《保险数字科技支付应用安全管理要求》
团体标准编制说明

一、立项的意义

当前，保险行业数字化转型深入推进，数字科技与支付业务深度融合，移动支付、区块链等技术广泛应用，带来业务创新的同时，也产生网络攻击、数据泄露、交易欺诈等新型风险，而现有标准难以适配保险业务特性，存在监管空白。

该规范立项，将构建覆盖保险支付全流程的安全管理体系，明确保险机构、支付平台等多方权责，规范新兴技术应用，有效防范系统性风险。从行业发展看，可提升机构风控能力，降低合规成本，促进行业协同；对监管而言，为政策落地提供抓手，增强监管效能；对消费者，通过严格的数据保护与身份核验机制，保障资金与信息安全。规范的制定是推动保险行业数字化转型安全、有序发展的关键举措，对维护金融安全、促进行业高质量发展具有战略意义。

二、本标准适用范围及概要

（一）适用范围

《保险数字科技支付应用安全管理要求》适用于开展保险支付业务的各类主体，包括保险公司、保险经纪公司、保险代理公司及提供保险支付技术服务的第三方科技公司。

（二）概要

1.总体要求：将保险数字科技支付应用分为资金交易类、

信息采集类和资讯查询类，明确不同类型应用的安全管理重点（如资金交易类需符合全流程安全要求，信息采集类侧重信息保护），覆盖投保到理赔全流程数字化支付与管理。

2.应用安全要求：

（1）身份认证：支持多因素认证（如用户名/密码、生物识别等），要求交易时根据风险等级采用单因素或多因素组合认证，敏感信息加密存储传输，限制认证失败尝试次数。

（2）逻辑安全：强调系统设计阶段的风险评估与漏洞识别，遵循最小权限原则分配权限，建立实时风险监测与交易回退机制，防范逻辑漏洞导致的安全风险。

（3）安全功能设计：要求避免使用存在漏洞的组件，保护接口安全，部署防火墙、入侵检测系统等防护设备，通过代码加密、混淆等手段提升抗攻击能力。

（4）密码与数据安全：采用符合国家标准的密码算法，严格密钥全生命周期管理；数据采集、传输、存储各环节实施加密、脱敏、访问控制，防止数据泄露或篡改。

3.应用管理要求：对设计、开发、发布、维护全流程提出规范，包括遵循数据最小收集原则、严格代码安全测试、发布前安全评估与数字签名、建立应急响应机制等，确保应用全生命周期安全可控。

三、国内外相关标准情况

随着金融科技的快速发展，保险数字科技支付应用的安

全至关重要。国内外出台了众多相关标准，与《保险数字科技支付应用安全管理要求》相互关联、相互补充，共同保障支付安全。这些标准从信息安全、支付系统安全、数据安全等多个维度出发，为保险数字科技支付应用提供了全面的安全规范和指导。

1. 国内相关标准

《保险移动应用信息安全基本要求》：属于推荐性行业标准，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，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，与《保险数字科技支付应用安全管理要求》一样聚焦保险领域的应用安全，不过该标准侧重移动应用系统全生命周期的信息安全管理，而《保险数字科技支付应用安全管理要求》更强调支付应用的安全管理，二者在保障保险行业数字化安全方面具有互补性。

《第三方支付服务信息系统安全框架指南》（ISO/TS 9546）：由网联清算公司牵头制定的国际标准，但在中国也有重要应用。该标准对第三方支付服务的安全框架、设计原则、功能要求等方面进行了规范，有助于增强信息系统安全、降低支付交易风险、保障用户资金安全。《保险数字科技支付应用安全管理要求》在支付安全管理上可参考其安全框架和功能要求等内容，尤其是涉及第三方支付服务时，能借鉴

