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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

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

© ISO/IEC 2020

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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

 © ISO/IEC 2020 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

 © ISO/IEC 2020 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

3.30
non-repudiation of origin token
NROT
data item which allows *recipients* (3.47) to establish *non-repudiation of origin* (3.29) for a message

3.31
non-repudiation policy
set of criteria for the provision of non-repudiation services

Note 1 to entry: More specifically, it is a set of rules to be applied for the generation and verification of *evidence* (3.11) and for adjudication.

3.32
non-repudiation process
set of interrelated or interacting activities which provides one or more non-repudiation services

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

3.33
non-repudiation of receipt
service intended to protect against a *recipient's* (3.47) false denial of having received a message

3.34
non-repudiation of sending
service intended to protect against the *sender's* (3.43) false denial of having sent a message

3.35
non-repudiation of submission
service intended to provide *evidence* (3.11) that a *delivery authority* (3.8) has accepted a message for transmission

3.36
non-repudiation of submission token
NRST
data item which allows either the *originator* (3.43) or the *delivery authority* (3.8) (sender) to establish *non-repudiation of submission* (3.35) for a message having been submitted for transmission

Note 1 to entry: A non-repudiation of submission token is generated by the initial receiver except when the receiver is a *recipient* (3.47).

3.37
non-repudiation token
NRT
special type of *security token* (3.51), consisting of *evidence* (3.11), and, optionally, of additional data

3.38
non-repudiation of transport
service intended to provide *evidence* (3.11) for the message *sender* (3.43) that a *delivery authority* (3.8) has delivered a message to the intended *recipient* (3.47)

Note 1 to entry: A non-repudiation of transport token is generated by the initial receiver except when the receiver is a *recipient* (3.47).

3.39
non-repudiation of transport token
NRTT
data item which allows either the *originator* (3.43) or the *delivery authority* (3.8) to establish non-repudiation of transport for a message

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

3.40
notary authority
NA
trusted third party (3.55) trusted to provide *evidence* (3.11) 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

3.41
notarization
provision of *evidence* (3.11) by a notary about the properties of the entities involved in an action or event, and of the data stored or communicated

Note 1 to entry: Notarization can also extend the lifetime of an existing token.

3.42
notarization token
NT
non-repudiation token (3.37) generated by a notary

3.43
originator
sender
entity that sends a message to the *recipient* (3.47) or makes available a message for which non-repudiation services are to be provided

3.44
private key
key (3.20) of an entity's asymmetric key pair which can only be used by that entity

Note 1 to entry: In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.

3.45
public key
key (3.20) of an entity's asymmetric key pair which can be made public

Note 1 to entry: In the case of an asymmetric signature scheme, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key might only be available to all members of a pre-specified group.

3.46
public key certificate
public key (3.45) information of an entity signed by the *certification authority* (3.3) and thereby rendered unforgeable

[SOURCE: ISO/IEC 11770-3:2015, 3.34]

3.47
recipient
entity that gets (receives or fetches) a message for which non-repudiation services are to be provided

3.48
secret key
key (3.20) used with symmetric cryptographic techniques and usable only by a set of specified entities

[SOURCE: ISO/IEC 11770-3:2015, 3.36, modified — In the definition, “and usable only” has been added and “specified set of entities” has been changed to “set of specified entities”]

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

 © ISO/IEC 2020 – All rights reserved

3.49
secure envelope
SENV
set of data items which is constructed by an entity in such a way that any entity holding the *secret key* (3.48) can verify their integrity and origin

Note 1 to entry: For the purpose of generating *evidence* (3.11), the SENV is constructed and verified by a *trusted third party* (3.55) (TTP) with a secret key known only to the TTP.

Note 2 to entry: Cryptographic check functions are used to generate secure envelopes.

3.50
security policy
set of criteria for the provision of security services

3.51
security token
set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities

3.52
signer
entity generating a *digital signature* (3.9)

3.53
time-stamp
time variant parameter which denotes a point in time with respect to a common time reference

[SOURCE: ISO/IEC 18014-1:2008, 3.12]

3.54
time-stamping authority
TSA
trusted third party (3.55) trusted to provide a time-stamping service

[SOURCE: ISO/IEC 18014-1:2008, 3.17]

3.55
trusted third party
TTP
security authority, or its agent, trusted by other entities with respect to security-related activities

Note 1 to entry: In the context of the ISO/IEC 13888 series, a trusted third party is trusted by the *sender* (3.43), the *recipient* (3.42), and/or the *delivery authority* (3.8) for the purposes of non-repudiation, and by another party such as an *adjudicator* (3.1).

