ICS 35.240.40
A 11

Q/Bank of Qinhuangdao

秦皇岛银行股份有限公司企业标准

Q/Bank of Qinhuangdao 004—2023
代替 Q/Bank of Qinhuangdao 003-2022

开放银行应用程序接口安全管理规范

Open banking application programming interface secure management specification

企业标准信息公共服务平台
公开 2023年09月07日 10点10分

2023－09－07 发布　　2023－09－07 实施

秦皇岛银行股份有限公司　　发布

企业标准信息公共服务平台
公开 2023年09月07日 10点10分

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》的规则起草。

本文件由秦皇岛银行股份有限公司提出并归口。

本文件起草部门：信息科技部

本文件起草人：侯玮山、韩卫静、李建庆

本标准所代替标准的版本发布情况为：

—— Q/Bank of Qinhuangdao 003-2022。

企业标准信息公共服务平台
公开 2023年09月07日 10点10分

开放银行应用程序接口安全管理规范

1 范围

本文件规定了秦皇岛银行开放银行平台应具备的安全级别、安全设计、安全部署、安全集成、安全运维等相关要求。

本文件适用于秦皇岛银行对外提供服务的安全设计和应用，指导集成接口服务的应用方开展相关工作行。

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 17859-1999计算机信息系统安全等级保护划分准则

GB/T 18336 信息技术 安全技术 信息技术安全性评估准则

GB/T 22239-2019 信息技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

JR/T 0124-2014 金融机构编码规范

JR/T 0044-2008 银行业信息系统灾难恢复管理规范

JR/T 0071-2020 金融行业网络安全等级保护实施指引

JR/T 0171-2020 个人金融信息保护技术规范

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

下列术语和定义适用于本文件。

3.1

开放银行 open banking

开放银行是一组服务组件的集成，是指利用开放API技术（Application Programming Interface，即应用程序编程接口）实现银行与第三方机构之间的数据共享，从而提升客户体验的平台合作模式。

本文件是以秦皇岛银行各类资源为目的，通过API、SDK等服务和产品形态，对外提供可管控、可追踪的安全资源访问服务。

3.2

应用程序接口 application programming interface

一组开放预先定义好的功能，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。

3.3

网络安全 network security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.4

开发者 developer

开放银行的使用用户，即接口使用方，包括但不限于企业、商户、第三方合作伙伴，使用该平台对外发布的应用程序接口而进行的自身应用的开发。

3.5

OAuth 2.0协议 OAuth 2.0 Agreement

OAuth协议为用户资源的授权提供了一个安全的、开放而又简单的规范。

3.6

数字证书 digital certificate

用来标志和证明网络通信双方身份的数字信息文件,通常是经授权中心数字签名的包含公钥信息的文件。

4 缩略语

下列术语适用于本文件。

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

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

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）

SSL：安全套接层协议（Secure Sockets Layer）

MAC：消息鉴别码（Message Authentication Code）

5 概述

开放银行平台是秦皇岛银行将自身的服务通过应用程序接口对接的共享方式，提供给开发者（包括但不限于企业、商户及第三方合作伙伴）而搭建的应用平台。开发者可以使用API或者SDK等方式进行对接（逻辑构架见图1）。API和SDK接口规范遵循《商业银行应用程序接口安全管理规范》（JR/T 0185-2020）。开放银行平台重点实现对接过程中的基本功能，包含安全认证、流量控制、故障隔离、报文转换、服务组合等功能。

