Q/TCJHYH

塔 城 津 汇 村 镇 银 行 企 业 标 准

Q/TCJH 0001-2023

网上银行服务规范

Service standards of internet banking

2023－08－20 发布　　2023－08－20 实施

塔城津汇村镇银行有限责任公司　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由塔城津汇村镇银行有限责任公司提出并归口。

本标准起草单位：塔城津汇村镇银行有限责任公司。

本标准主要起草人：林乐成。

本标准为首次发布。

网上银行服务规范

1 范围

本标准规定了网上银行系统安全规范、客服体验与服务规范、创新性规范。

本标准适用于网上银行系统建设、运营及服务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 32315-2015 银行业客户服务中心基本要求

GB/T 35273 信息安全技术 个人信息安全规范

JR/T 0068-2020 网上银行系统信息安全通用规范

JR/T 0071-2012 金融行业信息系统信息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

3 术语与定义

下列术语和定义适用于本文件。

3.1 网上银行 internet banking

商业银行等金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供的网上金融服务。

3.2 互联网 internet

因特网或其他类似形式的通用性公共计算机通信网络。

3.3 敏感信息 sensitive information

影响网上银行安全的密码、密钥以及交易敏感数据等信息，密码包括但不限于转账密码、查询密码、登录密码、证书的PIN等，密钥包括但不限于用于确保通讯安全、报文完整性等的密钥，交易敏感数据 包括但不局限于完整磁道信息、有效期、CVN、CVN2、证件号码等。

3.4 客户端程序 client program

为网上银行客户提供人机交互功能的程序，以及提供必需功能的组件，包括但不限于：可执行文件、控件、静态链接库、动态链接库等，不包括IE等通用浏览器。

3.5 USB Key

一种USB接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥 以及数字证书。

3.6 USB Key 固件 USB key firmware

影响USB Key安全的内置在USB Key内的程序代码。

3.7 移动终端 mobile terminal

本标准中特指区别于传统PC机方式,以手机、平板电脑等通过通信网络访问网上银行的移动设备。

3.8 强效加密 strong encryption

一个通用术语，表示极难被破译的加密算法。加密的强壮性取决于所使用的加密密钥。密钥的有效长度应不低于可比较的强度建议所要求的最低密钥长度。

3.9 资金类交易 funds transaction

通过网上银行进行资金操作交易，如转账、订单支付、缴费等。本人名下的投资理财、托管账户以及本人签订委托代扣协议的委托代扣等风险可控的资金变动不属于此范畴。

3.10 信息及业务变更类交易 information & business changing transaction

通过网上银行变更客户相关信息或开通、取消业务的交易，如客户修改基本信息、调整交易额度、授权委托交易、修改交易订单、开通（签订）新业务、取消某项业务、电子合同签署、电子保单等。

3.11 企业网银 corporate banking

面向企事业单位和其他组织提供的网上金融服务。

3.12 个人敏感信息 personalsensitiveinformation

一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。 注1:个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行 踪轨迹、住宿信息、健康生理信息、交易信息、14周岁以下(含)儿童的个人信息等。

3.13 客户 customer

已经或将要发生直接或间接关系的对象。

3.14 客服代表 customer service representative （CSR） 座席 agent

客户服务中心前台一线工作人员。

4 符号和缩略语

以下缩略语和符号表示适用于本标准：

CA 数字证书签发和管理机构
Cookies 为辨别客户身份而储存在客户本地终端上的数据
COS 卡片操作系统

C/S 客户机/服务器
DoS/DDoS 拒绝服务/分布式拒绝服务
IDS/IPS 入侵检测系统/入侵防御系统
IPSEC IP 安全协议
OTP 一次性密码
PKI 公钥基础设施
SSL 安全套接字层
SPA/DPA 简单能量分析/差分能量分析
SEMA/DEMA 简单电磁分析/差分电磁分析
TLS 传输层安全
WTLS 无线传输层安全
VPN 虚拟专用网络
IMEI 国际移动设备身份码
IMSI 国际移动用户识别码

5 网上银行服务安全

网上银行技术、管理安全应遵循 JR/T 0071-2012 相关要求。

5.1 安全技术规范

5.1.1 物理安全

机房应选择合理物理位置，采取措施控制访问、防盗窃、防破坏、防雷击、防火、防水、防潮、防静电、控制温湿度、提供电力供应、电磁屏蔽。

5.1.2 网络安全

本项要求包括：

a) 应合理部署网上银行系统的网络架构

- 应合理划分网络区域，并将网上银行网络与办公网及其他网络进行隔离。
- 应在网络边界、所有互联网入口以及隔离区（DMZ）与内部网络之间部署防火墙，对非业务必需的网络数据进行过滤，控制粒度为端口级。
- 应通过合理的路由控制，在柜员终端、运维区域监控终端等业务终端与网上银行服务器之间建立安全的访问路径。
- 应维护与当前运行情况相符的网络拓扑图，并区分可信区域与不可信区域。
- 应采用 IP 伪装技术隐藏内部 IP，防止内部网络被非法访问。
- 应保证主要链路的防火墙、交换机等网络设备的处理能力具备冗余空间，满足业务高峰期需要的 1 倍以上。
- 应建立带宽管理策略，保证互联网带宽具备冗余空间，充分满足业务高峰期和业务发展需要。
- 应通过网络设备 QoS 策略、带宽管理等手段，保证网络发生拥堵时，优先保护网上银行业务流量。

b) 访问控制

- 应在网络结构上实现网间的访问控制，采取技术手段控制网络访问权限。
- 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。

