芷江农村商业银行股份有限公司企业标准

Q/ZJRCB 0002—2021

应用程序接口服务规范

Application Program Interface Service

企业标准信息公共服务平台
公开 2021年07月14日 09点39分

2021-07-14 发布　　2021-07-15 实施

芷江农村商业银行股份有限公司　发布

目　次

企业标准信息公共服务平台
公开　2021年07月14日 09点39分

前　言

本标准按照 GB/T 1.1-2020 给出的规则起草。

为切实提高芷江农村商业银行标准水平，增加对外标准供给，构建金融标准体系，提升芷江农村商业银行金融服务风险防控能力，提升安全标准级别，全应用程序接口的类型与安全级别、安全设计、安全部署、安全集成、安全运维、服务终止与系统下线、安全管理等安全技术与安全保障等制定全方位安全体系，特制定本接口服务规范。

企业标准信息公共服务平台
公开 2021年07月14日 09点39分

应用程序接口服务规范

1 范围

本规范规定了芷江农商银行提供开放应用程序接口时，在接口类型、安全级别、安全设计、安全部署、安全集成、安全运维、服务终止与系统下线、安全管理等方面的规范要求，接口符合JR/T0185-2020、JR/T0092-2019、JR/T0149-2016、JR/T0171-2019、GB/T35273-2017、GB/T22239-2019、GB/T28448-2019等标准和规范的基本要求。

本规范适用于所有应用程序的接口标准。

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。

JR/T 0185-2020 商业银行应用程序接口安全管理规范

JR/T 0092-2019 移动金融客户端应用软件安全管理规范

JR/T 0149-2016 中国金融移动支付支付标记化技术规范

JR/T 0171-2019 个人金融信息保护技术规范

GB/T 35273-2017 信息安全技术个人信息安全规范

GB/T 22239-2019 信息安全技术网络安全等级保护测评要求

GB/T 28448-2019 信息安全技术网络安全等级保护测评要求、金融科技(FinTech)发展规划(2019-2021 年)

3 术语与定义

下列术语和定义适用于Q/CRCB 0002-2020的本服务参照规范。

3.1 应用程序 application program

应用程序，指为完成某项或多项特定工作的计算机程序，它运行在用户模式，可以和用户进行交互，具有可视的用户界面。

3.2 API

API（Application Programming Interface，应用程序接口）是一些预先定义的函数，或指软件系统不同组成部分衔接的约定。[1] 用来提供应用程序与开发人员基于某软件或硬件得以访问的一组例程，而又无需访问源码，或理解内部工作机制的细节。

3.3 报文 message

报文是网络中交换与传输的数据单元，即站点一次性要发送的数据块。报文包含了将要发送的完整的数据信息，其长短很不一致，长度不限且可变。

3.4 敏感数据 sensitive data

敏感数据是指泄漏后可能会给社会或个人带来严重危害的数据。包括个人隐私数据，如姓名、身份证号码、住址、电话、银行账号、邮箱、密码、医疗信息、教育背景等；也包括企业或社会机构不适合公布的数据，如企业的经营情况，企业的网络结构、IP 地址列表等。

3.5 HTTPS

HTTP 是以安全为目标的 HTTP 通道，在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性。

3.6 会话保持 conversation persistence

是指在负载均衡器上的一种机制，可以识别客户端与服务器之间交互过程的关连性，在作负载均衡的同时还保证一系列相关连的访问请求都会分配到一台机器上。用人话来表述就是：在一次会话过程中发起的多个请求都会落到同一台机器上。

3.7 分布式服务 distributed services

分布式资源共享服务器就是指数据和程序可以不位于一个服务器上，而是分散到多个服务器，以网络上分散分布的地理信息数据及受其影响的数据库操作为研究对象的一种理论计算模型服务器形式

3.8 负载均衡 enterprise internet banking

指建立在现有网络结构之上，它提供了一种廉价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

3.9 数据灾备 data backup

全称为数据灾难备份，是指为防止出现操作失误或系统故障导致数据丢失，而将全系统或部分数据集合，从应用主机的硬盘或阵列复制到其他存储介质的过程。亚洲最大灾备数据中心万国数据成都数据中心在 2010 年 12 月初将正式竣工并投入运营。

