ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17903.3—2024
代替 GB/T 17903.3—2008

信息技术　安全技术　抗抵赖 第3部分：采用非对称技术的机制

Information technology—Security techniques—Non-repudiation—Part 3：Mechanisms using asymmetric techniques

（ISO/IEC 13888-3：2020，Information security—Non-repudiation—Part 3：Mechanisms using asymmetric techniques，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

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3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 17903.3—2008《信息技术　安全技术　抗抵赖　第3部分：采用非对称技术的机制》。与GB/T 17903.3—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了关于数字签名的安全性要求(见第5章)；

b) 增加了时间保证机制(见第11章)。

本文件修改采用ISO/IEC 13888-3:2020《信息安全　抗抵赖　第3部分：采用非对称技术的机制》。

本文件与ISO/IEC 13888-3:2020的技术差异及其原因如下：

a) 增加了规范性引用的GB/T 20520(见第3章)，引用了此标准的术语；

b) 删除了ISO/IEC 13888-3:2020的第3章定义“3.2　时间戳服务”，此术语已在规范性引用的GB/T 20520中给出了定义；

c) 用规范性引用的GB/T 17903.1替换了ISO/IEC 13888-1(见第3章、第4章)，以适应我国的技术条件；

d) 修改了对抗碰撞杂凑函数的要求，以适应我国的技术条件(见第5章)；

e) 用规范性引用的GB/T 15851(所有部分)替换了ISO/IEC 9796(所有部分)，以及用规范性引用的GB/T 17902(所有部分)替换了ISO/IEC 14888(所有部分)(见第7章)，以适应我国的技术条件；

f) 用规范性引用的GB/T 20520替换了ISO/IEC 18014(所有部分)(见11.2)，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3部分：采用非对称技术的机制》；

b) 删除了ISO/IEC 13888-3:2020中资料性引用的ISO/IEC 10118(所有部分)；

c) 用资料性引用的GB/T 16264.8—2005替换了ISO/IEC 9594-8(见第6章)。

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。

本文件由全国网络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、长春吉大正元信息技术股份有限公司、北京中关村实验室、中国科学院大学、中电科网络安全科技股份有限公司、中国电子技术标准化研究院、奇安信科技集团股份有限公司、国民认证科技(北京)有限公司、格尔软件股份有限公司、北京信安世纪科技有限公司、西安西电捷通无线网络通信股份有限公司。

本文件主要起草人：张严、张立武、张振峰、冯登国、张妍、王蕊、刘丽敏、殷其雷、张立廷、林阳荟晨、张宝欣、黄亮、汪宗斌、郑强、李俊、李汝鑫、杜志强、杨领波、钱维、王现方。

本文件及其所代替文件的历次版本发布情况为：

——1999年首次发布为GB/T 17903.3—1999；

——2008年第一次修订；

——本次为第二次修订。

引　言

抗抵赖服务旨在生成、收集、维护、利用和验证有关已声称的事件或动作的证据，以解决关于此事件或动作的已发生或未发生的争议。GB/T 17903 旨在描述抗抵赖机制的模型及采用对称密码技术和非对称密码技术的具体抗抵赖机制。拟由三个部分构成。

——第 1 部分：概述。目的在于给出抗抵赖机制的一般模型，作为 GB/T 17903 的其他部分中规定的使用密码技术的抗抵赖机制的一般模型。

——第 2 部分：采用对称技术的机制。目的在于给出采用对称密码技术的具体抗抵赖机制。

——第 3 部分：采用非对称技术的机制。目的在于给出采用非对称密码技术的具体抗抵赖机制。

信息技术　安全技术　抗抵赖
第3部分：采用非对称技术的机制

1　范围

本文件确立了若干特定的抗抵赖机制，用于提供原发抗抵赖、交付抗抵赖、传输抗抵赖和提交抗抵赖。

本文件适用于采用非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 15851（所有部分）　信息技术　安全技术　带消息恢复的数字签名方案［ISO/IEC 9796（所有部分）］

注1：GB/T 15851.3—2018　信息技术　安全技术　带消息恢复的数字签名方案　第3部分：基于离散对数的机制（ISO/IEC 9796-3：2006，MOD）

GB/T 17902（所有部分）　信息技术　安全技术　带附录的数字签名［ISO/IEC 14888（所有部分）］

注2：GB/T 17902.1—2023　信息技术　安全技术　带附录的数字签名　第1部分：概述（ISO/IEC 14888-1：2008，IDT）

GB/T 17902.2—2023　信息技术　安全技术　带附录的数字签名　第2部分：基于身份的机制（ISO/IEC 14888-2：1999，IDT）

GB/T 17902.3—2023　信息技术　安全技术　带附录的数字签名　第3部分：基于证书的机制（ISO/IEC 14888-3：1998，IDT）

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—2024，ISO/IEC 13888-1：2020，MOD）

GB/T 20520　网络安全技术　公钥基础设施　时间戳规范

ISO/IEC 29192-4　信息技术　安全技术　轻量级密码学　第4部分：使用非对称技术的机制（Information technology—Security techniques—Lightweight cryptography—Part 4：Mechanisms using asymmetric techniques）

3　术语和定义

GB/T 17903.1 及 GB/T 20520 界定的以及下列术语和定义适用于本文件。

3.1

时间公证服务　time-marking service

提供用于证明某条记录发生早于特定时间点的证据的服务。

注：该证据包含一个杂凑码以及所使用的杂凑函数的标识符。