INTERNATIONAL STANDARD

ISO/IEC 13888-1

First edition
1997-12-01

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 13888-1:1997(E)

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. 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.

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

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*

Annex A of this part of ISO/IEC 13888 is for information only.

Information technology — Security techniques — Non-repudiation

Part 1:
General

1 Scope

The goal of the Non-repudiation service is to generate, collect, maintain, make available and validate 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 describes a model for non-repudiation mechanisms providing evidence based on cryptographic techniques. 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.

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. There are two main types of evidence the nature of which depends on cryptographic techniques employed:

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

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, of additional data. Non-repudiation tokens may be stored as non-repudiation information that may 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, e.g.,

- 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.

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 standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 13888. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 13888 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*

ISO/IEC 9796 (all parts), *Information technology – Security techniques – Digital signature schemes giving message recovery.*

ISO/IEC 9797:1994, *Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

ISO/IEC 10118-1:1994, *Information technology – Security techniques – Hash-functions – Part 1: General.*

ISO/IEC 10181-1:1996, *Information technology – Open Sy-*

stems Interconnection – Security frameworks for open systems – Part 1: Overview.

ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 4: Non-repudiation framework.*

ISO/IEC 14888-1[1)] *Information technology – Security techniques – Digital signatures with appendix – Part 1: General.*

ISO/IEC 11770-3[1)] *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.*

3 Definitions

3.1 Definitions from ISO 7498-2

- accountability: *The property that ensures that the actions of an entity may be traced uniquely to the entity.*
- data integrity: *The property that data has not been altered or destroyed in an unauthorised manner.*
- data origin authentication: *The corroboration that the source of data received is as claimed.*
- 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.*
- security policy: *The set of criteria for the provision of security services.*

3.2 Definitions from ISO/IEC 9594-8

- certification authority: *An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys.*

3.3 Definitions from ISO/IEC 10118-1

- hash-code: *The string of bits that is the output of a hash-function.*
- hash-function: *A 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.*

3.4 Definitions from ISO/IEC 10181-1

- security certificate: *a 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.*
- security token: *a set of security relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority.*
- trust: *a 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.*
- trusted third party: *a security authority or its agent, trusted by other entities with respect to security-related activities.*

3.5 Definitions from ISO/IEC 10181-4

- evidence generator: *an entity that produces non-repudiation evidence.*
- evidence subject: *an entity whose involvement in an event or action is established by evidence.*
- evidence user: *an entity that uses non-repudiation evidence.*
- evidence verifier: *an entity that verifies non-repudiation evidence.*
- non-repudiation service requester: *an entity that requests that non-repudiation evidence be generated for a particular event or action.*

3.6 Definitions from ISO/IEC 11770-3

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

3.7 Definitions unique to this Standard on Non-repudiation

For the use of this multipart standard the following definitions apply:

3.7.1 Certificate: An entity's data rendered unforgeable with the private or secret key of a certification authority.

3.7.2 Data storage: A means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority.

3.7.3 Delivery authority: An 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.

3.7.4 Distinguishing identifier: Information which unambiguously distinguishes an entity in the non-repudiation process.

3.7.5 Evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.

NOTE – Evidence does not necessarily prove truth or existence of something (*see* proof) but contributes to establish proof.

3.7.6 Evidence requester: An entity requesting evidence to be generated either by another entity or by a trusted third party.

3.7.7 Evidence subject: the entity responsible for the action, or associated with the event, with regard to which evidence is generated.

3.7.8 Imprint: A string of bits, either the hash-code of a data string or the data string itself.

3.7.9 Message Authentication Code: A data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of a message by any entity holding the secret key.

3.7.10 Monitor (Monitoring Authority): A trusted third party monitoring the actions and events and is trusted to provide evidence about what was monitored.

3.7.11 Non-repudiation exchange: A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.

1) To be published.

3.7.12 Non-repudiation information: A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.

3.7.13 Non-repudiation of Creation: This service is 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).

3.7.14 Non-repudiation of Delivery: This service is intended to protect against a recipient's false denial of having received the message and recognised the content of a message.

