ICS 03.060
A11

Q/GXGB

广西北部湾银行股份有限公司企业标准

Q/GXGB 0001—2023

广西北部湾银行移动金融客户端应用软件安全管理标准

Guangxi Beibu Gulf Bank Financial Mobile Application Software Security Management Specification

企业标准信息公共服务平台
公开 2023年10月31日 14点55分

2023－10－31 发布　　2023－08－31 实施

广西北部湾银行股份有限公司　发布

目　次

企业标准信息公共服务平台
公开 2023年10月31日 14点55分

前　言

本标准按照GB/T1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本标准代替Q/GXGB 0001—2021《广西北部湾银行移动金融客户端应用软件安全管理标准》。

本标准与Q/GXGB 0001—2021相比，主要变化如下：

——规范标准引用描述；

——整合丰富原“设计管理要求”和“开发管理要求”，形成“客户端应用软件设计及开发要求”内容（见6）；

——增加了“开发安全管理要求”、“上线管理要求”内容（见6.2.1、6.2.3）；

——修改了“认证方式”、“安全输入”、“密码的设定与重置”、“逻辑安全设计”、“风险控制”各部分内容描述（见7.1.1、7.1.2.1、7.1.4、7.2.1、7.2.3）；

——“密码算法”增加了商用密码相关内容要求（见7.4.1）；

——“服务创新”增加了适老化功能、无障碍功能内容（见9.1）；

——“技术创新”增加了指纹识别、人脸识别、视频客服技术应用内容（见9.2）。

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：梁生安、卢朗、李鸿生、韦文磊、黄秦。

本标准所代替标准的历次版本发布情况为：

——本标准于2020年9月首次编制。

——本次为第二次修订。

广西北部湾银行移动金融客户端应用软件安全管理标准

1 范围

本标准规定了本行移动金融客户端应用软件的安全要求，以及本行客户端应用软件设计、开发、维护和发布的管理要求。

本标准适用于本行移动金融客户端应用软件的设计、开发维护及发布过程，也适用于本行评估部门对相关应用进行安全性和标准符合性评估。

2 规范性引用文件

下列文件对于本标准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标准。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。

JR/T 0092-2019《移动金融客户端应用软件安全管理规范》

JR/T 0171-2020《个人金融信息保护技术规范》

JR/T 0098.3-2012《中国金融移动支付检测规范第3部分：客户端软件》

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

GB/T 35273-2020《信息安全技术 个人信息安全规范》

GB/T 41391—2022《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》

3 定义和术语

下列术语和定义适用于本标准文件。

3.1

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。

3.2

资金交易类客户端应用软件 capital transaction client application software

直接面向用户提供资金交易服务的移动金融客户端应用软件。

注： 包括但不限于手机银行、支付 APP 等。

3.3

信息采集类客户端应用软件 information collection client application software

不直接向用户提供资金交易服务，但需采集个人敏感信息的移动金融客户端应用软件。

3.4

个人金融信息 personal financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、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、借贷信息及其他反映特定个人某些情况的信息。

3.5

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。

3.6

SSL/TLS 协议 secure socket layer protocol/transport layer security

位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持。

3.7

错误拒绝辨识率 false-negative identification-error rate

在辨识过程中，注册用户被系统错误辨识为其他注册用户的次数与总测试次数的比率的测定值。

注：错议拒绝辨识率=1-正确辨识率。

3.8

错误接受辨识率 false-positive identification-error rate

在辨识过程中，非注册用户被系统辨识为某个注册用户的次数与总测试次数的比率的测定值。

注：错误接受辨识率依赖于 a)注册数据库的大小，b)匹配得分的判别阈值以及返回的匹配识别数目。

4 缩略语

下列缩略语适用于本文件。

APP：客户端应用软件（Application software）

URI：统一资源标识符（Uniform Resource Identifier）

TEE：可信执行环境（Trusted Execution Environment）

SDK：软件开发工具包（Software Development Kit）

SE：安全单元（Secure Element）

SSL/TLS：安全套接字层/传输层安全性协议（secure socket layer/transport layer security）

5 总体要求

客户端应用软件分为资金交易类、信息采集类。资金交易类客户端应用软件应符合资金交易、信息保护等所有技术及管理安全要求。信息采集类客户端应用软件应重点符合信息保护相关技术及管理安全要求。

