
**Information technology — Security
techniques — Non-repudiation —**

Part 2:
Mechanisms using symmetric techniques

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

Partie 2: Mécanismes utilisant des techniques symétriques



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 13888-2 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*

Further parts may follow.

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

© ISO/IEC 1998

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Information technology — Security techniques — Non-repudiation —

Part 2:

Mechanisms using symmetric 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 provides descriptions of generic structures that can be used for non-repudiation services, and of some specific, communication related mechanisms which can be used to provide non-repudiation of origin (*NRO*), non-repudiation of delivery (*NRD*), non-repudiation of submission (*NRS*), and non-repudiation of transport (*NRT*) services. Other non-repudiation services can be built using the generic structures described in Clause 8 in order to meet the requirements defined by the security policy.

This part of ISO/IEC 13888 relies on the existence of a trusted third party (*TTP*) to prevent fraudulent repudiation. Usually an on-line trusted third party is needed.

Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific to each non-repudiation service. Non-repudiation tokens used in this part consist of Secure Envelopes 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 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 9797:1994, *Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*.

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 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*.

3 Definitions

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

4 Notation and Abbreviations

4.1 Notation

4.1.1 Notation from ISO/IEC 13888-1

<i>Imp(y)</i>	<i>imprint of data string y, either (1) the hash-code of data string y, or (2) the data string y.</i>
<i>SENV_X</i>	<i>the secure envelope generated with the secret key x of entity X.</i>

<i>text</i>	<i>a data item forming part of a token that may contain additional information, e.g., key identifier and/or the message identifier.</i>
$y z$	<i>the result of the concatenation of y and z in that order.</i>

4.1.2 Notation unique for the purposes of this part of ISO/IEC 13888

a	<i>a secret key known only to entity A and a TTP.</i>
A	<i>the distinguishing identifier of entity A.</i>
b	<i>a secret key known only to entity B and a TTP.</i>
B	<i>the distinguishing identifier of entity B.</i>
da	<i>secret key of the Delivery Authority DA.</i>
f, f_j	<i>data item (flag) indicating the kind of non-repudiation service in effect.</i>
m	<i>a message for which evidence is generated.</i>
$MAC_X(y)$	<i>the cryptographic check value computed on the data y using the key of entity X.</i>
T_g	<i>date and time the evidence was generated.</i>
T_j	<i>date and time the event or action took place.</i>
ttp	<i>a secret key known only to the TTP to generate non-repudiation tokens.</i>
x	<i>a secret key known either to two entities or only to the trusted third party.</i>
z_1	<i>a data field consisting of data fields relevant for the provision of the NRO token.</i>
z_2	<i>a data field consisting of data fields relevant for the provision of the NRD token.</i>
z_3	<i>a data field consisting of data fields relevant for the provision of the NRS token.</i>
z_4	<i>a data field consisting of data fields relevant for the provision of the NRT token.</i>
z_5	<i>a data field consisting of data fields relevant for the provision of the TST.</i>

4.2 Abbreviations

DA	<i>Delivery Authority.</i>
$GNRT$	<i>Generic Non-Repudiation Token.</i>
NRD	<i>Non-Repudiation of Delivery.</i>
$NRDT$	<i>Non-repudiation of delivery token.</i>
NRO	<i>Non-Repudiation of Origin.</i>
$NROT$	<i>Non-repudiation of origin token.</i>
NRS	<i>Non-Repudiation of Submission.</i>
$NRST$	<i>Non-repudiation of submission token.</i>
NRT	<i>Non-Repudiation of Transport.</i>
$NRTT$	<i>Non-repudiation of transport token.</i>
Pol	<i>the distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence.</i>
PON	<i>Positive Or Negative, the result of a verification process.</i>
TSA	<i>Trusted time Stamping Authority.</i>
TST	<i>Time Stamping Token generated by the TSA.</i>
TTP	<i>Trusted Third Party.</i>

5 Requirements

5.1 Two entities wishing to use one of the mechanisms specified in this part of ISO/IEC 13888 must both trust the same third party.

5.2 Prior to the use of these mechanisms, it is assumed that each entity shares a secret key with the trusted third party. The trusted third party (*TTP*) also holds a single key known only to itself.

NOTE – Key management, key generation and key establishment mechanisms are defined in the multipart standard ISO/IEC 11770.

5.3 A common function *Imp* is shared 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.

5.4 A function *MAC* chosen for envelope (*SENV*) creation must be held by all participants in the non-repudiation service.

5.5 The *TTP* generating the non-repudiation tokens shall be able to access the time and date.

5.6 The strength of the mechanisms specified in this part of 13888 is dependent on the length and the secrecy of the key, on the nature of the function *MAC*, and on the length of the check value. These parameters shall be chosen to meet the required security level, as may be specified by the security policy.

6 Organization of this part of ISO/IEC 13888

The mechanisms described in this part of ISO/IEC 13888 require that each of the two entities involved are able to communicate separately with the *TTP*. They require the use of secure envelopes described in clause 7. The basic concepts for the generation and verification of non-repudiation tokens, and thus of evidence, are described in clause 8. The mechanisms described in clause 9 require the use of a *TTP* which needs to be called for every evidence generation and every evidence verification. Three variants of this mechanism are further described as examples in clause 10.

7 Secure envelopes

Two entities that share a secret key (known only to them) may send messages to one another using a method for data integrity known as a Secure ENvelope, *SENV*. A *SENV* is formed by protecting the input data items with a secret key. A *SENV* can also be used by a *TTP* for generating and verifying evidence, using the secret key held only by the *TTP*.

The method of creating a secure envelope is through the use of symmetric integrity techniques. The secret key x of entity X is used to compute a cryptographic check value $MAC_X(y)$ which is appended to the data y :

$$SENV_X(y) = y || MAC_X(y),$$

where $MAC_X(y)$ can be the message authentication code as specified in ISO/IEC 9797.

The function *MAC* shall fulfill the following requirements as specified in ISO/IEC 9798-4:

- for any key x and data string y , it shall be practical to compute $MAC_X(y)$;
- for any fixed key x , and given no prior knowledge of x , it shall be computationally infeasible to find a new pair (y', z) such that $MAC_X(y') = z$; even given knowledge of a set of pairs (y_i, z_i) such that $MAC_X(y_i) = z_i$ ($i=1, 2, \dots$), where the value of y_i may have been chosen after observing the value of z_i ($i=1, 2, \dots, i-1$).

8 Generation and verification of non-repudiation tokens

In the non-repudiation mechanisms described in this clause, the *TTP* acts as an evidence generation and an evidence verification authority. It is trusted to maintain the integrity of certain records and is directly involved in the resolution of any dispute.

8.1 Creation of tokens by the *TTP*

The *TTP* issues "tokens" to be associated with a message m . A token is a secure envelope formed by the *TTP* using its secret key on data specific to a message. Because no other entity knows secret key tp , the *TTP* is the only one that can create or verify tokens. In ISO/IEC 13888-1 the generic non-repudiation token (*GNRT*) is defined as follows:

$$GNRT = text \parallel SENV_X(y).$$

The *TTP* should check also the data items present in the evidence request before the tokens are issued.

8.2 Data items used in the non-repudiation mechanisms

8.2.1 Data items used in secure envelopes

The following data fields will form the contents of secure envelopes

$$SENV_X(z) = z \parallel MAC_X(z)$$

to be exchanged during the non-repudiation mechanisms described in this part of ISO/IEC 13888:

$$z = Pol \parallel f_i \parallel A \parallel B \parallel C \parallel D \parallel E \parallel T_g \parallel T_i \parallel Q \parallel Imp(m).$$

The data field z consists of the following data items:

- Pol* the distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence,
- f_i* the type of non-repudiation service being provided,
- A* the distinguishing identifier of the originating entity,
- B* the distinguishing identifier of the entity interacting with the originating entity,
- C* the distinguishing identifier of the evidence generator,
- D* the distinguishing identifier of the evidence requester when different from the originating entity,
- E* the distinguishing identifiers of other entities involved with the action,
- T_g* the date and time the evidence was generated,
- T_i* the date and time the event or action took place,
- Q* optional data that need to be protected,

Imp(m) the imprint of a message m related to the action (either the hash-code of the message m or the message m itself).

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

8.2.2 Data items used in non-repudiation tokens

Non-repudiation tokens contain a text field denoted by *text*:

$$Non-repudiation\ token = text \parallel SENV_{TTP}(z)$$

text includes additional data (like a message identifier or key identifier) that does not need to be cryptographically protected but may be needed to identify the message and the key used in the computation of the integrity check value *MAC*. This information depends upon the technique being used.

8.3 Non-repudiation tokens

Evidence is provided by non-repudiation tokens, and, if the policy requires it, by additional tokens such as a time stamping token (*TST*), and a token provided by another trusted fourth party (e.g., a Notary) giving additional assurance about an event or action, or about the existence of a message.

If the trusted third party is able to generate a trusted time stamp itself, the addition of a time stamping token (*TST*) as evidence is unnecessary. The time included in non-repudiation tokens (*NROT*, *NRDT*, *NRST* and *NRTT*) is regarded secure as it was provided by a trusted authority.

If the trusted third parties (*TTP*, *DA*) are unable to provide a trusted time stamp, then a time stamping token (*TST*) provided by the trusted time stamping authority (*TSA*) shall be added to the set of non-repudiation information to complete the evidence.

8.3.1 Non-repudiation of origin token

A non-repudiation of origin token (*NROT*) is created by the *TTP* at the request of the originator:

$$NROT = text \parallel z_1 \parallel MAC_{TTP}(z_1), \text{ with}$$

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

The information z_1 necessary for the *NROT* consists of the following data items:

- Pol* the distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence,
- f₁* a flag indicating non-repudiation of origin,
- A* the distinguishing identifier of the originator,
- B* the distinguishing identifier of the intended recipient,
- C* the distinguishing identifier of the *TTP* generating the evidence,
- D* the distinguishing identifier of the observer, if an independent observer is involved,
- T_g* the date and time the evidence was generated,
- Q* optional data that need to be protected,
- Imp(m)* the imprint of the message m .