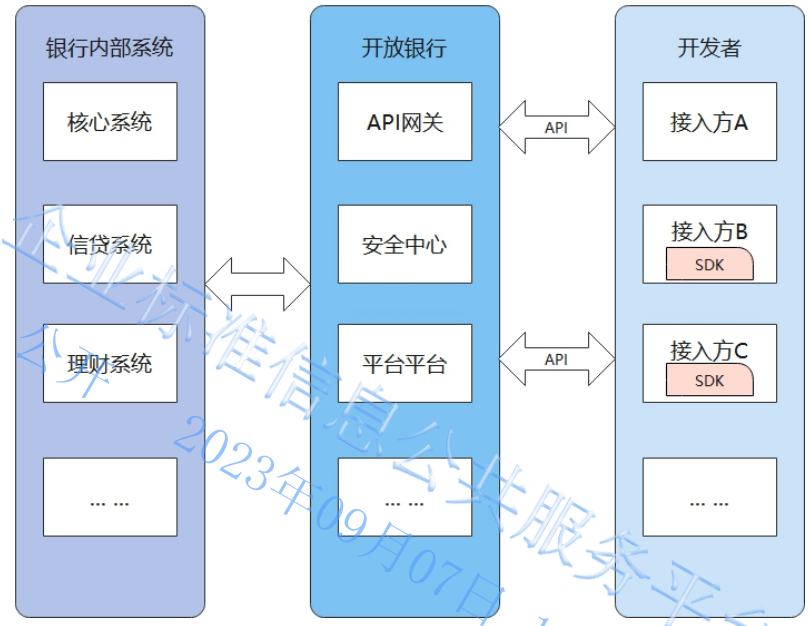

图 1　逻辑架构图

6　接口类型与安全级别

6.1　接口类型

接口类型分为金融交易和非金融交易。金融交易主要包括支付、转账、提现等动账类交易；非金融交易主要包括交易状态查询、产品信息查询等查询类交易。

按照应用集成方式，分为服务端对服务端集成方式、移动端对服务端集成方式、WEB端对服务端集成方式三种：

a）服务端对服务端集成方式

i. 应用方服务端直接调用开放银行平台开放接口，支持HTTPS、TCP协议，SOAP、REST多种风格类型；

ii. 应用方服务端集成开放银行平台提供的SDK包，其中SDK包包含了应用方部分身份信息，实现了信息传输过程中的报文加密加签、验密验签等算法封装，无需进行二次开发，极大的方便了应用方进行业务对接；

iii. 对于应用方使用PHP等语言实现的服务端，开放银行平台提供桥接方式及具体算法(服务端对接加密算法图解如图2)实现方式，应用方按照算法要求开发即可。

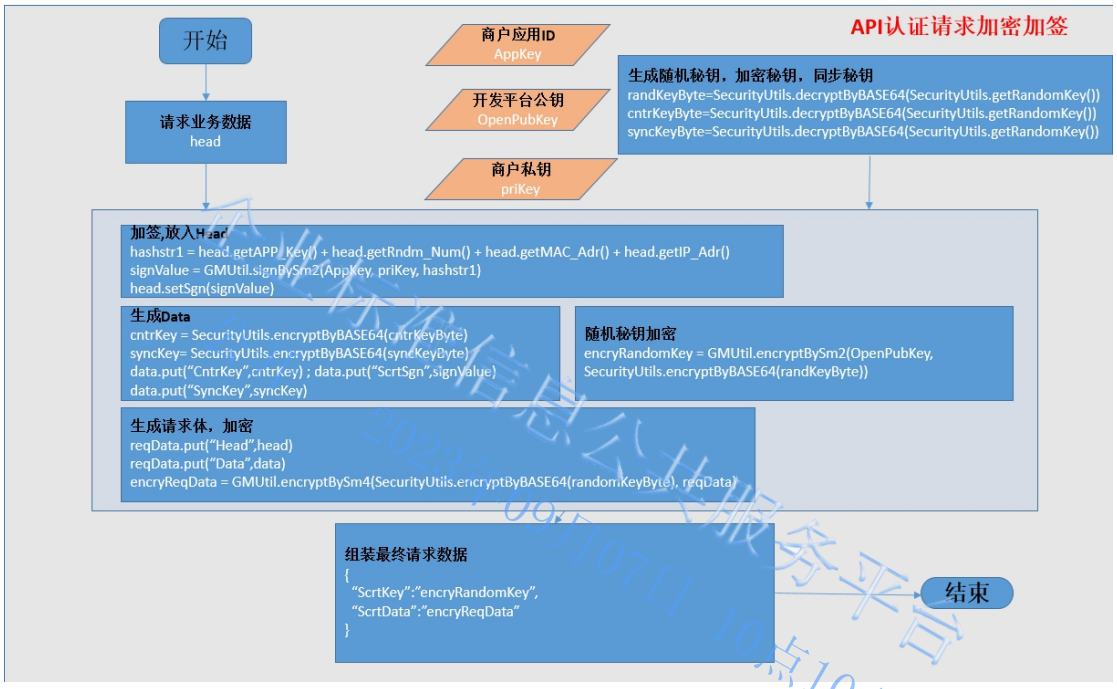

图 2　服务端对接加密算法图解

b）移动端对服务端集成方式

i．应用方移动端直接调用开放银行平台开放接口，此类接口只提供秦皇岛银行公开信息、服务等查询业务；

ii．应用方移动端集成H5 SDK包，H5 SDK包实现了信息传输过程中的加密加签、验密验签等算法封装（算法逻辑如图3），同时对业务进行组合封装，提供移动端用户的身份认证，实名认证等功能，并可以根据需要提供密码键盘，保障移动端用户进行密码输入过程的安全加密。

图 3　H5 SDK 算法逻辑

c）WEB端对服务端集成方式

WEB端分为WEB端H5直接访问和WEB服务端访问，其集成方式参考以上两种即可。

6.2 安全级别

安全级别分为A1、A2两类，非金融交易类接口为A1级安全标准，按照开放银行平台通用标准进行开放，金融交易类接口为A2级安全标准，实施高安全防护要求，安全防护要求从A2至A1递减：

