ICS 35.040
L 80

GM

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。

3.5

远程支付系统　remote payment system

为远程支付提供移动终端接入、交易信息及结算数据的处理等功能的系统。

3.6

账户管理系统　account management system

为银行账户或支付账户提供资金管理、结算等业务的系统。

3.7

密钥管理系统　key management system

用来对密钥的生成、加载、存储、备份、分发、更新、归档、销毁等生命周期各环节进行管理的系统。

3.8

证书认证机构　certificate authority;CA

证书的签发机构，是负责签发证书、认证证书、管理已颁发证书的机构，负责制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权，也称认证中心。

3.9

客户端　client software

在移动终端上实现金融支付功能的应用软件。

3.10

动态口令　one time password;OTP

也称一次性密码，它指在认证过程中只使用一次，下次认证时则更换使用另一个口令，每个密码只使用一次。动态口令身份认证目前主要有基于时间同步机制、基于事件同步机制和基于挑战/应答(异步)机制三种技术模式。

3.11

短信动态密码　SMS dynamic code

又称短信密码，是后台系统以手机短信形式发送到用户绑定手机上的随机数，用户通过回复该随机数进行身份认证。

3.12

数字证书　digital certificate

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.13

数字签名　digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.14

实体　entity

人、组、设备或进程。

4　缩略语

下列缩略语适用于本文件。

APP　应用软件(Application)

CA　证书认证机构(Certificate Authority)
HTML　超文本标记语言(HyperText Mark-up Language)
MAC　消息鉴别码(Message Authentication Code)
OTP　动态口令(One-time Password)
SSL　安全套接层(Secure Sockets Layer)
WAP　无线应用通信协议(Wireless Application Protocol)

5　远程移动支付密码应用模式

远程移动支付密码应用模式框图如图 1 所示。

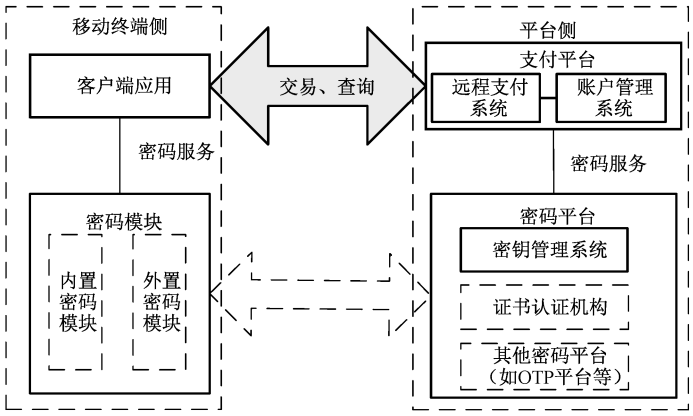

图 1　远程移动支付密码应用模式框图

远程移动支付系统主要包括两大部分:移动终端侧和平台侧(含远程支付系统、账户管理系统和密码平台)。

移动终端安装远程支付所需的客户端应用,形式包括 APP、WAP、HTML 等,功能包括远程通信服务、支付应用功能、密码模块管理等。移动终端具备安全的远程移动支付功能,还需要密码模块提供安全的密钥管理和密码运算服务,密码模块从物理上分为内置和外置两种形式。

远程支付系统是为远程移动支付提供应用服务的核心业务系统。(1)与移动设备的客户端应用进行通信和数据交换,完成远程支付和交易结算;(2)与账户管理系统交互,完成对用户账号信息的获取和管理;(3)与密码平台中的密钥管理系统通信和交互,完成对移动终端的身份鉴别和密钥管理。

根据远程移动支付密码应用过程中采用不同的认证方式,密码平台包括不同的系统。如果采用证书认证方式,则密码平台包括密钥管理系统和证书认证机构(CA);如果采用其他认证方式(如 OTP 等),则密码平台包括密钥管理系统和其他密码平台。密钥管理系统为平台侧的密码模块提供密钥管理服务。证书认证机构是指提供证书认证服务的机构。在远程移动支付密码应用过程中,如果不采用证书认证方式,则只需要密钥管理系统即可;如果采用证书的认证方式,则还需要证书认证机构提供证书认证服务。

