ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.4—1999
idt ISO/IEC 9798-4:1995

信息技术　安全技术　实体鉴别
第4部分:采用密码校验函数的机制

Information technology—Security techniques—Entity authentication—Part 4:Mechanisms using a cryptographic check function

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局　发布

前　言

本标准等同采用国际标准 ISO/IEC 9798-4:1995《信息技术　安全技术　实体鉴别　第 4 部分:采用密码校验函数的机制》。

本标准为实体间的信息交换规定了使用密码校验函数的实体鉴别机制,它适合于我国使用。

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。

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定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 9798-4 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。

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。

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、B、C 和 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4部分：采用密码校验函数的机制

GB/T 15843.4—1999
idt ISO/IEC 9798-4:1995

Information technology—Security techniques—Entity authentication—Part 4:Mechanisms using a cryptographic check function

1　范围

本标准规定了采用密码校验函数的实体鉴别机制。其中有两种是单个实体的鉴别(单向鉴别)，其余的是两个实体的相互鉴别。

本标准所规定的机制采用诸如时间标记、顺序号或随机数等时变参数，以防止有效的鉴别信息以后又被接受。

如果采用时间标记或顺序号，对于单向鉴别只需一次传递，而要达到相互鉴别则需两次传递。如果采用了使用随机数的询问和应答方法，单向鉴别需两次传递，而达到相互鉴别需要三次传递。

密码校验函数的例子见附录C。

2　引用标准

下列标准所包含的条文，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 15843.1—1999　信息技术　安全技术　实体鉴别　第1部分：概述
(idt ISO/IEC 9798-1:1997)

3　定义和记法

本标准使用了GB/T 15843.1中描述的定义和记法。此外还使用下列定义和记法：

3.1　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(见GB/T 9387.2)。

3.2　$f_K(Z)$

密码校验值，它是以密钥K和任意字符串Z作为输入，使用密码校验函数f所得的结果。

3.3　T_A / N_A

由实体A原发的时变参数，它或者是时间标记T_A，或者是顺序号N_A。

4　要求

本标准规定的鉴别机制中，待鉴别的实体通过表明它拥有某个秘密鉴别密钥来证实其身份。这可通过由该实体以其秘密密钥和特定数据作为输入，使用密码校验函数获得密码校验值来达到。密码校验值可由拥有该实体的秘密鉴别密钥的任何实体来校验，这个实体能重新计算密码校验值并与所收到的值

国家质量技术监督局1999-11-11批准　　2000-05-01实施