ICS 35.240.40
A 11

SZDB/Z

深 圳 市 标 准 化 指 导 性 技 术 文 件

SZDB/Z 204—2016

金融服务移动应用信息安全指南

Information Security Guide for Mobile Application of Financial Services

2016－11－04 发布　　2016－12－01 实施

深圳市市场监督管理局　　发 布

目　　次

前　言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　基本原则 2
5　安全管理要求 2
6　业务安全要求 3
7　客户端安全要求 4
8　服务器安全要求 6
附录 A　客户端安全风险评分 8
参考文献 12

前　言

本指南按照 GB/T 1.1-2009 给出的规则起草。

本指南适用于金融相关业务组织的金融服务移动应用系统的安全防护，金融服务移动应用系统包括但不限于业务组织内部与外部使用的移动应用系统以及其合作的金融服务接口系统。

本指南由金融服务业标准联盟提出并归口。

本指南主要起草单位：深圳市金融信息服务协会、中国平安保险（集团）股份有限公司、深圳海云安网络安全技术有限公司等。

本指南主要起草人：谢朝海、李绅、韩梅、陈铁勇、熊少军、聂君、熊莹、罗振伟、金文佳、陈镜萍、李杰、殷春富、郑太海、张瑞峰、陈胜芬、占长敬、唐秀江、邓华威、吴国友等。

本指南为首次制定。

金融服务移动应用信息安全指南

1 范围

本指南规定了金融服务移动应用系统信息安全风险管理中的信息安全管理、业务安全、客户端安全和服务器端安全的基本要求。

本指南适用于指导深圳市辖区内的金融机构以及其他从事金融相关业务的组织进行金融服务移动应用系统的需求、设计、编码、测试、发布、运行、维护等过程的安全保护。

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/T 5271.8 信息技术 词汇 第8部分：安全

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求

GB/T 30279-2013 信息安全技术 安全漏洞等级划分指南

GB/T 27910-2011 金融服务 信息安全指南

JR/T 0060-2010 证券期货业信息系统安全等级保护基本要求

JR/T 0068-2012 网上银行系统信息安全通用规范

JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

3 术语和定义

GB/T 5271.8和GB/T 30279-2013所确立的以及下列术语和定义适用于本标准。

3.1

金融服务移动应用安全评估 security assessment for mobile application of financial services

由外部评估机构或内部独立部门执行的对移动应用系统面临的信息安全风险进行的评估工作，评估内容包括但不限于安全管理、业务安全、客户端安全、服务器端安全等重要环节的风险管控能力。

3.2

敏感信息 sensitive information

一旦遭到泄露或修改，会对标识的信息主体造成不良影响的信息，例如金融服务中个人客户的敏感信息包括但不限于姓名、身份证号码、手机号码、地址等信息的组合。

3.3

关键业务 critical business

在移动应用系统上进行的、对金融服务客户有重大影响的业务，包含但不限于：转账、积分兑换、银行卡绑定等操作，修改姓名、地址、手机号、密码等操作。

4 基本原则

a）纵深防御原则

在移动应用系统上采取各种安全措施时，在整体上应保证各种安全措施的组合从客户端到服务器构成一个纵深的安全防御体系，以保证移动应用系统整体的安全保护能力。

b）重点保护原则

应根据应用领域和业务特点，对不同重要程度的移动应用系统实施不同强度的安全保护，集中资源，优先保护重要性高的移动应用系统。

c）动态调整原则

应根据移动应用系统的运行机制、运行环境等方面的变化，及时调整安全保护措施，确保移动应用系统的安全。

d）充分评估原则

应根据本指南及相关政策标准要求，做好移动应用系统的安全测试评估工作，充分评估移动应用系统的安全风险，尽早采取应对措施保障移动应用系统的安全。

5 安全管理要求

5.1. 组织架构

5.1.1. 应建立分工明确、报告关系清晰的内部移动应用安全管理组织，以保证移动业务管理、信息科技管理和审计监督职能的有效履行。

5.1.2. 应设立移动应用信息安全相关技术和管理岗位，并制定明确的岗位职责要求和人员配置要求。

5.2. 安全管理制度

5.2.1. 应建立覆盖移动应用管理的安全策略、安全管理制度、安全操作规程和操作记录手册等层次的

完善的安全管理制度体系，并及时更新。

5.2.2. 应建立有效的移动应用数据安全管理机制，对信息数据进行分类分级管理，并从数据创建、传输、存储、使用、销毁等环节对数据安全采取技术防护措施。

5.2.3. 应建立有效的移动应用安全开发生命周期管理机制，对移动应用系统需求分析、规划、采购、开发、测试、部署、维护、升级和报废环节采取有效的安全防护措施，以保证软件全生命周期的安全性。

