ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0185—2020

商业银行应用程序接口安全管理规范

Commercial bank application programming interface secure management specification

2020－02－13 发布　　2020－02－13 实施

中国人民银行　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国金融电子化公司、中国银联股份有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、中国邮政储蓄银行股份有限公司、招商银行股份有限公司、上海浦东发展银行股份有限公司、中信银行股份有限公司、兴业银行股份有限公司、中国民生银行股份有限公司、中国光大银行股份有限公司、平安银行股份有限公司、广发银行股份有限公司、北京银行股份有限公司、徽商银行股份有限公司、山东省城市商业银行合作联盟有限公司、齐鲁银行股份有限公司、浙江网商银行股份有限公司、中信百信银行股份有限公司、山东省农村信用社联合社、北京中金国盛认证有限公司、北京银联金卡科技有限公司、中金金融认证中心有限公司、中国外汇交易中心。

商业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。

本标准适用于商业银行对外互联的应用程序接口的设计和应用，以指导从事或参与商业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，并为第三方安全评估机构等单位开展安全检查与评估工作提供参考（接口类型关系详见附录A）。其他类型应用程序接口的设计和应用可参照本标准执行。

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

3 术语和定义

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。

3.4

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

商业银行依据行业主管部门发布的编码规则，生成的商业银行应用程序接口统一识别码。

注：用于标识商业银行机构代码、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。

3.7

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1：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。

注2：改写 GB/T 35273—2017，定义 3.1。

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。

[JR/T 0149—2016，定义 3.1]

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。

[GB/T 35273—2017，定义 3.6]

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）

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）

MAC：消息鉴别码（Message Authentication Code）

5 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（外部 API，详见附录 A），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。

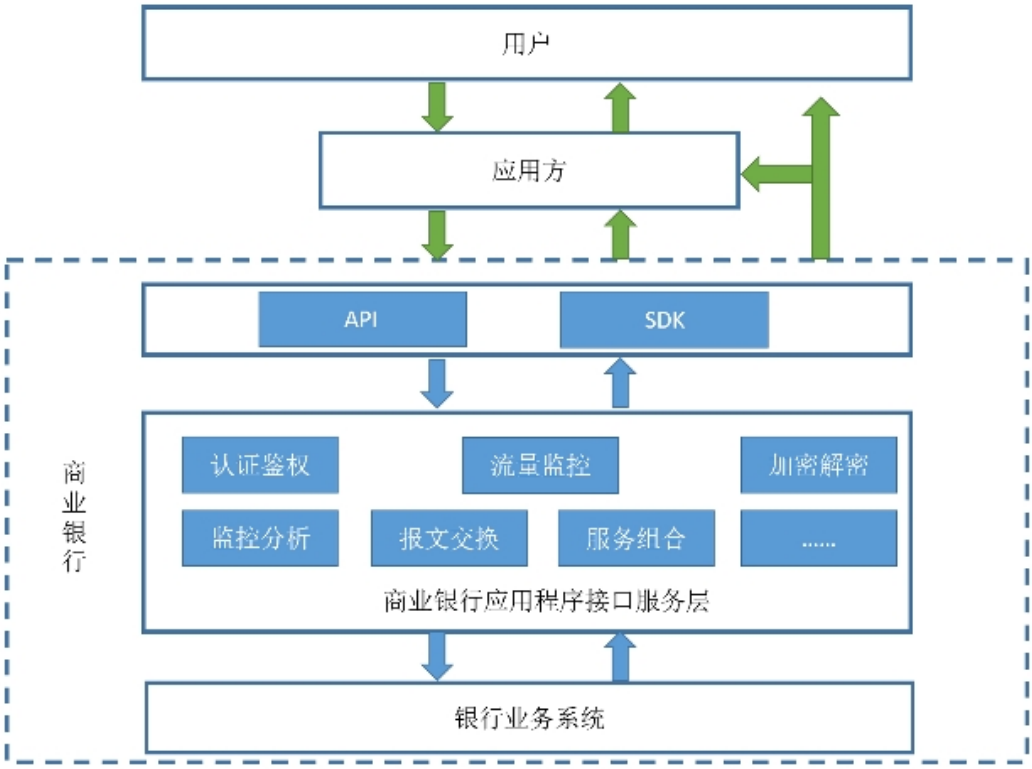


图1 商业银行应用程序接口逻辑结构图

6 接口类型与安全级别

6.1 接口类型

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）。

——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 SDK 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。