该标准完善自身安全规范。

《银行保险机构数据安全管理办法》：国家金融监督管理总局发布，对银行保险机构的数据安全管理组织架构、数据全生命周期管理、安全技术保护等提出具体要求。《保险数字科技支付应用安全管理要求》在数据安全管理部分，如数据分类分级、数据处理安全等方面，可与该办法相呼应，确保保险支付应用的数据安全符合行业监管要求。

2.国外相关标准

PCI DSS认证（支付卡行业数据安全标准）：是全球适用于处理信用卡信息App的标准，核心要求包括持卡人数据加密、漏洞管理、访问控制等，且需年审维护。若保险数字科技支付应用涉及信用卡支付等业务，可参考PCI DSS认证标准来加强支付卡信息的安全保护，《保险数字科技支付应用安全管理要求》在相关业务场景下可借鉴其对支付卡数据安全管理的要求，提升自身安全防护水平。

支付应用数据安全标准（PA DSS）：是国际上保障支付应用程序安全的最佳实践标准，旨在帮助软件供应商和其他机构开发安全的支付应用系统，确保禁止存储的数据不被保存，减少数据泄露事件。《保险数字科技支付应用安全管理要求》在应用程序安全开发、敏感数据存储管理等方面，可参考PA DSS的理念和要求，完善自身的应用安全规范。

四、标准编制原则和主要技术内容确定的依据

《保险数字科技支付应用安全管理要求》的编制旨在应对保险行业数字化转型中支付安全的挑战。其编制原则与主要技术内容确定依据，紧密围绕行业需求、法律法规、技术发展趋势等多方面因素，以保障保险数字科技支付应用的安全、可靠、合规运行。

（一）标准编制原则

遵循法律法规原则：以《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等相关法律法规为基础，确保标准在数据安全、信息保护等方面的要求与法律规定保持一致，使保险数字科技支付应用的安全管理有法可依，从法律层面保障用户权益和行业安全稳定发展。

适应行业需求原则：保险行业数字化转型加速，线上投保、理赔等支付场景日益复杂，涉及多方主体和大量敏感信息。该标准针对保险支付业务的特点，如资金交易的安全性、信息采集的合规性等，制定相应的安全管理要求，以满足保险行业在数字科技支付应用中的实际需求，防范各类安全风险。

技术科学性原则：结合当前先进的信息技术，如加密技术、身份认证技术、大数据分析技术等，确保标准中的技术要求具有科学性和前瞻性。例如在密码算法及密钥管理方面，选用符合国家及行业标准的算法，并对密钥进行全生命周期

严格管理，保证数据的保密性、完整性和可用性。

（二）主要技术内容确定的依据

行业实践经验：参考保险机构、第三方科技公司在保险数字科技支付应用中的实践经验，总结过往安全事件的教训和成功的安全管理案例。如在数据安全方面，依据实际业务中数据泄露、篡改等问题的发生情况，制定数据获取、传输、存储、展示和销毁等环节的安全措施，确保数据全生命周期的安全性。

相关标准借鉴：借鉴金融行业信息安全等级保护系列标准、《保险移动应用信息安全基本要求》等相关标准。如在身份认证安全、逻辑安全等方面，参考这些标准中关于认证方式、权限控制等的要求，结合保险支付应用的特点进行细化和完善，使标准既符合行业共性要求，又具有保险支付领域的针对性。

技术发展趋势：随着移动支付、区块链、生物识别等技术在保险支付领域的广泛应用，标准的主要技术内容紧跟技术发展趋势。例如在安全功能设计中，要求应用具备抵御静态分析、动态调试等操作的能力，防止使用存在已知漏洞的系统组件与第三方组件，以适应新技术带来的安全挑战，保障应用的安全性和稳定性。

五、技术保障及工作进度计划

（一）技术保障

1.专业团队组建

成立跨领域技术团队，成员涵盖密码学、网络安全、保险业务等专业人才，负责标准中技术方案的论证与实施。例如，在身份认证安全设计中，由密码专家主导制定多因素认证技术方案，结合保险业务风险等级细化验证规则，确保技术可行性与业务适配性。同时，设立安全开发团队，负责代码审计、漏洞扫描等工作，如在开发阶段采用静态代码分析工具（如SonarQube）排查安全隐患，保障应用程序代码安全。

