ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0068—2020
代替 JR/T 0068—2012

网上银行系统信息安全通用规范

General specification of information security for internet banking system

2020-02-05 发布　　2020-02-05 实施

中国人民银行　发布

目 次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替JR/T 0068—2012《网上银行系统信息安全通用规范》。

本标准与JR/T 0068—2012相比，主要变化如下：

——增加了SM系列算法相关要求（见5.4）；

——删除了与JR/T 0071《金融行业信息系统信息安全等级保护实施指引》要求重复的内容（2012年版的6.1.4、6.2）；

——修改了客户端安全的表述，补充了自身防护、敏感信息保护等安全要求（见6.2.1.1，2012年版的6.1.1）；

——增加了条码支付相关要求（见6.2.1.1、6.2.4.3）；

——修改了专用安全设备的安全要求，并改名为“专用安全机制”（见6.2.2，2012年版的6.1.2）；

——增加了安全单元和移动终端支付可信环境相关要求（见6.2.2.1、6.2.2.5）；

——增加了生物特征相关要求（见6.2.2.5）；

——增加了云计算安全相关要求(见6.2.4.1、6.3.1）；

——增加了IPv6相关要求（见6.2.4.3）；

——增加了虚拟化安全相关要求(见6.2.4.4）；

——增加了网上银行系统与外部系统连接安全的基本描述和安全要求（见6.2.5）；

——修改了业务连续性与灾难恢复安全要求（见6.3.7，2012年版的6.2.6中的k、l）；

——修改了安全事件与应急响应的安全要求（见6.3.8，2012年版的6.2.6中的m、n）；

——增加了II、III类银行结算账户及交易安全锁相关要求（见6.4.1）；

——删除了附录中的基本的网络防护架构参考图、增强的网络防护架构参考图和物理安全（2012年版的附录A、附录B、附录C）。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国银联股份有限公司、银行卡检测中心、中国工商银行股份有限公司、中国建设银行股份有限公司、中国农业银行股份有限公司、中国邮政储蓄银行股份有限公司、招商银行股份有限公司、中国民生银行股份有限公司、国家信息技术安全研究中心、中金金融认证中心有限公司。

本标准主要起草人：李伟、陈立吾、车珍、周恒、眷新、夏磊、闫晋国、曲维民、沈筱彦、赵乔伟、何朔、华锦芝、杨阳、徐燕军、章明、汤洋、渠韶光、孟飞宇、张志波、高志民、孙茂增、高强裔、马哲、李博文、赵梦洁、李京春、李冰、曹岳、苏建明、姜城、伍红卫、李徽、王宁、杨杰、廖敏飞、刘红波、梁智扬、廖渊、夏雷、梁剑锋、吴欣、李晓、武德港、李强、曾庆祥、季小杰、李超、马春旺、赵胜利、黄春芳、薛金川、蒋健骁、李为、侯漫丽。

本标准所代替标准的历次版本发布情况为：

——JR/T 0068—2012。

引　言

本标准通过收集、分析在评估检查中发现的网上银行系统信息安全问题和已发生的网上银行案件，针对性地提出安全要求。

本标准旨在有效增强现有网上银行系统安全防范能力，促进网上银行规范、健康发展。本标准既可作为各单位网上银行系统建设、改造升级以及开展安全检查、内部审计的安全性依据，也可作为行业主管部门、专业检测机构进行检查、检测及认证的依据。

网上银行系统信息安全通用规范

1 范围

本标准规定了网上银行系统安全技术要求、安全管理要求、业务运营安全要求，为网上银行系统建设、运营及测评提供了依据。

本标准适用于中华人民共和国境内设立的商业银行等银行业金融机构所运营的网上银行系统，其他金融机构提供网上金融服务的业务系统宜参照本标准执行。

注1：本标准分为基本要求和增强要求两个层次，基本要求为最低安全要求，增强要求是进一步提升系统安全性的要求。各单位应在遵照执行基本要求的同时，按照增强要求，积极采取改进措施，不断提高安全保障能力。

注2：本标准条款中如无特别指明“企业网银”，则同时适用于个人网银和企业网银。

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—2010 信息安全技术 术语

GB/T 27912—2011 金融服务 生物特征识别 安全框架

GM/Z 0001—2013 密码术语

GM/T 0002—2012 SM4分组密码算法

GM/T 0003—2012 SM2椭圆曲线公钥密码算法

GM/T 0004—2012 SM3密码杂凑算法

GM/T 0021—2012 动态口令密码应用技术规范

JR/T 0071 金融行业网络安全等级保护实施指引

JR/T 0098.5 中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

JR/T 0118—2015 金融电子认证规范

JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

JR/T 0156—2017 移动终端支付可信环境技术规范

JR/T 0166—2018 云计算技术金融应用规范 技术架构

JR/T 0167—2018 云计算技术金融应用规范 安全技术要求

JR/T 0168—2018 云计算技术金融应用规范 容灾

中国人民银行关于改进个人银行账户服务加强账户管理的通知（银发〔2015〕392号），2015-12-25

中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016-06-13

中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知（银发〔2016〕261号），2016-09-30

中国人民银行关于落实个人银行账户分类管理制度的通知（银发〔2016〕302号），2016-11-25

中国人民银行办公厅关于强化银行卡磁条交易安全管理的通知（银办发〔2017〕120号），2017-05-31

条码支付安全技术规范（试行）（银办发〔2017〕242号文印发），2017-12-22

中国人民银行关于改进个人银行账户分类管理有关事项的通知（银发〔2018〕16号），2018-01-10

中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知（银发〔2019〕85号），2019-03-22

3 术语和定义

GB/T 25069—2010、GM/Z 0001—2013界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GM/Z 0001—2013中的一些术语和定义。