6.2 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；
- 对于上述服务，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。

7 安全设计

7.1 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，并依照安全编码规范进行开发。

——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披露和更新情况，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。

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) 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。
2) 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。

7.2.2 接口交互安全

商业银行应用程序接口交互安全要求如下：

——商业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。

——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。

7.3 服务安全设计

7.3.1 授权管理

商业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SDK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。

7.3.3 安全监控

安全监控安全要求如下：

——商业银行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：

- 商业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

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。

8 安全部署

商业银行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，见图2，进行商业银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、IDS/IPS、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。

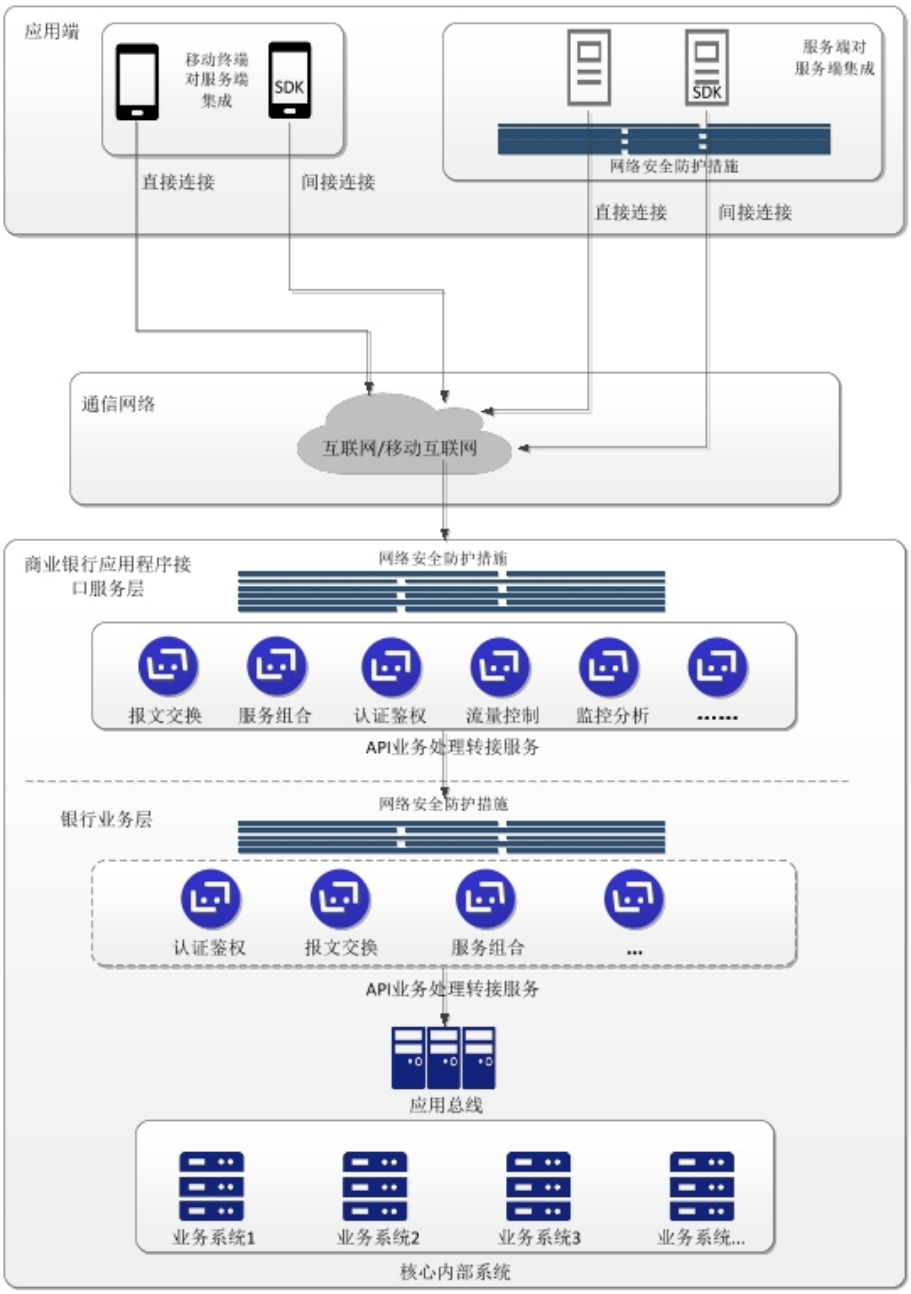


图 2 商业银行应用程序接口网络部署示意图

商业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。商业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。