4 接口安全设计规范

4.1 设计基本要求

我行开放平台的所有加密算法应采用国密算法，包括：非对称加密算法 SM2、对称加密算法 SM4 等。

所有第三方开发人员在进行接口开发前均需要通过我行组织的安全编码培训，并严格依照我行指定的安全编码规范进行开发。

开发中如需使用第三方应用组件，则应使用通过芷江农商银行开发平台安全性验证的第三方组件，并注意组件的版本号要求。请持续关注相关平台的信息披露和更新情况，适时更新相关组件。

芷江农商银行开放平台所有产品接口的源代码均需要经过专业的安全专项审计，需聘请第三方安全公司进行安全渗透测试，并通过自动化工具进行定期的审计工作。

芷江农商银行开放平台制定了严格的接口版本管理与控制规程，并通过开放平台、消息通知等方式，就接口废止、变更等情况与应用方及时保持信息同步。

我行在向应用方提供接口服务的异常与调试信息时，不会泄漏任何服务器、中间件、数据库等软硬件信息或内部网络信息。

4.2 接口安全设计

应用方在芷江农商银行开放平台注册之后，平台会自动为应用方生成 AppId（创建成功之后无法修改）和 AppSecret，AppSecret 需要开发者点击“生成”按钮进行生成和保存，平台不保存该明文密钥，如需后续查看，只能重新生成。

产品 token 是芷江农商银行开放平台每个产品的全局唯一接口调用凭据，是产品接口身份认证要求的重要因子。应用方通过在开放平台注册时获取的 AppId 和 AppSecret，使用 SDK 或者调用对应产品 API 的 token 接口来获取产品 token。产品 token 的存储至少要保留 512 个字符空间。产品 token 的有效期目前为 2 个小时，需定时刷新，重复获取将导致上次获取的产品 token 失效。

应用方在发起接口调用时，必须对请求报文进行签名计算。芷江农商银行开放平台采用国密 SM2 算法生成公私钥对，加密强度 256 位，SM2 公钥 64 字节，私钥 32 字节。开发者生成的应用私钥须自己妥善保存，应用公钥须上传至我行开放平台。再使用请求报文 body、签名密钥 signature、时间戳 ts，计算得出签名信息 sign。请求报文签名的具体规则如下：

报文前拼接签名密钥，后面拼接时间戳（毫秒）字符串：signature（签名密钥）+body（请求 JSON 报文）+ts（时间戳，毫秒）

使用上传至开放平台的 SM2 公钥，以 ECC 算法针对上述生成的字符串签名，得到的结果（Base64 编码的）即为签名值

芷江农商银行开放平台采用国家标准的对称密钥算法 SM4 对接口的业务字段进行加解密，该算法密钥分组长度 128 位，密钥长度 128 位。密钥可以开发者自己生成或由平台生成，密钥须上传至我行开放平台。

4.2.1 身份认证安全设计

根据产品的安全等级，对身份认证的安全要求会有所区别。针对 A1 级的接口认证，需做到:

校验产品 token 是否有效

校验产品 token 是否与应用方的 AppId 保持一致

校验调用方的源 IP 地址是否在应用方的 IP 白名单中

针对安全防护等级较高的 A2 级别的产品接口，需要在满足 A1 级接口身份认证要求的基础上，还需做到：

使用应用方 AppId 关联的 SM2 公钥，以 SM2 国密算法对请求报文数据进行验签操作，对 AppId 和 SM2 公钥进行双向认证。

使用应用方 Appid 关联的 SM4 密钥，对请求报文中的业务字段进行解密，并对 AppId 和 SM4 密钥进行双向认证。

而在进行用户身份认证时，则至少使用双因子认证的方式来进行身份校验：校验用户输入的交易密码及短信验证是否正确，二者是否关联一致。

在针对 A2 级别的产品用户认证则需要使用三因子的身份认证：校验用户输入的交易密码、短信验证码和 Ukey 的临时密码是否正确，三者是否关联一致。

4.2.2 接口交互安全设计

芷江农商银行开放平台会严格校验接口报文的版本号及参数格式要求，使用 SM2 算法签名验签来保证数据的完整性和不可抵赖性，使用 SM4 针对业务字段来进行对称加密以保证敏感数据不被泄露。