3.1

网上银行 internet banking

商业银行等银行业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

个人网银 personal internet banking

商业银行等银行业金融机构面向个人用户提供的网上金融服务。

3.3

企业网银 corporate internet banking

商业银行等银行业金融机构面向企事业单位和其他组织提供的网上金融服务。

3.4

支付敏感信息 payment sensitive information

影响网上银行安全的密码、密钥以及交易敏感数据等。

注：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、报文完整性等的对称密钥、私钥等，交易敏感数据包括但不限于完整磁道信息、有效期、CVN、CVN2等。

3.5

移动终端 mobile terminal

区别于PC机方式，以手机、平板电脑、可穿戴设备等访问网上银行的移动设备。

3.6

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。

注：包括但不限于可执行文件、控件、静态链接库、动态链接库等。本标准中客户端程序包括运行于移动终端上的应用软件，不包括IE等通用浏览器。

3.7

智能密码钥匙 cryptographic smart token

提供密码运算、密钥管理等密码服务的终端密码设备，一般使用USB、蓝牙、音频、SD等接口形态。

3.8

智能密码钥匙固件 cryptographic smart token firmware

内置在智能密码钥匙内的影响智能密码钥匙安全的程序代码。

3.9

动态口令 one-time-password(OTP),dynamic password

基于时间、事件等方式动态生成的一次性口令。

[GM/Z 0001—2013，定义2.15]

3.10

动态口令令牌 one time password token

用来生成动态口令的设备。

[GM/Z 0001—2013，定义2.16]

3.11

生物特征 biometric

人类生理上的或行为上的可测量特征，并由此可以可靠地区分某个人不同于其他人，以便识别登记者的身份，或者确认其所声称的已登记的身份。

[GM/Z 0001—2013，定义4.4]

3.12

资金类交易 funds transaction

通过网上银行进行的资金操作交易。

注：例如，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。

3.13

信息及业务变更类交易 information and 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。

注：例如，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。

4 缩略语

下列缩略语适用于本文件。

CDN：内容分发网络（Content Delivery Network）

COS：芯片操作系统（Chip Operating System）

DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）

DNS：域名系统（Domain Name System）

DoS/DDoS：拒绝服务/分布式拒绝服务（Denial of Service/Distributed Denial of Service）

ESN：电子序列号（Electronic Serial Number）

IDS/IPS：入侵检测系统/入侵防御系统（Intrusion Detection System/Intrusion Prevention System）

IMEI：国际移动设备身份码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identification Number）

IPSec：互联网安全协议（Internet Protocol Security）
IPv4：互联网协议第4版（Internet Protocol Version 4）
IPv6：互联网协议第6版（Internet Protocol Version 6）
MAC：消息认证码（Message Authentication Code）
MEID：移动设备识别码（Mobile Equipment Identifier）
NTP：网络时间协议（Network Time Protocol）
SD：安全数码（Secure Digital）
SDK：软件开发工具包（Software Development Kit）
SE：安全单元（Secure Element）
SEMA/DEMA：简单电磁分析/差分电磁分析（Simple Electromagnetism Analysis/Differential Electromagnetism Analysis）
SPA/DPA：简单能量分析/差分能量分析(Simple Power Analysis/Differential Power Analysis)
TEE：可信执行环境（Trusted Execution Environment）
USB：通用串行总线（Universal Serial Bus）
VPN：虚拟专用网络（Virtual Private Network）

5 网上银行系统概述

5.1 系统标识

在系统标识中应标明以下内容：
——名称：××银行网上银行系统；
——所属银行。

5.2 系统描述

网上银行系统将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网、移动通信网络、其他开放性公众网络或专用网络向客户进行延伸，是商业银行等银行业金融机构在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系等变革的重要举措，提高了商业银行等银行业金融机构的社会效益和经济效益。网上银行系统主要包括通过PC、手机、平板电脑、智能电视、可穿戴设备等终端访问的网上银行系统，例如，手机银行、微信银行、直销银行、银企直联、小微企业银行等系统。网上银行系统涵盖个人网银系统和企业网银系统。

5.3 系统组成部分

5.3.1 概述

网上银行系统主要由客户端、通信网络和服务器端组成，并可通过不同类型的通信网络连接到外部系统，开展各类合作业务，其中服务器端包括网上银行访问子网、网上银行业务系统、中间隔离设备和银行处理系统等，如图1所示。

