ICS 35.040
L 80

GM

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

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。

3.5

近场支付　proximity payment

移动终端通过实体受理终端在交易现场以联机或脱机方式完成交易处理的支付方式。

3.6

远程支付　remote 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。

3.7

短信支付　SMS payment

预先建立手机号码与支付账户的绑定关系，通过短信进行支付的业务。

3.8

安全单元　secure element；SE

在移动支付中负责交易关键数据的安全存储和运算功能的部件。

3.9

密钥组件　key module

将完整密钥分块分别保存的部分。

3.10

手机银行系统　mobile banking system

通过网络将客户的移动终端与银行连接，客户通过手机客户端的方式发出交易指令，在终端界面上直接完成各种金融服务的一种业务系统。

3.11

生物识别　biometric authentication

利用人体固有的生理特性，如指纹、虹膜，与行为特征来进行个人身份的鉴定，是使用密码技术进行身份认证的辅助认证措施。

4　缩略语

下列缩略语适用于本文件。

ECC　椭圆曲线密码算法(elliptic curve cryptography algorithm)

OTP　一次性口令(One-Time Password)

PIN　个人标识码(Personal Identification Number)

RSA　一种基于大整数因子分解的公钥密码算法(Rivest Shamir Adleman)

SE　安全单元(Secure Element)

SM2　一种椭圆曲线公钥密码算法(SM2 algorithm)

SSL　安全套接层(Secure Sockets Layer)

TLS　安全传输层协议(Transport Layer Security)

VPN　虚拟专用网络(Virtual Private Network)

5　手机银行信息系统模型

典型的手机银行信息系统由手机银行移动应用的客户端及服务端组成，如图 1 所示。

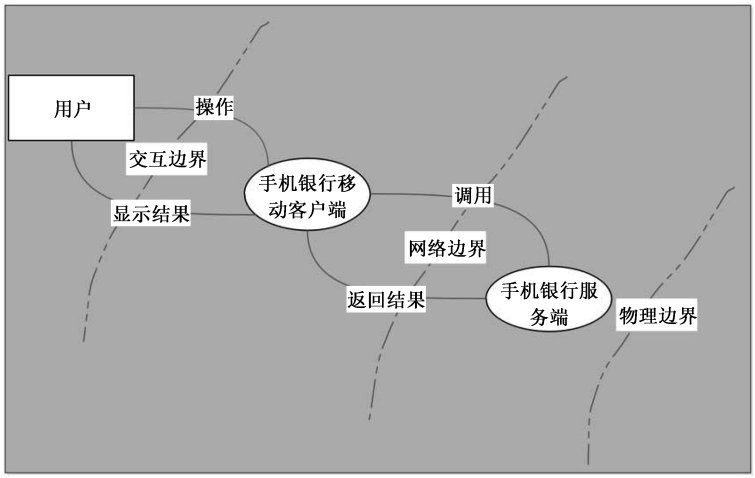

图 1　手机银行的基本架构

用户：具有对手机银行的移动应用客户端进行操作行为的主体。

手机银行移动客户端：指手机银行的移动应用客户端程序，能够为用户提供本地电子银行服务。

手机银行服务端：指手机银行移动客户端对应的能够提供针对性服务的服务器端，本标准规定的服务端既包含软件程序，也包含承载和运行程序的硬件设备。

边界：指主体之间互联互通的界限，包括交互边界、网络边界、物理边界等。

6　密码应用基本要求和密码应用功能要求

手机银行信息系统密码应用基本要求和密码应用功能要求遵照 GM/T 0054—2018 第 5 章、第 6 章的要求。

7　手机银行信息系统密码技术安全保护二级要求[1)]

7.1　基本技术要求

应按照 GM/T 0054—2018 中第二级指标要求。

7.2　密码技术安全要求

7.2.1　物理和环境安全

7.2.1.1　总则

参照 GM/T 0054—2018 中物理和环境安全密码应用总则。

7.2.1.2　密码硬件安全

“密码硬件安全”“物理环境安全”和“电子门禁系统”是手机银行信息系统“物理和环境安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“物理和环境安全-密码硬件安全”指标做如下要求：

1)　该级别的全部安全要求与其他级别的对比请参照附录 A 安全要求对照表，下同。

a） 系统的专用硬件或固件以及密码设备应具有有效的物理安全保护措施；

注：本标准中“有效措施”是指能满足“保证项”要求的手段或能实现系统设定的安全目标的方法，以下注释同。

b） 系统的专用硬件或固件以及密码设备应满足运行环境可靠性要求。

7.2.1.3 物理环境安全

“密码硬件安全”“物理环境安全”和“电子门禁系统”是手机银行信息系统“物理和环境安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“物理和环境安全-物理环境安全”指标做如下要求：

宜使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。

7.2.1.4 电子门禁系统

“密码硬件安全”“物理环境安全”和“电子门禁系统”是手机银行信息系统“物理和环境安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“物理和环境安全-电子门禁系统”指标做如下要求：

a） 宜使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性；

b） 采用的门禁系统资质、架构、部署应符合 GM/T 0036—2014 技术规范；

c） 宜制定相应规章制度以确保门禁系统使用的合规性、正确性、有效性。

7.2.2 网络和通信安全

7.2.2.1 总则

参照 GM/T 0054—2018 中网络和通信安全密码应用总则。

7.2.2.2 通信安全

“通信安全”和“身份鉴别”是手机银行信息系统“网络和通信安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“网络和通信安全-通信安全”指标做如下要求：

a） 为防止访问通讯数据被篡改、截获、假冒和重用，宜使用密码技术的完整性服务、机密性服务和真实性服务对网络边界、系统资源访问控制信息进行保护；

b） 在进行数据传输时，宜使用数字证书、加密解密等密码技术，建立安全的传输层会话通道。

7.2.2.3 身份鉴别

“通信安全”和“身份鉴别”是手机银行信息系统“网络和通信安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“网络和通信安全-身份鉴别”指标做如下要求：

