ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.2—2008/ISO/IEC 9798-2:1999
代替 GB 15843.2—1997

信息技术　安全技术　实体鉴别 第2部分:采用对称加密算法的机制

Information technology—Security techniques—Entity authentication—Part 2:Mechanisms using symmetric encipherment algorithm

(ISO/IEC 9798-2:1999,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

可能还会增加其他后续部分。

本部分为GB/T 15843的第2部分，等同采用ISO/IEC 9798-2:1999《信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制》(英文版)，仅有编辑性修改。

本部分代替GB 15843.2—1997《信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制》。本部分与GB 15843.2—1997相比，主要变化如下：

——本部分更新了第4章“要求”，对加密函数以及与它对应的解密函数应具有的属性提出了要求，同时增加了对时变参数特性的要求。

——本部分在内容上增加了对于基于单向密钥来完成鉴别过程的考虑，因而在对应的各个章条部分都增加了相应的叙述。

——本部分废止了旧版中关于实体A和B之间共享一个秘密密钥K'_{AB}，而K'_{AB}只用于B对A的鉴别的相关叙述。

——本部分删除了ISO/IEC　前言，增加了引言。

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、许长志、高能、向继、夏鲁宁。

本部分所代替标准的历次版本发布情况为：

——GB 15843.2—1997。

引　言

本部分等同采用国际标准 ISO/IEC 9798-2:1999,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。

本部分规定了采用对称加密算法的实体鉴别机制,包括单向鉴别机制和相互鉴别机制,不涉及可信第三方的鉴别机制和涉及可信第三方的鉴别机制,并给出了这些鉴别机制的 5 项要求。

在不涉及可信第三方的情况下,单向鉴别机制包括一次传递鉴别和两次传递鉴别两种,相互鉴别机制包括两次传递鉴别和三次传递鉴别两种。如果涉及可信第三方,相互鉴别机制则需要进行四次或者五次传递。

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2部分:采用对称加密算法的机制

1　范围

本部分规定了采用对称加密算法的实体鉴别机制。其中有四种是两个实体间无可信第三方参与的鉴别机制,而这四种机制中有两种是单个实体鉴别(单向鉴别),另两种是两个实体相互鉴别。其余的机制都要求有一个可信第三方参与,以便建立公共的秘密密钥,实现相互或单向的实体鉴别。

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。

如果没有可信第三方参与同时又采用时间戳或序号,则对于单向鉴别只需传递一次信息,而要实现相互鉴别必须传递两次。如果没有可信第三方参与同时又采用使用随机数的激励—响应方法时,单向鉴别需传递两次信息,而相互鉴别则需要传递三次。如果有可信第三方参与,则一个实体与可信第三方之间的任何一次附加通信都需要在通信交换中增加两次传递。

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)

ISO/IEC 11770-2:1996　信息技术　安全技术　密钥管理　第2部分:采用对称技术的机制

3　术语、定义和符号

GB/T 15843.1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知道某秘密鉴别密钥来证实其身份。这可由该实体用其秘密密钥加密特定数据达到,与其共享秘密鉴别密钥的任何实体都可以将加密后的数据解密。

这些鉴别机制有下列要求,若其中任何一个不满足,则鉴别过程就会受到攻击,或者不能成功完成。

a)　向验证方证实其身份的声称方,在应用第5章的机制时,应和该验证方共享一个秘密鉴别密钥,在应用第6章的机制时,每个实体应和公共的可信第三方都分别共享一个秘密鉴别密钥。这些密钥应当在正式启动鉴别机制前就为有关各方知道,达到这一点所采用的方法已超出了本部分的范围。

b)　如果涉及到可信第三方,它应得到声称方与验证方的共同信任。

c)　声称方与验证方共享的秘密鉴别密钥,或实体与可信第三方共享的秘密鉴别密钥,应仅为这两方或双方都信任的其他方所知。

注1:加密算法与密钥生命周期的选择应保证密钥在其生命周期内就被推算出来在计算上是不可行的。此外,在选择密钥生命周期时还应防止已知明文和选择明文的攻击。