INTERNATIONAL STANDARD

ISO/IEC 13888-3

First edition
1997-12-01

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 13888-3:1997(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 13888-3 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 3: Mechanisms using asymmetric techniques

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

Non-repudiation mechanisms are specified to establish 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. Non-repudiation tokens consist of digital signatures and additional data. Non-repudiation tokens shall be stored as non-repudiation information that may be used subsequently in case of 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 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 the multipart Standard of Security Frameworks for open systems - Part 4: Non-repudiation Framework, ISO/IEC 10181-4.

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 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

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

ISO/IEC 13888-1:1997, *Information technology – Security techniques – Non-repudiation – Part 1: General.*

ISO/IEC 14888 (all parts), *Information technology – Security techniques – Digital signatures with appendix.*

3 Definitions

For the purposes of this part of ISO/IEC 13888, the definitions and notation described in ISO/IEC 13888-1 apply.

4 Symbols and abbreviations

A	the distinguishing identifier of the message originator A.
B	the distinguishing identifier of the message recipient B.
DA	Delivery Authority, a trusted third party.
f_i	a data item (flag) indicating the kind of non-repudiation service in effect.
Imp(y)	the imprint of the data *y*, consisting of data *y* or the hash-code of *y*.
m	the message which is sent from entity A to entity B in respect of which non-repudiation services are provided.
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	the distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence.
Q	an optional data item that may contain additional information, e.g., the distinguishing identifiers of the message *m,* signature mechanism, or hash-function.
S_X	the signature operation using a signature algorithm and the private key of entity *X.*
T_i	date and time the event or action took place.
T_g	date and time the evidence was generated.
text	an optional data item that may contain additional information, e.g., key identifier and/or the message identifier.
TSA	Time Stamp Authority.
TST	Time Stamp Token.
y||z	the result of the concatenation of *y* and *z* in that order.

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:

5.1 The entities of a non-repudiation exchange shall trust the same trusted third party (TTP), which may be composed of several independent TTPs bound by non-repudiation agreements.

5.2 The signature key belonging to an entity must be kept secret by that entity.

5.3 The digital signature mechanism used shall satisfy the security requirements specified by the policy.

5.4 Prior to the generation of evidence, the evidence generator must know which non-repudiation policies the evidence shall be generated in accordance with, what type of evidence is to be generated, and which mechanisms are to be used to verify the evidence.

5.5 The mechanisms for generating or verifying evidence must be available to the entities of the particular non-repudiation exchange, or a trusted authority must be available to provide the mechanisms.

5.6 The evidence generator and verifier may need access to a trusted time stamping or notary facility.

6 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. A single trusted third party may act in one or more of these roles, namely:

- A Delivery Authority (DA) is trusted to deliver the message to the intended recipient and to provide the non-repudiation of submission or transport token.
- The use of asymmetric cryptographic techniques may require the involvement of at least a trusted third party to guarantee the authenticity of the public verification keys, as described in, e.g., ISO 9594-8.
- The non-repudiation policy in force may require that the evidence be generated partly or totally by a trusted third party.
- A Time Stamp Authority (TSA) may be involved to provide trusted time stamping. TSA may also be used to ensure that a non-repudiation token remains valid even after the key used to sign the token has been compromised or revoked.
- A Notary Authority may be involved to certify the entities involved, to certify the data communicated and to extend the life of an existing token beyond its expiry or beyond subsequent revocation.
- An Evidence Recording Authority may be involved to record evidence that can later be retrieved in case of dispute.

Trusted third parties may be involved to differing degrees in the phases of non-repudiation. When exchanging evidence, the parties must either have the knowledge, or be informed, or agree which non-repudiation policy is to be applicable to the evidence.

7 Digital signatures

Non-repudiation tokens are created by using digital signatures. There are two types of digital signatures specified by ISO/IEC 9796 and ISO/IEC 14888, namely,

- signature giving message recovery, where the verification process reveals the message together with its specific redundancy,
- signature with appendix, where the verification process requires the message as part of the input.

The choice of the signature mechanism is specified by the policy applied and is beyond the scope of this standard.

Signature algorithms and keys may have a pre-defined lifetime that is stated in the key's certificate issued by the certification authority. Therefore, the tokens defined in this standard may also have a definite lifetime specified by non-repudiation policy. The mechanisms described in A.2 can be used to extend the lifetime of a token.

8 Non-repudiation tokens

The usage of each non-repudiation token is depicted in Figure 1.

8.1 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 authority C),
- sent by A to the recipient B,
- stored by the recipient B after verification.

