

INTERNATIONAL STANDARD

ISO/IEC
13888-1

First edition
1997-12-01

Information technology — Security techniques — Non-repudiation —

Part 1: General

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

Partie 1: Généralités



Reference number
ISO/IEC 13888-1:1997(E)
AVA Documents
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 13888-1 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 1: General

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 describes a model for non-repudiation mechanisms providing evidence based on cryptographic techniques. Non-repudiation mechanisms generic to the various non-repudiation services are first described and then applied to a selection of specific non-repudiation services such as:

- non-repudiation of origin,
- non-repudiation of delivery,
- non-repudiation of submission,
- non-repudiation of transport.

Non-repudiation services establish evidence: evidence establishes accountability regarding a particular event or action. The entity responsible for the action, or associated with the event, with regard to which evidence is generated, is known as the evidence subject. There are two main types of evidence the nature of which depends on cryptographic techniques employed:

- Secure Envelopes generated by an evidence generating authority using symmetric cryptographic techniques,
- Digital signatures generated by an evidence generator or an evidence generating authority using asymmetric cryptographic techniques.

Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific to each non-repudiation service. Non-repudiation tokens consist of Secure Envelopes and/or digital signatures and, optionally, of additional data. Non-repudiation tokens may be stored as non-repudiation information that may be used subsequently by disputing parties or by an adjudicator to arbitrate in 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 data created or 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.

This part of ISO/IEC 13888 serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. ISO/IEC 13888 provides non-repudiation mechanisms for the following phases of non-repudiation:

- evidence generation,
- evidence transfer, storage and retrieval, and
- evidence verification.

Dispute arbitration is outside the scope of ISO/IEC 13888.

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 9797:1994, *Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*.

ISO/IEC 10118-1:1994, *Information technology – Security techniques – Hash-functions – Part 1: General*.

ISO/IEC 10181-1:1996, *Information technology – Open Sy-*

systems Interconnection – Security frameworks for open systems – Part 1: Overview.

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

ISO/IEC 14888-1¹⁾ *Information technology – Security techniques – Digital signatures with appendix – Part 1: General.*

ISO/IEC 11770-3¹⁾ *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.*

3 Definitions

3.1 Definitions from ISO 7498-2

- **accountability:** *The property that ensures that the actions of an entity may be traced uniquely to the entity.*
- **data integrity:** *The property that data has not been altered or destroyed in an unauthorised manner.*
- **data origin authentication:** *The corroboration that the source of data received is as claimed.*
- **digital signature:** *Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.*
- **security policy:** *The set of criteria for the provision of security services.*

3.2 Definitions from ISO/IEC 9594-8

- **certification authority:** *An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys.*

3.3 Definitions from ISO/IEC 10118-1

- **hash-code:** *The string of bits that is the output of a hash-function.*
- **hash-function:** *A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:*
 - *it is computationally infeasible to find for a given output an input which maps to this output,*
 - *it is computationally infeasible to find for a given input a second input which maps to the same output.*

3.4 Definitions from ISO/IEC 10181-1

- **security certificate:** *a set of security relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication.*
- **security token:** *a set of security relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority.*
- **trust:** *a relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not violate the given security policy.*
- **trusted third party:** *a security authority or its agent, trusted by other entities with respect to security-related*

activities.

3.5 Definitions from ISO/IEC 10181-4

- **evidence generator:** *an entity that produces non-repudiation evidence.*
- **evidence subject:** *an entity whose involvement in an event or action is established by evidence.*
- **evidence user:** *an entity that uses non-repudiation evidence.*
- **evidence verifier:** *an entity that verifies non-repudiation evidence.*
- **non-repudiation service requester:** *an entity that requests that non-repudiation evidence be generated for a particular event or action.*

3.6 Definitions from ISO/IEC 11770-3

- **key:** *A sequence of symbols that controls the operations of a cryptographic transformation (e.g., encipherment, decipherment, cryptographic check-function computation, signature calculation, or signature verification).*

3.7 Definitions unique to this Standard on Non-repudiation

For the use of this multipart standard the following definitions apply:

3.7.1 Certificate: An entity's data rendered unforgeable with the private or secret key of a certification authority.

3.7.2 Data storage: A means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority.

3.7.3 Delivery authority: An authority trusted by the sender to deliver the data from the sender to the receiver, and to provide the sender with evidence on the submission and transport of data upon request.

3.7.4 Distinguishing identifier: Information which unambiguously distinguishes an entity in the non-repudiation process.

3.7.5 Evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.

NOTE – Evidence does not necessarily prove truth or existence of something (see proof) but contributes to establish proof.

