ICS 03.060
A11

Q/131003L

廊坊市广阳舜丰村镇银行应用程序接口服务企业标准

Q/131003L004—2024

廊坊市广阳舜丰村镇银行应用程序接口服　务

Application programming interface Service of Lang Fang Guang Yang ShunFeng Rural Bank

2024－10－10 发布　　2024－10－10 实施

广阳舜丰村镇银行　　发布

目　　次

前　　言

本标准根据JR/T 0185-2020商业银行应用程序接口安全管理规范起草制定。

本标准由廊坊市广阳舜丰村镇银行股份有限公司提出。

本标准起草单位：廊坊市广阳舜丰村镇银行股份有限公司。

本标准主要起草人：财务会计部

本标准为首次发布

引　　言

本标准内容涉及服务安全技术、操作风险和防范措施、实施保障三个方面，旨在明确应用程序接口服务企业标准，增强应用程序接口安全防范能力，促进应用程序接口服务规范、健康发展。

廊坊市广阳舜丰村镇银行应用程序接口服务企业标准

1 范围

本标准规定了应用程序接口服务要求，明确了安全性和服务标准，确立了服务实施保障机制。

本标准适用于本行所有机构。

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 32315-2015 银行业客户服务中心基本要求

GB/T 35273-2020 信息安全技术个人信息安全规范

JR/T 0171-2020 个人金融信息保护技术规范

JR/T 0185-2020 商业银行应用程序接口安全管理规范

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 术语与定义

下列术语和定义适用于 Q/131003L004—2020 的本标准（本部分）。

3.1

应用程序接口 application programming interface

一组预先定义好的功能，开发者可通过该功能（或功能的组合）便捷地访问相关服务，而无需关注服务的设计与实现。

3.2

移动金融客户端应用软件 Financial mobile application software

在移动终端上为用户提供金融交易服务的应用软件。

3.3

支付敏感信息 payment sensitive information

支付信息中涉及支付主体隐私和身份识别的重要信息。

3.4

个人金融信息 personal financial information

金融机构通过提供金融产品和服务或其他渠道获取/加工和保存的个人信息。

3.5

应用方 application agency

调用商业银行应用程序接口的机构。

3.6

应用程序接口唯一标识 application programming interface unique ID

由商业银行自行定义，用于区分商业银行应用程序接口功能的唯一标识。

4 接口类型与安全级别

4.1 接口类型

商业银行应用程序接口按照应用集成方式，分为服务端对服务端集成方式与移动终端对服务端集成方式两种。

对于服务端对服务端集成方式，主要包含两种实现形式:

应用方服务端直接调用商业银行应用程序接口(如REST、SOAP协议)

一应用方服务端使用商业银行提供的服务端SDK，间接访问商业银行应用程序接口。

其中，服务端SDK主要实现商业银行通用接入算法的封装，为降低应用方接入开发难度，一般此类SK不包含业务逻辑。

对于移动终端对服务端集成方式，主要包含两种实现形式:

应用方移动终端应用软件直接调用商业银行应用程序接口。

应用方移动终端应用软件使用商业银行提供的移动终端应用SDK，间接访问商业银行应用程序接口。

其中，应用方移动终端应用软件直接调用商业银行应用程序接口的方式，主要以与用户个体无直接关联的金融服务为主，如提供商业银行公开信息查询、公开服务查询等。

移动终端应用SDK除封装商业银行通用接入算法外，还可封装业务逻辑、个人金融信息安全保护(例如密码数据的安全加固)等功能。

在移动终端对服务端模式下，对于仅使用H5(超文本标记语言版本5.0)技术，提供银行金融产品和服务访问链接的情况，由于H5页面本身并未直接调用(或封装)商业银行应用程序接口，不将其单独列为商业银行应用程序接口的一种类型。

4.2 安全级别

按照服务类型将商业银行应用程序接口安全级别划分为两级，安全保护要求从A2至A1递减。

A2:资金交易与账户信息查询应用类，此类金融产品和服务与用户个体直接关联，实施高等级安全保护强度，此类商业银行应用程序接口包括但不限于商业银行通过SDK，提供资金交易类服务，如支付、转账以及金融产品与服务购买等:商业银行通过SDK，提供用户账户信息查询类服务，如账户余额、交易历史、账户限额、付款时间、金融产品和服务持有情况等于上述服务，若确需使用API直接连接方式进行服务调用，商业银行应对接入风险进行评估，并制定专门的接口与应用方进行对接，实施高等级的安全保护强度要求。

A1:金融产品和服务信息查询应用类，此类金融产品和服务与用户个体并无直接关联，实施通用的安全保护强度，此类商业银行应用程序接口包括但不限于:商业银行提供银行金融产品和服务的详细信息的“只读”查询服务。

