ICS 35.240.40
A 11

Q/CMBC

中 国 民 生 银 行 企 业 标 准

Q/CMBC 003—2022
代替 Q/CMBC 003-2021

中国民生银行应用程序接口安全管理规范

CMBC application programming interface secure management specification

2022－08－31 发布　　2022－08－31 实施

中国民生银行　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

本文件由中国民生银行股份有限公司提出并归口。

本文件起草部门：中国民生银行股份有限公司。

本文件主要起草人：刘衍波、蔡丹平、陶江、邹长龙、彭真山、李晓东、楼晔、毕永军、虞刚、战扬、段博超、杨朝、竺铁生、闫涛、缴建、崔航、殷和雨、王广驰、袁丽欧。

本文件代替Q/CMBC 003-2021《中国民生银行应用程序接口安全管理规范》，与Q/CMBC 003-2021相比，除编辑性改动外，主要的变化如下：

a) 更改了身份认证安全中关于用户身份认证安全要求的部分内容（见7.2.1-b）；

b) 更改了攻击防护的部分内容（见7.3.2）；

c) 更改了算法和密钥管理的部分内容（见7.3.4）；

d) 更改了身份认证中与应用方之间的身份认证要求的部分内容（见9.2.1-b）；

e) 更改了安全传输中的数据传输要求的部分内容（见9.2.2-c）；

f) 更改了应用方安全能力要求的部分内容（见9.3.4-c）；

g) 更改了运维监测要求的部分内容（见10.1.1-b、d）；

h) 更改了服务风险控制要求，增加了本行应用服务可靠性要求以及服务性能要求（见10.2.1）；

i) 删除了创新及前瞻性中API业务连续性节点，增加了人工智能技术创新应用和应用多活技术创新应用两个节点（见13.3、13.4）。

本文件及其所代替文件的历次版本发布情况为：

——2020年首次发布为Q/CMBC 003-2020；

——2021年第一次修订为Q/CMBC 003-2021，代替Q/CMBC 003—2020；

——本次为第二次修订。

中国民生银行应用程序接口安全管理规范

1 范围

本文件规定了中国民生银行（下称“本行”、“我行”或“民生银行”）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，明确了本行应用程序接口服务创新及前瞻性标准，确立了本行应用程序接口服务实施保障机制。

本文件适用于本行对外互联的应用程序接口的设计和应用，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。

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。

GB/T 1.1—2020 标准化工作导则 第1部分：标准化文件的结构和起草规则

GB/T 25069 信息安全技术 术语

JR/T 0071.2-2020 金融行业信息系统信息安全等级保护实施指引 第2部分：基本要求

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 术语和定义

GB/T 25069、JR/T 0185-2020界定的术语和定义适用于本文件。

4 缩略语

下列术语适用于本文件。

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)

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

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。通过为应用方提供用以互联的应用程序接口，输出我行金融服务能力与信息技术能力，提高我行场景化金融服务水平，构建开放、合作、共赢的金融服务生态体系。应用方能够通过互联网渠道（公网或者专线），调用我行产品和服务的应用程序接口，获取我行提供的各类服务，其逻辑结构见图 1。

民生银行应用程序接口服务的参与方主要包括用户、应用方及民生银行，民生银行通过 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，实现服务的对外输出。

用户发起应用程序接口应用请求，并接收由应用方或民生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民生银行提交相关请求、接收返回结果，依照流程进行服务请求处理或反馈用户。

民生银行构建应用程序接口、应用程序接口接入层、集成层和场景层以提供应用程序接口服务。应用程序接口接入层负责接收应用方请求，进行安全管控检查及相关处理，转发应用方请求至集成层，集成层将应用方请求转发至场景层及相关业务系统处理，并将处理结果反馈应用方或用户，不涉及具体业务逻辑处理，实现对应用程序接口和应用方的管理。

