ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.3—2008/ISO/IEC 9798-3:1998
代替 GB/T 15843.3—1998

信息技术　安全技术　实体鉴别 第3部分:采用数字签名技术的机制

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

(ISO/IEC 9798-3:1998,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3部分，等同采用ISO/IEC 9798-3:1998《信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制》，仅有编辑性修改。

本部分代替GB/T 15843.3—1998《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》。本部分与GB 15843.3—1998相比，主要变化如下：

——本部分修改了名称。

——本部分根据GB/T 15843.1的修订，更改了部分术语。

——本部分删除了ISO/IEC前言，并增加了引言。

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、王平建、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 15843.3—1998。

引　言

本部分等同采用国际标准 ISO/IEC 9798-3:1998,它是由 ISO/IEC 联合技术委员会 JTC1(信息技术)的分委员会 SC27(IT 安全技术)起草的。

本部分定义了采用数字签名技术的实体鉴别机制,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、三次传递鉴别和两次传递并行鉴别。

由于签名所使用的证书的分发方式超出本部分范围,证书的发送在所有的机制中是可选的。

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3部分:采用数字签名技术的机制

1　范围

本部分规定了采用数字签名技术的实体鉴别机制。有两种鉴别机制是单个实体的鉴别(单向鉴别),其余的是两个实体的相互鉴别机制。

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,则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,相互鉴别则需三次或四次传递(依赖于所采用的机制)。

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 15851—1995　信息技术　安全技术　带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

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私有签名密钥来证实其身份。这要由实体使用其私有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验证密钥的任何实体来验证。

鉴别机制有下述要求:

a)　验证方应拥有声称方的有效公开密钥;

b)　声称方应拥有仅由声称方自己知道的私有签名密钥。

若这两条要求中的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。

注1:获得有效公开密钥的一种途径是用证书方式(见 GB/T 15843.1—2008 的附录C)。证书的产生、分发和撤销都超出了本部分的范围。为了以证书形式获取有效公开密钥,可以引入可信第三方。另一种获得有效公开密钥的途径是利用可信的信使。

注2:有关数字签名方案的参考文献在 GB/T 15843.1—2008 的参考文献中有描述。

5　机制

5.0　概述

本部分规定的实体鉴别机制使用了时变参数,如时间戳、序号或随机数(见 GB/T 15843.1—2008 的附录B和下面的注1)。

本部分中,权标的形式如下: