ICS 35.240.40
A11

团　　体　　标　　准

T/PCAC 0008-2020

商业银行应用程序接口安全管理检测规范

Testing specification on commercialbank application programming interface secure management

2020－11－20 发布　　2020－11－20 实施

中国支付清算协会　发布

目　　录

前　言

本规范由中国支付清算协会提出。

本规范由中国支付清算协会安全与技术标准专业委员会归口。

本规范主要起草单位：中国支付清算协会、中国工商银行股份有限公司、中国农业银行股份有限公司、中国建设银行股份有限公司、招商银行股份有限公司、中信银行股份有限公司、民生银行股份有限公司、北京银行股份有限公司、山东省农村信用社联合社、浙江网商银行股份有限公司、中国银联股份有限公司、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、北京软件产品质量检测检验中心、国信在线（北京）经济文化发展中心、上海云从企业发展有限公司、航天中认软件测评科技（北京）有限责任公司等单位。

本规范主要起草人：陈波、马国光、刑桂伟、于沛、何一江、陈旭东、薛宇、相海飞、姜城、卓越、孙勇、杨文涛、苏晨、赵海龙、李明捷、贾海明、朱文义、穆庆新、虞刚、李晓东、宗勇涛、张奔、刘亚军、杨荣明、宋铮、左敏、蒋慧科、尹祥龙、刘力慷、张健、渠韶光、侯晓晨、张勇、王飞宇、高峰、张鹏、于泉、吴冬宇、朱震宇、许劭华、李军、孙明慧、石跃超等。

本规范为首次发布。

商业银行应用程序接口安全管理检测规范

1　范围

本规范规定了商业银行应用程序接口在安全设计、安全部署、安全集成、安全运维、服务终止与系统下线、安全管理等方面的检测要求。

适用于开展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。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　商业银行安全设计检测

3.1　基本要求

检测目的：验证商业银行应用程序接口及接口服务层的安全设计是否满足基本要求。

检测方法：

1) 检查商业银行应用程序接口及接口服务层使用的密码算法和密码算法的用途、使用范围、实现方式（软件、硬件或固件）是否安全有效；检查使用的密码算法和技术是否符合国家密码管理部门和行业主管部门发布的国家标准或行业标准；检查使用的密码产品是否获得具备资质（国家密码管理部门和行业主管部门授权）的商用密码认证机构颁发的商用密码产品认证证书；
2) 检查商业银行是否制定了安全编码规范；
3) 检查商业银行是否就安全编码规范对开发人员进行培训并核查培训记录；访谈开发人员对安全编码规范执行情况，查看应用程序接口源代码是否依据安全编码规范进行开发；
4) 检查商业银行应用程序接口开发中使用的第三方应用组件，是否进行安全性验证并形成验证结论；核查商业银行是否持续关注第三方应用组件发布平台的信息披露和更新情况，适时更新相关组件并形成更新记录；
5) 检查商业银行针对应用程序接口代码安全专项审计的工作方式；查看已有应用程序接口的代码安全专项审计报告，并核查报告中所披露的脆弱点是否得到妥善处置；
6) 检查商业银行是否制定源代码和应用程序接口版本管理与控制规程，查看规程中是否包含源代码和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相关内容；核查源代码和应用程序接口版本管理是否符合规程要求，是否具有变更记录和说明；
7) 检查商业银行向应用方提供的异常与调试信息是否泄漏服务器、中间件、数据库等软硬件信息或内部网络信息。

通过标准：

1) 商业银行应用程序接口及接口服务层使用的密码算法和密码算法的用途、使用范围、实现方式（软件、硬件或固件）安全有效；使用的密码算法和技术符合国家密码管理部门和行业主管部门发布的国家标准或行业标准；使用的密码产品获得具备资质（国家密码管理部门和行业主管部门授权）的商用密码认证机构颁发的商用密码产品认证证书；
2) 商业银行具有安全编码规范；
3) 商业银行定期对开发人员进行安全编码培训并保留培训记录；开发人员按照编码规范要求开发且代码符合安全编码规范要求；
4) 商业银行对已使用第三方应用组件的安全性进行验证并形成安全验证记录，记录内容包括但不限于对象、方法和结论；具有持续关注第三方应用组件发布平台的信息披露和更新情况的机制，并适时更新相关组件，具有更新记录；
5) 商业银行对应用程序接口开展代码安全审计，具有代码安全审计报告，报告中所披露的脆弱点已妥善处置；
6) 商业银行具有源代码和应用程序接口版本管理与控制规程，规程中明确源代码和和应用程序接口版本管理措施，接口废止、变更等情况与应用方保持信息同步相关内容；源代码和应用程序接口版本管理符合规程要求，具有变更记录和说明；
7) 商业银行向应用方提供的异常与调试信息，未泄露服务器、中间件、数据库等软硬件信息或内部网络信息。

3.2 接口安全设计

3.2.1 接口身份认证安全

检测目的：验证商业银行应用程序接口及接口服务层对应用方身份认证是否满足要求。

检测方法：

1) 检查应用程序接口对应用方身份认证使用的验证要素是否满足如下方案：
    a) App_ID、App_Secret；
    b) App_ID、数字证书；
    c) App_ID、公私钥对；
    d) 上述 3 种方案的组合。
2) 检查 A2 级接口应用方身份认证时，是否使用包含数字证书或公私钥对的方式进行双向身份认证，使用的数字证书及密码算法符合国家密码主管部门要求。

通过标准：

1) 商业银行应用程序接口对应用方身份认证使用的验证要素为以下任意一种或多种组合：
    a) App_ID、App_Secret；
    b) App_ID、数字证书；
    c) App_ID、公私钥对。
2) 商业银行 A2 级应用程序接口应使用包含数字证书或公私钥对的方式对应用方进行双向身份认证，使用的数字证书及密码算法符合国家密码主管部门要求。

