ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0225—2021

保险移动应用信息安全基本要求

Basic Requirements for Information Security of Insurance Mobile Applications

2021-10-9 发布　　2021-10-9 实施

中国银行保险监督管理委员会　发布

目　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国金融标准化技术委员会保险分技术委员会（SAC/TC 180/SC1）提出并归口。

本文件起草单位：中国太平洋保险（集团）股份有限公司、中国平安保险（集团）股份有限公司、阳光保险集团股份有限公司。

本文件主要起草人：李丽红、韩梅、王琼、万强、夏蕊、张军、刘鸣、范华、马宁、蔡嘉勇、张扬、高亭宇、赵波、申瑞峰、彭同心、王珩强、熊喆。

本文件为首次制定。

保险移动应用信息安全基本要求

1 范围

本文件规定了保险移动应用系统信息安全风险管理中的安全技术、安全管理方面的基本要求。

本文件适用于保险移动应用系统在需求、设计、编码、测试、发布、运行、维护各阶段的安全建设与管理。

2 规范性引用文件

下列文件的内容通过文中的规范性引用而构成本文件必不可少的条款。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 34975-2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

GB/T 35273-2020 信息安全技术 个人信息安全规范

JR/T 0092-2019 移动金融客户端应用软件安全管理规范

JR/T 0171-2020 个人金融信息保护技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动智能终端 Smart Mobile Terminal

指接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

[来源:GB/T 34975-2017,3.1]

3.2

移动应用软件 Mobile Application Software

指安装或运行在移动智能终端上,通过网络链接服务端进行交互操作的应用程序软件,包括移动App、微信应用、小程序等。

3.3

个人敏感信息 Personal Sensitive Information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[来源:GB/T 35273-2020,3.2]

3.4

签名 Signature

签名，就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

3.5

关键业务 Critical Business

在移动应用系统上进行的、对保险服务用户有重大影响的业务，包括但不限于：投保、给付、变更、理赔、贷款、转账、银行卡绑定、积分兑换等操作，信息变更如修改姓名、身份证、地址、手机号、密码等操作。

4 缩略语

下列缩略语适用于本文件。

APP：客户端应用软件（Application software）

XSS：跨站脚本漏洞（Cross Site Scripting）

NFC：近场通信（Near Field Communication）

5 安全原则

5.1 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。

5.2 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。

5.3 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。

5.4 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。

5.5 个人信息保护原则

APP运营者收集个人信息时，要严格履行网络安全法规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。应始终遵循公开告知原则、合法收集原则、最小化收集原则。

6 安全技术要求

6.1 移动应用客户端安全

6.1.1 安装与卸载

6.1.1.1 安装要求

移动应用软件的安装需得到明确授权，其安装过程只能运行在特定环境中且不能破坏其运行环境。具体技术要求如下：

a) 程序应包含可有效表征供应者或开发者身份的签名信息、软件属性信息；
b) 正确安装到相关移动智能终端上，并提供查询或卸载的途径；
c) 安装时所需的终端数据或权限应提示用户并获取授权；
d) 不应对移动智能终端操作系统和其他应用软件的正常运行造成影响；
e) 移动应用版本更新时，应可正常覆盖安装，并保留上个版本的数据。如版本更新后移动智能终端的资源调用和权限发生变动，应提示用户并获取授权。

6.1.1.2 卸载要求

移动应用软件卸载后，不影响移动智能终端的正常使用。具体技术要求如下：

a) 应能删除安装和使用过程中产生的资源文件、配置文件和用户数据；
b) 删除用户使用过程中生成的数据时应有提示。

6.1.2 源代码安全

客户端的源代码应保证保密性、完整性。具体技术要求如下：

a) 移动应用的源代码应采用混淆（IOS 应用）或加壳（Android 应用）等措施防止反编译及动态调试；
b) 移动应用应具备源代码完整性校验能力；
c) 移动应用应对签名信息进行安全校验；
d) 应删除移动应用中敏感的冗余或注释代码。比如开发人员信息、调试信息等。

6.1.3 组件安全

Android移动应用软件应合理设置自身组件权限。具体技术要求如下：

a) 若组件不需要与其他 App 共享数据或交互，应设置 APP 组件的 exported 值为 false，防止 APP 自身不必要的组件暴露；
b) 若组件需要与其他 App 共享数据或交互，应对组件进行权限控制和参数校验。

