ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 15843.4—2008/ISO/IEC 9798-4:1999
代替 GB/T 15843.4—1999

# 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**

(ISO/IEC 9798-4:1999,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

以后还可能增加其他后续部分。

本部分为GB/T 15843的第4部分，等同采用ISO/IEC 9798-4:1999《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》，仅有编辑性修改。

本部分代替GB/T 15843.4—1999《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》。本部分与GB/T 15843.4—1999相比，主要变化如下：

——本部分删除了ISO/IEC前言，并增加了引言。

——本部分根据GB/T 15843.1的修订，更改部分术语。

——本部分为与ISO/IEC 9798-4:1999一致，删除了GB/T 15843.4—1999中的3.1，3.2，3.3。

——本部分删除了GB/T 15843.4—1999的附录B、附录C、附录D，而统一使用GB/T 15843.1的附录B、附录C和参考文献。

本部分的附录A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、吕春利、夏鲁宁、高能、向继。

本部分所代替标准的历次发布情况为：

——GB/T 15843.4—1999。

# 引　言

本部分等同采用国际标准 ISO/IEC 9798-4:1999,它是由 ISO/IEC 联合技术委员会 JTC 1(信息技术)的分委员会 SC 27(IT 安全技术)起草的。

本部分定义了采用密码校验函数的实体鉴别机制,分为单向鉴别和相互鉴别两种。其中单向鉴别按照消息传递的次数,又分为一次传递鉴别和两次传递鉴别;相互鉴别根据消息传递的次数,分为两次传递鉴别和三次传递鉴别。

有关密码校验函数的例子,见 GB 15852。

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4部分:采用密码校验函数的机制

## 1　范围

本部分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。

本部分中规定的机制采用诸如时间戳、序号或随机数等时变参数,防止先前有效的鉴别信息以后又被接受或者被多次接受。

如果采用时间戳或序号,对于单向鉴别只需一次传递,而相互鉴别则需两次传递。如果采用使用随机数的激励—响应方法,单向鉴别需两次传递,相互鉴别则需三次传递。

密码校验函数的例子见GB 15852。

## 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 15843.1—2008　信息技术　安全技术　实体鉴别　第1部分:概述(ISO/IEC 9798-1:1997,IDT)

GB 15852—1995　信息技术　安全技术　用块密码算法作密码校验函数的数据完整性机制(idt ISO/IEC 9797:1994)

## 3　术语、定义和符号

GB/T 15843.1—2008中确立的术语、定义和符号适用于本部分。

## 4　要求

本部分规定的鉴别机制中,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。这可由该实体使用其秘密鉴别密钥和密码校验函数对指定数据计算密码校验值来实现。密码校验值可由拥有该实体的秘密鉴别密钥的任何其他实体来校验,其他实体能重新计算密码校验值并与所收到的值进行比较。

这些鉴别机制有下述要求,如果其中任何一条没有得到满足,则鉴别过程会被攻击,或者不能成功完成:

a) 向验证方证实其身份的声称方与该验证方共享一个秘密鉴别密钥。在正式启动鉴别机制之前,此密钥应为有关各方所知道。向各个实体分发密钥的方法不属本部分的范围。

b) 声称方和验证方共享的秘密鉴别密钥应仅为这两个实体,以及双方都信任的其他实体所知。

c) 机制的安全强度依赖于密钥的长度和安全性、密码校验函数的特性,以及密码校验值的长度。这些参数应被仔细选取以满足既定的安全级别,参数选取和安全级别可能在安全策略中有明确规定。

## 5　机制

### 5.0　概述

这些鉴别机制中,实体A和B在启动鉴别机制之前应共享一个秘密密钥$K_{AB}$或两个单向秘密密钥