3.2.2 用户认证安全

检测目的：验证商业银行应用程序接口及接口服务层的用户身份认证是否满足要求。

检测方法：

1) 检查商业银行是否结合金融服务场景，对不同安全级别的应用程序接口设计不同级别的用户身份认证机制，并检查不同级别的用户身份认证机制的有效性和安全性；
2) 检查用户身份认证安全设计和实现方式，认证是否在商业银行执行，核查 A2 级别接口中资金交易类服务的用户身份认证方式，是否满足至少使用双因子认证的方式。

通过标准：

1) 商业银行依据规范要求将应用程序接口分为 A1 和 A2 等级，不同级别的应用程序接口设计不同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。

3.2.3 接口交互安全（连通性）

检测目的：验证商业银行应用程序接口及接口服务层的连通有效性是否满足要求。

检测方法：

1) 检查商业银行应用程序接口交互安全设计是否包含连通有效性的验证机制，核查连通有效性验证是否与设计方案一致，如接口版本、参数格式等要素是否与平台设计保持一致。

通过标准：

2) 商业银行应用程序接口及平台设计具有连通有效性验证机制，且实现和设计保持一致。

3.2.4 接口交互安全（数据完整性）

检测目的：验证商业银行应用程序接口及接口服务层的数据完整性是否满足要求。

检测方法：

1) 检查商业银行应用程序接口交互数据的完整性保护机制及实现方式，核查是否安全有效；
2) 检查商业银行 A2 级别的接口是否使用数字签名来保证数据的完整性和不可抵赖性，使用的密码算法是否符合国家密码主管部门要求。

通过标准：

1） 商业银行应用程序接口具有对交互数据的完整性保护机制，且安全有效；
2） 商业银行 A2 级别的应用程序接口，使用数字签名保证数据的完整性和不可抵赖性，密码算法符合国家密码主管部门要求。

3.2.5 接口交互安全（个人金融信息保护）

检测目的：验证商业银行应用程序接口及接口服务层的个人金融信息保护是否满足要求。

检测方法：

1) 检查商业银行应用程序接口相关设计方案是否包含对数据交互过程中支付敏感信息（如登录口令、支付密码等）的安全防护措施，包括但不限于替换输入框原文、自定义软键盘、防键盘窃听、防截屏等措施，通过应用监听、报文分析等方式核查防护措施的安全性和有效性，无法获取支付敏感信息明文；
2) 检查商业银行应用程序接口相关设计方案对个人金融信息（如账号、卡号、卡有效期、姓名、证件号码、手机号码等）在传输过程中的加密机制，包括但不限于使用集成在 SDK 中的加密组件进行加密及对相关报文进行整体加密处理等机制；核查商业银行向应用方反馈账户、卡号和姓名时是否使用了脱敏或者去标识化处理；核查应用接口程序是否包含清分与清算、差错对账等接口，传输卡号等支付账号至应用方时是否使用加密通道，是否具有信息完整性保护措施；
3) 检查商业银行 A2 类只读信息查询（金融产品持有份额、用户积分等）的连接方式，核查使用 API 直接连接方式进行查询 A2 类只读信息查询的对接请求是否使用防护措施（如加密）保证查询信息的完整性与保密性。

通过标准：

1) 商业银行应用程序接口相关设计方案具有对数据交互过程中支付敏感信息（如登录口令、支付密码等）的安全防护措施，包括但不限于替换输入框原文、自定义软键盘、防键盘

窃听、防截屏等措施，措施安全和有效，无法获取支付敏感信息明文；

2) 商业银行应用程序接口相关设计方案具有对个人金融信息（如账号、卡号、卡有效期、姓名、证件号码、手机号码等）在传输过程中的加密机制，包括但不限于使用集成在SDK 中的加密组件进行加密及对相关报文进行整体加密处理等机制，安全有效；商业银行向应用方反馈账户、卡号和姓名时具有脱敏或者去标识化处理；商业银行应用接口程序处理清分与清算、差错对账传输卡号等支付账号至应用方时使用加密通道，具有信息完整性保护措施；

3) 商业银行使用 API 直接连接方式的 A2 类只读信息查询（金融产品持有份额、用户积分等）具有防护措施（如加密）保护信息的完整性与保密性。

3.3 服务安全设计

3.3.1 授权管理

检测目的：验证商业银行应用程序接口服务层是否对接口的权限进行授权管理。

检测方法：

1) 检查商业银行是否具有根据不同应用方的服务需求对相应接口权限进行授权管理机制和最小授权原则，检查接口权限的授权管理和最小授权是否落实执行；服务需求变更时，是否对涉及接口权限变更的需求进行评估，是否具有评估记录和接口权限调整记录。

通过标准：

2) 商业银行具有根据不同应用方的服务需求对相应接口权限进行授权管理机制和最小授权原则且有效落实；涉及接口权限变更的服务需求进行评估，具有评估记录和接口权限调整记录。

3.3.2 攻击防护

检测目的：验证商业银行应用程序接口服务是否具有攻击防护能力。

检测方法：

1) 查看商业银行服务安全设计是否具备攻击防护能力，具有哪些攻击防护能力。

2) 检查商业银行 API 和 SDK 设计方案是否具有对常见网络攻击的安全防护能力；API 和 SDK 是否具有对常见的网络攻击的安全测试报告，测试发现的脆弱性已修复。

3) 检查商业银行动终端应用 SDK 是否具有静态逆向分析防护能力，相关的安全测试是否包含静态逆向分析攻击测试，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测试验证是否能获得有关 SDK 实现方式的技术细节。

4) 检测商业银行移动终端应用 SDK 是否具有动态调试防护能力，如未实现记录结论作为建议；如实现查看相关的安全测试是否包含动态调试攻击测试，否则通过挂接动态调试器、动态跟踪程序的方式测试验证是否能控制程序行为，通过篡改文件、动态修改内存代码等方式测试验证是否能控制程序行为，如防护措施存在问题同样作为建议项。

通过标准：

1） 商业银行服务安全设计具备攻击防护能力。

2） 商业银行 API 和 SDK 设计具有对防 SQL/可执行脚本注入、防越权访问、防报文重放等常见网络攻击的安全防护能力；具有 API 和 SDK 对常见的网络攻击的安全测试报告，测试发现的脆弱性已修复。

