(G, *)$ with a finite number of elements

Note 1 to entry: If $a^0 = e$, and $a^{n+1} = a * a^n$ (for $n \geq 0$) is defined recursively, the order of $a \in G$ is the least positive integer n, such that $a^n = e$.

Note 2 to entry: In some cases, such as when G is the set of points on an elliptic curve, arithmetic in the finite set G is described using additive notation.

3.6
finite field
field (3.4) such that the underlying set of elements is finite

Note 1 to entry: For any positive integer, m and a prime p, there exists a finite field containing exactly $q = p^m$ elements. This field is unique up to an isomorphism and is denoted by F_q.

[SOURCE: ISO/IEC 18033-2:2006, 3.21]

3.7
group
set of elements G and an operation * defined on the set of elements such that: i) $(a * b) * c = a * (b * c)$ for every a, b and c in G, ii) there exists an identity element, e in G, such that $a * e = e * a = a$ for every a in G, and iii) for every a in G, there exists an inverse element, a^{-1} in G, such that $a * a^{-1} = a^{-1} * a = e$

3.8
security parameters
variables that determine the security strength of a mechanism

© ISO/IEC 2016 – All rights reserved