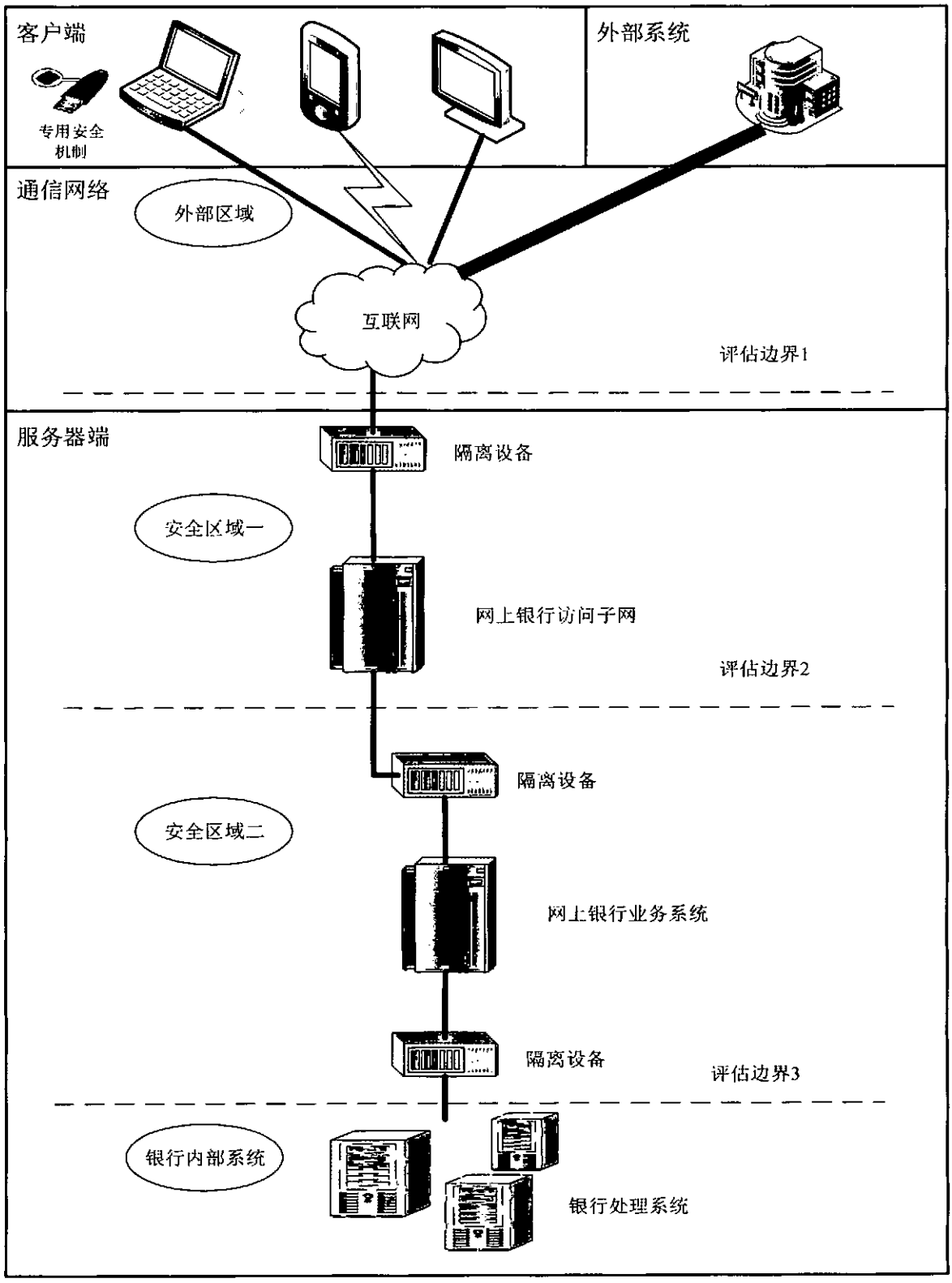

图1　网上银行系统组成示意图

注1：外部区域：网上银行的用户或外部机构，利用网上银行客户端，通过互联网、移动通信网络、其他开放性公众或专用网络访问网上银行业务系统；

注2：安全区域一：网上银行访问子网，提供基于WEB、客户端的访问或跳转服务；

注3：安全区域二：网上银行业务系统，主要进行网上银行的业务处理；

注4：银行内部系统：银行处理系统，主要进行银行内部的数据处理；

注5：隔离设备：不限于硬件或软件等具体形态，主要起到隔离不同安全区域的作用。

5.3.2 客户端

网上银行系统客户端主要包括客户端程序和客户端环境。客户端环境是指客户端程序所在的硬件终端（目前主要包括PC、手机、平板电脑、智能电视、可穿戴设备等终端，将来可能包括其他形式的终端）及该终端上的操作系统、浏览器和其他程序所组成的整体运行环境。客户端环境通常不具备或不完全具备专用金融交易设备的可信输入能力、可信输出能力、可信通讯能力、可信存储能力和可信计算能力，因此，需要使用专用安全机制，并通过接受、减轻、规避及转移的策略来应对交易风险。金融机构应从软硬件合法性验证、程序完整性保护、数据访问控制、数据输入安全、数据传输安全、数据存储安全以及可信执行环境等方面保证客户端的安全性。

5.3.3 通信网络

网上银行借助互联网、移动通信网络等技术向客户提供金融服务，易受到通讯层面的安全威胁，金融机构应从通讯协议、安全认证、通信链路安全等层面，采取措施有效应对相关风险。

5.3.4 服务器端

网上银行系统服务器端提供网上银行应用服务和核心业务处理功能，金融机构应充分利用物理环境、通信网络、计算环境等领域的防护技术，在攻击者和受保护的资源间建立多道严密的安全防线。

5.3.5 与外部系统连接

网上银行除直接向用户提供金融服务外，也可能与外部机构开展业务合作。在网上银行系统设计、开发、部署和运营过程中，应充分考虑外部机构的系统可能存在的安全风险，并针对各类风险进行有效防护。

5.4 系统安全性描述

网上银行系统应根据应用系统、客户对象、数据敏感程度等划分安全域。通过对安全域的描述和界定，可更好地对网上银行系统信息安全保障进行描述。

金融机构应采取专用安全机制，包括数字证书、动态口令、短信验证码、生物特征等，保障网上银行系统安全。金融机构应按照其在交易中具备的可信通讯能力、可信输入能力、可信输出能力、可信存储能力和可信计算能力五种能力的组合对安全机制进行分类管理，并制定与之适应的交易安全风险防范策略。

金融机构在网上银行系统中应用云计算技术前，应结合网上银行系统的业务重要性和数据敏感性、发生安全事件的危害程度等，充分评估应用云计算技术的科学性、安全性和可靠性，在确保系统业务连续性、数据和资金安全的前提下，秉持安全优先、对用户负责的原则，充分评估可能存在的风险隐患，谨慎选用与业务系统相适应的金融领域云计算部署模式。网上银行系统在采用云计算技术时应遵循JR/T 0166—2018、JR/T 0167—2018、JR/T 0168—2018等技术标准与行业主管部门的相关要求。