a） 在对登录网络设备的用户进行身份鉴别时，为防止鉴别信息被重用和假冒，宜使用密码技术的真实性服务对鉴别信息进行防重用和防假冒保护，其密码功能应确保正确、有效；

b） 网络设备系统管理用户身份标识应具有不易被冒用的特点，关键网络设备的静态密码应在6位以上，由字母、数字、符号等混合组成并定期更换；

c） 信息系统对通过身份认证后的实体，应使用密码技术生成唯一的随机的标识符，并确保该功能正确、有效。

7.2.3 设备和计算安全

7.2.3.1 总则

参照 GM/T 0054—2018 中设备和计算安全密码应用总则。

7.2.3.2 审计记录

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“设备和计算安全-审计记录”指标做如下要求：

为防止审计记录被非法修改，宜使用密码技术的完整性服务对审计记录进行完整性保护，其密码功能应确保正确、有效。

7.2.3.3 身份鉴别

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“设备和计算安全-身份鉴别”指标做如下要求：

a) 在身份鉴别机制中，为防止鉴别信息被假冒和重用，宜使用密码技术的真实性服务对鉴别信息进行防假冒和重用保护，其密码功能应确保正确、有效；
b) 宜使用安全散列函数对用户的口令进行处理，然后再进入身份鉴别模块，散列函数应确保正确、有效；
c) 在进行关键业务流程，如转账、交易、修改资料时，宜使用多种密码技术保证用户身份的真实性、有效性；
d) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，关键系统的静态口令应在6位以上并由字母、数字、符号等混合组成并定期更换。

7.2.3.4 验证码与动态口令

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“设备和计算安全-验证码与动态口令”指标做如下要求：

a) 使用手机短信或其他渠道发送验证码时，应使用正确的密码技术，确保发送的动态口令完全随机，不可预测；
b) 使用手机短信或其他渠道发送验证码时，应确保不会泄露验证码的内容；
c) 如果使用OTP令牌进行身份校验，应使用正确的密码技术，确保OTP完全随机，不可预测。

7.2.3.5 密码模块

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“设备和计算安全-密码模块”指标做如下要求：

应使用符合GM/T 0028—2014的二级及以上密码模块或通过国家密码管理机构核准的硬件密码产品实现密码运算和密钥管理：

a) 系统的专用硬件或固件以及密码设备应实现授权控制、非授权访问的检测、运行状态指示等安全功能，保证密码模块能够在核准的工作模式下正确运行；
b) 系统的专用硬件或固件以及密码设备应能够防止非授权地泄露模块的内容或关键安全参数；
c) 系统的专用硬件或固件以及密码设备应能够防止对密码模块和密码算法进行非授权或检测不到的修改。

7.2.4 应用和数据安全

7.2.4.1 总则

参照 GM/T 0054—2018 中应用和数据安全密码应用总则。

7.2.4.2 数据传输

“数据传输”“数据存储”和“终端应用”是手机银行信息系统“应用和数据安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“应用和数据安全-数据传输”指标做如下要求：

a) 在数据传输安全方面，可使用密码技术的完整性服务实现对重要用户数据在传输过程中的完整性校验，其密码功能应确保正确、有效；

b) 通过客户端发送的报文的关键要素宜利用密码技术进行数字签名，以确保支付内容的真实性和不可抵赖性；

c) 对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性；

d) 客户端到远程支付系统的 SSL/TLS 版本应符合 GM/T 0024 的要求；用于签名的 RSA 密钥长度应不低于 1 024 位；用于签名的 ECC 密钥长度应不低于 256 位或 SM2 密钥长度应不低于 256 位。

7.2.4.3 数据存储

“数据传输”“数据存储”和“终端应用”是手机银行信息系统“应用和数据安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“应用和数据安全-数据存储”指标做如下要求：

在数据存储安全方面，可使用密码技术的完整性服务来实现对系统管理数据、鉴别信息、关键配置信息和重要业务数据在存储过程中完整性的检测，其密码功能应确保正确、有效。

7.2.4.4 终端应用

“数据传输” “数据存储”和“终端应用”是手机银行信息系统“应用和数据安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“应用和数据安全-终端应用”指标做如下要求：

a) 移动终端应用不应明文或编码存储用户的口令、支付密码、PAC、CVV 等敏感信息；

b) 移动终端应用应对于密码、PAC、CVV 等敏感数据进行脱敏处理；

c) 移动终端应用在处理用户输入的敏感数据时，如口令、支付密码等，宜采取安全措施，保证敏感数据的机密性，确保不被非授权获取；

d) 移动终端应用不应将用户的口令、个人信息、PAC、CVV 等敏感数据泄露给其他实体，如本地其他进程、互联网数据服务器等。

7.2.5 密码配用策略要求

7.2.5.1 密码算法配用

“密码算法配用”“密码协议使用”和“密码设备使用”是手机银行信息系统“密码配用策略要求”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密码配用策略要求-密码算法配用”指标做如下要求：

宜采用国家密码管理机构批准使用的算法。

7.2.5.2 密码协议使用

“密码算法配用”“密码协议使用”和“密码设备使用”是手机银行信息系统“密码配用策略要求”的组

成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密码配用策略要求-密码协议使用”指标做如下要求：

宜采用通过国家密码管理机构安全性评审的密码协议。

7.2.5.3 密码设备使用

“密码算法配用”“密码协议使用”和“密码设备使用”是手机银行信息系统“密码配用策略要求”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密码配用策略要求-密码设备使用”指标做如下要求：

a) 宜选用国家密码管理机构批准的密码设备；
b) 信源加密、完整性校验、身份鉴别应选用可信密码模块、智能密码钥匙、智能 IC 卡、密码卡、密码机等密码设备；
c) 信道加密应选用链路密码机、网络密码机、VPN、VPN 安全网关等密码设备；
d) SE 模块密钥对可在 SE 中生成或在硬件加密设备中生成，再写入 SE 模块中。SE 模块密钥对若在硬件加密设备中生成，要保证密钥写入 SE 模块后，不会留存任何备份。应充分保证产生的密钥数据不会重复。