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商业银行应用程序接口相关应用服务。

商业银行的安全控制要求依据 JR/T 0071 部署相应级别的安全控制措施。应用方部署商业银行应用程序接口有关安全控制措施，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。

9 安全集成

9.1 应用方核准

9.1.1 应用方准入

商业银行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：

——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。

——应在应用方申请接入时全面审慎地考察、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。

——应制定商业银行应用程序接口合作协议，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与应用方进行约定。

——不应通过开放应用程序接口的方式变相开展跨机构清算业务。

9.1.2 应用方身份核验

商业银行在应用方接入注册与审批阶段，应通过线上或线下手段，对应用方身份进行核验和管理：

——应用方应按照商业银行要求，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。

——应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。

9.2 接入安全控制

9.2.1 身份认证

商业银行与应用方之间的身份认证要求如下：

a) 应用方身份声明：

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

2) 商业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) 应用方在请求商业银行应用程序接口时，商业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) 商业银行应对商业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) 商业银行应具备对商业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

商业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,保证商业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,保证商业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TLS 1.2及以上版本。

9.3 运行安全

9.3.1 用户身份认证

商业银行对用户身份的认证要求如下:

——用户身份认证应在商业银行完成,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。

——商业银行应对应用方上送的用户相关信息进行核验。

——商业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

商业银行应对接口权限进行有效控制,包括:

——商业银行应用程序接口权限控制应满足以下安全要求:

- 商业银行应按应用方、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;
- 商业银行应对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)。

——商业银行应为用户提供关闭商业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

应用方在数据安全保护方面的安全要求如下:

——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)。

——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,应部署商业银行SDK、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。

——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。
——数据删除与销毁：在合作终止后，应依据与商业银行约定的方式删除（或销毁）通过商业银行应用程序接口获取的商业银行及其用户的相关数据。
——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 应用方安全能力

应用方在安全能力方面的要求如下：
——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。
——应遵循商业银行的安全设计要求，使用商业银行提供的安全接口，并依据用户手册和安全规范进行集成。
——应留存与商业银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。
——应通过技术手段与管理措施等，防止接口滥用。

9.3.5 应用方接口集成

应用方在接口集成方面的要求如下：
——应用方应根据商业银行提供的用户手册以及商业银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，应用方应按照商业银行提供的用户手册，妥善使用和保管相关密钥、数字证书。
——如商业银行提供封装了商业银行应用程序接口调用的SDK，则应用方需使用商业银行提供的SDK进行API调用，应用方不得对商业银行提供的SDK进行反编译、篡改或二次封装。
——若应用方发现商业银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商业银行。应用方未经商业银行许可，不得将缺陷细节透露给任何其他第三方。
——禁止应用方利用商业银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。

9.4 应用方退出

应用方退出时，商业银行应制定有序、可行的应用方退出机制，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，商业银行应对认证信息（如App_Secret、公私钥对等）进行作废处理，归档并保存待查。

应用方应按照商业银行的要求，妥善处理其通过商业银行应用程序接口获取的用户信息与商业银行业务有关资料，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 安全监测

10.1.1 运维监测

运维监测的要求如下：
——商业银行应建立商业银行应用程序接口运维监测平台，或将商业银行应用程序接口运维监测纳入商业银行统一监测平台并重点监测。
——运维监测应具备以下监测能力：

- 监控商业银行应用程序接口相关服务器运行状态并建立告警机制；
- 监控商业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；
- 商业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。

——应用方应对其集成商业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

异常监测的要求如下：

——商业银行应具备流量监控、故障隔离、黑名单控制等商业银行应用程序接口调用控制能力：

- 应具备商业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商业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商业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。

——应用方应具备故障识别与隔离能力：

- 调用商业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、商业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；
- 调用商业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

商业银行实施服务风险控制的要求如下：

——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。

——应根据应用方调用商业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。

——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

交易流程控制的要求如下：

——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。

——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

商业银行交易风险监控的要求如下：

——应将商业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。

——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。

——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。

10.3 变更控制

接口变更的要求如下：

——商业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。

——应用方对商业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、对商业银行应用程序接口集成方案进行修改等可能对商业银行系统安全性、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，并及时告知商业银行，同时充分履行用户告知义务。

