ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36644—2018

信息安全技术
数字签名应用安全证明获取方法

Information security technology—
Methods for obtaining security attestations for digital signature applications

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　数字签名应用安全证明获取 …… 2
5.1　概述 …… 2
5.2　私钥拥有属性的安全证明获取 …… 3
5.2.1　证明时刻确定的私钥拥有属性安全证明获取时效模型 …… 3
5.2.2　证明时刻不确定的私钥拥有属性安全证明获取时效模型 …… 3
5.2.3　私钥拥有属性安全证明获取过程 …… 4
5.2.4　具体的私钥拥有属性安全证明获取流程 …… 7
5.3　公钥有效性的安全证明获取 …… 10
5.3.1　总则 …… 10
5.3.2　拥有者的公钥有效性安全证明获取 …… 10
5.3.3　验证者的公钥有效性安全证明获取 …… 11
5.3.4　公钥有效性验证过程 …… 11
5.4　数字签名的生成时间安全证明获取 …… 11
5.4.1　总则 …… 11
5.4.2　从 TTSA 获取时间的方式获取签名生成时间证明 …… 11
5.4.3　用验证方提供的数据获得签名生成时间证明 …… 20
附录 A（资料性附录）　SM2 签名算法公钥有效性获取流程 …… 24
参考文献 …… 25

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院数据与通信保护研究教育中心、中国科学院软件研究所、重庆大学。

本标准主要起草人:王跃武、刘丽敏、吕娜、张严、荆继武、雷灵光、牛莹姣、刘志娟、向宏、夏晓峰、周荃、夏鲁宁。

引　言

参与数字签名生成或验证的实体取决于过程的真实性，该真实性可以通过获取私钥拥有属性的安全证明、公钥有效性的安全证明、数字签名的生成时间来保证。本标准旨在规定一套数字签名应用安全证明获取方法，用以规范数字签名应用安全证明过程，主要应用于需要提供数字签名生成过程安全性和对签名生成时间有明确要求的签名应用场景。

本标准在制定的过程中参考了 NIST SP 800-89《数字签名应用安全保证获取建议》和 NIST SP 800-102《数字签名适时性证明获取建议》。本标准与两个参考标准在技术内容上保持一致，但忽略了其与美国具体的签名算法标准相关部分，强调了安全证明获取的一般过程。此外，本标准将参考标准中与密码相关的术语和规定改成了与我国密码政策相符的规定。

信息安全技术
数字签名应用安全证明获取方法

1 范围

本标准规定了一套数字签名应用安全证明获取方法，用以规范数字签名应用安全证明过程。

本标准适用于需要提供数字签名生成过程安全性和对签名生成时间有明确要求的签名应用场景。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 25069—2010 信息安全技术 术语

GB/T 32918.1—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第2部分：数字签名算法

3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

公钥有效性证明 attestation of public key validity

证明用于验证签名的公钥的有效性的证据。

3.2

私钥拥有属性安全证明 attestation of private key possession

证明声称的签名者确实实际拥有用于生成签名的私钥的证据。

3.3

证明消息 attestation message

用于获取私钥拥有属性安全证明的，具有特定格式的消息。

3.4

证明签名 attestation signature

作用于证明消息的数字签名。

3.5

证明时间 attestation time

私钥拥有属性安全证明获取的时间。

3.6

证明水平 attestation level

私钥拥有属性安全证明的可信程度，分为高、中、低三个层次，依赖于证明获取的手段。