5 安全设计

5.1 设计基本要求

商业银行应用程序接口安全设计基本要求如下:使用的密码算法、技术及产品应符合国家密码管理部门及行业主管部门要求应制定安全编码规范。应对开发人员进行安全编码培训，并依照安全編码规范进行开发。开发中如需使用第三方应用组件，应对组件进行安全性验证，并持续关注相关平台的信息技露和更新情况，适时更新相关组件。应对商业银行应用程序接口进行代码安全专项审计，审计工作可通过人工或工具自动化方式开展应制定源代码和商业银行应用程序接口版本管理与控制规程,规范源代码和商业银行应用程序接口版本管理，并就接口废止、变更等情况与应用方保持信息同步。商业银行向应用方提供的异常与调试信息，不应泄漏服务器、中间件、数据库等软硬件信息或内部网络信息..。

5.2 接口安全设计

5.2.1 身份认证安全

a)接口身份认证安全要求如下:

1)对于应用方身份认证应使用的验证要素包括

—App_ID、App_ Secret。

—AppID、数字证书。

—ApID、公私钥对。

上述三种方案的组合。

2) 对于 A2 级别接口、应用方身份认证时，应使用包含数字证书或公私钥对的方式进行双向身份认证。

b)用户身份认证安全要求如下

1)商业银行应结合金融服务场景,对不同安全级别的商业银行应用程序接口设计不同级别的用户身份认证机制。

3) 用户身份认证应在商业银行执行，对于 A2 级别接口中的资金交易类服务，用户登录身份认证应至少使用双因子认证的方式来保护账户财产安全。

5.2.2 接口交互安全

应用程序接口交互安全要求如下:

应用程序接口应对连通有效性进行验证，如接口版本、参数格式等要素是否与平台设计保持一致。

应对通过商业银行应用程序接口进行交互的数据进行完整性保护，对于 A2 级别的接口，商业银行

和应用方应使用数字签名来保证数据的完整性和不可抵赖性。

对于支付敏感信息等个人金融信息，应采取以下措施进行安全交互:

登录口令、支付密码等支付敏感信息在数据交互过程中应使用包括但不限于替换输入框原文、自定义软键盘、防键盘窃听、防截屏等安全防护措施，保证无法获取支付敏感信息明文账号、卡号、卡有效期、姓名、证件号码、手机号码等个人金融信息在传输过程中应使用集成在 SDK 中的加密组件进行加密，或对相关报文进行整体加密处理;若确需使用商业银行应用程序接口将账号、卡号、姓名向应用方进行反馈，应脱敏或去标识化处理，因清分与清算、差错对账等需求，确需将卡号等支付账号传输至应用方时，应使用加密通道进行传输，并采取措施保证信息的完整性对于金融产品持有份额、用户积分等 A2 类只读信息查询，可使用 API 直接连接方式进行查询请求对接，应采取加密等措施保证查询信息的完整性与保密性，查询结果在应用方本地不得保存。

应在交易认证结束后及时清除用户支付敏感信息，防范攻击者通过读取临时文件、内存数据等方式获得全部或部分用户信息。

5.3 服务安全设计

5.3.1 授权管理

根据不同应用方的服务需求，按照最小授权原则，对其相应接口权限进行授权管理，当服务需求变更时，需及时评估和调整接口权限。

5.3.2 攻击防护

服务安全设计应具备以下攻击防护能力:

API 和 SDK 应对常见的网络攻击具有安全防护能力。

移动终端应用 SDK 应具备静态逆向分析防护能力，防范攻击者通过静态反汇编、字符串分析、导入导出函数识别、配置文件分析等手段获得有关 SDK 实现方式的技术细节。

移动终端应用 SK 宜具备动态调试防护能力，包括但不限于:具有防范攻击者通过挂接动态调试器、动态跟踪程序的方式控制程序行为的能力:具有防范攻击者通过篡改文件、动态修改内存代码等方式控制程序行为的能力。

5.3.3 安全监控

安全监控安全要求如下

——应对接口使用情况进行监控，完整记录接口访问日志。

——日志应满足以下要求：

- 相关日志应至少包括交易流水号、应用唯一标识、接口唯一标识、调用耗时、时间戳、返回结果(成功或失败)等
- 因清分清算、差错对账等业务需要，应用方接口日志中应以部分屏蔽的方式记录支付账号或其等效信息)，除此之外的个人金融信息不应在应用方接口日志中进行记录。

5.3.4 密钥管理

密钥管理安全要求如下:

加密和签名宜分配不同的密钥，且相互分离。

不应以编码的方式将私钥明文(或密文)编写在商业银行应用程序相关代码中， App Secret或私钥不应存储于商业银行与应用方本地配置文件中，防止因代码泄露引发密钥泄露。