7.3 密钥安全与管理要求

7.3.1 总则

参照 GM/T 0054—2018 中密钥管理总则。

7.3.2 密钥安全

7.3.2.1 密钥生成

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥安全-密钥生成”指标做如下要求：

a) 应使用符合国家标准的随机数发生器产生密钥；
b) 密钥应在密码设备内部生产，不得以明文方式出现在密码设备之外；
c) 应具备检查和剔除弱密钥的能力；
d) 密钥对生成应由密钥对的所有者或其代理方完成；
e) 非对称密钥对的生成方式应保证私钥的机密性以及公钥的完整性；对用于不可否认服务的非对称密钥对的生成，应能向第三方证明公钥的完整性。

7.3.2.2 密钥存储

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥安全-密钥存储”指标做如下要求：

a) 密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；
b) 应通过口令保护系统中存储的密钥或其组件。

7.3.2.3 密钥分发

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥安全-密钥分发”指标做如下要求：

密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

7.3.2.4 密钥使用

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥安全-密钥使用”指标做如下要求：

a) 对于公钥密码体制，在使用公钥之前应对其进行验证。

b) 在非对称密码系统中，密钥对中的每个密钥都用于单独的功能。除非另有说明，密钥对的两个密钥应满足下述要求：

——严格禁止私钥的非授权使用；

——公钥只有在其真实性与完整性通过验证后才可使用；

——应防止继续使用被怀疑泄露的密钥。

c) 在对称密码系统中，应满足下述要求：

——一个密钥最多只应被两个通信方使用；

——应防止继续使用被怀疑泄露的密钥。

7.3.3 密钥管理

7.3.3.1 密钥的导入与导出

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥管理-密钥的导入与导出”指标做如下要求：

a) 应在密钥管理员、密码设备操作员在场的情况下进行密钥导入与导出，安全审计员也宜在场，并记录操作备忘录，提交安全审计日志、安全审计文档等。

b) 密钥的传输、导入与导出过程应按照双重控制、密钥分割的原则进行。如需使用密钥组件，则所需的密钥组件应由密钥组件持有者分别导入。

c) 在传输和导入密钥时，应确认：

——只有当密码设备至少鉴别了两位以上的被授权人身份时，如通过口令的方式，才可以传输密钥。对于人工方式分发的密钥，应使用管理流程，如纸质授权的方式，对被授权人的身份进行鉴别。

——只有确信密码设备在使用前没有受到任何可能导致密钥或敏感数据泄露的篡改时，才可以将私钥导入到密码设备中。

——只有确信密码设备接口处没有安装可能导致传输密钥的任何元素泄露的窃听装置时，才可以在密码设备之间进行私钥的传输。

——应使用密码设备在生成密钥和使用密钥的设备间传输私钥。

——在将密钥导入到目标设备后，密钥传送设备不应保留任何可能泄露该密钥的信息。

——当使用密钥传送设备时，密钥(如果使用显式密钥标识符，还包括密钥标识符)应从产生密钥的密码设备传输到密钥传送设备，这一设备应被物理运输到实际使用密钥的密码设备所在处。

d) 在使用密钥组件时，应确认：

——构成密钥的密钥组件应通过手工或密钥传输设备导入或导出到设备中，密钥组件的传输过程不应向任何非授权的个人泄露密钥组件的任何部分。

——当密钥组件以可读的形式分发时，每一个密钥组件都应通过在开启前不会泄露密钥组件值的密钥信封进行分发。

——在输入密钥组件之前，应检查密钥信封或密码设备有无被篡改的迹象。如果组件之一被

篡改，这一套密钥组件就不应被使用，且应遵循 GB/T 21078.1—2007 中说明的程序将其销毁。

——密钥组件应由密钥组件的每一个持有者单独输入并验证密钥组件的输入是否正确。

e) 密钥管理员应负责检查密钥导入与导出时所生成校验值的一致性。

f) 当密钥组件输入密码设备后，密钥信封应加以销毁或密封在另一个防篡改的密钥信封内，以备将来可能的使用。

g) 密钥注入后，将存储备份密钥的介质保存至密码信封中，由专人监督确认后，锁入保险柜中。

7.3.3.2 密钥的存储与保管

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥管理-密钥的存储与保管”指标做如下要求：

a) 应制定密钥存储与保管的文档化规定；

b) 密钥资料须保存在保险柜内，保险柜钥匙由密钥管理员负责，保证只有指定的密钥管理人员能打开保管的设备；

c) 密码只能存储在符合 GB/T 20547.2—2006 中规定的密码设备中；

d) 若使用密钥组件，应确保密钥组件通过特定的密钥信封或密钥传输设备传送给被授权人。密钥信封的印刷，应保证信封在开启后才能看到密钥组件。信封应只显示将密钥信封递交给授权人所必需的最少信息。密钥信封的结构应使得意外的或欺骗性的开启易于被接收方发现，如果出现这种情况，密钥组件就不应再被使用。

7.3.3.3 密钥的使用与更换

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥管理-密钥的使用与更换”指标做如下要求：

a) 密钥应明确用途，并按用途正确使用；

b) 应对密钥使用各环节建立跟踪与核查制度；

c) 在密钥使用过程中，应有安全措施防止密钥的泄露和替换；

d) 在密钥使用过程中，应按照密钥更换周期要求更换密钥，密钥更换允许中断系统运行；

e) 密钥泄露时，应立即停止使用，并启动相应的应急处理和响应措施；

f) 对密码机、密码管理设备的系统管理员密码、用户密码、用户权限进行管理，一旦发生泄漏或者权限失控应启动核查跟踪程序，根据权限失控的情况进行事件等级评估，并适时更新相关密钥。