6　密码应用安全需求

6.1　概述

密码应用安全需求主要是远程移动支付过程中数据的机密性、完整性、身份鉴别以及抗抵赖性。

6.2 数据的机密性

交易敏感数据在客户端应用输入、在移动终端侧存储、在移动终端侧与平台侧之间传输、在平台侧存储、在平台侧不同系统平台之间传输的过程中不能被非授权实体明文获取从而被利用或者泄露。

6.3 数据的完整性

客户端应用与密码模块之间传输的数据、移动终端与远程支付系统之间传输的数据、远程支付系统与其他系统平台之间传输的数据不能被做非授权的修改与破坏。

6.4 身份鉴别

远程移动支付中应确认各个实体的身份，防止身份被占用或假冒。

6.5 抗抵赖性

远程移动支付中应保证交易信息的发送实体不能事后虚假地否认它发送的消息。

7 密码安全技术要求

7.1 概述

依据远程移动支付中的密码安全要素，对远程移动支付中密码应用提出的安全技术要求主要包括：密码算法使用、终端侧安全要求、平台侧安全要求、通信安全要求。

7.2 密码算法使用要求

密码算法的配置和使用应符合相应规范，包括分组密码、非对称密码、杂凑函数、随机比特生成器的配置和使用：

a) 分组密码应符合 GB/T 32907 的规定；

b) 非对称算法和技术应符合 GB/T 32918、GB/T 35275、GB/T 35276、GM/T 0015 的规定；

c) 杂凑函数应符合 GB/T 32905 的规定；

d) 随机比特生成器生成的随机比特应符合 GB/T 32915 的规定。

7.3 终端侧安全要求

7.3.1 密码模块安全要求

密码模块的安全性设计应符合 GB/T 37092 的规定，业务方可为不同安全需求的支付业务场景选用不同安全等级的密码模块。

7.3.2 密钥管理安全要求

7.3.2.1 密钥生成

移动终端密码模块应具备密钥生成功能，可根据客户端应用需求生成分组密码或流密码的对称密钥，或 SM2 非对称密钥对。

生成密钥时所需的随机比特应采用随机比特生成器生成的真随机比特，随机比特应符合 GB/T 32915的规定。

7.3.2.2 密钥存储

若需要对对称密钥或SM2私钥进行存储，则必须安全存储到移动终端的密码模块中，确保密钥存储的安全，防止密钥的泄露和非法替换。

当移动终端密码模块失效时，存储的密钥必须随之失效。

7.3.2.3 密钥使用

密钥需要指定属性，防止密钥被非授权使用或乱用。

密钥使用要求：

a) 密钥只能用于指定应用；

b) 密钥只能用于指定用途或功能；

c) 当已知密钥被泄露时，应停止使用；

d) 当怀疑密钥被泄露时，可以主动停止使用。

7.3.2.4 密钥更新

应能根据密钥更新策略进行密钥的更新。

7.3.2.5 密钥销毁

根据密钥管理策略，可以对密钥进行销毁，要求从各种已用的介质中销毁待销毁密钥。销毁结果要求不可逆，不可从销毁结果中恢复原密钥。

7.3.3 密码应用安全要求

7.3.3.1 终端数据机密性保障要求

终端数据机密性保障要求适用于客户敏感信息输入环节、关键操作报文传输以及终端APP对自身存储数据的处理环节，对于存在泄密风险的敏感信息数据都应加强其机密性。

安全要求：

a) 使用安全密码键盘保障终端客户密码（静态密码、动态密码）的输入安全；

b) 终端应使用SSL或其他安全传输协议保证关键操作信息数据的传输安全，其中SSL安全传输协议应遵循GM/T 0024；

c) 终端应对存储的敏感信息数据进行加密处理，保障终端APP对自身存储数据的机密性。

7.3.3.2 终端信息完整性保障要求

终端信息完整性保障要求适用于客户登录及所有业务交互过程，客户进行业务操作时所产生的所有关键信息报文（如登录请求、密码修改、转账交易等）都应采取有效的完整性保障手段，避免关键信息报文被非法篡改。