应依据商业银行应用程序接口等级设置不同的密钥有效期，并对密钥进行定期更新。

6 安全部署

与应用方应遵循商业银行应用程序接口网络部署逻辑结构示意图，进行应用程序接口的安全部署。商业银行及应用方都应在互联网边界部署如防火墙、1DS/IPS、DoS防护等具备访问控制、入侵防范相关安全防护能力的网络安全防护措施应用程序接口系统满足7*24小时不间断运行。

7 实施保障

7.1 组织保障

本行应用程序接口业务由财务会计部、风险合规部、营业室及各支行共同负责管理。

7.1.1 财务会计部职责

——负责组织制定应用程序接口业务的各项规章制度。

——负责制定应用程序接口发展规划、开展业务分析、统计、组织产品宣传和推广。

——负责应用程序接口业务开办机构的资格审查。

——负责应用程序接口内管系统参数配置、机构及柜员维护、角色设定及分配、银行公告发布等管理工作。

——负责组织系统内应用程序接口业务培训。

——负责组织应用程序接口业务需求提出、立项及产品研发。

——负责应用程序接口业务系统升级改造测试工作。

——负责应用程序接口网络维护工作的管理，确保网络畅通。

——负责向监管部门报送应用程序接口相关业务报表等材料。

7.1.2 风险合规部职责

——负责应用程序接口业务风险管控工作。
——负责向监管部门报送应用程序接口相关业务报表等材料。
——负责对应用程序接口业务需求进行论证，并提供科技支撑和服务。
——负责应用程序接口应用软件项目、基础设施项目建设。
——负责协助金电公司托管中心保障应用程序接口系统安全稳定运行。
——负责应用程序接口系统安全管理工作。
——负责应用程序接口安全技术方面培训。

7.2 岗位分工

7.2.1 应用程序接口部岗位设置

——业务管理岗：设置专职岗位，负责组织制定应用程序接口业务的各项规章制度；负责应用程序接口业务开办机构的资格审查；负责应用程序接口内管系统管理录入工作；负责组织系统内应用程序接口业务培训；负责组织应用程序接口业务需求提出、立项及产品研发；负责与农信银沟通协调工作；负责应用程序接口业务指标制定、落实和考核。
——风险管理监控岗：设置专职岗位，负责应用程序接口业务风险管控工作；负责监督检查应用程序接口的运行和安全情况；负责对可疑交易、虚假交易的监控；定期组织安全评估，对应用程序接口业务运营中出现的安全隐患及时提出控制措施；负责应用程序接口内管系统管理授权工作；负责组织系统内应用程序接口业务培训；负责参与应用程序接口业务需求提出、立项及产品研发。
——业务测试岗：设置专职岗位，负责应用程序接口日常业务及系统升级改造测试工作；负责参与应用程序接口业务需求提出、立项及产品研发；负责拟定业务测试计划，按业务需求内容进行业务测试、联调测试。
——业务推广岗：负责制定应用程序接口发展规划、开展业务分析、统计、组织产品宣传和推广。负责督导全省应用程序接口业务宣传、营销、新业务推广等工作。
——综合岗：负责应用程序接口业务数据的收集、统计、汇总、分析工作；负责向监管部门报送应用程序接口相关业务报表等材料；负责业务指标完成情况监测、考核；负责对应用程序接口各项故障业务及可疑交易的通报工作；负责应用程序接口综合管理工作。

7.2.2 信息科技部岗位设置

——业务开发岗：负责对应用程序接口业务需求进行论证，提供科技支撑和服务；负责应用程序接口应用软件项目建设。
——业务运维岗：负责应用程序接口系统安全管理工作；负责应用程序接口基础设施项目建设；负责应用程序接口安全技术方面的培训。

7.3 管理制度

为确保本行应用程序接口业务正常开展，规范和完善应用程序接口业务管理，维护本行和客户的合法权益，本行先后制定了《广阳舜丰村镇银行应用程序接口业务发展规划》、《广阳舜丰村镇银行应用程序接口业务管理办法》、《广阳舜丰村镇银行应用程序接口服务章程》、《广阳舜丰村镇银行应用程序接口风险管理技术措施》、《广阳舜丰村镇银行应用程序接口业务风险管理体系及规章制度》、《广阳舜丰村镇银行应用程序接口业务风险管理办法及策略》、《广阳舜丰村镇银行应用程序接口业务运行应急计划和业务连续性计划》等。

7.4 企业标准宣传及实施机制

企业标准宣传:应建立企业标准宣传机制，借助自有和外部的宣传渠道，如官方网站、微信公众号、相关营销媒体及网点厅堂等，对企业标准进行宣传；

企业标准培训:应建立企业标准学习、培训机制，开发相应培训课程，全行进行学习；

企业标准实施监督机制:针对企业标准实施情况，应建立相应的监督机制，并定期组织检查定期公布检查结果，发现问题及时整改。