ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0095—2012

中国金融移动支付　应用安全规范

China financial mobile payment—Specification for application security

2012－12－12 发布　　2012－12－12 实施

中国人民银行　　发布

目　　次

前　言

本部分按照 GB/T 1.1-2009 给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、中国银联股份有限公司、交通银行、中信银行、中国邮政储蓄银行、中移电子商务有限公司、支付宝（中国）网络技术有限公司、深圳市财付通科技有限公司、北京通融通信息技术有限公司、开联通网络技术服务有限公司、中金国盛认证中心、东信和平智能卡股份有限公司、深圳市新国都技术股份有限公司、大唐微电子技术有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、姜云兵、杜宁、李兴锋、刘力慷、曲维民、刘运、史大鹏、雷斌、李春欢、杨帅、唐邦富、李竹、延冰、刘宁锋、仇哲、庞杰、张永成、甄旭、王庆、张礼文、郝静华、廖宗俐、邓苏军、陈耔宇、王永吉、赵如愿、张彦杰。

引　言

移动支付是一种涉及多个行业的新兴支付方式，近年来在国内外迅速发展且发展前景及潜力巨大。当前，随着移动支付的发展，移动支付应用将逐渐增多，亦面临着一系列风险，包括资金安全风险、交易欺诈风险、个人信息泄露风险、洗钱风险、网络攻击风险等。

本规范在收集、分析和评估移动支付风险的基础上，从技术、管理、交易过程等方面对移动支付应用安全所涉及的各参与主体提出安全要求。

中国金融移动支付 应用安全规范

1 范围

本标准规定了移动支付应用中的安全要求，包括实体安全（如移动终端、受理终端、远程支付系统、收单系统和账户管理系统等实体）、交易安全、密钥体系和安全管理。

本标准适用于参与移动支付业务的设备生产、应用发行、交易管理以及应用系统研制、开发、集成和维护等相关组织。

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，仅所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 4943.1-2011 信息技术设备 安全 第1部分：通用要求

