INTERNATIONAL STANDARD

ISO/IEC 13888-3

Second edition
2009-12-15

Information technology — Security techniques — Non-repudiation —

Part 3: Mechanisms using asymmetric techniques

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

Partie 3: Mécanismes utilisant des techniques asymétriques

Reference number
ISO/IEC 13888-3:2009(E)

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

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

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 13888-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 13888-3:1997), which has been technically revised to remove ambiguity in the definitions of mechanisms.

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 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 only addresses the following non-repudiation services:

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

Such evidence may be produced either directly by an end entity or by a trusted third party.

Non-repudiation mechanisms involve the exchange of non-repudiation tokens specific for each non-repudiation service. The non-repudiation mechanisms defined in this part of ISO/IEC 13888 consist of digital signatures and additional data. Non-repudiation tokens are stored as non-repudiation information and are used subsequently in the event of disputes.

Additional information is required to complete the non-repudiation token. Depending on the non-repudiation policy in effect for a specific application and the legal environment within which the application operates, that additional information should take one of the following two forms:

- information provided by a time-stamping authority which provides assurance that the signature of the non-repudiation token was created before a given time.
- information provided by a time-marking service which provides assurance that the signature of the non-repudiation token was recorded before a given time.

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.

Information technology — Security techniques — Non-repudiation —

Part 3: Mechanisms using asymmetric techniques

1 Scope

This part of ISO/IEC 13888 specifies mechanisms for the provision of specific, communication related, non-repudiation services using asymmetric cryptographic techniques.

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 13888-1:2004, *Information technology — Security techniques — Non-repudiation — Part 1: General*

ISO/IEC 18014-1:2008, *Information technology — Security techniques — Time-stamping services — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 13888-1 apply.

4 Symbols and abbreviated terms

A	the claimed message originator
B	the message recipient or the intended message recipient
C	the distinguishing identifier of the trusted third party
CA	certification authority
D_i	distinguishing identifier of the i th delivery authority, a trusted third party ($i \in \{1, 2, ..., n\}$, where n is the number of delivery authorities in the system)
f_i	data term (flag) indicating the type of non-repudiation service in effect ($i \in$ {origin, delivery, submission, transport})
$Imp(y)$	imprint of data y, consisting of either y or the hash code of y together with an identifier of the hash-function being used

M	message which is sent from entity A to entity B in respect of which non-repudiation services are provided
NR	non-repudiation
NRD	non-repudiation of delivery
$NRDT$	non-repudiation of delivery token
NRO	non-repudiation of origin
$NROT$	non-repudiation of origin token
NRS	non-repudiation of submission
$NRST$	non-repudiation of submission token
NRT	non-repudiation of transport
$NRTT$	non-repudiation of transport token
Pol	distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence
Q	optional data item that may contain additional information, e.g., the distinguishing identifiers of the message m, signature mechanism, or hash-function
S	signature operation performed using a signature algorithm. The signature of a message m computed using the private key of entity X is denoted by $S(X, m)$
T_i	date and time the i th type of event or action took place (i is the index of events or actions, $i \in \{1, 2, 3, 4\}$)
T_g	date and time that the evidence was generated
$text_i$	optional data item that may contain additional information, e.g., a key identifier and/or the message identifier ($i \in \{1, 2, 3, 4, 5, 6\}$)
TSA	time-stamping authority
TST	time-stamp token
TTP	trusted third party
X, Y	variables used to indicate entity names
$y \| z$	result of the concatenation of y and z in that order. When concatenating data items, an appropriate encoding must be used so that the individual data items can be recovered from the concatenated string

5 Requirements

Depending on the basic mechanism used for generating non-repudiation tokens, 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 in this part of ISO/IEC 13888:

- The entities performing a non-repudiation exchange shall trust the same Trusted Third Parties (TTPs).
- The signature key belonging to an entity must be kept secret by that entity.
- A common function *Imp* shall be supported by all entities in the non-repudiation service. The function *Imp* shall be either the identity function or a collision-resistant hash-function as defined in ISO/IEC 10118.