5.2.4. 应建立有效的移动应用系统安全运行管理机制，从物理安全、逻辑安全、第三方人员安全、运行操作安全、事件管理、应急响应处置、变更管理、系统监控、容量管理、入侵防御等方面保证移动应用系统的安全运行。

5.2.5. 应将移动应用业务纳入到本单位业务连续性管理体系中，并进行持续的维护更新，以降低业务中断给业务带来的风险。

5.2.6. 应妥善管理移动应用系统相关外包服务，制定外包服务管理规范，以确保客户资料等敏感信息的安全，降低因外包服务中断给移动业务持续运行带来的影响。

6 业务安全要求

6.1 业务流程管理

6.1.1. 业务流程建立应符合行业监管要求，并采取充分的控制措施进行风险防范。

6.1.2. 对于需要开通资产交易等高风险业务的客户，应要求客户本人主动申请并书面确认，同时对其进行风险提示，并验证客户的身份信息，不得由他人代理申请。

6.1.3. 客户已通过电子签名等确保客户身份被有效验证的情况下，在移动端申请开通资产交易等高风险业务，视同客户本人主动申请并书面确认。

6.1.4. 应确保在移动业务注销环节中，通过自助办理、网点人工办理等不同渠道的操作结果具备同等风险控制有效性。应加强移动业务注销环节的风险管理，经客户同意完成注销后应同步关闭移动端资产交易等高风险业务功能，并应妥善处置系统后台所存储的客户相关信息。

