INTERNATIONAL STANDARD

ISO/IEC 13888-1

Third edition
2009-07-15

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 13888-1:2009(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 13888-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 13888-1:2004), which has been technically revised.

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 a 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 defines a model for non-repudiation mechanisms providing evidence based on cryptographic check values generated using symmetric or asymmetric cryptographic techniques.

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.

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, additional data:

- Secure envelopes are generated by an evidence generating authority using symmetric cryptographic techniques.

- Digital signatures are generated by an evidence generator or an evidence generating authority using asymmetric techniques.

Non-repudiation tokens can be stored as non-repudiation information that can 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, for example:

- 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.

Specific 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.

Additional non-repudiation services mentioned in this part of ISO/IEC 13888 are:

- non-repudiation of creation,

- non-repudiation of receipt,

- non-repudiation of knowledge,

- non-repudiation of sending.

Information technology — 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. 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 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 10181-4:1997, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework*

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