- The digital signature mechanism used shall satisfy the security requirements specified by the non-repudiation policy.
- Prior to the generation of evidence, the evidence generator must know which non-repudiation policies the evidence shall be generated in accordance with, the type of evidence to be generated, and the mechanisms to be used to verify the evidence.
- The mechanisms for generating or verifying evidence must be available to the entities performing the particular non-repudiation exchange, or a trusted authority must be available to provide the mechanisms.
- Either the evidence generator or the evidence verifier needs to use a Time-stamping service or a Time-marking service.

6 Trusted Third Party involvement

Trusted Third Parties are involved in the provision of non-repudiation services, their precise role depending on the mechanisms used and the non-repudiation policy in force. A Trusted Third Party may act in one or more of the following roles:

- A Delivery Authority (DA) is trusted to deliver the message to the intended recipient and to provide the non-repudiation of submission or non-repudiation of transport token.
- The use of asymmetric cryptographic techniques may require the involvement of a Trusted Third Party to guarantee the authenticity of the public verification keys, as described in, e.g., ISO/IEC 9594-8.
- The non-repudiation policy in force may require that the evidence is generated partly or totally by a Trusted Third Party.
- A Time-stamping token issued by a Time-stamping Authority (TSA) may also be used to ensure that a non-repudiation token remains valid.
- A Time-marking Authority may be involved to provide assurance that the signature of a given non-repudiation token was recorded before a given time.
- An Evidence Recording Authority may be involved to record evidence that can later be retrieved if there is a dispute.

Trusted Third Parties may be involved to differing degrees in the various phases of the provision of a non-repudiation service. When exchanging evidence, the parties must know, or agree, which non-repudiation policy is to be applicable to the evidence.

7 Digital signatures

For the mechanisms specified in this part of ISO/IEC 13888, non-repudiation tokens are created using digital signatures. The digital signature technique used to generate these digital signatures shall conform to ISO/IEC 9796 or ISO/IEC 14888.

The public key to be used to verify a signature shall be included in a public key certificate. This certificate shall include a time period indicating the period during which the CA handles the revocation status of the certificate.

A signature from an NR Token shall be verifiable at least during the validity period of the certificates to be used to validate public verification key used to verify the signature, and also once the validity period of these certificates has expired. In order to achieve this goal the use of either a Time-stamping service or a Time-marking service is necessary (See Clause 11). The mechanisms described in Clause 11 must be used to guarantee that the non-repudiation token will remain valid once the certificate to be used to verify the signature of the NR token has expired, or if that certificate is revoked.

8 Use of non-repudiation tokens with and without delivery authorities

The use of non-repudiation tokens in the case where Delivery Authorities are not used is shown in Figure 1. Mechanisms adhering to this model are specified in Clause 9. Trusted Third Party *C* as NRO and NRD tokens generator is optional in this particular instance of the non-repudiation services.

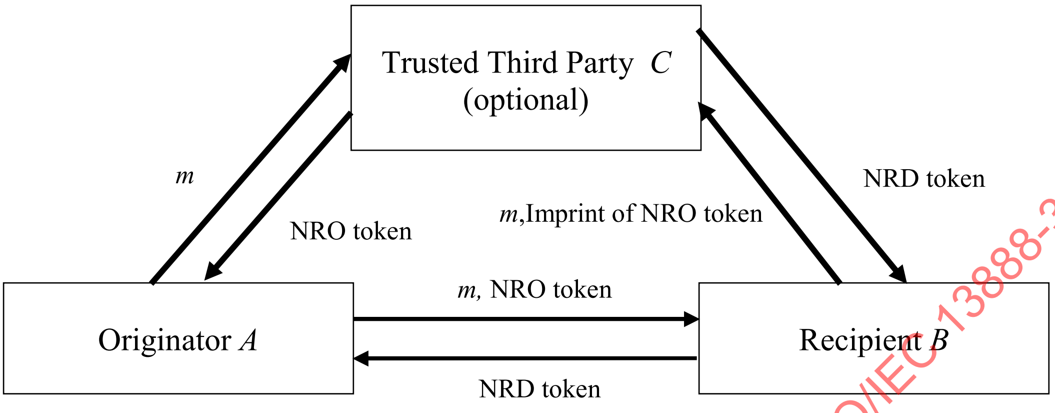

Figure 1 – Use of non-repudiation tokens without a Delivery Authority

Figure 2 shows the use of the four types of non-repudiation tokens in the case where third party Delivery Authorities are used. Mechanisms adhering to this model are specified in Clause 10.

