ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38646—2020

信息安全技术　移动签名服务技术要求

**Information security technology—
Technical requirements of mobile signature service**

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

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:中国移动通信集团有限公司、中移(杭州)信息技术有限公司、中国信息通信研究院、北京数字认证股份有限公司、中国电信股份有限公司、工业和信息化部电子工业标准化研究院。

本标准主要起草人:于蓉蓉、张滨、杨志强、张锦卫、邱勤、樊山、杨超、路晓明、刘海龙、罗红、董靖宇、贾倩、鲁青、黄伟湘、林雪焰、杨正军、崇静、许东阳、于乐、蒋周良、安宝宇、马臣云、霍薇靖、蔡准。

信息安全技术　移动签名服务技术要求

1　范围

本标准规定了实现移动签名服务的技术要求，包括移动签名服务的基本框架、基本服务流程、参与移动签名服务的主要实体功能、接口功能及安全要求等。

本标准适用于移动签名服务的设备研制和平台开发。

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 19713　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 25064—2010　信息安全技术　公钥基础设施　电子签名格式规范

GB/T 25065—2010　信息安全技术　公钥基础设施　签名生成应用程序的安全要求

GM/T 0028—2014　密码模块安全要求

3　术语和定义

GB/T 25064—2010、GB/T 25065—2010 界定的以及下列术语和定义适用于本文件。

3.1

应用提供者　application provider

为用户提供业务应用服务的实体。

3.2

移动设备　mobile device

可随身携带并能够随时接入移动通信网络的电子设备。

注：如手机、平板电脑、笔记本或其他专用设备。

3.3

移动签名　mobile signature

使用移动设备中的专用安全模块对数据进行电子签名的通用方法。

3.4

移动签名服务　mobile signature service

在移动设备上使用专用安全模块实现电子签名的服务。

3.5

移动签名服务平台　mobile signature service platform

向应用提供者和用户提供移动签名服务的功能实体。

3.6

移动签名设备　mobile signature device

移动设备中能够对电子签名完成处理的专用安全模块。