ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.5—2005/ISO/IEC 9798-5:1999

信息技术　安全技术　实体鉴别
第5部分:使用零知识技术的机制

Information technology—Security techniques—Entity authentication—Part 5:Mechanisms using zero knowledge techniques

(ISO/IEC 9798-5:1999,IDT)

2005-04-19 发布　　2005-10-01 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》，由以下几部分组成：

——第1部分：概述

——第2部分：使用对称加密算法的机制

——第3部分：使用数字签名技术的机制

——第4部分：使用密码校验函数的机制

——第5部分：使用零知识技术的机制

本部分为GB/T 15843的第5部分，等同采用国际标准ISO/IEC 9798-5:1999《信息技术　安全技术　实体鉴别　第5部分：使用零知识技术的机制》(英文版)。

本部分的附录A，附录B，附录C，附录D，附录E和附录F是资料性附录。

本部分由中华人民共和国信息产业部提出；

本部分由全国信息安全标准化技术委员会归口；

本部分由中国电子技术标准化研究所、信息安全国家重点实验室起草。

本部分主要起草人：陈星、罗锋盈、胡磊、叶顶锋、张振峰、黄家英。

信息技术　安全技术　实体鉴别
第5部分:使用零知识技术的机制

1　范围

GB/T 15843的本部分详细说明了三种使用零知识技术的实体鉴别机制。所有在GB/T 15843的本部分中阐述的机制都提供单向鉴别。这些机制应用零知识的原理所构造,但是根据附录A的严格定义,对所有参数的选择,这些机制本身并不是零知识的。

第一种机制称为基于身份的机制。可信的认可机构为每一个声称者提供私有认可信息,该私有认可信息是作为声称者的标识数据和认可机构的私有密钥的函数计算出来的。

第二种机制称为基于使用离散对数的基于证书的机制。每一个声称者都拥有一对用于此机制的公开密钥和私有密钥对。每一个声称者身份的验证者必须拥有该声称者公开验证密钥的可信拷贝;其获取的方法已经超出了本标准的范围,但是它可以通过由可信第三方签名的证书的分发来获得。

第三种机制称为基于使用非对称加密系统的基于证书的机制。每一个声称者都拥有一对用于非对称加密系统的公开密钥和私有密钥对。每一个声称者身份的验证者必须拥有该声称者公开验证密钥的可信拷贝;其获取的方法已经超出了本标准的范围,但是可以通过由可信第三方签名的证书的分发来获得。

2　规范性引用文件

下列文件中的条款通过GB/T 15843的本部分的引用而成为本部分的条款。凡是注日期的引用文件,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 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)

GB/T 15843.1—1999　信息技术　安全技术　实体鉴别　第1部分:概述(idt ISO/IEC 9798-1:1997)

GB/T 18238(所有部分)　信息技术　安全技术　散列函数(idt ISO/IEC 10118)

3　术语和定义

GB/T 15843.1—1999中确立的下列术语和定义适用于GB/T 15843的本部分。

3.1

非对称密码技术　asymmetric cryptographic technique

3.2

非对称加密系统　asymmetric encipherment system

3.3

非对称密钥对　asymmetric key pair

3.4

询问　challenge

3.5

声称者　claimant