7.3.3.4 密钥的备份与恢复

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“密钥管理-密钥的备份与恢复”指标做如下要求：

a) 应建立密钥恢复与修正工作流程，明确密钥替换、修正的触发情况，规定密钥替换、修正的标准作业流程，并保留密钥替换、修正作业记录；

b) 如怀疑密钥泄露或设备的安全性受到威胁，则应将密钥撤回或更换（例如销毁或废止）；

c) 应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；

d) 密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等；

e) 应有安全措施防止密钥的泄露和替换；
f) 应确保密钥储存位置和形式的安全，限制密钥的访问权限；
g) 如果根据攻击者已经获得的信息，可以确认已经发生了未经授权的密钥替换，则应遵循下列步骤进行密钥更换：
——擦除任何已经确认被替代的存储密钥的加密版本，确认现存的所有加密的密钥是否合法。如果有不合法的密钥，则应被删除。
——由某个新的密钥加密密钥对合法存储的加密的密钥重新加密。
——将旧的密钥加密密钥从所有运行位置上删除。

7.4 安全管理要求

7.4.1 概述

应根据国家相关密码管理政策，遵循金融业数据安全保密的国家标准，结合组织实际情况，设立密钥管理人员、安全审计人员、密码设备操作人员岗位。

7.4.2 安全管理制度

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“安全管理要求-安全管理制度”指标做如下要求：

a) 应对所有密钥的生成、存储、注入、使用、分发、备份、恢复、归档、销毁等操作建立管理制度；
b) 应建立密码设备、密码系统的标准作业规程，明确各步骤的操作标准流程，各阶段操作应生成作业表格，并归档留存；
c) 定期检查密码设备与密钥系统的安全管理状况，依据密钥安全管理制度要求，填报有关表格和报告。

7.4.3 人员管理要求

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“安全管理要求-人员管理要求”指标做如下要求：

a) 依据主管部门要求与组织实际情况，应配备一定数量的密钥管理人员、安全审计人员、密码设备操作人员等岗位人员，上述岗位人员不可互相兼任；
b) 应配备专职密钥管理人员，该岗位人员不可由其他岗位人员兼任；
c) 应建立岗位责任制度，明确相关人员在密码设备管理与密钥系统管理中的职责和权限，相关设备与系统的管理和使用账号不得多人共用；
d) 密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理；
e) 应对密码管理、密码设备操作建立人员选拔制度和审查制度，确定专职人员承担相关工作，对相关人员实施必要的审查；
f) 应建立人员考核制度，定期进行岗位人员考核；
g) 应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

7.4.4 密码设备管理

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“安全管理要

求-密码设备管理”指标做如下要求：

a） 系统应建立密码设备安全管理制度；

b） 系统应采用经国家密码管理机构认证的密码产品；

c） 密码设备操作人员应经过专业培训和考核；

d） 系统应配备密码设备维护人员和管理人员。

7.4.5 使用密码的业务终端要求

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“安全管理要求-使用密码的业务终端要求”指标做如下要求：

a） 终端设备密码模块应符合国家密码管理机构与行业主管部门相关规定和标准；

b） 终端设备应通过测试满足密码运算的基本功能和性能要求；

c） 终端设备密钥与密码的操作应依据操作手册和操作规程进行；

d） 终端设备报废时应将存储在该设备中的密钥删除和销毁，销毁终端密码应用相关软件。

8 手机银行信息系统密码技术安全保护三级要求

8.1 基本要求

应满足 GM/T 0054—2018 中第三级指标要求。

8.2 密码技术安全要求

8.2.1 物理和环境安全

8.2.1.1 总则

参照 GM/T 0054—2018 中物理和环境安全密码应用总则。

8.2.1.2 密码硬件安全

“密码硬件安全”“物理环境安全”和“电子门禁系统”是手机银行信息系统“物理和环境安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“物理和环境安全-密码硬件安全”指标做如下要求：

a） 系统的专用硬件或固件以及密码设备应具有有效的物理安全保护措施；

注：本标准中“有效措施”是指能满足“保证项”要求的手段或能实现系统设定的安全目标的方法，以下注释同。

b） 系统的专用硬件或固件以及密码设备应满足运行环境可靠性要求。

8.2.1.3 物理环境安全

“密码硬件安全”“物理环境安全”和“电子门禁系统”是手机银行信息系统“物理和环境安全”的组成部分。在手机银行信息系统密码技术安全保护二级要求中，对“物理和环境安全-物理环境安全”指标做如下要求：

应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。

8.2.1.4 电子门禁系统

“密码硬件安全”“物理环境安全”和“电子门禁系统”是手机银行信息系统“物理和环境安全”的组成

部分。在手机银行信息系统密码技术安全保护三级要求中，对“物理和环境安全-电子门禁系统”指标做如下要求：

a) 在电子门禁系统中，应使用密码技术的完整性服务保证电子门禁系统进出记录的完整性，其密码功能应确保正确、有效；
b) 在电子门禁系统中，应使用密码技术的完整性服务保证电子门禁系统进出记录的完整性，其密码功能应确保正确、有效；
c) 门禁系统要求读卡方式宜使用非接触读卡方式，避免使用磁条卡；
d) 当门禁系统检测到无法识别的卡片尝试非法进入时，应提供警告信息并能对非法尝试的卡片进行定位；
e) 采用的门禁系统资质、架构、部署应符合 GM/T 0036—2014 要求的技术规范；
f) 宜制定相应规章制度以确保门禁系统使用的合规性、正确性、有效性。

8.2.2 网络和通信安全

8.2.2.1 总则

参照 GM/T 0054—2018 中网络和通信安全密码应用总则。

8.2.2.2 通信安全

“通信安全”和“身份鉴别”是手机银行信息系统“网络和通信安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“网络和通信安全-通信安全”指标做如下要求：

a) 为防止访问通讯数据被篡改、截获、假冒和重用，应使用密码技术的完整性服务、机密性服务和真实性服务对网络边界、系统资源访问控制信息进行保护，并对其中关键敏感数据，如 PAC、CVV 等进行单独加密，其密码功能应确保正确、有效。
b) 在进行数据传输时，应使用数字证书、加密解密等密码技术，建立安全的传输层会话通道。传输数据的主体应对客体的身份信息进行鉴别，保障数据的机密性。
c) 在使用安全传输层协议进行数据传输时，主体应对客体的身份信息进行鉴别，保障数据的机密性。
d) 为防止通过控制通信的一端获得数据传输内容，在通信时应对其中关键敏感数据，如 PAC、CVV 等进行单独加密，其密码功能应确保正确、有效。
e) 应使用密码技术的抗抵赖服务来提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖，其密码功能应确保正确、有效。
f) 对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性。

