ICS 35.240.40
A 11

Q/GLB

桂林银行股份有限公司企业标准

Q/GLB 04—2024

代替 Q/GLB 04—2020

桂林银行应用程序接口安全管理规范

Application program interface security Management specification of Guilin Bank

2020－11－27 发布　　2020 － 11 － 27 实施

桂林银行股份有限公司　　发 布

目　　次

前　　言 II
1 范围 1
2 规范性引用文件 1
3 术语与定义 1
4 缩略语 2
5 规范概述 2
6 接口类型与安全级别 3
7 安全设计 4
8 安全部署 5
9 安全集成 5
10 安全运维 6
11 服务终止与系统下线 7
12 安全管理 7
13 创新及前瞻性 8
14 实施保障 8

前　言

本标准根据GB/T 1.1-2009给出的规则起草。

本标准代替Q/GLB 04—2020《桂林银行应用程序接口安全管理规范》，与Q/GLB 04—2020相比，除结构调整各编辑性改动外，主要变化如下：

a）平台主管部门与应用程序接口服务相关制度制定职责部门变更（见14.1）；

本标准由桂林银行股份有限公司提出。

本标准由桂林银行股份有限公司信息技术部归口。

本标准起草单位：桂林银行股份有限公司。

本标准主要起草人：刘清萌、李玲华、沈桂斌、邓明志、首清贵。

本标准于2020年首次发布，本次为第一次修订。

桂林银行应用程序接口安全管理规范

1 范围

本标准规定了桂林银行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要求。

本标准适用于桂林银行对外互联应用程序接口的设计和应用，并为第三方安全评估机构安全检查与评估工作提供参考。

2 规范性引用文件

下列文件对于本标准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标准。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 25069 信息安全技术　术语

JR/T 0071.2—2020 金融行业网络安全等级保护实施指引

JR/T 0124-2014 金融机构编码规范

JR/T 0185-2020 商业银行应用程序接口安全管理规范

3 术语与定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

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

应用方 application agency

调用商业银行应用程序接口的机构。

3.3

应用软件开发工具包 software development kit

基于特定软件包、软件框架、硬件平台、操作系统等建立应用程序时所使用的软件开发工具集合。

3.4

应用唯一标识 application unique ID

在应用方身份核验通过后，根据其调用的金融产品与服务类型，由商业银行为其授予的唯一标识。

注：包括服务器端应用标识与移动终端应用软件标识两种。

3.5

应用鉴别密文 application secret

应用合法性鉴别凭证，与应用唯一标识配套使用，以验证通过API方式接入的应用合法性，接入验证通过后，即可完成系统对接，调用应用程序接口或使用程序接口提供的功能和数据。

3.6

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。

注：包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反应特定个人某些情况的信息。

3.7

支付敏感信息 payment sensitive information

支付信息中设计支付主体隐私和身份识别的重要信息。

注：包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

3.8

支付账号 payment account

具有金融交易功能的银行账户、非银行支付机构支付账户的编码及银行卡卡号。

3.9

明示同意 explicit consent

个人金融信息主体通过书面声明或主动做出肯定性动作，对其个人金融信息进行特定处理做出明确授权的行为。

注：肯定性动作包括个人信息主体主动作出声明（电子或纸质形式），主动勾选、主动点击“同意”“注册”“发送”“拨打”等。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口(Application Programming Interface)

App_ID：应用唯一标识(Application unique ID)

App_Secret：应用鉴别密文(Application Secret)

SDK：应用软件开发工具包(Software Development Kit)

SSL：安全套接层协议(Secure Sockets Layer)

TLS：安全传输层协议(Transport Layer Security)

5 规范概述

商业银行应用程序接口服务是一种依托 API 技术实现内部与外部互联的金融服务模式，商业银行通过为合作伙伴提供用以互联网的应用程序接口，输出自身金融服务能力与信息技术能力，为增加金融生态黏性提供有益补充。外部机构能够通过互联网渠道，调用商业银行应用程序接口，获取商业银行提供

