BS ISO/IEC 20008-1:2013

BSI Standards Publication

Information technology — Security techniques — Anonymous digital signatures

Part 1: General

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 20008-1:2013.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

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 2013. Published by BSI Standards Limited 2013

ISBN 978 0 580 73397 0

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 December 2013.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20008-1:2013

INTERNATIONAL STANDARD

ISO/IEC 20008-1

First edition
2013-12-15

Information technology — Security techniques — Anonymous digital signatures —

Part 1: General

Technologies de l'information — Techniques de sécurité — Signatures numériques anonymes —

Partie 1: Général

Reference number
ISO/IEC 20008-1:2013(E)

Documents
Document Sharing Hub
© ISO/IEC 2013

Full document details: BS ISO/IEC 20008-1:2013

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20008-1:2013

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Terms and definitions **1**
3 Abbreviations and legend for figures **8**
4 Options for a group public key and multiple public keys **9**
5 General requirements **11**
6 Mechanisms using a group public key **12**
6.1 General model 12
6.2 Entities 13
6.3 Key generation process 13
6.4 Group signature process 14
6.5 Group signature verification process 14
6.6 Group membership opening process 14
6.7 Group signature linking process 15
6.8 Group signature revocation process 16
7 Mechanisms using multiple public keys **19**
7.1 General model 19
7.2 Entities 19
7.3 Key generation process 19
7.4 Ring signature process 19
7.5 Ring signature verification process 19
Bibliography **20**

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20008-1:2013

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 20008-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 20008 consists of the following parts, under the general title *Information technology — Security techniques — Anonymous digital signatures*:

— *Part 1: General*

— *Part 2: Mechanisms using a group public key*

Further parts may follow.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20008-1:2013

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity. A digital signature mechanism enables the holder (or holders) of a private key (or keys) to singly or collectively generate a digital signature for a message. The corresponding verification key (or keys) can be used to verify the validity of the signature on the message. A digital signature mechanism satisfies the following requirements.

— Given either or both of the following:

  — the verification key but not the signature key,

  — a set of signatures on a sequence of messages that an attacker has adaptively chosen,

  it should be computationally infeasible for an attacker:

  — to produce a valid signature on a new message,

  — to recover the signature key, or

  — in some circumstances, to produce a different valid signature on a previously signed message.

— It should be computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE Computational feasibility depends on the specific security requirements and environment.

Anonymous digital signature mechanisms are a special type of digital signature mechanism. In an anonymous digital signature mechanism, given a digital signature, an unauthorised entity, including the verifier, cannot discover the signer's identifier. However, such a mechanism still has the property that only a legitimate signer can generate a valid signature. For authorised entities involved in an anonymous signature mechanism, there are four different cases:

a) a mechanism involving an authorised entity that is capable of identifying the signer of a signature;

b) a mechanism involving an authorised entity that is only capable of linking two signatures created by the same signer without identifying the signer;

c) a mechanism involving both of the authorised entities in Cases a) and b);

d) a mechanism involving neither of the authorised entities in Cases a) and b).

An example application of anonymous digital signatures is to achieve anonymous entity authentication. Anonymous entity authentication mechanisms are specified in ISO/IEC 20009.

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

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

— a process for creating an anonymous digital signature that uses the signature key;

— a process for verifying an anonymous digital signature that uses the verification key.

NOTE A private signature key is also known as a signing key or a private key, and a public verification key is also known as a verification key or a public key.

One of the major differences between a conventional digital signature and an anonymous digital signature is in the nature of the public keys used to perform the signature verification. To verify a conventional digital signature, the verifier makes use of a single public verification key which is bound to the signer's identifier. To verify an anonymous digital signature, the verifier makes use of either a group public key or multiple public keys, which are not bound to an individual signer. In the literature,

AVA Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 20008-1:2013

an anonymous signature using a group public key is commonly known as a group signature, and an anonymous signature using multiple public keys is commonly known as a ring signature. The anonymity strength (i.e. degree of anonymity) provided by a mechanism depends upon the size of the group and the number of public keys.

Like conventional digital signature mechanisms, the security of anonymous digital signature mechanisms depends on 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 and the discrete logarithm problem in an appropriate group. The mechanisms specified in ISO/IEC 20008 are based on at least one of these and other similar problems.

ISO/IEC 20008 specifies anonymous digital signature mechanisms. This part of ISO/IEC 20008 specifies principles and requirements for two categories of anonymous digital signatures mechanisms: signature mechanisms using a group public key, and signature mechanisms using multiple public keys. ISO/IEC 20008-2 specifies a number of anonymous signature mechanisms in the first category.