A2：金融交易类接口，需实施高等级安全防护要求，对合作方资质及对接环境进行评估，此类接口服务包括：

a）资金交易类服务，如支付、转账、金融产品购买、充值等；

b）账户信息查询类服务，如账余额、账户交易详细信息、签约信息、金融产品持有情况信息等。

A1：金融产品和服务信息查询类接口，实施通用安全防护强度，此类接口服务包括秦皇岛银行金融产品和服务信息的“只读”查询服务。

7 安全设计

7.1 设计基本要求

开放银行平台及相关运行环境符合相关国家和行业基本安全要求。系统和网络等安全符合《计算机信息系统安全等级保护划分准则》（GB 17859-1999）、《信息安全 网络安全等级保护基本要求》（GB/T 22239-2019）、《金融行业网络安全等级保护实施指引》（JR/T 0071-2020）；密码算法应用及密钥管理实施符合国家密码管理部门有关要求。

7.2 网络安全

7.2.1 网络防火墙

采用双层网络防火墙进行保护，分别是互联网区和 DMZ 区设置一道防火墙，DMZ 区和应用区设置一道防火墙，设置防火墙网络安全策略，确保网络流量的合法性。

7.2.2 网络隔离区

使用DMZ网络隔离区，设立一个非安全系统与安全系统之间的缓冲区，有效保护内部网络区域的应用安全。

7.2.3 网络安全设备

借助SSL加速器和防火墙等网络安全设备实现SSL加速、应用攻击过滤以及拒绝服务(DDoS)攻击等安全防御功能。

7.2.4 转发代理

基于资源访问路径的负载路由，可以选择性的将内网应用的接口对外进行暴露。其他要求遵从《网络安全等级保护基本要求》（GB/T 22239-2019）。

7.3 通讯安全

对外通讯协议统一采用HTTPS协议，使用HTTPS链路加密的通讯模式，保证链路安全。HTTPS协议采用服务器证书（SSL证书），SSL证书按适用域名数量分类有：通配符型SSL证书、万能型SSL证书、单域名SSL证书、多域名SSL证书。

7.4 系统安全

系统安全应包括合作机构身份认证、互联网用户身份认证、权限控制、颁发认证令牌、令牌回收、超时重新登录等安全机制，在系统架构层面防护非法调用、暴力破解、信息劫持攻击行为，需经严格的代码审核，保证产品的安全性。

秦皇岛银行开放银行平台设有API网关及安全认证中心，应用采用Oauth2.0协议加token令牌认证，对于三方机构采用Oauth2.0授权码+令牌认证组合方式，保障了认证的安全及快捷，同时开放银行平台内部系统间提供Oauth2.0多层级别认证方式，保障系统间交互方便快捷；开放银行平台采用Spring Security安全框架进行权限控制管理，可以针对不同的用户设定不同的角色和权限，不同用户登录展示不同的菜单内容。开发者门户支持身份验证识别，采用密码加短信双重认证机制，对注册用户手机号、身份证等敏感信息进行加密脱敏操作，以防止信息在传输过程中泄露。对注册密码采用哈希算法加密，严格保护用户密码，防止泄露。用户登录内管平台30分钟内无操作，则系统强制用户退出，终端用户会话保持，当用户再次使用的时候，需要重新登录。最大限度的保证了应用系统的安全。

7.5 服务安全设计

7.5.1 授权管理

开放银行安全网关实行白名单访问控制 ：针对不同的合作方，按照“最小授权”原则建立API的访问控制，合作方仅能访问对其开放的API。

同时，合作方在接入秦皇岛银行开放银行平台时，应以法律合约的形式，声名和遵守接口使用相关条例：

a) 合作方应用声明公针对协议规定的方式和目的，合规调用接口；
b) 合作方应用应通过技术手段防止接口滥用；
c) 合作方应用声明不可访问未授权的银行信息，并通过技术手段限制；
d) 合作方应用声明最小化收集和使用个人信息，且符合《 信息安全技术 个人信息安全规范》(GB/T 35273-2020）相关要求。

7.5.2 攻击防护

开放银行安全网关模块对上送数据进行合规验证，包括App_ID与App_Secret与合作方信息是否一致，以及会话令牌（token）的有效性，防止非法访问。同时，平台支持服务熔断、故障隔离、流量控制等安全防护措施（见第9章节），保障系统的健壮性和稳定性。