8.2.2.3 身份鉴别

“通信安全”和“身份鉴别”是手机银行信息系统“网络和通信安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“网络和通信安全-身份鉴别”指标做如下要求：

a) 在对登录网络设备的用户进行身份鉴别时，为防止鉴别信息被重用和假冒，应使用密码技术的真实性服务对鉴别信息进行防重用和防假冒保护，其密码功能应确保正确、有效；
b) 网络设备系统管理用户身份标识应具有不易被冒用的特点，关键网络设备的静态密码应在 6 位以上，由字母、数字、符号等混合组成并定期更换；
c) 应设置鉴别警示信息，当出现越权访问或尝试非法访问时，系统会自动提示未授权访问；
d) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不易伪造的，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息；
e) 若使用短信验证码或 OTP 进行身份认证，应确保验证功能正确、有效，不可通过其他方式绕过

验证码或 OTP 的校验。

8.2.3 设备和计算安全

8.2.3.1 总则

参照 GM/T 0054—2018 中设备和计算安全密码应用总则。

8.2.3.2 审计记录

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“设备和计算安全-审计记录”指标做如下要求：

在审计记录方面，为防止审计记录被非法修改，应使用密码技术的完整性服务对审计记录进行完整性保护，其密码功能应确保正确、有效。

8.2.3.3 身份鉴别

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“设备和计算安全-身份鉴别”指标做如下要求：

a) 在身份鉴别机制中，为防止鉴别信息被假冒和重用，应使用密码技术的真实性服务对鉴别信息进行防假冒和重用保护，其密码功能应确保正确、有效。
b) 宜使用安全散列函数对用户的口令进行处理，然后再进入身份鉴别模块，散列函数应确保正确、有效。
c) 在进行关键业务流程，如转账、交易、修改资料时，宜使用多种密码技术保证用户身份的真实性、有效性。如使用生物识别进行身份认证，则应将其作为非密码技术的鉴别因子。
d) 用户通过移动终端登录手机银行时，需要输入登录密码，且登录系统后长时间无操作，再次进入系统需要重新输入密码。

8.2.3.4 验证码与动态口令

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“设备和计算安全-验证码与动态口令”指标做如下要求：

a) 使用手机短信或其他渠道发送验证码时，应使用正确的密码技术，确保发送的动态口令完全随机，不可预测；
b) 使用手机短信或其他渠道发送验证码时，应确保不会泄露验证码的内容；
c) 如果使用 OTP 令牌进行身份校验，应使用正确的密码技术，确保 OTP 完全随机，不可预测；
d) 使用手机短信或其他渠道发送验证码时，应确保每个验证码只能在有限的时间内使用一次；
e) 如果使用 OTP 令牌进行身份校验，应确保每个 OTP 只能在有限的时间内使用一次。

8.2.3.5 密码模块

“审计记录”“身份鉴别”“验证码与动态口令”和“密码模块”是手机银行信息系统“设备和计算安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“设备和计算安全-密码模块”指标做如下要求：

宜使用符合 GM/T 0028—2014 的三级及以上密码模块或通过国家密码管理机构核准的硬件密码产品实现密码运算和密钥管理：

a) 系统的专用硬件或固件以及密码设备应实现授权控制、非授权访问的检测、运行状态指示等安

全功能，保证密码模块能够在核准的工作模式下正确运行；

b) 系统的专用硬件或固件以及密码设备应能够防止非授权地泄露模块的内容或关键安全参数；

c) 系统的专用硬件或固件以及密码设备应能够防止对密码模块和密码算法进行非授权或检测不到的修改；

d) 系统的专用硬件或固件以及密码设备应能检测出密码模块运行中的错误，并防止这些错误非授权地公开、修改或使用关键安全参数。

8.2.4 应用和数据安全

8.2.4.1 总则

参照 GM/T 0054—2018 中应用和数据安全密码应用总则。

8.2.4.2 数据传输

“数据传输”“数据存储”和“终端应用”是手机银行信息系统“应用和数据安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“应用和数据安全-数据传输”指标做如下要求：

a) 在数据传输安全方面，宜使用密码技术的完整性服务实现对重要用户数据在传输过程中的完整性校验，其密码功能应确保正确、有效；

b) 对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性；

c) 通过客户端发送的关键报文应使用密码技术进行数字签名，以确保报文的真实性和不可抵赖性；

d) 应使用交易信息的安全通道传输协议(SSL/TLS，且应为 TLS1.0/SSL3.0 以上版本)进行加密传输；

e) 用于签名的 RSA 密钥长度应大于 1 024 位；用于签名的 ECC 密钥长度应大于 256 位或 SM2 密钥长度应大于 256 位。

8.2.4.3 数据存储

“数据传输”“数据存储”和“终端应用”是手机银行信息系统“应用和数据安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“应用和数据安全-数据存储”指标做如下要求：

a) 在数据存储安全方面，宜使用密码技术的机密性服务实现敏感信息的机密性存储，其密码功能应确保正确、有效；

b) 宜使用密码技术的完整性服务来实现对系统管理数据、鉴别信息、关键配置信息和重要业务数据在存储过程中完整性的检测，其密码功能应确保正确、有效。

8.2.4.4 终端应用

“数据传输”“数据存储”和“终端应用”是手机银行信息系统“应用和数据安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“应用和数据安全-终端应用”指标做如下要求：

a) 移动终端应用不应明文或编码存储用户的口令、支付密码、PAC、CVV 等敏感信息；

b) 移动终端应用应对于密码、PAC、CVV 等敏感数据进行脱敏处理；

c) 移动终端应用在处理用户输入的敏感数据时，如口令、支付密码等，宜采取安全措施，保证敏感数据的机密性，确保不被非授权获取；

d) 移动终端应用不应将用户的口令、个人信息、PAC、CVV 等敏感数据泄露给其他实体，如本地其他进程、互联网数据服务器等；

e) 宜使用密码技术的完整性服务来实现重要程序完整性校验，其密码功能应确保正确、有效。

8.2.5 密码配用策略要求

8.2.5.1 密码算法配用

“密码算法配用”“密码协议使用”和“密码设备使用”是手机银行信息系统“密码配用策略要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密码配用策略要求-密码算法配用”指标做如下要求：

