ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 15843.3—2023/ISO/IEC 9798-3:2019
代替 GB/T 15843.3—2016

信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制

Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques

（ISO/IEC 9798-3:2019,IT Security techniques—Entity authentication—Part 3:Mechanisms using digital signature techniques,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 15843《信息技术　安全技术　实体鉴别》的第3部分。GB/T 15843已经发布了以下部分:

——第1部分:总则;

——第2部分:采用对称加密算法的机制;

——第3部分:采用数字签名技术的机制;

——第4部分:采用密码校验函数的机制;

——第5部分:使用零知识技术的机制;

——第6部分:采用人工数据传递的机制。

本文件代替GB/T 15843.3—2016《信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制》,与GB/T 15843.3—2016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“符号与缩略语”(见第4章);

b) 增加了“通则”(见第5章);

c) 增加了“单向鉴别”(见8.2);

d) 增加了“七次传递鉴别”(见8.3.4);

e) 增加了“使用指南”(见附录B)。

本文件等同采用ISO/IEC 9798-3:2019《IT安全技术　实体鉴别　第3部分:采用数字签名技术的机制》。

本文件做了下列最小限度的编辑性改动:

——为与我国技术标准体系协调,将标准名称改为《信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制》;

——为符合我国技术表达习惯,将TP(第三方)统一改为TTP(可信第三方);

——为方便理解,分别在5.1、8.1、8.2.1增加了资料性说明的注。

本文件由全国信息安全标准化技术委员会(SAC/TC260)提出并归口。

本文件起草单位:西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、国家信息技术安全研究中心、中国移动通信集团有限公司、中能融合智慧科技有限公司、中国南方电网有限责任公司、北京数字认证股份有限公司、中国科学院软件研究所、公安部第一研究所、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、广西大学、中国广播电视网络集团有限公司、广西诚新慧创科技有限公司、格尔软件股份有限公司、广西通量能源技术有限公司、中国通用技术研究院、北京计算机技术及应用研究所。

本文件主要起草人:曹军、杜志强、张璐璐、王宏、陈宇、李琴、黄振海、王月辉、张变玲、铁满霞、张阳、王力、侯鹏亮、胡霄亮、郑骊、沙学松、赖晓龙、赵晓荣、颜湘、张国强、陈宝仁、张立武、张严、蒋才平、简练、周涛、李冬、李国友、陶洪波、尹玉昂、罗鹏、邓开勇、卢泉、李爽、韦利娜、郑强、韦昌才、刘科伟、于光明、王锐、李玉娇、朱正美、赵慧、贾嘉、刘鸿运、何双羽、李楠、井经涛、潘琪、陈维刚、白琨鹏、张芝军、孙硕、陈晓龙、芦亮、郭金发、田玉存。

本文件及其所代替文件的历次版本发布情况为:

——1998年首次发布为GB/T 15843.3—1998,2008年第一次修订,2016年第二次修订;

——本次为第三次修订。

引　言

本文件规定采用数字签名技术的实体鉴别机制，分为单向鉴别和双向鉴别两类。其中单向鉴别按照消息传递的次数，分为一次传递鉴别、两次传递鉴别和四次传递鉴别；双向鉴别根据消息传递的次数，分为两次传递鉴别、三次传递鉴别、五次传递鉴别和七次传递鉴别。

GB/T 15843 旨在规范实体鉴别技术，由 6 部分组成。

——第 1 部分：总则。目的在于规范实体鉴别技术的模型、框架以及通用要求。

——第 2 部分：采用对称加密算法的机制。目的在于规范六种基于对称加密算法的实体鉴别机制及关要求。

——第 3 部分：采用数字签名技术的机制。目的在于规范十种基于数字签名技术的实体鉴别机制及相关要求。

——第 4 部分：采用密码校验函数的机制。目的在于规范四种基于密码校验函数的实体鉴别机制及相关要求。

——第 5 部分：使用零知识技术的机制。目的在于规范五种基于零知识技术的实体鉴别机制及相关要求。

——第 6 部分：采用人工数据传递的机制。目的在于规范八种基于人工数据传递的实体鉴别机制及相关要求。

由于签名所使用的证书分发方式超出本文件范围，证书的发送在所有机制中是可选的。

本文件的发布机构提请注意，声明符合本文件时，可能涉及与第 8 章相关的 CN201510654832.X、US10，652，029B2、JP6543768B2、EP16853050.9、KR10-2107918、CN200910024191.4、US8，751，792B2、JP5425314B2、EP2472772、KR10-1405509、CN200910023774.5、CN200910023735.5、US8，763，100B2、JP5468138B2、KR10-1471259、CN200910023734.0、US8，732，464B2、JP5468137B2、KR10-1471827、CN200810150949.4、CN200810150951.1、CN200710199241.3、US8，417，955B2、JP5323857B2、KR10-1139547、RU2445741C2、CN200710018920.6、US8，356，179B2、EP2214429B1、JP5099568B2、KR10-1117393、RU2458481C2、CN201510654785.9、US10，615，978B2、JP6687728、EP16853041.8、KR10-2141289、CN201510654784.4 等专利的使用。

本文件的发布机构对于上述专利的真实性、有效性和范围无任何立场。

上述专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。上述专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：王丽珍

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

信息技术　安全技术　实体鉴别
第3部分:采用数字签名技术的机制

1　范围

本文件规定了两类采用数字签名技术的实体鉴别机制。第一类不引入在线可信第三方,包括两种单向鉴别机制和三种双向鉴别机制;第二类引入在线可信第三方,也包括两种单向鉴别机制和三种双向鉴别机制。

本文件适用于指导采用数字签名技术的实体鉴别机制的研究,以及相关产品和系统的研发与应用。

附录A定义了本文件规范的实体鉴别机制的对象标识符。

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 15843.1—2017　信息技术　安全技术　实体鉴别　第1部分:总则(ISO/IEC 9798-1:2010,IDT)

ISO/IEC 9796(所有部分)　信息技术　安全技术　带消息恢复的数字签名方案(Information technology—Security techniques—Digital signature schemes giving message recovery)

注: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)

ISO/IEC 14888(所有部分)　信息技术　安全技术　带附录的数字签名(Information technology—Security techniques—Digital signatures with appendix)

注:GB/T 17902.2—2005　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—2005　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)

3　术语和定义

下列术语和定义适用于本文件。

3.1

原子性业务　atomic transaction

不能再进一步拆分为多个更小业务的业务。

3.2

声称方　claimant

被鉴别的实体本身或者为了实现验证目标的某代表性实体。

注:声称方拥有鉴别交换时所需的参数和私有数据。

[来源:GB/T 15843.1—2017,3.6]