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)

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 ith 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

3.45
private key
key of an entity's asymmetric key pair which can only be used by that entity

[ISO/IEC 11770-3]

NOTE 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.

3.46
proof
corroboration that evidence is valid in accordance with the non-repudiation policy in force

NOTE Proof is evidence that serves to prove the truth or existence of something.

3.47
public key
key of an entity's asymmetric key pair which can be made public

[ISO/IEC 11770-3]

NOTE 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.

3.48
public key certificate
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[ISO/IEC 11770-3]

3.49
recipient
entity that gets (receives or fetches) a message for which non-repudiation services are to be provided

3.50
secret key
key used with symmetric cryptographic techniques and usable only by a set of specified entities

NOTE Adapted from ISO/IEC 11770-3:1999, 3.35.

3.51
security authority
entity that is responsible for the definition or enforcement of security policy

NOTE Adapted from ISO/IEC 10181-1, 3.3.17.

3.52
security certificate
set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication

NOTE Adapted from ISO/IEC 10181-1, 3.3.18.

3.53
secure envelope
SENV
set of data items which is constructed by an entity in such a way that any entity holding the secret key can verify their integrity and origin

NOTE For the purpose of generating evidence, the SENV is constructed and verified by a trusted third party (TTP) with a secret key known only to the TTP.

3.54
security policy
set of criteria for the provision of security services

[ISO 7498-2]

3.55
security token
set of security-relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority

NOTE Adapted from ISO/IEC 10181-1, 3.3.26.

3.56
signer
entity generating a digital signature

3.57
time-stamp
time variant parameter which denotes a point in time with respect to a common time reference

[ISO/IEC 18014-1]

3.58
time-stamping authority
trusted third party trusted to provide a time-stamping service

[ISO/IEC 18014-1]

3.59
trust
relationship between two elements, a set of activities and a security policy in which element *x* trusts element *y* if and only if *x* has confidence that *y* will behave in a well defined way (with respect to the activities) that does not violate the given security policy

NOTE Adapted from ISO/IEC 10181-1, 3.3.28.]

3.60
trusted third party
security authority, or its agent, trusted by other entities with respect to security-related activities

NOTE 1 Adapted from ISO/IEC 10181-1, 3.3.30.

NOTE 2 In the context of ISO/IEC 13888, a trusted third party is trusted by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as an adjudicator.

3.61
trusted time-stamp
time-stamp assured by a time-stamping authority

3.62
verification key
value required to verify a MAC

3.63
verifier
entity that verifies evidence

4 Symbols and abbreviated terms

A, B	Distinguishing identifiers for two entities.
CA	Certification authority.
$CHK_X(y)$	The cryptographic check value computed on the data y using the key of entity *X*.
DA	The distinguishing identifier of the delivery authority.
GNRT	Generic non-repudiation token.
Q	Optional data that need to be origin/ integrity protected,
Imp(*y*)	The imprint of the data string *y*, either (1) the hash-code of data string *y*, or (2) the data string *y*.
m	A message for which evidence is generated.
MAC	Message Authentication Code.
NA	Notary authority.
NRDT	Non-repudiation of delivery token.
NRI	Non-repudiation information.
NROT	Non-repudiation of origin token.
NRST	Non-repudiation of submission token.
NRTT	Non-repudiation of transport token.
NT	Notarization token.
OSI	Open Systems Interconnection.
Pol	The distinguishing identifier of the non-repudiation policy (or policies) which apply to evidence.
SENV	Secure envelope.
$SENV_X(y)$	Secure envelope computed on data *y* using the secret key of entity *X*.
SIG	Signed message.
$SIG_X(y)$	Signed message generated on data *y* by entity *X* using its private key.
$S_X(y)$	The signature computed on data *y* using a signature algorithm and the private key of entity *X*.
text	A 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.
T_i	Date and time the event or action took place.
TSA	The distinguishing identifier of the trusted time-stamping authority.
TST	Time-stamping token generated by the *TSA*.
TTP	The distinguishing identifier of the trusted third party.
$V_X(y)$	The 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*.
(*y*, *z*)	The result of the concatenation of *y* and *z* in that order.