应采用国家密码管理机构批准使用的算法。

8.2.5.2 密码协议使用

“密码算法配用”“密码协议使用”和“密码设备使用”是手机银行信息系统“密码配用策略要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密码配用策略要求-密码协议使用”指标做如下要求：

应采用通过国家密码管理机构安全性评审的密码协议。

8.2.5.3 密码设备使用

“密码算法配用”“密码协议使用”和“密码设备使用”是手机银行信息系统“密码配用策略要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密码配用策略要求-密码设备使用”指标做如下要求：

a) 应选用国家密码管理机构认证核准的密码设备。
b) 信源加密、完整性校验、身份鉴别、抗抵赖应选用可信密码模块、智能密码钥匙、智能 IC 卡、密码卡、密码机等密码设备。
c) 信道加密应选用链路密码机、网络密码机、VPN 安全网关等密码设备。
d) SE 模块密钥对可在 SE 中生成或在硬件加密设备中生成，再写入 SE 模块中。SE 模块密钥对若在硬件加密设备中生成，要保证密钥写入 SE 模块后，不会留存任何备份。应充分保证产生的密钥数据不会重复。
e) 需要配用独立的密钥管理系统或使用数字证书认证系统提供的密钥管理服务。

8.3 密钥安全与管理要求

8.3.1 总则

参照 GM/T 0054—2018 中密钥管理总则。

8.3.2 密钥安全

8.3.2.1 密钥生成

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥安全-密钥生成”指标做如下要求：

a) 应使用国家密码管理机构批准的硬件物理噪声源产生随机数；
b) 密钥应在密码设备内部生产，不得以明文方式出现在密码设备之外；
c) 应具备检查和剔除弱密钥的能力；
d) 密钥对生成应由密钥对的所有者或其代理方完成；
e) 非对称密钥对的生成方式应保证私钥的机密性以及公钥的完整性，并能够向第三方证明；
f) 若加密密钥与被加密的密钥形成上下级密钥关系，那么在密钥分级结构中，上级密钥与它们所

保护的密钥相比，安全级别应相等或更高；

g） 如果密钥对由不使用该密钥对的系统生成，则：

——在确认传输已经完成后，密钥对和所有相关的机密种子元素应被立即擦除；

——应确保私钥的完整性。

8.3.2.2 密钥存储

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥安全-密钥存储”指标做如下要求：

a） 密钥应加密存储在专用硬件中，并采取严格的安全防护措施，防止密钥被非法获取；

b） 应通过口令保护系统中存储的密钥或其组件；

c） 应采用两种或两种以上组合的鉴别技术，保护存储在密钥传输设备里的密钥组件，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。

8.3.2.3 密钥分发

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥安全-密钥分发”指标做如下要求：

密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施、应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

8.3.2.4 密钥使用

“密钥生成”“密钥存储”“密钥分发”和“密钥使用”是手机银行信息系统“密钥安全”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥安全-密钥使用”指标做如下要求：

a） 对于公钥密码体制，在使用公钥之前应对其进行验证；

b） 在非对称密码系统中，密钥对中的每个密钥都用于单独的功能。除非另有说明，密钥对的两个密钥应满足下述要求：

——严格禁止私钥的非授权使用；

——公钥只有在其真实性与完整性经过验证并且正确时才可以使用；

——应防止继续使用被怀疑泄露的密钥。

c） 在对称密码系统中，应满足下述要求：

——一个密钥最多只应被两个通信方使用；

——应防止继续使用被怀疑泄露的密钥。

8.3.3 密钥管理

8.3.3.1 密钥的导入与导出

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”和“密码的归档与销毁”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥管理-密钥的导入与导出”指标做如下要求：

a） 应在密钥管理员、安全审计员、密码设备操作员在场的情况下进行密钥注入，安全审计员也宜在场，并记录操作备忘录，提交安全审计日志、安全审计文档等。

b） 密钥的传输、导入与导出过程应按照双重控制、密钥分割的原则进行。如需使用密钥组件，则所需的密钥组件应由密钥组件持有者分别导入。

c） 在传输和导入密钥时，应确认：

——只有当密码设备至少鉴别了两位以上的被授权人身份时，如通过口令的方式，才可以传输

私钥。对于人工方式分发的密钥，应使用管理流程，如纸质授权的方式，对被授权人的身份进行鉴别。

——只有确信密码设备在使用前没有受到任何可能导致密钥或敏感数据泄露的篡改时，才可以将私钥导入到密码设备中。

——只有确信密码设备接口处没有安装可能导致传输密钥的任何元素泄露的窃听装置时，才可以在密码设备之间进行私钥的传输。

——在生成密钥和使用密钥的设备间传输私钥时所使用的设备应是密码设备。

——在将密钥导入到目标设备后，密钥传送设备不应保留任何可能泄露该密钥的信息。

——当使用密钥传送设备时，密钥（如果使用显式密钥标识符，还包括密钥标识符）应从产生密钥的密码设备传输到密钥传送设备，这一设备应被物理运输到实际使用密钥的密码设备所在处。