• 应限制 HTTP、FTP、TELNET 等风险较高的协议的使用。如果使用这些协议，应采取补偿的安全控制措施并实现对协议命令级的控制。

• 应在会话处于非活跃一定时间或会话结束后终止网络连接。

• 应限制网络最大流量数及网络并发连接数。

• 在不影响双机切换等情况下，应对重要主机的 IP 地址与 MAC 地址进行绑定，例如，Web服务器、中间件服务器、前置服务器、数据库服务器等主机。

• 应限制只有业务需要的用户才能访问网上银行服务器，控制粒度为单个用户。

• 应禁止开放远程拨号访问。

• 网络设备应按最小安全访问原则设置访问控制权限。

c) 网络设备的管理规范和安全策略

• 将关键网络设备存放在安全区域，应使用相应的安全防护设备和准入控制手段以及有明确标志的安全隔离带进行保护。

• 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术进行身份鉴别。

• 应对登录网络设备的用户进行身份鉴别。身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换：

♦ 至少每 90 天修改一次用户口令

♦ 口令最小长度不低于 8 个字符

♦ 使用包含数字和字母的口令

♦ 不允许提交与上次相同的新口令

• 网络设备用户的标识应唯一。

• 应对网络设备的管理员登录地址进行限制。

• 应禁止将管理终端主机直接接入核心交换机、汇聚层交换机、服务器群交换机、网间互联边界接入交换机和其他专用交换机。

• 应更改网络安全设备的初始密码和默认设置。

• 应指定专人负责防火墙、路由器和 IDS/IPS 的配置与管理，按季定期审核配置规则。

• 应实现设备特权用户的权限分离。

• 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施：

♦ 应通过锁定用户的方式限制连续的访问企图（最多不允许超过 6 次）

♦ 应锁定持续时间至少设定为 30 分钟或直至管理员为其解锁

♦ 如果一个会话空闲的时间超过 15 分钟，应要求用户再次输入口令以重新激活终端

• 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

• 在变更防火墙、路由器和 IDS/IPS 配置规则之前，应确保更改已进行验证和审批。

• 明确业务必需的服务和端口，不应开放多余的服务和端口。

• 应每天对网络设备运行状况进行检查。

• 应定期检验网络设备软件版本信息，避免使用软件版本中出现安全隐患。

• 应每季度检查并锁定或撤销网络设备中多余的用户账号及调试账号。

• 应定期对网络设备的配置文件进行备份，发生变动时应及时备份，确保备份配置文件的安全性。

d) 安全审计和日志

• 应对网络设备的运行状况、网络流量、管理员行为等信息进行日志记录，日志至少保存 6个月。

• 审计记录应包括但不限于：事件发生的时间、相关操作人员、事件类型、事件是否成功及其他与审计相关的信息。

• 应根据记录进行安全分析，并生成审计报表。

- 应对审计记录进行保护，避免被未授权删除、修改或者覆盖：
  - ♦ 只允许具有工作需要的人员查看
  - ♦ 及时备份到集中的日志服务器上或难以更改的介质上
  - ♦ 使用文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警
  - ♦ 每天复审所有系统的日志
- 应采取措施保障关键网络设备时间同步，例如，设置网络时间协议（NTP）服务器。

e）入侵防范

- 应部署入侵检测系统/入侵防御系统（IDS/IPS），对网络异常流量进行监控，监视并记录以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。
- 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标和攻击时间，在发生严重入侵事件时应提供报警或自动采取防御措施。
- 应制订合理的 IDS/IPS 的安全配置策略，并指定专人定期进行安全事件分析和安全策略配置优化。
- 应防范对网上银行服务器端的 DoS/DDoS 攻击。可参考的加固措施包括但不限于：
  - ♦ 与电信运营商签署 DoS/DDoS 防护协议
  - ♦ 防火墙只开启业务必需的端口并开启 DoS/DDoS 防护功能
  - ♦ 使用 DoS/DDoS 防护设备
  - ♦ 使用 IDS/IPS 设备
  - ♦ 使用负载均衡设备

f）边界完整性检查

- 应能够对非授权设备私自联到生产网络的行为进行检查，准确定出位置，并对其进行有效阻断。
- 应对能够访问生产网络的终端私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

g）恶意代码防范

- 应在网络边界部署入侵检测/防护系统、防病毒网关等防病毒设备，对恶意代码进行检测和清除。应定期对恶意代码防护设备进行代码库升级和系统更新。

5.1.3 主机安全

本项要求包括：

a）身份鉴别

- 应对登录操作系统和数据库的用户进行身份标识和鉴别，严禁匿名登录。
- 应为不同的操作系统和数据库访问用户分配不同的账号并设置不同的初始密码，禁止共享账号和密码。
- 应要求系统的静态口令在 8 位以上，由字母、数字、符号等混合组成。
- 首次登录系统时应强制修改密码，至少每 90 天更改一次密码，不允许提交与上次相同的新口令。
- 应有防范口令暴力破解攻击机制。
- 在收到用户重置密码的请求后，应先对用户身份进行核实再进行后续操作。
- 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施：
  - ♦ 通过锁定用户的方式限制连续的访问企图（最多不允许超过 6 次）
  - ♦ 锁定持续时间至少设定为 30 分钟或直至管理员为其解锁 • 应确保对密码进行强效加密保护，不允许明文密码出现。

• 对服务器进行远程管理时，如果数据通过不可信网络传输，应采取加密通信方式，防止认证信息在网络传输过程中被窃听。

• 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。

• 系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。

b）访问控制

• 应根据“业务必需”原则授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

• 应根据管理用户的角色（例如，系统管理员、安全管理员、安全审计员等）分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

• 应实现操作系统和数据库系统特权用户的权限分离。

• 严格限制默认用户的访问权限，重命名系统默认用户，修改默认用户密码，及时删除多余的、过期的用户及调试用户。

• 应严格控制操作系统重要目录及文件的访问权限。

c）安全审计

• 审计范围应覆盖到服务器和管理终端上的每个操作系统用户和数据库用户。

• 审计内容应包括重要用户行为、系统资源的异常使用和重要信息系统命令的使用、账号的创建分配与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件。

• 审计记录应包括时间、类型、访问者标识、访问对象标识和事件结果，保存时间不少于半年。

• 应根据记录数据进行安全分析，生成审计报表，并及时备份到集中的日志服务器上或难以更改的介质上。

• 应保护审计进程，避免受到未预期的中断。

• 应保护审计记录，避免遭受未授权的删除、修改或覆盖：

♦ 只允许具有工作需要的人员查看

♦ 使用文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警

♦ 每天复审所有系统的日志

d）入侵防范

• 应能够检测到对重要服务器进行入侵的行为，包括但不限于主机运行监视、特定进程监控、入侵行为监测和完整性检测等，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

• 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施或在检测到完整性即将受到破坏时进行事前阻断。

• 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，禁用所有不必要和不安全的服务和协议，移除所有不必要的功能。

• 应及时对主要服务器进行补丁升级。

• 应严格限制下载和使用免费软件或共享软件，应确保服务器系统安装的软件来源可靠，且在使用前进行测试。

e）恶意代码防范

• 应安装国家安全部门认证的正版防恶意代码软件，对于依附于病毒库进行恶意代码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，例如主动

防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击。

- 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。
- 应支持防恶意代码工具的统一管理。
- 应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。

f）资源控制

- 应通过设定终端接入方式、网络地址范围等条件限制终端登录，例如部署堡垒机统一管理终端接入。
- 应根据安全策略设置登录终端的操作超时锁定，超时时间应小于 15 分钟。
- 应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况，并提供资源使用异常情况下的报警功能。
- 应限制单个用户对系统资源的最大或最小使用限度。
- 应定期对系统的性能和容量进行规划，能够对系统的服务水平降低到预先规定的最小值进行检测和报警。
- 所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网等客户端操作。
- 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。
- 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。
- 应对重要信息资源设置敏感标记。
- 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

5.1.4 通信安全

本部分内容指数据在网络传输过程中采用的通讯协议和安全认证方式，不包括网络基础设施方面的内容

5.1.4.1 通讯协议

本项要求包括；

a)应使用强壮的加密算法和安全协议保护客户端与服务器之间所有连接，保证传输数据的机密性和完整性，例如，使用 SSL/TLS、IPSEC 和 WTLS 协议。

b) 如果使用 SSL.协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持。cd c)接入“电信网络新型违法犯罪交易风险事件管理平台”

d)采用了较高级别的安全协议，如支持 TLS1.2

e)验证服务器证书有效性(内置公铜证书的方式算)

f)网上银行客户端和服务端之间的通讯加密支付敏感信息

g)客户端和服务端之间的通讯如经过第三方服务器且通信数据中包含支付敏感信息时，有服务端和客户端之间的安全通道(如 VPN 等)

h)采用了国产密码算法

i) 应使用强壮的加密算法和安全协议保护网上银行支付网关与其他应用服务器之间所有连接，保证传输数据的机密性和完整性。

5.1.4.2 安全认证

本项要求包括：

a)网上银行客户踏与服务器应使用安全的协议和强壮的加密算法进行安全、可靠的双向身份认证.双向身份认证是指不仅客户端对服务器身份进行认证，服务器也应认证客户端身份。
b)整个通讯期间，经过认证的通讯线路应一致保持安全连接状态。
c)银行端 Web 服务器应使用权威机构颁发的数字证书以标识其真实性。
d)应确保客户获取的本行 Web 服务器的根证书真实有效，可采用的方法包括但不限于：在客户开通网上银行时分发根证书，或将根证书集成在客户端控件下载包中分发等。
应使用获得国家主管部门认定的具有电子认证服务许可证的 CA 证书及认证服务。