6 客户端应用软件设计及开发要求

客户端应用软件设计及开发应符合 JR/T 0092—2019《移动金融客户端应用软件安全管理规范》和 JR/T 0098.3—2012《中国金融移动支付检测规范第 3 部分：客户端软件》相关要求。

6.1 设计要求

6.1.1 整体设计要求

a) 客户端应用软件设计应考虑设计的合理性、安全性、规范性、正确性和完整性等进行控制，制定《概要设计说明书》《数据库设计说明书》《详细设计说明书》《接口设计说明书》等软件设计相关文档，指导客户端软件设计与开发。
b) 客户端应用软件设计应落实个人金融信息安全管理要求，按照合法、正当、必要的原则，收集个人金融信息或用户授权等操作前，向用户清楚、完整提示使用客户端软件需要收集的个人金融数据、获取的权限内容及用途，并经用户选择是否授权。
c) 客户端应用软件功能设计应严格按照《广西北部湾银行电子银行隐私政策》要求和用户实际授权情况，执行个人金融信息收集和运行权限使用。

6.1.2 兼容性要求

6.1.2.1 网络兼容性

6.1.2.1.1 弱网兼容性

客户端应用软件应检查客户端网络连接状态，提示用户当前接入网络类型（如 WIFI 或蜂窝网络），若处于弱网状态或无网络状态时，应提示和引导用户检查客户端网络连接，并对交易流程进行控制处理。

6.1.2.1.2 IPv6 兼容性

客户端应用软件应支持 IPv4 和 IPv6 网络环境的部署和使用，应优先使用 IPv6 地址与服务器建立连接，当 IPv6 网络环境异常时，应自动切换至 IPv4 地址运行。

6.1.2.2 操作系统兼容性

客户端应用软件应兼容主流操作系统版本，操作系统版本兼容策略包括但不限于：

a) iOS 操作系统应支持 iOS 10 及以上版本。
b) Android 操作系统应支持 Android 7.0 及以上版本。对于华为手机，应支持鸿蒙 HarmonyOS 2 及以上版本。
c) 客户端应用软件开展兼容性测试，测试机型数量应大于 100。

6.1.3 软件共存要求

客户端应用软件不应影响用户终端其他 APP 的正常使用，包括但不限于：

a) 破坏操作系统或其他 APP 目录结构。
b) 干扰操作系统或其他 APP（如杀毒软件等）的正常运行。

6.1.4 软件性能要求

6.1.4.1 启动时间

iOS 客户端应用软件冷启动时间应小于等于 1 秒，Android 客户端应用软件冷启动时间应小于等于 2 秒，并积极采取以下措施减少启动时间，包括但不限于：

a) 宜设置启动页主题，启动后宜立即显示启动视图，提前展现加载画面。
b) 宜将耗时操作进行异步处理，以减少启动过程时间消耗。
c) 宜将非必要网络操作进行异步处理，以减少启动过程时间消耗。
d) 宜延迟创建和懒加载处理主页面视图。

6.1.4.2 安装包大小

客户端应用软件安装包在满足功能设计要求的前提下，应尽量减小安装体积，可通过 APP 瘦身优化措施减少安装包大小，包括但不限于：

a) 针对 Android so 文件精简，宜使用 armeabi 和 arm64-v8a 架构的 so 文件，以减少 so 文件体积。
b) 针对资源优化，应对资源进行压缩处理，去除冗余和无用资源。
c) 针对代码优化，应及时移除无用代码。

6.1.4.3 资源管理

客户端应用软件应对 res、dex、lib 等 APP 资源文件进行管理和优化，包括但不限于：

a) 针对 res 资源文件管理（包括图片、文件、网页等内容），应及时清理无用资源。
b) 针对 dex 优化，应优化 dex 文件大小，及时删除不引用的无效代码。
c) 针对 lib 优化，应优化库、组件管理，以提高 lib 封装和运行效率。

