ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17902.1—2023/ISO/IEC 14888-1:2008
代替 GB/T 17902.1—1999

信息技术　安全技术　带附录的数字签名　第1部分:概述

Information technology—Security techniques—Digital signatures with appendix—Part 1:General

（ISO/IEC 14888-1:2008,IDT）

2023-03-17 发布　　2023-10-01 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 17902《信息技术　安全技术　带附录的数字签名》的第1部分。GB/T 17902已经发布了以下部分:

——第1部分:概述;

——第2部分:基于身份的机制;

——第3部分:基于证书的机制。

本文件代替GB/T 17902.1—1999《信息技术　安全技术　带附录的数字签名　第1部分:概述》,与GB/T 17902.1—1999相比,除结构调整和编辑性改动外,主要技术变化如下:

——将原“概述”部分调整至第5章(见第5章,1999年版的第3章);

——删除了“赋值”“无碰撞散列函数”“确定性的”“散列权标”“散列代码”“预签名”“随机化”“随机值”“签名方程”“签名函数”及“赋值”等术语(见1999年版的第4章),增加了“抗碰撞杂凑函数”“数据元”“域”“杂凑码”“密钥对”及“消息”等术语(见第3章);

——删除了“重新计算的散列权标”“准备好的部分消息”“赋值”“预签名”“重新计算的预签名”等符号以及“比较”的图例(见1999年版的第5章),增加了“可选数据”的图例(见4.3),并增加了“惯例”内容(见4.2);

——增加了“签名机制和杂凑函数的绑定选项”一章,描述了签名机制和杂凑函数绑定的几类选项(见第7章);

——将签名过程内容合并至第9章,并用通用模型,统一描述现有机制,较原内容更具有普适性(见第9章,1999年版的第8章、第9章);

——将验证过程合并至第10章,并更新了通用模型描述现有机制,较原内容更具有普适性(见第10章,1999年版的第9章)。

本文件等同采用ISO/IEC 14888-1:2008《信息技术　安全技术　带附录的数字签名　第1部分:概述》。

本文件做了下列最小限度的编辑性改动:

——第10章验证签名部分增加了注,便于理解。

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、成都卫士通信息产业股份有限公司、北京数字认证股份有限公司、中国电子技术标准化研究院、中国信息通信研究院。

本文件主要起草人:张振峰、何双羽、张严、白琨鹏、郝春亮、张立廷、王现方、傅大鹏、王惠莅、王榕。

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 17902.1—1999;

——本次为第一次修订。

引　言

数字签名机制是一类非对称密码机制，被广泛用于实体鉴别、数据来源鉴别、数据完整性和抗抵赖服务。有两种数字签名机制：

——若在验证过程中，需要消息作为输入的一部分，则此类机制称为“带附录的数字签名”，附录计算需要使用杂凑函数；

——若在验证过程中，披露全部或是部分消息，则此类机制称为“带消息恢复的数字签名”，签名生成和验证也会使用到杂凑函数。

带附录的数字签名在GB/T 17902中进行了规范，带消息恢复的数字签名在ISO 10118中进行了规范，杂凑函数则是在GB/T 18238(所有部分)中进行了规范。

GB/T 17902《信息技术　安全技术　带附录的数字签名》由三个部分组成。

——第1部分：概述。目的在于规范通用的带附录数字签名的整体框架和通用模型。

——第2部分：基于身份的机制。目的在于规范基于身份的带附录数字签名机制。

——第3部分：基于证书的机制。目的在于规范基于证书的数字签名机制。

信息技术　安全技术　带附录的数字签名
第1部分:概述

1　范围

GB/T 17902规定了几种对任意长度消息进行签名的带附录的数字签名机制。

本文件包括带附录的数字签名的一般原理与要求,同时也包括GB/T 17902各部分用到的定义与符号。

证书和密钥管理等相关技术不在本文件的规范范围内。更多此类信息见GB/T 16264.8—2005[2],ISO/IEC 11770-3[8]以及ISO/IEC 15945:2002[9]。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

附录　appendix

由签名和一个可选文本字段构成的比特串。

3.2

抗碰撞杂凑函数　collision-resistant hash-function

抗碰撞散列函数

满足如下性质的杂凑函数:找出映射到同一输出的任何两个不同输入在计算上不可行。

注:计算是否可行依赖于具体的安全需求和环境。

[来源:ISO/IEC 10118-1:2016,3.1]

3.3

数据元　data element

整数、比特串、整数集合或比特串集合。

3.4

域　domain

在单一安全策略下运行的一组实体。

示例:由单一机构或一组采用同一安全策略的机构创建的公钥证书。

3.5

域参数　domain parameter

对域中所有实体都是公共的且已知或可访问的数据元。