INTERNATIONAL STANDARD

ISO/IEC 13888-3

Third edition
2020-09

Information security — Non-repudiation —

Part 3: Mechanisms using asymmetric techniques

Sécurité de l'information — Non-répudiation —

Partie 3: Mécanismes utilisant des techniques asymétriques

Reference number
ISO/IEC 13888-3:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols ... **2**
5 Requirements ... **3**
6 Trusted third party involvement ... **3**
7 Digital signatures ... **4**
8 Use of non-repudiation tokens with and without delivery authorities ... **4**
9 Evidence produced by the end entities ... **5**
9.1 General ... 5
9.2 Non-repudiation of origin ... 5
9.2.1 Non-repudiation of origin token ... 5
9.2.2 Mechanism for non-repudiation of origin ... 6
9.3 Non-repudiation of delivery ... 6
9.3.1 Non-repudiation of delivery token ... 6
9.3.2 Mechanism for non-repudiation for delivery ... 7
10 Evidence produced by a delivery authority ... **8**
10.1 General ... 8
10.2 Non-repudiation of submission ... 8
10.2.1 Non-repudiation of submission token ... 8
10.2.2 Mechanism for non-repudiation of submission ... 9
10.3 Non-repudiation of transport ... 9
10.3.1 Non-repudiation of transport token ... 9
10.3.2 Mechanism for non-repudiation of transport ... 10
11 Mechanisms to ensure that an NRT was signed before a time *t* ... **11**
11.1 General ... 11
11.2 Mechanism using a time-stamping service ... 11
11.3 Mechanism using a time-marking service ... 11
Bibliography ... **13**

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 13888-3:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

— Clause 3 has been clarified;

— the terminology and notation issues have been fixed;

— a requirement has been changed into a recommendation in Clause 7; and

— a new requirement has been introduced in Clause 5.

A list of all parts in the ISO/IEC 13888 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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.

Such evidence can be produced either directly by an end entity or by a trusted third party.

This document only addresses the following non-repudiation services:

— non-repudiation of origin;

— non-repudiation of delivery;

— non-repudiation of submission;

— non-repudiation of transport.

Non-repudiation mechanisms involve the exchange of non-repudiation tokens specific for each non-repudiation service. The non-repudiation mechanisms defined in this document 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 takes 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 security — Non-repudiation —

Part 3:
Mechanisms using asymmetric techniques

1 Scope

This document specifies mechanisms for the provision of specific, communication-related, non-repudiation services using asymmetric cryptographic techniques.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

ISO/IEC 13888-1, *Information technology — Security techniques — Non-repudiation — Part 1: General*

ISO/IEC 14888 (all parts), *IT Security techniques — Digital signatures with appendix*

ISO/IEC 18014-1, *Information technology — Security techniques — Time-stamping services — Part 1: Framework*

ISO/IEC 29192-4, *Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 13888-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
time-marking service
service providing evidence that a hash code together with an identifier of a hash-function have been recorded before a certain point in time

3.2
time-stamping service
service providing evidence that a data item existed before a certain point in time