的各类服务，其逻辑结构见图 1。

商业银行应用程序接口服务的参与方主要包括用户、应用方以及商业银行，商业银行通过 API 直接连接或 SDK 间接连接方式向应用方和用户提供应用程序接口服务，实现商业银行服务的对外输出。

用户发起商业银行应用程序接口应用请求，并接收由应用方或商业银行返回的处理结果。

应用方负责接收并处理用户请求，通过应用程序接口向商业银行提交相关请求，接收返回结果，依照流程进行服务请求处理或反馈用户。

商业银行构建商业银行应用程序接口、应用程序接口服务层和银行业务系统以提供商业银行应用程序接口服务、商业银行应用程序接口服务层将应用方请求转发至银行业务系统处理，并将处理结果反馈应用方或用户，包含认证鉴权、流量控制、监控分析、报文交换、服务组合等功能，不涉及具体业务逻辑处理，实现对商业银行应用程序接口和应用方的管理。

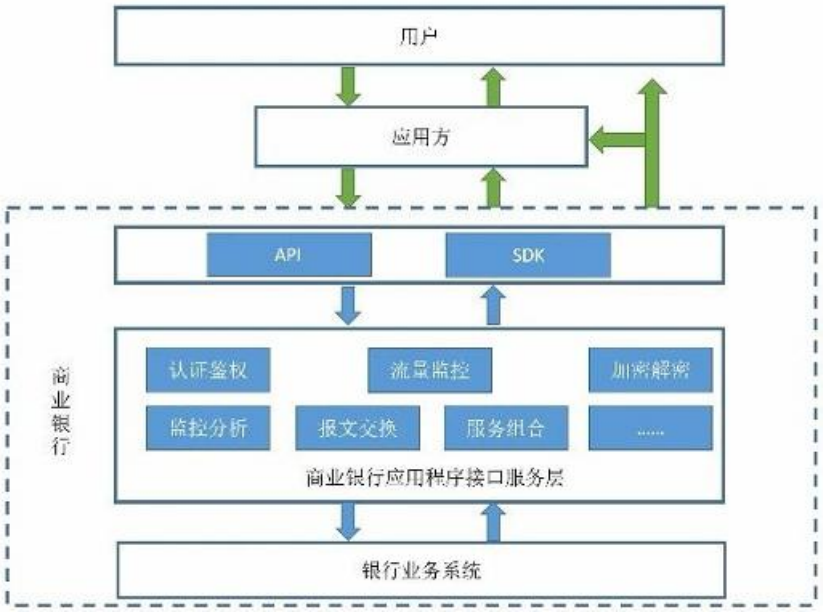

图 1 商业银行应用程序接口逻辑结构图

6 接口类型与安全级别

6.1 接口类型

本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，应用方服务端直接调用本行应用程序接口，或使用本行提供的服务端 SDK，间接访问本行应用程序接口。

对于移动终端对服务端集成方式，应用方移动终端应用软件应使用本行提供的移动终端应用 SDK，间接访问本行应用程序接口。

本行服务端 SDK 主要实现本行通用接入算法的封装，本行移动终端应用 SDK 除封装本行通用接入算法外，还封装了业务逻辑、个人金融信息安全保护等功能。

6.2 安全级别

按照服务类型将本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，实施高等级安全保护强度，此类应用程序接口包括通