[SOURCE: ISO/IEC 10181-1:1996, 3.3.30, modified — The abbreviated term "TTP" has been added. In the definition, "by other entities" has been added, "security-relevant" has been changed to "security-related" and the parentheses have been removed. Note 1 to entry has been added.]

3.56
trusted time-stamp
time-stamp (3.53) generated by a *time-stamping authority* (3.54)

3.57
verification key
value required to verify a *MAC* (3.22)

3.58
verifier
entity that verifies *evidence* (3.11)

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

4 Symbols and abbreviated terms

4.1 Symbols

A, B, C, D, E	distinguishing identifiers
$CHK_X(y)$	cryptographic check value computed on the data y using the key of entity X
DA	distinguishing identifier of a delivery authority
f	flag indicating the notary service
$GNRT$	distinguishing identifier of a generic non-repudiation token
$Imp(y)$	imprint of the data string y, either the hash-code of data string y, or the data string y
$MAC_X(y)$	MAC computed on the data y using the key of entity X
m	message for which evidence is generated
n	number of sub-delivery authorities in a chain of sub-delivery authorities
NA	distinguishing identifier of the notary authority
$NRDT$	distinguishing identifier of a non-repudiation of delivery token
NRI	distinguishing identifier of a non-repudiation information
$NROT$	distinguishing identifier of a non-repudiation of origin token
$NRST$	distinguishing identifier of a non-repudiation of submission token
$NRTT$	distinguishing identifier of a non-repudiation of transport token
NT	distinguishing identifier of a notarization token
Pol	distinguishing identifier of a non-repudiation policy (or policies) which apply to evidence
Q	optional data that needs to be origin/integrity protected
$SENV_X(y)$	secure envelope computed on data y using the secret key of entity X
$SIG_X(y)$	signed message generated on data y by entity X using its private key
$S_X(y)$	signature computed on data y using a signature algorithm and the private key of entity X
$text$	data item forming a part of the token that may contain additional information, e.g., a key identifier and/or message identifier
T_g	date and time the evidence was generated NOTE The date and time are represented as specified in ISO 8601. ISO 14641 provides guidance on methods for obtaining the current date and time.
T_i	date and time an event or action took place
TSA	distinguishing identifier of the time-stamping authority
TTP	distinguishing identifier of the trusted third party

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

$V_X(y)$ verification operation applied to data y (a secure envelope or a digital signature) by using a verification algorithm and the verification key of entity X

w, y, z different data

(y, z) result of the concatenation of y and z in that order

4.2 Abbreviated terms

GNRT generic non-repudiation token

TA trusted authority

TST time-stamp token

5 Document organization

Non-repudiation services are modelled by first specifying basic requirements in Clause 6, and then describing in Clause 7 the roles of the entities involved in the provision and verification of evidence. The involvement of trusted third parties in the various phases of non-repudiation, in particular in the provision and verification of evidence, is described in Clause 8. Evidence generation and verification mechanisms are described in Clause 9, involving the generation of secure envelopes and digital signatures based on symmetric and asymmetric cryptographic techniques. Cryptographic check functions common to both basic mechanisms are derived in order to better represent non-repudiation tokens. In Clause 10, three kinds of tokens are defined:

1) the generic non-repudiation token suitable for many non-repudiation services;

2) the time-stamp token generated by a time-stamping authority; and

3) the notarization token generated by a notary to provide evidence about the properties of the entities involved and of the data stored or communicated.

Specific non-repudiation services and non-repudiation tokens are described in Clause 11. An example of the use of specific non-repudiation tokens in a messaging environment is given in Clause 12.

6 Requirements

Depending on the nature of the CHK used for generating SENVs and SIGs, and independent of the non-repudiation service supported by the non-repudiation mechanisms, the following requirements hold for the entities involved in a non-repudiation exchange.

— The entities of a non-repudiation exchange shall trust any TTP involved in the exchange.

NOTE When using symmetric cryptographic algorithms, a TTP is always required. When using asymmetric cryptographic algorithms, a TTP is always required to either generate a public-key certificate or create a SIG for evidence.