7.5.3 接口安全监控

API 监控平台应对应用系统的资源、应用服务器、数据库服务器、系统运行、服务和产品运行、业务系统、开发者的第三方应用进行监控，并提供报表查询和下载。API 监控平台监控和提供的内容应包括：

a) API监控平台应提供系统资源运行情况；
b) API监控平台应提供服务运行监控功能情况；
c) API监控平台应提供各时段服务运行情况的统计报表；
d) API调用流水查询功能包括对所有API网关进行的交易流水进行查询，支持多种查询条件，如流水号、时间段、时间点、交易状态、交易返回码等；
e) 支持图形、邮件、短信的告警功能，并支持告警阈值的自定义设置。

7.5.4 算法及密钥管理

开放银行的接入需符合行业标准的信息安全与加密方案，优先支持国密算法SM2、SM3、SM4，同时支持MD5、RSA、HMAC_SHA1、AES等多种行业内可靠的算法。

a）国密算法加解密，提供基于国密算法的加密解密；

b）数字信封加解密，提供基于数字信封的加密解密；

c）SM2加签验签，提供基于SM2算法的加签验签；

d）数据脱敏，提供敏感数据的脱敏传输；

e）数据还原，提供敏感数据的脱敏还原。

8　安全部署

开放银行台功能整体上分为：开发者门户、安全中心、接入网关、接出网关、文件网关、服务治理、服务组合、安全管理、监控管理、参数运维，系统部署架构（部署架构图见图 4）。

为满足互联网开放平台系统对性能的需求，系统在架构设计上采用高性能、可伸缩的架构设计。执行效率高，有良好的资源管理机制。平台可以通过F5等硬件负载均衡设备或者Nginx软负载均衡应用，实现系统的横向扩展，解决系统的单点故障问题，平台的应用不存在任何的系统运行瓶颈，具备线性扩展的能力，可以根据企业内业务规模的发展随时增加系统的处理容量。平台内所有节点基于RESTFul的系统架构，所有服务都是无状态的，系统具备完全的线性横向扩展的能力。系统横向扩展架构能至少满足金融机构未来3-5年业务发展的需要。

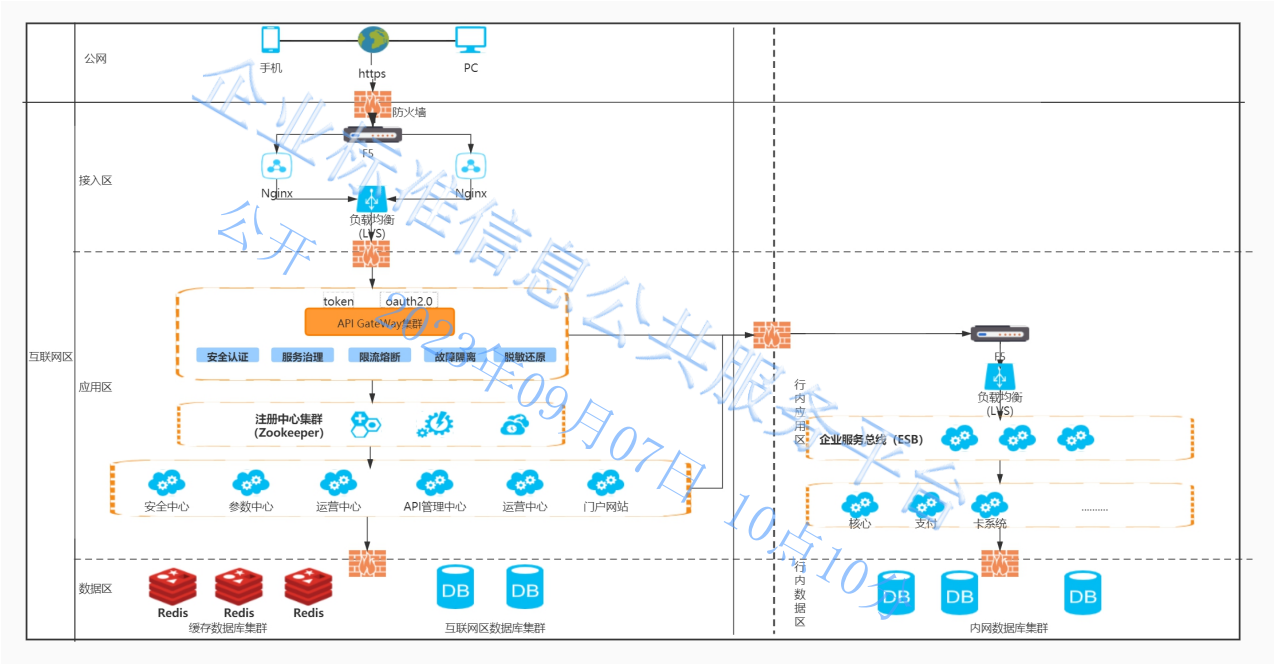

图 4　部署架构图

9　安全集成

9.1　应用方核准

9.1.1 应用方准入

合作方可通过开发者门户进行开发者注册，或向秦皇岛银行线下申请接入开放银行平台，提交企业基本信息资料（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），秦皇岛银行对合作提交的有效性、完整性、真实性审核通过后，为期分配App_ID和App_Secret，双方签订相关合作协议。