安全要求：

a) 终端信息完整性保障的方法包括但不限于：消息认证码（MAC）、数字签名等，各种方法应能够正确标识关键信息报文的完整性；

b) 当终端使用数字签名方法时，密码模块必须能够保护私钥的安全，避免私钥泄漏。

7.3.3.3 终端身份鉴别保障要求

终端身份鉴别保障要求适用于远程移动支付业务中的客户登录、支付环节，保障终端客户线上身份

的可信度以及登录和支付安全。

安全要求：

a) 至少同时使用两种或两种以上的身份鉴别方法，常规的方法包括但不限于：静态密码、绑定终端设备、短信动态密码、数字签名等。

b) 使用 SSL 或其他安全通讯协议创建终端与平台侧的连接并在退出前一直保持安全连接状态，其中 SSL 安全传输协议应遵循 GM/T 0024。终端应主动验证平台侧真实身份。

c) 当使用绑定终端设备方法时，应使用安全的杂凑算法或加密算法对所采集的设备原信息进行安全处理，避免设备原始信息泄露导致的伪造、重放攻击风险。

d) 当终端使用数字签名方法时，密码模块必须能够保护私钥的安全，避免私钥泄漏。

7.3.3.4 终端抗抵赖保障要求

终端信息抗抵赖保障要求适用于高风险的业务环节，例如转账交易。应采用证书认证等安全措施确保客户在这些业务环节中所做的操作、数据具有合法的抗抵赖效力。

安全要求：

a) 终端应对业务的关键敏感信息进行数字签名，并将敏感信息原文和相关签名数据一同发送给平台侧供其验证和保存；

b) 密码模块应保护私钥的安全，避免私钥泄漏。

7.3.3.5 终端密码算法要求

应选取国产密码算法保障信息数据的安全。密码算法的要求见 7.2。

7.4 平台侧安全要求

7.4.1 密码设备安全要求

密码设备应符合相关安全规定，至少包括以下要求：

a) 任何对密码设备的操作，需经批准后严格按照规程进行，并记录操作日志；

b) 禁止非法连接密码设备或把密码设备用做其他用途；

c) 应采用国家密码主管部门认可的密码设备。

7.4.2 密钥管理安全要求

7.4.2.1 密钥生成

密钥生成需使用专用物理安全设备，其安全芯片应遵循 GM/T 0008。

根密钥需使用物理噪声源产生。随机性检测应遵循 GB/T 32915。

7.4.2.2 密钥存储

若需要对对称密钥或 SM2 私钥进行存储，则必须采用安全的存储技术。防止未授权密钥的泄露和替换。针对不同密钥形态，具体的存储要求如下：

a) 明文密钥

需长期存储的明文密钥，应存储于安全密码设备的物理安全模块中，当物理安全模块失效时，其中存储的明文密钥立即失效。

b) 密文密钥

可以存储在密码设备内，也可以存储于密码设备外。若存储于密码设备外，需确保经过授权才能访问。

7.4.2.3 密钥分发

密钥分发可以通过人工加载、移动存储介质直接加载、专用密钥传输设备加载、网络分发等多种方式。

具体的分发要求如下：

a) 明文密钥

当明文密钥在两个安全密码设备之间传递时，应采用口令等方式进行保护。

b) 密文密钥

已加密密钥的分发需防止密钥篡改和密钥替换。

7.4.2.4 密钥使用

密钥需要指定属性，防止密钥被非授权使用或乱用。

密钥使用要求：

a) 密钥只能用于指定应用；

b) 密钥只能用于指定用途或功能；

c) 当已知密钥被泄露时，应停止使用；

d) 当怀疑密钥被泄露时，可以主动停止使用。

7.4.2.5 密钥更新

密钥管理系统需针对被管系统和被管设备设置密钥更新策略。

应能根据密钥更新策略进行密钥的更新。如果更新的密钥是密钥加密密钥或根密钥，所有被该密钥加密的密钥或子密钥都应更换。

因密钥更换带来的应用数据转加密，不由密钥管理中心负责。

密钥更新要求：

a) 严格按照密钥更新策略进行更新；

b) 新密钥不可逆向推导出旧密钥；

c) 不能增加其他密钥的泄露风险。

7.4.2.6 密钥归档