— Prior to the generation of evidence, the evidence generator shall know which non-repudiation policy is acceptable to the verifier(s), the kind of evidence that is required and the set of mechanisms that are acceptable to the verifier(s).

— Either the mechanisms for generating or verifying evidence shall be available to the entities of the particular non-repudiation exchange, or a trusted authority shall be available to provide the mechanisms and perform the necessary functions on behalf of the evidence requester.

— The relevant entities shall be in possession of (and, when necessary, share) the keys required for the mechanisms being used (i.e., private keys for asymmetric mechanisms, and secret keys for symmetric mechanisms).

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

— The evidence user and the adjudicator shall be evidence verifiers or shall trust an entity to perform the services of an evidence verifier.

— If a trusted time-stamp is required, or the clock provided by the party generating evidence cannot be trusted, then a time-stamping authority shall be accessible to the evidence generator or the evidence verifier.

— If a hash-function is required in any of the mechanisms described in the ISO/IEC 13888 series, it shall be a collision-resistant hash-function.

7 Generic non-repudiation services

7.1 Non-repudiation services

Non-repudiation involves the generation of evidence that can be used to prove that an event or action has taken place. Evidence is generated in the form of verifiable data describing the actions or events. Data and evidence are stored or communicated in a non-repudiation exchange between the parties involved. Evidence is transmitted in NRTs as part of non-repudiation exchanges.

Some non-repudiation services may be provided by grouping other services. For example, non-repudiation of origin can be provided by combining non-repudiation of creation and non-repudiation of sending, and non-repudiation of delivery can be provided by combining non-repudiation of receipt and non-repudiation of knowledge.

7.2 Entities involved in the provision and verification of evidence

A number of distinct entities are involved in the provision of a non-repudiation service.

Three entities are involved in the evidence generation phase:

— the evidence requester that wants to obtain evidence;

— the evidence subject that performs an action or is involved in an event;

— the evidence generator that generates evidence.

Two entities are involved in the evidence verification phase:

— the evidence user who may or may not be able to verify it directly;

— the evidence verifier that is able to verify evidence upon request from the evidence user.

In the evidence generation phase, the event or action is related to an evidence subject. The evidence may be provided upon request by the evidence requester or by the evidence subject itself.

In some cases, only two entities (the evidence subject and the evidence requester) are needed to provide evidence, but in other cases a third party is necessary to produce evidence. Evidence is then returned or made available to the evidence requester: evidence may then be transferred or made available to other entities.

In the evidence verification phase, an evidence user wishes to verify that the evidence is correct. If the evidence user is unable to verify the evidence directly, the evidence is verified by an evidence verifier upon request from the evidence user.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

8 Trusted third party involvement

8.1 General

Trusted third parties may be involved in the provision of non-repudiation services, depending on the mechanisms used and the non-repudiation policy in effect. The use of asymmetric cryptographic techniques requires authentic public keys which can be provided by certificates issued by third parties, e.g. by certification authorities. The use of symmetric cryptographic techniques requires the involvement of an online trusted third party to generate and verify SENVs. The non-repudiation policy in effect can require evidence to be generated partly or totally by a TTP.

The non-repudiation policy in effect can also require that:

— a trusted time-stamp be provided by a TSA;

— a notary be involved to verify data provided by one or more parties and to return data to the parties along with a SIG computed on this data ; and/or

— a monitoring authority be involved to provide evidence about the properties of the entities involved and of the data stored or communicated.

TTPs may be involved to differing degrees in the phases of non-repudiation. When exchanging evidence, the parties shall either know, be informed or agree as to which non-repudiation policy is to be applicable to the evidence.

There may be a number of TTPs involved acting in various roles (e.g., notary, time-stamping, monitoring, key certification, signature generation, signature verification, secure envelope generation, secure envelope verification, token generation or delivery roles), as dictated by the non-repudiation policy. A single TTP may act in one or more of these roles.

