



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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 手机银行信息系统模型	2
6 密码应用基本要求和密码应用功能要求	3
7 手机银行信息系统密码技术安全保护二级要求	3
7.1 基本技术要求	3
7.2 密码技术安全要求	3
7.2.1 物理和环境安全	3
7.2.2 网络和通信安全	4
7.2.3 设备和计算安全	4
7.2.4 应用和数据安全	6
7.2.5 密码配用策略要求	6
7.3 密钥安全与管理要求	7
7.3.1 总则	7
7.3.2 密钥安全	7
7.3.3 密钥管理	8
7.4 安全管理要求	10
7.4.1 概述	10
7.4.2 安全管理制度	10
7.4.3 人员管理要求	10
7.4.4 密码设备管理	10

7.4.5	使用密码的业务终端要求	11
8	手机银行信息系统密码技术安全保护三级要求	11
8.1	基本要求	11
8.2	密码技术安全要求	11
8.2.1	物理和环境安全	11
8.2.2	网络和通信安全	12
8.2.3	设备和计算安全	13
8.2.4	应用和数据安全	14
8.2.5	密码配用策略要求	15
8.3	密钥安全与管理要求	15
8.3.1	总则	15

8.3.2 密钥安全	15
8.3.3 密钥管理	16
8.4 安全管理要求	19
8.4.1 概述	19
8.4.2 安全管理制度	19
8.4.3 人员管理要求	19
8.4.4 密码设备管理	20
8.4.5 使用密码的业务终端要求	20
附录 A (规范性附录) 安全要求对照表	21
参考文献	22

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 **mobiledevice**

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 **devicesofkey**

具有传输密钥功能的设备。

3.4

移动支付 **mobilepayment**

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 **proximitypayment**

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 **remotepayment**

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 **SMSPayment**

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 **secureelement ; 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 **keymodule**

将完整密钥分块分别保存的部分。

3.10

手机银行系统 **mobilebankingsystem**

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 **biometricauthentication**

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。

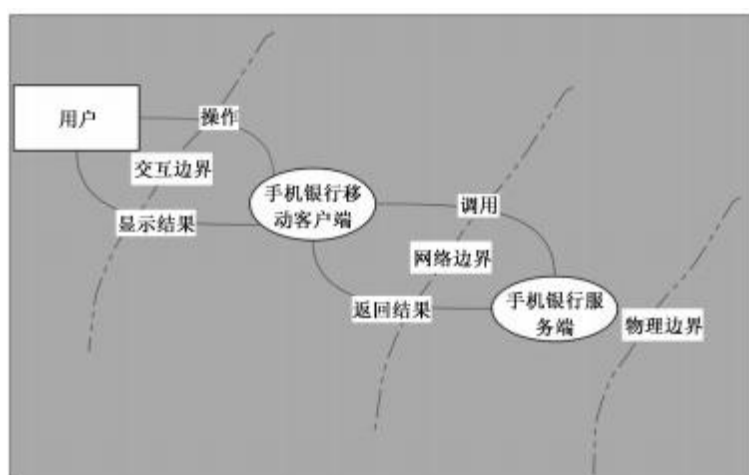


图 1 手机银行的基本架构

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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/758137024042006114>