



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	III
1 范围	1
2 规范性引用文件	1
3 概述	1
4 术语和定义	2
5 符号和记法	2
6 基于离散对数的数字签名机制	2
6.1 密钥生成过程	2
6.2 签名过程	3
6.3 验证过程	4
7 基于因子分解的数字签名机制	6
7.1 密钥生成过程	6
7.2 签名过程	6
7.3 验证过程	7
附录 A(规范性附录) 基于离散对数的带附录的基于证书的数字签名的例子	8
A.1 基于非椭圆曲线的例子	8
A.1.0 符号和记法	8
A.1.1 数字签名算法(DSA)	8
A.1.2 Pointcheval/Vaudenay 签名	10
A.2 基于椭圆曲线的例子	12
A.2.1 椭圆曲线 DSA	12
附录 B(规范性附录) 基于因子分解的带附录的基于证书的数字签名的例子	14
B.1 基于 GB 15851 的散列的数字签名	14
B.1.1 域参数的生成	14
B.1.2 签名密钥和验证密钥的生成	14
B.1.3 签名过程	14
B.1.4 验证过程	15
B.2 ESIGN	15
B.2.1 域参数的生成	15
B.2.2 签名密钥和验证密钥的生成	15
B.2.3 签名过程	15
B.2.4 验证过程	16
附录 C(资料性附录) FIPS PUB 186 素数 P 和 Q 的生成	17
附录 D(资料性附录) 椭圆曲线数学背景	18
D.1 椭圆曲线和点	18
D.1.1 F_p 上的椭圆曲线加法规则	18
D.1.2 F_{2^m} 上的椭圆曲线加法规则	18
附录 E(资料性附录) 带附录的基于证书的数字签名的数值例子	20

E.1	数字签名算法(DSA)	20
E.1.1	DSA 参数	20
E.1.2	DSA 签名密钥和验证密钥	20
E.1.3	DSA 每个消息的数据	20
E.1.4	DSA 签名	20
E.1.5	DSA 验证数值	20
E.2	Pointcheval/vaudenay 签名算法	20
E.2.1	Pointcheval/vaudenay 参数	20
E.2.2	Pointcheval/vaudenay 签名密钥和验证密钥	21
E.2.3	Pointcheval/vaudenay 每个消息的数据	21
E.2.4	Pointcheval/vaudenay 签名	21
E.2.5	Pointcheval/vaudenay 验证数值	21
E.3	椭圆曲线 DSA	21
E.3.1	例 1:域 F_{2^m} , $m=191$	21
E.3.2	例 2:域 F_p , 192 比特素数 p	22
E.4	基于 GB 15851—1995 的带散列的数字签名	23
E.4.1	v 为奇数($v=3$)的例子	23
E.4.2	v 为偶数($v=2$)的例子	25
E.5	ESIGN 签名算法	27
E.5.1	ESIGN 域参数	27
E.5.2	签名密钥和验证密钥	27
E.5.3	ESIGN 签名过程	27
E.5.4	ESIGN 验证	29
附录 F(资料性附录)	所选签名方案具有的特性	31
附录 G(资料性附录)	专利信息	32
参考文献		33
图 1	带随机性证据的签名过程	4
图 2	带随机化证据的验证过程	5

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、叶顶峰、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