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则

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 0025 中国金融集成电路（IC）卡规范

JR/T 0089.1-2012 中国金融移动支付 安全单元 第1部分：通用技术要求

JR/T 0091-2012 中国金融移动支付 受理终端技术要求

JR/T 0092-2012 中国金融移动支付 客户端技术规范

JR/T 0097-2012 中国金融移动支付 可信服务管理技术规范

3 系统安全

3.1 物理安全要求

物理安全应符合下列要求：

——按GB/T 22239-2008中第三级基本要求中的7.1.1执行；

——应满足GB/T 22239-2008中8.1.1.2的a)和d)项要求。

3.2 网络安全要求

按GB/T 22239-2008中第三级基本要求中的7.1.2执行。

3.3 主机安全要求

按GB/T 22239-2008中第三级基本要求中的7.1.3执行。

3.4 应用软件安全要求

3.4.1 通用安全

按GB/T 22239-2008中第三级基本要求中的7.1.4执行；其中，7.1.4.2中e）和f)为增强要求。

其他基本要求：

——GB/T 22239-2008 中第四级基本要求中的 8.1.4.3 中的 c)项；

——GB/T 22239-2008 中第四级基本要求中的 8.1.4.4 中的 a)项；

——用户通过应用系统对交易资源进行访问时，应用系统应保证在被访问的资源与用户之间能建立一条安全的信息传输路径；

——在移动互联网等开放网络环境中，建立交易连接之前，应采用密码技术进行会话初始化验证；

——应对交易过程中的整个报文或会话过程进行加密；

——应采用密码技术[1)]保证通讯过程中交易数据的完整性；应采用消息鉴别码（MAC）、数字签名等方式保证报文安全；

——不应在日志中记录敏感信息。

3.4.2 会话安全

会话应满足但不限于如下安全要求：

——会话标识应唯一、随机、不可猜测；

——会话过程中应维持认证状态，防止信息未经授权访问；

——会话应设置超时时间，当空闲时间超过设定时间应自动终止会话；

——会话结束后，应及时清除会话信息；

——应采取措施防止会话令牌在传输、存储过程中被窃取。

增强要求：

——应用审计日志应记录暴力破解会话令牌的事件。

3.4.3 常见攻击防范

应对常见的攻击（如跨站脚本攻击、注入攻击、拒绝服务攻击等）进行有效防范，包括但不限于如下手段：

——应在服务器端对提交的数据进行有效性检查（如对提交的表单、参数等进行合法性判断和非法字符过滤等），或对输出的数据进行安全处理；

——应具有防范暴力破解静态密码的保护措施，例如使用图形验证码等；

——应进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句等；

——应开发安全的接口，如通过避免语句的完全解释或采用参数化接口等方式实现；

——应采取有效措施防范针对服务器端的拒绝服务攻击；

——应对文件的上传和下载进行访问控制，避免执行恶意文件或未授权访问。

增强要求：

——数据库应使用存储过程或参数化查询，并严格定义数据库用户的角色和权限；

——应通过自动化工具（如弱点扫描工具、静态代码检测工具等）对应用程序进行检查；

——基于浏览器的应用，应使用安全控件等措施以降低恶意软件窃取用户敏感信息的风险。

3.5 数据安全及备份恢复

3.5.1 数据完整性

应符合GB/T 22239-2008中7.1.5.1所有要求。

---

1) 符合国家密码管理相关规定和标准的密码技术。

3.5.2 数据保密性

应符合GB/T 22239-2008中7.1.5.2所有要求。

3.5.3 备份和恢复

数据备份和恢复需满足下列要求：

——应根据法律法规和部门规章的要求，提供本地数据备份与恢复功能。对数据应进行定期备份，备份周期至少满足每天增量备份，每周一次全量备份；备份介质应场外存放；

——交易数据保存时间不少于法律法规及部门规章规定的年限；

——应采用冗余技术设计网络拓扑结构，避免存在关键网络单点故障；

——应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性；

——应提供异地备份功能，应及时将数据备份至灾难备份中心。

增强要求：

——应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，实现业务应用的无缝切换。

4 移动终端安全

移动终端安全需符合下列要求：

——移动支付客户端应符合 JR/T 0092-2012；

——移动终端安全单元（SE）应符合 JR/T 0089.1-2012 的有关要求。

5 受理终端安全

5.1 受理终端管理要求

受理终端管理应符合下列要求：

——应使用金融行业主管单位所认可机构认证的受理终端；

——应对受理终端软件按照业务规范和技术标准进行业务测试，通过验收后投入使用；

——应建立受理终端管理制度。

5.2 受理终端数据安全

受理终端数据安全需符合下列要求：

——应采用安全、可靠的加密算法，保证受理终端交易数据的完整性和保密性；

5.3 受理终端设备安全

受理终端设备需符合下列要求：

——受理终端硬件的基本安全应满足 GB 4943.1-2011 的要求；

——受理终端设备及其 PIN 输入设备应符合 JR/T 0091-2012 的要求。

5.4 受理终端密钥管理

5.4.1 受理终端密钥体系

受理终端的密钥应符合JR/T 0025的要求。对于对称密钥，受理终端应满足如下要求：

——应至少采用二级密钥，包含密钥加密密钥(KEK)和工作密钥(WK)；
——密钥应存放在受理终端安全单元中，至少采用双倍长密钥；
——同一个受理终端的MAC加密密钥(MAK)和PIN加密密钥(PIK)应有不同的取值。

5.4.2 密钥分发和存储

5.4.2.1 密钥加密密钥(KEK)

密钥加密密钥分发和存储需符合下列要求：
——KEK由受理终端应用提供方生成，应通过安全途径注入并存储到受理终端安全单元中；
——KEK用于对工作密钥(WK)进行加密保护，每台受理终端有唯一的KEK；
——应采用安全保护措施，确保KEK只能写入并参与运算，不能被读取。

5.4.2.2 工作密钥(WK)

工作密钥分发和存储需符合下列要求：
——工作密钥(WK)分为两种：PIN加密密钥(PIK)和MAC加密密钥(MAK)，PIK用于对个人识别码(PIN)的加解密，MAK用于报文鉴别码(MAC)的加解密；
——工作密钥(WK)由收单系统的加密机产生，联机下载到受理终端；
——WK的下载和传输都应受KEK的保护，以密文方式传输，受理终端收到密文WK后，将其传入受理终端安全单元存储；
——WK应根据安全策略定期更新。

6 交易安全

6.1 SE金融应用要求

SE金融应用需符合下列要求：
——SE嵌入式软件应符合JR/T 0098.5-2012；
——SE多应用管理应符合JR/T 0089.2-2012；
——SE应用下载应符合JR/T 0097-2012中10.5节SE应用下载安全要求；
——应用下载前，应用提供方与SE应进行双向身份鉴别；应用传输过程，应保证应用文件传输的完整性、机密性；应用安装失败时，SE应能恢复到安装应用前的安全状态。

增强要求：
——应提供用户开启和关闭SE中金融应用的有效手段，确保在必要时开启SE中金融应用。

6.2 交易过程安全

6.2.1 交易场景要求

移动支付技术在具体应用过程当中，基于有无SE参与、是否联机的安全角度，可将其分为如下四种种交易场景：基于SE的近场联机交易、基于SE的近场脱机交易、基于SE的远程支付和无SE的远程支付。不同的应用场景对信息安全风险控制的要求不尽相同，其身份认证强度也不尽相同。在业务实现过程中，应根据交易风险选择恰当的方式加以实现：

——基于SE的近场联机交易兼容金融IC卡标准，可用于金融IC卡类的交易应用；
——基于SE的近场脱机交易，则主要适用于小额、低风险交易，且在实现过程要考虑额外的控制

策略（如连续脱机交易不得超过规定次数，消费金额不得超过规定上限等）；
——基于 SE 的远程支付通过 SE 提供了额外的身份认证的手段，在进行高风险、大额交易时，宜在身份认证环节引入人工干预手段（如服务器端返回图形验证码、使用 OTP 令牌等）；
——无 SE 的远程支付，宜应用于小额、低风险交易，宜引入人工干预手段（如服务器端返回图形验证码、使用 OTP 令牌等）降低交易风险。

6.2.2 交易报文安全

交易报文安全需符合下列要求
——应可防止对交易的重放攻击；
——宜保证交易的抗抵赖性，包含但不局限于证书签名等技术手段；
——应用系统应保证在一段时期内同一商户交易、订单的唯一性；
——应用系统应检查交易请求报文中记载的交易要素是否完整并符合业务规则，并拒绝不完整或者不符合业务规则的交易请求；
——应用系统应防止对支付成功的订单重复支付；
——对于大额支付等高风险业务（支付机构可根据自身情况对高风险业务交易进行界定）应使用数字证书对交易数据中的关键要素进行签名，关键要素包括但不限于商户编号、订单号、订单日期时间、交易币种、交易金额、账号等；
——近场支付报文应符合 JR/T 0090-2012。

6.2.3 敏感信息保护

敏感信息保护需符合下列要求：
——用户账号及证件号码等敏感信息只能按业务要求进行保存和使用，显示时应进行屏蔽处理；
——应保证交易隐私信息的保密性，如姓名、有效身份证件号码、联系方式、交易内容等。

6.2.4 风险识别与干预

风险识别与干预需符合下列要求：
——应采取必要措施，在交易过程中给予必要的支付风险提示。支付风险的提示可每次提示，也可在业务开通时给予提示；
——支付机构从用户的账户管理机构获取的支付结果中应包含支付及风险防范相关的数据要素；
——应对交易过程进行风险识别与干预，防范潜在的非法交易、欺诈交易。

6.3 安全运营

6.3.1 客户与商户信息管理

客户与商户信息管理的基本要求如下：
——应按支付业务管理办法和反洗钱规定的要求，获取并保存客户和商户的基本信息；
——应通过安全有效的方式对客户和商户的有效身份证件或其他有效身份证明文件进行核实；
——应按照接入要求对客户和商户基本信息变更进行核实，并保存变更记录；
——应针对客户和商户的交易需求及安全属性分别设置交易限额，包括但不限于文件证书限额；
——应对商户进行分类及风险评估，并提供与风险评估结果匹配的支付服务；
——应通过信息系统管理客户和商户基本信息，确保信息的保密性与完整性。
增强要求：
——应通过信息系统建立商户风险评级体系，并提供与风险等级匹配的支付服务。

