CCS 03.060
A11

Q/GXGB

广西北部湾银行企业有限公司企业标准

Q/GXGB 0003—2020

广西北部湾银行应用程序接口安全管理规范

Guangxi Beibu Gulf Bank Application Programming Interface Secure Management Specification

2020－09－25 发布　　2020－09－25 实施

广西北部湾银行股份有限公司　发布

目　　次

前　　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由广西北部湾银行股份有限公司提出。

本标准起草单位：广西北部湾银行股份有限公司。

本标准主要起草人：汪成钢、梁生安、姜雄飞。

本标准为首次发布。

企业标准信息公共服务平台
公开 2020年09月27日 09点48分

广西北部湾银行应用程序接口安全管理规范

1 范围

本标准规定了商业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。

本标准适用于广西北部湾银行对外互联的应用程序接口（但不包括银行内部使用API和银企直连等定制API）的设计和应用，以指导从事或参与广西北部湾银行应用程序接口服务的银行业金融机构、集成接口服务的应用方开展相关工作。

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 25069 信息安全技术 术语

JR/T 0071 金融行业信息系统信息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 定义和术语

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

调用广西北部湾银行应用程序接口的机构。

3.3

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

由广西北部湾银行自行定义，用于区分广西北部湾银行应用程序接口功能的唯一标识。

3.4

应用程序接口统一识别码 uniform application programming interface ID

广西北部湾银行依据行业主管部门发布的编码规则，生成的广西北部湾银行应用程序接口统一识别码。

注：用于标识广西北部湾银行机构代码、接口类型、服务类别、接口顺序号等内容。

3.5

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。

3.6

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，由广西北部湾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。

3.7

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应用程序接口提供的功能和数据。

3.8

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。

注： 包括但不限于可执行文件、组件等。

3.9

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。

3.10

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。

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。

3.11

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。

3.12

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）

API_ID：接口唯一标识（Application Programming Interface unique ID）

App_ID：应用唯一标识（Application unique ID）

App_Secret：应用鉴别密文（Application Secret）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

U_API_ID：应用程序接口统一识别码（Uniform Application Programming Interface ID）

SSL：安全套接层协议（Secure Sockets Layer）

TLS：安全传输层协议（Transport Layer Security）

MAC：消息鉴别码（Message Authentication Code）

5 总体概述

广西北部湾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。广西北部湾银行通过为合作伙伴提供用以互联的应用程序接口，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，调用广西北部湾银行应用程序接口，获取广西北部湾银行提供的各类服务。

6 接口类型与安全级别

6.1 接口类型

广西北部湾银行应用程序接口主要为服务端对服务端集成方式。

应用方服务端直接调用广西北部湾银行应用程序接口（如REST、SOAP协议），访问广西北部湾银行信息系统。

6.2 安全级别

按照服务类型将广西北部湾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，此类广西北部湾银行应用程序接口包括但不限于：

a）广西北部湾银行通过API，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；

b）广西北部湾银行通过API，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；

对于上述服务，若确需使用API直接连接方式进行服务调用，广西北部湾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，此类广西北部湾银行应用程序接口包括但不限于：广西北部湾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。

7 安全设计

7.1 设计基本要求

a)使用的密码算法、技术及产品符合国家密码管理部门及行业主管部门要求，优先支持国密加密算法。

b)应用程序开发程度编码严格按照安全编码规范执行，防范代码安全缺陷。

c)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及测试，并持续关注该应用组件相关漏洞信息和版本更新情况，及时更新相关组件。

d)应用程序接口上线投产前进行代码安全扫描，确保代码安全可靠。

e)应用程序接口源代码版本按照广西北部湾银行软件管理与控制规程执行，并就接口废止、变更等情况与应用方保持信息同步。

f)广西北部湾银行向应用方提供的异常与调试信息，禁止包含服务器、中间件、数据库等软硬件信息或内部网络信息。

7.2 接口安全设计

7.2.1 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。

App_ID、数字证书。

App_ID、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) 广西北部湾银行应结合金融服务场景，对不同安全级别的广西北部湾银行应用程序接口设计不同级别的用户身份认证机制。

2) 用户身份认证应在广西北部湾银行执行，对于A2级别接口中的资金交易类服务，用户登录身份认证至少使用双因子认证的方式来保护账户财产安全。

7.2.2 接口交互安全

a) 广西北部湾银行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。

b）应对通过广西北部湾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，广西北部湾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。

c）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密码控件类安全产品，执行替换输入框原文、防键盘窃听、防截屏等安全防护措施，确保客户支付敏感信息安全；

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加密算法进行加密；若确需使用广西北部湾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，应使用密码技术执行传输通道加密、签名保证信息的机密性和完整性；