The structure of the NRO token is:

$$\text{NRO token} = text_1 \,||\, z_1 \,||\, S_A(z_1), \quad \text{with}$$

$z_1 = Pol \| f_1 \| A \| B \| C \| T_g \| T_1 \| Q \| Imp(m).$

The information z_1 necessary for 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_1 a flag indicating non-repudiation of origin,

A the distinguishing identifier of the originator of the message *m*,

B the distinguishing identifier(s) of the intended recipient(s) of the message *m* (optional),

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 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 or hash-function, and information regarding certificates and validity of public keys,

Imp(m) the imprint of the message *m*, consisting of message *m* or the hash-code of *m*.

8.2 Non-repudiation of delivery (NRD) token

An NRD token is used to provide protection against the recipient's false denial of having received and recognised 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 verification.

The structure of an NRD token is:

NRD token = $text_2 \| z_2 \| S_B(z_2)$ with

$z_2 = Pol \| f_2 \| A \| B \| C \| T_g \| T_2 \| Q \| Imp(m).$

The information z_2 necessary for 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_2 a flag indicating non-repudiation of delivery,

A the distinguishing identifier that is claimed by B to be the originator of the message *m* (optional),

B the distinguishing identifier of the recipient of the message *m*,

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 NRO token 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 or hash-function, and information regarding certificates and validity of public keys,

Imp(m) the imprint of the message *m*, consisting of message *m* or the hash-code of *m*.

8.3 Non-repudiation of submission (NRS) token

An NRS token is created by a delivery authority. The evidence generator in this case is the delivery authority DA. The originator A or a preceding delivery authority X has sent a message *m* to the delivery authority DA. Delivery authority DA receives the message *m* and sends the NRS token to A or the preceding transfer agent X, thus providing evidence that the message has been submitted for onward delivery.

The NRS token is

- generated by the delivery authority DA,
- sent by DA to the message originator A or a preceding delivery authority X,
- stored by A or X after verification.

The structure of an NRS token is:

NRS token = $text_3 \| z_3 \| S_{DA}(z_3)$ with

$z_3 = Pol \| f_3 \| A \| B \| C \| D \| E \| T_g \| T_3 \| Q \| Imp(m).$

The information z_3 necessary for 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_3 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* may or may not have been verified by DA,

B the distinguishing identifier of the intended recipient of the message *m*,

C the distinguishing identifier of the delivery authority DA,

D the distinguishing identifier of the delivery authority X (if applicable),

E the distinguishing identifier of the delivery authority Y (if applicable),

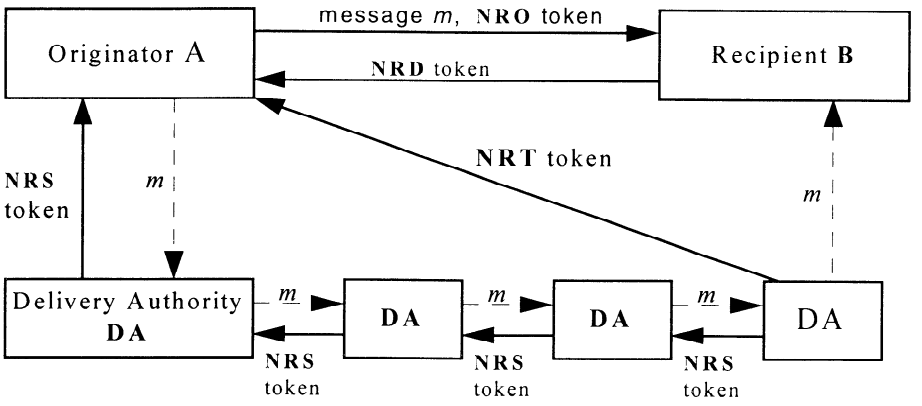

Figure 1 — Non-repudiation tokens and their usage

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 or hash-function, and information regarding certificates and validity of public keys,

Imp(m) the imprint of the message *m*, consisting of message *m* or the hash-code of *m*.

8.4 Non-repudiation of transport (NRT) token

An NRT token is used by the message originator as evidence that the message *m* has been transferred to B by a delivery authority DA. The evidence generator in this case is the delivery authority DA. The originator A or the preceding delivery authority X has sent a message *m* to DA. DA transfers the message *m* to the recipient B or to the following delivery authority. The DA that transfers the message *m* to the recipient B also sends the NRT token to the originator A of the message *m*, thus providing evidence that the message *m* has been transferred to B.

The NRT token is

- created by the delivery authority DA,
- sent by DA to the message originator A,
- stored by A after verification.