3.7.15 Non-repudiation of Knowledge: This service is intended to protect against a recipient's false denial of having taken notice of the content of a received message.

3.7.16 Non-repudiation of Origin: This service is intended to protect against the originator's false denial of having created the content of a message and of having sent a message.

3.7.17 Non-repudiation of Receipt: This service is intended to protect against a recipient's false denial of having received a message.

3.7.18 Non-repudiation of Sending: This service is intended to protect against the sender's false denial of having sent a message.

3.7.19 Non-repudiation of Submission: This service is intended to provide evidence that a delivery authority has accepted the message for transmission.

3.7.20 Non-repudiation of Transport: This service is intended to provide evidence for the message originator that a delivery authority has delivered the message to the intended recipient.

3.7.21 Non-repudiation policy: A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.

3.7.22 Non-repudiation token: A special type of security token as defined in ISO/IEC 10181-1 consisting of evidence, and, optionally, of additional data.

3.7.23 Notarization: The 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.

3.7.24 Notarization token: A non-repudiation token generated by a notary.

3.7.25 Notary (notary authority): a 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.

3.7.26 NRD token: Non-repudiation of delivery token. A data item which allows the originator to establish non-repudiation of delivery for a message.

3.7.27 NRO token: Non-repudiation of origin token. A data item which allows recipients to establish non-repudiation of origin for a message.

3.7.28 NRS token: Non-repudiation of submission token. A 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.

3.7.29 NRT token: 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.

3.7.30 Originator: The entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided.

3.7.31 Private key: That key of an entity's asymmetric key pair which is usable only by that entity. In the case of an asymmetric signature system, the private key and the associated algorithms define the signature transformation.

3.7.32 Proof: The corroboration that evidence is valid in accordance with the non-repudiation policy in force.

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

3.7.33 Public key: That key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system, the public key and the associated algorithms define the verification transformation.

3.7.34 Public key certificate: A security certificate which binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates the validity of the corresponding private key.

3.7.35 Recipient: The entity that gets (receives or fetches) a message for which non-repudiation services are to be provided.

3.7.36 Redundancy: Any information that is known and can be checked.

3.7.37 Secret key: A key usable with symmetric cryptographic techniques and usable only by a set of specified entities.

3.7.38 Secure Envelope (SENV): A 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. For the purpose of generating evidence, the SENV is constructed and verified by a TTP with a secret key known only to the TTP.

3.7.39 Signer: The entity generating a digital signature.

3.7.40 Trusted third party: A security authority, or its agent, trusted by other entities with respect to security related activities. In the context of this multipart standard, 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.

3.7.41 Trusted time stamp: A data item with time and date information assured by a trusted time stamping authority.

3.7.42 Trusted time stamping authority: A trusted third party trusted to provide evidence which includes the time when the trusted time stamp is generated.

3.7.43 Verification key: A value required to verify a cryptographic check value.

3.7.44 Verifier: An entity that verifies an evidence.

4 Notation and Abbreviations

A	the distinguishing identifier of entity A.
B	the distinguishing identifier of entity *B*.
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.
f_i	a data item (flag) indicating the kind of non-repudiation service in effect.
GNRT	Generic Non-repudiation Token.
H(y)	the hash-code of data string *y*.
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
PoI	the distinguishing identifier of the non-repudiation policy (or policies) which apply to evidence.
SENV	Secure Envelope.
SIG	the digital signature obtained by applying a digital signature operation to a message.
S_X	the signature operation 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., key identifier and/or the 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	Verification operation applied to a Secure Envelope or a digital signature by applying a verification algorithm using the verification key of entity *X*.
y||z	denotes the result of the concatenation of *y* and *z* in that order.

5 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:

5.1 The entities of a non-repudiation exchange shall trust a trusted third party *(TTP)*.

NOTE – When using symmetric cryptographic algorithms a TTP is always required. When using asymmetric cryptographic algorithms a public key certificate has to be generated by an off-line TTP. A public key certificate is not necessarily required if the digital signature is generated by a TTP

5.2 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).