3.7.6 Evidence requester: An entity requesting evidence to be generated either by another entity or by a trusted third party.

3.7.7 Evidence subject: the entity responsible for the action, or associated with the event, with regard to which evidence is generated.

3.7.8 Imprint: A string of bits, either the hash-code of a data string or the data string itself.

3.7.9 Message Authentication Code: A data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of a message by any entity holding the secret key.

3.7.10 Monitor (Monitoring Authority): A trusted third party monitoring the actions and events and is trusted to provide evidence about what was monitored.

3.7.11 Non-repudiation exchange: A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.

¹⁾ To be published.

3.7.12 Non-repudiation information: A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.

3.7.13 Non-repudiation of Creation: This service is intended to protect against an entity's false denial of having created the content of a message (i.e., being responsible for the content of a message).

3.7.14 Non-repudiation of Delivery: This service is intended to protect against a recipient's false denial of having received the message and recognised the content of a message.

3.7.15 Non-repudiation of Knowledge: This service is intended to protect against a recipient's false denial of having taken notice of the content of a received message.

3.7.16 Non-repudiation of Origin: This service is intended to protect against the originator's false denial of having created the content of a message and of having sent a message.

3.7.17 Non-repudiation of Receipt: This service is intended to protect against a recipient's false denial of having received a message.

3.7.18 Non-repudiation of Sending: This service is intended to protect against the sender's false denial of having sent a message.

3.7.19 Non-repudiation of Submission: This service is intended to provide evidence that a delivery authority has accepted the message for transmission.

3.7.20 Non-repudiation of Transport: This service is intended to provide evidence for the message originator that a delivery authority has delivered the message to the intended recipient.

3.7.21 Non-repudiation policy: A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.

3.7.22 Non-repudiation token: A special type of security token as defined in ISO/IEC 10181-1 consisting of evidence, and, optionally, of additional data.

3.7.23 Notarization: The provision of evidence by a notary about the properties of the entities involved in an action or event, and of the data stored or communicated.

3.7.24 Notarization token: A non-repudiation token generated by a notary.

3.7.25 Notary (notary authority): a trusted third party trusted to provide evidence about the properties of the entities involved and of the data stored or communicated, or to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation.

3.7.26 NRD token: Non-repudiation of delivery token. A data item which allows the originator to establish non-repudiation of delivery for a message.

3.7.27 NRO token: Non-repudiation of origin token. A data item which allows recipients to establish non-repudiation of origin for a message.

3.7.28 NRS token: Non-repudiation of submission token. A data item which allows either the originator (sender) or the delivery authority to establish non-repudiation of submission for a message having been submitted for transmission.

3.7.29 NRT token: Non-repudiation of transport token.

A data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message.

3.7.30 Originator: The entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided.

3.7.31 Private key: That key of an entity's asymmetric key pair which is usable only by that entity. In the case of an asymmetric signature system, the private key and the associated algorithms define the signature transformation.

3.7.32 Proof: The corroboration that evidence is valid in accordance with the non-repudiation policy in force.

NOTE – Proof is evidence that serves to prove truth or existence of something.

3.7.33 Public key: That key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system, the public key and the associated algorithms define the verification transformation.

3.7.34 Public key certificate: A security certificate which binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates the validity of the corresponding private key.

3.7.35 Recipient: The entity that gets (receives or fetches) a message for which non-repudiation services are to be provided.

3.7.36 Redundancy: Any information that is known and can be checked.

3.7.37 Secret key: A key usable with symmetric cryptographic techniques and usable only by a set of specified entities.

3.7.38 Secure Envelope (SENV): A set of data items which is constructed by an entity in such a way that any entity holding the secret key can verify their integrity and origin. For the purpose of generating evidence, the SENV is constructed and verified by a TTP with a secret key known only to the TTP.

3.7.39 Signer: The entity generating a digital signature.

3.7.40 Trusted third party: A security authority, or its agent, trusted by other entities with respect to security related activities. In the context of this multipart standard, a trusted third party is trusted by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as an adjudicator.

3.7.41 Trusted time stamp: A data item with time and date information assured by a trusted time stamping authority.

3.7.42 Trusted time stamping authority: A trusted third party trusted to provide evidence which includes the time when the trusted time stamp is generated.

3.7.43 Verification key: A value required to verify a cryptographic check value.

3.7.44 Verifier: An entity that verifies an evidence.

4 Notation and Abbreviations

A	the distinguishing identifier of entity A.
B	the distinguishing identifier of entity B.
CA	Certification Authority.
$CHK_X(y)$	the cryptographic check value computed on the data y using the key of entity X .