ICS 35.040
L 80

中华人民共和国国家标准

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

信息技术　安全技术　实体鉴别
第1部分：概述

Information technology—Security techniques—Entity authentication—Part1:General

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局　发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 实体鉴别
第 1 部 分：概 述
GB/T 15843.1—1999
*
中 国 标 准 出 版 社 出 版 发 行
北京西城区复兴门外三里河北街 16 号
邮政编码：100045
http://www.bzcbs.com
电话：63787337、63787447
2000 年 6 月第一版 2004 年 11 月电子版制作
*
书号：155066·1-16714

前　言

本标准等同采用国际标准 ISO/IEC 9798-1:1997《信息技术　安全技术　实体鉴别　第 1 部分:概述》。

本标准为实体间的信息交换规定了使用安全技术的实体鉴别机制一般模型和要求,它适合于我国使用。

本标准是对 GB 15843.1—1995 的修订。两个版本的主要差别是:更改了标准名称,增加了 25 条术语定义,增加了“文本字段的使用”和“时变参数”两个附录。

GB/T 15843 在总标题《信息技术　安全技术　实体鉴别》下,由以下几个部分组成:

——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:采用公开密钥算法的实体鉴别;

——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。

本标准的附录 A、附录 B、附录 C 和附录 D 均是提示的附录。

本标准从实施之日起,同时代替 GB 15843.1—1995。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准由中国电子技术标准化研究所、西南通信技术研究所负责起草。

本标准主要起草人:罗韧鸿、向维良、雷利民。

本标准于 1995 年 12 月首次发布,1999 年 11 月第一次修订。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制订针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 9798-1 是由联合技术委员会 ISO/IEC JTC1(信息技术)的分委员会 SC27(IT 安全技术)起草的。

该第二版对第一版(ISO/IEC 9798-1:1991)进行了技术修改,它取代第一版。

ISO/IEC 9798 在总标题《信息技术　安全技术　实体鉴别机制》下由下列部分组成:

——第 3 部分:采用公开密钥算法的实体鉴别;

ISO/IEC 9798 在总标题《信息技术　安全技术　实体鉴别》下由下列部分组成:

——第 1 部分:概述;

——第 2 部分:采用对称加密算法的机制;

——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。

注:上述第 3 部分的总标题在下一个修订版中将调整为第 1、第 2、第 4 和第 5 部分之前的总标题。

也可能还有其他部分跟随其后。

本标准的附录 A、附录 B、附录 C 和附录 D 均是提示性的附录。

中华人民共和国国家标准

信息技术　安全技术　实体鉴别
第1部分：概述

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

代替 GB 15843.1—1995

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

1　范围

本标准规定了采用安全技术的实体鉴别机制的鉴别模型及一般要求和限制。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，通过表明他确实知道某个秘密来证明其身份。这些机制定义为实体间的信息交换。若有必要，还可以同可信的第三方进行交换。

这些机制的详细情况和鉴别交换的内容未在本标准中规定，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在ISO/IEC 13888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　引用标准

下列标准所包括的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

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/IEC 7498-2:1989）

ISO/IEC 9594-8:1995　信息技术　开放系统互连　目录　第8部分：鉴别框架

ISO/IEC 10181-2:1996　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

ISO/IEC 13888-1:1997　信息技术　安全技术　抗抵赖　第1部分：概述

3　定义

3.1　GB/T 15843使用了GB/T 9387.2中定义的以下有关安全的术语：

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用以确认数据单元的来源和完整性，并保护数据，防止被人（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 15843使用了ISO/IEC 10181-2中定义的以下有关安全术语：

3.2.1　声称者　claimant

为了鉴别的目的，他是本体本身或者是代表本体的实体。一个声称者包括代表本体从事鉴别交换所

国家质量技术监督局1999-11-11批准　　2000-05-01实施