5.3 The mechanisms for generating or verifying evidence have to be either available to the entities of the particular non-repudiation exchange, or a trusted authority has to be available to provide the mechanisms and perform the necessary functions on behalf of the evidence requester.

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

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

5.6 The time information required in an evidence consists of both the time the event took place and of the time the evidence was generated.

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

6 Organisation of the Standard

Non-repudiation services are modelled by first 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 using specific non-repudiation tokens in a messaging environment is given in clause 12.

7 Generic Non-repudiation Service

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 wants to verify evidence but cannot 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.

If neither the evidence subject nor the evidence requester is able to provide evidence directly, evidence is produced by an evidence generator. 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

This general model applies to the following six fundamental non-repudiation services: non-repudiation of creation, non-repudiation of sending, non-repudiation of receipt, and non-repudiation of knowledge, non-repudiation of submission, and non-repudiation of transport. Other non-repudiation services may be provided by grouping some of these fundamental services. Non-repudiation of origin can be provided by combining non-repudiation of creation and non-repudiation of sending, non-repudiation of delivery can be provided by combining non-repudiation of receipt and non-repudiation of knowledge.

8 Trusted Third Party Involvement

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 the involvement of an off-line trusted third party to guarantee the genuineness of the keys. The trusted third party may be part of a chain of TTPs provided that they are bound by agreements on non-repudiation services. The use of symmetric cryptographic techniques requires the involvement of an on-line trusted third party to generate and validate 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 certify the properties of the entities involved and of data stored or communicated, or to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation, 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.

8.1 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.

– 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 part 2 of ISO/IEC 13888.
– As an in-line evidence generation authority, the trusted third party generates the evidence by itself, e.g., as delivery authority.
– 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.
– 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.
– As a digital signature generating authority, the trusted third party generates digital signatures on behalf of the evidence subject or an evidence requester.
– As a time stamping authority, the trusted third party is trusted to provide evidence which includes the time when the time stamping token was generated.
– 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.
– As a monitoring authority, the trusted third party monitors the actions and events and is trusted to provide evidence about what was monitored.

8.2 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.

– 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.

8.3 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 tech-

niques, it can only be verified by a trusted third party, otherwise the involvement of a trusted third party may be optional.

The non-repudiation token is verified according to the techniques used:

- Secure Envelopes can only be verified by a trusted third party.
- Digital signatures may be verified by 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 at the time the evidence is presented. In some cases this may be years later.
- (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.
- If evidence generated by Time Stamping Authorities is required by the non-repudiation policy, it shall be used in the following way. The time enclosed in that evidence (i.e., in the time stamping token) has to be compared with the time enclosed in the evidence produced by the generating entity, a trusted third party or an evidence requester. When these times are verified to be sufficiently close according to the security policy, then the evidence generated 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

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, 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.

9.1 Secure Envelopes

For a Secure Envelope *(SENV)* to become a part of evidence it has to 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 entities 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.

The method of creating a secure envelope is through the use of symmetric integrity techniques on data y using a secret key x of entity X providing a cryptographic check value $CHK_X(y)$ which is appended to the data y:

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

The function *CHK* may be represented by different data integrity mechanisms, such as:

$$CHK_X(y) = MAC.$$

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

NOTE – *MAC* can be the message authentication code as specified in ISO/IEC 9797.

9.2 Digital Signatures

An entity X can sign a message y by transforming it using a digital signature operation using its private key. The result 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. If the digital signature operation allows message recovery, part 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 $S_X(y)$.

NOTES

1 Digital signatures giving message recovery are specified in the multipart standard ISO/IEC 9796.

2 Digital signatures with appendix are specified in the multipart standard ISO/IEC 14888.

9.3 Evidence Verification Mechanism

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

Secure Envelopes are verified only 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 authority providing the identity-based keys to the signer.

With digital signatures a chain of public key certificates or identities may have to be verified subsequently to obtain the necessary assurance.

10 Non-repudiation Tokens

A non-repudiation service is mediated by non-repudiation information. A 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 validate 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 standard. 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)*.

10.1 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, or 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 to 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:

- 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 of the keys to the signer.