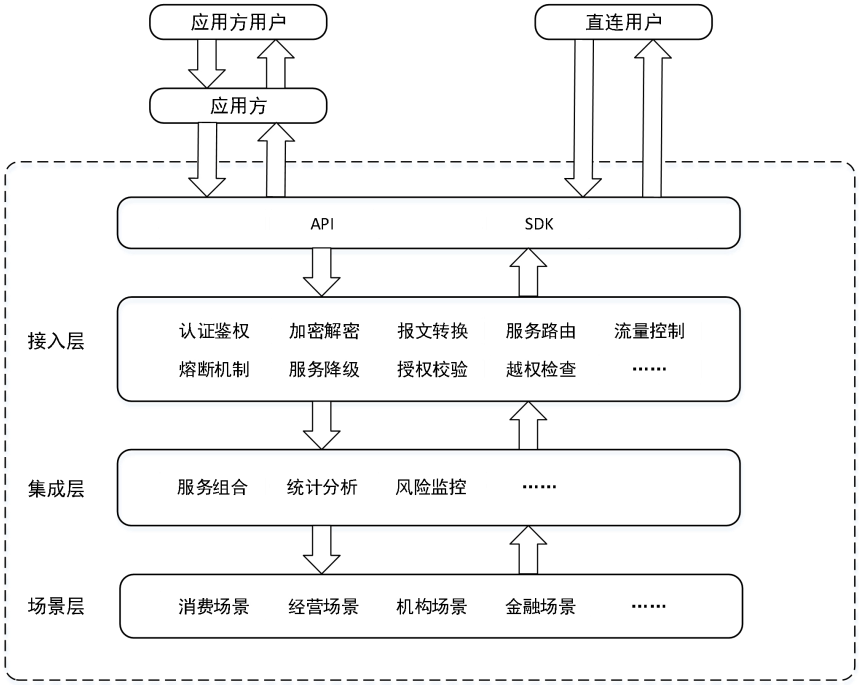

图 1　民生银行应用程序接口逻辑结构图

6　接口类型与安全级别

6.1　接口类型

我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：

a）应用方服务端直接调用我行应用程序接口（如REST、SOAP协议）。

b）应用方服务端使用我行提供的服务端SDK，间接访问我行应用程序接口。

其中，服务端SDK主要实现我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：

a）应用方移动终端应用软件直接调用我行应用程序接口。

b）应用方移动终端应用软件使用我行提供的移动终端应用SDK，间接访问我行应用程序接口。

其中，应用方移动终端应用软件直接调用我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，如提供我行公开信息查询、公开服务查询等。

移动终端应用SDK除封装我行通用接入算法外，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）我行应用程序接口，不将其单独列为我行应用程序接口的一种类型。

6.2 安全级别

我行按照服务类型将应用程序接口安全级别划分为三级，安全保护要求从A1至A3递增：

a) A1：金融产品和公共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，实施通用等级安全保护强度，此类应用程序接口包括但不限于：本行提供银行金融产品和服务的详细信息的“只读”查询服务。

b) A2: 账户信息查询应用类，此类金融服务与产品关乎用户个体的信息安全，实施高等级安全保护强度，此类应用程序接口包括但不限于：

本行通过SDK提供用户账户信息查询类服务，如账户余额、交易明细、账户限额、电子回单、金融产品和服务持有情况等。

c) A3: 资金交易与服务签约类，此类金融服务与产品关乎用户个体的账户与资金安全，实施最高等级安全保护强度，此类本行应用程序接口包括但不限于：

本行通过SDK提供资金交易类服务，如支付、转账、金融产品及服务的购买、交易权限或限额设定等；提供服务签约类交易，如产品签约等。

对于A2、A3类服务，若确需使用API直接连接方式进行服务调用，本行应对接入风险进行评估，严格评估应用方资质并制定专门的接口与应用方进行对接，应用方调用前应得到用户明确授权并签署授权协议。

7 安全设计

7.1 设计基本要求

应用程序接口安全设计应满足以下要求：

a) 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；

b) 应制定安全编码规范；

c) 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；

d) 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；

e) 应对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，应在应用程序接口上线前对代码进行安全扫描及渗透测试，扫描及测试通过后方可上线；

f) 应制定源代码和应用程序接口版本管理与控制规程，规范源代码和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；

g) 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、A3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。

3）对应用方身份认证应能识别应用方应用，App_ID和其他验证要素（App_Secret、数字证书或公私钥对）一一对应。

b) 用户身份认证安全要求如下：

1）应结合金融服务场景，对不同安全级别的应用程序接口采用不同级别的用户身份认证机制：

——A2 级别接口应采用 APP_ID、数字证书、用户 ID、用户授权识别码组合的方式进行身份认证。

——A3 级别接口应在 A2 级别的身份认证机制之上通过本行网上银行、手机银行等渠道对用户身份进行二次认证：

- 在本行企业网上银行、企业手机银行进行 A3 级别接口二次身份认证时，应使用本行颁发的硬件承载的数字证书以及登录密码进行身份认证；
- 在本行个人网上银行、个人手机银行进行 A3 级别接口二次身份认证时，应使用本行颁发的硬件承载的数字证书、登录密码、交易密码、短信验证码、生物特征码等多因子组合的方式进行身份认证。