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。

7.3 服务安全设计

7.3.1 授权管理

广西北部湾银行应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

服务安全设计应具备以下攻击防护能力：

API对常见的SQL注入、跨站攻击等网络攻击具有安全防护能力。

API通信严格执行通信认证与权限控制，防范未授权访问和信息泄露。

7.3.3 安全监控

a）广西北部湾银行应对接口使用情况进行监控，完整记录接口访问日志。

b）日志应满足以下要求：

广西北部湾银行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。

7.3.4 密钥管理

a）加密和签名宜分配不同的密钥，且相互分离。

b）不应以编码的方式将私钥明文（或密文）编写在广西北部湾银行应用程序相关代码中，App_Secret或私钥不应存储于广西北部湾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。

c）应依据广西北部湾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。

8 安全部署

a）广西北部湾银行与应用方应遵循广西北部湾银行网络安全防护架构部署。广西北部湾银行及应用方都应在互联网边界部署硬件网络防火墙、IDS/IPS、WAF、DDoS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。

b）广西北部湾银行应用程序接口服务层应部署流量控制、监控分析、认证鉴权、报文交换、服务组合等服务，其中认证鉴权、报文交换、服务组合等服务也可部署在银行业务层。广西北部湾银行应用程序接口服务层与银行业务层之间应部署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。

c）广西北部湾银行的安全控制要求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。

9 安全集成

9.1 应用方核准

9.1.1 应用方准入

应对申请接入商业银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。各参与开展业务机构应从如下方面开展应用方接入审核：

应对应用方开展准入审核，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。同时应全面审慎地考察、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。

9.2 接入安全控制

9.2.1 身份认证

a）应用方身份声明：

1）应用方准入审核通过后，广西北部湾银行配置唯一标识 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，广西北部湾银行应对应用方上传的公钥进行登记。

2）广西北部湾银行应对应用唯一标识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。

b）应用方身份认证：

1）应用方在请求广西北部湾银行应用程序接口时，广西北部湾银行应对应用方身份进行认证，认证方式包括但不限于以下任意一种方式：

基于应用唯一标识App_ID和应用鉴别密文App_Secret对应用方身份进行认证。

基于应用唯一标识App_ID和数字证书方式对应用方进行身份认证。

基于应用唯一标识App_ID和公私钥对方式对应用方进行身份认证。

基于应用唯一标识App_ID与应用鉴别密文App_Secret、数字证书（或公私钥对）的组合，对应用方进行身份认证。

2）对于 A2 类，应用方身份认证应使用 1）中第二条至第四条给出的任意一种方式进行双向身份认证。

3）广西北部湾银行应对广西北部湾银行应用程序接口连接时间进行限制（如设置接口会话或令牌有效期），依据业务必须的最小时间设计有效期，避免长期有效连接。

4）广西北部湾银行应具备对广西北部湾银行应用程序接口主动断开连接（如主动失效令牌）的功能，具备发现恶意连接可主动处理的能力。

9.2.2 安全传输

广西北部湾银行与应用方之间使用互联网方式进行数据传输应符合下列安全要求：

对于A1类应采用MAC校验等手段，保证广西北部湾银行与应用方之间数据传输的完整性，必要时可使用数字签名技术。

对于A2类应采用数字签名等手段，保证广西北部湾银行与应用方之间数据传输的完整性与不可抵赖性。

应采用SSL/TLS等安全通道连接进行通信，宜使用TLS1.2及以上版本。

9.3 运行安全

9.3.1 用户身份认证

a）用户身份认证应在广西北部湾银行完成，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。

b）广西北部湾银行应对应用方上送的用户相关信息进行核验。

c）广西北部湾银行应结合具体场景，依据业务必须的最小时间设计用户会话有效期，用户长期处于无业务操作时，应结束会话。

9.3.2 权限控制

a）广西北部湾银行应用程序接口权限控制应满足以下安全要求：

广西北部湾银行应按应用方、应用唯一标识App_ID、接口、用户等维度，依据最小授权原则进行授权，对于未授权的资源禁止访问；

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

广西北部湾银行应对API的调用有效期进行控制（如单次有效、阶段性有效、协议期限内有效）。

b）广西北部湾银行应为用户提供关闭广西北部湾银行应用程序接口相关服务的申请渠道，如电子银行或营业网点等。

9.3.3 数据安全

a）数据完整性保护：

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）。

b）数据机密性保护：

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，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。

c）数据抗抵赖性保护：

应使用数字签名等技术确保A2类数据的不可抵赖性。

d）数据删除与销毁：

在合作终止后，应依据与广西北部湾银行约定的方式删除（或销毁）通过广西北部湾银行应用程序接口获取的广西北部湾银行及其用户的相关数据。

e）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。

9.3.4 应用方退出

应用方退出时，应用方应协同本行提供有序、可行的退出方案，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，应通过内部管理平台对认证信息（如App_Secret、公私钥对等）进行作废处理，并对应用方申请使用的应用进行下架处理。