6.1.4.4 后台响应时间

客户端应用软件的后台服务器平均响应时间应小于等于 1 秒，并建立联机响应时间记录机制，可通过监控系统进行后台响应时间监控。

6.1.4.5 后台并发量

客户端应用软件的后台服务器应满足业务高峰时段并发需求，应支持根据交易并发设置数据库连接数和应用连接数。

6.1.4.6 CPU 占用

客户端应用软件在一般业务高峰期 CPU 占用率不应超过 30%。

6.1.4.7 内存占用

客户端应用软件应避免内存占用过大或内存泄露问题，包括但不限于：

a） 控制大文件，数据库、图片、接口服务等内容内存使用，避免占用内存过大。
b） 对象使用后应进行立即释放。
c） 提交应用市场送审前，应进行内存检查和测试，确保应用无内存泄漏。

6.1.5 客户端更新要求

客户端应用软件应支持不同客户端升级策略，包括但不限于：
a） 针对提示升级，用户可选择升级最新客户端或不升级最新客户端。
b） 针对强制升级（如安全加固更新），用户只有升级最新客户端才能使用。

6.2 开发要求

6.2.1 开发安全管理要求

a） 客户端应用软件开发严格按照《广西北部湾银行金融科技项目管理办法》《广西北部湾银行源代码安全设计规范》等要求，严格落实开发流程、项目管理流程和编码安全规范，进行完整的测试，避免存在漏洞风险。
b） 在立项分析阶段，应对立项材料中涉及应用安全管控要求的内容进行分析和必要的安全评估。
c） 在需求编制阶段，应对需求中涉及应用安全管控要求的内容进行分析，完成相关业务需求分析说明书的编写。
d） 在设计阶段，应对业务需求涉及应用安全及业务风险防控内容进行分析，并在总体方案对应的安全设计章节中体现。对于交易流程中的安全控制，应在功能模块的处理流程中体现。
e） 在编码阶段，应根据业务需求文档、总体方案中的安全管控要求进行编码，包括但不限于服务端的数据合法性检查、权限检查、SQL 注入防范、恶意文件上传防范等要求。
f） 在测试阶段，应根据业务需求文档、总体方案中的安全管控要求，对项目涉及的安全及业务风险防控内容执行安全及业务风险防控测试，包括但不限于交易失败、交易串户、重复记账、记账差错、记账失败等异常的业务场景，并按照安全测试问题时效进行处理。
g） 版本交付前，应完成当期版本专项安全测试并进行软件代码扫描。
h） 客户端应用软件的生产投产和变更，须通过源码扫描和安全渗透测试等安全检查流程验证无风险，并经审批后执行。
i） 客户端应用软件开发应严格按照项目文档管理要求，制定完整、可操作的源代码说明、开发手册和运维手册等开发文档。

6.2.2 开发缺陷管理要求

6.2.2.1 缺陷问题分类

客户端应用软件开发阶段发现缺陷应严格按照《广西北部湾银行软件测试管理办法》要求，根据缺陷严重程度和类型等进行缺陷分类定级（致命、严重、一般、轻微、建议），正确、清晰记录缺陷信息。

6.2.2.2 缺陷解决时效

缺陷问题解决时效应达到以下要求：
a） 致命缺陷应在 2 个小时内解决。
b） 严重缺陷应在 1 个工作日内解决。

c） 一般、轻微和建议缺陷应在 2 个工作日内解决。

6.2.2.3 缺陷解决率

缺陷问题解决率应达到以下要求：

a） 致命和严重缺陷修复率为 100%。

b） 一般、轻微和建议缺陷解决率为≥95%。

6.2.3 上线管理要求

客户端应用客户端软件正式上线运行前，应落实以下工作：

a） 聘请具有专业资质的外部机构对客户端软件开展风险测评，完成客户端软件实名备案。

b） 应至少提前 30 个工作日向当地中国人民银行报备，备案内容包括客户端软件概况说明、技术方案、个人信息保护政策（隐私政策）、风险防控措施及应急预案。

7 客户端应用软件安全要求

客户端应用软件安全要求应符合 GB/T 35273—2020《信息安全技术 个人信息安全规范》、GB/T 41391—2022《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》和 JR/T 0171—2020《个人金融信息保护技术规范》相关要求，具体要求如下：