2）用户身份认证应在本行完成，对于A3级别接口，用户登录身份认证应至少使用双因子认证方式来保护账户财产安全。

7.2.2 接口交互安全

民生银行应用程序接口交互安全要求如下：

a) 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) 应对通过应用程序接口进行交互的数据进行完整性保护，对于A2、A3级别的接口，本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) 应对通过应用程序接口进行交互的数据进行安全性保护，对于A2、A3级别的接口，本行和应用方应使用数字证书加解密机制来保证数据的安全性和保密性，防止敏感信息的泄露；

d) 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：

1）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；

2）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和安全性；

3）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。

e) 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

a) 应用方权限管理

1) 应根据不同应用方的服务需求，按照最小授权原则对应用方进行应用程序接口授权；

2) 应在对应用方进行应用程序接口授权时，充分审核应用方的相关资质及应用程序接口使用范围；

3) 应及时根据应用方的服务需求变化、相关资质变更情况进行评估并调整接口权限；对于已解约的应用方不允许调用接口；

4）如使用OAuth2.0机制，应满足如下安全要求：

——授权码长度应不少于4位且使用次数限制和超时机制。

——应对授权码等敏感信息进行标记化处理。

——token长度不应少于16位字符，对token应具备生成、存储、更新、超时等安全管理。

——仅允许应用方通过服务端调用本行的token获取、更新接口，同时应避免token明文暴露在客户的终端设备中。

b) 用户授权

1) 在ISV模式或第三方参与开放银行服务的场景下，用户根据需要获取的服务需求，对开放给应用方的接口及数据等权限进行授权管理，对于未授权的资源禁止开放给应用方;

2) 应通过有效手段对合作方使用客户信息的形式、周期等进行约束;

3) 授权应识别是否由用户本人发起，并核实本人意愿；应对用户身份及权限进行校验，防止水平越权或垂直越权；授权内容应包含授权有效期或者使用次数限制；

4) 针对存在代理方的合作模式，用户及代理方需均是商业银行用户，且用户及代理方应分别对商业银行进行授权；

5) 对于涉及客户授权的接口服务，应为客户提供关闭应用程序接口相关服务的渠道，包括不限于手机银行、网上银行、营业网点等；

6）对应用方访问用户数据的客户机制，可采用OAuth2.0机制。如使用OAuth2.0机制，应符合7.3.1节 a) 中第4条要求。

7.3.2 攻击防护

a) API和SDK应对常见的网络攻击如DDos拒绝服务攻击、DNS查询攻击、目录遍历、XSS跨站脚本攻击、CSRF跨站请求伪造等具有安全防护能力，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；

b) 应用程序接口应具备防API网络攻击能力，对常见的攻击类型如API参数篡改、中间人攻击、内容篡改、高频访问、低频撞库、越权访问、SQL注入等攻击采取包括但不限于网络专线、IP管控、隧道加密、认证鉴权、签名验签、双重签名、加密解密、参数校验、防重放、敏感字符筛查、流量控制、熔断控制、服务降级、授权校验、越权检查、敏感信息标记化、监测告警等防护措施；

c) 应用接口服务上线前，应完成科技安全风险评估和安全测试；

d) 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；

e) 移动终端应用SDK应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；

f) 移动终端应用SDK应对自身进行安全加固，应具备保持自身完整性、真实性，防止篡改及注入的功能，应具有已知漏洞的防范能力；

g) 移动终端应用SDK加固应采用vmp虚拟指令技术，实现SDK核心代码层隐藏加密、防逆向分析和防动态调试攻击。

7.3.3 接口安全监控

a) 应完整的记录应用程序接口访问日志。日志应满足以下要求：

1）本行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、失败、未知）、返回信息等；

2）应以文件、数据库等多种方式对接口访问日志进行保存；

3）应建立接口访问日志的定期备份机制；

4）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（或其他等效信息），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。

b) 应建立对应用程序接口的监控机制，包括：

1）应实现对应用程序接口调用情况的监控、分析，对于运行时异常接口调用及时预警；

2）应定期对应用程序接口调用情况进行回顾、分析，及时发现异常的接口调用行为并进行反馈。

7.3.4 算法及密钥管理

a) 算法管理要求如下：

1）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，使用的加密和签名算法应分配不同的密钥，且相互分离，数字证书签名和验签环节、交易报文加密和解密环节均应使用国家密码管理部门认可的国产密码算法；

2）我行与应用方之间的数字证书应使用国家权威第三方安全认证机构颁发的数字证书。

b) 密钥管理要求如下：

1）不应以编码的形式将私钥明文（或密文）编写在本行应用程序相关代码中；

2）非对称密码算法私钥应在可信环境生成，不进行传递，防止因代码泄露引发密钥泄露；

3）对于使用对称加密算法的单次会话，为避免攻击者通过获取明文密文组对密钥进行字典攻击，宜使用密钥变换、密钥协商等方法生成一次性密钥（会话密钥），以对设备或客户端主密钥进行保护。

c) 数字证书管理

1）应用方应使用我行证书下载平台进行线上证书下载操作；

2）应用方证书下载所需的信息应通过手机短信、邮件等方式直接发送给应用方，不应由我行管理人员获取应用方证书后进行转发；

3）应对数字证书的使用情况进行监控，发现异常可疑情况应及时暂停应用方数字证书的使用权限；

4）若出现应用方服务终止或系统下线等情况导致应用方不再使用数字证书的情况，应及时对应用方数字证书进行作废操作；

5）应依据本行应用程序接口等级设置不同的证书有效期，并对证书进行定期更新；

6）应在证书到期前及时通知应用方进行证书更新操作，避免因证书到期导致应用方接口调用失败。

8 安全部署

我行与应用方应遵循民生银行应用程序接口网络部署逻辑结构示意图，见图2，进行民生银行应用程序接口的安全部署。我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。