若移动应用软件使用第三方组件，应保证第三方组件使用安全性。具体技术要求如下：

a) 移动应用软件应对组件权限进行限制，避免第三方移动应用随意调用组件内容；
b) 移动应用软件应对组件进行安全配置，避免发生劫持组件的安全问题；
c) 移动应用软件应避免使用有漏洞的开源第三方应用组件及代码。

6.1.4 算法安全

移动应用软件应保证密码算法的安全性，应保证密钥生成、存储、使用过程的安全性。具体技术要求如下：

a) 密码算法应符合国家密码管理局的有关要求；
b) 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；
c) 密钥使用时，应采取必要的安全防护措施，防止密钥被非法使用；
d) 密码传输时，应保证传输过程的安全，防止中间人窃取密钥；
e) 密钥泄露时，应停止使用，并启动相应的应急处理和响应措施；

f） 应按照密钥更换周期要求更换密钥。

6.1.5 数据安全

6.1.5.1 数据完整性

在移动应用软件上，组件是构成业务或者功能模块的基本单位，个人敏感信息在本地程序组件间或通过公共网络传输时，应采取措施（如数字签名等）确保其完整性。客户端应用软件与本地其他应用软件间传输个人敏感信息时，应采取措施确保其完整性。

6.1.5.2 数据保密性

移动应用软件应保证数据传输、存储过程中的保密性。具体技术要求如下：

a） 移动应用软件中的个人敏感信息通过公共网络传输时应采取加密措施，保证个人敏感信息传输的保密性。

b） 客户端应用软件与本地其他应用软件间传输个人敏感信息时，应采取措施确保其保密性；

c） 存储个人敏感信息，应采用加密等安全措施；存储个人生物识别信息时，应采用技术措施处理后再进行存储。

6.1.5.3 数据不可抵赖性

通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字签名技术。

6.1.6 权限安全

6.1.6.1 基于用户的控制

用户访问移动应用软件应明确用户的授权范围。具体技术要求如下：

a） 移动应用软件应对访问用户进行有效的访问控制，保证授权用户访问的内容不能超出授权的范围；

b） 敏感业务如大额资金交易类的用户登陆应采用双因素认证方式，具体依据 JR/T 0092-2019 中 5.1 的要求。

6.1.6.2 对应用软件的限制

移动应用软件访问移动智能终端数据应得到用户明确的许可。具体技术要求如下：

a） 未得到许可前不应访问、修改、删除和对外传输移动智能终端数据；

b） 移动应用软件向用户申请终端权限时，应遵循权限最小化原则。

6.1.6.3 对后台管理的限制

应保证移动应用软件的后台管理安全，移动应用软件的后台管理界面不能向互联网暴露。

6.1.7 日志安全

6.1.7.1 日志存储安全

在程序运行结束后，客户端不应在本地存储个人敏感信息。如需存储，应对相关数据采用操作系统提供的文件加密函数或其他符合国家密码管理局要求的算法进行加密保护。

系统为验证用户身份真实性而在客户端采集的个人敏感信息不应保存在本地日志中，也不应发送到服务器中。

6.1.7.2 日志运行安全

客户端运行时不应生成与业务运行流程相关的日志数据。

客户端运行时不应生成含有个人敏感信息的日志数据。

6.1.8 通信安全

客户端程序处理与服务器交互个人敏感信息时，应采用安全加密传输协议保证数据的保密性、完整性和不可抵赖性。

个人敏感信息加密传输时，应采用权威的加密算法对数据进行安全防护，并应采用适当的密钥长度。不应利用私有加密算法进行通信防护。

客户端和服务端之间的通讯如经过第三方服务器时，应建立服务端和客户端之间的安全通道，避免信息被第三方获取或修改。

6.1.9 环境安全

6.1.9.1 开发环境安全

软件开发使用的工具应确保来源可靠。

代码存储应采取合理措施防止代码泄漏或外传。

开发用机应安装终端安全管控软件。

开发用机应安装防恶意代码的安全防护软件，并保持软件特征库的有效性和实时性。

开发环境应实行网络控制，与外网隔离。

开发测试环境应和生产环境有效隔离，测试数据不应涉及真实信息且需受到严格控制。控制手段包括但不限于严格控制测试软件的分发、严格控制测试账号的分发等。

实施信息化工作外包的公司，在签订外包服务合同时，应同样遵循如上要求。

6.1.9.2 运行环境安全

涉及敏感操作内容的客户端应能够对运行环境进行检测（如Android的ROOT机和IOS的越狱机），并对其进行相应的提示。例如可限制具有敏感操作行为的移动应用在ROOT或越狱等环境下使用。