过 SDK 提供的资金交易类、用户账户信息查询类等服务。

——A1：金融产品和服务信息查询应用类，实施通用的安全保护强度，此类应用程序接口包括：提供本行金融产品和服务的详细信息的“只读”查询服务等。

7 安全设计

7.1 设计要求

安全设计是提供高服务质量的基础保证,本行应用程序接口安全设计需符合JR/T 0185-2020规定。其中，密码算法支持国家密码管理部门认可的国产密码算法。

7.2 接口安全设计

7.2.1 身份认证安全

本行身份认证安全分为接口身份认证和用户身份认证，其中：

接口身份认证使用的验证要素包括APP_ID与APP_Secret、数字证书、公私钥对三类中的一种或几种组合；

用户身份认证要求：对资金交易类服务，用户登录身份认证至少使用双因子认证的方式。

7.2.2 接口交互安全

本行接口交互安全要求如下：

——必须进行接口联通有效性验证，如接口版本、参数格式等要素。

——必须进行接口交互的数据进行完整性保护，如数字签名技术。

——必须采取措施对支付敏感信息等个人金融信息进行保护，如：

- 登录口令、支付密码等支付敏感信息在数据交互过程中需替换输入框原文，使用本行规定的自定义软键盘、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需对相关报文进行整体加密处理；若确需使用接口将账号、卡号、姓名向应用方进行反馈，应脱敏；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，需使用加密通道进行传输并保证信息的完整性。

——必须在交易结束后及时清除用户支付敏感信息。

7.3 服务安全设计

7.3.1 授权管理

本行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。

7.3.2 攻击防护

本行对外提供服务的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。

7.3.3 安全监控

本行对接口使用情况进行监控，完整记录接口访问日志，日志内容包含交易流水号、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）。

7.3.4 密钥管理

密钥管理安全要求如下：

——加密和签名分配不同的密钥，且相互分离；

——避免私钥硬编码，且不可本地储存；

——设置密钥有效期，定期更新密钥。

8 安全部署

本行应用程序接口的安全部署架构符合JR/T 0185-2020规定，在互联网边界部署如防火墙等具备访问控制、入侵防范相关安全防护能力的网络安全防护措施。安全控制要求至少符合JR/T 0071.2—2020中第二级安全保护能力要求。

本行对接外部服务系统主要包括：开放银行、中间业务平台、企业服务总线等，本行业务系统原则上统一通过对外服务系统提供互联网服务，若因特殊原因必须直接对接互联网，该系统安全能力需达到本规范中的各项要求。

9 安全集成

9.1 应用方准入

应对申请接入本行应用程序接口的应用方进行审核，并制定和签署相关合作协议，在应用方接入注册和审批阶段，通过线上或线下手段，对应用方进行核验和管理。

9.2 接入安全控制

9.2.1 身份认证

本行与应用方之间的身份认证要求如下：

——应用方身份说明：

- 应用方准入审核通过后，本行配置唯一标识 App_ID 及与之相匹配的应用鉴别密文 App_Secret、数字证书（或公私钥对）或应用鉴别密文 App_Secret 与数字证书（或公私钥对）的组合。对于采用公私钥对方式认证的情况，本行对接外部公共平台应对应用方上传的公钥进行登记。
- 本行对应用唯一标识 App_ID 进行存储与统一管理，并根据应用唯一标识 App_ID 进行应用身份认证、状态校验和权限控制等。

——应用方身份验证：

- 应用方在请求本行接口时，本行对应用方身份进行认证，认证方式为 App_ID 与 App_Secret、或数字证书、或公私钥对的组合认证。
- 本行对接口连接时间进行限制，应具备最小有效期限制、具备主动断开功能。

9.2.2 安全传输

本行与应用方之间使用互联网进行传输，应使用SSL/TLS等安全通道进行连接通信，并使用数字签名技术保证数据传输的完整性和不可抵赖性。其中，推荐使用TLS1.2及以上版本。

9.2.3 服务性能

应用方在接入前应在联调环境开展全流程联调性能测试,且各项测试指标满足本行相关要求后方可接入。

9.3 运行安全

9.3.1 用户身份认证

用户身份认证应在本行服务端完成，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。结合具体场景，本行依据业务必须的最小时间设计用户会话有效期，用户长期处于无业务操作时结束回话。

9.3.2 权限控制

本行对接口权限进行有效控制，按应用方、接口等维度，依据最小授权原则进行授权，对于未授权的资源禁止访问。涉及用户敏感信息获取、变更类操作必须取得用户明示同意，同时提供关闭应用程序接口相关服务的申请渠道。