10.2 Time Stamping Token

If a trusted time is required or the clock provided by the non-repudiation token generating party cannot be trusted, it is necessary to rely on a trusted third party, a Time Stamping Authority *(TSA)*. Its role is to establish further evidence indicating the time the token was generated.

Data y is provided by the entity requesting the time stamping service .

The time stamping token *(TST)* is defined as follows:

$TST = text \| w \| CHK_{TSA}(w),$ with

$w = Pol \| f \| TSA \| T_g \| Q \| Imp(y)$

The data element w 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,
- *TSA* the distinguishing identifier of the Time Stamping Authority,
- T_g the date and time when the time stamping operation was performed,
- Q optional data that need to be origin/ integrity protected,
- *Imp(y)* the imprint of the data y for which a trusted time stamp is to be provided.

10.3 Notarization Token

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

The data y is provided by the service requesting entity.

NOTE – 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 be certified by the notary.

The Notarization Token *(NT)* is defined as follows:

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

$w = Pol \| f \| X \| NA \| T_g \| Q \| Imp(y)$

The data element w consists of the following data items:

- *Pol* the policy (or policies) which apply to the evidence,
- f a flag indicating the notary service,
- X the distinguishing identifier of entity X requesting the notary service,
- *NA* the distinguishing identifier of the Notary Authority,
- T_g the date and time when the notarization was performed,
- Q optional data that need to be origin/ integrity protected,
- *Imp(y)* the imprint of the data y for which a notary service is to be provided.

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

Non-repudiation involves the generation of evidence that can be used to prove that some kind of event or action has taken place. Evidence is generated on the data describing the facts 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.

The following considers 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 considered.

Entity *A* creates a message *m* and establishes non-repudiation of origin stimulated by his own interest or 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 that may be the originator itself or a trusted third party.

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

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* – and, if present – together 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* – and, if present – together with the non-repudiation token *NROT* to the data storage of entity *B*, the intended recipient, by generating a non-repudiation of transport token *NRTT*.

Depending on the non-repudiation policy in effect it may be required to have a time stamp token *(TST)* or a notarization token *(NT)* provided as (additional) evidence to the existing non-repudiation token.

NOTE – Denial of sending or receiving a message includes the possibility that a sender (or receiver), while not denying that a message was sent (or received), may dispute the time at which this message was sent (or received).

11.1 Non-repudiation of Origin

The non-repudiation of origin service covers the case where the sender of a message both created and sent that message.

This service is intended to protect against a sender's false denial of being both the creator (the author of the content) of a message and the sender of that message.

The service may be provided by the sender itself or an authority acting on behalf of the sender.

11.2 Non-repudiation of Delivery

The non-repudiation of delivery service covers the case where the recipient acknowledges the fact that it has both received a message and taken notice of the content of the message.

11.3 Non-repudiation of Submission

This service requires the existence of a delivery authority involved in the transfer of a message between a sender and one or more recipients. The delivery authority is trusted by the sender to accept a message from it and then to make its best effort to deliver that message. By accepting the message the delivery authority provides evidence about the submission of the message by the sender. The delivery authority acknowledges the fact that a message has been sub-