6.3.2 交易查询

交易查询应满足如下要求：

——应保证仅用户或授权人员能够查询交易账户信息；

——应将查询结果中的敏感信息进行屏蔽。

6.3.3 交易监控

交易监控应满足如下要求：

——应建立交易监控系统，能够甄别并预警潜在风险交易，例如套现、洗钱、欺诈等可疑交易，并生成风险监控报告；

——应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、复核、查结机制；

——应对监控到的风险交易进行及时分析与处置；

——应依据已识别并确认的风险数据，建立黑名单数据库。

6.3.4 用户教育

用户教育应满足如下要求：

——应通过多种方式对用户进行安全风险提示，对安全控制措施进行说明；

——应在风险类业务的操作前、操作中进行风险提示；或在用户第一次交易时进行风险提示和安全教育。

增强要求：

——建立业务功能的演示版或尝试机制，让用户充分了解业务处理流程和功能实现；

——提供风险类业务操作的手册，对用户进行宣传和教育。

7 密钥体系

7.1 密码算法

移动支付使用的密码算法主要有对称加密算法、非对称加密算法和摘要算法，应满足如下要求：

——应选择符合国家行业主管部门要求的算法；

——支持的对称加密算法包括但不限于：SM4、DES、3DES、AES、SSF33；

——支持的非对称加密算法包括但不限于：SM2、RSA；

——支持的摘要算法包括但不限于：SM3、SHA-1；

——用于近场支付的密码算法应能够实现 JR/T 0025 中所描述的安全机制。

7.2 数据认证

7.2.1 近场支付

近场支付的数据认证方式应符合JR/T 0025的要求。

7.2.2 远程支付

7.2.2.1 密钥和证书

远程支付所涉及的证书/密钥主要有：

——服务器证书：安装在服务器上用于标识服务器真实身份的数字证书；

——客户端证书：安装在客户端（通常保存在 SE 中）上用于与服务器端进行身份认证的数字证书；
——用户证书：通常保存在移动终端 SE 中，由账户管理机构/应用提供方签发的用于标识用户身份的数字证书；
——会话密钥：用于移动终端与移动支付相关信息系统间会话加密；会话密钥通常采用对称密钥，由安全协议协商临时产生；如果移动终端与移动支付系统通讯采用固定的会话密钥，则须采取技术措施确保会话密钥的存储和使用安全，并定期更换。

7.2.2.2 通讯认证要求

通讯认证需符合下列要求
——应在与移动终端直接通讯的远程移动支付系统服务器上安装服务器证书,用于标识服务器真实身份；
——宜采用客户端证书，用于服务器端验证客户端身份合法性。

7.2.2.3 用户认证要求

用户数据认证可采用多种形式（如数字证书、一次性口令等），当客户端采用数字证书认证时，应使用用户证书对关键要素或报文整体进行签名，由应用系统验证签名有效性。

7.3 密钥管理安全

7.3.1 基本要求

本节主要规定移动支付中密钥管理要求，基本要求如下：
——应采用安全可靠的加密算法；
——基于 SE 的应用，其相关密钥的存贮和交易信息的加密 / 解密应在硬件加密设备中进行；
——应遵循金融业数据安全保密的国家标准和国际标准；
——应加强对人员的管理要求；
——应定期更换密钥。

7.3.2 基于 SE 的应用密钥

数据认证过程中所涉及的密钥包括：
——认证中心公私钥对，认证中心会产生多个公私钥对，每个公私钥对都将分配一个唯一的认证中心公钥索引。认证中心公钥及其索引由收单行加载到终端，认证中心私钥由认证中心保管并保证其私密性和安全性；
——发卡行公私钥对，支持数据认证都需要发卡行产生发卡行公私钥对，并从认证中心获取发卡行公钥证书；
——SE 公私钥对，支持动态数据认证还要求发卡行为 SE 产生 SE 公私钥对；
——应用密文密钥，由发卡行唯一管理。
应用系统之间传输所采用的密钥包括：
——主密钥，用于加、解密本地存放的其他密钥数据；
——成员主密钥，用于加、解密需传递的工作密钥，实现工作密钥的联机实时传输或其他形式的异地传输；
——工作密钥，包括成员 PIN 保护密钥(PIK)、成员信息完整性密钥(MAK)，用于加密各种数据，保证数据的保密性、完整性、真实性。

