Q/GZYH

赣州银行股份有限公司企业标准

Q/GZYH 008-2022

赣州银行开放平台服务规范

2022-8-31 发布　　2022-9-1实施

赣州银行股份有限公司　　发 布

目　　次

前　言

为切实提高赣州银行开放平台标准水平，提升开放平台程序接口类型与安全级别、安全涉及、安全部署、安全运维等安全技术与安全保障，特制订本服务规范设计说明书。

开放平台服务规范

1 通讯规范

外部渠道使用国密对报文加密加签后,并且将密文使用HTTPS通讯协议POST形式发送到开放平台,开放平台加处理后的结果报文进行加密加签后同步返回给外部渠道。相关通讯方式、加密方式以及接口交互安全通讯规范如下:

1.1 通讯方式

调用方式	HTTPS
请求方式	POST
字符集	UTF-8
数据格式	JSON

1.2 加密方式

加密算法	国密
加签算法	国密

1.3 接口交互安全

网络层	防火墙表名单控制，保证接口交互权限唯一可靠
数据层	HTTPS通讯，数据加密/验签，且数据不可篡改

2 接入模式

2.1 标准接入模式

在标准接入模式下,服务请求方系统组织交易请求报文,通过HTTP通讯协议将交易请求报文发送到标准接入层,等待处理完毕之后,再从标准接入层获取交易响应报文;若交易过程中出现异常,一方面组织交易报文返回至服务消费方,另外一方面则组织异常监控报文,将异常报文发送到监控服务中(此路径为可选)。

在标准接入模式下,服务提供方系统开启监听程序,标准接出层使用HTTP通讯协议发送交易请求信息至服务提供方,服务提供方接收报文,进行解析并处理完毕之后,组织交易响应报文,使用HTTP通讯协议将交易响应报文发送到标准接出层;若交易过程中出现异常,一方面组织异常响应报文返回至消费方,另外一方面将异常报文发送到监控服务中(此路径为可选)。

2.2 适配器接入模式

为了尽量减少某些存量系统的改造，可以采用适配器接入模式。

在适配器模式下，服务请求方系统不需改变原有交易请求报文和通讯协议，直接将交易请求发送至接入适配器，接入适配器接收到交易请求后，进行协议转换，并将报文转换成符合标准的XML报文，然后将报文发送至标准接入层，等待处理完毕之后，适配器从标准接入层获取交易响应报文，然后返回到服务消费方；若交易过程中出现异常，通过适配器将异常报文，返回给消费方，另外可以组织监控报文将异常信息发送至监控服务（此路径为可选）。

在适配器模式下，服务提供方系统开启监听接口，接出适配器使用socket发送交易请求报文至服务提供方，服务提供方处理完毕后，使用socket将交易响应报文发送到接出适配器；若交易过程中出现异常，接出适配器将异常报文返回，将异常报文发送至监控服务（此路径为可选）。

在适配器模式下，服务提供方系统开启监听接口，接出适配器使用socket发送交易请求报文至服务提供方，服务提供方处理完毕后，使用socket将交易响应报文发送到接出适配器；若交易过程中出现异常，接出适配器将异常报文返回，将异常报文发送至监控服务（此路径为可选）。

3 请求报文头

报文头原则：最小结构，同一类业务不从多个角度重复定义，适应全业务。

一般来讲，报文头需要回答下面 6 个问题：

What：交易是什么？最好一个交易码说明一切。

Which：这个交易是哪笔？需要用全局操作流水号唯一指定一笔交易。

Who：是谁提交的？谁操作就填上谁的 ID，包括客户 ID 和柜员 ID。

Where：从哪里发起，可以包括渠道、服务器 ID、终端号等，采用全行统一的编码规则和业务规则。

When：什么时候发生的？应采用统一的自然日期。

How：必要的报文控制信息，包括安全、交易模式、特殊交易的处理标示。

4 接口安全设计规范

渠道应用方在完成sit、uat环境测试后由行方发布相应的渠道应用ID（APPID），并且与渠道应用方互相交换国密公钥。

APPID作为渠道应用在开放平台中的唯一身份标示，使用自身的私钥以及对方公钥按照接口加密解密规范对报文进行加密加签操作。

应用方准入审核通过后，我行会给应用方配置唯一的标识APPID及与之相互匹配用于关于业务方字段加密的SM2密钥。应用方还应自己生成SM2公私钥对用于报文签名验签，然后将公钥发至我行科技人员。在正常的接口中SM4的秘钥因在每次报文中重新定义，并且使用SM2进行加密。注意，SM2的私钥不应与SM4的密钥相同。

我行再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，并对业务方字段进行SM4对称加密。

5 接口安全部署规范

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。

6 接口安全运维规范

6.1 运维检测

针对开放平台建立相应的监控管理平台，针对服务接口进行平均相应时间、最大响应时间、最小相应时间进行监测。API网关为集群部署，针对不同的网关进行交易量以及响应时长监测。