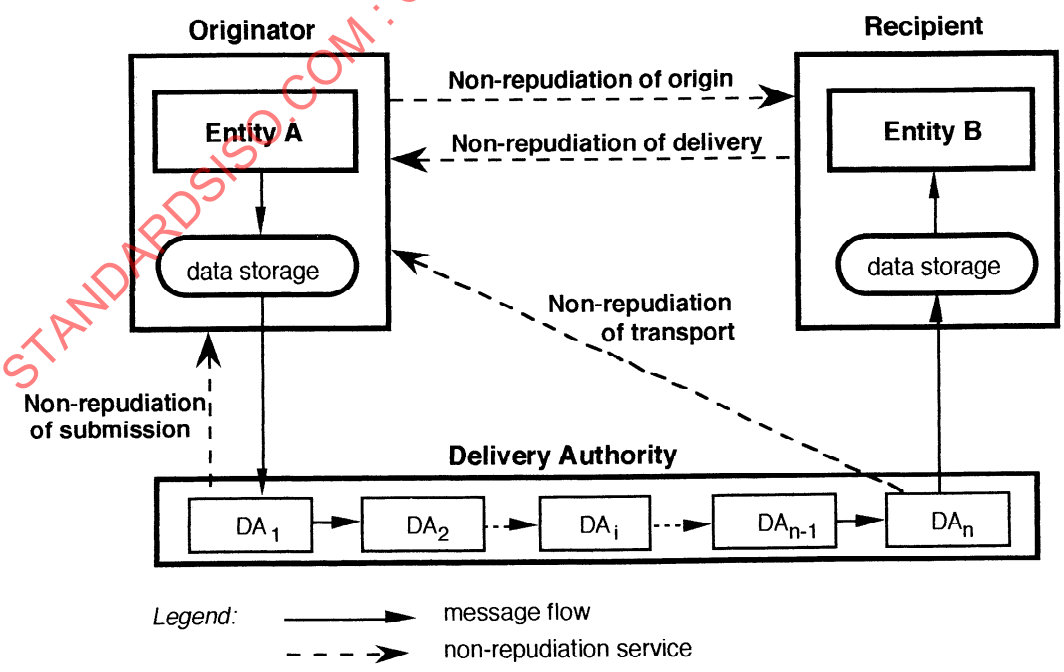

Figure 1 – Specific non-repudiation services

mitted but does not care what the content of the message is.

11.4 Non-repudiation of Transport

This service requires the existence of a delivery authority involved in the transfer of a message between a sender and a receiver. The delivery authority is trusted by the sender to deliver a message in a place where it is made available to the receiver. While delivering the message the delivery authority provides evidence about the deposit of the message in the data storage of the recipient. The delivery authority acknowledges the fact that a message has been deposited but does not care what the content of the message is. The delivery authority cannot guarantee that the message is duly received by the recipient.

12 Use of specific Non-repudiation Tokens in a Messaging Environment

The non-repudiation tokens *(NROT, NRST, NRTT, NRDT)* for the specific non-repudiation services discussed in the previous clause are defined in the subsequent parts of 13888 using the generic non-repudiation token *GNRT* as given in clause 10.1. These four tokens can be used in the following way, in particular if the delivery authority system consists of a chain of *n* sub-delivery authorities DA_i, $i=1 \ldots n$.

In that case each sub-delivery authority generates a non-repudiation of submission token $NRST_i$ at the time of receiving the message from the submitting entity or the preceding delivery authority. This establishes a chain of intermediate $NRST_i$ tokens to be stored as evidence by the respective receiver. The first NRS token $NRST_1$ is sent to the sender (originator) for storing it as the non-repudiation of submission token *NRST*. A non-repudiation of transport token *NRTT* is generated only by the last sub-delivery authority DA_n at the time of providing the message to the data storage of the intended recipient (see Figure 2).

Requested either by the non-repudiation policy in effect or by the originator, entity *B* establishes non-repudiation of delivery by generating evidence on receipt of the message *m* and sending a non-repudiation of delivery token *NRDT* back to the originator *A* for storing it as evidence in the case of disputes.