7.1 身份认证安全

7.1.1 认证方式

a） 客户端应用软件登录时，采用密码、短信验证码、手势密码、生物特征识别和语音外呼（风控触发）等组合认证手段，严格认证用户身份。

b） 资金交易类应用软件登录，应采用两种或两种以上的要素（如密码+短信验证码）对用户身份进行认证。

c） 客户端应用软件执行资金交易或敏感信息修改时，应按照相关业务管理要求对用户身份进行认证。如：对于资金交易，客户端应采用两种或两种以上要素对用户身份进行认证等。

d） 采用手势密码作为验证要素，手势密码要求至少设置连续不间断的 4 个点。

e） 采用短信验证码作为验证要素，短信验证码仅能使用一次，仅限于在规定时间内使用，图形验证码应由服务器生成，短信验证码具备长度（6 位）和随机性的要求，客户端源文件中不应包含图形验证码文本内容，短信验证码所在的短信内容中，告知用户短信验证码的用途。

f） 图形验证码不得作为独立的身份验证要素。

g） 若采用生物特征识别作为验证要素，应当符合国家、金融行业标准和相关信息安全管理要求，防止非法存储、复制和重放。

h） 资金交易类客户端应用软件在用户身份认证后，客户端应用软件进入终端系统后台时，如果超过设定时限后被唤醒切换到前台，应采取措施对用户身份重新认证。

7.1.2 认证信息安全

7.1.2.1 安全输入

a） 客户端应用软件应采用加密技术对用户输入敏感信息（如密码）进行安全保护，包括但不限于登录、交易密码加密存储和加密传输。
b） 用户密码保护可使用专业的密码控件产品向客户提供输入密码的即时防护功能。
c） 密码控件产品提供替换输入框原文、逐字符加密和防范键盘窃听等安全控制措施。

7.1.2.2 个人金融信息展示

a） 客户端应用软件的密码框默认屏蔽明文显示，采用同一特殊字符（例如*或•）代替密码明文。
b） 客户端应用软件禁止明文显示银行卡密码和网络支付交易密码。
c） 客户端应用软件用户处于未登录状态时，不展示与个人信息主体相关的用户鉴别信息（如：卡片验证码、卡片有效期、登录密码、支付密码等）。
d） 客户端应用软件用户处于已登录状态时， 除银行卡有效期外，用户鉴别信息（如：卡片验证码、登录密码、支付密码等）禁止明文展示。
e） 对于银行卡号、客户法定名称、手机号码、证件类或其他识别标识信息等可以直接或组合后确定信息主体的信息进行有效屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应履行客户端身份验证，防范信息泄露风险。
f） 涉及其他信息主体的信息时，宜进行屏蔽展示，当满足如下条件之一时可不脱敏：
1）其他方主动发起的活动包含的信息，如其他方发起交易、收付款。
2）与其他方已建立信任关系（间接授权），如向其他方收款、其他方已付款、向其他方申请代付、其他方同意付款或者其他方在自己业务应用范围内的联系人。

7.1.3 认证失败处理

a） 客户端应用软件具备认证失败处理功能，认证失败处理后采取结束会话、限制失败登录次数和自动退出等措施。
b） 在提示客户认证失败时，应模糊错误提示信息，防止错误提示信息中泄露用户账号、交易金额等敏感数据。

7.1.4 密码的设定与重置

a） 客户端应用软件具备密码复杂度校验功能，交易密码复杂度由后端系统进行判断，保证用户设置的密码达到一定的强度，避免采用简单密码或与用户身份信息（身份证号、手机号等）相似度过高的密码。
b） 资金交易类应用软件，密码设置页面具备密码安全提醒，提醒用户设置使用强密码。
c） 客户端应用软件不设置初始密码，登录密码与交易密码均由用户自行设置。
d） 客户端应用软件在修改密码前，应对用户身份进行重新验证。
e） 客户端应用软件修改密码时对原密码进行验证并限制密码输入错误次数。
f） 客户端应用软件修改密码时新密码不应与原密码相同。
g） 客户端应用软件在重置密码时，使用短信验证码、用户注册信息、人脸认证、身份证联网核查等方式，对用户身份进行校验。