5.1.5 应用安全

本项要求包括：
a)身份鉴别
- 禁止明文显示密码，应使用相同位数的同一特殊字符(例如★和#)代替。
- 密码应有复杂度的要求，包括：
  - 长度至少 6 位，支持字母和数字共同组成
  - 在客户设置密码时，应提示客户不使用简单密码
  - 如右初始密码，首次登录时应得制客户修造初始密码
- 应具有防范暴力破解静态密码的保护措施，例如在登录和交易时使用图形认证码，图形认证码应满足：
  - 由数字和字母等字符混合组成
  - 随机产生
  - 采取图片底纹干扰、颜色变换、设置非连续性及旋转图片字体、变异字体显示样式等有效方式，防范恶意代码自动识别图片上的信息
  - 具有使用时间限制并仅能使用一次
  - 图形认证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容
  - 图片验证过程应该由服务器端进行，应先验证验证码，再验证用户名和密码。
  - 图片验证码长度最低 4 位。
- 使用软键盘方式输入密码时，应采取对整体键盘布局进行随机干扰等方式，防范密码被窃取。
- 应保证密码的加案密钥的安全
- 应采取有效措施防范登录操作的重放攻击，如在登录交互过程提交的认证数据中增加服务器生成的随机信息成分
- 应可判断客户的空闲状态，当空闲超过一定时间后，自动关闭当前连接，客户再次操作时会话标识应随机并且唯一，会话过程中应维持认证状态，防止客户通过直接输入登录后的地址访问登录后的页面。
- 应禁止在客户端缓存密码、密钥等敏感信息，例如，在包含上述信息的页面设置禁止缓存参数，防范未授权用户通过浏览器后退等方式获取敏感信息。
- 退出登录或客户端程序、浏览器页面关闭后，应立即终止会话，保证无法通过后退、直接
- 退出登录时应提示客户取下专用安全设备，例如 USB Key。
- 修改客户敏感参数(例如，密码、转账限额等)时，应再次认证客户身份。
- 显示客户身份证件信息时，应屏蔽部分关键内容。
- 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。
- 用户认证失败的提示应该模糊处理，不应明确提示 “用户名不存在”或“密码错误’
- 地址、机器码等，如发生变化，应再次对客户身份进行认证，否则服务器端自动终止会话。应保证

用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中

b)访问控到

- 应建立安全的访问控制机制，防止用户访问无权访问的功能或资源，例如越权访问他人账
- 号的信息，在低级别的认证方式下访问高级别认证方式才能访问的功能等
- 台设置，操作员由管理员设置，操作员权限应根据录入、复核、授权职责分离的原则设置应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关
- 应建立完善的交易验证机制，每次处理的客户信息均以服务端数据为准，并对客户请求指令的逻辑顺序进行合理控制
- 应每季度检查并锁定或撤销应用系统及数据库中多余的、过期的用户及调试用户。

c)安全审计

- 应具有保存和显示客户历史登录信息(例如，时间、IP 地址、MAC 地址等)的功能，支持客户查询登录(包括成功登陆和失败登录)，交易等历史操作
- 应具有详细的交易流水查询功能，包括但不限于日期、时间、交易卡号、交易金额和资金余额等信息。
- 审计功能应覆盖所有对网上银行数据的管理操作，包括用户开通、证书发放、密码修改冻结解冻、权限变更等操作，应对用户开通、专用安全设备更换、重要信息变更、冻结解冻等重要操作进行稽核。
- 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，并定期各份审计记录，保存时间不少于半年。
- 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。
- 合理分配交易日志的管理权限，禁止修改日志，确保日志的机密性、完整性和可用性

d) 软件容错

- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长
- 度符合系统设定要求。
- 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。

e)资源控制

- 应能够对系统的最大并发会话连接数进行限制。
- 应能够对单个用户的多重并发会话进行限制。
- 应能够对一个时间段内可能的并发会话连接数进行限制。
- 应用系统通信双方中的一方在指定时间内未作任何响应，另一方应能够自动结束会话。应能够对一个访问账户或者一个请求进程占用的资源分配最大限额和最小限额。
- 应能够对系统服务水平降低到预先规定的最小值进行检测和报警。
- 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。
- 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。
- 应具有对重要信息资源设置敏感标记的功能。
- 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作

f) Web 应用安全

- 防范敏感信息泄露
  - 在网上银行系统上线前，应删除 Web 目录下所有测试脚本、程序

- 如果在生产服务器上保留部分与 Web 应用程序无关的文件，应为其创建单独的目录，使其与 Web 应用程序隔离，并对此目录进行严格的访问控制。
- 禁止在 Web 应用程序错误提示中包含详细信息，不向客户显示调试信息。
- 禁止在 Web 应用服务器端保存客户敏感信息。
- 应对网上银行系统 Web 服务器设置严格的目录访问权限，防止未授权访问.统一目录访问的出错提示信息，例如对于不存在的目录或禁止访问的目录均以“目录不存在”提示客户。
- 禁止目录列表浏览，防止网上银行站点重要数据被未授权下载。
- 敏感信息在应用层保持端到灌加密，即保证数据在从源点到终点的过程中始终以密文形式存在。

- 防范 SQL 注入攻击
  - 网上银行系统 Web 服务器应用程序应对客户提交的所有表单、参数进行有效的合法性
  - 判断和非法字符过滤，防止攻击者瑟意构造 SQL 语句实施注入攻击。
  - 禁止仅在客户端以脚本形式对客户的输入进行合法性判断和参数字符过滤。数据库应尽量使用存储过程或参数化查询，并严格定义数据库用户的角色和权限。
- 防范跨站脚本攻击
  - 应通过严格限制客户端可提交的数据类型以及对提交的数据进行有效性检查等有效措施防止跨站脚本注入。
  - 应对 Web 页面提供的链接和内容进行控制，定期检查外部链接和引用内容的安全性。应采取网站页面防篡改措施，例如部署网页防篡改系统等。
  - 应采取有效措施防范由于客户使用第三方浏览器(例如手机平台浏览器)带来的敏感信息泄露、交易数据篡改等重要信息安全风险。

g)防钓鱼

- 应具有防网络钓鱼的功能，例如，显示客户预留信息、使用预留信息卡、客户自定义个性化界面等。
- 应采取防钓鱼网站控件、钓鱼网站监控工具、钓鱼网站发现服务等技术措施，及时监测发现钓鱼网站，并建立钓鱼网站室件报告及快速关闭钓鱼网站的处置机制。
- 应加强防钓鱼的应用控制和风险监控措施，例如，增加客户端提交的 Referer/IP 信息的枝验、设置转康白名单等。
- 采用已有的和 E 或其它浏览器相关联的可信网址的认证机制，保证登录的 UL 经过第二方权威机构的安全认证。

h) 域名解析服务

- 域名继析系统应不间断运行，在挂除不可抗因素的情况下，按月统计，权威服务器和递归服务器业务可用性均应大于 99.99%
- 递归服各器自身不应同时兼各积威服务器功能，同时不提供除了域名服务之外的其触服务：对权威域名服务系统，应保持主服务器对辅服务器(组)的记录信息进行更新，保证数据同步。
- 应采用内外网隔离或加密等保护措施避免远程访问和域名数据在公共互联网的明文传输。
- 应建立对关键数据和重要信息进行各份和恢复的管理和控制机制，关键数据包括但不限干域名系统架构、域名解析软件及配置、域名区文件、域名解析日志、域名系统监控数据。
- 如采用委托第三方运营的域名解析系统，应要求其提供与自建域名解析系统相同的安全防护要求。