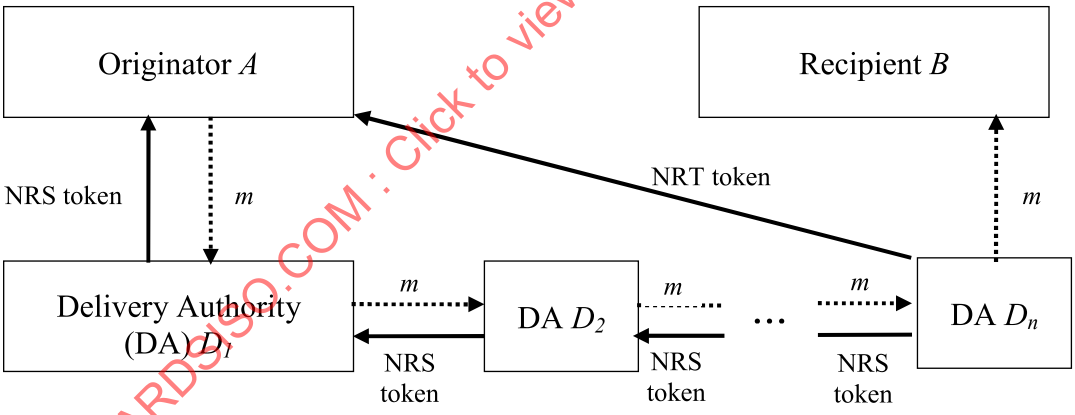

Figure 2 – Use of non-repudiation tokens with Delivery Authorities

9 Evidence produced by the end entities

9.1 General

The non-repudiation mechanisms specified in this clause allow for generation of evidence for non-repudiation of origin (NRO) and delivery (NRD) without the participation of a third party Delivery Authority. It is assumed that entity *A* wishes to send a message *m* to entity *B*, and thus will be the originator of the non-repudiation transfer. Entity *B* will be the recipient.

It is assumed that entity *A* knows its own public key certificate and associated private key, entity B knows its own public key certificate and associated private key, and that the corresponding public key certificates are available to all the entities concerned.

If Trusted Third Party *C* is involved (optional), *C* must keep all NRO tokens generated and record whether or not each of NRO token is used to generate a NRD token.

Two different mechanisms for non-repudiation are described.

9.2 Non-repudiation of origin

9.2.1 Non-repudiation of origin (NRO) token

An NRO token is used to provide protection against the originator's false denial of having originated the message.

The NRO token is

- generated by the originator *A* of the message *m* (or by authority *C*),
- sent by *A* to the recipient *B*,
- stored by the recipient *B* after *B* has verified the NRO token using *A*'s public key certificate.

The structure of the NRO token (*NROT*) is:

$$NROT = text_1 \,||\, z_1 \,||\, S(A, z_1),$$

where

$$z_1 = Pol \,||\, f_{origin} \,||\, A \,[||\, B] \,||\, C \,||\, T_g \;[||\, T_1] \,||\, Q \,||\, Imp\,(m).$$

The data string z_1 within an NRO token consists of the following data items:

Pol — the distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence,

f_{origin} — a flag indicating non-repudiation of origin,

A — the distinguishing identifier of the originator of the message *m*, e.g. an e-mail address,

B — the distinguishing identifier(s) of the intended recipient(s) of the message *m* (optional), e.g. an e-mail address,

C the distinguishing identifier of the authority involved (optional): if the token is generated by authority C then this data item is mandatory and the signature $S(A, z_1)$ in the NRO token, *NROT*, should be replaced by $S(C, z_1)$,

T_g the date and time, according to the token generator, at which the token was generated,

T_1 the date and time, according to the originator, at which the message *m* was sent (optional),

Q an optional data item that may contain additional information, e.g., the distinguishing identifiers of the message *m*, signature mechanism and/or hash-function, and information regarding certificates and validity of public keys,

$Imp(m)$ the imprint of data *m*, consisting of either *m* or the hash code of *m* together with an identifier of the hash-function being used.

