ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17903.2—2021
代替 GB/T 17903.2—2008

信息技术　安全技术　抗抵赖 第2部分：采用对称技术的机制

Information technology—Security techniques—Non-repudiation—Part 2：Mechanisms using symmetric techniques

（ISO/IEC 13888-2：2010 MOD）

2021-10-11 发布　　2022-05-01 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

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2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 17903.2—2008《信息技术　安全技术　抗抵赖　第2部分：采用对称技术的机制》。与GB/T 17903.2—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了第5章 符号；

b) 删除了原第6章 本文件各章的组织；

c) 增加了9.1 抗抵赖机制；

d) 增加了图1和图2；

e) 删除了原9.3和9.4中的技术内容；

f) 将原第10章的技术内容移至附录A中。

本文件使用重新起草法修改采用ISO/IEC 13888-2:2010《信息技术　安全技术　抗抵赖　第2部分：采用对称技术的机制》。

本文件与ISO/IEC 13888-2:2010的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用等同采用国际标准的GB/T 17903.1代替了ISO/IEC 13888-1。
- 删除了规范性引用文件ISO/IEC 9798-1:1997和ISO/IEC 10118(所有部分)，这些规范性引用文件仅在术语中作为来源引用。
- 增加了规范性引用文件GB/T 15852，GB/T 15852规定了消息鉴别码算法，是本文件中应用的重要密码算法。
- 增加了规范性引用文件GB/T 20520和GB/T 25069。

——增加了图1和图2，以帮助理解第9章的技术内容。

——删除了部分与GB/T 25069重复的通用术语，改为在第3章引用GB/T 25069的形式。

本文件做了下列编辑性修改：

——纳入了ISO/IEC 13888-2:2010/Cor.1:2012的技术勘误，所涉及的条款的外侧页边空白位置用垂直双线(‖)进行了标示。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院软件研究所、网神信息技术(北京)股份有限公司、中国科学院数据与通信保护研究教育中心、联想(北京)有限公司、上海格尔软件股份有限公司。

本文件主要起草人：张严、张振峰、张立武、黄亮、李敏、李汝鑫、郑强、李俊、蔡冉。

本文件及其所代替文件的历次版本发布情况为：

——2008年首次发布为GB/T 17903.2—2008；

——本次为第一次修订。

引　言

GB/T 17903 旨在对抗抵赖服务的通用模型以及特定的抗抵赖机制进行规范，抗抵赖服务通过生成、收集、维护、利用和验证有关已声称事件或动作的证据，以解决有关该事件或动作已发生或未发生的争议，由三个部分构成。

——第 1 部分：概述。目的在于规定抗抵赖服务的通用模型。

——第 2 部分：采用对称技术的机制。目的在于规定若干特定的、采用对称技术的抗抵赖机制。

——第 3 部分：采用非对称技术的机制。目的在于规定若干特定的、采用非对称技术的抗抵赖机制。

信息技术　安全技术　抗抵赖
第2部分:采用对称技术的机制

1　范围

本文件确立了抗抵赖服务的通用结构,以及若干特定的抗抵赖机制,用于提供原发抗抵赖(NRO)与交付抗抵赖(NRD)。

本文件适用于采用对称技术实现的消息抗抵赖相关应用的设计、实现与测试。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 15852(所有部分)　信息技术　安全技术　消息鉴别码[ISO/IEC 9797(所有部分)]

GB/T 17903.1　信息技术　安全技术　抗抵赖　第1部分:概述(GB/T 17903.1—2008,ISO/IEC 13888-1:2004,IDT)

GB/T 20520　信息安全技术　公钥基础设施　时间戳规范

GB/T 25069　信息安全技术　术语

3　术语和定义

GB/T 17903.1 和 GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

密码校验函数　cryptographic check function

以秘密密钥和任意字符串作为输入,并以密码校验值作为输出的密码变换。不知道秘密密钥就不可能正确计算校验值。

3.2

数据完整性　data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

3.3

证据生成者　evidence generator

产生抗抵赖证据的实体。

3.4

杂凑函数　hash-function

将任意长比特串映射为定长比特串的函数,满足如下属性:

——给定一个输出比特串,寻找一个输入比特串来产生这个输出比特串,在计算上是不可行的;

——给定一个输入比特串,寻找另一个不同的输入比特串来产生相同的输出比特串,在计算上是不可行的。

注1:计算上的可行性取决于特定安全要求和环境。