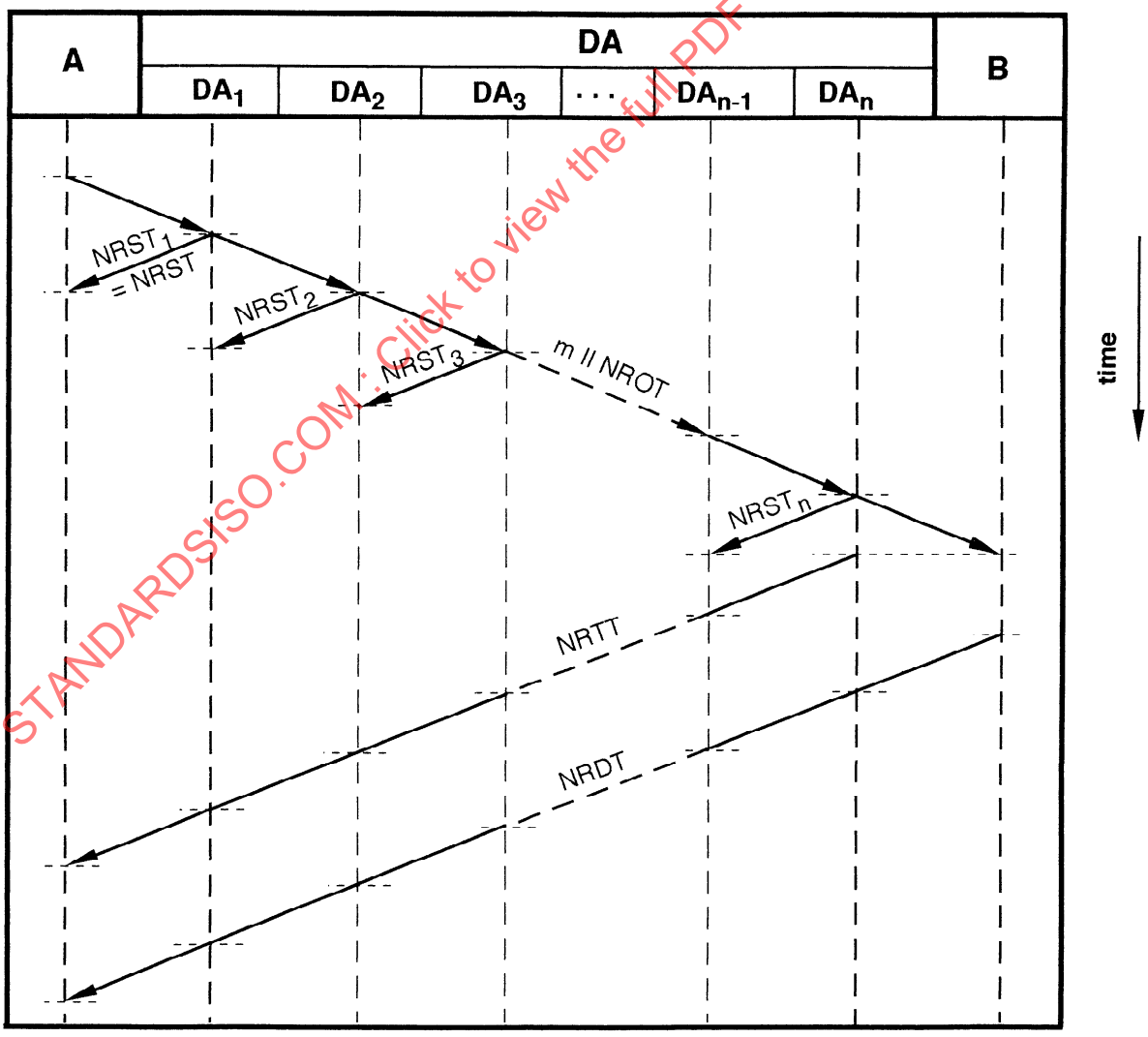

Figure 2 – Non-repudiation service protocols (example)

Annex A

(informative)

Bibliography

ISO/IEC 9796:1991	*Information technology – Security techniques – Digital signature scheme giving message recovery.*
ISO/IEC 9796-2:1997	*Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function.*
ISO/IEC 9798-1:1997	*Information technology – Security techniques – Entity authentication – Part 1: General.*
ISO/IEC 10118-1:1994	*Information technology – Security techniques – Hash-functions – Part 1: General.*
ISO/IEC 10118-2:1994	*Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm.*
ISO/IEC 10118-3:[1)]	*Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*
ISO/IEC 10118-4:[1)]	*Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic.*
ISO/IEC 13888-2:[1)]	*Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques.*
ISO/IEC 13888-3: 1997	*Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.*
ISO/IEC 14888-1:[1)]	*Information technology – Security techniques – Digital signatures with appendix – Part 1: General.*
ISO/IEC 14888-2:[1)]	*Information technology – Security techniques – Digital signatures with appendix – Part 2: Identity-based mechanisms.*
ISO/IEC 14888-3:[1)]	*Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms.*

[1)] To be published.