ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.1—2008/ISO/IEC 9798-1:1997
代替 GB/T 15843.1—1999

信息技术　安全技术　实体鉴别
第1部分:概述

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

(ISO/IEC 9798-1:1997,IDT)

2008-06-19 发布　　2008-11-01 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》分为五个部分：

——第1部分：概述

——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

可能还会增加其他后续部分。

本部分为GB/T 15843的第1部分，等同采用ISO/IEC 9798-1:1997《信息技术　安全技术　实体鉴别　第1部分：概述》(英文版)，仅有编辑性修改。

本部分代替GB/T 15843.1—1999《信息技术　安全技术　实体鉴别　第1部分：概述》。本部分与GB 15843.1—1999相比，主要变化如下：

——本部分标准修订了第3章中的部分术语、定义和记法。

——本部分对第6章“一般要求和约束”中的部分叙述进行了文字修订。

——本部分删除了ISO/IEC前言，增加了引言。

——本部分删除了原附录D，增加了参考文献。

本部分的附录A、附录B和附录C均为资料性附录。

本部分由全国信息安全标准化技术委员会提出并归口。

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(信息安全国家重点实验室)。

本部分主要起草人：荆继武、向继、高能、夏鲁宁。

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。

引　言

本部分等同采用国际标准 ISO/IEC 9798-1:1997,它是由 ISO/IEC 联合技术委员会 JTC1(信息技术)的分委员会 SC 27(IT 安全技术)起草的。

本部分给出了 GB/T 15843 的所有部分中使用的术语和符号,并给出了它们的定义。

本部分给出了实体鉴别机制的一般模型,各种鉴别机制的细节在 GB/T 15843 后续部分中规定。本部分还给出了实体鉴别机制的一般要求和约束,各种鉴别机制的具体要求分别在 GB/T 15843 的其他各部分中规定。

本部分中还给出了在实体鉴别机制中使用文本字段、时变参数和证书的一般要求。

本部分凡涉及密码算法的相关内容,按国家有关法规实施。

信息技术　安全技术　实体鉴别
第1部分:概述

1　范围

本部分规定了一个鉴别模型以及采用安全技术的实体鉴别机制的一般要求和约束。这些机制用于证实某个实体就是他所声称的实体。待鉴别的实体通过表明它确实知道某个秘密来证明其身份。这些机制定义实体间的信息交换以及需要时与可信第三方的信息交换。

这些机制的细节和鉴别交换的内容未在本部分中规定,而在GB/T 15843的其他部分中规定。

GB/T 15843其他各部分规定的机制能用于帮助提供GB/T 17903中规定的抗抵赖服务。抗抵赖服务的有关内容不在GB/T 15843的范围之内。

2　规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注明日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 18794.2—2002　信息技术　开放系统互连　开放系统安全框架　第2部分:鉴别框架(idt ISO/IEC 10181-2:1996)

3　术语和定义

3.1　GB/T 9387.2中确立的下列术语和定义适用于本部分。

3.1.1

密码校验值　cryptographic check value

通过在数据单元上执行密码变换而得到的信息。

3.1.2

数字签名(签名)　digital signature (signature)

附加在数据单元上的一些数据,或是对数据单元所作的密码变换,这种数据或变换允许数据单元的接收者确认数据单元的来源和完整性,并防止数据单元被人(例如接收者)伪造。

3.1.3

冒充　masquerade

一个实体伪装成另一个实体。

3.2　GB/T 18794.2中确立的下列术语和定义适用于本部分。

3.2.1

声称方　claimant

以鉴别为目的,是本体本身或者是代表本体的实体。一个声称方包含了代表本体从事鉴别交换所必需的功能。