9.3.3 应用方接口集成

本行对应用方在接口集成方面的要求如下：

——应用方应根据本行提供的用户手册以及授权使用的服务类型，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，应用方应按照本行提供的用户手册，妥善使用和保管相关密钥、数字证书。

——如本行提供封装了接口调用的 SDK，则应用方需使用本行提供的 SDK 进行 API 调用，应用方不得对本行提供的 SDK 进行反编译、篡改或二次封装。

——若应用方发现本行接口存在安全缺陷,应采取补救措施并及时通知本行,应用方未经本行许可，不得将缺陷细节透露给任何其它第三方。

——禁止应用方利用本行接口漏洞，进行网络攻击、信息窃取或交易欺诈等非法操作。

——应用方与本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，日志保留期应满足国家与行业主管部门要求，日志留存应不少于 6 个月。

9.4 应用方退出

应用方退出时，本行应用系统应按照退出机制，保障账户、资金、信息安全，充分履行用户告知义务，应用方退出后，对认证信息（App_Secret、公私钥对等）进行作废处理，归档并保存待查。

应用方应按照本行的要求，妥善处理其通过本行接口获取的用户信息与银行业务有关资料，并在双方协定的期限内承担后续的保密责任。

10 安全运维

10.1 安全检测

10.1.1 运维监测

本行建立外部应用程序接口运维监测平台，对接口相关服务器运行状态、接口服务状态（包括耗时、交易量、成功率等参数）等进行检测并建立告警机制。

本行外部应用程序接口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。

10.1.2 异常监测

本行外部应用程序接口具备流量监控、故障隔离、黑名单控制等调用控制能力。

流量控制规则包括最大允许接口调用并发数、单位时间最大交易调用量等，控制措施包括告警、暂停、拒绝。具备故障监测和恢复能力，具备应用方黑名单管理能力。

10.2 风险控制

本行建立服务风险控制、交易流程控制、交易风险控制等控制措施，风险控制指标符合JR/T 0185-2020规定。

10.3 变更控制

本行充分履行用户告知义务,在应用程序接口发生变更时会及时评估影响并通知应用方,制定变更方案和应急预案,按需进行接口变更发布。

10.4 运维巡检

本行定期对外部应用程序接口进行安全巡检，包括源代码安全审计、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，确保应用方在调用时真实有效。

10.5 事件处理

公共平台和外部服务提供系统应制定应急处理方案,对运维过程中检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。

11 服务终止与系统下线

本行外部应用程序接口服务终止前应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。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。

本行系统（接口）下线之后应将有关数据进行归档处理，数据保留期限按照国家与行业主管部门、商业银行相关规定与规则执行。

12 安全管理

12.1 管理制度

本行应用程序接口应符合本行现行安全管理体系。建立信息公告制度，通过官方网站渠道发布外部接口内容，并及时更新，提供开发手册指导应用方安全集成本行外部接口，保障外部接口效率及安全性。

12.2 应用安全责任

本行与应用方以合同方式，明确规定本行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。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时，需获得金融消费者的明示同意，并向金融消费者说明个人信息收集方并非本行，也与本行服务无关。应用方不应将通过本行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。

12.3 安全审计

本行具备以下安全审计能力：

——完整记录外部接口访问日志。

——依据业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。

——对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。

13 创新及前瞻性

13.1 服务创新性

服务创新性应满足以下要求：

——本行依据 API 接口平台化建设规范要求建设开放银行系统，输出自身金融服务能力与信息技术能力，实现资源最大化利用，构建开放、合作、共赢的金融服务生态体系。

——应在符合国家法律、监管规定和本行有关规章制度的前提下依法合规开展，对涉及的风险进行全面客观的分析，并在上线前落实相关风险管控措施和报告程序。同时在上线后加强风险监控，并视情况适时追加风险缓释及控制措施；

