

This is a preview of "BS ISO/IEC 18370-2:2016". Click here to purchase the full version from the ANSI store.

**BS ISO/IEC 18370-2:2016**



**BSI Standards Publication**

# **Information technology — Security techniques — Blind digital signatures**

Part 2: Discrete logarithm based  
mechanisms

This is a preview of "BS ISO/IEC 18370-2:2016". [Click here to purchase the full version from the ANSI store.](#)

This British Standard is the UK implementation of ISO/IEC 18370-2:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.  
Published by BSI Standards Limited 2016

ISBN 978 0 580 80110 5

ICS 35.040

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2016.

**Amendments/corrigenda issued since publication**

Date	Text affected
------	---------------

---

This is a preview of "BS ISO/IEC 18370-2:2016". [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of "BS ISO/IEC 18370-2:2...". Click here to purchase the full version from the ANSI store.



## **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

This is a preview of "BS ISO/IEC 18370-2:2016". Click here to purchase the full version from the ANSI store.

## Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols</b> .....	<b>3</b>
<b>5 General requirements</b> .....	<b>4</b>
<b>6 Blind signature mechanisms</b> .....	<b>4</b>
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
<b>7 Blind signature mechanisms with partial disclosure</b> .....	<b>6</b>
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
<b>8 Blind signature mechanisms with selective disclosure</b> .....	<b>10</b>
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
<b>9 Traceable blind signature mechanisms</b> .....	<b>13</b>
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
<b>Annex A (normative) Object identifiers</b> .....	<b>19</b>
<b>Annex B (normative) Conversion functions</b> .....	<b>20</b>
<b>Annex C (normative) Group description</b> .....	<b>21</b>
<b>Annex D (informative) Special hash-functions</b> .....	<b>22</b>

This is a preview of "BS ISO/IEC 18370-2:2...". [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of "BS ISO/IEC 18370-2:2016". Click here to purchase the full version from the ANSI store.

## 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](http://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](http://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.

## 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.



This is a preview of "BS ISO/IEC 18370-2:2...". Click here to purchase the full version from the ANSI store.

# 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  $G$