9.1.2 应用方身份核验

9.2 接入安全控制

9.2.1 身份认证

合作方进行开发者认证时，上送App_ID、App_Secret等关键参数，通过API网关调用安全中心的开发者认证接口，安全中心对上送的信息解密，验签，对App_Secret进行校验，校验用户是否可以用，再通过OAuth2.0返回Token给合作方（流程图见图5）。

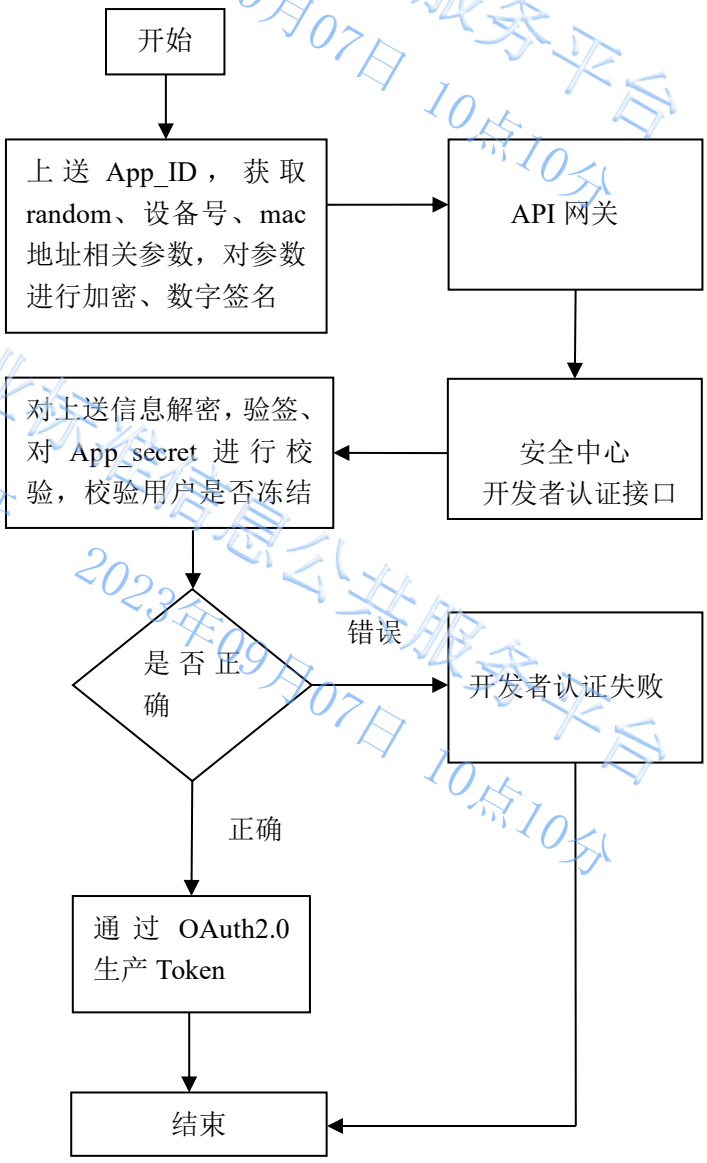

图5 流程图

9.2.2 安全传输

为保障开放银行平台与合作方之间的安全传输，所有接口采用全报文加密及加签防篡改的方式，根据合作方信息生成数字证书，在发起交易时进行合作方认证。加密方式同时支持国际加密与国密算法，采用安全度最高的对称及非对称算法SM2、SM3、SM4等组合方式、国际算法RSA、AES、3DES、SHA256等组合方式。

9.3 运行安全

9.3.1 授权和认证

互联网业务应支持集中管理授权和认证，如基于OAuth2.0的授权标准，采用Redis高速缓存存储授权认证信息，进行统一的授权管理和认证。交易在运行中，可以基于多个层面进行安全认证，其中一个环节认证失败，则整个交易失败。合作方在开发者门户上申请应用后，开发者门户会为该应用生成App_ID和App_Secret；合作方可以在门户上进行API的申请，后台会有相关的审核功能，审核通过后，该合作方底下的所有审核通过的应用对这些API均有访问权限，该权限检验是基于App_ID来完成,对于商户app_id和app_secret，互联网开放平台运营中心采用加密方式存储，保障商户信息安全。

