T/SZFCC

苏州市金融业商会团体标准

T/XXX XXXX—XXXX

保险数字科技支付应用安全管理要求

Security management requirements for digital technology payment applications in the insurance industry

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

XXXX - XX - XX 实施

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 总体要求	1
5 应用安全要求	1
5.1 安全分级	1
5.2 身份认证安全	2
5.3 逻辑安全	3
5.4 安全功能设计	4
5.5 密码算法及密钥管理	4
5.6 数据安全	5
6 应用管理要求	6
6.1 设计要求	6
6.2 开发要求	6
6.3 发布要求	7
6.4 维护要求	7
参考文献	8

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

保险数字科技支付应用安全管理要求

1 范围

本文件规定了应用软件的总体要求、应用安全要求和应用管理要求。

本文件适用于开展保险支付业务的各类主体，包括但不限于保险公司、保险经纪公司、保险代理公司，以及提供保险支付技术服务的第三方科技公司。

2 规范性引用文件

下列文件中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。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239 信息安全技术 网络安全等级保护基本要求
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 39786 信息安全技术 信息系统密码应用基本要求
JR/T 0071（所有部分） 金融行业网络安全等级保护实施指引

3 术语和定义

下列术语和定义适用于本文件。

3.1

保险数字科技支付应用 insurance digital technology payment application

依托大数据、人工智能、区块链、移动互联等数字技术，在保险业务全流程中实现支付环节数字化、智能化升级的应用体系。

注：全文简称“应用软件”

3.2

支付敏感信息 payment-sensitive information

在支付交易过程中产生、传输或存储，一旦泄露、滥用、篡改或丢失，可能导致用户财产安全受到威胁、身份被冒用或支付系统安全受损的关键数据。

3.3

动态模块 dynamic module

在软件系统、程序或应用运行过程中，能够被动态加载、卸载、更新或替换的功能单元或代码模块。

4 总体要求

4.1 应用软件分为资金交易类、信息采集类和资讯查询类，具体要求如下：

- a) 资金交易类应用软件应符合资金交易、信息保护等所有技术及管理安全要求；
- b) 信息采集类应用软件应重点符合信息保护相关技术及管理安全要求；
- c) 资讯查询类应用软件参照执行相关应用安全和管理要求。

4.2 保险支付科技应用包含多种关键系统及功能模块，实现保险业务从投保到理赔全流程的数字化支付与管理。

4.3 通过数字化手段，应用可对保险账户进行精准管理，方便保险公司及客户随时查询与核对信息，提升客户服务质量与满意度。

4.4 网络信息安全应符合 GB/T 22239 的具体要求，明确安全物理环境、通信网络等多维度要求。

5 应用安全要求

5.1 安全分级

不同业务场景、不同机构规模面临的风险等级和所能投入的安全资源差异大，应根据应用所处理的资金额度、数据敏感性、业务关键性等因素，应符合JR/T 0071（所有部分）的要求，划分要求如下：

- a) 基础级：适用于纯信息查询、小额保费续缴等低风险场景，强制执行标准中的核心安全要求；
- b) 增强级：适用于投保支付、大额理赔、账户信息修改等高风险场景。

5.2 身份认证安全

5.2.1 认证方式

5.2.1.1 支持多种认证方式，包括但不限于用户名/密码、短信验证码、指纹识别、面部识别、数字证书等。应根据业务风险等级，为用户提供单因素或多因素组合认证方式，具体要求如下。

- a) 应用软件登录时应采用适宜的验证要素，包括但不限于口令、短信验证码、手势密码、生物特征识别等方式；
- b) 应确保采用的身份验证要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露，如：用于登录验证的口令和用于交易的口令不能一致；
- c) 应用软件交易时应按照相关业务管理要求对用户身份进行认证，根据风险策略自行定义大额资金阈值并文档化；
- d) 对于手势密码、短信验证码、生物特征信息作为验证要素或验证要素组合中的一种时，应满足如下要求：
 - 1) 若采用手势密码作为验证要素，手势密码应至少设置连续不间断的4个点；
 - 2) 若采用短信验证码作为验证要素，短信验证码应仅使用一次，仅限于在规定时间内使用，短信验证码应具备长度和随机性的要求，短信验证码所在的短信内容中，应告知用户短信验证码的用途；
 - 3) 若采用生物特征识别作为验证要素，应当符合国家、金融行业标准和相关信息安全管理要求，防止非法存储、复制和重放。
- e) 若采用图形验证码作为验证的辅助要素，图形验证码应具有使用时间限制并仅能使用一次，图形验证码应由服务器生成，保险数字科技支付源文件中不应包含图形验证码的文本内容。
- f) 图形验证码不应作为独立的身份验证要素。