——应用方使用商业银行应用程序接口发生重大变更时，商业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 运维巡检

商业银行应定期对商业银行应用程序接口进行安全巡检，包括：

——应对商业银行应用程序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。

——应对应用方的商业银行应用程序接口安全集成情况进行检查。

应用方应定期对商业银行应用程序接口进行安全巡检，包括：应定期对其调用商业银行应用程序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。

10.5 事件处理

商业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

商业银行应制定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：

——服务终止前，商业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。

——商业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。

——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。

——商业银行在系统（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、商业银行相关规定与规则执行。

12 安全管理

12.1 管理制度

商业银行管理制度要求如下：

——应将商业银行应用程序接口的管理纳入商业银行现行管理体系中，对商业银行应用程序接口进行全生命周期的安全管理。

——应用程序接口应采用统一格式的识别码，并在相关平台进行注册和登记，编码规则详见附录 B。

——应建立信息公告制度，通过官方网站等公开渠道发布其商业银行应用程序接口内容，并及时更新。

——应建立覆盖商业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，以确保商业银行应用程序接口的一致性和连贯性，保障商业银行应用程序接口效率及安全性。

——应提供开发手册以指导应用方安全集成商业银行应用程序接口，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

商业银行与应用方应以合同或协议的方式，明确规定商业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，包括但不限于：

——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。

——明确商业银行与应用方的信息安全责任。

——应用方不应将通过商业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。

——无论合作关系是否续存，应用方应依据与商业银行的协议约定，履行用户信息保密责任。

12.3 安全审计

商业银行应具备以下安全审计能力：

——应完整记录商业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。

——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）。

——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。

应用方应具备以下安全审计能力：

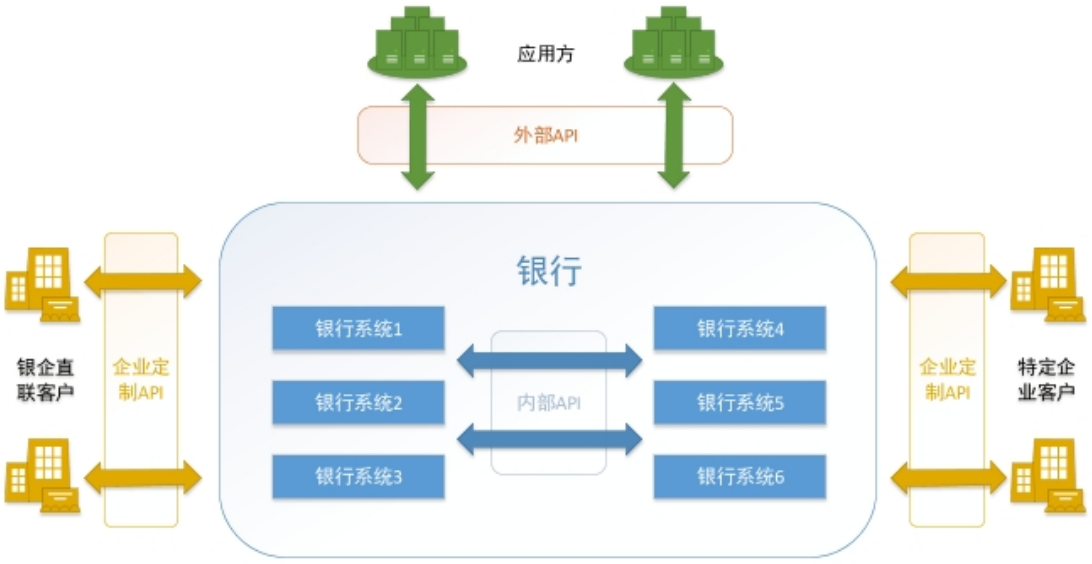
——应完整记录商业银行应用程序接口访问日志，日志记录应符合 7.3.3 所述日志要求。

——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。

——应提供查询应用方用户商业银行应用程序接口相关登录、授权、交易等历史操作日志功能。

附 录 A
（规范性附录）
商业银行应用程序接口关系示意

商业银行使用的 API 类型可分为内部 API、企业定制 API 与外部 API 三种类型，分类示意如图 A.1 所示。



图A.1 银行 API 示意

内部 API（Private APIs）：指银行内部信息系统间的 API，它促进了业务系统之间的信息互通，仅供银行内部开发者使用。

企业定制 API（Partner APIs）：指银行与特定的合作伙伴之间进行定制集成，目标是支持特定的业务流程或产品的 API，有时甚至约定使用专有网络进行通信。目前银行“银企直联”模式属于此类范畴。

