INTERNATIONAL STANDARD

ISO/IEC 13888-3

Third edition
2020-09

Information security — Non-repudiation —

Part 3: Mechanisms using asymmetric techniques

Sécurité de l'information — Non-répudiation —

Partie 3: Mécanismes utilisant des techniques asymétriques

Reference number
ISO/IEC 13888-3:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

This third edition cancels and replaces the second edition (ISO/IEC 13888-3:2009), which has been technically revised.

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

— Clause 3 has been clarified;

— the terminology and notation issues have been fixed;

— a requirement has been changed into a recommendation in Clause 7; and

— a new requirement has been introduced in Clause 5.

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

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

Introduction

The goal of 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.

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

This document only addresses the following non-repudiation services:

— non-repudiation of origin;

— non-repudiation of delivery;

— non-repudiation of submission;

— non-repudiation of transport.

Non-repudiation mechanisms involve the exchange of non-repudiation tokens specific for each non-repudiation service. The non-repudiation mechanisms defined in this document 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 takes 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 security — Non-repudiation —

Part 3: Mechanisms using asymmetric techniques

1 Scope

This document specifies mechanisms for the provision of specific, communication-related, non-repudiation services using asymmetric cryptographic techniques.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 13888-1, *Information technology — Security techniques — Non-repudiation — Part 1: General*

ISO/IEC 14888 (all parts), *IT Security techniques — Digital signatures with appendix*

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

ISO/IEC 29192-4, *Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques*

3 Terms and definitions

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

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

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

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

3.1
time-marking service
service providing evidence that a hash code together with an identifier of a hash-function have been recorded before a certain point in time

3.2
time-stamping service
service providing evidence that a data item existed before a certain point in time

4 Symbols

A	claimed message originator
B	message recipient or the intended message recipient
C	Trusted third party
D_i	ith delivery authority, a trusted third party ($1 \leq i \leq n$, 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})
ID_A, ID_B, ID_C, ID_{D_i}	distinguishing identifiers of the entities A, B, C and D_i
$Imp(y)$	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
$NRDT$	non-repudiation of delivery token
$NROT$	non-repudiation of origin token
$NRST$	non-repudiation of submission token
$NRTT$	non-repudiation of transport token
Pol	distinguishing identifier of the non-repudiation policy (or policies) which applies (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
$SIG_X(m)$	signed message generated on data m by entity X using its private key
T_i	date and time that the i th type of event or action took place (i is the index of events or actions, $i \in$ {1, 2, 3, 4})
	NOTE The date and time can be represented according to ISO 8601 (all parts). The date and time can be obtained by using a time source, as specified in ISO 14641.
T_g	date and time when 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})
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 shall be used so that the individual data items can be unambiguously 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 document.

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

— The signature key belonging to an entity shall be kept secret by that entity.

— An agreed way of obtaining an imprint of data shall be supported by all entities in the non-repudiation service. The identity function or a collision-resistant hash-function as defined in ISO/IEC 10118 (all parts) shall be used for this purpose.

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

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

— Either the evidence generator or the evidence verifier needs to use a time-stamping service or a time-marking service.

— The mechanisms in this document require that the digital signatures are certificate-based digital signatures. Identity-based digital signatures are not permitted.

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 effect. A TTP may act in one or more of the following roles.

— A delivery authority 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 TTP to guarantee the authenticity of the public verification keys, as described, for example, in ISO/IEC 9594-8.

— The non-repudiation policy in effect may require that the evidence is generated partly or totally by a TTP.

— A time-stamping token issued by a time-stamping authority 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 shall know, or agree, which non-repudiation policy is to be applicable to the evidence.

7 Digital signatures

For the mechanisms specified in this document, non-repudiation tokens are created using SIGs. The digital signature technique used to generate these SIGs shall conform to ISO/IEC 9796 (all parts), ISO/IEC 14888 (all parts) or ISO/IEC 29192-4.

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 the 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 should be used to guarantee that the non-repudiation token remains 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. The use of a TTP *C* to generate NROTs and NRDTs is optional in this particular instance of the non-repudiation services.