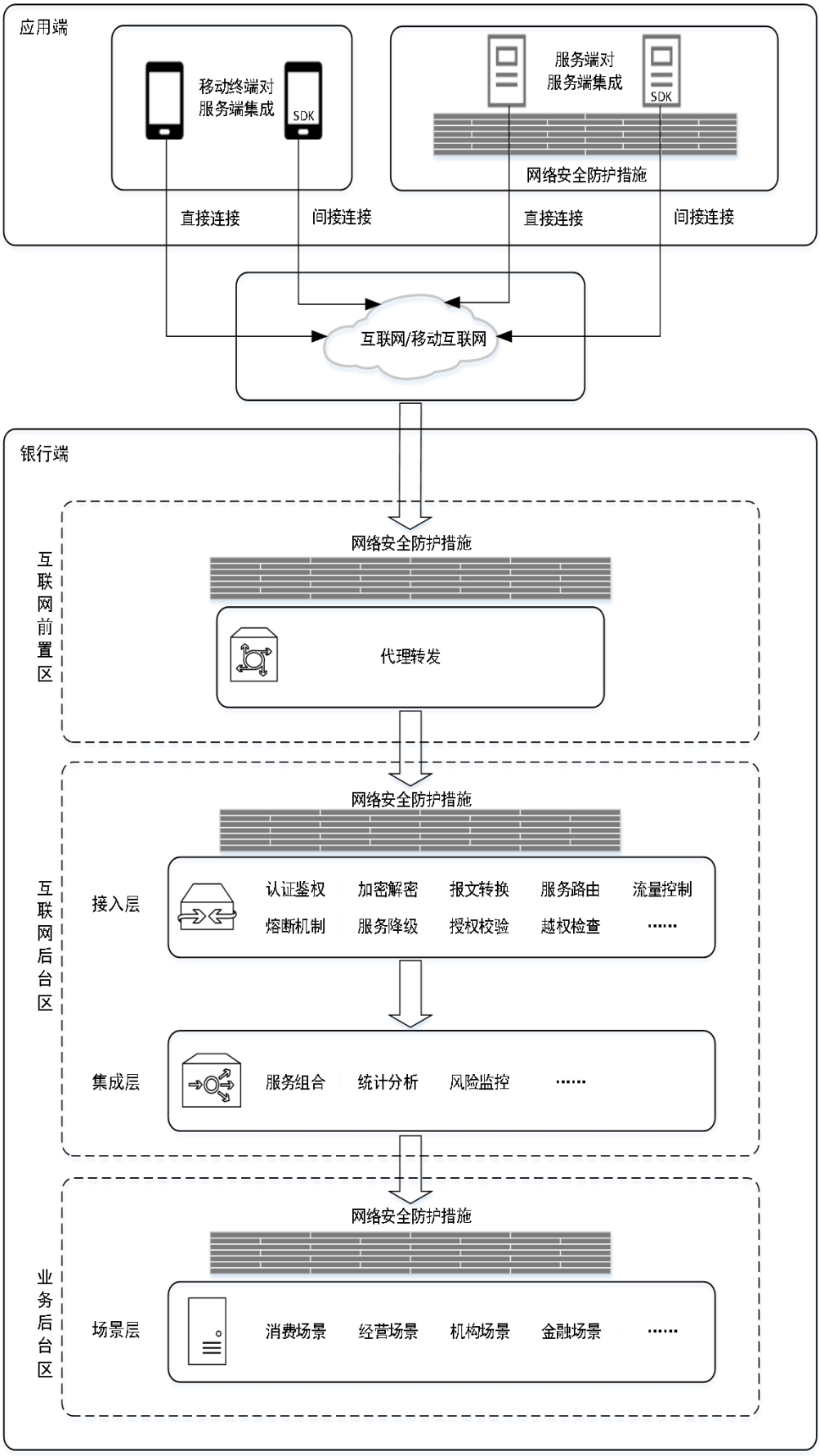
应用端
移动终端对
服务端集成
SDK
服务端对
服务端集成
SDK
网络安全防护措施
直接连接
间接连接
直接连接
间接连接
互联网/移动互联网
银行端
互联网前置区
网络安全防护措施
代理转发
互联网后台区
网络安全防护措施
接入层
认证鉴权
加密解密
报文转换
服务路由
流量控制
熔断机制
服务降级
授权校验
越权检查
……
集成层
服务组合
统计分析
风险监控
……
业务后台区
网络安全防护措施
场景层
消费场景
经营场景
机构场景
金融场景
……