8.2 Evidence generation phase

Evidence is information that can be used to resolve disputes and is generated by an evidence generator on behalf of an evidence subject, a trusted third party or upon request of an evidence requester. A TTP can be involved in an evidence generation phase in the following ways (for definitions of online, in-line and offline authority, see ISO/IEC TR 14516):

— directly:

  — when acting as an online authority actively involved in every instance of the non-repudiation service, the TTP generates evidence alone on behalf of the evidence subject. Online generation of cryptographic check values and NRTs may be required when symmetric cryptographic techniques are used for the provision of evidence, i.e. to generate SENVs as defined in ISO/IEC 13888-2;

  — when acting as an in-line evidence generation authority, the TTP generates the evidence by itself, e.g. as a delivery authority;

— indirectly:

  — when acting as an off-line authority which is not involved in every instance of a non-repudiation service, the TTP provides off-line public key certificates related to entities generating evidence based on SIGs;

  — when acting as a token generation authority, the TTP constructs an NRT composed of one or more NRTs provided by the evidence subject or by one or more trusted authorities;

  — when acting as a SIG generating authority, the TTP generates SIGs on behalf of the evidence subject or an evidence requester;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

— when acting as a TSA [see ISO/IEC 18014 (all parts)], the TTP is trusted to provide evidence which includes the time when the time-stamp token was generated;

— when acting as a notary authority (notary), the TTP is trusted to provide evidence about the properties of the entities involved and of the data stored or communicated between the entities. In some cases, the notary is trusted to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation;

— when acting as a monitoring authority, the TTP monitors actions and events and is trusted to provide evidence about what was monitored.

8.3 Evidence transfer, storage and retrieval phase

During this phase, evidence is transferred between parties, or to and from storage. Depending on the non-repudiation policy in effect, the activities of this phase may not always occur in all cases of a non-repudiation service. The activities of this phase may be performed by TTPs or other parties.

— When acting as a delivery authority, the TTP is in-line for non-repudiation of submission and non-repudiation of transport.

— When acting as an evidence record keeping authority, the TTP records evidence that can later be retrieved by an evidence user or an adjudicator.

8.4 Evidence verification phase

When acting as an evidence verification authority, the TTP acts as an online authority which is trusted by the evidence user to verify non-repudiation information provided in the NRT. When evidence is generated using symmetric cryptographic techniques, it can only be verified by a TTP. Otherwise, the involvement of a TTP may be optional.

The means used to verify an NRT depend on the techniques used to create it.

— SENVs can only be verified by a TTP.

— SIGs may be verified using one or more public key certificates and certificate revocation lists which were all valid at the time the evidence was generated.

— Public key certificates valid at the time the evidence is presented shall be verified for the time the evidence was generated. In the case where a public key certificate has either expired or revoked at the time the evidence is presented, this may be accomplished by verifying the public key certificate for the time asserted in a time-stamp token or a notarization token included in the evidence, according to the non-repudiation policy in effect.

— (Public key) Certificate revocation lists valid at the time the evidence was generated shall be verified at the time the evidence is presented. In some cases, this may be years later.

— Where the non-repudiation service requires the use of a TSA to provide evidence, it shall be presented in the following way. The time value enclosed in that evidence (i.e. in the TST) has to be compared with the time value enclosed in the evidence produced by the generating entity, a TTP or an evidence requester. When the validity of these time values has been verified according to the security policy, then the evidence of their generation by the generating entity, a TTP or an evidence requester can be accepted.

— Additional NRTs (e.g. notarization token) are verified according to the techniques used for their generation.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

9 Evidence generation and verification mechanisms

9.1 General

In these phases, evidence is represented by NRTs consisting of either SENVs or SIGs. Both are based on cryptographic check values generated by either symmetric or asymmetric cryptographic techniques. When using certificate-based signatures, the NRT consists of the signed message (which consists of the message and the signature) and associated public key certificate(s). If an appropriate public key certificate is not provided with the SIG, the certificate shall be made available to the appropriate parties by other means. When using identity-based signatures [see ISO/IEC 14888 (all parts)], the NRT consists of the signed message, the signing entity's identification data and the identity (i.e. the distinguishing identifier) of the authority providing one or both keys to the signer.

9.2 Secure envelopes

For a SENV to become valid evidence, it shall be generated by a TTP using a secret key known only to the TTP.

A SENV is created through the use of symmetric integrity techniques on data y, using the secret key of entity X to provide $MAC_X(y)$ which is appended to the data y:

$$SENV_X(y) = (y, MAC_X(y))$$

NOTE The function *MAC* can be a message authentication code as specified in the ISO/IEC 9797 series.

