INTERNATIONAL STANDARD

ISO/IEC 18370-1

First edition
2016-11-15

Information technology — Security techniques — Blind digital signatures —

Part 1: General

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

Partie 1: Généralités

Reference number
ISO/IEC 18370-1:2016(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 ISO documents 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 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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

A list of all parts in the ISO/IEC 18370 series can be found on the ISO website.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity.

Blind signature mechanisms are a special type of digital signature mechanisms, as specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts), 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 actual message or the resulting signature.

There are several variants of blind signature mechanisms. In some variants, the signer does not completely lose control over the signed message. In a blind signature mechanism with partial disclosure, the signer can include explicit information in the resulting signature based on an agreement with the requestor, whereas in a blind signature mechanism with selective disclosure, the choice of the message is restricted and conforms to certain rules. In other mechanisms, such as traceable blind signature mechanisms, an authorized entity is allowed to trace a signature to the requestor who requested it.

As is the case for conventional digital signature mechanisms, blind signature mechanisms are based on asymmetric cryptographic techniques and involve three basic operations:

— a process for generating a private signature key and a public verification key;

— a process for creating a blind signature that uses the private signature key;

— a process for verifying a blind signature that uses the public verification key.

Blind signatures and their variants can be used to provide users anonymity in a variety of electronic communication and transaction systems. Examples include Internet voting, electronic payment instruments, online auctions, public transport ticketing, road-toll pricing, and loyalty schemes. These mechanisms could also be used to achieve anonymous entity authentication. Anonymous entity authentication mechanisms are specified in ISO/IEC 20009 (all parts).

Like conventional digital signature mechanisms, the security of blind signature mechanisms 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 ISO/IEC 18370 (all parts) are based on the latter problem. However, security of some mechanisms also depends on the fact that some numbers are not only random but also unique.

The ISO/IEC 18370 series specifies three variants of blind signature mechanisms: blind signature mechanisms with partial disclosure, blind signature mechanisms with selective disclosure, and traceable blind signature mechanisms. This document specifies principles and requirements for these mechanisms. ISO/IEC 18370-2 specifies specific instances of these mechanisms.

The mechanisms specified in the ISO/IEC 18370 series use a variety of other standardized cryptographic algorithms, such as the following.

— They may use a collision-resistant hash-function to hash the message to be signed and to compute signatures. ISO/IEC 10118 (all parts) specifies hash-functions.

— They may use a conventional digital signature mechanism to certify public keys when such certification is required. Conventional digital signature mechanisms are specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts).

— They may require the use of a conventional entity authentication mechanism, if the signer needs to authenticate the requestor before issuing a blind signature. Entity authentication mechanisms are specified in ISO/IEC 9798 (all parts).

— They may require the use of a conventional asymmetric encryption mechanism, if certain information of the entities involved in the blind signature mechanism is required to be encrypted

for the purposes of privacy and confidentiality. Asymmetric encryption mechanisms are specified in ISO/IEC 18033-2.

Information technology — Security techniques — Blind digital signatures —

Part 1: General

1 Scope

This document specifies principles, including a general model, a set of entities, a number of processes, and general requirements for blind digital signature mechanisms, as well as the following variants of blind digital signature mechanisms:

— blind signature mechanisms with partial disclosure;

— blind signature mechanisms with selective disclosure;

— traceable blind signature mechanisms.

It also contains terms, definitions, abbreviated terms and figure elements that are used in all parts of ISO/IEC 18370.

See Annex A for a comparison on the blind digital signature mechanisms.

2 Normative references

There are no normative references in this document.