7.3.3 基于 SE 的密钥生命周期管理要求

7.3.3.1 密钥的生成

密钥生成要求如下:

——密钥应在国家密码管理机构许可的硬件加密设备中生成;

——生成对称密钥时，可选择在硬件加密设备中随机生成，或利用随机生成的分量进行合成操作;

——针对不同的业务类型必须生成不同的对称密钥，不同业务类型不可使用同一套对称密钥;

——SE 模块密钥对的生成包括两种方式:

- 在 SE 中生成;
- 在硬件加密设备中生成，再写入到 SE 模块中，但要保证密钥写入 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。

7.3.3.2 密钥的传输

密钥传输要求如下:

——密钥传输时应采用足够安全的方式进行，不得明文传输;

——各类密钥传输交接过程必须履行严格的操作审批手续，详细记录，相关人员签名确认，文档资料必须妥善保管，保存期限应不低于记录对象的生命周期，确保各类密钥传输的安全性与规范性。

7.3.3.3 密钥的存储

非临时密钥的存储包括两种方式:

1) 存放于硬件加密设备中;
2) 以加密形式存储在其他介质中。

密钥存储要求如下:

——硬件存储介质应放置在防磁、防静电干扰的环境中，应保证存储介质不被意外（如水、火、电磁干扰）破坏;

——应采取严格的控制机制防止未授权的访问，以确保密钥的完整性并防止泄露;

——SE 密钥写入 SE 模块后，应确保 SE 密钥信息在任何情况下均不会被导出;

——可以采用存储对称密钥分量的方式存储密钥，但必须保证分量保管在安全的物理环境中，并确保不同分量分离保管。

7.3.3.4 密钥的备份

密钥备份要求如下:

——应对密钥进行异地备份，并确保其安全性;

——密钥备份应满足如下要求:

- 密钥的备份可采用硬件加密设备备份，也可以采用文件的方式进行备份，无论何种备份方式均应采用 2 名以上的密钥管理人员同时控制，采用文件方式备份应对密钥进行加密;
- 备份的密钥的存储介质应保存在密钥管理机构核心区的安全保管区内，并建立严格的保管制度和访问控制制度。

7.3.3.5 密钥的恢复

密钥恢复要求如下:

——密钥恢复时，应至少 2 名密钥管理员同时到达现场，在硬件加密设备中进行;