5.1.6 客户端安全

5.1.6.1 客户端程序

本项要求包括：

a)应采取有效技术措施保证客户端处理的敏感信息、客户端与服务器交互的重要信息的机密性和完整性：应保证所提供的客户端程序的真实性和完整性，以及敏感程序逻辑的机密性，
b)客户端程序上线前应进行严格的代码安全测试，如果客户端程序是外包给第三方机构开发的，应要求开发商进行代码安全测试。应建立定期对客户端程序进行安全检测的机制。
c)客户端程序应通过指定的第三方中立测试机构的安全检测，每年至少开展一次。
d)应对客户端程序进行签名，标识客户端程序的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构。
e)客户端程序在启动和更新时应进行真实性和完整性校验，防范客户端程序被篡改或替换。f)客户端程序的临时文件中不应出现敏感信息，临时文件包括但不限于 Cookies。客户端程序应禁止在身份认证结束后存储敏感信息，防止敏感信息的泄露。
g)客户端程序应提供客户输入敏感信息的即时加密功能，例如采用密码保护控件。
h)客户端如果集成了第三方 SDK，严禁 SDK 进行热更新操作。
i)客户登录后的首页，应在合适位置显示客户上次登录的信息，如上次登录的时间、ip 地址等信息。当系统发现登录异常时，采用合适的界面提示客户注意。
i)在输入敏感信息时，禁用键盘缓存，并禁用复制/粘贴功能。比如密码输入。
k)应用密钥不得直接硬编码到程序代码中。
l)客户端必须控制申请采集的权限，不得侵犯客户隐私或申请不必要的权限。
m)客户端程序且有明确的应用标识符和版本序号。
n)对用户输入信息采取逐字符加密、自定义软键盘，防范键盘窃听技术等措施。
o)在本地存储用户的支付敏感信息。
p)有密钥安全保护机制。
q)客户端应用软件在收集、使用客户信息之前，明示收集、使用信息的目的、方式和范围，公开其收集、使用规则，并取得客户的明示同意。
下面的条款只针对 PC 客户端；
a)客户端程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和慕改。
b)客户端程序应防范恶意程序获取或篡改敏感信息，例如使用就览器接口保护控件进行防范。
c)客户端程序应防范键盘窃听敏感信息，例如防范采用挂钩 Windows 键盘消息等方式进行键盘窃听，并应具有对通过挂钩窃听键盘信息进行预警的功能。
d 客户端程序应保护在客户端启动的用于访问网上银行的进程，防止非法程序获取该进程的访问权限。
e)客户端程序应采用反屏幕录像技术，防范非法程序获取敏感信息。
下面的条款只针对移动终端客户端：
a)客户端程序应提供敏感信息机密性、完整性保护功能，例如采取随机布放按键位置、防范键盘窃听技术、计算 MAC 校验码等措施。
b)客户端程序应采取代码混淆等技术手段，防范攻击者对客户端程序的调试、分析和篡改。c)客户端程序开发设计过程中应注意规避各终端平台存在的安全漏洞，例如，按键输入记录、自动拷屏机制、文档显示缓存等。
d)采用生物识别技术，生物识别技术是否符合标准要求。
e)支持多种登录方式。
f)支持手势密码。
g)支持人脸识别，人脸识别具备活体检测能力。
h)支持对设备 MAC 的识别。
i)根据不同的场景、客户组合不同认证手段。

j)大额支付支持人工回呼确认。
k)支持对操作环境 IP/LBS/经纬度识别。
1)对设备标识的识别。
m)对更换设备登录做加强身份校验。
n)对操作设备及环境存在同机多账户判断。

5.1.6.2 客户端环境安全

本项要求包括：
a)应采取有效措施提升客户端环境安全级别，例如，在线杀毒服务、安全检测工具等，并在显著位置予以提醒。
b)当发现客户端平台存在重大安全缺陷或安全威胁时，应在门户站点发布警示通知，并通过短信、邮件等方式警示客户。

5.1.7 与外部系统连接安全

本项要求包括：
a)应使用具有电子认证服务许可证的证书颁发机构颁发的数字证书，并使用经国家密码主管部门认定的签名算法，对报文嶺要数据进行规范化处理后，进行数字签名。
b)发往外部机构的报文应进行传输加密，加密信息应包括报文中的关键信息和客户敏感信息。

5.1.8 数据安全

本项要求包括：
a) 数据完整性
- 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
- 应能够检测到系线管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复猜施。

b) 数据保密性
- 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。
- 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

c) 备份和恢复
- 应建立重要数据的定期数据备份机制，至少做到增量数据备份每天一次，完整数据备份每周一次，并将备份介质存放在安全区域内，数据保存期限依照国家相关规定。
- 数据备份存放方式应采用多冗余方式,完全数据备份至少保证以一个星期为周期的数据冗余
- 核心层、汇聚层的设备和重要的接入层设备均应双机热备，例如，核心交换机、服务器群接入交换机、重要业务管理终端接入交换机、核心路由器、防火墙、均衡负载器、带宽管理器及其他相关重要设备。
- Web 服务器、中间件服务器、前置服务器、数据库服务器等关键数据处理系统均应双机热备或多机集群，并设置磁盘冗余阵列以避免单一部件故障影响设备运行的风险。
- 应提供冗余遗信线路，遵照与主用通讯线路不同运营商和不同物理路径的原则选择冗余进讯线路。应对关键数据进行同城和异地的实时备份，保证业务应用能够实现及时切换。
- 个人信息安全应遵循 GB/T 35273-2017 相关要求。

5.2 安全管理规范

本项要求包括：

a)应制定安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案。

b) 应在网上银行统一的应急预案框架下，制订针对不同事件的应急预案，应急预案至少包括各类事件场景下启动应急预案的条件、应急处理流程、系统恢复流程、事件信息收集、分析、报告制度、事后经验总结和培调等内容。

5.3 5.3 业务运作安全规范

5.3.1 业务申请及开通

a)应充分考虑并采取有效措施防范网上银行资金类交易开通的安全风险。网上银行资金类交易的开通必须由客户本人到柜台申请，申请时，应对其进行风险提示，验证客户的有效身份，并要求客户书面确认，客户通过已采取电子签名验证的网上银行渠道申请资金类交易的，视同客户本人主动申请并书面确认。以下资金类交易可不受上述限制；开通同一客户账户之间转账并且本行能有效识别转入、转出方为同一客户账户的,客户预先通过柜台签约对转入账户进行绑定同时指定交易电话的。

b) 网上银行资金类业务关闭后，重新申请开通该功能，必须要求客户本人持有效身份证件到柜台或采取电子签名验证的网上银行渠道申请。采取网上银行渠道申请时，应通过验证发向可靠的预留手机号码的短信验证码等方式，请求客户本人对业务重新开通操作进行确认，