3） 商业银行移动终端应用 SDK 应具有静态逆向分析防护能力，相关的安全测试包含静态逆向分析攻击测试，通过静态反汇编、字符串分析、导入导出函数识别、配置文件分析等无法获得有关 SDK 实现方式的技术细节。

4） 商业银行移动终端应用 SDK 宜具备动态调试防护能力。

3.3.3 安全监控

检测目的：验证商业银行应用程序接口服务层日志是否满足安全监控要求。

检测方法：

1) 检查商业银行是否对接口使用情况进行监控且有效运行，查看接口访问日志记录是否完整；
2) 查看相关日志是否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）等信息。

通过标准：

1) 商业银行相关日志情况监控措施且有效运行，接口访问日志记录完整；
2) 商业银行相关日志中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）等信息。

3.3.4 密钥管理

检测目的：验证商业银行的密钥管理和本地配置文件是否符合要求。

检测方法：

1) 检查商业银行应用程序接口加密和签名相关的设计文档和代码，是否使用了不同的密钥，且相互分离；
2) 检查商业银行应用程序接口相关代码是否包含私钥明文（或密文）；查看商业银行本地配置文件，是否存储了 App_Secret 或私钥；
3) 检查商业银行是否具有对不同等级的应用程序接口设置不同的密钥有效期，是否具有更新机制，是否具备安全控制措施以防范密钥泄露，查看密钥管理系统并访谈密钥管理人员，核查是否按设计要求有效执行。

通过标准：

1) 商业银行应用程序接口加密和签名宜分配不同的密钥，且相互分离；
2) 商业银行应用程序接口相关代码未包含私钥明文（或密文），相关本地配置文件未存储 App_Secret 或私钥；
3) 商业银行应依据应用程序接口等级设置不同的密钥有效期，并具有密钥到期更新机制，同时应具备安全控制措施防范密钥泄露。密钥管理人员应按要求执行密钥更新。

4 商业银行安全部署检测

4.1 接口服务层部署要求

检测目的：验证商业银行是否遵循 JR/T 0185—2020 中商业银行应用程序接口网络部署逻辑结构示意图，进行商业银行应用程序接口的安全部署。

检测方法：

1) 检查商业银行是否在互联网边界部署了具备访问控制、入侵防范相关安全防护能力的网络安全防护措施，如：防火墙、IDS/IPS、DDoS 防护等，同时检查安全防护措施是否配置了有效的防护规则；
2) 检查商业银行应用程序接口服务层是否部署流量控制、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；
3) 检查商业银行应用程序接口服务层与银行业务层之间是否部署具备相关访问控制、入侵防范安全防护能力的网络安全防护措施，如防火墙等；
4) 检查商业银行的安全控制要求是否依据JR/T 0071部署相应级别的安全控制措施。

通过标准：

1) 商业银行在互联网边界部署了具备访问控制、入侵防范相关安全防护能力的网络安全防护措施，并配置了有效的防护规则。
2) 商业银行应用程序接口服务层部署了流量控制、监控分析等服务，商业银行应用程序接口服务层或银行业务层部署了认证鉴权、报文交换、服务组合等服务。
3) 商业银行应用程序接口服务层与银行业务层之间部署了具备相关访问控制、入侵防范安全防护能力的网络安全防护措施。
4) 商业银行的安全控制要求是依据JR/T 0071部署相应级别的安全控制措施。

5 商业银行安全集成检测

5.1 应用方核准

5.1.1 应用方准入要求

检测目的：验证商业银行是否建立应用方准入制度。

检测方法：

1) 访谈相关人员，确认商业银行是否对应用方进行了准入审核，审核内容是否包含服务客群、服务场景、市场份额、运营能力、风控能力等方面，并查看相关审核材料是否与访谈内容一致，审核项是否包含服务客群、服务场景、市场份额、运营能力、风控能力等内容；
2) 访谈相关人员，确认商业银行是否对申请接入的应用方的技术能力和管理水平进行了评估，核查对应的评估报告、结果记录等材料，确认评估指标中是否将应用方对用户信息保护能力作为重要评价指标；
3) 访谈相关人员，了解商业银行是否有在必要时对应用方的安全保护能力和管理水平进行技术评估的措施，核查对应的评估报告、结果记录等材料，确认评估范围是否包含应用方信息安全建设水平；
4) 访谈相关人员，了解商业银行是否制定了商业银行应用程序接口合作协议，查看并确认合作协议，确认协议内容是否包含合作业务场景、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约定条款；
5) 访谈相关人员，并可结合应用程序接口源代码审查、网络流量分析等方式，了解应用程序接口是否开启了跨机构清算业务。

通过标准：

1) 商业银行对应用方进行了准入审核，包括但不限于对服务客群、服务场景、市场份额、运营能力、风控能力等方面进行了考察；
2) 商业银行在应用方申请接入时应对应用方的技术能力和管理水平进行了评估，应用方对用户信息保护能力作为重要的评价指标；
3) 在必要情况下，商业银行应对应用方的安全保护能力和管理水平进行了技术评估，评估范围包含应用方信息安全建设水平；
4) 商业银行制定了应用程序接口合作协议，并与应用方签署了应用程序接口合作协议，协议内容包含合作业务场景、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约定条款；
5) 商业银行未通过开放应用程序接口的方式变相开展跨机构清算业务的情况。

5.1.2 应用方身份核验

检测目的：验证商业银行是否在应用方接入与审批阶段对其身份进行核验和管理。
检测方法：
1） 访谈相关人员，检查相关核验和管理材料，确认商业银行是否在应用方接入与审批阶段对其进行了身份核验和管理。
通过标准：
1） 商业银行在应用方接入与审批阶段，应通过线上或线下手段，对应用方提交资料的有效性、完整性、真实性进行了审核，对应用方身份进行了合规性核验。

