INTERNATIONAL STANDARD

ISO/IEC 13888-1

Fourth edition
2020-09

Information security — Non-repudiation —

Part 1: General

Sécurité de l'information — Non-répudiation —

Partie 1: Généralités

Reference number
ISO/IEC 13888-1:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1 *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 13888-1:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

— Clause 3 has been updated;

— terminology issues have been fixed; and

— a new requirement has been introduced when using hash functions.

A list of all parts in the ISO/IEC 13888 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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 document 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 can 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 document are:

— non-repudiation of creation;

— non-repudiation of receipt;

— non-repudiation of knowledge;

— non-repudiation of sending.

Information security — Non-repudiation —

Part 1: General

1 Scope

This document serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques.

The ISO/IEC 13888 series 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 the ISO/IEC 13888 series.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
adjudicator
entity which arbitrates disputes between parties

3.2
certificate
entity's data rendered unforgeable with the private or *secret key* (3.48) of a *certification authority* (3.3)

Note 1 to entry: Unforgeable means impossible to copy or imitate unlawfully.

3.3
certification authority
CA
authority trusted by one or more entities to create and assign *certificates* (3.2) or digitally signed *public key certificates* (3.46)

[SOURCE: ISO/IEC 9594-8:2017, 3.5.19, modified — In the definition, the initial article has been removed and "assign certificates" has been added.]

3.4
collision-resistant hash-function
hash-function (3.18) satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

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

[SOURCE: ISO/IEC 10118-1:2016, 2.1, modified — In Note 1 to entry, the second sentence has been removed.]

3.5
cryptographic check function
CHK
either a *MAC* (3.22) function or a *digital signature* (3.9) function, i.e. a function that takes as an input a message and a secret or *private key* (3.44) and returns a string of bits that can be used to verify the origin and integrity of the message

3.6
cryptographic check value
output of a *cryptographic check function* (3.5)

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)

3.8
delivery authority
DA
authority trusted by the *sender* (3.43) to deliver the data from the sender to the receiver, and to provide the sender with *evidence* (3.11) on the submission and transport of data upon request

3.9
digital signature
SIG
data appended to, or a cryptographic transformation of, a data unit that allows the *recipient* (3.47) of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ISO 7498-2:1989, 3.3.26 modified — The abbreviated term "SIG" has been added.]

3.10
distinguishing identifier
information which unambiguously distinguishes an entity in the *non-repudiation process* (3.32)

3.11
evidence
information supporting the occurrence of an event or action

Note 1 to entry: Evidence does not necessarily prove the truth or existence of something but can contribute to the establishment of such a proof.

3.12
evidence generator
entity that produces non-repudiation *evidence* (3.11)

[SOURCE: ISO/IEC 10181-4:1997, 3.4.4, modified — The initial article has been removed from the definition and the Note has been deleted]

3.13
evidence user
entity that uses non-repudiation *evidence* (3.11)

[SOURCE: ISO/IEC 10181-4:1997, 3.4.6, modified — The initial article has been removed from the definition.]

3.14
evidence verifier
entity that verifies non-repudiation *evidence* (3.11)

[SOURCE: ISO/IEC 10181-4:1997, 3.4.7, modified — The initial article has been removed from the definition.]

3.15
evidence requester
entity that requests *evidence* (3.11) to be generated either by another entity or by a *trusted third party* (3.55)

3.16
evidence subject
entity responsible for the action, or associated with the event, with regard to which *evidence* (3.11) is generated

3.17
hash-code
string of bits that is the output of a *hash-function* (3.18)

[SOURCE: ISO/IEC 10118-1:2016, 3.3, modified — Note 1 to entry has been removed.]

3.18
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

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

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

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

Note 2 to entry: In the ISO/IEC 13888 series, hash-functions are required to be collision-resistant.

[SOURCE: ISO/IEC 10118-1:2016, 3.4, modified — In Note 1 to entry, the second sentence has been removed and Note 2 to entry has been added.]

3.19
imprint
string of bits, either the *hash-code* (3.17) 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. encryption, decryption, cryptographic check function computation, signature calculation, or signature verification)

[SOURCE: ISO/IEC 11770-3:2015, 3.17, modified — In the definition, "operation" has been replaced with "operations".]

3.21
monitoring authority
trusted third party (3.55) that monitors actions and events, and that is trusted to provide *evidence* (3.11) about actions and events that have been monitored

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

3.23
non-repudiation of creation
service intended to protect against an entity's false denial of having created the content of a message or the message itself (i.e. being responsible for the content of a message or the message itself)

3.24
non-repudiation of delivery
service intended to protect against a *recipient's* (3.47) false denial of having received a message and its content

3.25
non-repudiation of delivery token
NRDT
data item which allows the *sender* (3.43) to establish *non-repudiation of delivery* (3.24) for a message

3.26
non-repudiation exchange
sequence of one or more transfers of *non-repudiation information* (3.27) for the purpose of non-repudiation

3.27
non-repudiation information
NRI
set of information that may contain information about an event or action for which *evidence* (3.11) is to be generated and verified, the evidence itself, and the *non-repudiation policy* (3.31) in effect

Note 1 to entry: The exact format and specifications depend on the chosen mechanism.

3.28
non-repudiation of knowledge
service intended to protect against a *recipient's* (3.47) false denial of having taken notice of the content of a received message

Note 1 to entry: The exact format and specifications depend on the chosen mechanism.

3.29
non-repudiation of origin
service intended to protect against the *sender's* (3.43) false denial of having created the content of a message and of having sent a message