c) 企业网上银行开通必须由本企业人员到柜台申请，应审查其申请材料的真实性、完整性和合规性。

d) 企业网上银行客户加挂账户可通过柜台或通过需使用专用安全设备工具进行身份认证的双人复核机制后方可增加，同时应通过有效方式请求企业联系人确认。注销企业网上银行服务、重置专用安全设备工具密码必须到柜台办理。

e)通过手机终端访问网上银行的资金类交易开通必须有效验证客户身份，客户应通过柜台或者通过已采取电子签名验证等安全认证手段的网上银行渠道主动申请。在柜台办理签约时，应验证客户有效身份信息、银行账户密码等信息。应建立手机号和银行账户的关联关系，例如手机号与客户身份证绑定、手机号与客户银行账户信息绑定等，采用移动终端硬件加密模块的，应建立硬件加密模块与客户身份证或银行账户信息的关联关系。通过网上银行渠道申请时，应采取双因素身份认证验证客户的真实身份及银行卡交易密码，并通过验证发向可靠的预留手机号码的短信验证码等方式，请求客户本人对交易开通操作进行确认。

f) 如果网上银行登录密码以密码信封方式发送给客户或者初始登录密码由本行设置，应强制客户首次登录时修改初始密码。

g)客户重置登录密码及支付密码时，必须通过柜台或者通过已采取电子签名验证等安全认证手段的网上银行渠道申请。通过网上银行渠道申请时，本行必须采取双因素身份认证有效验证客户的真实身份，并通过验证发向可靠的预留手机号码的短信验证码等方式，请求客户本人对密码重置操作进行确认。

h)申请客户数字证书时，应验证公钥的有效性，证书签名请求在进入 SSL 通道前应采取安全保护措施。

i)下载客户数字证书时，应有身份认证的过程。通过提交授权码和参考码等方式保证客户数字证书只能被下载一次，身份认证信息应设置有效期，超出有效期而未下载证书，应重新办理。

j)客户申请 USB Key 作为数字证书载体或申请其他安全设备时，应持有效身份证件到柜台办理，应采取将安全设备序列号与客户信息进行绑定等措施，并在客户下载证书时将其作为客户身份认证因素之一，以防止证书被冒下。如果安全设备丢失，应持有效证件到柜台重新办理，原有安全设各和客户绑定关系解除。

k)网上银行专用安全设备在暂停、终止、挂失或注销后，如需要恢复、解除挂失需客户本人持有效身份证件到柜台或通过本行客服电话办理，应核实客户信息、网银账户信息并对预留手机号码进行验证。

5.3.2 业务安全交易机制

5.3.2.1 身份认证

本项要求包括：：

a)应按照市慎原则，采取有效、可靠的身份认证手段，保证资金类交易安全。

b) 网上银行资金类交易、重要信息及业务变更类等高风险业务应使用双因素身份认证。双因素身份认证由以下两种身份认证方式组成：一是客户知晓、注册的客户名称及密码。二是客户持有。特有并用于实现身份认证的信息，包括但不限于物理介质或电子设备等。以下资金类交易可不受上述限制：同一客户账户之间转账并且本行能有效识别转入、转出方为同一客户账户的。

c)禁止仅使用文件证书或使用文件证书加静态密码的方式进行资金类交易。

d) 使用企业网上银行进行资金类交易时，应至少使用硬件承载的数字证书进行签名等安全认证方式。

e)应采取有效措施引导客户设置与银行卡交易密码不同的网上银行登录、交易密码，使用不相同的登录密码及交易密码。

f) 客户登录网上银行时或登录后执行账户资金操作时，若身份认证连续失败超过一定次数(不超过 10 次)，应在短时间内锁定该客户网上银行登录权限或交易账户使用权限，并立即通过短信或申话等可靠的方式通知客户

g)本行用于发送网上银行交易提示短信、动态验证码等信息的客户预留手机号码变更时应符合下列要求之一：客户持有效身份证件到柜台办理；客户通过网上银行渠道变更预留手机号码，本行必须采取双因素身份认证验证用户的真实身份及银行卡交易密码，并通过验证发向原预留手机号码的短信验证码等可靠的方式，请求客户本人对预留手机号码变更操作进行确认。

如果通过网上银行系统开展网上支付业务，还应满足如下条款：

h)网上银行系统接受商户或非金融支付机构的系统建立连接请求时，应通过验证其服务器数字证书、预留 IP 地址比对等方式认证其系统的身份。应对网上银行系统和商户或第三方系统之间发送和接收的信息采用数字证书机制进行签名及验签，保证交易数据的完整性和不可抵赖性。

5.3.2.2 交易流程

本项要求包括：

a)应充分考虑、深入分析交易全流程的安全隐患，通过交易确认、交易提醒、限额设定等控制机制，有效防范交易风险。

b)资金类交易中，应具有防范客户端数据被篡改的机制，应由客户确认资金类交易关键数据（至少包含转入账号和交易金额)，并采取有效确认方式以保证待确认的信息不被篡改，例如，通过发送包含确认信息的短信验证码、在 USB Key 内完成确认等。

c) 资金类交易中，如果客户端对交易数据签名，签名数据除流水号、交易金额、转入账号、交易日期和时间等要素外，还应包含由服务器生成的随机数据。对于从网上银行客户端提交的交易数据，服务器应验证签名的有效性并安全存储签名。

d) 通过移动终端提交交易请求时，应采取有效措施鉴别客户身份，保证敏感信息和交易数据的机密性、完整性，并设置与安全防护能力相适应的交易限额以控制交易风险。通过移动终端客户端程序提交交易请求时，应上送终端相关信息，例如，IMEI、IMSI 等。后台服务器应对编号信息和登记信息进行一致性验证。如果对交易数据签名，签名数据应包含此类信息。

e) 在客户确认交易信息后，再次提交交易信息（例如收款方、交易金额)时，应检查客户确认的信息与最终提交交易信息之间的一致性，防止在客户确认后交易信息被非法篡改或替换。