7.2 逻辑安全

7.2.1 逻辑安全设计

a) 客户端应用软件应充分考虑业务和安全防护需求，合理设置业务流程，加强认证和校验控制措施。
b) 对于认证、校验等安全保证功能的流程设计，充分校验用户输入信息，避免出现逻辑控制漏洞，采用加密技术、证书认证技术和生物识别技术等新技术，确保认证流程无法被绕过。
c) 对于涉及交易处理功能，应严格落实用户身份认证、数据校验和权限控制要求，充分考虑业务交易控制校验逻辑，在服务端实现控制措施。
d) 客户端代码设计和实现时尽量避免使用具有漏洞风险开源组件或调用存在安全漏洞的函数，避免敏感数据硬编码。

7.2.2 软件权限控制

客户端应用软件向移动终端操作系统申请权限时，应遵循业务需要最小权限原则，并严格按照隐私条款执行。

7.2.3 风险控制

a) 客户端应用软件具备账户登录超时控制策略，当用户闲置在线状态超出时限时，强制用户离线，重新返回界面需要重新验证用户身份。
b) 客户端应用软件具备用户多点登录控制策略，一般采取禁止多点登录，后登录的会挤掉前面登录的账户并提示因为多点登录被退出，需要用户注意风险。
c) 资金交易类客户端应用软件具有交易风险控制策略，针对不同的资金交易金额使用不同的安全认证策略。
d) 资金交易类客户端应用软件具有限额和安全锁策略，允许用户针对不同的资金交易业务场景配置限制策略，如限制境内、境外不同渠道支付金额等。
e) 客户端应用软件系统接入反欺诈系统，通过大数据和智能模型技术，发现用户异常登录、进行风险支付等风险操作，根据业务规则和监管规定执行反欺诈风险提示和控制措施。
f) 加强客户端应用软件仿冒和钓鱼监测，采购专业第三方机构服务，监控全部互联网应用发布渠道，发现存在仿冒和钓鱼应用执行下架处置。

7.2.4 回退处理

交易过程中如遇交易失败或在交易完成前用户进行撤销操作，应返回到交易前的有效状态。

7.2.5 异常处理

a) 客户端应用软件发生故障产生的异常信息，应制作统一报错页面，禁止泄露用户的敏感数据。
b) 当交易出现异常时，客户端应用软件应向客户提示标准化的出错信息，禁止泄露用户的敏感数据。

7.2.6 风险提示

a) 客户端应用软件应默认关闭有风险的功能选项，如因为业务需要使用，在提示客户后由客户选择开启。
b) 对于有风险操作，客户端应用软件应能有效地提示客户。
c) Android 客户端应在退到后台时，通过提示信息向用户提醒，客户端软件已进入后台运行。
d) 用户打开 Android 客户端，提示用户当前网络环境，需要注意网络环境安全风险。

7.3 安全功能设计

7.3.1 组件安全

a) 客户端应用软件禁止使用存在已知漏洞的系统组件与第三方组件。
b) 客户端应用软件在使用第三方组件时，进行开源组件安全扫描和测试，并设计有效权限控制措施，避免第三方组件安全风险和未经授权收集用户信息。

7.3.2 接口安全

a) 客户端应用软件对软件接口进行有效权限控制和保护，防止其他应用对客户端应用软件接口进行非授权调用。
b) 客户端应用软件对传入的 URI 进行校验与安全处理，防止客户端应用软件运行异常或操作异常。
c) 当客户端应用软件需要与 TEE、SE 结合使用时，禁止使用存在已知漏洞的接口。

7.3.3 抗攻击能力

a) 客户端应用软件具备抗攻击能力，采用第三方安全加固服务对客户端进行安全加固，能抵御静态分析、动态调试等操作。
b) 客户端应用软件安装、启动、更新时对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。
c) 客户端应用软件采用密码控件，该控件应具备抵御安全攻击的能力，如具备：检测自身是否正在被调试、抵御键盘钩子攻击、内存信息泄露攻击等。