5.2 接入安全控制

5.2.1 身份认证

检测目的：验证商业银行应用程序接口及接口服务层的身份认证是否满足要求。
检测方法：
1) 检查商业银行是否提供应用方身份声明机制：
   a） 检查商业银行是否为准入审核通过的应用方配置唯一标识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。对于采用公私钥对认证的情况，检查商业银行是否对应用方上传的公钥进行登记。
   b） 检查商业银行是否对应用唯一标识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。
2) 检查商业银行是否对应用方进行身份认证：
   a） 检查商业银行是否在应用方请求其应用程序接口时对应用方的身份进行认证，认证方式是否为以下四种之一：
   ——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 和数字证书对应用方身份进行认证；
   ——基于应用唯一标识 App_ID和公私钥对方式对应用方身份进行认证；
   ——基于应用唯一标识 App_ID 和应用鉴别密文 App_Secret、数字证书（或公私钥对）的组合，对应用方身份进行认证。
   c） 对于 A2 类，检查应用方身份认证是否使用 a）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。
   d） 检查商业银行是否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）。
   e） 检查商业银行是否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，具备主动处理恶意连接的能力。
通过标准：
1） 应用方身份声明：
   a） 应用方准入审核通过后，商业银行应配置唯一标识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与数字整数（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了登记。
   b） 商业银行应对应用唯一标识App_ID进行了存储与统一管理，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。
2） 应用方身份认证为：

a) 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，认证方式为以下任意一种：
——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 和数字证书对应用方身份进行认证；
——基于应用唯一标识 App_ID 和公私钥对方式对应用方身份进行认证；
——基于应用唯一标识 App_ID 和应用鉴别密文 App_Secret、数字证书（或公私钥对）的组合，对应用方身份进行认证。
b) 对于 A2 类，应用方身份认证应使用 a）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。
c) 商业行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。
d) 商业银行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，具备主动处理恶意连接的能力。

5.2.2 安全传输

检测目的：验证商业银行与应用方之间的网络安全传输是否符合安全要求。
检测方法：
1) 检查对于A1类，是否采用 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；
2) 检查对于A2类，是否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；
3) 检查业银行与应用方之间数据传输是否采用 SSL/TLS 等安全通道连接进行通信及使用的 SSL/TLS 版本。
通过标准：
1) 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，必要时可采用数字签名技术；
2) 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；
3) 应采用 SSL/TLS 等安全通道连接进行安全通信，宜使用 TLS1.2 及以上版本。

5.3 运行安全

5.3.1 用户身份认证

检测目的：验证商业银行对用户身份的认证是否满足安全要求。
检测方法：
1) 检查用户身份认证是否在商业银行完成，若用户个人金融信息或支付敏感信息需在应用方输入，应评估该实现方式的合理性和安全性，确认是否必须在应用方输入；
2) 访谈相关人员，并检查商业银行是否对应用方上送的用户相关信息进行核验；
3) 检查商业银行是否结合具体场景，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，是否结束会话。
通过标准：
1) 用户身份认证应在商业银行完成，经评估确需在应用方输入时，用户个人金融信息或支付敏感信息方可在应用方输入；
2) 商业银行应对应用方上送的用户相关信息进行核验；

3） 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。

5.3.2 权限控制

检测目的：验证商业银行是否对接口权限进行有效控制。

检测方法：

1） 检查商业银行是否按应用方、应用唯一标识App_lD、接口、用户等维度，依据最小授权原则进行授权，对于未授权的资源是否禁止访问；

2） 检查商业银行是否对API的调用有效期进行控制；

3） 检查商业银行是否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。

通过标准：

1） 商业银行应按应用方、应用唯一标识App_lD、接口、用户等维度，依据最小授权原则进行授权，对于未授权的资源应禁止访问；

2） 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）；

3） 商业银行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。

5.4 应用方退出

检测目的：验证商业银行是否建立应用方退出管理制度。

检测方法：

1） 访谈相关人员，确认商业银行是否制定了应用方退出机制；核查退出机制，评估退出机制是否能够保障用户账户、资金、信息安全；

2） 检查退出机制，确认是否明确在应用方退出后，对APP_Secret、公私钥对等认证信息进行了作废处理，归档并保存待查。

通过标准：

1） 商业银行制定了有序、可行的应用方退出机制，退出机制能够保障用户账户、资金、信息安全，履行用户告知的义务；

2） 应用方退出机制明确在应用方退出后，商业银行对APP_Secret、公私钥对等认证信息进行作废处理，并对作废的APP_Secret、公私钥对等认证信息进行归档。

6 商业银行安全运维检测

6.1 安全监测

6.1.1 运维监测

检测目的：验证银行是否建立应用程序接口运维监测平台，将商业银行应用程序接口运维监测是否纳入商业银行统一监测平台并重点监测。

检测方法：

1) 访谈相关人员，确认商业银行是否建立了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是否纳入商业银行统一监测平台并重点监测；

2) 检查是否对应用程序接口相关服务器的运行状态、服务状态等进行监测，查看监测结果中的运行状况、服务状态（耗时、交易量、成功率等参数）、监控记录、报警方式和报警记录等内容；

3) 检查系统交易日志。

通过标准：

1) 商业银行建立了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；
2) 采取了相应措施对应用程序接口相关服务器的运行状态、服务状态等进行监测，查看监测结果中的运行状况、服务状态（耗时、交易量、成功率等参数）、监控记录、报警方式和报警记录等内容；
3) 系统交易日志保存期限不少于1年。

6.1.2 异常监测

检测目的：验证商业银行是否具有异常监测、故障隔离和黑名单控制等能力。

检测方法：

1) 检查商业银行是否具有异常监测、故障隔离和黑名单控制等能力，查看异常监测情况以及故障隔离和黑名单控制能力情况；
2) 检查是否对应用程序接口进行流量控制，分别查看控制规则是否包括最大允许商业银行应用程序接口调用的并发数、单位时间最大交易调用量等内容，控制措施是否包括告警、暂停、拒绝等内容；
3) 检查是否建立未授权和冒用商业银行应用程序接口的监测机制，发现问题时是否能以某种方式（如短信、邮件等）主动通知相关人员及时处置；
4) 检查系统是否具备故障监测、故障恢复和应用方黑名单管理能力。