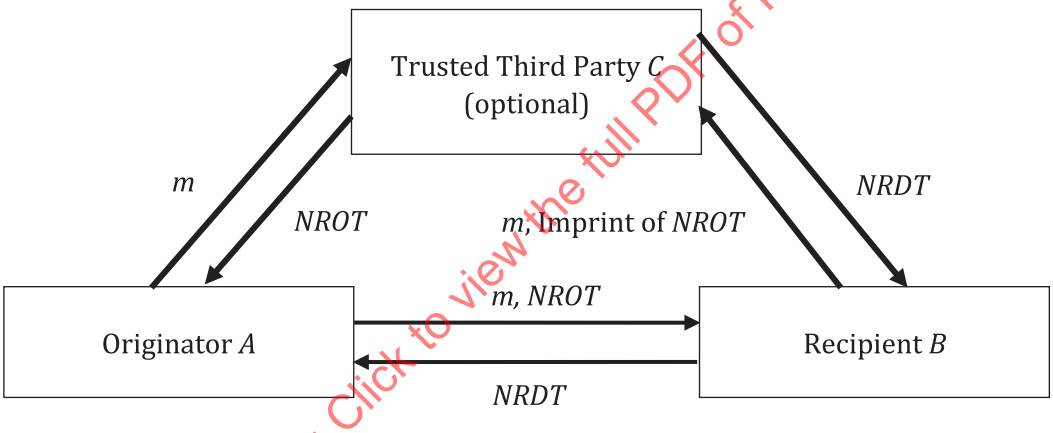

Figure 1 — Use of non-repudiation tokens without a DA

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.

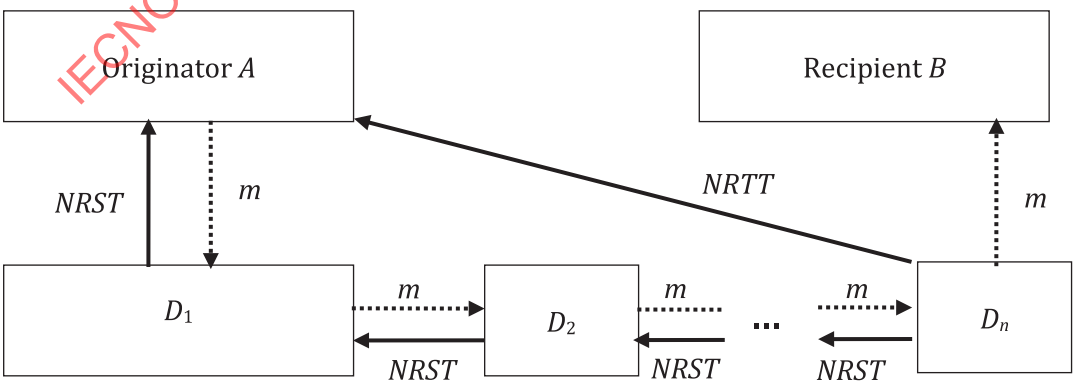

Figure 2 — Use of non-repudiation tokens with DAs

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 and delivery 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 is the originator of the non-repudiation transfer. Entity *B* is 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* shall keep all NROTs generated and record whether or not each NROT is used to generate an NRDT.

Two different mechanisms for non-repudiation are described.

9.2 Non-repudiation of origin

9.2.1 Non-repudiation of origin token

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

The NROT 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 NROT using *A*'s public key certificate.

The structure of the NROT *NROT* is:

$$NROT = (text_1, z_1, SIG_A(z_1))$$

where $z_1 = (Pol, f_{\text{origin}}, ID_A, ID_B, ID_C, T_g, T_1, Q, Imp(m))$.

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

Pol	the distinguishing identifier of the non-repudiation policy (or policies) which applies to the evidence,
f_{origin}	a flag indicating non-repudiation of origin,
ID_A	the distinguishing identifier of the originator of the message *m*, e.g. an e-mail address,
ID_B	the distinguishing identifier(s) of the intended recipient(s) of the message *m* (optional), e.g. an e-mail address,
ID_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 $SIG_A(z_1)$ in the NROT *NROT* should be replaced by $SIG_C(z_1)$,
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 the 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 NROT *NROT* 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 NROT *NROT* for message *m*;

2) *C* receives the message *m* and checks the validity of the request for an NROT;

3) *C* forms *NROT* as specified in 9.2.1;

4) *C* sends *NROT* to *A* and retains a copy;

5) *A* receives *NROT* from *C.*

Otherwise, *A* forms *NROT* as specified in 9.2.1.

b) *A* sends *NROT* (together with message *m*) to *B*.

B checks the validity of *NROT* and its contents by checking:

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

— the validity of the signature in *NROT*.

If it is valid, *NROT* is saved as evidence for non-repudiation of origin.

9.3 Non-repudiation of delivery

9.3.1 Non-repudiation of delivery token

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

The NRDT *NRTD* 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 NRDT by using *B*'s (or by authority *C*'s) public key certificate.

The structure of an NRDT *NRDT* is:

$$NRDT = (text_2, z_2, SIG_B(z_2))$$

where $z_2 = (Pol, f_{\text{delivery}}, ID_A, ID_B, ID_C, T_g, T_2, Q, Imp(m))$.