6.1.5. 应建立客户端硬件丢失时的数据安全策略和紧急风险控制方案

6.2 关键业务安全管理

6.2.1. 对于关键业务操作以及资产交易等高风险业务，系统应充分提示客户相关业务操作的安全风险并提供及时通知客户资产、信息等的变化。

6.2.2. 在使用一次性安全验证码如手机短信验证码作为多因素之一时，应防控因一次性验证码获取端与交易指令发起端为同一物理设备等隐含带来的风险。

6.2.3. 应对资产交易等高风险业务的交易限额提供控制机制，对不同分类的资产交易应允许客户在设定的限额下自主设定交易限额。

6.2.4. 宜在客户端为用户登录与敏感业务操作如资金交易分别创建口令，并建议用户设为不同口令。

6.3 业务风险监控

6.3.1. 应根据自身业务特点，建立完善的移动业务异常交易监控机制，识别并及时处理异常交易，监控范围包括但不限于客户登录、资产类交易等。

6.3.2. 应有效监控假冒金融业务等相关非法活动，及时发现风险并采取防范措施。

6.3.3. 应定期充分评估移动业务的安全风险，并积极采取有效控制措施。

6.3.4. 应加强服务人员的风险防范培训，以正确引导客户使用金融移动业务。

7 客户端安全要求

7.1 开发安全

7.1.1. 应建立安全开发基线，并在开发需求说明书中明确客户端程序的安全需求。

7.1.2. 应对开发人员进行安全编码意识培训。

7.1.3. 应具有移动业务程序安全开发编码规范。

7.1.4. 应对自主及外包开发的客户端程序源代码进行安全检测或者要求开发方提供第三方安全检测报告，以发现及消除可能存在的恶意代码和安全漏洞。

7.1.5. 客户端程序委托第三方进行外包开发或测试的，应对外包机构的资质进行审查。

7.1.6. 应加强客户端源代码程序文件的访问权限控制，防范源代码程序文件泄漏给无关的第三方。

7.1.7. 应建立完善的版本管理制度，对源代码的版本进行控制。

7.1.8. 应在客户端版本发布前由单独的测试团队对客户端的安全性进行测试，并宜委托第三方检测机构进行安全性检测，测试过程使用到的敏感数据应进行脱敏处理。

7.1.9. 应建立安全的软件编译构建机制，防止人为因素与环境因素等给客户端软件带来安全风险。

7.2 发布安全

7.2.1. 应确保发布的客户端遵循最小配置原则，不包含任何非业务必需的特性，例如非业务需要的功能模块、外部接口、调试信息、测试数据等。

7.2.2. 应在移动业务签约时对用户进行风险教育与风险提醒，如提醒用户从官方认可的渠道下载和更新客户端，再如提醒用户不要在不安全网络中使用客户端程序。

7.2.3. 应对客户端完整性进行校验，防范客户端被恶意篡改。

7.2.4. 应采取技术措施监测第三方渠道上的假冒客户端程序，及时发现和处理。

7.2.5. 应在客户端中设置版本检查功能，客户端版本过期或更新时应及时提醒用户更新。

7.2.6. 应妥善保存历史发布的每个版本的客户端源代码和程序文件。

7.3 软件自身安全

7.3.1. 在客户端安装或更新时宜通过校验数字签名等手段确认其来源于可信实体。

7.3.2. 应采取措施有效保护客户端文件和数据库不被其它程序非法读取或修改，例如设置客户端私有目录下文件的权限，禁止其他用户非法访问。在客户端启动时宜检查运行环境的安全性，如发现运行环境存在安全风险，应提示用户。宜采取措施有效保护客户端的内存数据不被其它程序非法读取或修改。

7.3.3. 应采取措施增加客户端软件被逆向分析的难度，如代码混淆、加密、添加花指令等。

7.3.4. 应合理设置组件之间的安全访问权限，例如设置安全的组件通讯权限。

7.3.5. 当使用第三方组件时,宜在系统的生命周期管理中明示对第三方组件的依赖性，宜对第三方组件在使用中的行为与漏洞建立档案，并建立相应应急响应策略，及时预警由于使用第三方组件带来的风险。

7.3.6. 程序启动时客户端宜检查自身软件的完整性。

7.3.7. 应具有必要的进程防护措施，能防止被动态注入恶意库文件，造成软件进程敏感信息窃取或其它恶意操作。

7.3.8. 客户端应具有出错保护机制，防止软件出现异常时输出敏感信息如调试用信息。

7.3.9. 应具有防界面劫持的机制，如提示用户安装第三方手机安全软件来防界面劫持。

7.4 用户操作安全

7.4.1. 应采取必要的防护措施检查用户输入的口令强度，禁止用户设置弱口令。

7.4.2. 应采取必要的防护措施，限制连续登录失败次数，超过限制次数时需进行登录锁定。

7.4.3. 在登录时客户端可使用安全的图形验证码, 图形验证码应由服务器端生成。

7.4.4. 客户端软件在运行中切换到后台时，可给予用户明确的运行提示，包括但不限于消息提示、通知栏等方式。

7.4.5. 应保护用户在客户端中输入用户口令、个人识别 PIN 码、卡确认 CVN2 码和有效期等敏感信息时不被其它程序非法窃取，例如具有防键盘劫持机制和反屏幕录像功能。

7.4.6. 应建立客户端硬件丢失时的数据安全策略和紧急风险控制方案。

7.5 数据安全

7.5.1. 应对客户端输入的数据进行有效性验证，如数据格式、长度、取值范围是否满足要求等。

7.5.2. 客户端应在用户输入用户口令、PIN、CVN2 和有效期等敏感信息后立即进行加密，在其他任何处理阶段都不应出现完整的明文信息。

7.5.3. 客户端应在显示密码等敏感信息时采用不可区分的特殊字符进行屏蔽。

7.5.4. 客户端应在显示实体卡的账号、手机号、身份证号等敏感信息时屏蔽部分字段。

7.5.5. 客户端应在用户注销后立即清除本地存储的 Token 等敏感信息。

7.6 通信安全

7.6.1. 客户端应使用安全协议保证与服务器或其它实体间通信的机密性和完整性，如使用 TLS 安全传输协议等，安全传输协议应及时更新版本。同时，也应对传输的密码等敏感信息进行加密通信。

7.6.2. 客户端应在建立连接时对服务器或其它实体的身份进行合法性认证。

7.6.3. 客户端与服务器之间的数据通信应具有防重放机制。

7.6.4. 客户端退出时应设置正常终止会话机制，清空会话信息。

7.6.5. 客户端在超过一段时间后无操作后，应设置会话超时并要求重新进行身份认证。

7.6.6. 在业务交易过程中，客户端遇到网络切换或者网络断开，宜提示用户选择是否继续交易。

8 服务器安全要求

8.1. 应满足《信息安全技术 服务器安全测评要求》(GB/T 25063-2010)的安全等级二级或二级以上的要求。

8.2. 应在服务器端生成防范暴力破解静态密码的保护措施，如增设图形认证码，对用户登录错误次数进行限制，预防撞库行为。应支持会话管理服务以跟踪特定用户信息，支持客户端程序退出时及时终止会话。