9.2.2 Mechanism for non-repudiation of origin

The non-repudiation of origin (NRO) token is generated by the message originator *A* and sent to the message recipient *B*.

Transaction - From entity *A* to entity *B*

a) If Trusted Third Party *C* is involved (optional),

1) *A* asks *C* to generate an NRO token for message *m*.

2) *C* receives the message *m* and checks the validity of the request for an NRO token.

3) *C* forms an NRO token as specified in clause 9.2.1.

4) *C* sends the NRO token to *A* and keeps it.

5) *A* receives the NRO token from *C*

Otherwise, *A* forms an NRO token as specified in clause 9.2.1.

b) *A* sends the NRO token (together with message *m*) to *B*.

B checks the validity of the NRO token and its contents by checking the

— types and values of data items in *NROT*, and

— validity of the signature in *NROT.*

If it is valid, the NRO token is saved as evidence for non-repudiation of origin.

9.3 Non-repudiation of delivery

9.3.1 Non-repudiation of delivery (NRD) token

An NRD token is used to provide protection against the recipient's false denial of having received and recognized the content of the message *m*.

The NRD token is:

- generated by the recipient *B* (or authority *C*),
- sent by *B* to one or more entities including the message originator *A*, if known,
- stored by these entities after *A* has verified the NRD token by using *B*’s (or by authority C’s) public key certificate.

The structure of an NRD token (*NRDT*) is:

$$NRDT = text_2 \,||\, z_2 \,||\, S(B, z_2),$$

where

$$z_2 = Pol \,||\, f_{delivery} \,[||\, A] \,||\, B \,[||\, C] \,||\, T_g \,[||\, T_2] \,||\, Q \,||\, Imp\,(m).$$

The data string z_2 within an NRD token consists of the following data items:

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

$f_{delivery}$ a flag indicating non-repudiation of delivery,

A the distinguishing identifier of the entity that is claimed by *B* to be the originator of the message *m* (optional), e.g. an e-mail address,

B the distinguishing identifier of the recipient of the message *m*, e.g. an e-mail address,

C the distinguishing identifier of the authority involved (optional): if the token is generated by authority *C* then this data item is mandatory and the signature $S(B, z_2)$ in the NRD token, *NRDT*, should be replaced by $S(C, z_2)$,

T_g the date and time, according to the token generator, at which the token was generated,

T_2 the date and time, according to the recipient, at which the message *m* was received (optional),

Q an optional data item that may contain additional information, e.g., the distinguishing identifiers of the message *m*, signature mechanism and/or hash-function, and information regarding certificates and validity of public keys,

$Imp\,(m)$ the imprint of data *m*, consisting of either *m* or the hash code of *m* together with an identifier of the hash-function being used.

9.3.2 Mechanism for non-repudiation for delivery

The non-repudiation of delivery (NRD) token is generated by the message recipient *B* and sent to the message originator *A* after *B* has received the message *m*.

Transaction 1 - From message originator *A* to message recipient *B*

A sends the message *m* and a request for an NRD token to *B*.

Transaction 2 - From entity *B* to entity *A*

a) *B* receives the message *m* and checks the validity of the request for NRD token.

b) If Trusted Third Party *C* is involved (optional),

1) *B* sends either *m* or *m*||*Imp*(*NROT*) (if *A* sent *NROT* with *m* and if *NROT* was generated by *C*) to *C* and asks it to generate an NRD token for message *m*.