网上银行系统在使用密码算法时应符合国家密码主管部门的要求，在支付敏感信息加密及传输、数字证书签名及验签等环节宜支持并优先使用SM系列密码算法（GM/T 0002—2012、GM/T 0003—2012、GM/T 0004—2012）。

6 安全规范

6.1 概述

本规范分为安全技术规范、安全管理规范和业务运营安全规范三个部分。金融机构应针对不同的业务类型采取相应级别的安全保障措施。考虑到业务相关性，本规范还包含针对网上银行系统外部连接的安全要求。网上银行系统应按照网络安全等级保护第三级安全要求进行建设与运维管理。

6.2 安全技术规范

6.2.1 客户端安全

6.2.1.1 客户端程序

基本要求：

a) 客户端程序开发设计过程中应注意规避各系统组件、第三方组件、SDK 存在的安全风险，应对开发框架和技术路线进行严格的论证，必要时应进行选型安全测试。
b) 客户端程序应具有明确的应用标识符和版本序号，设计合理的更新接口，当某一版本被证明存在重大安全隐患时，提示并强制要求用户更新客户端。
c) 客户端程序的每次更新、升级，应进行源代码审计、安全活动审查和严格归档，以保证客户端程序不存在隐藏的非法功能和后门。
d) 应采用安全的方式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、完整性校验（例如，联机动态校验等），防范客户端程序被篡改或替换。
f) 客户端程序应采取代码混淆、加壳等安全机制，防止客户端程序被逆向分析，确保客户端的敏感逻辑及数据的机密性、完整性。
g) 客户端程序应保证自身的安全性，避免代码注入、缓冲区溢出、非法提权等漏洞。
h) 客户端程序应采取进程保护措施，防止非法程序获取该进程的访问权限，扫描内存中的敏感数据或替换客户端页面等。
i) 客户端程序应对关键界面采用反录屏等技术，防范非法程序通过拷屏等方式获取支付敏感信息。
j) 客户端程序应提供客户输入支付敏感信息的即时防护功能，并对内存中的支付敏感信息进行保护，例如，采取逐字符加密、自定义软键盘、防范键盘窃听技术等措施。
k) 客户端软件不应以任何形式在本地存储用户的支付敏感信息，存储位置包括但不限于Cookies、本地临时文件和移动数据库文件等。
l) 客户端程序应采取有效措施保证所涉及密钥的机密性和完整性。
m) 客户端程序应采取措施对密码复杂度进行校验，保证用户设置的密码达到一定的强度。
n) 客户端程序密码框应禁止明文显示密码，应使用同一特殊字符（例如，*或•）代替。
o) 客户端程序登录后在一段时间内无任何操作，应自动登出，重新登录才能继续使用。

p) 客户端程序应配合服务器端采取有效措施，对登录请求、服务请求以及数据库查询等资源消耗较高行为的频率进行合理限制。
q) 客户端程序具备条码生成、展示或识读解析功能时，应符合《条码支付安全技术规范（试行）》（银办发〔2017〕242号文印发）要求。
r) 客户端程序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。
s) 客户端程序应支持通过IPv6连接访问网络服务，在IPv4/IPv6双栈支持的情况下，优先采用IPv6连接访问。
t) 客户端程序应具备隐私政策。
u) 客户端程序在收集、使用客户信息之前，应明示收集、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。在采集客户个人敏感信息前应对采集的用途和必要性进行提醒。
v) 客户端程序应禁止访问终端中非业务必需的文件和数据。应根据最小权限原则申请系统权限（例如，申请读取通讯录、地理位置等权限），并取得用户的明示同意。
w) 客户端应保留最少的客户信息，并限制数据存储量和保留时间。
x) 客户端程序退出时，应清除非业务功能运行所必须留存的业务数据，保证客户信息的安全性。
y) 应采取渠道监控等措施对仿冒客户端程序进行监测。

6.2.1.2 客户端环境

基本要求：

a) 应对客户端运行环境的安全状况进行检测并向后台系统反馈，并将此作为风控策略的依据。
b) 应采取有效措施提升客户端环境安全级别，针对不同的安全等级采取相应的风险控制措施。
c) 应在门户站点等渠道发布客户端环境安全的提示。
d) 当发现客户端环境存在重大安全缺陷或安全威胁时，应采取必要措施对用户进行警示或拒绝交易。

6.2.2 专用安全机制

6.2.2.1 智能密码钥匙

本标准所涉及的智能密码钥匙包含目前网上银行系统普遍应用的USB Key、蓝牙Key、音频Key、SD Key等基于硬件的Key产品，也包括将来可能出现的其他基于硬件的Key产品。

基本要求：

a) 金融机构应使用经国家或行业主管部门认可的第三方专业测评机构检测通过的智能密码钥匙。
b) 应在安全环境下完成智能密码钥匙的个人化过程。
c) 智能密码钥匙应采用具有密钥生成和数字签名运算能力的智能卡芯片，保证敏感操作在智能密码钥匙内进行。
d) 智能密码钥匙的主文件（Master File）应受到COS安全机制保护，防止非授权的删除和重建。
e) 密钥文件在启用期应封闭。
f) 应保证私钥在生成、存储和使用等阶段的安全：
   - 签名私钥应在智能密码钥匙内部生成，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。
   - 禁止以任何形式从智能密码钥匙读取私钥或写入签名私钥。
   - 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。
   - 在每次执行签名等敏感操作前，均应首先进行认证。