8.3. 需要在客户端输入的动态密码应由服务器端生产和管理，动态密码应有有效时长，并且有输入错误次数限制。

8.4. 应建立安全的访问控制机制，防止用户越权访问功能或资源，采取默认拒绝，并强制所有的请求

都通过访问控制检查。

8.5. 应在服务器端将所有来自于应用外部的输入进行安全校验，包括但不限于：校验 HTTP 头、cookies 以及 GET 和 POST 参数。

8.6. 应在服务器端保证业务逻辑的安全，包括业务异常和失败的场景。

8.7. 服务端程序代码应不包含有恶意代码，不包含有已知的高安全风险漏洞，应采取恰当的措施应对各种已知攻击，如参数化查询预防 SQL 注入，对数据进行编码以预防跨站脚本攻击等。

8.8. 应严格进行服务器端程序代码管理，控制对生产版本源代码的访问，有效地进行源代码版本控制，如发布版本涉及业务流程、系统架构等重大变化时宜通过第三方安全检测机构的测评。

8.9. 服务器端应防止防范敏感信息泄露，如应根据业务必需的原则向客户端提供数据，需对敏感数据进行加密，禁止提供不必要的数据。在显示经认证成功后的客户身份证件信息时，应屏蔽部分关键内容。程序出错信息不应反馈输出到客户端。

8.10. 服务器端应具有防网络钓鱼的功能，例如进行客户预留信息显示提示，显示上次登录时间或退出时间等。

8.11. 涉及文件上传功能应在服务器端限制上传的文件类型和文件大小，客户端上传的文件应由服务器端改写文件名后存储。

附录 A
（资料性附录）
客户端安全风险评分

A.1 目的

客户端APP是移动应用系统中相对较具特色的部分。客户端APP安全在移动应用信息安全中具有重要的现实意义。各单位进行移动应用信息安全风险评估时，往往需要单独对客户端APP的安全风险进行计分评估，以方便考察对比不同客户端APP以及同一客户端APP不同版本的安全状况。

基于本指南正文第7章客户端安全要求，本附录给出客户端APP的信息安全风险评分标准和评分方法。各单位在进行客户端APP信息安全风险时可以参照使用。

A.2 评分方法

A.2.1 综合评分

移动应用客户端APP安全风险评估的综合分数由安全分数和风险分数两大部分决定，最高分1000分，最低分0分，安全分数和风险分数分别用A.2.2和A.2.3节的方法评分。综合评分的具体计算公式为：

$$综合分数 = \begin{cases} 安全分数 - 风险分数 & ，安全分数 \geq 风险分数 \\ 0 & ，安全分数 < 风险分数 \end{cases}$$

根据综合评分的得分区间，对客户端APP的安全情况进行分级，共分为4级：A级（安全）、B级（较安全）、C级（不安全）和D级（很不安全）。具体安全等级与综合评分对应关系见表A.1。

表A.1 安全等级与综合评分对应关系一览表

安全等级		对应综合评分情况
A	安全	1000≥综合评分≥900
B	较安全	900〉综合评分≥700
C	不安全	700〉综合评分≥500
D	很不安全	500〉综合评分≥0

A.2.2 安全评分

移动应用客户端APP的安全分数是基于本指南正文第7章客户端安全要求进行逐项检测评估时，客户端APP所存在的安全问题的风险级别确定，共分为4档，判定依据见表A.2。

表A.2 安全分数的评分依据表

安全分数得分		判别依据
第 1 档	1000	客户端 APP 不存在任何高危、中危和低危等风险级别的安全检测项。

表A.2 安全分数的评分依据(续)

安全分数得分		判别依据
第 2 档	950	客户端 APP 不存在任何高危和中危风险级别的安全检测项但是存在低危风险级别的安全检测项。
第 3 档	800	客户端 APP 不存在任何高危风险级别的安全问题但是存在中危风险级别的安全检测项。
第 4 档	600	客户端 APP 存在高危风险级别的安全检测项。