对于支付敏感信息等个人金融信息，同时采取了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，会使用例如输入框原文校验及清理、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会使用集成在 SDK 中的加密组件进行分别加密，并对相关报文进行整体加密处理。若确需使用开放平台的产品接口提供的账号、卡号、姓名等，平台会自动脱敏或去标识化处理。如因清分与清算、差错对账等需求，确需将卡号等支付账号传输至应用方时，则需申请专线连接，并采取非对称+对称算法来保证信息的完整性和安全性。

对于金融产品持有份额、用户积分等接口安全等级为 A2 类的只读信息查询，仍使用 SM2 非对称加密算法来保证查询信息的完整性与保密性，且查询结果不得在应用方本地保存。应用方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。

4.3 服务安全设计

4.3.1 授权管理

芷江农商银行开放平台的产品接口采用最小授权原则，默认新的应用方无任何产品接口权限，需在开放平台管理端申请相应的产品授权，并经后台审核通过后方可发起调用。当服务需求变更时，需要开放平台管理端重新提交授权申请。

4.3.2 攻击防护

芷江农商银行开放平台服务安全设计具备了以下攻击防护能力：

API 和 SDK 应对常见的网络攻击具有安全防护能力，如防止 DDOS 攻击、跨域访问等。

移动终端应用 SDK 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 SDK 具备动态调试防护能力，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第改文件、动态修改内存代码等方式控制程序行为的能力。

4.3.3 安全监控

芷江农商银行开放平台会对应用方的接口使用情况进行监控，完整记录接口访问日志。日志最长保留 1 年时间，且满足以下要求：

日志中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，应用方接口日志中会以部分屏蔽的方式记录支付账号（或其等效信息），除此之外应用方接口日志中不会对的个人金融信息进行记录。

4.3.4 密钥管理

密钥管理安全要求如下：

加密使用的 SM4 算法的密钥和签名使用 SM2 算法的私钥相互分离，且不能相同。

不应以编码的方式将私钥明文（或密文）编写在我行应用程序相关代码中，Ap Secret 或私钥不应存储于我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。—应依据我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。

5 接口安全集成规范

5.1 应用方核准

5.1.1 应用方准入

芷江农商银行开放平台会所有对申请接入产品接口的应用方进行准入审核，如从服务客群、服务场景、市场份额、运营能力、风控能力等方面对意向应用方进行考察。我行会全面审慎地考察、评估应用方的技术能力和管理水平，将用户信息保护能力作为重要评价指标，必要时应对应用方的安全保护能力进行技术评估，评估的范围包括但不限于应用方信息安全建设水平等内容。

同时，我行针对合作业务场景、接口应用范围与交易量预期、应用程序接口集成模式、不可访问未授权的信息、用户信息安全保障责任、交易安全保障责任等条款制定了一系列的应用程序接口合作协议。注意，我行不会以任何开放应用程序接口的形式变相开展跨机构清算业务。

应用方在正式接入我行产品接口服务应前，应在我行开放平台的联调环境开展全流程联调性能测试，且各项测试指标满足我行相关要求后方可接入。

5.1.2 应用方身份核验

芷江农商银行开放平台在对应用方接入注册与审批阶段，会通过以下手段对应用方身份进行核验和管理：

应用方应按照我行要求，提交必要的身份核验资料，包括运营资质、法人信息材料、主要应用开发人员的个人信息身份材料等。

我行对应用方提交资料的有效性、完整性、真实性进行审核，对应用方身份进行合规性核验。

5.2 接入安全控制

5.2.1 身份认证

芷江农商银行开放平台在对应用方的身份认证要求如下：

应用方身份声明：

应用方准入审核通过后，我行会给应用方配置唯一标识 AppId 及与之相匹配的应用鉴别密文 App Secret、用于关于业务字段加密的 SM4 密钥（也可以由应用方自己生成后上传至开放平台）。应用方还应自己生成 SM2 公私钥对用于报文签名验签，然后上传公钥至我行开放平台。注意，SM2 的私钥不应与 SM4 的密钥相同。

