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