ICS 35.030
L 80

中华人民共和国国家标准

GB/T 40018—2021

信息安全技术　基于多信道的证书申请和应用协议

Information security technology—Certificate request and application protocol based on multiple channels

2021-04-30 发布　　2021-11-01 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:中国科学院数据与通信保护研究教育中心、中国科学院大学、浙江蚂蚁小微金融服务集团股份有限公司、北京信安世纪科技股份有限公司、联想(北京)有限公司、国民认证科技(北京)有限公司、数安时代科技股份有限公司、上海市数字证书认证中心有限公司、北京数字认证股份有限公司。

本标准主要起草人:牛莹姣、荆继武、高能、陈星、刘丽敏、汪宗斌、贾世杰、雷灵光、杨楠、郑昉昱、马原、王平建、吕娜、钱文飞、张永强、王天华、林雪焰。

引　言

本标准从信息安全角度提出了基于多信道的证书申请和应用协议，多信道包括近场信道和网络信道。近场信道指智能移动设备和证书认证系统终端或业务系统终端近距离连接的信道，如人工信道、光学信道、NFC 等。网络信道指证书认证系统或业务系统通过网络连接智能移动设备的信道。近场信道的特征是带宽小，不能进行大量数据传输，数据以明文形式传递，但是通过该信道发送和接收的数据较不易被窃听，且能通过面对面的方式进行通信双方身份的鉴别。本标准通过引入近场信道协同网络信道完成证书申请和应用能更加有效地抵御信道窃听、数据篡改、终端假冒等攻击。

信息安全技术　基于多信道的证书申请和应用协议

1　范围

本标准规定了利用智能移动设备进行证书申请和应用协议，包括证书申请协议、数字签名与验签协议、文件加解密协议。

本标准适用于多信道环境中应用系统的设计、开发、测试。

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 25069—2010　信息安全技术　术语

GB/T 37092—2018　信息安全技术　密码模块安全要求

GM/T 0014—2012　数字证书认证系统密码协议规范

3　术语、定义和缩略语

3.1　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。

3.1.1

近场信道　near field channel

智能移动设备和证书认证系统终端或业务系统终端近距离连接的信道。

示例：人工信道、光学信道、NFC 等。

3.1.2

网络信道　network channel

证书认证系统或业务系统通过网络连接智能移动设备的信道。

3.1.3

厂商 ID　vendor ID

应用服务器分配给智能移动设备开发厂商、表明智能移动设备开发厂商身份的唯一标识。

3.1.4

厂商私钥　vendor private key

智能移动设备开发厂商在智能移动设备中预先植入的用于证明厂商是否可信的密钥对中的私钥。

3.1.5

厂商公钥　vendor public key

智能移动设备开发厂商在智能移动设备中预先植入的用于证明厂商是否可信的密钥对中的公钥。

3.2　缩略语

下列缩略语适用于本文件。