图 2　民生银行应用程序接口网络部署示意图

民生银行应用程序接口接入层应部署认证鉴权、加密解密、报文转换、服务路由、流量控制、熔断机制、服务降级、授权校验、越权检查等服务，集成层应部署风险监控、统计分析等服务。民生银行应用程序接口集成层与场景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我行应用程序接口相关应用服务。

我行的安全控制要求依据JR/T 0071.2-2020部署相应级别的安全控制措施。应用方部署我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

我行应对申请使用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：

a) 对应用方开展准入审核，重点考察包括但不限于：

1）服务客群、服务场景、市场份额、运营能力、风控能力等方面；

2）应用方应拥有开展合作业务的资质。

b) 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；

c) 应制定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、交易安全保障责任保护等条款与应用方进行约定；

d) 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

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：

a) 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；

b) 可采用现场或远程视频的方式，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

民生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，我行应为其配置唯一标识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，我行应对应用方上传的公钥进行登记。

2）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、A3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）我行应对应用程序接口连接采用短连接形式或者对连接时间进行限制（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。对于采用令牌方式提供的连接，应确保令牌一次一用，最长5分钟内有效，超时自动失效以及一定的防预测性。

4）我行应具备对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。

5）应支持对应用方接入的IP黑白名单的配置，保证IP白名单的校验及IP黑名单的拦截。

9.2.2 安全传输

根据数据传输的安全要求，应使用安全的算法组合。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：

a) 对于A1类应采用MAC校验等手段，保证我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；

b) 对于A2、A3类应采用数字签名等手段，保证我行与应用方之间数据传输的完整性与不可抵赖性；

c) 应采用SSL/TLS等安全通道连接进行通信，应使用TLS1.2及以上版本。

9.3 运行安全

9.3.1 用户身份认证

对用户身份的认证要求如下：

a) 用户身份认证应在我行完成，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) 应对应用方上送的用户相关信息进行核验；

c) 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；

d) 应对一次性密码或授权链接设置有效期，同时应保证此类密码或链接仅能使用一次。

9.3.2 接口权限控制

应对接口权限进行有效控制，包括：

a) 应用程序接口权限控制应满足以下安全要求：

1）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；

2）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；

3）应根据业务类型对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）；

4）应对API的访问并发数进行控制，并对API调用失败率进行监控，对于失败率高的应用方进行预警和人工干预。

b) 应为用户提供关闭应用程序接口相关服务的申请渠道，如网上银行、手机银行或营业网点等。

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：

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：

1）不应采集、存储用户个人金融信息或支付敏感信息；

2）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，应部署民生银行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；

3）应限定通过应用程序接口获得的数据仅可以在该特定应用中使用，不得将其使用在该特定应用之外或为其他任何目的进行使用，也不得以任何方式将其提供给他人；

4）应用方应向用户提供隐私保护政策，隐私保护政策须在应用界面上明显位置向用户展示。

c) 数据抗抵赖性保护：应使用数字签名等技术确保A2、A3类数据的不可抵赖性。

d) 数据删除与销毁：

1）在合作终止后，应依据与我行约定的方式删除（或销毁）通过民生银行应用程序接口获取的民生银行及其用户的相关数据；

2）应用方应向用户提供修改、删除用户数据的方式，确保用户要求删除其用户数据时可通过该方式自行操作完成，并确保相关数据被完全删除。

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 应用方安全能力

应用方在安全能力方面的要求如下：

a) 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；

b) 应遵循民生银行的安全设计要求，使用民生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；

c) 应留存与民生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，日志留存应大于6个月，日志应至少包括交易流水号、应用ID、接口唯一标识、调用耗时、时间戳、返回结果（成功或失败）等要素信息；

d) 应通过技术手段与管理措施等，防止接口滥用；

e) 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；

f) 应用方应定期对应用进行安全巡检。

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：

a) 应用方应根据民生银行提供的用户手册以及民生银行授权其使用的服务类型，正确合理使用API；

b) 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，应用方应按照民生银行提供的用户手册，妥善使用和保管相关密钥、数字证书；

c) 如民生银行提供封装了民生银行应用程序接口调用的SDK，则应用方需使用民生银行提供的SDK进行API调用，应用方不得对民生银行提供的SDK进行反编译、篡改或二次封装；

d) 若应用方发现民生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民生银行。应用方未经民生银行许可，不得将缺陷细节透露给任何其他第三方；

e) 禁止应用方利用民生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。

9.3.6 应用方退出

应用方退出时，民生银行应制定有序、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，民生银行应对认证信息（如App_Secret、数字证书等）进行作废处理，归档并保存待查。

应用方应按照民生银行的要求，妥善处理其通过民生银行应用程序接口获取的用户信息与民生银行业务有关资料，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