f)资金类交易中，应对客户端提交的交易信息间的隶属关系进行严格校验，例如验证提交的账号和卡号间的隶属关系以及账号、卡号与登录用户之间的关系。

g) 本行可根据自身情况界定高风险业务及其风险控制规则，对于资金类交易等触发风险控制规则的情

况，应使用可靠的第二通信渠道请求客户反馈确认交易信息。

h)对于资金类等高风险业务，应在确保客户有效联系方式前提下，充分提示客户相关的安全风险并提供及时通知客户资金变化的服务，实时告知客户其资金变化情况。

i)应采取适当的安全措施确保客户对所做重要信息及业务变更类交易的抗抵赖。

j)应根据业务类别、开通渠道及身份验证方式的不同设置不同的交易限额，同时允许客户在银行设定的限额下自主设定交易限额。

如果通过网上银行系统开展网上支付业务，还应满足如下条款：

a)本行在与商户及非金融支付机构合作时，应采取有效措施保证交易指令的安全性，并要求商户和非金融支付机构提供必要的订单信息，以用于客户交易确认，保障支付交易安全。

b)支付网关应对交易订单的唯一性进行检查，防止订单重复支付。

c)通过可靠的数字签名等机制保证订单信息的真实性、完整性，验证订单的有效性并存储订单，防止交易篡改、伪造订单等。

d)应与商户、非金融支付机构配合，在资金拨付前，校验、确认支付相关信息，以防范木马篡改或替换订单导致持卡人资金损失的风险，可采取的措施包括但不限于以下内容；

- 支付网关向客户发送确认信息，其中包含在商户网站生成的订单号，并提醒客户到商户网站确认此订单号对应的详细信息和所选购商品的一致性。
- 商户或非金融支付机构向客户确认订单信息的真实性和完整性，支付网关验证订单信息和支付用户信息的关联性，确保订单提交人与支付用户的一致性(代付情况除外)。例如，在生成订单时，商户或非金融支付机构应要求客户提交其银行账户绑定的手机号码，并将此手机号码作为订单信息的字段，商户或非金融支付机构向此手机号码发送确认消息(包含但不限于商户名称、商品类别、交易金额、收货人标识、订单提交人的客户标识等)，并将手机号码及订单关键信息(例如订单编号、订单金额)提交到支付网关，支付网关在进行划款支付时验证手机号码和客户银行账户的绑定关系。
- 本行提供可显示交易信息及计算校验码的第三方插件供商户调用，此插件对客户的关键订单信息(包含但不限于商户名称、商品类别、交易金额、收货人标识、订单提交人的客户标识等)计算校验码，并将此校验码作为唯一标识上送到支付网关，支付网关在和客户的确认消息中包含此校验码，并提醒客户到商户网站手工计算校验码并进行比对。
- 支付网关向客户发送确认信息，其中包含关键订单信息，客户据此确认订单的真实性和完整性，订单信息包含但不限于：非金融支付机构名称、商户名称、商品类别、交易金额、收货人标识、订单提交人的客户标识。

e) 订单信息中应包含商品类别信息，能够标识商品的实体状态（实物或虚拟）。对虚拟类商品：

- 应要求商户提供收货人地址或收货人标识，在支付界面上提供收货人地址或收货人标识供客户确认。
- 设置支付限额，超过支付限额，拒绝交易。
- 通过可靠的第二渠道向客户确认支付请求信息。

f)应设置网上支付类交易风险监控规则（例如交易限额和交易频率），对于触发风险监控规则的交易，应通过可靠的第二通信渠道发送确认消息，客户确认信息包含应至少包含关键订单信息或者订单标识信息(例如订单编号、订单校验码)、交易金额以及收款方名称。

g)支付网关在确认支付前，应向客户提示支付风险。

h)支付网关应准确完整记录交易的支付请求信息，例如，商户编号、商户名称、非金融支付机构名称、商户订单号、交易金额、交易日期及时间等。

i) 支付网关应准确完整记录交易的支付结果信息，例如，支付时间、交易金额、支付方式、付款方、收款方、支付状态等。

j)应禁止在支付网关应用系统的日志中保存敏感账户信息。

k) 应要求支付网关连接的商户和非金融支付机构采用可靠的密钥保护机制，例如采用专门的硬件加密设备，用来保存认证密钥。
1)应根据“业务必需”原则与商户、非金融支付机构及其他本行共享信息，本行未经客户直接授权，不得与其他机构共享客户的敏感信息，不得保存其他机构客户的敏感信息。
m) 如果商户和非金融支付机构系统参与敏感信息的处理，应禁止存储客户的敏感信息；对因业务需要存储的交易数据，应采取严格的访问控制措施。

5.3.2.3 交易监控

本项要求包括：
a) 应根据自身业务特点，建立完善的网上银行异常交易监控体系，识别并及时处理异常交易，交易监测范围至少包括客户签约、登录、查询、资金类交易以及与交易相关的行为特征、客户终端信息，应保证监控信息的安全性。
b)应制定网上银行异常交易监测和处理的流程和制度。
c)应根据审慎性原则，对于交易要素不完整、超过额度的转账支付和关注类账户的资金流动(例如疑似违规资金变动)等交易进行人工审核。
d) 应根据交易的风险特征建立风险交易模型，以此为基础，建立风险交易监控平台，对单个 IP 的异常登录尝试、短时间内单个账户在异地多笔交易、外部欺诈、身份冒用、套现、洗钱等异常情况进行有效监控并对检测到的可疑交易建立报告、复核、查结机制。
e) 应建立异常交易识别规则和风险处置机制，对监控到的风险交易进行及时分析与处置。f)本行的风险交易监控系统应通过分析用户交易习惯和群体用户行为习惯，提高交易分析的效率和准确率。
g) 本行的风险交易监控系统应通过分析欺诈行为特征创建反欺诈规则，对交易数据实时分析，根据风险高低产生预警信息，从而实现欺诈行为的侦测、识别、预警和记录。
h)本行的风险交易监控系统应能够不断更新反欺诈规则，能够实现各本行、主管部门和公安机关等机构间的信息共享和信息交换，完善反欺诈系统。
i)支持实时高效地监测和控制客户交易欺诈风险。

5.4 安全认知

5.4.1 数据透明可追踪

在网上银行操作过程中，客户提交的交易信息及各类出错信息都会清晰地显示在屏幕上，让客户清楚地了解该笔交易的详细信息。提供从登录、查询、交易等环节的短信或微信提醒服务，使用户随时掌握网上银行使用情况，

5.4.2 关键环节安全设计

本项要求包括：
a)首次登录网上银行时，强制要求用户修改在柜台签约时预留的登录密码，并对密码强度进行检测，要求客户不能使用简单密码。
b) 登录时对包括登录密码等身份认证错误次数进行了限制，超出限制次数，客户当日即无法进行登录，并通过短信或微信等可靠的方式通知客户。
c)资金类交易对包括交易密码等身份认证错误次数进行了限制，超出限制次数，对账户进行锁定，并通过短信或微信等可靠的方式通知客户。
d)资金类交易根据业务类别、开通渠道及身份验证方式的不同设置不同的交易限额，输入的交易金额超

限，提交时对客户进行提示。

5.5 服务连续在线可信性要求

本项要求包括：
a)应制订网上银行业务连续性策略及计划。
b)应将网上银行业务连续性管理整合到组织的流程和结构中，明确指定相关部门负责业务连续性的管理。应制订员工在网上银行业务连续性方面的培训计划和考核标准。
d)根据网上银行系统的业务影响性分析结果，制定不同数据的备份策略，并实施应用级备份，以保证灾难发生时，能尽快恢复业务运营。应定期测试并更新网上银行业务连续性计划与过程。
f)网上银行系统服务时间应满足 7*24 小时不间断运行。
g)应配备 7*24 小时运维应急人员。
h)WODH 网上银行系统可用率应大于 99.99%。
i)数据丢失时间 RTP 为 0，系统恢复时间小于 30 分钟。
j)系统及应用可用性监控覆盖了大于等于 99%。
k)网上银行系统应按照同城双活架构进行部署。

5.6 增强身份认证要求

5.6.1 USB Key

本项要求包括：
a)应使用指定的第三方中立测试机构安全检测通过的 USB Key.
应采取有效措施防范 USBKey 被远程挟持，例如通过可靠的第二通信渠道要求客户确认交易信息等。
b)应在安全环境下完成 USB Kev 的个人化过程
c)USB Key 应采用具有密钥生成和数字签名运算能力的智能卡芯片，保证敏感操作在 USB Key 内进行。
d)USB Key 的主文件(Master File)应受到 COS 安全机制保护，保证客户无法对其进行删除和重建。
e)应保证私钥在生成、存储和使用等阶段的安全：