客户端运行过程中应能够监测运行环境的变化，防止移动应用程序被恶意劫持。

客户端程序应具有明确的程序包名和版本序号，设计合理的更新接口，当某一版本被证明存在安全隐患时，应提示并强制要求用户更新客户端。

应安排专门的人员或团队跟踪监控客户端程序的下载和使用情况，并应及时处理异常情况。

存在重大安全隐患和旧版本的客户端程序，应及时下架。

6.2 移动应用服务端安全

6.2.1 身份及访问控制

6.2.1.1 身份认证

移动应用软件应对访问用户进行身份认证。基本技术要求如下：

a) 在用户访问应用业务前，移动应用软件对其身份进行鉴别，并提供鉴别失败处理措施，提供通用错误提示信息，避免提示信息被攻击者利用；

b) 移动应用软件应具有登录失败处理功能，应配置并启用限制非法登录次数等措施；

在进行业务确认、支付、信息采集或修改等关键业务操作场景下，还应满足以下要求：

a) 应采用多因素认证；

b) 应进行二次鉴权。

在进行个人敏感信息输入的场景下，应使用自定义软键盘。具体技术要求如下：

a) 在交易支付、查询等数字密码输入场景应使用自定义软键盘的按键随机分布；
b) 应取消自定义软键盘按键的回显，或缩短其回显时间。

6.2.1.2 口令安全机制

若移动应用软件使用过程中涉及用户口令功能。具体技术要求如下：

a) 在使用过程中不应以明文形式显示和存储；
b) 不应默认保存用户上次的账号及口令信息；
c) 具备口令强度检查机制，口令长度应不少于8位字符，至少包含字母、数字；
d) 具备口令时效性检查机制；
e) 修改或找回口令时，具备验证机制。

6.2.1.3 验证码安全

移动应用软件在使用图形验证码时，基本技术要求如下：

a) 图形验证码需由服务端生成并进行验证，不得在页面源文件返回；
b) 图形验证码应采取一定的干扰措施且不可预测；
c) 验证码在客户端每次提交后服务器自动更新失效验证码；验证码应具有有效期。

移动应用软件在使用短信验证码时，基本技术要求如下：

a) 控制短信发送频率，且应由服务端控制发送频率，避免客户端绕过形成短信炸弹；
b) 短信验证码必须通过服务端校验；
c) 对验证码提交次数做限制，使用数次后失效；
d) 使用正确验证码成功登录后需使其失效，防止被重用。

6.2.2 会话安全

移动应用软件应保证会话安全。具体技术要求如下：

a) 应采取会话保护措施，保证软件与后台服务器之间的会话不可被窃听、篡改、伪造、重放等；
b) 应设计合理的账户登录超时控制策略，当用户闲置在线状态超出时限时，移动应用软件自动退出登录状态；
c) 用户登录后需要使用新的会话标识，并且会话标识的生成应具有随机性；
d) 用户在移动应用软件注销会话后，服务端应同步使用户会话失效；
e) 避免在 URL、错误信息或日志中暴露会话标识符，会话标识符应当只出现在 HTTP 头信息中；
f) 限制应用用户账号的多重并发会话；
g) 限制同一设备或用户在单位时间内的查询次数；
h) 设备环境变更后，应使会话失效。

6.2.3 数据安全

移动应用软件服务端在进行敏感数据传输及存储时应加密或者混淆处理，具体技术要求如下：

a) 非业务上的必要，个人敏感信息在终端上展示时应做模糊处理，且应在后台进行敏感字段脱敏处理，如部分内容以*方式传输及显示；
b) 配置文件中对个人敏感信息进行加密；
c) 用户注销账号后，应删除其个人敏感信息或做匿名化处理；
d) 移动应用软件服务端的数据应定期备份，备份介质应妥善保管。