我行运维监测的要求如下：

a） 建立应用程序接口运维监测平台，将应用程序接口纳入行内统一监测平台并重点监测；

b） 对应用程序接口相关应用服务器及数据服务器运行状态进行实时监控，根据影响程度及紧急程度进行分级告警，告警首先由一线值班人员进行处理，如有必要，通知系统运维人员进行处理，同时派发工单进行跟踪；

c） 对应用程序接口的 TPS、交易量、耗时、成功率等进行监测，形成应用方调用统计视图，对异常情况进行报警并以短信通知运维和运营人员；

d） 交易日志应至少包含交易流水号、应用 ID、接口唯一标识、时间戳等交易要素及交易完整报文，并对报文中的敏感数据做脱敏处理，日志应有归档机制，保存期限不少于 1 年。

应用方应对集成应用程序相关接口服务器进行监测，发现异常及时处置。

10.1.2 异常监控

异常监测的要求如下：

a） 我行应具备流量监控、故障隔离、黑名单控制等应用程序接口调用控制能力，具体要求如下：

1）应具备应用程序接口调用流量控制能力，控制规则包括最大允许应用方对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，宜支持不同维度的限流控制，包括但不限于IP/域名级别的限流，应用程序接口、应用（应用唯一标识）等级别的限流。；

2）应建立未授权和冒用我行应用程序接口的监测机制，发现问题及时处置；

3）应具备故障监测和恢复能力；

4）应具备应用方黑名单管理能力；

5）应具备IP黑名单与白名单管理能力，可从全局级及应用级两个维度进行控制IP黑名单/白名单。全局维度进行黑名单限制，应用维度进行黑名单限制和白名单检查。

b）应用方应具备故障识别与隔离能力：

1）调用民生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、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；

2）调用我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

本行应用服务可靠性要求如下：

a) 应用部署架构应采用多活机制，应用应部署在我行私有云上，在变更或出现故障时，可以通过流量负载控制或容器快速扩缩容能力，保障服务的连续不间断和服务性能，提升服务可靠性；

b) 系统服务时间应满足 7×24 小时不间断运行；

c) 应配备 7×24 小时运维应急人员，建立应急管理制度和团队，能积极响应生产紧急事件，出现重大应急事件时，30 分钟内由应急领导小组指示启动应急预案，并随时向应急领导小组报告；

d) 全年实际系统可用率应达到 99.9%，单次故障停机时间不超过 2 小时；

e) 恢复点目标（IT RPO）：0；

f) 恢复时间目标（IT RTO）：2 小时。

本行应用服务性能要求如下：

a) 应对接口的交易量、响应时间、响应率、交易成功率等关键指标进行实时监控和告警；

b) 应对服务部署所在的容器资源使用情况进行监控和告警；

c) 应用系统交易处理能力大于 100 笔/秒；

d) 单笔交易的平均响应时间小于 1000 毫秒；

e) 单笔交易的最大响应时间小于 5000 毫秒。

应用方服务风险控制的要求如下：

a) 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) 根据应用方调用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) 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：

a) 对应用方发起交易应校验 App_ID、报文签名等内容，并识别交易是否由应用方发起；

b) 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；

c) 账户查询、资金交易、金融产品及服务申请类交易，应识别交易是否由用户本人发起（或本人授权发起），并核实用户本人意愿；

d) 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

我行交易风险监控的要求如下：

a) 应将应用程序接口纳入我行风险监控范围，对应用方和用户账户资金活动情况进行实时监控。

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

我行接口变更的要求如下：

a) 我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) 接口发生重大变更会影响应用方业务连续性时需提前以电子邮件、即时消息、公告等方式通知应用方；

c) 应用方对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、对应用程序接口集成方案进行修改等可能对民生银行系统安全性、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，并及时告知民生银行，同时充分履行用户告知义务。我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

我行应定期对我行应用程序接口进行安全巡检，包括：

a) 应对我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；

b) 应对应用方的应用程序接口安全集成情况进行检查。

应用方应定期对我行应用程序接口进行安全巡检，应定期对其调用我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

我行与应用方应制定应急事件处理方案，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

我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：

a) 计划下线系统（接口）时，应对要下架的系统（接口）进行功能评估关联性评估；

b) 应将服务终止有关事项告知各相关方，并向相关平台提交有关接口的统一识别码注销申请；

c) 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；

d) 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；

e) 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、我行相关规定与规则执行。

12 安全管理

12.1 管理制度

管理制度要求见14.2。

12.2 应用安全责任

我行与应用方应以合同或协议的方式，明确规定民生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：

a) 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：

1） 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，不应以使用民生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；