通过标准：

1) 商业银行具备异常监测、故障隔离和黑名单控制等能力，发生异常情况商业银行具备合理的处理措施及能力；
2) 采取了相应措施对应用程序接口进行流量控制，对应的控制规则包括最大允许商业银行应用程序接口调用的并发数、单位时间最大交易调用量等内容符合要求，控制措施需包括告警、暂停和拒绝等内容符合要求；
3) 建立了相关监测机制，明确了发生未授权和冒用商业银行应用程序接口情况时，对应处理措施，发生问题时以某种方式主动通知相关人员及时处置；
4) 系统具备故障监测、故障恢复和应用方黑名单管理能力。

6.2 风险控制

6.2.1 服务风险控制

检测目的：验证商业银行是否建立有效的服务风险控制体系。

检测方法：

1) 访谈相关人员，确认是否建立有效的服务风险控制体系，查看服务风险控制体系是否符合要求；
2) 检查是否建立应用方信息（如运营能力、风控能力等）更新和复审机制；
3) 检查业务日志等信息，是否定期对金融交易业务运营情况进行评估，对异常业务调用进行监控，是否有业务限流机制，能否以某种方式（短信、邮件等）通知应用方及时处理；
4) 检查商业银行风险控制机制是否明确评估应用方的风险承受能力相关要求，以确保用户与应用方相关账户关联、服务类型、交易额度等信息与其风险承受能力相匹配。

通过标准：

1) 商业银行建立了有效的服务风险控制体系，服务风险控制体系符合要求，并依据该体系运行实施；
2) 建立了应用方信息（运营能力、风控能力等）更新和复审机制；

3） 应定期对金融交易业务运营情况进行评估，具有评估记录，对发生异常业务调用情况，必要时需进行业务限流，并及时通知应用方相关人员进行事件调查及处理；
4） 商业银行具备完善的风险控制机制，评估应用方的风险承受能力，能够确保用户与应用方之间涉及的账户关联、服务类型和交易额度等信息达到风险承受能力匹配等要求。

6.2.2 交易流程控制

检测目的：验证商业银行是否建立交易流程控制体系。
检测方法：
1） 访谈相关人员，确认是否建立有效的交易流程控制体系，查看交易流程控制体系是否符合要求；
2） 检查身份认证服务等授权类服务以何种方式识别是否经过用户本人授权；
3） 检查账户查询、资金交易、金融产品及服务申请类交易以何种方式识别是否经过用户本人发起（或本人授权发起），核实用户本人意愿；
4） 验证发生资金类等高风险金融服务时，是否向用户提示相关安全风险。
通过标准：
1） 商业银行建立了有效的交易流程控制体系，交易流程控制体系符合要求，并依据该体系运行实施。
2） 发生身份认证服务类等授权服务操作时，系统应能够充分识别经过用户本人授权发起；
3） 发生账户查询、资金交易、金融产品及服务申请类交易操作时，系统应能够充分识别经过用户本人发起（或本人授权发起），并能够核实用户本人意愿；
4) 发生资金类交易等高风险金融服务时，系统应向用户提示相关安全风险。

6.2.3 交易风险监控

检测目的：验证商业银行是否将通过应用程序接口实现的业务纳入交易风险范围。
检测方法：
1） 检查商业银行业务纳入交易风险范围方式，是否通过应用程序接口实现；
2） 检查是否对应用方和用户账户资金活动情况进行实时监控；
3） 检查资金交易是否满足行业监管部门对反洗钱、反欺诈方面的相关要求；
4） 检查是否对大额、异常的资金收付逐笔进行监测与核查，查看监测结果中的监测记录、核查记录、报警方式和报警记录等内容，当监测到风险交易情况时，是否以某种方式主动通知相关人员及时处置。
通过标准：
1）商业银行通过应用程序接口方式实现的业务纳入交易风险范围。
2）应采取相应措施对应用方和用户账户资金活动情况进行实时监控。
3）查看资金交易相关处理方式，满足行业监管部门对反洗钱、反欺诈方面的相关要求。
4）定期对监控到的风险交易和核查记录进行分析、评审、发现异常行为，形成分析报告，采取必要的应对措施，当监控到风险交易时如：发生大额、异常交易等风险交易，具备对应处理措施，发生问题时以某种方式主动通知相关人员及时处置和分析并形成记录。

6.3 变更控制

检测目的：验证商业银行应用程序接口发生变更时，是否及时评估影响并告知应用方。
检测方法：
1） 检查商业银行应用程序接口发生变更时，是否及时评估影响并告知应用方，并且是否妥善留存完整的变更过程文档和记录；