6.2.4 异常处理

移动应用系统在发现异常访问或出故障时应有相应的处理措施。具体技术要求如下：

a) 应统一出错提示，应避免个人敏感信息泄露及显示详细错误信息；
b) 应对Android类APP添加运行时顶层activity界面检测机制，以防御activity界面劫持攻击；
c) 对于用户提交数据的字符类型、长度、格式和范围进行限制及验证，防止缓冲区溢出及其他不可预知的异常；
d) 文件上传应该验证文件的类型，只允许用户上传规定格式的文件；
e) 服务器应对通过系统界面提交的所有参数进行过滤，如“'”，“--”，“&”，“<”，“>”，“/”，“=”，“#”，“\r\n”，“\n\n”，“；”等字符，防止常见的SQL注入、XSS攻击等攻击行为；
f) 后台应保存详细的错误信息，支持运维人员及开发人员对故障进行分析定位。

6.2.5 日志安全

服务器端不应向客户端输出异常调试信息日志，防范服务器端信息泄露，如开发框架、调用堆栈信息等。

6.3 业务安全

6.3.1 业务流程管理

对移动应用的业务流程，应满足如下安全要求：

a) 业务流程应满足行业监管要求，并针对业务风险采取相应的控制措施，防范风险发生；
b) 移动应用如涉及用户个人信息的收集、使用等，应制定个人信息保护政策，由用户进行明示同意和明确授权，具体按照JR/T 0171-2020中要求执行；
c) 应通过安全有效的方式对客户和代理人的有效身份信息（如身份证件或其他有效身份证明文件）进行核实。对客户和代理人提交的业务资料信息进行核查；
d) 对于涉及高风险或高价值的业务，应在操作前和操作中通过多种方式进行风险提示，对安全控制措施进行说明。应对办理业务的客户或代理人采用多种验证方式进行联合身份验证；
e) 应对客户和代理人提交的个人敏感信息进行妥善保护。确保只有客户或授权人员能够查询、使用。应根据业务需求，查询显示时对个人敏感信息进行脱敏处理；
f) 应确保在移动客户端业务注销环节，与通过自助办理、网点人工办理等不同渠道的操作结果具备同等有效风险控制。经客户同意完成注销后，应同步关闭移动端高风险业务功能，并妥善处置后台客户相关信息；
g) 应建立客户端硬件丢失时，数据安全风险控制机制。

6.3.2 关键业务安全管理

对移动应用的关键业务操作，应满足如下安全要求：

a) 关键业务操作指会对用户造成重大影响的事务操作，主要包括资产类操作和个人敏感信息类操作；资产类操作，对包括不限于资金、保单、有价证券、具有现实价值的积分等对象进行新增、查询、修改（支付）、删除的操作。个人敏感信息类操作，对包括不限于自然人姓名、账户、身份证号、联系电话等对象进行新增、查询、修改、删除的操作；
b) 系统应充分提示客户关键业务操作的安全风险并提供及时通知客户资产、个人敏感信息等的变化；

c) 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，如请求一次性安全验证码时需在此动作前进行二次密码验证等操作，保证一次性安全验证码的请求为授权用户发起；
d) 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；
e) 应在客户端为用户登录与关键业务操作时创建与登录口令不同的二次认证口令，并建议用户在二次认证中选择多因素验证，如一次性安全验证码或生物识别特征；
f) 系统在访问设备数据如通讯录、位置信息等；使用设备资源如摄像头、NFC近场通讯等，应对用户做出明确提示，在用户明确许可之后方可访问和修改设备数据、设备资源、设备配置；
g) 系统应将关键业务操作纳入风险监控范围，并建立风险阈值监控模型，当关键操作明显超出正常模型范围，如短时间内大数量和大金额转账、支付，异地个人敏感信息修改等，应考虑挂起此关键操作，进行业务人工干预和确认。