- 私钥应在 USB Key 内部生成，不得固化密钥对和用于生成密钥对的素数。
- 应保证私钥的唯一性。
- 禁止以任何形式从 USB Kev 读取或写入私钥。
- 私钥文件应与普通文件类型不同，应与密钥文件类型相同或类似。
- USB Key 每次执行签名等敏感操作前均应经过客户身份鉴别。
- USB Key 在执行签名等敏感操作时，应具备操作提示功能，包括但不限于声音、指示灯、屏幕显示等形式。

f)参与密钥、PIN 码运算的随机数应在 USB Key 内生成，其随机性指标应符合国际通用标准的要求。
g)密钥文件在启用期应封闭。
h)签名交易完成后，状态机应立即复位。
i)应保证 PIN 码和密钥的安全：

- 采用安全的方式存储和访问 PIN 码、密钥等敏感信息
- 经客户端输入进行验证的 PIN 码在其传输到 USB Key 的过程中，应加密传输，并保证在传输过程中能够防范重放攻击，
- PIN 码连续输错次数达到错误次数上限(不超过 10 次)，USB Key 应锁定

- 同一型号 USB Key 在不同银行的网上银行系统中应用时，应使用不同的根密钥，且主控密钥、维护密钥、传输密钥等对称算法密钥应使用根密钥进行分散。

j)USB Kex 使用的密码算法应经过国家主管部门认定

k)应设计安全机制保证 1SR Kev 取动的安全，防被算改或换掉

l) 对 USB Key 固件进行的任何改动，都必须经过归档和审计，以保证 USB Key 中不含隐藏的非法功能和后门指令。

m)USB Key 应具备抵抗旁路攻击的能力，包括但不限于：

- 抗 SPA/DPA 攻击能力
- 抗 SEMA/DEMA 攻击能力

n)在外部环境发生变化时，USB Key 不应涯露敏感信息或影响安全功能。外部环境的变化包含但不限于；

- 高低温
- 高低电乐
- 强光干扰
- 电磁干扰
- 紫外线干扰
- 静电干扰
- 申压毛刺干扰

o)USB Kes 应能够防远程挟持且有屏幕显示或语音提示以及按键确认等确认功能，可对交易指

p)USB Key 应能够自动识别待签名数据的格式，识别后在屏幕上显示或语音提示交易数据，保证屏幕显示或语音提示的内容与 USB Key 签名的数据一致。

r) 未经按键确认，USB Key 不得签名和输出，在等待一段时间后，可自动清除数据，并复位状态。

s)USB Key 应能够自动识别其是否与客户端连接，应具备在规定的时间与客户端连接而未进行任

t)USB Key 在连接到终端设备一段时间内无任何操作，应自动关闭，必须重新连接才能继续使用，以防范远程挟持

5.6.2 文件证书

本项要求仅针对 C/S 模式客户端：

a)避免对个人网上银行客户的同业务麗发老个有效证书。

b)用于签名的公私钥对应在客户端生成禁止由服务器生成。私钥只允许在客户端使用和保存。c)应保证私钥的唯一性。

d)应强制使用密码保护私钥，防止私朝受到未授权的访问

e)应支持私钥不可导出选项

f) 私钥导出时，客户端应对客户进行身份认证，例如验证访问密码等

g)私钥备份时，应提示或强制放在移动设备内，各份的私钥应加密保存。

h)在各份或恢复私钥成功后，应通过可靠的第二通信渠道向客户发送提示消息

i)文件证书应与计算机主机信息绑定，防范证书被非法复制到其他机器上使用。

j)应采用验证码对关键操作(例如签名)进行保护，防范穷举攻击，

5.6.3 0TP 令牌

本项要求包括，

a) 应使用指定的第三方中立测试机构安全检测通过的 OTP 令牌设备及后台支持系统 b) 应 b)采取有效措施防范 OTP 令牌被中间人攻击，例如通过可靠的第 通信渠道要求客户确认交易信息等。

c) 应采取有效措施保证种子密钥在整个生命周期的安全，

d)口令生成算法应经过国家主管部门认定。
e)动态口令的长度不应少于 6 位。
f)应防范通过物理攻击的手段获取设备内的敏感信息，物理攻击的手段包括但不限于开盖，搭线、
g)OTP 令牌应具备抵抗旁路攻击的能力，包括但不限于：

- 抗 SPA/DPA 攻击能力
- 抗 SEVA/DEMA 攻击態力

h) 在外部环境发生变化时，OTP 令牌不应泄露敏感信息或影响安全功能。外部环境的变化包含但不限于：

- 高低温
- 强光干块
- 电磁干扰
- 紫外线干扰
- 静电干扰

i)对于基于时间机制的 OTP 令牌，为了时间同步，应在服务器端设置认证 OTP 密码的时间窗口，认证服务器可以接受的 OTP 密码时间窗口越小，口令被误用的风险越小，应设置此时间窗口最大不超过口令的理论生存期前后 60 秒（理论生存期是指如果令牌和服务器时间严格一致，令牌上出现口令的时间范围)，结合应用实践，设置尽可能小的理论生存期，以防范中间人攻击。
j)采用基于挑战应答的 OTP 令牌进行资金类交易时，挑战值应包含用户可识别的交易信息，例如转入账号、交易金额等，以防范中间人攻击。
k)如使用 OTP 令牌，登录和交易过程中口令应各不相同，且使用后立即失效。
l)OTP 令牌设备应使用 PIN 码保护等措施，确保只有授权客户才可以使用。
m)PIN 码和种子应存储在 OTP 今魏设备的安全区域内或使用其他措施对其进行保护
n)PIN 码连续输入错误次数达到错误次数上限(不超过 6 次)，OTP 令牌应锁定

5.6.4 动态密码卡

本项要求包括：
a)动态密码卡应与客户噫一绑定。
b)应使用涂层覆盖等方法保护口今。
c) 服务器端应随机产生口令位置坐标。
d)动态口令的长度不应少于 6 位。
e)应设定动态密码卡使用有效期，超过有效期应作废。
f)动态密码卡应具备有效使用次数。

5.6.5 短信动态密码

本项要求包括，
a)开通手机动态密码时，应使用人工参与控制的可靠手段验证客户身份并登记手机号码。更改于
b)交易的关键信息应与手机动杰密码一起发送给客户，并提示客户确认，
c)手机动态密码应随机产生，长度不应少于 6 位。
d)应设定手机动态密码的有效时间，最长不超过 6 分钟，超过有效时间应立即作废。
e)应采取有效措施防范恶意程序窃取、分析、篡改短信动态密码，保证短信动态密码的机密性和完整性，例如结合外部认证介质(如密码卡等)、采用问答方式等。

5.6.6 指纹识别

本项要求包括：
a)如里通过指约鉴制客户自份，旋防止拔的数据被记录和重放
b)禁止在远程身份鉴别中采用指纹识别。近距离身份鉴别(例如使用专用安全设备对使用者的身份鉴别)可采用指纹识别

5.7 风险控制能力

本项要求包括，
a)网上银行风险管理应纳入全行的风险管理体系，并根据业务发展阶段进行动态调整和修正。b)网上银行风险管理应以流程控制为主线，主要流程有风险监测、风险识别、风险控制、风险处置和风险评估。
c) 应建立网上银行交易风险监控系统，持续、及时对客户网上交易进行监控，发现可疑或异常交易后，快速响应处理，尽可能避免、减少或挽回客户损失；
d) 网上银行交易风险监控系统监控规则应至少包括且黑名单规则、反洗钱规则、异常操作规则等
e) 应在深入分析客户操作及交易行为的基础上，审慎处理，发出准确的风险提示；
f)监控机构和人员应对监控规则、风险特征、风险状况、客户数据等关键信息要严格保密，不得向无关人员泄露