The structure of an NRT token is:

$$\text{NRT token} = text_4 \,||\, z_4 \,||\, S_{DA}(z_4) \quad \text{with}$$

$$z_4 = \text{PoI} \,||\, f_4 \,||\, A \,||\, B \,||\, C \,||\, D \,||\, T_g \,||\, T_4 \,||\, Q \,||\, Imp(m).$$

The information z_4 necessary for an NRT token consists of the following data items:

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

f_4 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* may or may not have been verified by DA,

B the distinguishing identifier of the intended recipient of the message *m*,

C the distinguishing identifier of the delivery authority DA,

D the distinguishing identifier of the delivery authority X, if applicable (optional),

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 was delivered,

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

Imp(m) the imprint of the message *m*, consisting of message *m* or the hash-code of *m*.

9 Mechanisms without delivery authority

The non-repudiation mechanisms in this clause allow for generation of evidence for non-repudiation of origin (NRO) and delivery (NRD) without delivery authority participation. The entity A wishes to send a message *m* to the entity B and thus will be the originator of the non-repudiation transfer. The entity B will be the recipient.

It is assumed that entity A knows its own signature key, entity B knows its own signature key, and that the corresponding verification keys are known to all the entities concerned.

Two different mechanisms for non-repudiation are described.

9.1 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) Entity A forms NRO token as specified in Clause 8.1.

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

Entity B checks the validity of the NRO token and its contents. If it is valid, the NRO token is saved as the evidence of the non-repudiation of origin. If it is not valid, Entity B shall request A to send the NRO token again.

9.2 Mechanism for non-repudiation of 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.

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

Transaction 2 - From Entity B to Entity A

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

b) Entity B forms the NRD token as specified in Clause 8.2.

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

d) Entity A checks the NRD token and its contents. If it is valid, the NRD token is saved as the evidence that B has received the message *m*. If it is not valid, Entity A shall request B to send the NRD token again.

10 Mechanisms using a delivery authority

There may be a number of additional mechanisms using trusted third parties in a non-repudiation process. Such mechanisms may be incorporated into the basic mechanisms 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.

10.1 Mechanism for non-repudiation of submission

In the first transaction of this mechanism, a sending entity X sends a message to a delivery authority DA for onward delivery. In the second transaction, the NRS token is sent from the delivery authority DA to the entity X. The non-repudiation of submission is established in the second transaction.

Transaction 1 - From Entity X to delivery authority DA

Entity X sends the message *m* and a request for NRS token to DA.

Transaction 2 - From delivery authority DA to Entity X

a) DA forms the NRS token as specified in Clause 8.3.

b) DA sends the NRS token to Entity X.

c) Entity X checks the NRS token and its content. If it is valid, the NRS token is saved as the evidence for non-repudiation of submission (i.e., the message was submitted).

10.2 Mechanism for non-repudiation of transport

In the first transaction of this mechanism, a sending entity X sends message *m* to a delivery authority DA for onward delivery. In the second transaction, the message *m* is sent from the DA to the recipient B. In the third transaction, the NRT token is generated by DA and sent to entity A, the originator of the message *m*. The non-repudiation of transport is established in the third transaction.

Transaction 1 - From Entity X to delivery authority DA

Entity X sends the message *m* to DA.

Transaction 2 - From delivery authority DA to Entity B

DA sends the message *m* to Entity B.

Transaction 3 - From delivery authority DA to Entity A

a) DA forms the NRT token as specified in Clause 8.4.

b) DA sends the NRT token to Entity A.

c) Entity A checks the NRT token and its content. If it is valid, the NRT token is saved as the evidence for non-repudiation of transport (i.e., the message was delivered to the intended recipient B).

Annex A

(informative)

Mechanisms for other non-repudiation services

Depending on the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, the following mechanisms may be required to complete the non-repudiation services.

Mechanism for time stamping service to provide evidence including a trusted time stamp generated by a Time Stamping Authority.

Mechanism for notary service to provide evidence assurance about the action or event performed.

Mechanism for evidence recording service to keep records of operations for the purpose of recovering evidence prior to dispute resolution.

A.1 Mechanism for time stamping service

In this clause, the TTP provides a time stamping service by generating a Time Stamp Token (TST). When a trusted time reference is required and when the clock provided by the token generating party cannot be trusted, it is necessary to rely on a trusted third party, Time Stamping Authority (TSA). Its role is to countersign a message to establish further evidence indicating when the signature was generated.

Time stamping service may also be used to ensure that a non-repudiation token remains valid even after the key used to sign the token has been compromised or revoked.