外部 API（Public APIs）：指银行广泛地面向应用方提供标准接口，供外部合作伙伴使用的 API，较前两类 API 更深入、更广泛地面向外部合作者提供服务。**本标准所述商业银行应用程序接口即为外部 API。**

附 录 B
（规范性附录）
商业银行应用程序接口统一识别码编码规则

B.1 概述

本附录规定了银行使用的商业银行应用程序接口统一识别码的编码规则。商业银行应用程序接口统一识别码由商业银行依据编码规则生成。

B.2 接口统一识别码结构与长度

商业银行应用程序接口统一识别码（U_API_ID）编码格式为ASCII码，长度为24个字符，由2个字符的固定位，6个字符的商业银行机构代码、2个字符的接口类型编码、6个字符的服务类别编码、6个字符顺序码编码和2个字符的保留位编码组成。

B.3 接口统一识别码编码

B.3.1 接口统一识别码编码结构

商业银行应用程序接口统一识别码（U_API_ID）编码见表B.1。

表B.1 商业银行应用程序接口识别码编码结构

固定位	机构代码	接口类型	服务类别	顺序码	保留位
2个字符	6个字符	2个字符	6个字符	6个字符	2个字符

B.3.2 固定位

固定位值固定为字母“OP”，表示商业银行应用程序接口。

B.3.3 商业银行机构代码

商业银行机构代码应符合JR/T 0124—2014，采用金融机构编码的前6位字符。

B.3.4 接口类型编码

接口类型编码由2个字符组成。
00保留，01表示A1安全级别，02表示A2安全级别。

B.3.5 服务类别编码

服务类别编码由6个数字字符组成，分为一级标识与二级标识，各机构应根据自身商业银行应用程序接口类别实际情况按照如下规则自行编码。

对于一级标识，主要用于标识银行服务类型，对于二级标识，主要用于标识一级标识中的细分服务类型，具体编码格式见表B.2。

表 B.2 服务类别编码结构

一级标识	二级标识
2 个字符	4 个字符

一级标识：00 保留，01 账户服务、02 支付结算、03 投资理财、04 信贷、05 信用卡、06 行业服务、07 国际业务、08 科技服务，后续服务类别从 09 至 99 顺序编号。其中 06 行业服务指商业银行通过商业银行应用程序接口向其他行业提供金融服务。

二级标识在一级标识分类基础上，优先使用从 0001 至 9999 顺序编号，0000 为保留位。如，一级标识 01 账户服务类，二级标识为 0001 存管账户、0002 积分账户等。

B.3.6 顺序码编码

顺序码编码由6个字符组成，同一商业银行机构代码、同一接口类型、同一服务类别下，多个不同商业银行应用程序接口的顺序码优先使用从000001-999999的顺序连续编码。

B.3.7 保留位编码

保留位编码保留使用，默认值为00。

参 考 文 献

[1] GB/T 13016—2009 标准体系表编制原则和要求

[2] GB/T 13017—2008 企业标准体系表编制指南

[3] GB/T 35273—2017 信息安全技术 个人信息安全规范

[4] JR/T 0092—2019 移动金融客户端应用软件安全管理规范

[5] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

[6] JR/T 0171—2019 个人金融信息保护技术规范

[7] 中国人民银行. 中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知(银发〔2011〕17号)，2011年1月21日

[8] 中国人民银行. 中国人民银行关于银行业金融机构进一步做好客户个人金融信息保护工作的通知（银发〔2012〕80号），2012年3月27日

[9] 中国人民银行. 中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016年6月13日

[10] 中国银行保险监督管理委员会. 商业银行信息科技风险管理指引（银监发〔2009〕19号文印发），2009年3月3日

[11] 香港金融管理局. Open API Framework for the Hong Kong Banking Sector，2018年7月18日

[12] The Open Banking Standard. OBWG (Open Banking Working Group),UK

[13] The Association of Banks in Singapore (ABS) and Monetary Authority of Singapore. Finance-as-a-Service：API Playbook，Financial World