ICS 35.040
L 80

中华人民共和国密码行业标准

GM/T 0072—2019

远程移动支付密码应用技术要求

Technical requirements for the applying of cryptography in remote mobile payment

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：北京创原天地科技有限公司、北京三未信安科技发展有限公司、中金金融认证中心有限公司、武汉天喻信息产业股份有限公司、神州融安科技（北京）有限公司、大唐微电子技术有限公司、飞天诚信科技股份有限公司、恒宝股份有限公司、北京支付通电子设备有限公司、成都三零瑞通移动通信有限公司、上海动联信息技术股份有限公司、杭州信雅达科技有限公司。

本标准主要起草人：方恒禄、肖青海、高志权、李达、朱丹、岳云龙、陶涛、朱鹏飞、赵李明、王彦峰、徐青、裴婷、蒋晓旭、董学飞。

引　言

随着移动互联网应用和移动智能终端的飞速发展，移动支付业务以其方便快捷的服务越来越得到人们的关注。目前，金融行业内已有中国人民银行主导制定的一系列移动支付相关标准，但是缺少对移动支付中密码应用的具体要求。本标准作为补充，提出对远程移动支付中密码应用的技术要求。移动支付主要分为远程支付和近场支付。在远程支付中，用户可以在任何时间、任何地点使用移动智能终端发起支付，但是由于交易金额较大，系统对安全性要求较高，安全问题越来越成为人们关注的焦点，并成为影响远程移动支付发展的重要因素之一。

考虑到远程移动支付涉及面广、业务种类繁多以及各商业银行和非金融支付机构的业务系统现状，本标准仅对目前支付业务中比较成熟的基于密码模块的安全密码服务进行规范，从密码应用的角度，对由移动智能终端发起并通过密码模块提供密码服务的远程支付方式做了相应的密码应用技术要求。

远程移动支付密码应用技术要求

1 范围

本标准描述了基于密码模块的远程移动支付密码应用架构，规定了远程移动支付的密码安全要素以及密码应用的技术要求。

本标准适用于对基于密码模块的远程移动支付中密码应用需要考虑的密码安全要素以及遵循的技术要求提供指导。

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 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

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0008 安全芯片密码检测准则

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

JR/T 0095—2012 中国金融移动支付 应用安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动终端 mobile device

具有移动通信能力的终端设备，包括手机、平板电脑等。

3.2

密码模块 cryptographic module

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

3.3

移动支付 mobile payment

允许用户使用移动终端对所消费的商品或服务进行账务支付的一种服务方式，主要分为近场支付和远程支付两种。

3.4

远程移动支付 remote mobile payment

移动终端通过无线通信网络接入，直接与后台服务器进行交互完成交易处理的支付方式。