ICS 35.040
L 80

中华人民共和国密码行业标准

GM/T 0073—2019

手机银行信息系统密码应用技术要求

Cryptography technical requirements for mobile banking information systems

2019-07-12 发布　　2019-07-12 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
手机银行信息系统密码应用技术要求
GM/T 0073—2019
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019年10月第一版
*
书号:155066·2-34606

目　　次

前　言

本标准是信息安全等级保护银行业金融机构密码技术应用要求相关系列标准之一。与本标准相关的系列标准包括：

——GM/T 0075—2019《银行信贷信息系统密码应用技术要求》

——GM/T 0076—2019《银行卡信息系统密码应用技术要求》

——GM/T 0077—2019《银行核心信息系统密码应用技术要求》

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：国家密码管理局商用密码检测中心、中金金融认证中心有限公司、中国银行股份有限公司、中国民生银行股份有限公司。

本标准主要起草人：邓开勇、谢宗晓、张大健、马瑶瑶、介磊、郭晶莹、张众、杨辰。

引　言

本标准与GM/T 0054—2018《信息系统密码应用基本要求》、GM/T 0077—2019《银行核心信息系统密码应用技术要求》、GM/T 0076—2019《银行卡信息系统密码应用技术要求》、GM/T 0075—2019《银行信贷信息系统密码应用技术要求》共同构成了信息系统安全等级保护密码技术要求的相关配套标准。其中GM/T 0054—2018《信息系统密码应用基本要求》是基础性标准，本标准、GM/T 0077—2019、GM/T 0076—2019及GM/T 0075—2019是在GM/T 0054—2018基础上的进一步细化和扩展。

本标准在GM/T 0054—2018《信息系统密码应用基本要求》、GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》、JR/T 007—2012《金融行业信息系统信息安全等级保护实施指引》等技术类标准的基础上，根据现有技术的发展水平，提出和规定了不同安全保护等级的手机银行系统保护要求，包括安全技术要求和安全管理要求，本标准适用于指导不同安全保护等级的银行业金融机构手机银行系统中密码技术的安全建设、安全使用与监督管理。

银行业金融机构应依据信息安全等级保护有关技术标准与国家、行业主管部门要求，对手机银行系统开展包括系统定级在内的信息安全等级保护工作。目前手机银行系统安全级别为二级、三级，暂不存在安全级别为一级、四级和五级的系统，故本标准暂不对一级信息系统、四级信息系统和五级信息系统提出具体的密码技术要求。

手机银行信息系统应依据GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》，以及国家主管部门有关要求，进行定级。等级确定后，依据本标准选择相应级别的密码技术保护措施。

在本标准文本的各类安全要求中，“可”表示可以、允许；“宜”表示推荐、建议；“应”表示应该。

手机银行信息系统密码应用技术要求

1 范围

本标准在GM/T 0054—2018、JR/T 007—2012等标准基础上，结合手机银行信息系统的特点及该类信息系统等级保护安全建设工作中密码技术的应用需要，从密码安全技术要求、密钥安全与管理要求、安全管理要求等三方面，对不同安全保护等级的手机银行信息系统中密码应用提出具体的要求。

本标准适用于指导、规范和评估手机银行信息系统中的商用密码应用。

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 20547.2—2006 银行业务 安全加密设备(零售) 第2部分：金融交易中设备安全符合性检测清单

GB/T 21078.1—2007 个人识别码的管理与安全 第1部分：ATM和POS系统中联机PIN处理的基本原则和要求

GB/T 21079.1 银行业务 安全加密设备(零售) 第1部分：概念、要求和评估方法

GM/T 0028—2014 密码模块安全要求

GM/T 0036—2014 采用非接触卡的门禁系统密码应用指南

GM/T 0054—2018 信息系统密码应用基本要求

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 0001—2013界定的以及下列术语和定义适用于本文件。

3.1

事件 event

与信息系统安全策略相冲突的进程。

3.2

移动终端 mobile device

具有移动通讯能力的终端设备，包括手机、PDA等，在本标准中主要指手机。

3.3

密钥传输设备 devices of key

具有传输密钥功能的设备。

3.4

移动支付 mobile payment

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。