A.2.3 风险评分

移动应用客户端APP的风险分数由客户端APP各个检测项存在的具体安全问题及其对应的风险级别确定，是本指南正文第7章客户端安全要求所有对应检测项存在问题的安全风险分值的总和，具体计算公式如下：

风险分数=Σ（风险分值*权重系数）

本指南正文第7章客户端安全要求所对应检测项存在问题的风险分值是由评估人员根据实际评估结果进行分析后综合判断得到。风险级别总体上由高到低分为高危、中危、低危和通过四级，其级别划分标准和对应分值见表A.3。

表A.3 风险级别的评分依据表

风险级别	风险分值	判别依据
高危	5	不符合或部分符合第 7 章客户端安全要求相应检测项，对移动应用客户端 APP 的程序代码、数据信息或者操作行为等的机密性、完整性或可用性影响严重。
中危	3	不符合或部分符合第 7 章客户端安全要求相应检测项，对移动应用客户端 APP 的程序代码、数据信息或者操作行为等的机密性、完整性或可用性影响较轻。
低危	1	不符合或部分符合第 7 章客户端安全要求相应检测项，对移动应用客户端 APP 的程序代码、数据信息或者操作行为等的机密性、完整性或可用性影响很低。
通过	0	符合第 7 章客户端安全要求相应检测项，对移动应用客户端 APP 的程序代码、数据信息或者操作行为等的机密性、完整性或可用性无影响。

本指南正文第7章客户端安全要求所对应检测项的权重系数由其安全影响力和对应安全问题的利用复杂度两个方面综合决定的，其安全影响力越高且利用复杂度越低则该检测项的权重系数就越高，反之，如果检测项的安全影响力越小且利用复杂度越高则该检测项的权重系数就越低。权重系数取值区间为1到10之间的整数，分数越高安全权重越大。第7章客户端安全要求所对应检测项的权重系数可参考表A.4得到，也可由单位或第三方测评机构根据检测项的重要性自行给出。

表A.4 检测项权重系数一览表

序号	分类	检测项	权重系数
1	开发安全	7.1.1 安全开发基线	7
2		7.1.2 安全意识培训	7
3		7.1.3 安全编码规范	7
4		7.1.4 源代码检测	10
5		7.1.5 外包开发	7
6		7.1.6 源代码访问控制	10
7		7.1.7 版本管理	7
8		7.1.8 发布测试	9
9		7.1.9 软件构建	7
10	发布安全	7.2.1 最小配置	7
11		7.2.2 安全下载	4
12		7.2.3 完整性校验	4
13		7.2.4 第三方渠道监测	8
14		7.2.5 版本检查功能	7
15		7.2.6 历史版本管理	7
16	软件自身安全	7.3.1 应用来源校验	6
17		7.3.2 运行时保护	6
18		7.3.3 逆向分析	7
19		7.3.4 组件安全	7
20		7.3.5 第三方组件漏洞	10
21		7.3.6 启动完整性校验	5
22		7.3.7 进程保护	8
23		7.3.8 出错保护	10
24		7.3.9 防界面劫持	10
25	用户操作安全	7.4.1 弱口令	10
26		7.4.2 登录失败处理	7
27		7.4.3 图形验证码	10
28		7.4.4 后台运行提示	5
29		7.4.5 敏感信息输入	8
30		7.4.6 硬件丢失	8

表 A.4 检测项权重系数一览表（续）

序号	分类	检测项	权重系数
31	数据安全	7.5.1 输入有效性验证	10
32		7.5.2 输入数据加密	8
33		7.5.3 敏感信息显示	5
34		7.5.4 用户信息显示	4
35		7.5.5 敏感信息清除	7
36	通信安全	7.6.1 通信协议安全	10
37		7.6.2 实体身份认证	4
38		7.6.3 防重放攻击	7
39		7.6.4 会话终止	4
40		7.6.5 超时认证	3
41		7.6.6 断网提示	1

参考文献

[1] 《电子银行安全评估指引》（银监发[2006]9号）

[2] GB/T 20269-2006 信息安全技术 信息系统安全管理要求

[3] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 20274.1-2006 信息安全技术 信息系统安全保障评估框架：简介和一般模型

[5] 《证券公司合规管理有效性评估指引》（中证协发[2012]027号）

[6] 《银行业金融服务安全评估办法》