9.3.2 故障隔离

故障隔离是当发生故障的时候，系统可以无损隔离，不影响其他交易正常处理；故障隔离应支持分路隔离、渠道隔离、服务隔离和系统隔离。

a）分路隔离是指系统在多路部署的情况下，当其中某一分路发生故障或者需要重启的时候，可以对该分路进行隔离，隔离不影响其他分路的交易；

b）渠道隔离是指可以对服务请求方进行隔离，一般隔离的维度是在APP维度将某一个接入的应用进行隔离；

c）服务隔离是在API维度，针对某一个服务接口进行隔离；

d）系统隔离是在服务提供系统维度，针对某一个服务提供系统进行隔离。

9.3.3 数据安全

接口数据安全部分，遵守《商业银行应用接口安全管理规范》（JR/T 0185-2020）9.3.3。

支持识别应用中涉及的敏感数据。敏感数据包括但不限于《信息安全技术 个人信息安全规范》（GB/T 35273-2020）规定的个人敏感数据、《个人金融信息保护技术规范》（JR/T 0171-2020）规定的C3/C2类数据、银行规定的敏感业务数据。相应敏感数据的传输、存储应符合《商业银行应用接口安全管理规范》（GB/T 35273-2020）、《个人金融信息保护技术规范》（JR/T 0171-2020）以及银行规定的机密性和完整性保护要求。

支持运营人员对不同用户访问的数据进行控制。当设置为不可见时，用户访问该数据时，应不显示。业务应用系统要支持数据访问权限控制，防止出现开发者跨权限访问业务数据。

9.3.4 脱敏还原

与第三方平台在进行数据交互的时候，涉及到企业内部用户隐私数据的请求，均采用数据脱敏和脱敏还原机制，保障用户的个人信息安全不被泄露；脱敏的数据有：手机号、身份证号码、银行卡号。

9.3.5 流量控制

流量控制是指在单位时间内对系统内正在处理的交易量做出控制,避免系统接收超出自身处理极限的交易请求，而造成系统严重负载，甚至奔溃、瘫痪等严重事故。

a）开放银行平台总流量控制；
b）开发者流量控制，指针对某一个开发者的接入的总并发数和调用频度进行控制；
c）服务流量控制，指针对某一个API接口接出调用的并发数和调用频度进行控制；
d）服务系统流量控制，指针对某一个服务提供系统接出调用的并发数和调用频度进行控制。

9.3.6 应用方安全能力

应用方安全能力需要满足以下要求：
a）应用方符合国家网络安全等级保护要求，保障应用运行环境安全、稳定；
b）应用方应具备一定的安全防护能力，使用安全框架，用户及接口具有权限控制功能；
c）应用方应遵守普遍的代码开发规范，web应用遵守互联网应用安全规范，具备反渗透能力。

9.3.7 应用方接口集成

应用方接口集成需要满足以下要求：
a）应用方应根据秦皇岛银行提供的API对接手册，正确合理使用API；
b）应用方应妥善保管相关密钥、证书、APPID、APPSECRET等数据，并遵守约定定期更换密钥证书；
c）应用方应使用行内提供SDK进行集成，切勿私自反编译、篡改或二次开发；
d）应用方不得恶意使用API，如发现API漏洞应及时与行方沟通，未经允许不得私自授予其他渠道进行使用。

9.3.8 应用方退出

应用方退出使用时需及时通知秦皇岛银行，并在开放银行官方网站申请API及应用下架，待审核通过后及时销毁行方提供的密钥证书及SDK集成包等相关资料，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 运维控制

依据《商业银行应用程序接口安全管理规范》(JR/T 0185-2020)标准进行运维监控，开放银行平台建设了专门的运维监控系统，具体监测内容如下：
a）监控开放银行接口相关服务器运行状态并建立告警机制，结合开放银行特点，有针对性的制定服务器cpu、内存、文件系统、磁盘io、网卡流量等性能指标，确定告警阈值，超过阈值进行告警；
b）应对数据库运行状态进行监测和报警；
c）应建立告警机制，按照告警事件等级进行分类，通过页面、短信、邮件、电话等方式进行通知；
d）应划出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
e）应对网络链路、网络设备、安全设备等运行情况进行集中监测；
f）应对开放银行接口服务状态、耗时、交易量、成功率等指标进行监测。