5.2.1.2 应用软件登录应采用两种或两种以上的要素对用户身份进行认证。在用户身份认证后，应用软件进入终端系统后台时，如果超过设定时限后被唤醒切换到前台，应采取措施对用户身份重新认证。

5.2.2 认证信息安全

5.2.2.1 安全输入要求如下：

- a) 用户认证信息在存储和传输过程中应进行加密处理。采用高强度加密算法，对密码进行加密存储，防止认证信息在数据库中被窃取；
- b) 在传输时，使用SSL/TLS（安全套接层/传输层安全）协议加密通信链路，做到认证信息在网络传输过程中不被监听获取。同时，定期更新加密密钥，增强加密安全性；
- c) 应用软件应提供客户输入银行卡支付密码和网络支付交易密码的即时防护功能，保险数字科技支付应提供以下安全控制措施，或其他经攻击测试无法获取明文的安全防护措施；
- d) 应用软件应提供客户输入信息的即时防护功能，如：卡片验证码、卡片有效期、银行卡账号、身份证号码、手机号码等信息。

5.2.2.2 个人信息应符合GB/T 35273的要求，具体要求如下：

- a) 应用软件的口令框应默认屏蔽显示，屏蔽显示时应使用同一特殊字符代替；
- b) 应用软件不应明文显示银行卡密码和网络支付交易密码；
- c) 应用软件展示个人金融信息时，应符合以下要求。
 - 1) 处于未登录状态时，不应展示与个人信息主体相关的用户鉴别信息；
 - 2) 处于已登录状态时，银行卡号、客户法定名称、手机号码、证件类或其他识别标识信息等可以直接或组合后确定信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应履行身份验证，并做好此类信息管理，防范此类信息泄漏风险。

5.2.3 认证失败处理

- 5.2.3.1 当用户认证失败时，系统应限制连续尝试次数，如连续3次认证失败后，锁定账户一定时间。
- 5.2.3.2 应用软件应提供认证失败处理功能，可采取结束会话、限制失败登录次数和自动退出等措施。
- 5.2.3.3 在提示客户认证失败时，应模糊错误提示信息，防止错误提示信息中泄露用户全部账号、交易金额等敏感数据。

5.2.4 密码设定与重置

- 5.2.4.1 应用软件应配合服务端提供密码复杂度校验功能，保证用户设置的密码达到一定的强度，避免采用简单交易密码或与客户个人信息相似度过高的交易密码。
- 5.2.4.2 应严格限制使用初始登录密码与初始交易密码，具体要求如下：
 - a) 设置初始密码，应强制用户在首次登录后修改初始密码；
 - a) 修改密码前，应对用户身份进行重新验证；
 - b) 修改密码时应对原密码输入错误次数进行限制；
 - c) 修改密码时新密码不应与原密码相同；
 - d) 密码重置时，应使用短信验证码、用户注册信息校核等方式，对用户身份进行校验。
- 5.2.4.3 应采取技术性建议或限制客户设置与常用软件、网站相同或相似的用户名和密码组合，并采取有效措施引导客户设置独立的支付密码。

5.3 逻辑安全

5.3.1 逻辑安全设计

- 5.3.1.1 在系统设计阶段，进行全面的安全需求分析与风险评估，识别潜在逻辑漏洞。采用安全设计模式，如访问控制列表（ACL）、最小权限原则等，确保系统各模块间数据访问与操作的安全性。
- 5.3.1.2 对于认证、校验等安全保证功能的流程设计应充分考虑其合理性，避免逻辑漏洞的出现，确保认证流程无法被绕过。
- 5.3.1.3 对于交易处理功能逻辑设计应充分考虑其合理性，避免逻辑漏洞的出现，保证资金交易安全。
- 5.3.1.4 应用软件代码实现应尽量避免调用存在安全漏洞的函数，避免敏感数据硬编码。

5.3.2 应用权限控制

- 5.3.2.1 根据用户角色与业务需求，精细划分应用操作权限。
- 5.3.2.2 权限分配应遵循最小必要原则，避免权限过大导致的安全风险。定期对用户权限进行审查与更新，确保用户权限与实际工作需求相符。