2) *C* receives *m* (and, optionally, *Imp*(*NROT*)) and, if present, checks that the NRO token was generated by *C* and the NRD token corresponds to the imprint of the NRO token has not been generated. If this check fails, *C* rejects the request of NRD token.

3) *C* forms an NRD token as specified in clause 9.3.1 and records that this *NROT* was used to generate the NRD token.

4) *C* sends the NRD token to *B*.

5) *B* receives the NRD token from *C*

Otherwise, *B* forms an NRD token as specified in clause 9.3.1.

c) *B* sends the NRD token to *A*.

A checks the NRD token and its contents by checking the

- types and values of data items in *NRDT*, and
- validity of the signature in *NRDT.*

If it is valid, the NRD token is saved by *A* as evidence that *B* has received the message *m*.

10 Evidence produced by a Delivery Authority

10.1 General

The clause specifies a number of additional mechanisms in which evidence is produced by trusted Delivery Authorities as part of a non-repudiation process. Such mechanisms may be incorporated into the basic mechanisms specified in clause 9 in order to meet the requirements defined by the security policy.

The terms submission/transport are used where a Delivery Authority issues non-repudiation (NRS/NRT) tokens:

- An NRS token allows the originator or the preceding Delivery Authority to obtain evidence that a message has been submitted for transportation in a store and forward system.
- An NRT token allows the originator to obtain evidence that a message has been delivered by a Delivery Authority to the intended recipient.

10.2 Non-repudiation of submission

10.2.1 Non-repudiation of submission (NRS) token

In this mechanism, an NRS token is created by a Delivery Authority. The evidence generator in this case is the Delivery Authority. When the originator or a preceding Delivery Authority X (A or D_i, $i \in \{1, 2, \ldots, n-1\}$) has sent a message m to the Delivery Authority Y (D_1 or D_{i+1}, respectively) and after the Delivery Authority Y has received the message m, Y sends the NRS token to X. This provides evidence that the message has been submitted for onward delivery.

The NRS token is

- generated by the Delivery Authority Y,
- sent by Y to X (the message originator A or a preceding Delivery Authority D_i),
- stored by X after X has verified the NRS token using Y's public key certificate.

The structure of an NRS token ($NRST$) sent from D_{i+1} to D_i is:

$$NRST = text_3 \parallel z_3 \parallel S(D_{i+1}, z_3),$$

where

$$z_3 = Pol \parallel f_{submission} [\parallel A] \parallel B \parallel D_1 \parallel D_2 \parallel \ldots \parallel D_i \parallel D_{i+1} \parallel T_g \parallel T_3 [\parallel Q] \parallel Imp(m).$$

Following the name of the recipient, the names of the involved Delivery Authorities are listed in the order in which message m is delivered. The data string z_3 within an NRS token consists of the following data items:

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

$f_{submission}$ a flag indicating non-repudiation of submission,

A the distinguishing identifier of the originator of the message m (optional), where the validity of the identifier A, e.g. an e-mail address, may or may not have been verified by C,

B the distinguishing identifier of the intended recipient of the message m, e.g. an e-mail address,

D_i Delivery Authority, a Trusted Third Party ($i \in \{1, 2, \ldots, n\}$, where n is the number of Delivery Authorities in the system),

T_g the date and time, according to the token generator, at which the token was generated,

T_3 the date and time, according to the token generator, at which the message m was submitted,

Q an optional data item that may contain additional information, e.g., the distinguishing identifiers of the message m, signature mechanism and/or hash-function, and information regarding certificates and validity of public keys,

$Imp(m)$ the imprint of data m, consisting of either m or the hash code of m together with an identifier of the hash-function being used.

10.2.2 Mechanism for non-repudiation of submission

In the first transaction of this mechanism, a sending entity X (A or D_i, $i \in \{1, 2, ... , n -1\}$) sends a message to a Delivery Authority Y (D_1 or D_{i+1}, respectively) for onward delivery. In the second transaction, the NRS token is sent from the Delivery Authority Y to the entity X. Non-repudiation of submission is established in the second transaction.