NOTE If a business need for the development of mechanisms of the second category is discovered, then a new part of ISO/IEC 20008 should be added, which might, for example, be entitled Part 3: Mechanisms using multiple public keys.

The mechanisms specified in ISO/IEC 20008 use a variety of other standardised cryptographic algorithms, for example, as follows.

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

— They can 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 and ISO/IEC 14888.

— They can require the use of a conventional entity authentication mechanism, if the entities performing the mechanism require the data communicated as part of the mechanism to be authenticated. Entity authentication mechanisms are specified in ISO/IEC 9798.

— They can require the use of a conventional asymmetric encryption mechanism, if some information of the entities involved in the anonymous digital signature mechanisms is required to be encrypted for the purposes of privacy and confidentiality. Asymmetric encryption mechanisms are specified in ISO/IEC 18033-2.

Revocation is defined as 'the withdrawal of some power or authority that has been granted.' In the context of conventional digital signature mechanisms, it refers to withdrawing the power of a signing key that has been granted. Typically, a Certificate Revocation List is used for this purpose. Such a list specifies the certificate or public key corresponding to the signing key that needs to be revoked. A verifier can check whether or not a given signature was generated using a revoked signing key by checking the Certificate Revocation List. A verifier can also generate a personal blacklist of public keys as a local revocation list, and can then reject any signatures generated using a key corresponding to an entry in the list.

In an anonymous digital signature mechanism using multiple public keys, a public key can be revoked in the same way as in a conventional signature mechanism.

In an anonymous digital signature mechanism using a group public key, it is possible to revoke three different levels of authorization granted to an entity or a group of entities.

a) The entire group can be revoked.

b) The membership of a certain group member can be revoked. As a result, the revoked member is no longer authorised to create a group signature on behalf of the group.

c) A signature verifier can revoke the authorization for a group member to create a certain type of anonymous signature. After such a revocation, the member to whom the revocation applies might still be able to create other anonymous signatures on behalf of the group.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 20008-1:2013

INTERNATIONAL STANDARD ISO/IEC 20008-1:2013(E)

Information technology — Security techniques — Anonymous digital signatures —

Part 1: General

1 Scope

This part of ISO/IEC 20008 specifies principles, including a general model, a set of entities, a number of processes, and general requirements for the following two categories of anonymous digital signature mechanisms:

a) signature mechanisms using a group public key, and

b) signature mechanisms using multiple public keys.

2 Terms and definitions

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

2.1
anonymous digital signature
signature which can be verified using a group public key or multiple public keys, and which cannot be traced to the distinguishing identifier of its signer by any unauthorised entity including the signature verifier

Note 1 to entry: Anonymous digital signatures are also known as anonymous signatures or simply digital signatures.

2.2
anonymity strength
number derived from the probability that an unauthorised entity can correctly determine the true signer from a given signature

Note 1 to entry: An anonymity strength of n means that the probability that an unauthorised entity can correctly guess the true signer from a signature is $1/n$.

2.3
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

[SOURCE: ISO/IEC 10118-1:2000]

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment.

2.4
data element
integer, bit string, set of integers, or set of bit strings

[SOURCE: ISO/IEC 14888-1:2008]

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20008-1:2013

2.5
distinguishing identifier
information which unambiguously distinguishes an entity

[SOURCE: ISO/IEC 11770-2:2008]

2.6
domain
set of entities operating under a single security policy

[SOURCE: ISO/IEC 14888-1:2008]

EXAMPLE Public key certificates created by a single authority or by a set of authorities using the same security policy.

2.7
domain parameter
data element which is common to and known by or accessible to all entities within the domain

[SOURCE: ISO/IEC 14888-1:2008]

2.8
evidence of binding
data element which demonstrates the cryptographic binding between the signer and the signature, and which is an output from the group membership opening process

2.9
evidence evaluation process
process which takes as inputs the evidence of binding, the group signature, and the group public key, and gives as output the result of evidence evaluation: valid or invalid

Note 1 to entry: The group signature input to an evidence evaluation process must be valid, i.e. the signature shall have previously been successfully verified using the group signature verification process.

2.10
evidence evaluator
entity which checks the validity of the evidence of binding

2.11
group
set of entities operating under a single membership management policy

Note 1 to entry: A group includes multiple group members and each member has a membership credential which is created by a group membership issuer as part of the group membership issuing process.

2.12
group member
entity which has a group membership credential and can create a group signature on behalf of the group

2.13
group member private key
private data element which is part of the group member signature key, specific to a group member and usable only by the member in the group membership issuing and group signature processes

2.14
group member signature key
set of data elements specific to a group member, consisting of the group member private key and group membership credential, and usable only by the member in the group signature process

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20008-1:2013