ICS 35.040
L 80

中华人民共和国国家标准

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

Information technology—Security techniques—
Digital signature with appendix—
Part 1:General

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局　发布

目　　次

前　　言

本标准规定了带附录的数字签名方案，适合于我国使用。

GB/T 17902 在总标题《信息技术　安全技术　带附录的数字签名》下，由以下几个部分组成：

第 1 部分：概述；

第 2 部分：基于身份的方案；

第 3 部分：基于证书的方案。

本标准的附录 A 是标准的附录，附录 B 是提示的附录。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准由复旦大学、中科院软件所负责起草。

本标准主要起草人：鲍振东、赵一鸣、陶仁骥、计青。

引　　言

数字签名机制采用非对称密码技术，它可用来提供实体鉴别，数据原发鉴别，数据完整性和抗抵赖服务。有两种数字签名机制：

——若验证进程需要消息作为输入部分，这种机制称为“带附录的数字签名”。在计算附录时使用了散列函数。ISO/IEC 10118 规定了这类散列函数；

——若验证进程给出消息及其特定冗余（有时也称作消息影子），这种机制称为“带消息恢复的签名机制”。GB 15851 规定了这种机制。

这两种机制不是互斥的。具体地说，任何带消息恢复的签名机制，例如，ISO/IEC 9796-1 规定的机制，可以用来提供带附录的数字签名。这种情况下，可以对消息的散列权标使用签名进程来产生签名。

中华人民共和国国家标准

信息技术　安全技术
带附录的数字签名
第1部分：概述

GB/T 17902.1—1999

Information technology—Security techniques—
Digital signature with appendix—
Part 1:General

1　范围

系列标准GB/T 17902规定了几个任意长度消息的带附录数字签名机制。本标准包括了带附录的数字签名的基本原则和要求，同时也包括了在该系列标准的所有部分都用到的定义和符号。

2　引用标准

下列标准所包含的条文，通过在本标准中引用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 9796-1:1991　信息技术　安全技术　带消息恢复的数字签名方案　第1部分：使用冗余的机制

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 10118-1:1996　信息技术　安全技术　散列函数　第1部分：概述

ISO/IEC 11770-3[1)]　信息技术　安全技术　密码管理　第3部分：使用非对称密码技术的机制

3　概述

本标准所规定的机制是基于非对称密码技术的。所有非对称数字签名机制涉及三个基本操作：

——产生密钥对的进程：每对密钥包括签名密钥和相应的验证密钥；

——使用签名密钥的进程：称为签名进程；

——使用验证密钥的进程：称为验证进程。

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，或者更准确地讲，与(部分)签名实体的标识数据联系起来。如果这种联系是验证密钥自身所固有的，这种方案是“基于身份的”。如果不是，应该由其他途径提供正确的验证密钥与签名实体间的联系，无论使用何种途径，这种方案是“基于证书的”。

基于证书方案的验证密钥管理超出本标准的范围。ISO/IEC 11770-3提供了公开密钥分发的机制。

1) 待发布。

国家质量技术监督局1999-11-11批准　　2000-05-01实施