10.1.2 异常监控

开放银行平台具备流量监控、故障隔离、黑白名单等接口控制能力：
a）应具备流量控制能力，包括设置接口最大访问并发数，单位时间最大交易量，可以对异常流量进行监控，异常连接进行暂停、拒绝；
b）应具备故障监测和恢复能力；

c）应具备三方公司黑白名单控制能力；
d）RTO恢复时间在30分钟以内；
e）RPO响应时间在5分钟以内。

10.2 风险控制

10.2.1 服务风险控制

风险控制满足《商业银行应用程序接口安全管理规范》(JR/T 0185-2020)的要求。

10.2.2 交易流程控制

交易流程控制应满足以下要求：
a）涉及身份认证等授权类交易应充分告知客户，并确认是否由本人授权，必要时采用生物识别技术辅助验证；
b）涉及金融交易使用时，应充分提醒客户交易信息，并核实本人意愿；
c）涉及高风险金融交易时，应充分提示客户安全风险；
d）当客户端应用环境发生变化时，应重新对客户身份进行核实，必要时采用生物识别技术辅助验证。

10.3 变更控制

依据《秦皇岛银行信息科技生产变更管理办法》进行变更控制，变更前充分评估影响范围及风险，实行先申请再变更的管理要求；变更过程中详细记录操作时间，双人进行复核；变更后及时进行验证并总结经验，持续改进。

涉及对外接口服务发生变化的，及时通知相关合用方影响范围，并制定变更方案和应急预案。

10.4 运维巡检

运维巡检按照《商业银行应用程序接口安全管理规范》(JR/T 0185-2020)要求进行，包括：
a）定期对应用服务器进行漏洞扫描，及时进行修复；
b）定期或重大版本变更前，对源代码进行安全审计；
c）定期开展渗透性测试，及时处置安全漏洞，防控安全风险；
d）定期开展配置项检查；
e）定期对合作方接入使用情况进行分析，对存在非法使用接口的使用，责令其整改或下线接口。

10.5 事件处理

运维巡检按照《商业银行应用程序接口安全管理规范》(JR/T 0185-2020)以及《信息科技生产事件管理办法》要求进行，包括：
a）中心机房实行7X24值班制度，发现问题后根据事件响应要求，及时上报处置；
b）制定开放银行应急处置预案；
c）制定开放银行日常维护手册。

11 服务终止与系统下线

根据《秦皇岛银行项目管理办法》，已经达到生命期限的应用可申请下线处置。

涉及开放银行平台相关服务终止或下线的，提前通知相关方，并向相关方提交服务下线方案，双方签订补充协议，就数据归档、数据销毁、客户信息保护、资金安全等问题达成一致，并充分履行用户告知义务。

12 安全管理

12.1 管理制度

开放银行平台安全管理制度纳入秦皇岛银行现行管理体系，按照《秦皇岛银行项目管理办法》管理其生命周期。

12.2 应用安全责任

秦皇岛银行与合作方签订接入协议，明确规定双方责任与义务，包括：

a）接口使用的相关要求；

b）客户隐私保护的相关要求；

c）数据保护的相关要求；

d）双方架构安全的相关要求。

12.3 安全审计

按照《商业银行应用程序接口安全管理规范》(JR/T 0185-2020)实施安全审计，保证系统安全：

a) 保留交易日志流水，并具备与合作方日志流水进行核对的功能；

b) 安全策略，密码应定期更换，密码应具备一定强度、账号权限应符合最小授权要求等方式，建立安全策略；

c) 日志审计，应采集、分析系统日志，包括操作系统、数据库等的操作日志进行日志审计，并对日志进行保护，确保日志不被篡改、删除、覆盖；

d) 审计记录包括交易发起日期、时间、渠道类型等关键数据项，对敏感信息不进行存储。

附 录 A
（规范性附录）
秦皇岛银行开放银行平台接口安全标准

秦皇岛银行安全加密机制支持国密和国际通用算法，以下是国密安全控制流程：

A.1 初始化认证

a）商户服务端生成随机秘钥并生成两个工作随机数（加密随机数，同步随机数），使用SM2对拼接后的字符串进行哈希值计算并使用私钥B对哈希值进行加签，使用随机秘钥对数据进行SM4加密生成ScrtData，使用公钥S对随机密钥1进行SM2加密生成ScrtKey。

b）将生成的数据发送至OpneAPI，OpenAPI接收到数据后先使用平台私钥（私钥S）进行解密，解密后获取到随机密钥2，在使用随机密钥2对ScrtData进行解密，解密后得到业务参数，根据一定规则拼接业务数据使用商户公钥（私钥B）进行验签。

c）OpenAPI将验证开发者请求发送至开放平台安全认证中心（Oauth），Oauth对请求的数据进行验证，验证appkey，应用状态。验证成功后生成Token对象（包含随机工作密钥，随机同步密钥）并存在高速缓存Redis中，默认有效期为1小时，并将token返回至OpenAPI。

d）OpenAPI接受到返回数据对返回数据进行SM4加密加签后返回至商户服务端。

e）客户端将返回数据后，通过请求保存的随机秘钥进行SM4解密，获取到解析后的密文之后，再通过随机秘钥进行验签，验证成功后获取到Token，在后续交易中均要使用该Token，进行业务交易。