6 网上银行客户体验

6.1 基本要求

应设立全国统一客服电话 xxxx，为客户提供电话自助语音和人工服务

6.2 客户服务响应

本项要求包括：
a) 电话客服平均响应时间(转接人工客服后到人工客服接通平均时间)≤15 秒。
b) 线上客服平均响应时间≤10 秒
c) 人工客服服务时间 7×24 小时。
d) 电话客服接通率≥95%。
e)APP 闪退率(一天中发生闪退的设备数/益体活跃设备数) ≤0.05%。

6.3 客户代表行为及客户投诉

本项要求包括：
a)客户代表行为及客户投诉应遵循 GB/T 32315-2015 相关要求
b)客户投诉处理应坚持“以客户利益优先，公平、透明、合理、高效”的原则。

6.4 客户教育及权益保护

本项要求包括：
a)应切实加强客户教育和风险提示，向客户详细解释本机构网上银行业务流程和安全控制措施，在网银新产品(业务)推出、相关业务(操作)流程变更、安全控制措施变化时，及时告知客户。
c)应通过各种宣传渠道向大众提供正确的网上银行官方网址和呼叫中心号码，提示客户牢记本行官方网站地址和呼叫中心号码。
d) 应向客户印发通俗、易懂的网上银行信息安全宣传手册，在网上银行官方网站首页显著位置开设信

息安全教育栏目。
e) 应向客户明确提示网上银行相关的安全风险和注意事项，并根据网上银行安全形势的变化，及时更新相关事项，包括但不限于提示客户不在非自主可控的终端上登录网上银行，维护良好的客户端环境，及时更新操作系统及浏览器补丁，安装并更新客户端防病毒软件，避免设置与客户端常用软件相同的网上银行登录及交易密码，避免将本人网上银行登录及交易等敏感信息告知他人，避免将本人的网上银行专用安全设备转借他人使用，在网上银行操作完成后立即退出相关界面并及时拔下与终端相连的专用安全设备，不安装或运行来历不明的客户端软件和程序，不打开陌生人发送的电子邮件及其附件或网站链接，谨防虚假网上银行链接，注意对网上银行的敏感信息进行保护等内容。
f)应建立网上银行相关的侵犯客户权益行为的处置机制，开辟公众举报渠道，建立有效的问题机制，及时通过本行网站及其他可靠渠道向公众通报提示钓鱼网站、网络欺诈等重要信息。
g) 应建立网上银行相关的客户投诉、纠纷处理及舆情控制机制，严格按照行业、机构的相关规定和要求对外发布信息，有效维护客户权益及本行声誉。
h)应通过多种渠道及时公告网上银行相关的服务内容、协议、资费标准等重大调整，系统重要升级或变更影响正常服务等重大事项。

6.5 服务功能

本项要求包括：
a)网上银行系统功能建设应以客户为中心，为客户提供个性化的产品和服务。
b)要开发新产品、增加产品功能，不断满足不同人群金融需要。
c)能在线上办理的业务，为客户提供线上办理功能。
d)应简化操作流程及步骤，提供方便快捷的服务。

6.6 服务性能

本项要求包括：
a) 最大交易并发数不低于 1200
b)复杂交易平均响应时间(=2 秒
c)简单交易平均响应时间<=1 秒

7 网上银行服务创新性及前瞻性

7.1 服务创新性

本项要求包括：
a)应引入人工智能客服，7×24 小时为客户提供客户咨询服务
b)应使用指纹识别以及面部识别技术对登录以及风险交易进行辅助认证。
c)应使用大数据埋点技术对客户行为进行统计分析形成客户模型
d)使用云证书实现线上电子签章、签名，使线上签署合同成为可能

7.2 技术前唯性

本项要求包括：
a)引入智能语音搜索，为客户提供语音类服务。
b)采用分布式微服务架构模式，提供流量控制为系统运行保驾护航。

8 网上银行服务实施保障

8.1 组织保障

本项要求包括：
a)应建立与本行发展战略相适应的网上银行信息安全保题及风险管理组织塑松，建立由黄态高级管理层负责，相关各部门负责人及内部专家参与的网上银行信息安全领导协课机制，明确各个部门职责，对其所负责的安全保障及风险管理内容进行管理，明确各部门章程并详细定义各部门人员配置
b)应设立网上银行信息安全保障及风险管理工作的主要负责部门，由该部门组织制定、发布相关制度、规范，协调处置网上银行信息安全管理工作中的关键事项，组织跨部门应急演练等工作应合理设立部门内部岗位及人员职责，明确该部门和其他各相关部门的职责范围、工作流程和沟通协调机制。
c)应设置网上银行产品设计，系统研发、测试、集成、运行维护、管理，内部审计等部门或团队业条，技术，宙计笺久架门应明确未部门网上银行信自安全保及过监管理职毒，执行相应的风险评估、规划实施、应急管理、监督检查、跟踪整改等工作。相关人员应详细了解本部门网上银行相关的职责设置、信息安全保障机制等基本情况，
d)应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离。

8.2 管理制度

本项要求包括：
a)应建立贯穿网上银行业务运作、网上银行系统设计、编码、测试、集成、运行维护以及评估、应急处置等过程，井涵盖安全制度、安全规范、安全操作规程和操作记录手册等方面的信息安全管理制度体系
b)应对安全管理人员或操作人员执行的重要管理操作建立操作规程。
c)应指定或授权专门的部门或人员负责安全管理制度的制订。
d)安全管理制度应具有统一的格式，并进行版本控制
e)应定期组织相关部门和人员对安全管理制度体系的合理性和适用性进行审计，及时针对安全管理制度的不足进行修订。
f) 安全管理制度应通过正式、有效的方式发布。
g)安全管理制度应注明发布范围，并对收发文进行登记。

8.3 宣传与实施机制

本项要求包括：
a)网上银行服务规范应公布至全行人员进行学习，并严格按照要求实施，
b)网上银行服各趕范发布以后，应针对祖关执行人员组织培训，以确保规范的正确执行。
c)应至少每半年一次，开展网上银行服务规范自评估，针对漏洞、缺陷及问题，及时进行修订、完善。
d)应每年组织对网上银行服务规范执行情况进行监督检查，发现问题及时整改落实。

9 参考文献

GB/T 14394-2008 计算机软件可靠性和可维护性管理
GB/T 18336.1-2008 信息技术 安全技术信息技术安全性评估准则第 1 部分：简介和一般模型
GB/T 18336.2-2008 信息技术 安全技术 信息技术安全性评估准则第 2 部分：安全功能要求
GB/T 18336.3-2008 信息技术 安全技术 信息技术安全性评估准则第 3 部分：安全保证要求

GB/T 20983-2008 信息安全技术 网上银行系统信息安全保障评估准则
GB/T 20984-2007 信息安全技术信息系统风险评估规范
GB/T 22080-2008 信息技术 安全技术 信息安全管理休系要求
GB/T 22081-2008 信息技术 安全技术 信息安全管理使用规则
GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
GB/T 35273-2017 信息安全技术 个人信息安全规范
GB/T 32315-2015 银行业客户服务中心基本要求
JR/T 0068-2012 网上银行系统信息安全通用规范
JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引术语和定义
《中国人民银行关于进一步加强银行业本行信息安全保障工作的指导意见》(银发(2006)123 号)
《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》（银发（2009）142 号）
《中国人民银行办公厅关于贯彻落实<中国人民银行中国银行业监督管理委员会 公安部 国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知>的意见》（银办发（2009）149 号）