我行会严格对应用唯一标识 AppId 进行存储与统一管理，并根据应用唯一标识 AppId 进行应用身份认证、状态校验和权限控制等。

应用方身份认证：

应用方在调用我行开放平台的产品接口时，身份认证方式请见 2.2.1。我行在发现具备恶意的连接时，会对应用方的应用程序接口主动断开连接，并将产品 token 置为失效。

5.2.2 身份认证

我行在与应用方之间使用互联网方式进行数据传输时，强制使用HTTPS网络协议，且TLS版本>=1.2。会有SM2的公钥进行报文签名，并对关键业务字段进行SM4对称加密。

5.3 运行安全

5.3.1 用户身份认证

我行对用户身份的认证要求如下：

用户身份认证应在我行后台应用程序完成，若用户个人金融信息或支付敏感信息确需在应用方输入，应用方不应以任何方式在本地留存相关信息。

我行会对应用方上送的用户相关信息进行核验。

我行会结合具体场景，依据业务必须的最小时间设计用户会话有效期。若用户长期处于无业务操作时，则会主动结束会话。

5.3.2 权限控制

芷江农商银行开放平台依据最小授权的原则，对所有产品接口权限进行有效控制，对于未授权的资源禁止访问。我行会对 API 的调用有效期进行严格控制，如单次有效、阶段性有效、协议期限内有效等。

应用方调用接口时，对于获取、使用、变更用户信息、账户、资金等接口，应首先取得用户明示同意，其内容应包含授权有效期。

5.3.3 数据安全

应用方在数据安全保护方面，应保护数据的完整性，应对数据完整性进行校验，并在检测到完整性错误时采取必要的恢复措施（或停止执行请求）。同时在数据机密性方面，不应采集、存储用户个人金融信息或支付敏感信息。

对于需要用户输入支付敏感信息或身份鉴别信息的场景，应用方仅可作为信息的采集与传输通道，应使用我行的 SDK 发起接口调用，并采取报文加密等措施，保证采集与传输信息的机密性与完整性。

支付敏感信息与身份鉴别信息在应用方不得留存，应使用 SM2 公钥进行数字签名来确保 A2 类数据的不可抵赖性。

应用方在与我行终止业务合作后，应依据我行明确规定的方式删除（或销毁）通过我行产品接口获取的与我行或者用户相关的任何数据。

应用方应针对接口处理的数据，建立数据备份管理机制和应急灾备机制，并纳入机构灾备体系。在合作终止后，应依据行业主管部门有关要求，履行反洗钱、反欺诈等义务。

5.3.4 应用方安全能力

应用方在安全能力方面，应符合国家网络安全等级保护相应要求，进行安全设计、安全建设、安全保护。同时还应遵我行的安全设计要求，使用我行提供的安全接口，并依据用户手册和安全规范进行集成。还应通过技术手段与管理措施等，防止接口滥用。

应用方应留存与我行应用程序接口集成相关的应用系统、网络设备、主机设备、安全产品日志，日志留存应不少于 12 个月。

5.3.5 应用方接口集成

应用方在接口集成方面的须满足如下要求：

应用方应根据我行提供的用户手册以及我行授权其使用的服务类型，正确合理使用API.