- 智能密码钥匙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。
- 智能密码钥匙内部产生的私钥，不再需要时应及时销毁。

g) 签名交易完成后，状态机应立即复位。

h) 应保证 PIN 码和密钥的安全：
- PIN 码应具有复杂度要求。
- 采用安全的方式存储和访问 PIN 码、密钥等支付敏感信息。
- PIN 码和密钥（除公钥外）不能以任何形式输出。
- 经客户端输入进行验证的 PIN 码在其传输到智能密码钥匙的过程中，应进行加密，并保证在传输过程中能够防范重放攻击。
- PIN 码连续验证失败次数达到上限（不超过 10 次）时，智能密码钥匙应主动锁定。
- 同一型号智能密码钥匙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，且智能密码钥匙中的对称算法密钥应使用根密钥进行分散。
- 参与密钥、PIN 码运算的随机数应在智能密码钥匙内生成，其随机性指标应符合国家密码主管部门的要求。

i) 借助 SE 与 TEE 技术结合实现智能密码钥匙的相关功能时，应保证 SE 与 TEE 的安全：
- SE 的使用应符合 JR/T 0098.5 的要求。
- TEE 的使用应符合 JR/T 0156—2017 的要求。
- 智能密码钥匙所需的显示、PIN 输入等可信功能应在 TEE 中实现。
- 智能密码钥匙所需的签名验签、密钥与根密钥存储等敏感服务应在 SE 中实现。
- 应保证仅有网上银行系统客户端或相关的客户端程序能够访问 SE 中与其相对应的功能与数据。
- 应使用经国家或行业主管部门认可的第三方专业测评机构安全检测通过的 SE、TEE 产品。

j) 智能密码钥匙使用的密码算法应符合国家密码主管部门的要求。

k) 对智能密码钥匙固件进行的任何改动，都应经过归档和审计，以保证智能密码钥匙中不含隐藏的非法功能和后门指令。

l) 智能密码钥匙加密芯片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。

m) 在外部环境发生变化时，智能密码钥匙不应泄露支付敏感信息或造成安全风险。外部环境的变化包含但不限于：
- 高低温。
- 高低电压。
- 强光干扰。
- 电磁干扰。
- 紫外线干扰。
- 静电干扰。
- 电压毛刺干扰。

n) 应设计安全机制保证智能密码钥匙驱动程序的安全，防范被劫持、篡改或替换。

o) 应采取有效措施防范智能密码钥匙被远程挟持带来的风险，例如，采用具备客户主动确认功能的智能密码钥匙或通过可靠的第二通信渠道要求客户确认交易信息等。

p) 如智能密码钥匙不具备确认功能，则连接到终端设备一段时间内无任何操作后应自动关闭，应重新连接才能继续使用，以降低远程挟持的风险。

q) 具有屏幕显示、语音提示、按键确认等提示确认功能的智能密码钥匙，应符合下列要求：

- 应对交易指令的完整性进行校验、对交易指令的合法性进行鉴别、对关键交易数据进行输入、确认和保护，应采取有效措施防止确认环节被绕过。
- 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关键交易数据，保证屏幕显示或语音提示的内容与智能密码钥匙签名的关键数据一致。
- 应采取有效措施防止签名数据在客户最终确认前被替换。
- 未经按键确认等操作，智能密码钥匙不得签名和输出，在等待一段时间后，自动清除数据，并复位状态。

增强要求：

智能密码钥匙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何操作时的语音提示、屏幕显示提醒等功能。

6.2.2.2 文件证书

文件证书的使用应符合国家密码主管部门与行业主管部门的相关要求，同时应满足以下要求：

基本要求：

a) 应严格控制申请、颁发和更新流程，避免对个人网银客户的同一业务颁发多个有效证书。
b) 用于签名的公私钥对应由客户端生成，不应由服务器生成。私钥只允许在客户端（包括智能密码钥匙等安全设备）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，防止私钥受到未授权的访问。
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，备份的私钥应加密保存。
h) 文件证书的发放宜使用离线或专线方式，确需通过公众网络发放的，应提供一次性链接下载。
i) 文件证书应与终端信息绑定，防范证书被非法复制到其他终端上使用。
j) 应对关键操作（例如，签名）进行保护，防止证书被非授权调用。

增强要求：

在备份或恢复私钥成功后，金融机构应通过可靠的第二通信渠道向客户发送提示消息。

6.2.2.3 动态口令令牌

网上银行系统的动态口令令牌应优先选用符合GM/T 0021—2012的产品。

基本要求：

a) 金融机构使用的动态口令令牌设备及后台支持系统，应经过认可的第三方专业测评机构安全检测通过。
b) 应采取有效措施防范动态口令机制被中间人攻击，例如，通过可靠的第二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或相关变形在整个生命周期的安全。
d) 动态口令生成算法、密钥长度和密钥管理方式应符合国家密码主管部门的要求。
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支付敏感信息，物理攻击的手段包括但不限于开盖、搭线、复制等。
g) 对于基于时间机制的动态口令令牌，应设置此时间窗口最大不超过动态口令的理论生存期前后60s（理论生存期是指如果令牌和服务器时间严格一致，令牌上出现动态口令的时间范围），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。

h) 采用基于挑战应答的动态口令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。

i) 如使用动态口令机制，登录和交易过程中的动态口令应各不相同，系统应具备防重放、防猜解功能。

增强要求：

a) 动态口令令牌设备应使用PIN码保护等措施，确保只有授权客户才可以使用。

b) PIN码和种子应存储在动态口令令牌设备的安全区域内，或使用其他措施对其进行保护。

c) PIN码连续输入错误次数达到错误次数上限（不超过10次），动态口令令牌应锁定。

d) PIN码输入错误次数达到上限导致动态口令令牌锁定后，动态口令令牌系统应具备相应的自动或手动解锁机制。

e) 动态口令令牌加密芯片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。

f) 在外部环境发生变化时，动态口令令牌不应泄露支付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。
- 强光干扰。
- 电磁干扰。
- 紫外线干扰。
- 静电干扰。

