

IT security techniques — Non-repudiation —

Part 1: General

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 13888-1:2004 and implements it as the UK national standard. It supersedes BS ISO/IEC 13888-1:1997 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/133, IT — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to vi, pages 1 to 15 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 18 June 2004

© BSI 18 June 2004

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)



AVA Documents
Document Sharing Hub

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
3.1 Definitions from ISO 7498-2.....	2
3.2 Definitions from ISO/IEC 9594-8.....	2
3.3 Definitions from ISO/IEC 9797-1.....	2
3.4 Definitions from ISO/IEC 10118-1.....	2
3.5 Definitions from ISO/IEC 10181-1.....	2
3.6 Definitions from ISO/IEC 10181-4.....	3
3.7 Definitions from ISO/IEC 11770-3.....	3
3.8 Definitions from ISO/IEC 18014.....	4
3.9 Definitions unique to this International Standard on non-repudiation	4
4 Symbols (and abbreviated terms).....	7
5 Organisation of the remaining part of this part of the International Standard.....	8
6 Requirements.....	8
7 Generic non-repudiation services	8
7.1 Entities involved in the provision and verification of evidence.....	8
7.2 Non-repudiation services.....	9
8 Trusted third party involvement.....	9
8.1 Evidence generation phase	9
8.2 Evidence transfer, storage and retrieval phase	10
8.3 Evidence verification phase	10
9 Evidence generation and verification mechanisms.....	10
9.1 Secure envelopes	10
9.2 Digital signatures.....	11
9.3 Evidence verification mechanism.....	11
10 Non-repudiation tokens	11
10.1 Generic non-repudiation token	11
10.2 Time-stamping token.....	12
10.3 Notarization token	12
11 Specific non-repudiation services	13
11.1 Non-repudiation of origin.....	13
11.2 Non-repudiation of delivery	13
11.3 Non-repudiation of submission	13
11.4 Non-repudiation of transport.....	14
12 Use of specific non-repudiation tokens in a messaging environment	14

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.