7.3.4 客户端应用软件环境检测

客户端应用软件在运行时应具备对运行环境的检查能力，检查的范围可包括：系统是否已经 ROOT、程序运行环境是否可信（如：是否运行在模拟器或虚拟机中）等，并能向后台系统反馈设备信息等。

7.4 密码算法及密钥管理

7.4.1 密码算法

a) 客户端应用软件使用密码算法对资金有关交易或重要业务操作进行保护，优先使用国密加密算法。
b) 网络安全等级保护为三级的客户端应用软件系统，应制定有商用密码应用方案，同时每年开展商用密码应用安全性评估。
c) 客户端应用软件加密算法选择，应根据实际业务和安全防护需要选择合适加密算法。

d) 密码算法、密钥长度及密钥管理方式应符合国家密码主管部门的要求。

7.4.2 密钥管理

a) 密钥在传输过程中应使用密码算法对密钥进行保护。
b) 随机生成的密钥具有一定的随机性与不可预测性。
c) 密钥加密存储，并确保密钥储存位置和形式的安全。

7.5 数据安全

7.5.1 数据获取

7.5.1.1 数据防窃取

a) 客户端应用软件应禁止在内存中存储完整的银行卡密码和网络支付交易密码明文。
b) 客户端应用软件采用密码控件产品，使用强加密算法加密，防止内存中加密的敏感数据被还原为明文。
c) 客户端应用软件的临时文件中禁止出现支付敏感信息，临时文件包括但不限于 Cookies、本地临时文件等。
d) 客户端应用软件程序禁止在身份认证结束后存储支付敏感信息，防止支付敏感信息泄露。
e) 客户端应用软件运行日志中禁止打印支付敏感信息和完整的敏感数据原文。
f) 资金交易类客户端应用软件在身份认证过程中具备防截屏、录屏功能，如：输入手势验证码、登录密码等。

7.5.1.2 数据防篡改

用户输入关键交易数据时，如：收款人信息、交易金额、订单号等，采用密码技术执行通信链路加密、报文加密和签名等措施，防范数据遭受篡改保证数据完整性和正确性。

7.5.1.3 数据有效性

客户端应用软件在数据获取时提供有效性校验功能，确保通过人机接口或通信接口输入的数据格式或长度等信息符合业务和系统设定要求。

7.5.2 数据访问控制

a) 应采取严格的访问控制措施，保护客户端应用软件数据仅能被授权用户或授权应用组件访问。
b) 客户端应用软件严格遵守隐私文件声明授权范围，不访问客户手机终端非业务必需的文件和数据。

7.5.3 数据传输

7.5.3.1 通讯安全

a) 客户端应用软件与服务器之间通信链路，采用 SSL 安全应用网关进行加密，建立安全的信息传输通道，SSL 协议版本应及时更新至安全稳定版本，确保采用的安全协议不包含已知的公开危险漏洞。
b) 客户端应用软件与服务器应进行认证，通过密钥或证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。

7.5.3.2 数据安全性

a) 当因为业务需要，客户敏感数据（如：登录密码、支付敏感信息等）需要在客户端应用软件与本地其他应用软件间传输时，必须采取加密等措施确保其保密性，若本地其他应用软件不能提供与金融客户端软件相应等级的加密接口，则应评估敏感数据调用的风险，并设计补救措施。
b) 当因为业务需要，客户敏感数据（如：登录密码、支付敏感信息等）需要通过公共网络传输时，必须采取加密等措施确保其保密性。
c) 关键的交易数据，如：收款人信息、交易金额、订单号等，在客户端应用软件与本地其他应用软件间传输时，应采取措施（如：数字签名、MAC 等）确保其完整性，若本地其他应用软件不能提供与金融客户端软件相应等级的数据完整性保护措施，则应评估关键数据传输的风险，并设计补救措施。
d) 关键的交易数据、个人身份信息，如：收款人信息、交易金额、订单号、身份证号码等，在通过公共网络传输时，应采取措施（如：数字签名、MAC 等）确保其完整性。
e) 通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，优先采用数字证书技术。
f) 通过客户端应用软件发起的身份认证或资金类交易报文，应能够防止重放攻击。