g) 动态口令令牌设备应具备一定的抗跌落功能，防止意外跌落导致种子密钥丢失。

6.2.2.4 短信验证码

基本要求：

a) 开通短信验证码时，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。更改手机号码时，应对客户的身份进行有效验证。

b) 交易的关键信息应与短信验证码一起发送给客户，并提示客户确认。

c) 短信验证码应随机产生，长度不应少于6位。

d) 短信验证码应具有时效性，最长不超过6分钟，超过有效时间应立即作废。

e) 短信验证码在使用完毕后应立刻失效，应采取措施防范对验证码的暴力猜解攻击。

f) 短信验证码的关键信息不应由客户定制，例如，金额、卡号。

g) 应基于终端特性采取有效措施防止验证码被分析、窃取、篡改，保证短信验证码的机密性和完整性，例如，对验证码进行加密处理、结合外部认证介质、采用挑战应答等。

6.2.2.5 生物特征

金融机构在网上银行系统中使用生物特征技术进行身份确认或识别（不包含账户开户环节），遵循如下要求。

基本要求：

a) 应符合国家相关法律法规及主管部门有关管理要求，采用的生物特征解决方案应通过经国家或行业主管部门认可的第三方专业测评机构检测。

b) 应充分评估所使用的生物特征技术的特点及存在的风险，按照GB/T 27912—2011的要求建立完整的生物特征安全应用与管理体系。

c) 应采取适当的措施阻止已知的伪造攻击手段，降低伪造身份通过确认或识别的可能性。
d) 应确定合理的生物特征数据采集、传输、处理、存储的方式，采取适当的措施避免生物特征数据或相关信息被非法泄露或非法使用。
e) 当所使用的生物特征技术尚未经过充分验证时，应把生物特征技术作为安全增强手段，并与其他身份认证技术相结合，增强交易安全。
f) 采集的生物特征数据不得用于除预期业务外的其他用途。
g) 在移动终端上，如借助 TEE 技术实现生物特征的相关功能，要求如下：
   - TEE 的使用应符合 JR/T 0156—2017 的要求。
   - 生物特征数据的计算、活检、比对和存储等可信功能应在 TEE 中实现。
   - 应使用经国家或行业主管部门认可的第三方专业测评机构安全检测通过的 TEE 产品。
h) 如借助 SE 技术实现生物特征的相关功能，要求如下：
   - SE 的使用应符合 JR/T 0098.5 的要求。
   - 生物特征功能所需的密钥、根密钥存储、密码学运算等高安全服务应在 SE 中实现。
   - 应保证仅有相关的客户端程序及生物特征数据采集模块能够访问 SE 中与其相对应的功能与数据。
   - 应使用经国家或行业主管部门认可的第三方专业测评机构安全检测通过的 SE 产品。

6.2.2.6 其他机制

对于不明确属于上述分类的其他机制或在本标准发布后新出现的专用安全机制，应根据自身特点参照上述分类的部分或全部要求，保证专用安全机制自身的可靠性以及其所保护信息的安全性。

6.2.3 通信网络安全

6.2.3.1 通讯协议

基本要求：

a) 应在客户端程序与服务器之间建立安全的信息传输通道，采用的安全协议应及时更新至安全稳定版本，取消对存在重大安全隐患版本协议的支持。
b) 应采用每次交易会话采取独立不同密钥的加密方式对业务数据进行加密处理，防止业务数据被窃取或者篡改。
c) 根据数据传输的安全要求，应使用安全的算法组合。

增强要求：

应使用加密算法和安全协议保护网上银行服务器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。

6.2.3.2 安全认证

基本要求：

a) 通过公开网络进行数据传输时，应通过密钥、证书等密码技术手段进行双向认证。
b) 客户端程序应对服务器端证书的合法性进行验证。
c) 整个通讯期间，经过认证的通讯线路应一直保持安全连接状态。
d) 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。
e) 应确保客户获取的金融机构 Web 服务器的根证书真实有效，例如，可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程序安装包中分发等。

增强要求：

客户端程序和本地其他实体（指除支付软件自身外的其他软件及硬件）间的数据通信应采用安全的方式，确保通信数据不被监听和篡改。

6.2.3.3 通信链路

基本要求：

a) 网上银行客户端和服务端之间的通讯，若通信数据中包含支付敏感信息，则应对支付敏感信息加密，支付敏感信息不应以明文形式出现。

b) 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，应建立服务端和客户端之间的安全通道（例如，VPN 等）避免信息被第三方获取或修改。

6.2.4 服务器端安全

6.2.4.1 等级保护要求

网上银行系统应满足JR/T 0071“安全通用要求”中有关安全技术要求。网上银行系统采用云计算技术的，应满足JR/T 0071“云计算安全扩展要求”中有关安全技术要求。采用移动互联相关技术的，应满足JR/T 0071“移动互联安全扩展要求”中有关安全技术要求。