5 Organisation of the remainder of this part of ISO/IEC 13888

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 respectively. 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, firstly, the generic non-repudiation token suitable for many non-repudiation services, secondly, the time-stamping token generated by a trusted time-stamping authority and, thirdly, 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 derivation of the cryptographic check value used for generating secure envelopes and digital signatures, 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 trusted third party (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 digital signature for evidence.

— Prior to the generation of evidence, the evidence generator has to 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.

— Keys appropriate to the mechanisms being used (i.e., private keys for asymmetric mechanisms, and secret keys for symmetric mechanisms) shall be possessed (and, where necessary, shared) by the relevant entities.

— The evidence user and the adjudicator are required to be able to verify evidence.

— 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 by the evidence generator or the evidence verifier.

7 Generic non-repudiation services

7.1 Entities involved in the provision and verification of evidence

A number of distinct entities may be 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 with 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 do it directly,

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

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

7.2 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 is stored (non-OSI environment) or communicated in a non-repudiation exchange between the parties involved. Evidence is transmitted in non-repudiation tokens as part of non-repudiation protocols.

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.

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 force. 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 on-line trusted third party to generate and verify secure envelopes (SENV). The non-repudiation policy in force may require evidence to be generated partly or totally by a trusted third party.

The non-repudiation policy in force may also require that:

— a trusted time-stamp be provided by a trusted time-stamping authority, or

— a notary be involved to verify data of one or more parties and to return data to the parties with an electronic signature, and/or

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

Trusted third parties 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 trusted third parties 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 trusted third party 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 a definition of online, inline, and offline authority see ISO/IEC TR 14516):

— directly:

  — When acting as an on-line authority actively involved in every instance of the non-repudiation service, the trusted third party generates evidence alone on behalf of the evidence subject. On-line generation of cryptographic check values and non-repudiation tokens may be required when symmetric cryptographic techniques are used for the provision of evidence, i.e., to generate secure envelopes as defined in ISO/IEC 13888-2.

  — When acting as an in-line evidence generation authority, the trusted third party generates the evidence by itself, e.g., as delivery authority.

— indirectly:

  — When acting as an off-line authority which is not involved in every instance of a non-repudiation service, the trusted third party provides off-line public key certificates related to entities generating evidence based on signatures.

  — When acting as a token generation authority, the trusted third party constructs any type of non-repudiation token composed of one or more non-repudiation tokens provided by the evidence subject or by one or more trusted authorities.

  — When acting as a digital signature generating authority, the trusted third party generates digital signatures on behalf of the evidence subject or an evidence requester.

  — When acting as a time-stamping authority (see ISO/IEC 18014), the trusted third party is trusted to provide evidence which includes the time when the time-stamping token was generated.

  — When acting as a notary authority (notary), the trusted third party is trusted to provide evidence about the properties of the entities involved and of the data stored or communicated between the entities. 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 trusted third party 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 trusted third parties or other parties.

— When acting as a delivery authority, the trusted third party will be in-line for non-repudiation of submission and non-repudiation of transport.

— When acting as an evidence record keeping authority, the trusted third party 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 trusted third party acts as an on-line authority which is trusted by the evidence user to verify each kind of non-repudiation information provided in the non-repudiation token. When evidence is generated using symmetric cryptographic techniques, it can only be verified by a trusted third party; otherwise the involvement of a trusted third party may be optional.

The means used to verify a non-repudiation token depend on the techniques used to create it:

— Secure envelopes can only be verified by a trusted third party.

— Digital signatures 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 was generated have to 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-stamping 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 produced have to be verified at the time the evidence is presented. In some cases this may be years later.

— Where the non-repudiation requires the use of a time-stamping authority to provide evidence, it shall be presented in the following way. The time value enclosed in that evidence (i.e., in the time-stamping token) has to be compared with the time value enclosed in the evidence produced by the generating entity, a trusted third party or an evidence requester. When these time values are verified to be valid according to the security policy, then the evidence their generation by the generating entity, a trusted third party or an evidence requester can be accepted.