6.3.3 业务风险监控

在业务风险监控方面应满足如下安全要求：
a) 应当对关键业务进行日志埋点，完善其他类型日志记录，预先制定异常日志识别规则，实时或定期对埋点日志进行分析，使用但不限于时间维度和用户维度分析异常操作行为；
b) 应当做好设备指纹的采集工作，做好设备与用户绑定，应当关注用户更换设备的操作行为；
c) 建议做好异常设备（ROOT或越狱）或异常应用（应用重打包）的识别工作，并重点关注该类用户的操作行为；
d) 重点关注账户安全，应做好防止爆破和撞库等攻击的措施；
e) 重点关注支付/积分等功能，对大额支付做到人工核验，对疑似异常交易（切换设备，设备越狱，不在常住地，非正常时间段等）开启短信二次验证；多次错误交易锁定账户，并进行人工核验；
f) 重点关注奖励/抽奖等业务，结合自身业务特点，应有效识别虚假注册/薅羊毛等行为；
g) 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；
h) 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；
i) 应加强服务人员的风险防范培训，以正确引导客户使用保险移动业务。

7 安全管理要求

7.1 组织架构

组织架构应满足如下要求：
a) 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；
b) 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。

7.2 安全管理制度

管理制度应满足如下要求：
a) 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；
b) 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；

c） 应建立移动应用的个人信息保护政策，对于个人信息的收集、使用、保护等进行说明。如移动应用安装时如涉及个人信息收集等应公开、征得用户明示同意，并遵循最小需要原则。移动应用应以最小需要原则访问智能终端的其他信息（如通讯录、短信息、麦克风、摄像头、照片、位置信息等）；

d） 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；

e） 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；

f） 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；

g） 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，以确保客户资料等个人敏感信息的安全，降低因外包服务中断给移动业务持续运行带来的影响。

7.3 生命周期管理

7.3.1 概述

生命周期安全管理要求指移动应用在需求、设计、开发、测试、交付运营的风险防范与应对能力。

7.3.2 需求阶段

需求分析阶段是移动应用开发过程的重要阶段，对移动应用需要实现的功能进行详细分析，应遵循但不限于以下安全要求：

a） 移动应用产品需求阶段，应充分将本标准涉及的安全要求纳入到安全设计方案中；

b） 应建立内部安全需求库，持续完善移动应用安全要求；

c） 应将相关行业安全规范纳入到安全要求中。

7.3.3 设计阶段

设计阶段是对移动应用进行设计，应遵循但不限于以下安全要求：

a） 应对移动应用进行威胁建模，全面发现其威胁点；

b） 应针对每一个威胁点，研究相应的应对措施，并应用到移动应用的设计过程。

7.3.4 开发阶段

开发阶段是移动应用的具体实现阶段，应遵循但不限于以下安全要求：

a） 开发过程中应建立完备的安全编码规范体系；

b） 对于通用开发技术，应建立专用的模块库；

c） 开发过程中应建立完善的代码审核机制。

7.3.5 测试阶段

本阶段应遵循但不限于以下安全要求：

a） 测试阶段应有完善的安全测试方法（包括白盒测试和黑盒测试）；

b） 测试项以本标准安全要求为准。

7.3.6 交付阶段

交付的移动应用应满足但不限于以下安全要求：

a） 交付的移动应用应具备适当的抵御恶意攻击的能力。如防范反汇编和二次打包攻击能力；

b） 交付的渠道应安全可靠，应具备对移动应用软件进行安全评估的能力，具备一定防范相关交付风险的能力。

7.3.7 运营阶段

本阶段保障移动应用的正常运行，应满足但不限于以下安全要求：

a） 运营阶段应建立快速响应平台，对发现的安全漏洞应有快速修复的能力；

b） 应对提供的移动应用进行安全监控，发现安全风险并为用户提供安全更新。

生命周期安全管理要求由移动应用所有者依据自身安全需求进行选用。

参考文献

[1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 34975-2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法
[3] GB/T 35273-2020 信息安全技术 个人信息安全规范
[4] JR/T 0092-2019 移动金融客户端应用软件安全管理规范
[5] JR/T 0171-2020 个人金融信息保护技术规范
[6] SZDB/Z 204-2016 金融服务移动应用信息安全指南
[7] 保险公司信息化工作管理指引(试行)（保监发〔2009〕133号）