d) 在使用密钥组件时，应确认：

——构成密钥的密钥组件应通过手工或密钥传输设备导入到设备中，密钥组件的传输过程不应向任何非授权的个人泄露密钥组件的任何部分；

——当密钥组件以可读的形式分发时，每一个密钥组件都应通过在开启前不会泄露密钥组件值的密钥信封进行分发；

——在输入密钥组件之前，应检查密钥信封或密码设备有无被篡改的迹象。如果组件之一被篡改，这一套密钥组件就不应被使用，且应遵循 8.3.3.5 说明的程序将其销毁；

——密钥组件应由密钥组件的每一个持有者单独输入并验证密钥组件的输入是否正确。

e) 密钥管理员应负责检查密钥注入时所生成校验值的一致性。

f) 当密钥组件输入密码设备后，密钥信封应加以销毁或密封在另一个防篡改的密钥信封内，以备将来可能的使用。

g) 密钥导入或导出后，将存储备份密钥的介质保存至密码信封中，由安全审计员监督确认后，锁入保险柜中。

h) 密钥在导入或导出时应确定导入或导出的设备或者程序没有被非正常监控。

8.3.3.2 密钥的存储与保管

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”和“密码的归档与销毁”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥管理-密钥的存储与保管”指标做如下要求：

a) 应制定密钥存储与保管的文档化规定。

b) 密钥资料须保存在保险柜内，保险柜钥匙由密钥管理员负责，保证只有指定的密钥管理人员能打开保管的设备，并将该规定落实在岗位责任制中，定期对该规定的落实情况进行检查。

c) 密码只能存储在符合 GB/T 20547.2—2006 规定的密码设备中。

d) 若使用密钥组件，应确保密钥组件通过特定的密钥信封或密钥传输设备传送给被授权人。密钥信封的印刷，应保证信封在开启后才能看到密钥组件。信封应只显示将密钥信封递交给授权人所必须的最少信息。密钥信封的结构应使得意外的或欺骗性的开启易于被接收方发现，如果出现这种情况，密钥组件就不应再被使用。

e) 应具有密钥泄露时的应急处理和响应措施。

f) 应制定密钥存储与保管的文档化规定，对密钥的存储位置、传输方式、传输介质、导入与导出流程，以及存储于保管岗位人员与责任提出要求，定期对该规定的落实情况进行检查。

g) 明文密钥只能存储在符合 GB/T 21079.1 和 GB/T 20547.2—2006 规定的密码设备中。

8.3.3.3 密钥的使用与更换

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”和“密码的归

档与销毁”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥管理-密钥的使用与更换”指标做如下要求：

a) 密钥应明确用途，并按用途正确使用；
b) 应对密钥使用各环节建立跟踪与核查制度；
c) 在密钥使用过程中，应有安全措施防止密钥的泄露和替换；
d) 在密钥使用过程中，应按照密钥更换周期要求更换密钥，密钥更换允许中断系统运行；
e) 密钥泄露时，应立即停止使用，并启动相应的应急处理和响应措施；
f) 对密码机、密码管理设备的系统管理员密码、用户密码、用户权限进行管理，一旦发生泄漏或者权限失控应启动核查跟踪程序，根据权限失控的情况进行事件等级评估，并适时更新密钥，必要时应立即更换密钥；
g) 应对密钥使用各环节建立跟踪与核查制度，并在日常工作中定期进行密钥状态审查。

8.3.3.4 密钥的备份与恢复

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”和“密码的归档与销毁”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥管理-密钥的备份与恢复”指标做如下要求：

a) 应建立密钥恢复与修正工作流程，明确密钥备份与恢复的触发情况，规定密钥恢复、修正的标准作业流程，对关键节点建立授权审批制度，并保留授权审批文件以及密钥备份、恢复作业记录；
b) 如怀疑密钥泄露或设备的安全性受到威胁，则应将密钥撤回或更换（例如销毁或废止）；
c) 应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；
d) 密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等；
e) 应有安全措施防止密钥的泄露和替换；
f) 应确保密钥储存位置和形式的安全，限制密钥的访问权限；
g) 如果根据攻击者已经获得的信息，可以确认已经发生了未经授权的密钥替换，则应遵循下列步骤进行密钥更换：
   ——擦除任何已经确认被替代的存储密钥的加密版本，确认现存的所有加密的密钥是否合法。如果有不合法的密钥，则应被删除。
   ——由某个新的密钥加密密钥对合法存储的加密的密钥重新加密。
   ——将旧的密钥加密密钥从所有运行位置上删除。
h) 密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

8.3.3.5 密钥的归档与销毁

“密钥的导入与导出”“密钥的存储与保管”“密钥的使用与更换”“密钥的备份与恢复”和“密码的归档与销毁”是手机银行信息系统“密钥管理”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“密钥管理-密码的归档与销毁”指标做如下要求：

a) 应采取有效的安全措施，保证归档密钥的安全性和正确性；
b) 归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；
c) 密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；
d) 归档密钥应进行数据备份，并采用有效的安全保护措施；
e) 应具有紧急情况下销毁密钥的措施；
f) 当密码设备从服务中永久删除时，设备中存储的全部私钥都应被销毁；

g) 私钥的销毁可通过使用新密钥值或使用非机密值完全覆盖原密钥值实现，这样关于被擦除密钥的信息不会再保留；
h) 密钥销毁的操作要求不可逆，即不可从删除结果中恢复原密钥；
i) 密钥的销毁应在密钥管理员、安全审计员的监督下进行，并应对终止过程与结果进行记录，并归档保存；
j) 硬件密码机应具有密钥自动销毁功能，当密码机送检、维修或者运输时应启动自动销毁功能，保证硬件密码机中的所有密钥被彻底删除，在执行该类操作时，应在密钥管理员、安全审计员的监督下进行，确保密钥被销毁，并应对终止过程与结果进行记录，并归档保存；
k) 对于业务系统终端中的密钥，应通过在某一运行位置擦除所有形式的密钥来实现，必要时宜采用物理销毁的方法删除密钥，并对终止过程与结果进行记录，并归档保存。

8.4 安全管理要求

8.4.1 概述

应根据国家相关密码管理政策，遵循金融业数据安全保密的国家标准和国际标准，结合组织实际情况，成立密钥管理小组，制定并落实密钥管理小组岗位责任制；密钥管理小组应至少包含密钥管理人员、安全审计人员、密码设备操作人员，上述岗位人员不可互相兼任。