应用方密钥存储应采取加密等方式进行安全防护，防范密钥丢失或泄露，应用方应按照我行提供的用户手册，妥善使用和保管相关 SM2 公私钥对和 SM4 密钥。

针对 A2 类级别的接口，应用方需使用我行提供的 SDK 进行 API 调用，应用方不得对我行提供的 SDK 进行反编译、篡改或二次封装。

若应用方发现我行应用程序接口存在安全缺陷，应采取补救措施并及时通知我行，应用方未经我行许可，不得将缺陷细节透露给任何其他第三方。

禁止应用方利用我行应用程序接口漏洞，进行网络攻击、信息窃取或交易欺诈等非法操作。

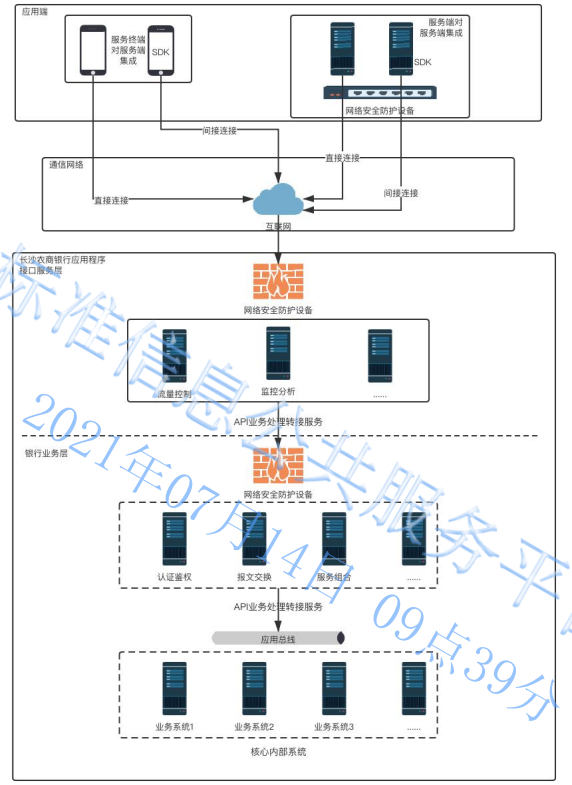
5.3.6 应用方退出

我行制定了有序、可行的应用方退出机制，会严格保障账户、资金、信息安全，充分履行用户告知义务。在应用方退出后，我行会对认证信息（如App Sccret、公私钥对等）进行作废处理，归档并保存待查。

应用方应按照我行的要求，妥善处理其通过我行应用程序接口获取的用户信息与我行业务有关资料，并在双方协定的期限内承担后续的保密责任。

6 接口安全部署规范

我行与应用方的应用程序接口网络部署逻辑结构示意图如下：



我行会在互联网边界部署如防火墙、IS/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。应用方也应具备同等的网络安全防护措施。

我行应用程序接口服务层部署了流量控制、监控分析、认证鉴权、报文交换、服务组合等服务，业务层部署了认证鉴权、报文交换、服务组合等服务。我行应用程序接口服务层与银行业务层之间都部署了如防火墙等具备相关访问控制、入侵防范安全防护能力的网络安全防护措施。应用方服务器应部署在应用方互联网接入安全防护设备之后的逻辑隔离区域，通过互联网、移动互联网网络访问我行应用程序接口相关应用服务。

我行的安全控制严格依据 JR/T0071 部署相应级别的安全控制措施，而应用方部署的接口应用程序有关安全控制措施，应符合国家网络安全等级保护有关标准二级及以上安全要求。

7　接口安全运维规范

7.1 安全监测

7.1.1 运维监测

我行建立了开放平台产品接口运维监测平台，能够监控产品接口相关服务器运行状态，如：CPU、内存、网络等；同时也能监控产品接口应用服务的运行状态，如耗时、交易量、成功率等。如有任何异常将及时告警，会通过短信、邮件、声音等形式向运维人员、相关负责人发送告警提示。

我行开发品台的产品接口的 RPO/RTO 时间为 30 分钟，满足了 7×24 小时不间断运行的要求，且服务可用率为 99.99%。

我行开放平台已经做到接口响应时间平均 100ms 以内，TPS 达到 5000/s,资源使用情况均低于服务器阈值的 80%，且交易成功率能够达到 95%。

我行所有的交易日志按照国家会计准则要求予以保存，系统日志保存期限不少于 1 年。

应用方也应对其集成了我行产品接口的运行状态进行监测，发现异常后及时处置。

7.1.2 异常监测

芷江农商银行开放平台具有流量监控、故障隔离、黑名单控制等接口调用控制能力。在流量控制方面能灵活设置控制规则，包括：最大允许调用并发数、单位时间最大交易谓用量等，流量控制措施则包括了：告警、暂停、拒绝等。

