ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.1—2017/ISO/IEC 9798-1:2010
代替 GB/T 15843.1—2008

信息技术　安全技术　实体鉴别
第1部分:总则

Information technology—Security techniques—Entity authentication—Part 1:General

(ISO/IEC 9798-1:2010,IDT)

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 15843《信息技术　安全技术　实体鉴别》分为六个部分：

——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：采用零知识技术的机制；

——第6部分：采用人工数据传递的机制。

本部分为GB/T 15843的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 15843.1—2008《信息技术　安全技术　实体鉴别　第1部分：概述》，与GB/T 15843.1—2008相比，主要变化如下：

——将标准名称改为《信息技术　安全技术　实体鉴别　第1部分：总则》；

——前言增加了GB/T 15843的第6部分；

——修改了术语“非对称加密方法”“非对称签名方法”“挑战”“解密”“加密”“主体”“私有解密密钥”“对称加密算法”“令牌”的定义；

——增加了附录B的B.1内容，原有章条序号依次后移。

本部分使用翻译法等同采用ISO/IEC 9798-1:2010《信息技术　安全技术　实体鉴别　第1部分：总则》。

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这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分主要起草单位：中国科学院数据与通信保护研究教育中心、普华诚信信息技术有限公司。

本部分主要起草人：王雷、查达仁、向继、沈嘉荟、李丹仪、荆继武、郭晓博、谢超。

本部分所代替标准的历次版本发布情况为：

——GB/T 15843.1—1995、GB/T 15843.1—1999、GB/T 15843.1—2008。

引　言

在实时通信系统中，实体鉴别是一项重要的基础安全服务。针对特定应用与安全目标，实体鉴别机制即可通过一次传输协议来实现单向鉴别，又可通过多次传递协议完成通信实体间的单向或双向鉴别。

实体鉴别机制的目的是证实某一身份的声称方是否为其所声称的实体。在密码学上，该目标的实现基于一个能够将实体身份与公开密钥关联起来的基础设施(如，公钥基础设施 PKI)，但是该类基础设施的建立并不属于 GB/T 15843 的内容范围。

实体鉴别机制拥有两种主要模型，一种模型是通过声称方与验证方的直接通信确认声称方身份；另一种模型是通过可信第三方来证实声称方身份。

GB/T 15843 详细说明了实体鉴别机制中不同种类的实体鉴别协议。实体鉴别协议的选择基于系统的安全特性，包括以下几点：

——是否抗重放攻击；

——是否抗反射攻击；

——是否抗暴力延迟；

——单向或双向鉴别；

——是否存在预设的秘密信息可以使用，或者是否需要可信第三方帮助建立共享秘密信息。

例如，不关注重放攻击的特定系统，声称方与验证方之间仅需简单的传输协议即可实现实体鉴别；而可能发生中间人攻击或重放攻击的复杂通信系统，则需要某个多次传输协议来确保安全。

信息技术　安全技术　实体鉴别
第1部分:总则

1　范围

GB/T 15843的本部分详细指明了实体鉴别机制中的鉴别模型和一般性约束要求,并基于此验证实体身份真实性,待鉴别的实体通过展示某个私密信息来证明身份。实体鉴别机制确定了如何进行实体间的信息交换,以及实体与可信第三方的信息交换。

实体鉴别机制的细节和鉴别交换的内容不属于本部分标准内容,在GB/T 15843的其他部分中规定。

2　规范性引用文件

本部分不使用任何规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

非对称密码技术　asymmetric cryptographic technique

使用两种相关变换的密码技术:一种是由公开密钥定义的公开转换,另一种是由私有密钥定义的私有变换。

注:在给定公开变换的情况下,推导出私有变换在计算上是不可行的。

3.2

非对称加密方法　asymmetric encryption system

基于非对称密码技术的加密方法,其公开变换用于加密,而私有变换用于解密。

3.3

非对称密钥对　asymmetric key pair

一对相关的密钥,其中私有密钥定义私有变换,公开密钥定义公开变换。

3.4

非对称签名方法　asymmetric signature system

基于非对称密码技术的签名方法,其私有变换用于签名,而公开变换用于验证。

3.5

挑战　challenge

由验证方随机产生并发送给声称方的数据项:声称方将该数据项和其拥有的秘密信息共同产生一个响应发送给验证方。

3.6

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必需的参数和私有数据。