

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
Documents
ISO/IEC 13888-3:1997(E)
Document Sharing Hub

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.

© ISO/IEC 1997

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 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.
<i>Pol</i>	the distinguishing identifier of the non-repudiation policy (or policies) which apply to the evidence.
<i>Q</i>	an optional data item that may contain additional information, e.g., the distinguishing identifiers of the message <i>m</i> , signature mechanism, or hash-function.
<i>S_X</i>	the signature operation using a signature algorithm and the private key of entity <i>X</i> .
<i>T_i</i>	date and time the event or action took place.
<i>T_g</i>	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.
<i>y z</i>	the result of the concatenation of <i>y</i> and <i>z</i> 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:

$$\text{NRO token} = \text{text}_1 || z_1 || S_A(z_1), \text{ with}$$