6.2.4.2 安全通信网络

基本要求：

a) 结构安全：
- 应使用前置设备实现跨机构联网系统与入网金融机构业务主机系统的隔离，防止外部系统直接对入网金融机构业务主机的访问和操作。
- 应对进出网络的数据包进行过滤，识别可疑的数据包并进行处置。
- 应加强对于运维区、监控区等网段的安全防护，防止攻击者通过特权网段进行跳转。
- 应定期对无线访问点进行排查，应在连接无线访问点的网络和其他网络之间采取隔离等有效的防护措施，避免访问者渗透到其他网络。
- 应具备自动或快速封禁 IP 的技术措施。
- 具备互联网访问入口的测试环境，网络安全防护要求应同生产环境保持一致。

b) 访问控制：
- 网络设备应按最小安全访问原则设置访问控制权限。
- 应定期对网络设备、安全设备、堡垒机、VPN 等设备的密码进行排查，避免使用默认密码、常见弱口令以及包含个人、机构和设备等信息的口令，避免使用存在一定规律的口令。
- 应对设备管理界面的访问地址进行严格限定，对异常的访问请求进行记录和预警。
- 应采取有效措施防范无线网络接入风险，例如，绑定无线网络终端的 MAC 地址、除静态密码外采用动态因素二次认证等方式。
- 应在与分支机构、合作单位等网络边界设置基于协议及应用内容的访问控制措施。

c) 入侵防范：
- 制定合理的 IDS/IPS 的安全策略配置，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异常流量攻击。可参考的防护措施包括但不限于：
  - 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。
- 使用恶意流量清洗技术。
- 使用具备安全防护能力的 CDN。

d) 网络设备防护：

- 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。
- 不应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。
- 应更改设备的初始密码和默认设置，并定期采用技术手段进行检测等方式以识别不安全的配置。
- 指定专人负责防火墙和路由器的配置与管理，并指定他人定期（不超过 6 个月）审核配置规则。
- 在变更防火墙、路由器和 IDS/IPS 配置规则之前，确保变更已进行验证和审批。
- 应对网络设备运行状况进行日常监控和检查，发现异常应及时报警和处理。
- 应采取沙箱、蜜罐、防病毒等措施，对网络攻击进行预防、监测和处置。
- 应不定期组织针对开源系统或组件的安全测评，及时进行漏洞修复和加固处理。
- 应对 VPN、堡垒机的操作行为进行监控和审计，对异常的账户创建、设备访问等行为进行监控和预警。
- 应定期对软硬件资产进行核查，对设备进行人工、自动化排查探测，对已弃用设备进行下线处理。

e) 恶意代码防范：

- 应对网络流量进行安全分析，分析可疑的网络攻击与入侵行为、僵尸网络、病毒和蠕虫的网络传播等。

增强要求：

网络设备防护：

- 宜使用带外管理的方式对网络设备进行管理，以保障数据网络和管理网络的物理信道分离。
- 网络设备应支持 IPv6，针对 IPv6 的防护强度应不弱于针对 IPv4 的防护强度。

6.2.4.3 安全计算环境

基本要求：

a) 身份鉴别：

- 应使用符合国家密码主管部门要求的加密算法对密码进行加密保护，在传输和存储过程中不允许明文密码出现。
- 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，拆阅后的口令密码经使用后应立即更改并再次密封存放。
- 应对登录主机的地址进行限制，对于违规的登录尝试进行报警。
- 应防范口令暴力破解攻击，记录攻击源地址，并报警。
- 不应明文显示密码，应使用同一特殊字符（例如，*或）代替。
- 应引导用户设置不易猜解的密码，应采取技术手段对脆弱密码进行检测。
- 针对批量或高频登录等异常行为，应利用 IP 地址、终端设备标识等信息进行综合识别，

及时采取附加验证、拒绝请求等手段。

- 应采取有效措施防范登录操作的重放攻击，例如，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。
- 应使用即时加密等安全措施降低恶意软件窃取用户支付敏感信息的风险，使用软键盘方式输入密码时，应采取自定义键盘等措施防范密码被窃取。
- 应保证密码的加密密钥的安全。
- 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。
- 不得在客户端缓存密码、密钥等支付敏感信息，不应在日志中记录支付敏感信息，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支付敏感信息。
- 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、直接输入访问地址等方式重新进入登录后的网上银行页面。
- 退出登录时应提示客户取下（或断开）专用安全设备，例如，智能密码钥匙。
- 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，例如，屏蔽身份证后六位信息等。

b) 访问控制：

- 应实现操作系统和数据库系统特权用户的权限分离，系统管理员只具备操作系统的运维管理权限，数据库管理员只具备数据库的运维管理权限。
- 应根据业务必需和最小权限原则，对主机系统的访问控制规则进行精细化配置，例如，通过系统防火墙对允许访问本机的地址和端口进行限制，对异常的访问请求进行拦截和报警。
- 应对统一身份认证系统、运维终端管理系统，域控、补丁升级、防病毒、邮件、文件中转共享服务器等提供集中管控或基础服务的设施进行严格的访问控制，对异常的访问请求进行拦截和报警。
- 企业网银可支持客户选择使用管理员和操作员两类用户，管理员用户初始登录密码应在银行柜台设置，操作员用户由管理员用户设置或在柜台设置，操作员用户权限应根据录入、复核、授权职责分离的原则设置。
- 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器端数据为准，当服务器端检测到客户提交的信息被篡改时，应当及时中断交易，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。
- 应对开放的 API 接口进行统一准入管理。

c) 安全审计：

- 应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。
- 应及时对中间件日志、应用日志、错误日志等文件进行分析，识别异常的访问行为。

d) 入侵防范：

- 应严格限制下载和使用免费软件或共享软件，确保软件来源可靠，且在使用前应经过严格测试。
- 应建立允许使用的软件列表，对软件安装包进行统一管理，定期对列表中软件的安全状况进行跟踪。
- 应采取技术手段对攻击活动进行检测和报警，例如，文件完整性监控、主机型入侵检测、进程白名单、父子进程关联检测、攻击脚本检测等。

