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—Securitytechniques—Non-repudiation—
Part3:Mechanismsusing asymmetrictechniques

(ISO/IEC 13888-3:2020,Information security—Non-repudiation—
Part3:Mechanismsusing asymmetrictechniques,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 ..... Ⅰ
引言 ..... Ⅱ
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　符号 1
5　要求 2
6　可信第三方的参与 2
7　数字签名 3
8　抗抵赖令牌 3
9　由终端实体生成证据的机制 4
9.1　一般规则 4
9.2　原发抗抵赖机制 4
9.3　交付抗抵赖机制 5
10　由交付机构生成证据的机制 6
10.1　一般规则 6
10.2　提交抗抵赖机制 6
10.3　传输抗抵赖机制 7
11　时间保证机制 8
11.1　一般规则 8
11.2　采用时间戳的机制 9
11.3　采用时间公证服务的机制 9
参考文献 10

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/T17903《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/IEC14888(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/IEC9594-8(见第 6章) 。