8.4.2 安全管理制度

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“安全管理要求-安全管理制度”指标做如下要求：

a) 应对所有密钥的生成、存储、注入、使用、分发、备份、恢复、归档、销毁等方面建立管理制度；
b) 应建立密码设备、密码系统的标准作业规程，明确各步骤的操作标准流程，各阶段操作应生成作业表格，并归档留存；
c) 对密码管理与密钥管理工作中的重要业务终端，应建立严格的终端访问与使用要求；
d) 根据密钥系统特性妥善保管密码卡、密码应用软件、源代码；
e) 定期检查密码设备与密钥系统的安全管理状况，依据密钥安全管理制度要求，填报有关表格和报告，检查间隔不得大于 6 个月。

8.4.3 人员管理要求

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“安全管理要求-人员管理要求”指标做如下要求：

a) 依据主管部门要求与组织实际情况，应配备一定数量的密钥管理人员、安全审计人员、密码设备操作人员等岗位人员；
b) 应配备密钥管理人员，实行 A、B 岗制度；
c) 应建立岗位责任制度，明确相关人员在密码设备管理与密钥系统管理中的职责和权限，密钥管理、安全审计、密码设备操作岗位人员职责不得交叉，相关设备与系统的管理和使用账号不得多人共用；
d) 密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理；
e) 应对密码管理、密码设备操作建立人员选拔制度和审查制度，确定专职人员承担相关工作，对相关人员实施必要的审查；
f) 应建立人员考核制度，定期进行岗位人员考核；
g) 应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务；

h） 信息技术重要岗位上的信息技术人员应定期进行轮换。

8.4.4 密码设备管理

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“安全管理要求-密码设备管理”指标做如下要求：

a） 系统应建立有效的密码设备安全管理制度；

b） 系统应采用经国家密码管理机构认证的密码产品；

c） 密码设备操作人员应经过专业培训和考核；

d） 系统应配备专门的密码设备维护人员和管理人员。

8.4.5 使用密码的业务终端要求

“安全管理制度”“人员管理要求”“密码设备管理”和“使用密码的业务终端要求”是手机银行信息系统“安全管理要求”的组成部分。在手机银行信息系统密码技术安全保护三级要求中，对“安全管理要求-使用密码的业务终端要求”指标做如下要求：

a） 终端设备密码模块应符合国家密码管理机构与行业主管部门相关规定和标准；

b） 终端设备应通过测试满足密码运算的基本功能和性能要求；

c） 终端设备密钥与密码的操作应依据操作手册和操作规程进行；

d） 终端设备报废时应依据密码终端设备报废规程，将存储在该设备中的密钥删除和销毁，销毁终端密码应用相关软件，并留存销毁记录。

附 录 A
（规范性附录）
安全要求对照表

本标准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对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、安全管理要求三方面，提出了具体要求。手机银行信息系统应按照“安全要求对照表”相应要求项进行排查和实施，如表 A.1 所示。

表 A.1 安全要求对照表

指标要求			第二级	第三级
密码安全技术要求	物理和环境安全	密码硬件安全	√	√
		物理环境安全	√	√
		电子门禁系统	√	√
	网络和通信安全	通信安全	√	√
		身份鉴别	√	√
	设备和计算安全	审计记录	√	√
		身份鉴别	√	√
		密码模块	√	√
		验证码与动态口令	√	√
	应用和数据安全	数据传输	√	√
		数据存储	√	√
		终端应用	√	√
	密码配用策略要求	密码算法配用	√	√
		密码协议使用	√	√
		密码设备使用	√	√
密钥安全与管理要求	密钥安全	密钥生成	√	√
		密钥存储	√	√
		密钥分发	√	√
		密钥使用	√	√
	密钥管理	密钥的导入与导出	√	√
		密钥的存储于保管	√	√
		密钥的使用与更换	√	√
		密钥的备份与恢复	√	√
		密钥的归档与销毁	—	√
安全管理要求	安全管理制度		√	√
	人员安全管理		√	√
	密码设备的安全管理	密码机管理	√	√
		使用密码的业务终端要求	√	√

注：“—”表示该项不做要求；“√”表示具有该项要求。

参 考 文 献

[1] 中华人民共和国标准化法(2017 年修订版)

[2] GB/T 1.1—2009 标准化工作导则 第 1 部分:标准的结构和起草规则

[3] GB/T 10112—1999 术语工作 原则与方法

[4] GB/T 16785—2012 术语工作 概念与术语的协调

[5] GB/T 20001.1—2001 标准编写规则 第 1 部分:术语

[6] GB/T 21078.2—2011 银行业务 个人识别码的管理与安全 第 2 部分:ATM 和 POS 系统中脱机 PIN 处理的要求

[7] GB/T 21078.3—2011 银行业务 个人识别码的管理与安全 第 3 部分:开放网络中 PIN 处理指南

[8] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[9] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

[10] GB/T 25070—2010 信息安全技术 信息系统等级保护安全设计技术要求

[11] GB/T 5271.8 信息技术 词汇 第 8 部分:安全

[12] GM/T 0021—2012 动态口令密码应用技术规范

[13] JR/T 0092—2012 中国金融移动支付 客户端技术规范

[14] JR/T 0093.5—2012 中国金融移动支付 远程支付应用 第 5 部分:短信支付技术规范

[15] JR/T 0093.6—2012 中国金融移动支付 远程支付应用 第 6 部分:基于安全单元(SE)的安全服务技术规范

[16] JR/T 0096.6—2012 中国金融移动支付 联网联合 第 6 部分:安全规范

[17] JR/T 0097—2012 中国金融移动支付 可信服务管理技术规范

[18] JR/T 0098.1—2012 中国金融移动支付 安全单元 第 1 部分:通用技术要求

[19] JR/T 0098.2—2012 中国金融移动支付 安全单元 第 2 部分:多应用管理规范

[20] JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引

[21] JR/T 0091—2012 中国金融移动支付 受理终端技术要求

[22] 信息安全等级保护商用密码技术实施要求

[23] 中国金融集成电路(IC)卡密钥体系管理规范(征求意见稿)

[24] 银联卡支付应用软件安全检测标准