ICS 35.040
L 80

中华人民共和国密码行业标准

GM/T 0074—2019

网上银行密码应用技术要求

Technical requirements on cryptographic application for internet banking

2019-07-12 发布　　2019-07-12 实施

国家密码管理局　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：天地融科技股份有限公司、国民技术股份有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司、中钞研究院、银行卡检测中心、成都卫士通信息产业股份有限公司、北京华大智宝电子系统有限公司。

本标准起草人：李明、牟宁波、杨贤伟、李美祥、汪宗斌、林雪焰、李向锋、平庆瑞、汪小八、张文科、张立廷、陈跃、何智、史晓峰。

引　言

网上银行是指银行通过互联网向客户提供金融服务的业务。作为对银行传统渠道的一种补充，网上银行的开展可以极大地降低银行的经营成本，增加业务交易量并获得收益，同时也可以为客户提供更便捷和创新的银行服务。对用户而言，网上银行没有时间和空间的限制，节省用户的使用成本，满足多种形式的需求，具有良好的发展趋势。然而，由于互联网的开放性和固有缺陷，与传统服务渠道相比，网上银行存在更大的安全隐患和安全威胁。

密码技术作为信息安全核心防护手段，已广泛应用于网上银行的安全建设中。因此，从技术层面对网上银行系统中密码技术的设计、实现与使用进行要求，具有重大的现实意义。

本标准根据国内网上银行业务特点及密码应用功能需求，制定网上银行业务密码应用技术要求，以促进国内网上银行密码应用的技术规范化与健康发展。

网上银行密码应用技术要求

1 范围

本标准规定了密码技术在网上银行业务中应用的相关要求，包括密码算法、密钥管理、证书管理、安全通道、密码设备及数字签名六个方面。

本标准适用于指导网上银行业务中密码技术相关安全功能的设计、实现和使用，对于网上银行系统中密码子系统的测试、管理可参照使用。

手机银行等系统中相关部分内容也可以参照本标准。

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 15843(所有部分) 信息技术 安全技术 实体鉴别

GB/T 19713 信息安全技术 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 28447 信息安全技术 电子认证服务机构运营管理规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

GM/T 0021 动态口令密码应用技术规范

GM/T 0022 IPSec VPN 技术规范

GM/T 0023 IPSec VPN 网关产品规范

GM/T 0024 SSL VPN 技术规范

GM/T 0025 SSL VPN 网关产品规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0029 签名验签服务器技术规范

GM/T 0030 服务器密码机技术规范

GM/T 0033 时间戳接口规范

GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范