5.3.3 风险控制

- 5.3.3.1 应建立实时风险监测与预警机制，对异常交易行为进行监控。
- 5.3.3.2 运用大数据分析技术，对历史交易数据进行建模分析，设定风险阈值，当交易行为偏离正常模型达到阈值时，宜及时发出风险提示。
- 5.3.3.3 应设计合理的登录风险控制策略，包括但不限于：
 - a) 当用户闲置在线状态超出时限，应设计合理的账户登录超时控制策略；
 - b) 合理的多点登录策略，如：提示登录信息或退出先登录的账户等策略；
 - c) 合理的长期未登录控制策略，当用户长时间未登录时，应综合考虑风险情况，增大认证强度。
- 5.3.3.4 应设计合理的交易风险控制策略，包括但不限于：
 - a) 针对不同的资金交易金额，应设计合理的身份认证策略；
 - b) 针对不同的资金交易业务场景，应设计合理的策略，如：限额控制策略、时限控制策略等。
- 5.3.3.5 应用软件应配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。

5.3.4 回退处理

在业务操作过程中，如投保、理赔等涉及资金变动的操作，若因系统故障、网络中断等原因导致操作失败，系统应具备自动回退功能，确保数据一致性与完整性。

5.3.5 异常处理

5.3.5.1 对于系统运行过程中出现的各类异常情况，如程序错误、数据库连接失败、网络超时等，系统应进行妥善处理。向用户提供安全的错误提示信息，避免泄露系统内部敏感信息。

5.3.5.2 应将异常信息详细记录到日志文件中，包括异常发生时间、位置、错误类型等，便于技术人员及时定位与解决问题。对常见异常情况，设置自动恢复机制，提高系统稳定性。

5.4 安全功能设计

5.4.1 组件安全

5.4.1.1 应用软件应避免使用存在已知漏洞的系统组件与第三方组件。在使用第三方组件时，应避免第三方组件未经授权收集应用软件信息和个人信息。

5.4.1.2 对应用所使用的第三方组件、开源库进行每年至少一次定期的安全评估与漏洞扫描。及时更新存在安全漏洞的组件版本，如发现开源库存在高危漏洞，在官方发布修复版本后，应在规定时间内完成更新。

5.4.1.3 建立组件白名单机制，允许使用经过安全认证的组件，不应引入恶意或存在安全隐患的组件。对自研组件进行严格的代码审查与安全测试，确保组件安全性。

5.4.2 接口安全

5.4.2.1 应用软件应对软件接口进行保护，防止其他应用对应用软件接口进行非授权调用。

5.4.2.2 应用软件应对所有外部输入(包括 URI、Header、Body 等)进行严格的输入验证、过滤和编码，不宜软件运行异常或操作异常。

5.4.2.3 当应用软件需要与 TEE、SE 结合使用时，应避免使用存在已知漏洞的接口。

5.4.3 抗攻击能力

5.4.3.1 应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。

5.4.3.2 应部署防火墙、入侵检测系统(IDS)、入侵防御系统(IPS)等安全防护设备，对网络流量进行实时监测与过滤，防止外部攻击。

5.4.3.3 定期进行渗透测试，模拟黑客攻击手段，检测系统是否存在安全漏洞。对发现的漏洞及时进行修复，如在发现 SQL 注入漏洞后，应在规定时间内完成修复并进行复测。加强系统自身安全加固。

5.4.3.4 保险数字科技支付代码应使用代码加密、代码混淆、检测调试器等手段对应用软件进行安全保护。

5.4.3.5 应用软件安装、启动、更新时应应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

5.4.3.6 应用软件应使用安全输入控件，有效防护键盘钩子、界面劫持、截屏录屏等常见攻击手段。

5.4.4 应用环境监测

5.4.4.1 对应用运行环境进行实时监测，包括服务器 CPU 使用率、内存占用率、磁盘空间、网络带宽等指标。当指标超出正常阈值时，及时发出预警信息。

5.4.4.2 定期对应用环境进行安全检查，如检查服务器操作系统是否存在未安装的安全补丁、服务器日志是否被篡改等，确保应用环境安全稳定。

5.5 密码算法及密钥管理

5.5.1 密码算法

5.5.1.1 应选用符合国家及行业标准的密码算法，根据业务场景与安全需求，合理选择密码算法强度。

5.5.1.2 在构建安全的信息系统时，应禁止使用已知不安全算法(如 MD5、DES、SHA-1)或默认参数(如 RSA 密钥长度 2048 位)；推荐使用国家密码管理部门推广的国密算法(如 SM2、SM3、SM4)。