2） 检查商业银行是否对重大变更进行风险和影响评估以对应处置措施。

通过标准：

1） 商业银行应用程序接口发生变更时及时对变更结果进行评估并告知应用方，按需进行接口发布，具备完整的变更过程文档和记录；

2） 商业银行针对重大变更进行了风险和影响评估进行分析、评审，并形成分析报告，具备相应处置措施。

6.4 运维巡检

检测目的：验证商业银行是否均定期对商业银行应用程序接口进行安全巡检。

检测方法：

1） 检查商业银行是否定期对商业银行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。

2） 检查商业银行否定期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。

通过标准：

1） 商业银行定期对商业银行应用程序接口进行源代码审计、渗透测试技术检查以及应用程序接口安全集成情况进行检查，并及时处理安全漏洞，有效控制安全风险；

2） 商业银行采用了恰当的方法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，具备相关检查记录。

6.5 事件处理

检测目的：验证商业银行对运维过程中监测到的异常情况事件处理是否符合要求。

检测方法：

1） 检查商业银行对运维过程中监测到异常情况实践处理是否符合要求，是否具备对应处理记录；

2） 检查是否按重要程度进行分级报警，重要报警是否能以某种方式（如短信、邮件等）主动通知相关人员及时处置，是否及时处理生产事件，并协调应用方配合事件调查；

3） 检查安全事件报告和处置管理制度中，是否明确安全事件的类型，是否规定了安全事件的现场处理、事件报告和后期恢复的管理职责；

4） 检查是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，采取必要的应对措施；

5） 检查安全事件报告和响应处理程序中，是否明确事件的报告流程，是否明确响应和处置的范围、程度，以及处理方法等。

通过标准：

1） 商业银行对运维过程中监测到异常情况实践处理符合要求，具备对应处理记录；

2） 按重要程度进行分级报警，重要报警能以某种方式（如短信、邮件等）主动通知相关人员及时处置，及时处理生产事件，并协调应用方配合事件调查；

3） 安全事件报告和处置管理制度中，明确了安全事件的类型，规定了安全事件的现场处理、事件报告和后期恢复的管理职责；

4） 组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，采取必要的应对措施；

5） 安全事件报告和响应处理程序中，明确了事件的报告流程，明确了响应和处置的范围、程度、处理方法并协调应用方配合事件调查。

7 商业银行服务终止与系统下线检测

检测目的：验证商业银行是否建立服务终止与系统下线的制度和步骤。
检测方法：

1) 检查商业银行服务终止前，是否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；
2) 检查商业银行是否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；
3) 检查商业银行系统（接口）下线是否在相关服务确认终止之后执行，在下线之前是否设置挡板（如服务终止提示信息），明示应用方服务已终止；
4) 检查商业银行在系统（接口）下线之后是否将有关数据进行归档处理，数据保留期限是否按照国家与行业主管部门、商业银行相关规定与规则执行。

通过标准：

1) 商业银行服务终止前，能够做到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；
2) 商业银行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能够充分达成一致，明确相关责任，并充分履行用户告知义务；
3) 商业银行系统（接口）下线是在相关服务确认终止之后执行，在下线之前设置挡板（如服务终止提示信息），明示应用方服务已终止；
4) 商业银行在系统（接口）下线之后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。

8 商业银行安全管理检测

8.1 管理制度

检测目的：验证商业银行是否建立应用程序接口管理制度。
检测方法：

1) 检查商业银行是否将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；
2) 检查商业银行应用程序接口是否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JR/T 0185的附录B；
3) 检查商业银行是否建立信息公告制度，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；
4) 检查商业银行是否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；
5) 检查商业银行是否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。

通过标准：

1) 商业银行将应用程序接口的管理纳入到了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；
2) 商业银行应用程序接口采用统一格式的识别码，并在相关平台进行注册和登记；

3) 商业银行建立了信息公告制度，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；

4) 商业银行建立了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；

5) 商业银行提供了开发手册以指导应用方安全集成商业银行应用程序接口，开发手册包括安全集成要求、集成示例，以及测试环境的使用等。

8.2 应用安全责任

检测目的：验证商业银行与应用方是否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。

检测方法：

1) 检查合同或协议中是否明确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；

2) 检查合同或协议中是否明确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；

3) 检查合同或协议中是否明确商业银行与应用方的信息安全责任；

4) 检查合同或协议中是否明确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；

5) 检查合同或协议中是否明确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。

通过标准：

1) 商业银行与应用方的合同或协议中明确了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；

2) 商业银行与应用方的合同或协议中明确了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；

3) 商业银行与应用方的合同或协议中明确了商业银行与应用方的信息安全责任；

4) 商业银行与应用方的合同或协议中明确了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；

5) 商业银行与应用方的合同或协议中明确了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。

8.3 应用审计

检测目的：验证商业银行是否具备安全审计能力。

检测方法：

1) 检查商业银行是否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；

2) 检查商业银行是否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）；

3） 检查商业银行是否对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。

通过标准：

1) 商业银行记录了完整的商业银行应用程序接口访问日志，日志记录包括交易流水号、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；

2） 商业银行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）；

3） 商业银行对日志记录有完整性保护措施，能够确保日志不被篡改、删除、覆盖。

9 应用方安全设计检测

9.1 接口安全设计

9.1.1 接口交互安全（个人金融信息保护）

检测目的：验证应用方的个人金融信息保护是否满足要求。

检测方法：

1） 检查应用方对于商业银行 A2 类只读信息查询（如金融产品持有份额、用户积分等）结果是否在应用方本地保存。

通过标准：

1） 应用方对于商业银行 A2 类只读信息查询（如金融产品持有份额、用户积分等）结果未在应用方本地保存。

9.1.2 接口交互安全（支付敏感信息保护）

检测目的：验证应用方的支付敏感信息保护是否满足要求。

检测方法：

1） 检查应用方在交易认证过程是否生成了包含支付敏感信息的临时文件或内存数据，如有是否制定及时清除用户支付敏感信息的措施，可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。

通过标准：

1） 应用方在交易认证过程生成的包含支付敏感信息的临时文件或内存数据应具有及时清除用户支付敏感信息的措施，可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。

9.2 服务安全设计

9.2.1 安全监控

检测目的：验证应用方日志是否满足安全监控要求。

检测方法：

1） 检查应用方清分清算、差错对账等业务相关的接口日志中是否以部分屏蔽的方式记录支付账号（或其等效信息）；除此外个人金融信息是否在应用方日志中进行记录。

通过标准：

1） 应用方因清分清算、差错对账等业务需要时，相关的接口日志应采用部分屏蔽的方式记录支付账号（或其等效信息）；除此之外应用方日志不应记录个人金融信息。

9.2.2 密钥管理

检测目的：验证应用方的密钥管理和本地配置文件是否符合要求。

检测方法：

1） 检查应用方本地配置文件中是否存储了商业银行应用程序接口的 App_Secret 或私钥。

通过标准：

1） 应用方本地配置文件中未存储商业银行应用程序接口的 App_Secret 或私钥。

10 应用方安全部署检测

10.1 接口服务层部署要求

检测目的：验证应用方是否遵循 JR/T 0185—2020 中商业银行应用程序接口网络部署逻辑结构示意图，进行商业银行应用程序接口的安全部署。

检测方法：

1) 检查应用方是否在互联网边界部署了具备访问控制、入侵防范相关安全防护能力的网络安全防护措施，如：防火墙、IDS/IPS、DDoS 防护等，同时检查安全防护措施是否配置了有效的防护规则；