In the first transaction of this mechanism, the requesting entity X requests a time stamping service by sending the data *y* which it wants to be countersigned with time stamp, where *y* can be a message, a non-repudiation token, the hash-code of a meesage, the hash-code of a token, or any data that the user wants to be countersigned with time stamp. In the second transaction, the Time Stamping Authority responds by sending the counter-signature with time stamp over the data *y*.

Transaction 1 - From Entity X to Time Stamping Authority

a. Entity X forms request *R*:

R = text || y.

The text may include:

- an indication that *R* is a request for time stamping service,
- the distinguishing identifier of the requester X,
- the distinguishing identifier of the TSA,
- the request policy.

b. Entity X sends the request to TSA.

Transaction 2 - From TSA to Entity X

a. TSA generates Time Stamp Token (TST):

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

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

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

Pol the policy (or policies) which apply to the evidence,

f a flag indicating Time Stamping Token,

TSA the distinguishing identifier of the Time Stamping Authority,

T_g the date and time when the evidence was generated,

Q optional data that need to be protected, e.g., the distinguishing identifiers of the data *y*, signature mechanism or hash-function, and information regarding certificates and validity of public keys,

Imp(y) the imprint of the data *y*, consisting of *y* or the hash-code of *y*.

b. TSA sends the TST to Entity X.

c. Entity X verifies the TST.

A.2 Mechanism for notary service

The notary service is used to provide evidence by a Notary Authority to certify the entities involved, to certify the data communicated and to extend the life of an existing non-repudiation token beyond its expiry or beyond subsequent revocation.

In the first transaction of this mechanism, the requesting entity X requests notary certification by sending the data *y* which it wants to be certified, where *y* can be a message, a non-repudiation token, the hash-code of a meesage, the hash-code of a token, or any data that the user wants to be certified by the Notary Authority. In the second transaction, the Notary Authority responds by returning the certified data.

Transaction 1 - From Entity X to Notary Authority

a. Entity X forms request *R*:

R = text || y.

The text may include:

- an indication that *R* is a request for notary service,

- the distinguishing identifier of entity X,
- the distinguishing identifier of the Notary Authority,
- the date and time of the request generation.

b. Entity X sends the request R, or the signed request $S_X(R)$ to Notary Authority.

Transaction 2 - From Notary Authority to Entity X

a. Notary Authority checks the validity of the request.

b. Notary Authority sends the Notarization Token (NT) of certified data to Entity X:

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

$w = PoI \,||\, f \,||\, X \,||\, NA \,||\, T_g \,||\, Q \,||\, Imp(y)$.

The data element w consists of the following data items:

PoI	the policy (or policies) which apply to the evidence,
f	a flag indicating notary service,
X	the distinguishing identifier of Entity X,
NA	the distinguishing identifier of the Notary Authority,
T_g	the date and time when the evidence was generated,
Q	optional data that need to be protected, e.g., the distinguishing identifiers of the data y, signature mechanism or hash-function, and information regarding certificates and validity of public keys,
$Imp(y)$	the imprint of the data y, consisting of data y or the hash-code of y.

c. Entity X checks the certified data and stores it.

A.3 Mechanism for evidence recording service

The evidence recording service is provided to keep records of operations so that they will be available for the purpose of resolving any disputes that may arise at some time in the future. The Evidence Recording Authority is trusted by the evidence owner to record and keep the evidence securely.

In the first transaction of this mechanism, the requesting entity X requests an evidence recording service by sending the evidence y which it wants to be recorded (e.g., y can be a message or a non-repudiation token). In the second transaction, the Evidence Recording Authority responds by returning an acknowledgment.

Transaction 1 - From Entity X to Evidence Recording Authority

a. Entity X forms request R:

R = text || y.

The text may include:

- an indication that R is a request for evidence recording service,
- the distinguishing identifier of the evidence generator,
- the distinguishing identifier of the requester X,
- the distinguishing identifier of the Evidence Recording Authority,
- the date and time of the request generation.

b. Entity X sends request R, or signed request $S_X(R)$ to Evidence Recording Authority.

Transaction 2 - From Evidence Recording Authority to Entity X

a. Evidence Recording Authority checks the validity of the request and keeps correct time reference and R securely.

b. Evidence Recording Authority sends the Acknowledgment to Entity X:

Acknowledgment = text || recording number.

The text may include:

- data item indicating that the data is an acknowledgment of the evidence recording service,
- all or part of the request R,
- the policy (or policies) which apply to the evidence,
- the date and time of the evidence recording,
- signature of the Evidence Recording Authority.