INTERNATIONAL STANDARD

ISO/IEC 13888-2

First edition
1998-04-01

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

Reference number
ISO/IEC 13888-2:1998(E)

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 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

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