2） 检查应用方通过互联网、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的服务器，是否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；

3） 检查应用方部署商业银行应用程序接口有关安全控制措施，是否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。

通过标准：

1) 应用方在互联网边界部署了具备访问控制、入侵防范相关安全防护能力的网络安全防护措施，并配置了有效的防护规则；

2） 应用方通过互联网、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的服务器，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；

3） 应用方部署商业银行应用程序接口的有关安全控制措施，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。

11 应用方安全集成检测

11.1 应用方核准

11.1.1 应用方身份核验

检测目的：验证应用方在接入注册与审批阶段是否按商业银行要求提供身份核验资料。

检测方法：

1) 访谈相关人员，并检查相关材料，确认应用方是否按照商业银行的要求，在注册与审批阶段向商业银行提交了运营资质、法人信息材料、主要应用开发人员的个人信息身份材料等必要的身份核验材料。

通过标准：

1) 在应用方接入注册与审批阶段，应用方按照商业银行要求，提交必要的身份核验资料，包括但不限于运营资质、法人信息材料、主要应用开发人员的个人信息身份材料等。

11.2 接入安全控制

11.2.1 安全传输

检测目的：验证商业银行与应用方之间的网络安全传输是否符合安全要求。

检测方法：

1) 检查对于 A1 类，是否采用 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；

2) 检查对于 A2 类，是否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；
3) 检查商业银行与应用方之间数据传输是否采用 SSL/TLS 等安全通道连接进行通信及使用的 SSL/TLS 版本。

通过标准：

1) 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，必要时可采用数字签名技术；
2) 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；
3) 应采用 SSL/TLS 等安全通道连接进行安全通信，宜使用 TLS1.2 及以上版本。

11.3 运行安全

11.3.1 用户身份认证

检测目的：验证应用方在用户身份认证方面是否满足安全要求。

检测方法：

1) 检查若用户个人金融信息或支付敏感信息确需在应用方输入，应用方是否在本地留存相关信息。

通过标准：

2) 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。

11.3.2 权限控制

检测目的：验证应用方调用敏感接口时是否满足安全要求。

检测方法：

1) 检查对于获取、使用、变更用户信息、账户、资金等接口，应用方调用接口时，是否首先取得用户明示同意，其内容是否包含授权有效期。

通过标准：

1) 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，首先应取得用户明示同意，其内容应包含授权有效期。

11.3.3 数据安全

检测目的：验证应用方在数据安全保护方面是否满足安全要求。

检测方法：

1) 数据完整性保护：检查应用方是否对数据完整性进行校验，并在检测到完整性错误时是否采取必要的恢复措施。

   数据机密性保护：

   a) 检查应用方是否采集、存储用户个人金融信息或支付敏感信息；
   b) 检查对于需要用户输入支付敏感信息或身份鉴别信息的场景，应用方是否仅作为信息的采集与传输通道，是否部署商业银行 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是否在应用方进行留存；
   c) 数据抗抵赖性保护：检查应用方是否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：检查应用方是否承诺在合作终止后，将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；

e) 检查针对接口处理的数据，应用方是否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。检查应用方是否承诺在合作终止后，依据行业主管部门有关要求，履行反洗钱、反欺诈等义务。

通过标准：

1) 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）。

2) 数据机密性保护：

a) 不应采集、存储用户个人金融信息或支付敏感信息；

b) 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不应在应用方留存；

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：应用方通过签署相关协议等有效方式承诺在合作终止后，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；

e) 针对接口处理的数据，应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。检查应用方通过签署相关协议等有效方式承诺在合作终止后，依据行业主管部门有关要求，履行反洗钱、反欺诈等义务。

11.3.4 应用方安全能力

检测目的：验证应用方安全防护是否满足安全要求。

检测方法：

1) 查看应用方安全建设方案、验收报告、最近的等保测评报告等材料，确认其是否按照国家网络安全等级保护相应要求，进行了安全设计、安全建设和安全保护；

2) 查看应用方源代码，确认应用方是否遵循商业银行的安全设计要求，使用了商业银行提供的安全接口，依据用户手册和安全规范进行了集成；

3) 查看应用登录相关设备，检查应用方是否存留了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，确认存留的日志是否不少于 6 个月；

4) 通过访谈、文档审查、配置检查、查看源代码等方式确认应用方是否通过有效的技术手段和管理措施等防止接口滥用。

通过标准：

1) 应用方应按照国家网络安全等级保护相应要求，进行安全设计、安全建设和安全保护；

2) 应用方应遵循商业银行的安全设计要求，使用了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了集成；

3) 应用方应存留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，日志存留不少于 6 个月；

4) 应通过有效的技术手段和管理措施防止接口滥用。

11.3.5 应用方接口集成

检测目的：验证应用方接口集成是否满足安全要求。

检测方法：

1) 查看应用方接口集成程序源代码，确认其是否按照商业银行提供的用户手册以及授权其使用的服务类型要求，正确合理的使用 API；

2) 查看应用方接口集成程序源代码，确认应用方是否对密钥加密存储，密钥加密使用的密码算法是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求，相关密钥、数字证书的使用和保管是否符合商业银行提供的用户手册要求；
3) 如商业银行提供封装了商业银行应用程序接口调用的 SDK，审查应用方接口集成程序源代码，分析应用方是否使用商业银行提供的 SDK 进行 API 调用，是否对商业银行提供的 SDK 进行了篡改或二次封装，应用方是否承诺不会对商业银行提供的 SDK 进行反编译；
4) 访谈应用方相关人员，了解应用方是否承诺若发现商业银行应用程序接口存在安全缺陷，将采取合理的补救措施并及时通知商业银行；了解应用方是否承诺未经商业银行许可，不会将发现的缺陷细节透露给任何其他第三方；
5) 查看相关资料，确认应用方是否承诺不会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。