同时我行建立了未授权和冒用我行产品接口的监测机制，发现问题能够及时处置。具备故障监测和恢复能力、具备应用方黑名单管理能力。

而应用方则应具备故障识别与隔离能力，在调用我行产品接口时应设计熔断机制，熔断规则包括：设置失败笔数阀值、接口调用失败阈值等，熔断措施包括：拒绝交易、暂停服务调用等，同时应该建立完善的异常告警处理机制。

7.2 风险控制

7.2.1 服务风险控制

芷江农商银行开放平台建立了应用方信息（如运营能力、风控能力等）更新和复审机制，能够根据应用方调用我行产品接口的业务日志等信息，定期评估其金融交易业务的运营情况，并在协议框架内对异常的业务调用进行监控，必要时进行业务限流，并及时通知应用方进行事件调查。同时也会定期评估应用方的风险承受能力，确保用户与应用方相关的账户关联、服务类型、交易额度等与其风险承受能力相匹配。

7.2.2 交易流程控制

芷江农商银行开放平台要求交易流程控制的必须满足以下条件：

身份认证服务等授权类服务应充分识别是否经过用户本人授权。

账户查询、资金交易、金融产品及服务中请类交易，应充分识别交易是否由用户本人发起（或本人授权发起），核实用户本人意愿。

资金类等高风险金融服务，应提示用户相关的安全风险，充分履行用户告知义务。

7.2.3 交易风险监控

芷江农商银行开放平台将产品接口纳入了我行风险监控范围，对应用方和用户账户资金活动情况进行实时监控。所有资金交易均满足行业监管部门对反洗钱、反欺诈方面的相关要求。对大额、异常的资金收付应逐笔监测与核查，及时预警、及时控制。对监控到的风险交易应进行及时分析与处置。

7.3 变更控制

当我行开发平台的产品接口发生变更时，会及时评估影响并告知应用方，制定详细变更方案和应急预案，按需进行接口变更发布，并充分履行用户告知义务。

应用方对我行产品接口的使用发生重大变更时，如其交易量预期发生变化、对我行产品接口集成方案进行修改等，可能对我行系统安全性、业务连续性等造成重大影响的有关事项，应制定详细的变更方案和应急预案，评估变更带来的风险，并及时告知我行，同时充分履行用户告知义务。当应用方使用我行产品接口发生重大变更时，我行会对其变更进行风险和影响评估，并采取相应的处置措施。

7.4 运维巡检

我行会定期对我行产品接口进行安全巡检，对我行产品接口进行源代码安全审计、渗透测试等技术检查，及时处理安全漏洞，有效控制安全风险。同时也会定期对应用方的我行产品接口安全集成情况进行检查。

应用方则应定期对我行产品接口进行安全巡检，包括：应定期对其调用我行产品接口的应用系统进行安全评估，及时处理安全漏洞，确保调用的真实有效。

7.5 事件处理

我行制定了详细的应急处理方案，对运维过程中监测到的异常情况及时告警和处置，及时处理生产事件，并协调应用方配合事件调查。

8 服务终止与系统下线规范

我行制定了完善的服务终止和系统（接口）下线的相关制度和步骤，以便各参与方有序处理相关服务。在服务终止前，我行会将服务终止有关事项提前告知相关方，并向相关平台提交有关接口的统一识别码注销申请。

同时，我行会与应用方就服务终止后相关数据归档、数据删除（或销毁）、个人金融信息保护、用户资金和账户安全、消费者权益保护等问题充分达成一致，明确相关责任，并充分履行用户告知义务。所有系统（接口）下线会在相关服务确认终止之后执行，在下线之前会设置相应的挡板（如服务终止提示信息），明示应用方服务已终止。在系统（接口）下线之后应将有关数据进行归档处理，数据保留期限则按照国家与行业主管部门、商业银行相关规定与规则执行。

9 接口安全管理

9.1 管理制度

我行将开放平台的产品接口管理纳入了我行现行的管理体系中，对产品接口进行全生命周期的安全管理。所有应用程序接口采用统一格式的识别码，并在相关平台进行注册和登记。同时通过开放平台发布了所有产品接口的内容，并随时保持更新。