6.2 日常需求新增以及变更规范

日常需求新增以及变更需要做好相应的变更记录，新增的功能需要完成相关的测试流程，变更的功能需做好相应的影响性分析。在上线前完成上线部署手册、上线检查项以及相关的部署文件的准备工作。

7 实施保障规范

7.1 组织保障

科技部负责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、统一应用程序版本发布以及部署规范。

7.2 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：必须遵守统一的服务规范、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。

7.3 安全保障

开放平台在投产之前需经过安全渗透测试等安全检测，并且对检测出的漏洞以及安全风险完全修复，在运行期间也许定期的进行安全检测工作。

8 接口地址规范

开放平台对外服务地址为：{host}/api/services/服务码，其中服务码为对应的接口名称。测试、准生产以及生产的host地址互不相同。各环境的公钥以及appId也互相独立，需要单独申请。

9 管理制度

提供管理制度，对应用程序接口服务研发、测试、投产、生产运营、应急响应等全流程提出建立相关管理制度的要求。

提供应用程序接口项目实施方法论，实施过程中，应按照实施方法论进行实施，并充分发挥工具和技术在项目管理过程中的应用：

1.进度管理和资源管理：在项目执行过程中，跟踪各项目时间表、进展、关键路径和各项项目任务的相关性，管理关键项目人员和物理资源的有效使用。

2.需求管理：工程项目管理在很大程度上依赖对需求的获取、跟踪和变更的管理。

3.变更控制管理:监控工作/项目/变更要求的提出、批准和排序过程。

4.配置管理:确保系统文档、代码的一致性,保证项目重要产出物的安全管理。

5.质量管理:制订质量管理策略和计划,按照规范的流程执行项目,确保项目的交付物和管理过程的质量。

6.问题管理:使用适当的管理工具,记录、排序和跟踪项目问题的情况,并确保所有的问题都得到正确及时的处理。

7.风险管理:在项目开始前和项目执行过程中及时识别和分析风险,采取有效措施,以降低风险对项目目标的影响。

10 实施机制

对应用程序接口企业标准宣传、培训和实施机制提出要求。

业务、技术人员需要参与项目的阶段包括:

1、业务需求分析阶段

2、系统设计阶段

3、编码及单元测试阶段

4、集成测试阶段

5、验收测试阶段

6、系统切换阶段

7、试运行与推广阶段

业务、技术人员需要参与的具体工作包括:

1、功能模块需求分析

2、业务界面设计

3、业务逻辑设计

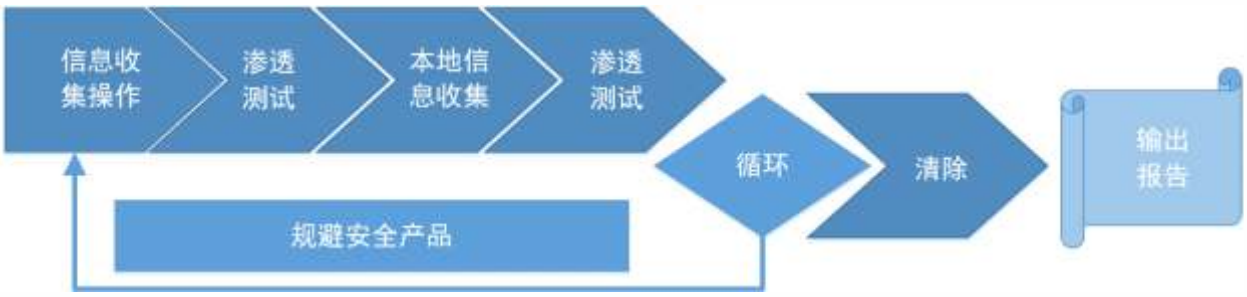
4、测试计划和测试案例设置

5、业务功能测试、集成测试和验收测试

6、技术人员可以参与部分开发工作

7、以及环境管理、质量管理、配置管理、文档编制等各方面的工作。

提供安全检测及安全评估保障,应用程序接口实施中,应满足服务安全检测及安全评估等要求。



每个接口上线前,均进行渗透测试,具体渗透测试流程如图所示,并遵循下述几个原则。

1.标准性原则:测试方案的设计和实施依据行业、国家、国际的相关标准进行;

2.规范性原则:工作过程和所有文档,具有很好的规范性,以便于项目的跟踪和控制;

3.可控性原则:在保证测试质量的前提下,按计划进度执行,保证对测试工作的可控性。安全评估的工具、方法和过程要在双方认可的范围之内合法进行;

4.整体性及有限性原则:测试的内容未经授权不得减小或扩大渗透性测试的范围和对象;

5.最小影响原则:测试工作应避免影响系统和网络的正常运行,不能对正常运行的系统和网络构成破坏和造成停产;