— Additional non-repudiation tokens (e.g., notarization token) are verified according to the techniques used for generating.

9 Evidence generation and verification mechanisms

9.1 General

In these phases evidence is represented by non-repudiation tokens consisting of either secure envelopes (SENV) or digital signatures (SIG). Both are based on cryptographic check values (CHK) generated by either symmetric or asymmetric cryptographic techniques, respectively. Using certificate-based signatures, the non-repudiation token consists basically of the signed message (which consists of the message and the signature) and its public key certificate(s). If the public key certificate is not provided with the digital signature, it has to be available to the appropriate parties. Using identity-based signatures (see ISO/IEC 14888-2), the non-repudiation token 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 of the keys to the signer.

9.2 Secure envelopes

For a secure envelope (SENV) to become valid evidence, it must be generated by a trusted third party using a secret key known only to the trusted third party.

NOTE SENVs may also be used for the origin/integrity protected communication between the evidence requestor of a non-repudiation exchange and a TTP. In that case the SENV is generated and verified with a key known by both the entity concerned and the TTP.

A secure envelope is created through the use of symmetric integrity techniques on data y, using the secret key of entity X to provide a cryptographic check value $CHK_X(y)$ which is appended to the data y:

$$SENV_X(y) = (y\ ,\ CHK_X(y)).$$

The function $CHK_X(y)$ may be represented by various data integrity mechanisms, such as MACs.

NOTE A MAC can be a message authentication code as specified in ISO/IEC 9797.

Further mechanisms may be specified in the specific parts of ISO/IEC 13888.

9.3 Digital signatures

An entity *X* can sign a message *y* using a digital signature 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 digital signature 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 digital signature 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 ISO/IEC 9796.

NOTE 2 Digital signatures with appendix are specified in ISO/IEC 14888.

9.4 Evidence verification mechanism

Secure envelopes (SENV) or digital signatures (SIG) are verified by applying the verification operation $V_X(SENV)$ *or* $V_X(SIG)$ respectively using the verification key of the evidence generating entity *X*. The result of the verification is positive or negative.

Secure envelopes can only be verified by a trusted third party holding the secret key used to generate the secure envelope.

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

Digital signatures can be verified by any entity holding the public key of the signer. The provision of the public verification key to the verifier depends on the type of signature scheme applied to generate the digital signature.

— Certificate-based signatures are verified using the public key of the signer available in the public key certificate issued by the certification authority (CA).

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

When using digital signatures, a chain of public key certificates or identities may also have to be verified to obtain the necessary assurance.

10 Non-repudiation tokens

10.1 General

A non-repudiation service is mediated by non-repudiation information. Non-repudiation information is composed of one or more non-repudiation tokens. The evidence generator has to provide at least one non-repudiation token derived from the Generic Non-Repudiation Token (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 Time-Stamping Authorities). Three generic tokens are described within this part of ISO/IEC 13888, namely the Generic Non-Repudiation Token (GNRT), the Time-Stamping Token (TST), and the Notarization Token (NT). The tokens derived from the generic

non-repudiation token are generated by an evidence generator, while other tokens are generated by a trusted third party: the time-stamping token is generated by a Time-Stamping Authority (TSA); the notarization token by a Notary Authority (NA).

Non-repudiation services can only be offered for a defined period of time. It may be necessary to alter the lifetime after the token has been issued, e.g. to shorten its lifetime if an attack on a particular signature scheme is found. On the other hand, if a non-repudiation token can still be seen as (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 notarization token from a Notary Authority).

10.2 Generic non-repudiation token

The generic non-repudiation token (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 the non-repudiation policy (or policies) which apply to the evidence,

f the type of non-repudiation service being provided,

A the distinguishing identifier of the evidence subject,

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

C the 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 the distinguishing identifier of the evidence requester when different from the evidence subject,

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

T_g the date and time when the evidence was generated,

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

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

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

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

The distinguishing identifier *A* is always present. All 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 that 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 depends upon the technique being used: