ICS 35.020
L 80

中华人民共和国国家标准

GB 15851—1995
idt ISO/IEC 9796:1991

信息技术　安全技术
带消息恢复的数字签名方案

Information technology—Security techniques—
Digital signature scheme giving message recovery

自 2017 年 3 月 23 日起，本标准转为推荐性标准，编号改为 GB/T 15851—1995。

1995-12-13 发布　　1996-08-01 实施

国家技术监督局　发布

目　　次

前言 …… Ⅲ
ISO/IEC 前言 …… Ⅳ
引言 …… Ⅴ
1　范围 …… 1
2　定义 …… 1
3　符号和缩略语 …… 1
4　概述 …… 2
5　签名进程 …… 2
5.1　填充 …… 3
5.2　扩展 …… 3
5.3　冗余 …… 3
5.4　截取和强置 …… 3
5.5　签名产生 …… 3
6　验证进程 …… 4
6.1　签名开启 …… 4
6.2　消息恢复 …… 4
6.3　冗余校验 …… 5
附录 A(提示的附录)　用于数字签名的公开密钥体制例子 …… 6
附录 B(提示的附录)　关于附录 A(提示的附录)的说明实例 …… 8
附录 C(提示的附录)　为抵抗对附录 A(提示的附录)各种潜在攻击所采取的若干预防措施 …… 16
附录 D(提示的附录)　参考文献 …… 16

前　言

本标准等同采用国际标准 ISO/IEC 9796:1991《信息技术　安全技术　带消息恢复的数字签名方案》。

该国际标准规定的对有限长消息进行数字签名的方案，适合于我国使用。

本标准的附录 A、附录 B、附录 C 和附录 D 都是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位：电子工业部第三十研究所。

本标准主要起草人：龚奇敏、黄月江、方关宝、雷利民、李桂茹。

根据中华人民共和国国家标准公告(2017 年第 7 号)和强制性标准整合精简结论，本标准自 2017 年 3 月 23 日起，转为推荐性标准，不再强制执行。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)形成了世界范围内的标准化专门体系。ISO 或 IEC 的成员国,通过由处理特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准的开发。ISO 和 IEC 的技术委员会在共同感兴趣的领域内合作,其他与 ISO 和 IEC 有联络的官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO 和 IEC 已建立了一个联合技术委员会 ISO/IEC JTC1。被联合技术委员会接受的国际标准草案送给各成员国表决。一个国际标准的发布,需要至少 75%的成员国投赞成票。

国际标准 ISO/IEC 9796 是由信息技术联合技术委员会 ISO/IEC JTC1 制定的。

附录 A、B、C 和 D 只作为参考。

引　言

电子信息交换中的数字签名和传统邮件中的手写签名十分相似。

大多数数字签名方案都基于某种公开密钥体制。所有公开密钥体制均包含三种基本操作：

——产生密钥对的进程，该密钥对由一个秘密密钥和一个公开密钥组成；

——使用秘密密钥的进程；

——使用公开密钥的进程。

在所有公开密钥数字签名方案中，秘密密钥用于消息的签名进程，公开密钥用于签名的验证进程，因而数字签名方案的密钥对由一个“秘密签名密钥”和一个“公开验证密钥”组成。

明显地，有两类数字签名方案：

——当验证进程需要消息作为输入的一部分时，该方案称作“带附录的签名方案”，在计算附录中将使用散列函数；

——当验证进程同时揭示消息及其冗余（有时称作“消息影子”）时，该方案称作“带消息恢复的签名方案”。

本标准规定了有限长消息的数字签名方案。

该数字签名方案的验证进程只需要尽量少的资源。它不涉及到使用散列函数，从而避免了对这种一般算法的已知攻击。

消息不一定要用自然语言写，可以是任意一种有限长的比特串。此类消息的例子有保密密钥材料以及对更长消息进行散列运算后的结果，又称为“消息印鉴”。由保密软硬件所产生的几个比特串组成的结构化组便是一个特例，其中一个比特串是对该硬件内产生的控制信息编码的结果。

注：本标准的使用可能涉及到某些专利条款。

中华人民共和国国家标准

信息技术　安全技术
带消息恢复的数字签名方案

GB 15851—1995
idt ISO/IEC 9796:1991

Information technology—Security techniques—
Digital signature scheme giving message recovery

1　范围

本标准规定了对有限长消息使用公开密钥体制的带消息恢复的数字签名方案。

这种数字签名方案包含下列两个进程：

——签名进程，它使用秘密签名密钥和签名函数来对消息签名；

——验证进程，它使用公开验证密钥和验证函数来验证签名，同时恢复出消息。

签名进程中，必要时，欲签名的消息需填充和扩展，然后加上与消息本身有关的人为的冗余，对消息中是否存在自然的冗余不作假定。这人为的冗余将由验证进程揭示出来，把这人为的冗余去掉便恢复出消息。

本标准不规定密钥产生进程、签名函数和验证函数。附录A(提示的附录)给出了一个公开密钥体制的例子，包含密钥产生、签名函数和验证函数。附录B(提示的附录)通过例子来说明这些操作的各步。

这个方案中的若干参数与安全性有关：本标准不规定为要达到给定的安全性水平而对这些参数应取什么值。然而以这样一种方式规定，即在本标准使用中，如果这些参数中有的必须要改变时，使所作的改变最小。

2　定义

本标准采用下列定义。

2.1　消息　message

有限长的比特串。

2.2　签名　signature

由签名进程最后得到的比特串。

3　符号和缩略语

MP	填充后的消息
ME	扩展后的消息
MR	带冗余的扩展后的消息
IR	中间整数
Σ	签名
K_s	签名的比特数
IR'	恢复后的中间整数
MR'	恢复后的带冗余的消息

国家技术监督局1995-12-13批准　　1996-08-01实施