ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.6—2018/ISO/IEC 9798-6:2010

信息技术　安全技术　实体鉴别
第6部分:采用人工数据传递的机制

Information technology—Security techniques—Entity authentication—Part 6:Mechanisms using manual data transfer

(ISO/IEC 9798-6:2010,IDT)

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
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。

本部分为GB/T 15843的第6部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用翻译法等同采用ISO/IEC 9798-6:2010《信息技术　安全技术　实体鉴别　第6部分：采用人工数据传递的机制》。

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。

本部分起草单位：中国科学院数据与通信保护研究教育中心、北京数字认证股份有限公司、飞天诚信科技股份有限公司。

本部分主要起草人：夏鲁宁、张国柱、张琼露、林雪焰、朱鹏飞。

引　言

在日常通信中，两个设备之间经常需要通过非安全通道执行实体鉴别，但非安全通道易受主动或被动的攻击，所谓主动攻击包括恶意第三方在非安全通道执行数据插入、篡改、删除或重放等动作。

GB/T 15843的其他部分指定的鉴别机制适用于两个设备共享同一个秘密密钥，或者彼此拥有对方的非对称公钥。

GB/T 15843 的本部分所述的实体鉴别机制无需假定双方预先建立共享密钥关系，而是使用人工手段进行鉴别，即实体鉴别通过从一个设备到另一个设备人工传递短数据串来实现，或通过人工对比两个设备输出的短数据串是否一致来实现。

在本部分中，“实体鉴别”这个术语的含义与其他部分有所不同，鉴别涉及的两个设备都由同一个用户持有，或由两个彼此之间存在可信通信途径的不同用户持有，用户验证两个设备在执行了本部分的鉴别机制后是否成功共享了数据串。当然，数据串可以包含两个设备或其中一个设备的标识符。

如资料性附录 B 和附录 C 所描述的那样，人工鉴别机制可作为建立秘密密钥共享或可靠交换公钥的基础。此外，人工鉴别机制还可被用作其他秘密或公开安全参数的交换，包括安全策略声明或时间戳等。

本部分凡涉及密码算法的相关内容，按国家有关法规实施；凡涉及到采用密码技术解决保密性、完整性、真实性、不可否认性需求的按密码相关国家标准和行业标准实施。

信息技术　安全技术　实体鉴别
第6部分:采用人工数据传递的机制

1　范围

GB/T 15843的本部分规定了在设备之间基于人工数据传递进行实体鉴别的8种机制。本部分指明了这些机制如何被用来支持密钥管理功能,以及如何安全地选择各机制的参数。对于这8种机制,本部分给出了其ASN.1定义,并对它们的安全性水平和效率进行了分析比较。

这些机制可以适用于多类应用场景。一种典型的应用是在个人网络中,作为设备接入网络的过程的一部分,用户对于自己掌握的两个具备无线通信能力的设备执行二者相互间的实体鉴别。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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)

3　术语和定义

GB/T 15843.1—2017界定的以及下列术语和定义适用于本文件。

3.1

检验值　check-value

一个比特串,由某种检验函数计算产生,从通信的发起方传递给通信的接收方,且接收方有能力检验其正确性。

3.2

检验函数　check-value function

函数f,将一个比特串和一个短密钥映射为一个定长为b位的检验值,短密钥可容易地被输入到用户设备或从中读取。检验函数满足以下属性:

——对于任何密钥k和任何比特串d,函数$f(d,k)$可以被有效计算;

——寻找两个不同的比特串d和d',使得对于密钥k有$f(d,k)=f(d',k)$,在计算上是不可行的,尽管能够满足上述等式的k值在k的取值空间中并不是一小部分。

注:在实践中,一个典型的短密钥包含4～6个数字或字母。

3.3

数据起源鉴别　data origin authentication

对于接收到的数据,确认其来源的真实性。

[ISO 7498-2]

3.4

摘要值　digest-value

一个比特串,由某种摘要函数计算产生,从通信的发起方传递给通信的接收方,且接收方有能力检