通过标准：

1) 应用方 API 使用正确合理，符合商业银行提供的用户手册和授权其使用的服务类型要求；
2) 应用方对密钥加密存储，相关密钥、数字证书的使用和保管符合商业银行提供的用户手册要求；
3) 如商业银行提供封装了商业银行应用程序接口调用的 SDK，应用方需使用商业银行提供的 SDK 进行 API 调用，不得对商业银行提供的 SDK 进行篡改或二次封装；应用方通过签署相关协议等有效方式承诺承诺不会对商业银行提供的 SDK 进行反编译；
4) 若应用方发现商业银行应用程序接口存在安全缺陷，应采取合理的补救措施并及时通知商业银行。应用方通过签署协议等有效方式承诺未经商业银行许可，不得将缺陷细节透露给任何其他第三方；
5) 应用方应承诺不会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。

11.4 应用方退出

检测目的：验证应用方是否制定了符合商业银行要求的退出机制。

检测方法：

1) 访谈应用方相关人员，并审核相关材料，了解应用方若要退出，其对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的处理措施，并确认应用方是否承诺在双方协定的期限内承担后续保密的责任。

通过标准：

1) 应用方通过签署相关协议等有效方式承诺将按照商业银行的要求，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。

12 应用方安全运维检测

12.1 安全监测

12.1.1 异常监测

检测目的：验证应用方是否具有故障识别与隔离能力。

检测方法：

1) 检查应用方是否具有故障识别与隔离能力，查看应用故障识别与隔离能力情况；

2) 检查应用方是否具有熔断机制，查看熔断规则和熔断措施是否包括失败笔数阈值、商业银行应用程序接口调用失败阈值、拒绝交易和暂停服务调用等；
3) 检查是否建立异常告警处理机制。

通过标准：

1) 应用方具备故障识别与隔离能力，发生异常情况应用方具备合理的处理措施及能力；
2) 应用方具有熔断机制，并依据制度执行，查看熔断规则和熔断措施是否包括失败笔数阈值、商业银行应用程序接口调用失败阈值、拒绝交易和暂停服务调用等内容，相关要求配置合理；
3) 建立了相关异常告警处理机制，明确了异常告警时，对应处理措施，发生问题时以某种方式主动通知相关人员及时处置。

12.2 风险控制

12.2.1 交易流程控制

检测目的：验证应用方是否建立交易流程控制体系。

检测方法：

1) 访谈相关人员，确认是否建立有效的交易流程控制体系，查看交易流程控制体系是否符合要求；
2) 检查身份认证服务等授权类服务以何种方式识别是否经过用户本人授权；
3) 检查账户查询、资金交易、金融产品及服务申请类交易以何种方式识别是否经过用户本人发起（或本人授权发起），核实用户本人意愿；
4) 验证发生资金类等高风险金融服务时，是否向用户提示相关安全风险。

通过标准：

1) 应用方建立了有效的交易流程控制体系，交易流程控制体系符合要求，并依据该体系运行实施；
2) 发生身份认证服务类等授权服务操作时，系统应能够充分识别经过用户本人授权发起；
3) 发生账户查询、资金交易、金融产品及服务申请类交易操作时，系统应能够充分识别经过用户本人发起（或本人授权发起），并能够核实用户本人意愿；
4) 发生资金类交易等高风险金融服务时，系统应向用户提示相关安全风险。

12.3 变更控制

检测目的：验证应用方是否采取有效的变更控制措施。

检测方法：

1) 检查应用方是否具备有效的变更方案和应急预案；
2) 检查是否具备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相关的变更方案和应急预案。

通过标准：

1) 应用方具备变更方案和应急预案相应控制措施，明确了当应用程序接口的使用发生变更时应及时对变更结果进行评估并告知商业银行，同时充分履行用户告知义务，具备完整的变更过程文档和记录；
2) 具备发生重大变更时对应的变更方案和应急预案，明确了相关处理流程且具备完整的变更过程记录。

12.4 运维巡检

检测目的：验证应用方是否定期对商业银行应用程序接口进行安全巡检。
检测方法：
1) 检查应用方是否定期对商业银行应用程序接口进行安全巡检，包括：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。
通过标准：
1) 应用方采用了恰当的方法定期对商业银行应用程序接口进行安全巡检，巡检内容包括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，并及时处理了安全漏洞，具备相关记录。

13 应用方安全管理检测

13.1 应用安全责任

检测目的：验证商业银行与应用方是否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。
检测方法：
1) 检查合同或协议中是否明确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；
2) 检查合同或协议中是否明确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；
3) 检查合同或协议中是否明确商业银行与应用方的信息安全责任；
4) 检查合同或协议中是否明确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；
5) 检查合同或协议中是否明确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。
通过标准：
1) 商业银行与应用方的合同或协议中明确了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。
2) 商业银行与应用方的合同或协议中明确了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。
3) 商业银行与应用方的合同或协议中明确了商业银行与应用方的信息安全责任。
4) 商业银行与应用方的合同或协议中明确了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。
5) 商业银行与应用方的合同或协议中明确了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。

13.2 应用审计

检测目的：验证应用方是否具备安全审计能力。
检测方法：
1) 检查应用方是否完整记录商业银行应用程序接口访问日志，日志记录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。

2) 检查应用方是否对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。

3) 检查应用方是否提供查询应用方用户商业银行应用程序接口历史操作日志功能，日志内容是否包含登录、授权、交易等。

通过标准：

1) 应用方记录了完整的商业银行应用程序接口访问日志，日志记录中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未在应用方接口日志中进行记录；

2) 应用方对日志记录有完整性保护措施，能够确保日志不被篡改、删除、覆盖；

3) 应用方提供了查询应用方用户商业银行应用程序接口历史操作日志功能，日志内容包含登录、授权、交易等。