2） 向金融消费者说明个人信息收集方并非民生银行，也与民生银行服务无关。

b) 明确民生银行与应用方的信息安全责任。

c) 应用方不得为合同协议约定之外的目的使用与银行合作项目相关的客户数据及运营数据，不得为合同协议约定之外任何目的擅自保存相关数据。

d) 应用方不应将通过民生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。

e) 无论合作关系是否续存，应用方应依据与民生银行的协议约定，履行用户信息保密责任。

12.3 安全审计

民生银行应用程序接口应具备以下安全审计能力：

a) 应完整记录应用程序接口访问日志，日志记录应至少包括交易流水号、应用方唯一标识、接口唯一标识、交易时间、返回结果等内容；

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；

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。

应用方应具备以下安全审计能力：

a) 应完整记录民生银行应用程序接口访问日志；

b) 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；

c) 应提供查询应用方用户访问民生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。

13 创新及前瞻性

13.1 大数据技术创新应用

13.1.1 数据标准

应用程序接口建设，业务字段、接口字段、数据库字段设计上应严格执行我行数据标准及质量规范。

13.1.2 数据应用

应根据接口安全级别及具体应用场景应建立数据指标分析机制，并根据以下类型设计指标：

a) 经营分析指标：基于客户的日常交易数据指标，主要用于本行经营机构和客群部门日常经营情况分析、智能获客、舆情分析、市场洞察及经营策略制定；

b) 业务风险指标：基于应用方及客户A2级以上接口的统计分析指标，主要用于应用方风险管理、欺诈风险预警、银行风险内控、反洗钱预警等方面；

c) 系统安全指标：基于应用系统及应用方的系统运行指标，主要用于对本行系统安全的监控、评估及风险预警。

根据具体使用场景使用上述指标并结合大数据技术制定相关指标分析工具、指标预警机制及相关预测模型，实现应用程序接口的数字化运营、风险分析及预警、系统安全监控。

13.2 API 接口平台化建设规划

为提升全行场景金融、生态金融服务能力，建立标准化开放服务输出环境，提高应用方对接效率和运营效率，规范应用程序接口服务业务管理，防范业务及技术风险，保障客户信息安全，我行应对API接口开展平台化建设，构建开放银行服务平台。

对外，平台应具备标准化接入能力，包括统一服务接入、统一接口规范、统一身份认证、自助沙箱联调等，并通过门户网站提供开发文档、接口申请、应用监控、数据统计等功能，为开发者提供便捷地对接体验。

对内，平台应具备并支持API自动生成开发文档、服务快捷上线能力，提供API生命周期管理、应用管理服务流程、服务审核信息触达、API分组权限管控等功能，为我行应用程序接口提供高效地管理工具。

13.3 人工智能技术创新应用

在应用程序接口服务的运维监测、风险识别等方面，面向本行系统级、主机级和服务级的交易监控指标，提取关键特征，利用机器学习回归算法，学习指标的历史运行规律，形成正常运行基带。一旦出现违反正常运行基带的监控数据，则发出告警并及时介入分析处理。

13.4 应用多活技术创新应用

本行应用服务应用层应采用双机房双活部署架构，数据库应采用MHA高可用架构，每年应定期进行服务器重启及跨机房切换演练，保证系统的高可用性及服务的可靠性。对数据库日志应有归档备份机制，可根据具体情况选择备份时间点进行数据恢复，满足灾难恢复要求。

13.5 IPV6 支持

根据《中国民生银行互联网应用系统支持IPv6协议规范》要求，我行应用程序接口应支持应用方采用IPv6进行接入。

14 实施保障

14.1 组织机构保障

14.1.1 业务牵头部门

业务牵头部门的具体职能包括：

a) 统筹管理全行开放银行（应用程序接口）业务，制定和组织实施业务发展规划；

b) 统筹应用程序接口服务标准制定，包括对外接口形式、数据及信息安全标准、报文格式规范、消费者权益保护等；

c) 统筹前台渠道、管理后台、安全工具等基础设施建设；

d) 牵头日常运营，包括平台运行监测、权限管理、安全评估、服务目录维护等；

e) 牵头平台服务协议的制定；

f) 协助经营机构开展业务合作对接；

g) 牵头开展全行业务培训、宣传推广工作。

14.1.2 产品管理部门

产品管理部门的具体职能包括：

a) 各自领域产品服务建设，包括风险与合规性分析、立项申请、需求编写、业务测试、服务上线、生产验证等工作；

b) 各自领域合作项目审批，制定各自产品和服务的合作准入条件、管理制度和产品服务协议及定价；

c) 各自领域产品的营销宣传和市场推广等工作，维护门户网站相关产品服务的对外展示信息；

d) 各自领域产品的服务运营维护，对客户及应用方提出的事件和工单进行处理答复。

14.1.3 信息科技部

信息科技部的具体职能包括：

a) 业务系统的技术架构、技术标准等技术规范的制定；

b) 业务系统的项目实施和生产运维支持工作，以及为应用方对接提供技术支持工作；

c) 系统安全运行，灾难备份，保障业务连续和应用系统安全性。

14.1.4 法律事务部

法律事务部的具体职能包括：

负责业务合法性审核，相关合同、协议等法律文本的审查，业务法律风险日常管理，及重大法律合规风险事件的处理。

14.1.5 运营管理部

运营管理部的具体职能包括：

负责资金清算、账务处理、网点柜台的操作流程制定与管理，受理客户业务的咨询、投诉和建议。

14.1.6 经营机构

经营机构的具体职能包括：

a) 业务推广，引入应用方，基于应用程序接口为应用方提供解决方案；

b) 与应用方签署产品管理部门要求的产品服务协议，对合作项目进行商务管理和运营维护；

c) 根据市场反馈挖掘业务需求和合作场景。

14.2 管理制度

14.2.1 产品研发类制度

a) 应规范研发项目的管理流程，以确保相关产品研发资源合理安排，提高研发效率，具体包括：产品创新制度、项目评审制度、项目管理制度，项目开发规范、设计规范、后评估机制等。

b) 应提供开发手册以指导应用方安全集成应用程序接口，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。