5.5.1.3 定期关注密码算法安全动态，对所使用密码算法的新型攻击手段或安全漏洞，及时评估并调整密码算法策略。

5.5.1.4 应用软件应使用密码算法对资金有关交易或重要业务操作进行保护。

5.5.1.5 密码算法、密钥长度及密钥管理方式应符合国家密码主管部门的要求。

5.5.2 密钥管理

5.5.2.1 应建立完善的密钥管理系统，对密钥的生成、存储、分发、使用、更新与销毁全生命周期进行严格管理，应符合 GB/T 39786 的要求。

5.5.2.2 密钥生成应采用安全随机数生成器，确保密钥的随机性与不可预测性。密钥存储应采用加密方式。密钥分发应采用安全渠道，通过加密通信链路或专用密钥传输设备。

5.5.2.3 密钥在传输过程中应使用密码算法对密钥进行保护，随机生成的密钥应具有一定的随机性与不可预测性。

5.6 数据安全

5.6.1 数据获取

应用软件数据获取的要求如下。

- a) 数据防窃取：
 - 1) 采用访问控制、加密存储、数据脱敏等措施防止数据被窃取；对存储在数据库中的敏感数据进行加密存储；在数据展示与传输过程中，对敏感信息进行脱敏处理；
 - 2) 应用软件应保证内存中不存在完整的银行卡密码和网络支付交易密码明文；
 - 3) 应用软件的临时文件中不应出现支付敏感信息，临时文件包括但不限于 Cookies、本地临时文件等；
 - 4) 应用软件程序应禁止在身份认证结束后存储支付敏感信息，防止支付敏感信息泄露；
 - 5) 应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。
- b) 数据防篡改：运用数字签名、数据校验码等技术保证数据完整性，防止数据被篡改；定期对数据进行完整性检查；
- c) 数据有效性：在数据录入环节，对数据进行严格校验，确保数据格式、范围等符合业务规则；建立数据质量监控机制，对数据准确性、完整性、一致性等进行定期评估与修复；
- d) 数据访问控制：依据用户角色与业务需求，制定细粒度的数据访问控制策略；不同角色限定访问其职责范围内的数据。

5.6.2 数据传输

应用软件数据获取的要求如下。

- a) 通信安全：
 - 1) 应在应用软件与服务器之间建立安全的信息传输通道，协议版本应及时更新至安全稳定版本；
 - 2) 应确保采用的安全协议不包含已知的公开漏洞；
 - 3) 应用软件与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与应用软件之间的安全认证。
- b) 数据保密性：
 - 1) 通过加密算法对传输数据进行加密；确保加密密钥的安全性与保密性，防止密钥泄露导致数据被解密；
 - 2) 敏感数据（如：登录口令、支付敏感信息等）在应用软件与本地其他应用软件间传输时，应采取加密等措施确保其保密性，若本地其他应用软件不能提供与金融保险数字科技支付软件相应等级的加密接口，则应评估敏感数据调用的风险，并设计补救措施；
 - 3) 敏感数据（如：登录口令、支付敏感信息等）在通过公共网络传输时，应采取加密等措施确保其保密性。
- c) 数据完整性：
 - 1) 利用数字签名等保证数据在传输过程中不被篡改；
 - 2) 关键的交易数据，应在技术可行的情况下，优先采用加密等措施（如：数字签名、MAC 等）确保其完整性，若无法实现，则应进行充分的风险评估并有书面记录，同时在用户协议中明确告知风险；
 - 3) 关键的交易数据、个人身份信息，如：收款人信息、交易金额、订单号、身份证号码等，在通过公共网络传输时，应采取保护措施（如：数字签名、MAC 等）确保其完整性。

- d) 数据抗抵赖：
 - 1) 通过数字签名技术实现数据抗抵赖功能。发送方对数据进行数字签名，接收方验证签名后，可确认数据来源及发送方无法否认发送过该数据；
 - 2) 在保险理赔数据传输中，利用数字签名确保证据申请方与处理方无法抵赖相关操作。
- e) 数据防重放：
 - 1) 采用时间戳、随机数等机制防止数据重放攻击；
 - 2) 在数据传输中添加时间戳，接收方验证时间戳是否在合理范围内，使用随机数作为一次性标识符，每次数据传输生成不同随机数，确保数据的唯一性与不可重复性。

5.6.3 数据存储

5.6.3.1 应用软件不应以任何形式存储用户的支付敏感信息与金融业务查询口令。在满足法律、管理规定的情况下，应用软件应仅保存业务必需的个人金融信息，并限制数据存储量。