2.技术合作与交流

加强与行业协会、第三方安全机构的合作，引入外部技术资源。例如，与CA认证机构合作实现数字证书全生命周期管理，确保密钥安全；与网络安全厂商共建威胁情报共享机制，及时获取新型攻击特征，更新入侵防御系统规则。此外，定期组织技术研讨会，邀请国内外专家分享前沿技术（如零信任架构、联邦学习在数据安全中的应用），推动标准技术内容与国际先进实践接轨，提升保险支付应用的整体安全防护水平。等方面提供专业支持，为指南编制提供专业视角和技术建议。

（二）工作进度计划

（一）标准起草阶段（第1～2个月）

1.组建起草组：成立由保险公司、第三方科技公司、行业协会、安全技术专家组成的起草小组，明确分工与职责。

2.现状调研：调研保险行业数字支付应用的安全现状、典型风险案例及现有标准执行情况，收集国内外相关标准（如PCI DSS、《保险移动应用信息安全基本要求》）作为参考。

3.框架设计：结合调研结果，确定标准的总体框架（如范围、术语、安全要求、管理要求），初步划分技术章节（如身份认证、数据安全）和管理章节（如开发、发布、维护）。

（二）技术内容编制阶段（第3～5个月）

1.技术要求细化：

身份认证安全：明确多因素认证组合方式、验证码有效期、生物识别技术标准（如活体检测阈值）。

数据安全：制定数据加密算法选择规则、脱敏策略、存储期限要求（如交易日志保存不超过5年）。

安全功能设计：规定组件白名单审核流程、接口安全测试方法、抗攻击能力测试指标（如抵御10万次/秒并发攻击）。

2.管理要求编制：

开发阶段：明确代码安全规范（如禁止硬编码敏感数据）、测试用例设计要求（覆盖80%以上业务场景）。

发布阶段：制定数字签名流程、漏洞扫描报告审核机制、版本回滚预案。

维护阶段：建立安全监控指标体系（如CPU使用率阈值80%）、应急响应流程（1小时内启动预案）。

3.内部评审：起草组内部对技术内容进行评审，邀请行业专家对密码算法选型、风险模型设计等关键技术点进行论证，形成标准初稿。

（三）征求意见与修改阶段（第6～7个月）

1.公开征求意见：通过行业协会官网、标准平台发布标准征求意见稿，面向保险机构、支付平台、监管部门、用户代表等收集反馈意见。

2.意见汇总与处理：对反馈意见进行分类整理，逐条分析合理性，必要时组织专题研讨会。

3.标准修订：根据意见修改标准初稿，完善技术细节（如调整密码算法强度要求）和管理流程（如简化中小机构合规操作步骤），形成标准征求意见修改稿。

（四）审查与发布阶段（第8个月）

1.专家审查：组织行业主管部门、标准化机构、技术专家召开标准审查会，对标准的合规性、科学性、可操作性进行评审，形成审查意见。

2.报批与发布：根据审查意见修改完善标准，形成最终报批稿，提交行业协会或标准化主管部门审批。审批通过后，按规定程序发布标准，明确实施日期（如发布后3个月正式实施）。

（五）实施与宣贯阶段（第9～10个月）

1.培训与宣贯：组织标准宣贯会，面向保险机构、科技企业开展技术培训，解读标准重点内容（如多因素认证实施步骤、数据脱敏技术方案）。

2.试点应用：选取3～5家不同规模的保险机构进行试点，验证标准在实际场景中的适用性，收集实施反馈并形成案例库。

3.持续改进：建立标准实施评估机制，定期收集行业反馈，根据技术发展（如新型攻击手段、合规要求变化）适时启动标准修订，确保其持续有效。

六、其他需要说明的内容

无。