14.2.2 测试投产类制度

应制定测试投产类制度，以确保相关系统的项目安全、高效、顺利实施，具体包括：测试过程管理规范、测试质量管理规范、系统投产规范等。

14.2.3 生产运维类制度

应制定生产运维类制度，确保相关系统的生产安全与运维规范，具体包括：生产运维规范、配置规范、变更规范，以及系统、网络、机房、数据、安全等配套管理规定。

14.2.4 业务管理类制度

a) 应将应用程序接口的管理纳入现行业务管理体系中，对应用程序接口进行全生命周期的安全管理；

b) 应用程序接口应采用统一格式的识别码，并在相关平台上进行注册和登记；

c) 应建立信息公告制度，通过官方网站等公开渠道发布应用程序接口内容，并及时更新。

14.2.5 风险控制类制度

应制定风险控制类制度，制定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，以确保应用程序接口的一致性和连贯性，保障应用程序接口效率及安全性。

14.2.6 应急响应类制度

应制定应急响应类制度，以确保相关业务具备应急响应措施，妥善处理各类突发事件，保证业务的连续性，具体应包括：信息系统、反洗钱、流动性、消费者权益保护等突发事件应急预案、业务连续性应急预案、生产系统事件管理办法等。

14.3 企业标准宣传及实施机制

14.3.1 宣传与培训机制

应确定企业标准的管理部门，建立总行、事业部、分行的分层宣传与培训机制，确保层层传导。

全行各级机构应针对标准定期组织开展多层次的业务培训和文化建设活动，提升相关人员的专业知识和标准服务意识。

全行各级机构应认真学习企业标准，管理部门应对各部门进行业务培训，有条件的宜进行考试及认证工作，按要求落实企业标准要求。

应将企业标准上传公示至标准信息公共服务平台，并将企业标准纳入行内广告投放与宣传的计划范围内。

14.3.2 实施监督机制

全行各级机构应制定贯彻落实企业标准的工作机制，建立严格的实施监督制度，各级机构可将企业标准分解指标，纳入相关团队的考核。

全行各级机构应将对企业标准的执行情况定期上报，企业标准的管理部门应对各机构情况进行汇总和通报，对出现不符合标准的情况，应及时督导整改。

企业标准的管理部门应根据行内业务实际的发展情况，每年对标准进行维护和更新，并将最新版的标准进行公示和行内发布。

14.4 安全检测及安全评估保障

我行应主动地、定期地对应用程序接口系统进行安全检测与评估来保障应用程序接口可以更安全的为应用方服务，包括：

a) 网络层安全：信息系统网络架构设计是否安全合理、网络访问控制是否严格有效、网络安全审计是否有效、是否存在“非法外联”行为、网络入侵防范措施是否有效、恶意代码防范措施是否有效以及网络设备、安全设备配置是否安全、有效；

b) 主机系统安全：后台维护人员的权限是否是最小授权、安全审计记录是否完整、主机系统资源使用是否可控、是否能对主机系统用户设置恰当的身份鉴别手段、后台维护人员的逻辑访问路径是否可信等；

c) 应用程序接口系统安全：是否能对通过应用程序接口访问的用户设置恰当的身份鉴别手段、用户访问权限是否是最小授权、是否能保证交易的抗抵赖性、安全审计记录是否完整等；

d) 信息流分析：根据业务流程和正确数据流向，通过抓取数据包判断信息系统范围内是否有非法数据流和异常连接；

e) 日志分析：分析系统安全威胁来源，威胁源可能采用的攻击方式，对疑似黑客行为进行分析并提供相应的解决方法。

附 录 A
（规范性附录）
商业银行应用程序接口统一识别码编码规则

A.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。

A.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。

A.3 接口统一识别码编码

A.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 A.1。

表 A.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

A.3.2 固定位

固定位值固定为字母“0P”，表示商业银行应用程序接口。

A.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。

A.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、A3 安全级别。

[**注**：此处增加了 A3 级别]

A.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，备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 A.2。

表 A.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。

A.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。

A.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 22239—2019 网络安全等级保护基本要求
[2] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[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—2020 个人金融信息保护技术规范
[7] 中国民生银行互联网应用系统支持IPv6协议规范