Transaction 1 - From entity X to Delivery Authority Y

X sends the message m and a request for an NRS token to Y.

Transaction 2 - From Delivery Authority Y to entity X

a) Y forms the NRS token as specified in clause 10.2.1.

b) Y sends the NRS token to X.

Entity X checks the NRS token and its content by checking the

- types and values of data items in *NRST*, and
- validity of the signature in *NRST.*

If it is valid, the NRS token is saved by X as evidence for non-repudiation of submission (i.e., the message that was submitted).

10.3 Non-repudiation of transport

10.3.1 Non-repudiation of transport (NRT) token

An NRT token is used by the message originator as evidence that the message m has been sent to B by the final Delivery Authority in the Delivery Authority chain. The evidence generator in this case is Delivery Authority D_n (see Figure 2). When the originator or one of the preceding Delivery Authorities X (A or D_i, $i \in \{1, 2, ... , n - 1\}$) has sent a message m to the Delivery Authority Y (D_1 or D_{i+1}, respectively) and after the last Delivery Authority D_n has received the message m, D_n transfers the message m to the recipient B and also sends the NRT token to the originator A of the message m. This provides evidence that the message m has been transferred to B.

The NRT token is

- created by the Delivery Authority D_n,
- sent by D_n to the message originator A,
- stored by A after A has verified the NRT token using D_n's public key certificate.

The structure of an NRT token (*NRTT*) sent from D_n to A is:

$$NRTT = text_4 \mid\mid z_4 \mid\mid S(D_n, z_4),$$

where

$$z_4 = Pol \mid\mid f_{transport} \, [\mid\mid A] \mid\mid B \mid\mid D_1 \mid\mid D_2 \mid\mid ... \mid\mid D_n \mid\mid T_g \mid\mid T_4 \, [\mid\mid Q] \mid\mid Imp\,(m).$$

Following the name of the recipient, the names of involved delivery authorities are listed in the order in which message m is delivered. The data string z_4 within an NRT token consists of the following data items:

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

$f_{transport}$ a flag indicating non-repudiation of transport,

A the distinguishing identifier of the originator of the message *m* (optional), where the validity of the identifier *A*, e.g. an e-mail address, may or may not have been verified by *C*,

B the distinguishing identifier of the intended recipient of the message *m*, e.g. an e-mail address,

D_i Delivery Authority, a Trusted Third Party ($i \in \{1, 2, ..., n\}$, where *n* is the number of Delivery Authorities in the system),

T_g the date and time, according to the token generator, at which the token was generated,

T_4 the date and time, according to the token generator, at which the message *m* was delivered,

Q an optional data item that may contain additional information, e.g., the distinguishing identifiers of the message *m*, signature mechanism and/or hash-function, and information regarding certificates and validity of public keys,

Imp (*m*) the imprint of data *m*, consisting of either *m* or the hash code of *m* together with an identifier of the hash-function being used.

10.3.2 Mechanism for non-repudiation of transport

In the first transaction of this mechanism, a sending entity *X* (*A* or D_i, $i \in \{1, 2, ... , n - 1\}$) sends message *m* to a Delivery Authority *Y* (D_1 or D_{i+1}, respectively) for onward delivery. In the second transaction, the message *m* is sent from D_n to the recipient *B*. In the third transaction, the NRT token is generated by D_n and sent to entity *A*, the originator of the message *m*. Non-repudiation of transport is established in the third transaction.

Transaction 1 - From entity *X* to Delivery Authority *Y*

X sends the message *m* to *Y*.

Transaction 2 - From Delivery Authority D_n to entity *B*

D_n sends the message *m* to *B*.

Transaction 3 - From Delivery Authority D_n to entity *A*

a) D_n forms the NRT token as specified in clause 10.3.1.

b) D_n sends the NRT token to *A*.

A checks the NRT token and its content by checking the

— types and values of the data items in *NRTT*, and

— validity of the signature in *NRTT.*

If it is valid, the NRT token is saved by *A* as evidence for non-repudiation of transport (i.e., the message was delivered to the intended recipient *B*).