——密钥恢复过程应当在监督人员监督下进行，并详细记录操作记录。

7.3.3.6 密钥的归档

当密钥到期后，密钥管理机构应将其归档保存，归档期限至少为5年，并应确保归档后的密钥对不会再次被使用。

7.3.3.7 密钥的销毁

密钥归档期结束后，密钥管理机构应进行销毁，且备份的密钥也应一同销毁。密钥的销毁需要在密钥管理员与所有密钥分管员参与下进行，销毁过程应有详细的操作记录。

7.3.3.8 密钥的更新

密钥更新要求如下：

——密钥更新过程与生成过程的要求相同；

——应定期更换密钥，包括但不限于服务器证书、通讯密钥、加密密钥等。

7.3.4 认证中心公钥管理要求

本节规定认证中心的公钥（CA公钥）管理(包括公钥的分发、更新、回收等)，应符合JR/T 0025的要求，并实现如下要求：

——应保证认证中心分发的认证中心公钥的完整性；

——应能正确处理认证中心公钥更换，并分发到各受理终端以保证其正常处理业务；

——受理终端可通过本地下载、远程下载等方式导入认证中心公钥；

——在认证中心公钥失效之后，应在规定的期限内将认证中心公钥从受理终端中删除。

8 安全管理

8.1 组织架构

组织架构应满足如下要求：

——应建立信息安全管理架构，设置专门的信息安全工作的职能部门或团队；

——应设置专门的支付系统研发、测试、运行维护、安全、风险控制等部门或团队；

——应明确相关部门的信息安全职责，并详细定义部门人员配置及岗位职责；

——信息安全相关部门人员应详细了解本单位研发、运行及管理机构职责设置。

8.2 管理制度

管理制度应满足如下要求：

——应建立安全管理制度体系，明确工作职责、规范工作流程、降低安全风险，应制订移动支付安全管理工作的总体方针和策略；

——应建立贯穿支付系统设计、编码、测试、运行维护、评估以及应急处置等过程，并涵盖安全制度、安全规范、安全操作规程和操作记录手册等方面的信息安全管理制度体系；

——应指定或授权专门的部门或人员负责安全管理制度的制订，并确保通过有效而正式的方式进行发布；

——应每年组织相关部门和人员对安全管理制度体系的合理性和适用性审计，及时修订安全管理制度的不足；

——应定期对员工进行安全培训，培训内容包括各类安全制度、信息系统运维手册和应急预案等。

8.3 安全策略

安全策略应满足如下要求：

——应制订明确的支付系统总体安全保障目标；

——应制订针对支付系统设计与开发、测试与验收、运行与维护、备份与恢复、应急事件处置以及用户信息保密等的安全策略；

——应制订支付系统使用的应用系统、网络设备、安全设备的配置和使用的安全策略；

——应维护详细的资产清单，资产清单应包括资产的价值、所有人、管理员、使用者和安全等级等条目，并根据安全等级制订相应的安全保护措施；

——应明确系统存在的威胁，并根据威胁分析系统的脆弱性，对已发现的风险应尽快修补或制订规避措施；

——应针对不同的风险规定相应的可能性等级列表，并根据风险严重等级制订应急恢复方案和演练计划。

增强要求：

——应按照 GB/T 22239-2008 规定所有数据的安全级别，并制订与其安全级别相应的保护措施。

8.4 人员及文档管理

人员及文档管理应满足如下要求：

——应设置信息安全管理岗位，明确相关岗位在信息安全管理过程中所承担的责任；

——应与涉密岗位员工签署保密协议，或在劳动合同中设置保密条款，确保员工理解认同公司相关信息安全策略，承诺安全责任与义务；

——应对关键岗位设定人员后备措施，并加强其安全培训，确保员工了解各自岗位职责以及违反安全规定可能导致的后果；

——应具有员工岗位调动或离职的安全管理制度，避免账号、设备、技术资料及相关信息等泄露；

——应建立外来人员管理制度，提交操作记录，必要时要求其签订保密协议；

——应建立文档管理制度，文档资料按密级或敏感程度进行登记、分类并由专人保管，重要文档资料的使用、外借或销毁应经过审批流程并进行记录。

8.5 运行维护管理

应按照GB/T 22239-2008中第三级基本要求中的7.2.5执行。

8.6 系统性能及能力评估

系统性能及能力评估的应满足如下要求：

——应根据业务特点制定系统性能及能力评估指标；

——应对系统的性能和能力进行评估，评估范围包括但不限于数据中心、服务器、存储、数据库、应用和网络等；

——应每年进行全面的系统性能和能力评估，形成完整的系统性能和能力评估报告，报告内容中应包含评估内容、评估结果、评估结论、评估日期等。

8.7 业务连续性管理

8.7.1 业务连续性

业务连续性管理应满足GB/T 22081-2008第14章的要求。

8.7.2 灾难恢复

应建立支付系统的灾难恢复机制、灾难恢复的工作范围、组织机构、规划的管理、外部协作等，具体应按GB/T 20988-2007中第三级的要求执行。

8.8 外包管理

外包风险管理应满足如下要求：

——外包内容应符合法律法规的要求；

——应对外包行为和外包模式进行风险评估；

——确定外包行为前应对外包服务提供方的经验和能力、硬件资源、财务状况、资金构成、人员构成、主管部门审批等资质进行评估；

——应与外包服务提供方就外包内容签订合同，合同中应明确各方的权利、义务及责任和争议解决办法；

——应在合同中设定安全保密条款或单独签署安全保密协议；

——应在合同中设定条款要求外包服务提供方提供的外包服务符合本规范要求；

——应制订对外包的控制制度、事件报告程序和应急计划；

——应制订详细的外包交付清单，并对外包相关人员进行业务培训，保障顺利交付外包内容；

——应指定或授权专门的部门或人员负责对外包服务进行管理和监督，定期评估外包商的运营状况，定期审查合同条款的履行情况。

参 考 文 献

[1] GM/T 0002-2012 SM4分组密码算法
[2] GM/T 0003-2012 SM2椭圆曲线公钥密码算法
[3] GM/T 0004-2012 SM3密码杂凑算法