芷江农商银行开放平台建立了覆盖产品接口全生命周期的应用安全管理制度与控制措施，并对管理制度与控制措施的有效性进行验证，确保了产品接口的一致性和连贯性，保障产品接口效率及安全性。同时，在我行开放平台上提供了详细的开发手册，以指导应用方安全集成产品接口，其中开发手册包括：安全集成要求、集成示例，以及测试环境的使用等。

9.2 应用安全责任

在应用方注册我行开放平时是，会用户的协议明确规定产品接口的信息安全与金融消费者数据保护等方面的安全责任，包括：

应用方若出于自身服务需求收集金融消费者个人金融信息，应直接获得金融消费者的明示同意，并依据最少够用原则进行信息收集，不应以使用商业银行应用程序接口为理由不履行明示同意等个人金融信息保护义务;

向金融消费者说明个人信息收集方并非商业银行，也与商业银行服务无关。

应用方不应将通过产品接口获得的金融服务能力与数据以任何方式转移、共享或分包给其他第三方。无论合作关系是否续存，应用方都应依据与我行的协议约定，履行用户信息保密责任。

9.3 安全审计

芷江农商银行开放平台具备以下安全审计能力：

（1）完整记录产品接口访问日志，日志记录包括了 2.3.3 所述日志内容。

（2）依据商业服务需求和风险控制要求，遵循最少够用原则适当保留应用方上送报文（全部或部分信息）。

（3）对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖

而应用方则应具备以下安全审计能力：

（1）完整记录产品接口访问日志，日志记录应符合 2.3.3 所述日志要求。

（2）对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。

（3）提供查询应用方用户产品接口相关登录、授权、交易等历史操作日志功能。

10 实施保障

10.1 组织保障

省联社负责统一全省应用程序接口规范制定，本行基于省联社接口标准制定相关规范。

信息技术部负责统一全行应用程序接口标准制定、全行应用程序编写规范、统一安全规范、统一渗透测试验证规范、统一应用程序版本管理规范、统一应用程序接口版本发布与部署规范等。

法律合规部负责指导在标准和制度制定过程中的法律风险把控。

10.2 管理制度

应用程序服务接口必须严格按照管理制度执行，包括但不限于应用程序接口服务研发、接口测试、投产部署、生产运营、应急响应等。

1、服务研发：必须遵守统一的接口规范、安全规范；

2、接口测试：必须对每一个接口进行全面的单元测试、UAT 验证测试；

3、投产部署：投产部署发布前，对于面向互联网提供的应用程序接口，必须要经过安全渗透测试；

4、生产运营：通过监控软件每日巡检接口状态，遇到异常情况，及时反馈处理；

5、应急响应：建立应急响应机制，应急小组负责所有接口服务的应急处理工作，决定接口服务应处理的的重大工作事项，组织实施、业务协调和发布信息系统应急指令，发布接口服务故障级别，决策处理方案，加强日常巡检工作。

10.3 宣传实施

本行应当将 《芷江农村商业银行股份有限公司应用程序接口服务规范》在企业标准信息公众服务平台进行注册发布，对外进行应用程序接口服务规范公示。

10.4 安全保障

本行在应用程序接口服务正式投产前，必须进行安全渗透测试以及等保测评，确保检测出漏洞和安全风险完全修复。

参考文献

[1]JR/T 0185-2020 商业银行应用程序接口安全管理规范
[2]JR/T 0092-2019 移动金融客户端应用软件安全管理规范
[3]JR/T 0149-2016 中国金融移动支付支付标记化技术规范
[4]JR/T 0171-2019 个人金融信息保护技术规范
[5]GB/T 35273-2017 信息安全技术个人信息安全规范
[6]GB/T 22239-2019 信息安全技术网络安全等级保护测评要求
[7]GB/T 28448-2019 信息安全技术网络安全等级保护测评要求、金融科技(FinTech)发展规划(2019-2021 年)

企业标准信息公共服务平台
公开 2021年07月14日 09点39分