ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17902.3—2005/ISO/IEC 14888-3:1998

信息技术　安全技术　带附录的数字签名　第3部分:基于证书的机制

Information technology—Security techniques—Digital signatures with appendix—Part 3:Certificate-based mechanisms

(ISO/IEC 14888-3:1998,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 17902《信息技术　安全技术　带附录的数字签名》由以下几个部分组成：

第1部分：概述；

第2部分：基于身份的机制；

第3部分：基于证书的机制。

本部分为GB/T 17902的第3部分，等同采用国际标准ISO/IEC 14888-3:1998《信息技术　安全技术　带附录的数字签名　第3部分：基于证书的机制》(英文版)。

本部分的附录A和附录B是规范性附录，附录C到附录G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：叶茅枫、陈星、罗锋盈、胡磊、叶顶锋、张振峰、黄家英。

信息技术　安全技术　带附录的数字签名
第3部分:基于证书的机制

1　范围

GB/T 17902规定了任意长度消息的带附录的数字签名机制并适用于提供数据原始鉴别、抗抵赖和数据完整性的方案。

GB/T 17902的本部分规定了带附录的基于证书的数字签名机制。特别是,本部分提供了:

1)　基于证书的签名机制的一般描述,其安全性是基于所用交换群上的离散对数问题的困难性(见第6章)。

2)　基于证书的签名机制的一般描述,其安全机制是基于因子分解的困难性(见第7章)。

3)　使用任意长度消息的基于证书机制的带附录的各种常规数字签名机制(见附录A和附录B)。

2　规范性引用文件

下列文件中的条款通过GB/T 17902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 17902.1—1999　信息技术　安全技术　带附录的数字签名　第1部分:概述

GB/T 17902.2—2005　信息技术　安全技术　带附录的数字签名　第2部分:基于身份的机制(ISO/IEC 14888-2:1999,IDT)

GB/T 18238.3—2002　信息技术　安全技术　散列函数　第3部分:专用散列函数(idt ISO/IEC 10118-3:1998)

ISO/IEC 9796-2:1997　信息技术　安全技术　带消息恢复的数字签名方案　第2部分:使用散列函数的机制

ISO/IEC 10118-4:1998　信息技术　安全技术　散列函数　第4部分:使用模数算法的散列函数

3　概述

在GB/T 17902的本部分中使用了GB/T 17902.1—1999中所给的定义、符号、数字长度和记法。

数字签名的验证需要签名实体的验证密钥。所以,验证方必须把正确的验证密钥与签名实体关联起来。对基于证书的机制来说,这种关联必须通过某种证书的方法来提供。例如,验证密钥是取自一个证书。

GB/T 17902的本部分的目的是规定GB/T 17902.1—1999中描述的一般模型的下列过程和函数:

a)　生成密钥的过程

　　1)　生成域参数

　　2)　生成签名和验证密钥

b)　形成签名的过程

　　1)　(可选)形成预签名

　　2)　为签名准备消息