INTERNATIONAL STANDARD

ISO/IEC 13888-1

Third edition
2009-07-15

Information technology — Security techniques — Non-repudiation —

Part 1: General

Technologies de l'information — Techniques de sécurité — Non-répudiation —

Partie 1: Généralités

Reference number
ISO/IEC 13888-1:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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

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.

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 13888-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 13888-1:2004), which has been technically revised.

ISO/IEC 13888 consists of the following parts, under the general title *Information technology — Security techniques — Non-repudiation*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric techniques*
- *Part 3: Mechanisms using asymmetric techniques*

Introduction

The goal of a non-repudiation service is to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non occurrence of the event or action. This part of ISO/IEC 13888 defines a model for non-repudiation mechanisms providing evidence based on cryptographic check values generated using symmetric or asymmetric cryptographic techniques.

Non-repudiation services establish evidence; evidence establishes accountability regarding a particular event or action. The entity responsible for the action, or associated with the event, with regard to which evidence is generated, is known as the evidence subject.

Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific to each non-repudiation service. Non-repudiation tokens consist of secure envelopes and/or digital signatures and, optionally, additional data:

- Secure envelopes are generated by an evidence generating authority using symmetric cryptographic techniques.
- Digital signatures are generated by an evidence generator or an evidence generating authority using asymmetric techniques.

Non-repudiation tokens can be stored as non-repudiation information that can be used subsequently by disputing parties or by an adjudicator to arbitrate in disputes.

Depending on the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, additional information may be required to complete the non-repudiation information, for example:

- evidence including a trusted time-stamp provided by a time-stamping authority,
- evidence provided by a notary which provides assurance about data created or the action or event performed by one or more entities.

Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment. Non-repudiation policies are described in ISO/IEC 10181-4.

Specific non-repudiation mechanisms generic to the various non-repudiation services are first described and then applied to a selection of specific non-repudiation services such as:

- non-repudiation of origin,
- non-repudiation of delivery,
- non-repudiation of submission,
- non-repudiation of transport.

Additional non-repudiation services mentioned in this part of ISO/IEC 13888 are:

- non-repudiation of creation,
- non-repudiation of receipt,
- non-repudiation of knowledge,
- non-repudiation of sending.

Information technology — Security techniques — Non-repudiation —

Part 1: General

1 Scope

This part of ISO/IEC 13888 serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. ISO/IEC 13888 provides non-repudiation mechanisms for the following phases of non-repudiation:

- evidence generation;
- evidence transfer, storage and retrieval; and
- evidence verification.

Dispute arbitration is outside the scope of ISO/IEC 13888.

2 Normative references

The following referenced documents are indispensable for the application 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 10181-4:1997, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework*

ISO/IEC 18014 (all parts), *Information technology — Security techniques — Time-stamping services*

3 Terms and definitions

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

3.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2]

3.2
certificate
entity's data rendered unforgeable with the private or secret key of a certification authority

3.3
certification authority
authority trusted by one or more users to create and assign certificates

NOTE 1 Adapted from ISO/IEC 9594-8:2001, 3.3.17.

NOTE 2 Optionally the certification authority can create the users‘ keys.

3.4
cryptographic check function
cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output

3.5
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

3.6
data origin authentication
corroboration that the source of data received is as claimed

[ISO 7498-2]

3.7
data storage
means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority

3.8
delivery authority
authority trusted by the sender to deliver the data from the sender to the receiver, and to provide the sender with evidence on the submission and transport of data upon request

3.9
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO 7498-2]

3.10
distinguishing identifier
information which unambiguously distinguishes an entity in the non-repudiation process

3.11
evidence
information which is used, either by itself or in conjunction with other information, to establish proof about an event or action

NOTE Evidence does not necessarily prove the truth or existence of something (see proof) but can contribute to the establishment of such a proof.

3.12
evidence generator
entity that produces non-repudiation evidence

[ISO/IEC 10181-4]

3.13
evidence user
entity that uses non-repudiation evidence

[ISO/IEC 10181-4]

3.14
evidence verifier
entity that verifies non-repudiation evidence

[ISO/IEC 10181-4]

3.15
evidence requester
entity requesting evidence to be generated either by another entity or by a trusted third party

3.16
evidence subject
entity responsible for the action, or associated with the event, with regard to which evidence is generated

3.17
hash-code
string of bits that is the output of a hash-function

[ISO/IEC 10118-1]

3.18
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— it is computationally infeasible to find for a given output an input which maps to this output;

— it is computationally infeasible to find for a given input a second input which maps to the same output

[ISO/IEC 10118-1]

3.19
imprint
string of bits, either the hash-code of a data string or the data string itself

3.20
key
sequence of symbols that controls the operations of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check-function computation, signature calculation, or signature verification)

[ISO/IEC 11770-3]

3.21
monitoring authority
monitor
trusted third party monitoring actions and events, and that is trusted to provide evidence about what has been monitored

3.22
Message Authentication Code
MAC
string of bits which is the output of a MAC algorithm

[ISO/IEC 9797-1]

NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

3.23
Message Authentication Code algorithm
MAC algorithm
algorithm for computing a function that maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

- for any key and any input string the function can be computed efficiently;
- for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first $i - 1$ function values

NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2).

NOTE 2 Computational feasibility depends on the user's specific security requirements and environment.

[ISO/IEC 9797-1]

3.24
non-repudiation of creation
service intended to protect against an entity's false denial of having created the content of a message (i.e. being responsible for the content of a message)

3.25
non-repudiation of delivery
service intended to protect against a recipient's false denial of having received a message and recognised the content of a message

3.26
non-repudiation of delivery token
data item which allows the originator to establish non-repudiation of delivery for a message

3.27
non-repudiation exchange
sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation

3.28
non-repudiation information
set of information that may contain information about an event or action for which evidence is to be generated and verified, the evidence itself, and the non-repudiation policy in effect

3.29
non-repudiation of knowledge
service intended to protect against a recipient's false denial of having taken notice of the content of a received message

3.30
non-repudiation of origin
service intended to protect against the originator's false denial of having created the content of a message and of having sent a message

3.31
non-repudiation of origin token
data item which allows recipients to establish non-repudiation of origin for a message

3.32
non-repudiation policy
set of criteria for the provision of non-repudiation services

NOTE More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.

3.33
non-repudiation of receipt
service intended to protect against a recipient's false denial of having received a message

3.34
non-repudiation of sending
service intended to protect against the sender's false denial of having sent a message

3.35
non-repudiation service requester
entity that requests that non-repudiation evidence be generated for a particular event or action

3.36
non-repudiation of submission
service intended to provide evidence that a delivery authority has accepted a message for transmission

3.37
non-repudiation of submission token
data item which allows either the originator (sender) or the delivery authority to establish non-repudiation of submission for a message having been submitted for transmission

3.38
non-repudiation token
special type of security token as defined in ISO/IEC 10181-1, consisting of evidence, and, optionally, of additional data

3.39
non-repudiation of transport
service intended to provide evidence for the message originator that a delivery authority has delivered a message to the intended recipient

3.40
non-repudiation of transport token
a data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message

3.41
notary authority
trusted third party trusted to provide evidence about the properties of the entities involved and of the data stored or communicated, or to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation

3.42
notarization
provision of evidence by a notary about the properties of the entities involved in an action or event, and of the data stored or communicated

3.43
notarization token
non-repudiation token generated by a notary

3.44
originator
entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided