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

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. 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.

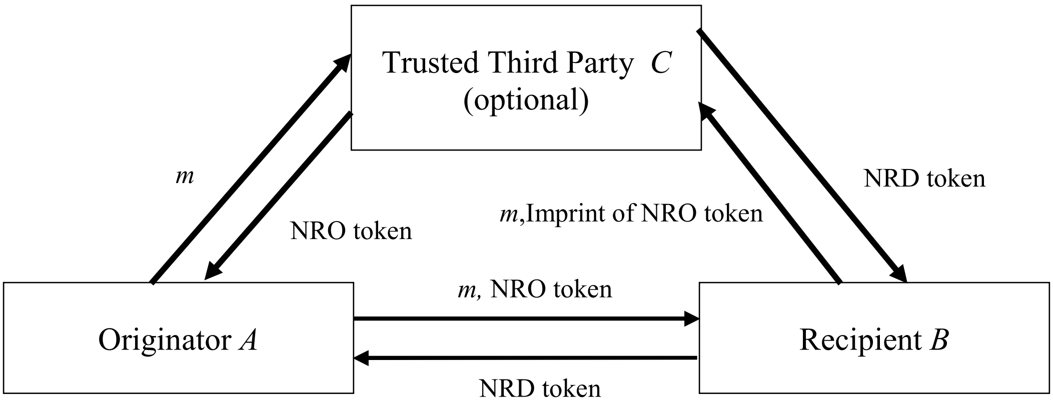

Figure 1 – Use of non-repudiation tokens without a Delivery Authority

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.

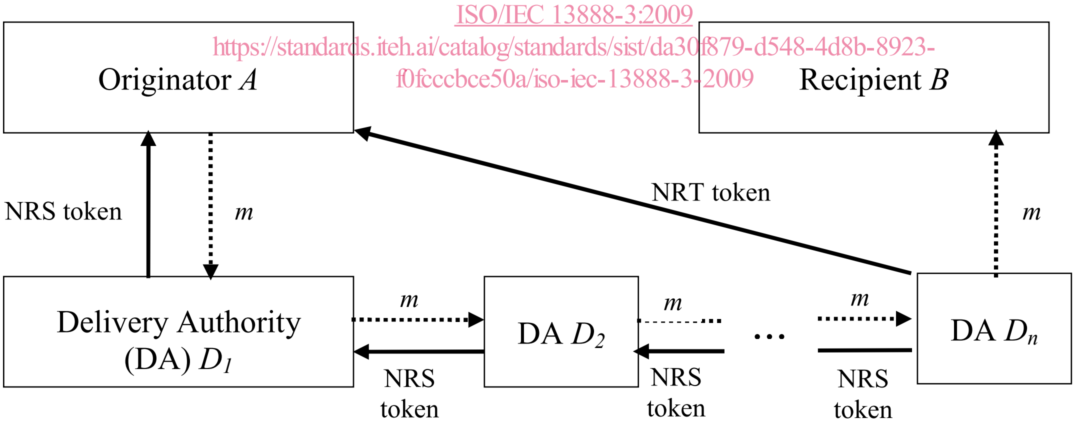

Figure 2 – Use of non-repudiation tokens with Delivery Authorities

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,