7.5.4 数据存储

7.5.4.1 个人金融信息存储

a) 客户端应用软件不应以任何形式存储用户的支付敏感信息与金融业务查询密码。
b) 在满足法律、管理规定的前提下，客户端应用软件应仅保存业务必需的个人金融信息，并限制数据存储量。

7.5.4.2 加密密钥存储

客户端应用软件应确保无法通过逆向工程等手段直接从本地文件系统中恢复完整的密钥明文。

7.5.5 数据展示

除交易对账、转账收款方确认等必须由用户确认的情况外，客户端应用软件在显示个人信息，如：银行账号、身份证号码、手机号码等时应屏蔽关键字段。

7.5.6 数据销毁

7.5.6.1 残余信息保护

a) 客户端应用软件在敏感数据使用完毕后，应立即对其进行清除。

b） 客户端应用软件进程被结束时，清除非业务功能运行所必需留存的业务数据，保证客户信息的安全性。
c） 客户端应用软件卸载完成后，文件系统中不残留任何个人金融信息。

7.5.6.2 页面返回保护

客户端应用软件应支持页面返回后自动清除银行卡密码、网络支付交易密码、登录密码等支付敏感信息的机制。

7.5.6.3 会话失效

客户端应用软件在安全退出登录时，向服务器发送会话结束请求，使当前会话状态失效。

8 客户端应用软件管理要求

8.1 发布管理要求

a） 客户端应用软件发布严格遵守上线发布流程，由应用软件的所有方对应用软件进行签名和保护，标识应用软件的来源和发布者，提供安全可靠的应用软件下载、发布、升级渠道。
b） 客户端应用软件删除调试或测试中存留的敏感数据。
c） 客户端应用软件安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不得篡改、覆盖、删除系统文件和其他软件。
d） 客户端应用软件有新版本时，不能未经用户允许自动安装新版本。
e） 若客户端应用软件支持动态模块更新，应使用加密信道与服务端通信传输更新模块或对更新模块进行签名校验；动态模块更新后不得影响用户使用，不得修改用户已有的安全配置。

8.2 维护管理要求

a） 客户端应用软件日常维护，严格执行运维管理策略和制度，明确各类角色的工作协同、实施步骤、质量管控、安全检测等，规范日常运维流程。
b） 客户端应用软件具有明确的应用标识符和版本序号，具有合理的升级更新接口，当某一版本被证明存在安全隐患时，及时进行修复更新。

9 客户端应用软件创新及前瞻性

9.1 服务创新

9.1.1 适老化功能实现要求

a） 客户端应用软件内嵌适老版界面的应在首页设置版本切换入口，支持切换至适老版，或在首次进入时给予显著切换提示，且在“设置”中提供适老版切换入口。
b） 适老版中通过增大页面字体与图标、精选老年客群常用功能、支持页面内容语音播报并支持通过手势、人脸、指纹、密码等方式进行认证登录。

c） 针对老年客户进线咨询，我行客服中心可一键接入人工客服，简化老年客群拨打客服热线操作。同时为客户提供 24 小时粤语、桂柳话、客家话等多种本地方言服务，为客户解答业务问题。

9.1.2 无障碍服务体系建设

客户端应用软件已建立基于适老版功能、远程银行、智能客服为基础的无障碍服务体系，后期将利用最新技术不断完善客户端应用软件无障碍服务体系。

9.1.3 服务创新

通过使用远程视频以及生物识别技术，在客户端应用软件引入远程银行服务，由远程柜员通过视频为客户办理业务。

9.2 技术创新

9.2.1 指纹特征识别应用

a） 移动金融客户端软件应具备指纹登录功能。
b） 在指纹特征识别系统错误拒绝率≤3%的情况下，客户端软件的错误接受率应≤0.001%。

9.2.2 人脸特征识别应用

a） 移动金融客户端软件应具备人脸登录功能。
b） 在人脸特征识别系统错误拒绝率≤5%的情况下，客户端软件的错误接受率应≤0.01%。

9.2.3 视频客服应用

移动金融客户端应用软件使用远程视频交互技术实现视频客服能力，为客户提供面对面的视频客服服务，为客户远程办理金融业务。