5.6.3.2 应用软件应确保无法通过逆向工程等手段直接从本地文件系统中恢复完整的密钥明文。

5.6.4 数据展示

5.6.4.1 在数据展示时，对敏感信息进行脱敏处理，隐藏身份证号、银行卡号、手机号码中间部分数字。

5.6.4.2 根据用户权限，展示相应级别的数据，对数据展示页面进行安全加固，防止通过页面源代码获取敏感信息。

5.6.5 数据销毁

应用软件数据获取的要求如下。

- a) 残余信息保护：
 - 1) 在数据销毁时，确存储介质上的数据无法恢复；
 - 2) 应用软件应在敏感数据使用完毕后，对其立即进行清除；
 - 3) 应用软件进程被结束时，应清除非业务功能运行所必须留存的业务数据，保证客户信息的安全性；
 - 4) 应用软件卸载完成后，文件系统中不应残留任何个人金融信息。
- b) 页面返回保护：应用软件的客户端和服务端联动实现支持页面返回后自动清除银行卡密码、网络支付交易密码、登录口令等支付敏感信息的机制；
- c) 会话失效：设置合理的会话超时时间，当用户关闭应用或退出登录时，应终止会话，清除服务端与保险数字科技支付相关会话信息，防止会话恶意利用获取数据。

6 应用管理要求

6.1 设计要求

6.1.1 应用软件设计应遵循安全、可靠、易用、可维护和可扩展等原则，制定用于指导应用软件设计与开发的总体方案。

6.1.2 应用软件应提供易用、风格统一、体验良好的用户界面。

6.1.3 应用软件应遵循合法、正当、必要的原则，不收集与所提供服务无关的个人金融信息。

6.1.4 应用软件收集个人金融信息或用户授权等操作前，应以通俗易懂、简单明了的方式展示个人金融信息收集使用规则，并经个人金融信息主体自主选择同意。

6.1.5 应用软件不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反与用户的约定收集使用个人金融信息。

6.2 开发要求

6.2.1 应用软件开发过程中应遵守严格的开发流程、项目管理流程和编码安全规范，进行完整的测试，引入安全开发生命周期(Secure-SDLC)的概念，将安全活动(如威胁建模代码审计、安全测试)贯穿于开发全过程。

- 6.2.2 应用软件开发过程中应建立并维护开发文档。
- 6.2.3 应用软件开发完成后，应同步完成产品手册、用户手册或提供在线帮助说明功能。
- 6.2.4 应用软件的每次重要更新、升级，应经过严格归档、源代码扫描、发布审核等步骤。

6.3 发布要求

- 6.3.1 在应用发布前，进行全面的安全测试与评估，包括功能测试、性能测试、安全漏洞扫描、渗透测试等。确保应用不存在已知安全漏洞，性能满足业务需求。
- 6.3.2 对发布版本进行数字签名，保证版本完整性与来源可靠性。建立发布审批流程，经安全部门、业务部门等相关部门审批通过后，方可发布应用。发布后，及时向用户推送安全更新信息，提醒用户及时更新应用，修复潜在安全问题。
- 6.3.3 应用软件应有规范的上线发布流程，由应用软件的所有方对应用软件进行签名和保护，标识应用软件的来源和发布者，提供安全可靠的应用软件下载、发布、升级渠道。
- 6.3.4 应用软件应当删除调试或测试中存留的敏感数据。
- 6.3.5 应用软件安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不得篡改、覆盖、删除系统文件和其他软件。
- 6.3.6 应用软件有新版本时，不能未经用户允许自动安装新版本。
- 6.3.7 应用软件应支持动态模块更新，使用加密信道与服务端通信传输更新模块或对更新模块进行签名校验；动态模块更新后，应对动态模块的权限进行严格隔离和限制，不应影响用户使用，不应修改用户已有的安全配置。

6.4 维护要求

- 6.4.1 建立应用安全监控机制，实时监测应用运行状态、安全事件等。对监控数据进行分析，及时发现并处理安全隐患。
- 6.4.2 定期对应用进行性能优化，确保应用高效稳定运行。
- 6.4.3 建立应急响应机制，当发生安全事件时，能够快速响应与处置，启动应急响应流程，采取相应措施降低损失。
- 6.4.4 应制定科学、合理的管理策略和执行制度，指导各类角色的工作协同、实施步骤、质量管控、安全检测等，规范日常运维流程。
- 6.4.5 应用软件应具有明确的应用标识符和版本序号，设计合理的更新接口，当某一版本被证明存在安全隐患时，应及时进行修复更新。
- 6.4.6 以 SDK 等形式对外提供金融交易类服务时，应记录 SDK 信息及引用本 SDK 的外部应用软件信息。

参 考 文 献

- [1] 《中华人民共和国网络安全法》
 - [2] 《中华人民共和国数据安全法》
 - [3] 《中华人民共和国个人信息保护法》
-