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

Pol	the distinguishing identifier of the non-repudiation policy (or policies) which applies to the evidence,
f_{delivery}	a flag indicating non-repudiation of delivery,
ID_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,
ID_B	the distinguishing identifier of the recipient of the message *m*, e.g. an e-mail address,
ID_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 $SIG_B(z_2)$ in the NRDT *NRDT* should be replaced by $SIG_C(z_2)$,
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 the 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 NRDT *NRDT* 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 NRDT to *B*.

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

a) *B* receives the message *m* and checks the validity of the request for an NRDT.

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 NRDT for message *m*;

   2) *C* receives *m* (and, optionally, *Imp*(*NROT*)) and, if present, checks that *NROT* was generated by *C* and that *NRDT* corresponding to the imprint of *NROT* has not previously been generated. If this check fails, *C* rejects the request for an NRDT;

   3) *C* forms *NRDT* as specified in 9.3.1 and records that the specific *NROT* was used to generate an NRDT;

   4) *C* sends *NRDT* to *B*;

   5) *B* receives *NRDT* from *C*.

   Otherwise, *B* forms *NRDT* as specified in 9.3.1.

c) *B* sends *NRDT* to *A*.

   1) *A* checks *NRDT* and its contents by checking:

      — the types and values of data items in *NRDT*; and

— the validity of the signature in *NRDT*.

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

10 Evidence produced by a delivery authority

10.1 General

Clause 10 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 NRSTs and NRTTs:

— An NRST 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 NRTT 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 token

In this mechanism, an NRST *NRST* 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, $i \in \{1, 2, \ldots, n\text{-}1\}$) 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 *NRST* to *X*. This provides evidence that the message has been submitted for onward delivery.

NRST 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 *NRST* using *Y*'s public key certificate.

The structure of *NRST* sent from D_{i+1} to D_i is:

$$NRST = (text_3, z_3, SIG_{D_{i+1}}(z_3))$$

where $z_3 = (Pol, f_{\text{submission}}, ID_A, ID_B, D_1, D_2, \ldots, D_i, D_{i+1}, T_g, T_3, Q, Imp(m))$.

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 NRST consists of the following data items:

Pol	the distinguishing identifier of the non-repudiation policy (or policies) which applies to the evidence,
$f_{\text{submission}}$	a flag indicating non-repudiation of submission,
ID_A	(optional) the distinguishing identifier of the originator of the message *m*, e.g. an e-mail address, whose validity may or may not have been verified by *C*,
ID_B	the distinguishing identifier of the intended recipient of the message *m*, e.g. an e-mail address,

D_i	DA, a TTP ($1 \leq i \leq n$, where n is the number of DAs involved in the transfer of m),
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 the 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, $1 \leq i \leq n-1$) sends a message m to a delivery authority Y (D_1 or D_{i+1}, respectively) for onward delivery. In the second transaction, the NRST *NRST* 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 NRST to Y.

Transaction 2 — From delivery authority Y to entity X

a) Y forms *NRST* as specified in 10.2.1.

b) Y sends *NRST* to X.

Entity X checks *NRST* and its content by checking;

— the types and values of data items in *NRST*; and

— the validity of the signature in *NRST*.

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

10.3 Non-repudiation of transport

10.3.1 Non-repudiation of transport token

An NRTT *NRTT* 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, $1 \leq i \leq n-1$) 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 *NRTT* to the originator A of the message m. This provides evidence that the message m has been transferred to B.

NRTT is

— created by the delivery authority D_n,

— sent by D_n to the message originator A,

— stored by A after A has verified it using D_n's public key certificate.

The structure of *NRTT* sent from D_n to *A* is:

$$NRTT = (text_4, z_4, SIG_{D_n}(z_4)),$$

where

$$z_4 = (Pol, f_{\text{transport}}, ID_A, ID_B, D_1, D_2, \ldots, D_n, T_g, T_4, Q, Imp(m)).$$

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 NRTT consists of the following data items:

Pol	the distinguishing identifier of the non-repudiation policy (or policies) which applies to the evidence,
$f_{\text{transport}}$	a flag indicating non-repudiation of transport,
ID_A	(optional) the distinguishing identifier of the originator of the message *m*, e.g. an e-mail address, whose validity may or may not have been verified by *C*,
ID_B	the distinguishing identifier of the intended recipient of the message *m*, e.g. an e-mail address,
D_i	DA, a TTP($1 \le i \le n$, where *n* is the number of DAs involved in the transfer of *m*),
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 the 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, $1 \le i \le n-1$) sends a 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 NRTT *NRTT* 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 *NRTT* as specified in 10.3.1.

b) D_n sends *NRTT* to *A*.

c) *A* checks *NRTT* and its content by checking:

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

