INTERNATIONAL STANDARD

# ISO/IEC 13888-1

Second edition
2004-06-01

## IT security techniques — Non-repudiation —

## Part 1: General

*Techniques de sécurité dans les TI — Non-répudiation —*
*Partie 1: Généralités*

Reference number
ISO/IEC 13888-1:2004(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 13888-1:2004 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 13888-1:1997), which has been technically revised.

ISO/IEC 13888 consists of the following parts, under the general title *IT 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 verify 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 check values generated by using symmetric or asymmetric 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.

# IT security techniques — Non-repudiation —

# Part 1: **General**

## 1 Scope

This part of ISO/IEC 13888 serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. This multipart International Standard 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 this International Standard.

## 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 7498-2:1989,* Information processing systems – Open Systems Interconnection – Basic Reference Model, Part 2: Security Architecture.

*ISO/IEC 9594-8:2001,* Information processing systems – Open Systems Interconnection – The Directory, Part 8: Authentication Framework.

*ISO/IEC 9796 (all parts),* Information technology – Security techniques – Digital signature scheme giving message recovery.

*ISO/IEC 9797 (all parts),* Information technology – Security techniques – Message authentication codes (MACs).

*ISO/IEC 9798-1:1997,* Information technology – Security techniques – Entity authentication mechanisms – Part 1: General

*ISO/IEC 10118 (all parts),* Information technology – Security techniques – Hash-functions.

*ISO/IEC 10181-1:1996,* Information technology – Open 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 11770-3:1999,* Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.

*ISO/IEC 13888-2:1998,* Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques

*ISO/IEC 13888-3:1997,* Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques

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

*ISO/IEC 18014 (all parts),* Information technology – Security techniques – Time-stamping services.

# 3 Terms and definitions

## 3.1 Definitions from ISO 7498-2

**3.1.1**
**Accountability**
The property that ensures that the actions of an entity may be traced uniquely to the entity.

**3.1.2**
**Data integrity**
The property that data has not been altered or destroyed in an unauthorised manner.

**3.1.3**
**Data origin authentication**
The corroboration that the source of data received is as claimed.

**3.1.4**
**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.

**3.1.5**
**Security policy**
The set of criteria for the provision of security services.

## 3.2 Definitions from ISO/IEC 9594-8

**3.2.1**
**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 9797-1

**3.3.1**
**Message Authentication Code (MAC)**
The string of bits which is the output of a MAC algorithm.

NOTE – A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

## 3.4 Definitions from ISO/IEC 10118-1

**3.4.1**
**Hash-code**
The string of bits that is the output of a hash-function.

**3.4.2**
**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.

## 3.5 Definitions from ISO/IEC 10181-1

**3.5.1**
**Security authority**
An entity that is responsible for the definition or enforcement of security policy.

**3.5.2**
**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.

**3.5.3**
**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.

**3.5.4**
**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.

## 3.6 Definitions from ISO/IEC 10181-4

**3.6.1**
**Evidence generator**
An entity that produces non-repudiation evidence.

**3.6.2**
**Evidence user**
An entity that uses non-repudiation evidence.

**3.6.3**
**Evidence verifier**
An entity that verifies non-repudiation evidence.

**3.6.4**
**Non-repudiation service requester**
An entity that requests that non-repudiation evidence be generated for a particular event or action.

## 3.7 Definitions from ISO/IEC 11770-3

**3.7.1**
**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).

**3.7.2**
**Private key**
That key of an entity's asymmetric key pair which can only be used by that entity.

NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

**3.7.3**
**Public key**
That key of an entity's asymmetric key pair which can be made public.

NOTE – In the case of an asymmetric signature scheme the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

**3.7.4**
**Public key certificate**
The public key information of an entity signed by the certification authority and thereby rendered unforgeable.

### 3.7.5
**Secret key**
A key used with symmetric cryptographic techniques and usable only by a set of specified entities.

## 3.8 Definitions from ISO/IEC 18014

### 3.8.1
**Time-stamp**
A time variant parameter which denotes a point in time with respect to a common time reference.

### 3.8.2
**Time-stamping authority**
A trusted third party trusted to provide a time-stamping service.

## 3.9 Definitions unique to this International Standard on non-repudiation

For the use of this multipart International Standard the following definitions apply:

### 3.9.1
**Certificate**
An entity's data rendered unforgeable with the private or secret key of a certification authority.

### 3.9.2
**Data storage**
A means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority.

### 3.9.3
**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.

### 3.9.4
**Distinguishing identifier**
Information which unambiguously distinguishes an entity in the non-repudiation process.

### 3.9.5
**Evidence**
Information either by itself, or 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.

### 3.9.6
**Evidence requester**
An entity requesting evidence to be generated either by another entity or by a trusted third party.

### 3.9.7
**Evidence subject**
The entity responsible for the action, or associated with the event, with regard to which evidence is generated.

### 3.9.8
**Imprint**
A string of bits, either the hash-code of a data string or the data string itself.

### 3.9.9
**Monitor (monitoring authority)**
A trusted third party monitoring the actions and events and is trusted to provide evidence about what was monitored.

**3.9.10**
**Non-repudiation exchange**
A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.

**3.9.11**
**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 verified, the evidence itself, and the non-repudiation policy in effect.

**3.9.12**
**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).

**3.9.13**
**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.

**3.9.14**
**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.

**3.9.15**
**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.

**3.9.16**
**Non-repudiation of receipt**
This service is intended to protect against a recipient's false denial of having received a message.

**3.9.17**
**Non-repudiation of sending**
This service is intended to protect against the sender's false denial of having sent a message.

**3.9.18**
**Non-repudiation of submission**
This service is intended to provide evidence that a delivery authority has accepted the message for transmission.

**3.9.19**
**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.

**3.9.20**
**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.

**3.9.21**
**Non-repudiation token**
A special type of security token as defined in ISO/IEC 10181-1 consisting of evidence, and, optionally, of additional data.