



中华人民共和国国家标准

GB/T 17903.1—2024

代替 GB/T 17903.1—2008

信息技术 安全技术 抗抵赖 第 1 部分:概述

Information technology—Security techniques—Non-repudiation—
Part 1: General

(ISO/IEC 13888-1:2020, Information security—
Non-repudiation—Part 1: General, MOD)

2024-03-15发布

2024-10-01实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
引言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	6
4.1 符号	6
4.2 缩略语	7
5 概述	7
6 要求	8
7 通用抗抵赖服务	8
7.1 抗抵赖服务概述	8
7.2 证据提供与验证过程中涉及的实体	8
8 可信第三方	9
8.1 概述	9
8.2 证据生成阶段	9
8.3 证据传输、存储和检索阶段	10
8.4 证据验证阶段	10
9 证据生成与验证机制	10
9.1 规则	10
9.2 安全信封	10
9.3 数字签名	11
9.4 证据验证机制	11
10 抗抵赖令牌	11
10.1 通用要求	11
10.2 通用抗抵赖令牌	12

10.3	时间戳令牌	12
10.4	公证令牌	12
11	特定的抗抵赖服务	13
11.1	概述	13
11.2	原发抗抵赖	14
11.3	交付抗抵赖	14
11.4	提交抗抵赖	14

11.5 传输抗抵赖	14
12 消息传输环境中特定抗抵赖令牌的使用	15
参考文献	16

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 17903《信息技术 安全技术 抗抵赖》的第1部分。GB/T 17903已经发布了以下部分：

- 第1部分：概述；
- 第2部分：采用对称技术的机制；
- 第3部分：采用非对称技术的机制。

本文件代替 GB/T 17903.1—2008《信息技术 安全技术 抗抵赖 第1部分：概述》。与 GB/T 17903.1—2008相比，除编辑性改动外，主要技术变化如下：

- a) 增加了对于杂凑函数的要求(见第6章,2008版的第6章)
- b) 更改了對抗抵赖服务的表述(见7.1、7.2,2008版的7.1、7.2)。

本文件修改采用 ISO/IEC 13888-1:2020《信息安全 抗抵赖 第1部分：概述》。

本文件与 ISO/IEC 13888-1:2020的技术差异及其原因如下：

- a) 用规范性引用的 GB/T 20520替换了 ISO/IEC 18014(所有部分)(见10.3),以适应我国的技术条件；
- b) 增加了规范性引用的 GB/T 25069,并使用 GB/T 25069中的术语定义替代了部分原有术语的定义(见第3章),以适应我国的技术条件；
- c) 删除了 ISO/IEC 13888-1:2020 中第4章的缩略语“TA”,此缩略语在正文未引用；
- d) 删除了 ISO/IEC 13888-1:2020 中第5章的“文档结构”,增加了“概述”,以使本文件符合国家标准的结构惯例；
- e) 修改了對抗碰撞杂凑函数的要求(见第6章),以适应我国的技术条件。

本文件做了下列编辑性改动：

- a) 为了与现有标准协调一致,将标准名称更改为《信息技术 安全技术 抗抵赖 第1部分：概述》；
- b) 调整了术语的排列顺序,将按英语字母顺序排列更改为按术语间关系排列(见第3章)；
- c) 用资料性引用的 GB/T 17903(所有部分)替换了 ISO/IEC 13888(所有部分)(见第6章)；
- d) 删除了 ISO/IEC 13888-1:2020 中 9.1 资料性引用的 ISO/IEC 14888(所有部分)；

e) 用资料性引用的 GB/T 15852(所有部分)替换了 ISO/IEC9797(所有部分)(见 9.2) ;

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要
下载或阅读全文，请访问：

<https://d.book118.com/967200154036006136>