A.2 业务交易

a）客户端拼装业务数据，使用国密对业务数据进行哈希计算，用商家APPKEY和公钥对计算的哈希值进行国密SM2加密加签生成ScrtSgn，使用随机密钥1（每次交易均重新生成）对业务数据进行国密SM4加密生成ScrtData，然后使用开放平台公钥对数据随机密钥1进行国密SM2加密生成ScrtKey。并将加密后数据发送至OpenAPI

b）OpenAPI收到数据后获取Redis中的Token对象（包含随机工作密钥，随机同步密钥），通过开放平台私钥对随机秘钥解密，通过随机密钥使用国密SM4对数据进行解密，解密后通过商家公钥对SM2进行验签，验签成功后获取Token，验证Token是否正确以及有效。并验证该应用使用接口是否可用，验证通过后将数据发送提供方系统

c）OpenAPI对返回数据也进行加密，加密后返回至客户端，客户端对数据进行解密。通过随机密钥对密文进行国密SM4解密。获取返回的密文签名值，通过国密SM4和随机密钥进行解密，之后再通过商家公钥，进行国密SM2解密验签。

附 录 B
（资料性附录）
秦皇岛银行开放银行平台 JAVA-SDK 开发者使用手册

B.1 SDK介绍

SDK是为调用方简化API开放平台调用专门提供的开发工具包，通过提供银行通用接入算法的封装、发起服务调用、返回结果解析等功能，达到降低应用方接入开发难度。本文档所述基于SDK的Java版本实现。

SDK开发运行环境：JDK1.8及以上。

每个已注册的应用会自动分配一个应用唯一标识 APP_KEY和一个开放平台的密钥公钥PrivateKey,调用方利用开放银行管理平台(以下简称为开放平台)提供的SDK(OpenSDK.generateKeyPair)生成公私钥对，并将公钥提供给开放平台。开放平台维护应用ID与公钥的对应关系。

SDK的工作原理简介：

a) 开发者认证阶段，SDK生成随机数，并采集运行环境中的MAC和IP地址，和应用ID一起组成字符串取哈希值后，开发者用自己的私钥对其加签，当认证报文发送到开放平台的API接入网关后，开放平台使用开发者的公钥对签值进行验签，通过后发放访问令牌。收到返回报文后，SDK使用开放平台的公钥对返回报文的签值进行验签，当双方互信后，SDK端才能从返回报文中获取到访问令牌。

b) SDK端获取到访问令牌后，就可以通过SDK提供的API服务调用方法使用银行对外输出的金融服务了。API接入网关会对每次API服务调用请求进行API调用权限、流量控制等检查和按照合约对API服务的使用流量进行计量计费。

c) SDK和API接入网关的每次报文交互都采用一次一密的加解密机制。请求信息的组装、签名、加密及响应信息的验签、解析、解密对调用方透明。

B.2 环境说明

a) SDK开发运行环境：JDK1.8及以上；

b) Java基础SDK及相应的产品SDK只支持UTF-8编码。

B.3 配置工程

下载 SDK 后，在工程中直接引用，并引用 lib 文件夹下的所有 jar 包。

qhdbank-SDK-x.x.x.jar 为必需集成 jar。

其他依赖 jar，需要一起加入到项目中。如果项目中已存在相同 jar 包可不替换；如版本不一致，请在不影响原系统使用的情况下更换成上述版本的 jar 包。如有冲突请联系秦皇岛银行的开放银行平台项目组。

B.4 快速开发

a) 报文编码及开发示例

开放平台的通信报文默认支持 UTF-8 编码方式(特殊约定的除外)。通过 Java 基础 SDK 发送交易主要需要两步：

第一步：使用 OPENSDK.init()方法 SDK 初始化；

第二步：使用 OPENSDK.send()方法发送交易。

b) SDK配置文件

应用方需按照要求填写 SDK 中配置信息，config.properties 可以是绝对路径，也可以是项目的相对路径。

B.5 API 服务返回信息

开放平台的返回信息和 API 服务归属后台系统的返回信息都是通过响应报文中返回#交易响应代码描

述 Txn_Rsp_Cd_Dsc 和#交易响应信息 Txn_Rsp_Inf 字段传递回来的。双方所用的编码规则不同。如果交易响应代码是以开放平台返回信息编码规则编码的，表示开放平台交易不成功；如果交易响应代码是以 API 服务归属后台系统返回信息编码规则编码的，表示报文在 API 服务归属后台系统的实际处理状态是否成功。

企业标准信息公共服务平台
公开 2023年09月07日 10点10分