——应与本行的发展战略、风险管理策略相匹配；

13.2 技术前瞻性

本行持续探索以下前沿技术：

——大数据。在客户身份识别、行为识别、资信等级识别、网络环境识别等方面进行安全风险综合判断，应支持使用大数据等安全防范手段；

——生物特征识别。应支持使用生物特征识别鉴别客户身份，具备活体检测和防御伪冒介质及篡改攻击的能力，简化服务操作流程，提升认证安全能力；

——支持 IPv6 网络。本行应用程序接口基于 IPv6 技术进行接口开发及通信的相关要求。

——高可用架构。应用程序接口服务应支持异地/同城双活接入的高可用架构，提高系统灾备能力，保证服务连续性要求。

14 实施保障

14.1 组织保障

应用程序接口平台相关的管理机构包括：数字银行管理部、渠道管理部、信息技术部、风险管理部，具体职责分工如下：

——数字银行管理部负责组织平台的业务规划、管理、协调、考核、培训和分析；负责应用程序接口服务的流程制定、风险管控、营销推广、数据分析和业务升级工作；负责研究应用程序接口服务的发展趋势，制定发展规划，实施服务的创新和落地工作。

——渠道管理部负责支付类应用程序接口的业务规划、管理、协调、考核、培训和分析；负责服务的流程制定、风险管控、营销推广、数据分析和业务升级等工作；

——信息技术部负责监督应用程序接口平台的开发、优化升级工作，以及现场人员管理、软件开发质量及进度跟踪、上线后的日常运行维护和向其他管理部门及时反馈等工作；负责应用程序接口服务相关制度的制定、修订和完善，对制度执行情况进行监督检查；

——风险管理部负责从风险管理角度对应用程序接口的风险进行管理，开展风险监测、分析及报告；

14.2 管理制度

14.2.1 产品研发、测试投产、应急响应管理

应用程序接口平台产品研发、测试投产、应急响应管理应满足以下要求：

——制定桂林银行信息科技需求及项目管理相关办法，规范信息科技系统建设，保障本行系统建设的工作规范、质量和效率；

——业务需求需要需求架构部对业务需求进行分析和梳理，形成需求规格说明书，制定相应的开发计划，并通过需求评审会；

——项目实施组根据需求规格说明书进行系统设计，形成相应的概要设计，详细设计，数据库设计和接口设计文档，并通过系统设计评审会；

——开发人员需要根据相应的设计文档进行开发，同时需参照信息科技开发规范进行有序开发或修订，并完成单元测试或技术测试；

——项目测试包括 sit、uat 测试，每个阶段的测试需要遵守信息科技部的测试规范进行，同时测试完成需要出具测试报告；

——项目投产需要提交测试报告、测试案例、代码清单、上线申请单，进行上线审批，审批通过才能上线；

——项目实施过程中需要每周汇报各个阶段实施进度，遇到风险及时汇报；

——严格按照桂林银行相关应急预案实施，对相关机构在应急响应中的职责范畴进行界定，全面提高对突发事件的综合管理水平和应急处置能力；

——定期开展应急演练，形成应急演练报告。

14.2.2 生产运营及业务管理

应用程序接口生产运营及业务管理应满足以下要求：

——制定应用程序接口开发规范，明确接口规范要求，保障业务安全；

——指定专门人员每年对平台涉及的管理办法、操作规程、营销指引等相关制度的制定和修订；

——通过内部 OA 正式公文、邮件、通知等正式、有效的方式进行制度发布，并进行版本控制。

14.2.3 企业标准宣传及实施机制

应用程序接口安全规范宣传及实施机制应满足以下要求：

——开展本规范全行培训体系，根据培训的目标和参加培训的人员采取相应的培训方式，确保全行人员理解并执行；

——应用程序接口安全规范实施监督考核机制，由相应管理部门负责监督和考核标准执行情况，发现问题及时整改落实。

14.2.4 安全检测及安全评估保障

应用程序接口安全检测及安全评估保障应满足以下要求：

——应用程序接口业务管理部门应对接口服务可行性进行研讨并提出要求；

——接口上线前应通过本行信息安全部或委托第三方安全检测机构对应用程序接口进行检测，保证技术安全；

——接口上线后应定期对应用程序接口进行巡检，保证接口服务质量。