10 安全运维

10.1 安全监测

10.1.1 运维监测

a）广西北部湾银行应建立广西北部湾银行应用程序接口运维监测平台，或将广西北部湾银行应用程序接口运维监测纳入广西北部湾银行统一监测平台并重点监测。

b）运维监测应具备以下监测能力：

监控广西北部湾银行应用程序接口相关服务器运行状态并建立告警机制；

监控广西北部湾银行应用程序接口服务状态（包括耗时、交易量、成功率等参数）并建立告警机制；

广西北部湾银行交易日志应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。

c）应用方应对其集成广西北部湾银行应用程序接口运行状态进行监测，发现异常应及时处置。

10.1.2 异常监测

a）广西北部湾银行应具备流量监控、故障隔离、黑名单控制等广西北部湾银行应用程序接口调用控制能力：

应具备广西北部湾银行应用程序接口调用流量控制能力，控制规则包括最大允许广西北部湾银行应用程序接口调用并发数、单位时间最大交易调用量等，控制措施包括告警、暂停、拒绝等；

应建立未授权和冒用广西北部湾银行应用程序接口的监测机制，发现问题及时处置；

应具备故障监测和恢复能力；

应具备应用方黑名单管理能力。

b）应用方应具备故障识别与隔离能力：

调用广西北部湾银行应用程序接口应设计熔断机制，熔断规则包括设置失败笔数阈值、广西北部湾银行应用程序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；

调用广西北部湾银行应用程序接口应建立异常告警处理机制。

10.2 风险控制

10.2.1 服务风险控制

a）应建立应用方信息（如运营能力、风控能力等）更新和复审机制。

b）应根据应用方调用广西北部湾银行应用程序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。

c）应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。

10.2.2 交易流程控制

a）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。

b）账户查询、资金交易、金融产品及服务申请类交易，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。

c）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。

10.2.3 交易风险监控

a）应将广西北部湾银行应用程序接口纳入银行风险监控范围，对应用方和用户账户资金活动情况进行实时监控。

b）资金交易应满足行业监管部门对反洗钱、反欺诈方面的相关要求。

c）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。

d）对监控到的风险交易应进行及时分析与处置。

10.3 变更控制

a）广西北部湾银行应用程序接口发生变更时，应及时评估影响并告知应用方，制定变更方案和应急预案，按需进行接口变更发布，并充分履行用户告知义务。

b）应用方对广西北部湾银行应用程序接口的使用发生重大变更时，如其交易量预期发生变化、对广西北部湾银行应用程序接口集成方案进行修改等可能对广西北部湾银行系统安全性、业务连续性等造

成重大影响的有关事项，应制定变更方案和应急预案，评估变更带来的风险，并及时告知广西北部湾银行，同时充分履行用户告知义务。

c）应用方使用广西北部湾银行应用程序接口发生重大变更时，广西北部湾银行应对其变更进行风险和影响评估，并采取相应的处置措施。

10.4 运行维护

广西北部湾银行应定期对广西北部湾银行应用程序接口进行安全检查，包括进行漏洞扫描、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。

10.5 事件处理

广西北部湾银行应制定应急处理方案，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。

11 服务终止与系统下线

a）服务终止前，广西北部湾银行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。

b）广西北部湾银行应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。

c）系统（接口）下线应在相关服务确认终止之后执行，在下线之前应设置挡板（如服务终止提示信息），明示应用方服务已终止。

d）广西北部湾银行在系统（接口）下线之后应将有关数据进行归档处理，数据保留期限应按照国家与行业主管部门、广西北部湾银行相关规定与规则执行。

12 安全管理

12.1 管理制度

a）应将广西北部湾银行应用程序接口的管理纳入广西北部湾银行现行管理体系中，对广西北部湾银行应用程序接口进行全生命周期的安全管理。

b）应建立覆盖广西北部湾银行应用程序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，以确保广西北部湾银行应用程序接口的一致性和连贯性，保障广西北部湾银行应用程序接口效率及安全性。

c）应提供开发手册以指导应用方安全集成广西北部湾银行应用程序接口，开发手册包括但不限于安全集成要求、集成示例，以及测试环境的使用等。

12.2 应用安全责任

a）广西北部湾银行与应用方应以合同或协议的方式，明确规定广西北部湾银行应用程序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。

b）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，不应以使用广西北部湾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广西北部湾银行，也与广西北部湾银行服务无关。

c）应用方不应将通过广西北部湾银行应用程序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。

d）无论合作关系是否续存，应用方应依据与广西北部湾银行的协议约定，履行用户信息保密责任。

12.3 安全审计

a）应完整记录广西北部湾银行应用程序接口访问日志，日志记录应至少包括 7.3.3 所述日志内容。

b）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）。

c）应对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。