当密钥超过使用期限，或不再使用，根据密钥管理策略可以被归档。

密钥可以采用下列形式归档：

a) 已归档的密钥只能用于证明在归档前进行的交易的合法性；

b) 已归档的密钥不应返回到操作使用中；

c) 归档密钥不能影响在用的密钥的安全。

7.4.2.7 密钥备份

密钥备份是存储密钥副本，用于恢复原密钥。备份密钥应具有访问控制权限，禁止通过非授权的方式恢复原密钥。密钥备份过程应保证密钥不被泄漏、替换和篡改。

7.4.2.8 密钥恢复

恢复的密钥不能以明文方式出现在密码设备外。

7.4.2.9 密钥销毁

根据密钥管理策略，可以对密钥进行销毁，要求从各种已用的介质中销毁待销毁密钥。销毁结果要

求不可逆，不可从销毁结果中恢复原密钥。

7.4.3 密码应用安全要求

7.4.3.1 平台侧数据机密性保障要求

平台侧数据机密性保障要求适用于终端数据受理、总体业务数据存储环节，对于在平台侧存在泄密风险的敏感信息数据都应加强其机密性。

安全要求：

a) 平台侧应支持对终端用户的密码（静态密码、短信动态密码）加密信息解密和验证；

b) 平台侧应使用 SSL 或其他安全传输协议保证关键操作信息数据的传输安全；

c) 平台侧应对存储的敏感信息数据进行加密处理，保障敏感信息数据的机密性。

7.4.3.2 平台侧信息完整性保障要求

平台侧信息完整性保障要求适用于受理客户登录及所有业务数据过程，平台侧应支持针对终端客户业务操作所产生的关键信息报文（如登录请求、密码修改、转账交易等）采取有效的完整性保障手段，避免关键信息报文被非法篡改。

安全要求：

平台侧信息完整性保障的方法包括但不限于：支持消息认证码（MAC）、数字签名等验证方法。

7.4.3.3 平台侧身份鉴别保障要求

平台侧身份鉴别保障要求适用于远程移动支付登录、支付等业务中平台侧受理和验证客户身份，保障客户线上身份的可信度以及登录和支付安全。

安全要求：

a) 平台侧应支持多种身份鉴别方法，常规的方法包括但不限于：静态密码、短信动态密码、数字签名等；

b) 使用 SSL 或其他安全通讯协议创建终端与平台侧的连接并在退出前一直保持安全连接状态。

7.4.3.4 平台侧抗抵赖保障要求

平台侧信息抗抵赖保障要求适用于高风险业务环节，例如转账交易。采取安全措施确保能够对终端客户在这些业务环节中所做的操作、数据具有合法的抗抵赖效力。

安全要求：

如果采用证书认证方式，平台侧在验证数字签名有效性后应继续验证签名者证书有效性，确保报文原始信息以及其数字签名受理时，签名者证书是合法、有效的。

7.4.3.5 平台侧密码算法要求

应选取国产密码算法保障信息数据的安全。密钥算法的要求见 7.2。

7.4.4 管理安全要求

管理安全要求：

a) 应建立安全管理架构，设置专门的信息安全、研发测试、运行维护、风险控制、应急处置等部门或团队，并明确和详细定义相关部门职责；

b) 应建立安全管理制度，包括安全制度、安全规范、安全操作规程和操作手册，以便规范工作流程、明确工作职责、降低安全风险；定期对安全管理制度的合理性和实用性进行审计，及时修订

安全管理制度的不足；

c) 应制定明确的安全策略，以确保设计开发、测试验收、运行维护、备份恢复、应急处置、灾难恢复等安全有效开展，并对应用系统、网络设备、安全设备等制定相应的安全保护措施；

d) 应对人员和文档进行有效管理，定期对相关员工进行运维操作、安全保密等培训，保证系统平稳运行，避免员工岗位变动导致信息泄漏等。应对文档等资料按密级进行登记、分类并由专人保管，重要资料的使用、外借、销毁应经过审批流程并进行记录。

7.5 通信安全要求

包含用户信息或账户信息的报文，应使用密码技术保证其机密性。

包含金额或账户管理系统脚本的报文，应使用密码技术保证其完整性。

交易报文安全要求见 JR/T 0095—2012 中 6.2.2。