ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.3—1998
idt ISO/IEC DIS 9798-3:1997

信息技术　安全技术　实体鉴别
第3部分：用非对称签名技术的机制

Information technology—Security techniques—
Entity authentication—Part 3:
Mechanisms using asymmetric signature techniques

1998-12-14 发布　　1999-08-01 实施

国家质量技术监督局　发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC DIS 9798-3:1997《信息技术　安全技术　实体鉴别　第 3 部分:用非对称签名技术的机制》。

本标准规定的单方鉴别和相互鉴别机制用于保证信息交换的安全。

该系列标准在总标题《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:用对称加密算法的机制

第 3 部分:用非对称签名技术的机制

第 4 部分:用密码检验函数的机制

第 5 部分:用零知识技术的机制

将来增加的部分可跟随其后。

本标准的附录 A 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:电子工业部标准化研究所、电子工业部第三十研究所。

本标准主要起草人:向维良、龚奇敏、吴世宗、雷利民、陶仁骥、郝伟刚。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)共同组成一个世界标准化专门系统。ISO 或 IEC 的国家成员体,通过涉及特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准开发。ISO 和 IEC 的技术委员会在共同感兴趣的领域内合作,与 ISO 和 IEC 有联络的其他官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO 和 IEC 已建立了一个联合技术委员会 ISO/IEC JTCI。由联合技术委员会采纳的国际标准草案需分发给各国家成员体表决。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 DIS 9798-3 是由联合技术委员会 ISO/IEC JTCI“信息技术”的 SC 27 分委会“IT 安全技术”制定的。

这个第二版取代了第一版(ISO/IEC 9798-3:1993),对它作了技术上的修订。

ISO/IEC 9798 在总标题《信息技术　安全技术　实体鉴别》下,由以下几部分组成:

——第 1 部分:概述

——第 2 部分:用对称加密算法的机制

——第 3 部分:用非对称签名技术的机制

——第 4 部分:用密码检验函数的机制

——第 5 部分:用零知识技术的机制

将来增加的部分可跟随其后。

本标准的附录 A 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3部分：用非对称签名技术的机制

GB/T 15843.3—1998
idt ISO/IEC DIS 9798-3:1997

Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using asymmetric signature techniques

1　范围

本标准规定了用非对称签名技术的实体鉴别机制。有两种鉴别机制属单个实体(单向)的鉴别，其余的属两个实体相互鉴别的机制。数字签名用于验证实体的身份，也可能有可信的第三方参与。

本标准中规定的机制，使用时变参数，如：时间标记、顺序号或随机数，可防止先前有效的鉴别信息以后又被接受。

若使用时间标记或顺序号，则单向鉴别只需要一次传递，而完成相互鉴别则需两次传递。若使用带有随机数的询问和响应方法，则单向鉴别需要两次传递，而当完成相互鉴别，则需要三次或四次传递(依赖于所使用的机制)。

2　引用标准

下列标准所包含的条文，通过在本标准中引有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。

ISO/IEC 9798-1:1997　信息技术　安全技术　实体鉴别　第1部分：概述

3　定义和记法

本标准采用 ISO/IEC 9798-1 中描述的定义和记法。

4　要求

本标准规定的鉴别机制中，待鉴别的实体要通过表明他知道某秘密签名密钥来证实其身份。这要由实体使用其秘密签名密钥对特定数据签名来完成。该签名能够由使用该实体的公开认证密钥的任何实体来验证。

鉴别机制有以下的要求：

a) 验证者应拥有声称者的有效公开密钥；

b) 声称者应拥有仅由他自己知道和使用的秘密签名密钥。

若这两者之一未能满足，则鉴别进程会受到损害，或者不能成功地完成。

注：获得有效公开密钥的一种途径是用证书的方式(见 ISO/IEC 9798-1:1997 的附录 C)。证书的产生、分发和撤消都超出了本标准的范围。为了这个目的，这里可以存在可信的第三方。另一种获得有效公开密钥的途径是利用可信的信使。

国家质量技术监督局 1998-12-14 批准　　1999-08-01 实施