Further secure envelope mechanisms can be specified in specific parts of the ISO/IEC 13888 series.

9.3 Digital signatures

An entity X can sign a message y using a digital signing operation and its private key. The resulting signed message is denoted by $SIG_X(y)$. The validity of the signed message $SIG_X(y)$ can be verified by anyone that has an authentic copy of the public key of entity X.

If the SIG operation does not allow message recovery, the signed message is formed by appending a signature $S_X(y)$ to the message y:

$$SIG_X(y) = (y, S_X(y))$$

If the SIG operation allows message recovery, part or all of the message y can be recovered from $S_X(y)$; then the signed message $SIG_X(y)$ can be formed by appending $S_X(y)$ to the part of y that cannot be recovered from the signature $S_X(y)$.

NOTE 1 Digital signatures giving message recovery are specified in the ISO/IEC 9796 series.

NOTE 2 Digital signatures with appendix are specified in the ISO/IEC 14888 series and lightweight digital signatures are specified in ISO/IEC 29192-4.

9.4 Evidence verification mechanism

SENVs or SIGs are verified by applying the verification operation $V_X(y)$, with y a SENV or a SIG respectively using the verification key of the evidence generating entity X. The output of the verification operation is positive or negative.

SENVs can only be verified by a TTP holding the secret key used to generate the secure envelope.

NOTE If the SENV is generated for origin/integrity protected communication, it can be verified by any entity holding the appropriate secret key.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

SIGs can be verified by any entity holding the public key of the signer. The means used to provide the public verification key to the verifier depends on the type of signature scheme applied to generate the SIG.

— Certificate-based signatures are verified using the public key of the signer, which can be retrieved from a public key certificate issued by the CA.

— Identity-based signatures are verified by any entity holding the signing entity's identification data and the public system parameters obtained from the TA providing the identity-based private keys to the signer.

When using SIGs, it is necessary, in some cases, to verify a chain of public key certificates or identities in order to obtain the necessary assurance.

10 Non-repudiation tokens

10.1 General

A non-repudiation service involves the generation and the verification of NRI. NRI is composed of one or more NRTs. The evidence generator shall provide at least one NRT derived from the GNRT. Additional tokens are normally required to verify the evidence. The additional tokens may or may not be provided to the verifier. When they are not provided, the verifier has to either fetch them (e.g. public key certificates and/or certificate revocation lists) or request them (e.g. time-stamping from TSAs). Three types of generic token are described within this document, namely the GNRT, the TST, and the NT. The tokens derived from the GNRT are generated by an evidence generator, while other tokens are generated by a TTP: the TST is generated by a TSA; the NT is generated by a NA.

Non-repudiation services can only be offered for a defined period of time. It can be necessary to alter the lifetime of a token after it has been issued, e.g. to shorten its lifetime if an attack on a particular signature scheme is found. On the other hand, if an NRT is adjudged to be (cryptographically) secure beyond its lifetime then the non-repudiation policy may allow the lifetime of that token to be extended (for example, by attaching to it a NT from a NA).

In the descriptions of generic tokens in Clause 10, $CHK_X(z)$ denotes either a MAC computed using the secret MAC key of entity X or a SIG computed using the private signature key of entity X. In the former case the generic tokens include a SENV.

10.2 Generic non-repudiation token

The GNRT *GNRT* is defined as follows:

$GNRT = (text, z, CHK_X(z))$ with

$z = (Pol, f, A, B, C, D, E, T_g, T_i, Q, Imp(m))$

The data field z consists of the following data items:

Pol distinguishing identifier(s) of the non-repudiation policy (or policies) which applies (apply) to the evidence;

f type of non-repudiation service being provided;

A distinguishing identifier of the evidence subject;

B distinguishing identifier of the evidence generator when different from the evidence subject;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

 © ISO/IEC 2020 – All rights reserved

C distinguishing identifier of the entity interacting with the evidence subject (e.g. the sender of a message; an intended recipient of a message or a delivery authority);

D distinguishing identifier of the evidence requester when different from the evidence subject;

E distinguishing identifiers of other entities involved with the action (e.g. the intended recipients of a message);

T_g date and time when the evidence was generated;

T_i date and time when the event or action took place;

Q optional data that need to be origin/ integrity protected;

$Imp(m)$ imprint of a message m related to an event or action.

