ICS 35.040
L 80

中华人民共和国国家标准

GB 15843.2—1997
idt ISO/IEC 9798-2:1994

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 algorithms

1997-09-02 发布　　1998-04-01 实施

国家技术监督局　发布

目　　次

前言 …… Ⅲ
ISO/IEC 前言 …… Ⅳ
1　范围 …… 1
2　引用标准 …… 1
3　定义和记法 …… 1
4　要求 …… 1
5　不涉及可信第三方的机制 …… 2
6　涉及可信第三方的机制 …… 5
附录 A(提示的附录)　文本字段的使用 …… 8
附录 B(提示的附录)　时变参数 …… 8
附录 C(提示的附录)　参考文献 …… 9

前　言

本标准等同采用国际标准 ISO/IEC 9798-2:1994《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》。

该标准规定了用对称加密算法实现的实体鉴别机制,它适合于我国使用。

GB 15843 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 1 部分:一般模型

GB 15843 在总标题《信息技术　安全技术　实体鉴别》下还由下列部分组成:

——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

本标准中的附录 A、附录 B、附录 C 都是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位:电子工业部第三十研究所、电子工业部标准化研究所。

本标准主要起草人:龚奇敏,方姝妹,杜明钰,李桂茹,向维良。

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 JTC 1。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 9798-2 是由联合技术委员会 ISO/IEC JTC 1(信息技术)的分委员会 SC 27(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 1 部分:一般模型

——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》下还由下列部分组成:

——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 1 部分和第 3 部分之前的总标题在下一个修订版中将调整为第 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 和附录 C 只作为信息提供。

中华人民共和国国家标准

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

GB 15843.2—1997
idt ISO/IEC 9798-2:1994

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

1　范围

本标准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。

本标准中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，防止先前有效的鉴别信息以后又被接受。

如果没有可信第三方参与，又采用时间标记或顺序号，则对于单向鉴别只需传送一次信息，而要达到相互鉴别必须传送两次。如果没有可信第三方参与，又采取使用随机数的询问—应答方法时，单向鉴别需传送两次信息，而相互鉴别则需要传送三次。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送。

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 15843.1—1995　信息技术　安全技术　实体鉴别机制　第1部分：一般模型(idt ISO/IEC 9798-1:1991)

3　定义和记法

本标准使用GB 15843.1中的定义和记法。

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，共享其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，则鉴别进程就会受到损害或根本不能实现。

a) 向验证者证实其身份的声称者，在应用第5章的机制时，应和该验证者共享一个秘密鉴别密钥，在应用第6章的机制时，每个实体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掌握，达到这一点所采用的方法已超出了本标准的范围。

b) 如果涉及到可信第三方，它应得到声称者与验证者的共同信任。

c) 声称者与验证者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

国家技术监督局1997-09-02批准　　1998-04-01实施