NOTE Depending on the non-repudiation policy in effect, some data items can be optional.

When included in the token, the data field z shall be encoded so that it can be uniquely and unambiguously decomposed into its elements, and so that the meaning of each element is unambiguous to any entity that processes the token.

The distinguishing identifier A shall always be present. The other distinguishing identifiers B, C, D, E need not be present. The distinguishing identifier B of the evidence generator is needed when the evidence is produced by an authority on behalf of the evidence subject. The distinguishing identifier C is needed in the case of the transfer of a message. The distinguishing identifier D of the evidence requester is needed to cover the case where the evidence requester is different from the evidence subject. The distinguishing identifier(s) E of the other entity(ies) involved in the action cover the case of non-repudiation of submission to a delivery authority and non-repudiation of transport by a delivery authority.

The "*text*" field includes additional data that does not need to be cryptographically protected. The information in this field depends on the technique being used.

— For certificate-based signatures, the "*text*" field may contain one or more public key certificates or simply the distinguishing identifier of a certification authority together with the certificate serial number assigned to the public key certificate.

— For identity-based signatures, the "*text*" field may contain the distinguishing identifier of the authority providing one or both keys to the signer.

10.3 Time-stamp token

If a trusted time-stamp is required or the clock provided by the NRT generating party cannot be trusted, it is necessary to rely on a TTP, a TSA. Its role is to establish further evidence indicating the time the token was generated.

The TST *TST* provided by the TSA *TSA* shall be created using any method specified in the ISO/IEC 18014 series.

10.4 Notarization token

The notary service is used to provide evidence by a NA about the properties of the entities involved and of the data presented, or to extend the lifetime of an existing non-repudiation token beyond its expiry or beyond subsequent revocation.

The data y to which the token refers to is provided by the service-requesting entity.

NOTE The data y can be a message, a non-repudiation token, the hash-code of a message, the hash-code of a token, or any data the service requester wants to have certified by the notary.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

© ISO/IEC 2020 – All rights reserved

The NT *NT* is defined as follows:

$NT = (text, w, CHK_{NA}(w))$, with

$w = (Pol, f, A, NA, T_g, Q, Imp(y))$

The data element *w* consists of the following data items:

Pol	distinguishing identifier(s) of the non-repudiation policy (or policies) which applies (apply) to the evidence;
f	flag indicating the notary service;
A	distinguishing identifier of the entity requesting the notary service *f*;
NA	distinguishing identifier of the notary authority;
T_g	date and time when the notarization was performed;
Imp(*y*)	imprint of the data *y* for which a notary service is to be provided.

When included in the token, the data field *w* shall be encoded so that:

— it can be uniquely and unambiguously decomposed into its elements; and

— the meaning of each element is unambiguous to any entity that processes the token.

A similar token may be used by the monitoring authority to generate evidence on data *y* provided by the evidence subject and/or generated by the monitoring authority itself.

11 Specific non-repudiation services

11.1 General

The following specifies a specific set of actions, all related to the transfer of messages between entity *A* and entity *B*. Intermediaries, such as a delivery authority, are also involved.

Entity *A* creates a message *m* and establishes non-repudiation of origin of its own volition or as requested by the non-repudiation policy in effect or by another entity (e.g. a recipient). Non-repudiation of origin is provided by the evidence generator, which can be the originator itself or a TTP.

Entity *A* sends the message *m*, together with the evidence contained in a NROT *NROT* to entity *B*, the recipient (see Figure 1).

In some circumstances, one or more trusted third parties may perform the functions of a delivery authority. Where there is a delivery authority, all of the non-repudiation services described in Clause 11 can be provided.

In other circumstances, there cannot be a delivery authority. Where there is no delivery authority, only some of the non-repudiation services described in Clause 11 can be provided, i.e. only non-repudiation of origin and non-repudiation of delivery services can be provided.

Depending on the specific application and on the non-repudiation policy in effect, the delivery system is trusted to generate evidence that it has:

— received the message *m* with the non-repudiation token *NROT* from entity *A* for transmission to entity *B* by generating a non-repudiation of submission token *NRST*;

— delivered the message *m* with the non-repudiation token *NROT* to the data storage of entity *B*, to the intended recipient, by generating a non-repudiation of transport token *NRTT*.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13888-1:2020

 © ISO/IEC 2020 – All rights reserved