e) Web 应用安全：
- 防范支付敏感信息泄露：
  - 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。
  - 不应在 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。
  - 不应在 Web 应用服务器端保存客户支付敏感信息。
  - 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。
- 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，防止攻击者恶意构造 SQL 语句实施注入攻击。
  - 不应仅在客户端以脚本形式对客户的输入进行合法性判断和特殊字符过滤。
  - 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、对提交数据进行有效性检查、设置响应头防护参数、对输出信息进行编码等措施防范跨站脚本注入攻击。
- 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。
- 应对开放的 API 接口进行安全评估与测试，保证接口的安全性和可靠性。
- 应采取网站页面防篡改措施，应具备对 Web 后门进行检测和报警的能力。
- 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）、第三方输入法带来的支付敏感信息泄露、交易数据篡改等重要信息安全风险。
- 应对条码中包含的网址等信息进行校验，对非法地址和恶意请求进行拦截。
- 应加强对开源及商业应用系统或组件的安全管理，进行安全评估并及时修复安全漏洞。
- 应对文件的上传和下载进行访问控制，避免攻击者执行恶意文件或发起未授权访问。
- 应采取有效措施防范针对服务器端应用层的拒绝服务攻击。

f) 图形验证码：
- 应随机产生。
- 应采取图片底纹干扰、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、交互式认证等有效方式，防止验证码被自动识别。
- 应具有使用时间限制并仅能使用一次。
- 图形验证码应由服务器生成，客户端源文件中不应包含验证码文本。

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。
- 用于访问应用以外的程序或系统的身份认证凭据应采取加密等方式进行保护。
- 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，并建立钓鱼网站案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，增加客户端提交的页面来源地址信息的校验、设置转账白名单等。
- 应采用已有和浏览器相关联的可信网址认证机制，保证登录的 URL 经过第三方权威机构的

安全认证。

h) 域名解析服务：

- 域名解析系统应不间断运行，在排除不可抗力的情况下，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%。
- 递归服务器自身不应同时兼备权威服务器功能，不应提供除域名服务之外的其他服务。
- 权威域名服务系统，应保持主服务器对辅服务器（组）的记录信息的更新频率，保证数据同步。
- 应建立对关键数据和重要信息进行备份和恢复的管理和控制机制。关键数据包括但不限于域名系统架构、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能力。
- 应支持 IPv6 访问与解析。

i) 数据库服务安全：

- 应采用技术手段控制非授权用户访问。
- 应采用技术手段对异常连接和请求进行控制和审计。

j) 关键组件应采取多点部署方式，不因单台服务器发生故障影响业务连续性。

k) 应用系统支持条码支付业务时，应符合《条码支付安全技术规范（试行）》要求。

l) 应对客户端的标识信息进行记录，并判断同一次登录后的重要操作使用的是否为同一终端，采用技术手段对风险进行识别，例如，验证客户端的 IP 地址、MAC 地址、机器码等，如发生变化，应再次对客户身份进行认证。

m) 数据保护：

- 应落实《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170 号）等相关要求，按照 JR/T 0149—2016 要求，对银行卡卡号、卡片验证码、支付账户等信息进行脱敏，支持基于支付标记化技术的交易处理，采取技术手段从源头控制信息泄露和欺诈交易风险。
- 对客户办理金融业务时留存的身份信息与相关影像资料、个人财产信息、征信信息等敏感客户资料，应参照国家及行业个人信息、个人金融信息相关保护要求，加强信息安全管理。

n) 数据备份和恢复：

- 应提供本地数据备份与恢复功能，增量数据备份每天一次，完全数据备份每周一次，备份介质场外存放，数据保存期限依照国家相关规定。
- 应具备异地实时备份或异步备份功能，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。
- 数据备份存放方式应以多冗余方式，完全数据备份至少保证以 1 个月为周期的数据冗余。

增强要求：

a) 不应使用系统管理员账号进行业务操作。

b) 应保证操作系统和数据库的用户鉴别信息、重要业务数据所在的存储空间，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。

c) 支付敏感信息在应用层保持端到端加密，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。

d) 应支持数据库审计，并对 SQL 注入等攻击进行监控和报警。

e) 应对非法攻击行为进行监控，对其终端特征（例如，终端标识、软硬件特征等）、网络特征（例如，MAC、IP、WIFI 标识等）、用户特征（例如，账户标识、手机号等）、行为特征、物理位置等信息进行识别、标记和关联分析，并与风险监控系统实现联动，及时采取封禁等防护措施。

f) 应对恶意攻击行为进行分析，对恶意攻击事件按照网络安全相关要求及时进行上报处理。

g) 应探索采用运行时应用自我保护等技术手段，对恶意行为进行识别、阻断，多层次增强应用的安全防护能力。

6.2.4.4 虚拟化安全

如果网上银行系统部署在虚拟化环境中，应满足JR/T 0167—2018有关技术要求，同时还应当满足以下安全要求。

基本要求：

a) 虚拟化环境加固：
- 应通过必要的安全配置、安装必要预置软件等措施实现安全加固，确保宿主机、虚拟机管理器、虚拟机安全稳定运行。
- 应规范虚拟机管理器和虚拟机的更新管理策略，及时对存在重大安全隐患的系统组件等进行更新，并在更新前对软件包进行兼容性和稳定性测试。

b) 虚拟化隔离：
- 应划分多个安全域，不同安全级别的应用和服务运行在不同的安全域中，防止不同安全级别的应用和服务互相干扰。
- 应采用技术手段，隔离虚拟机与宿主机物理资源，保证虚拟机对宿主机物理资源的使用由虚拟机管理器完成，满足安全隔离的要求。
- 应采用技术手段对不同虚拟机进行隔离，防止虚拟机间的互相干扰。

c) 虚拟化审计：
- 应采用适当的技术手段对虚拟机管理器、虚拟网络等审计对象进行安全审计，采集和存储操作日志。

d) 应对采集的审计操作日志进行安全分析、处理，发现系统中存在的安全隐患、违规事件等问题，并及时进行下一步处理。

e) 虚拟机镜像文件安全：
- 应制定合理的补丁更新策略，及时为虚拟机镜像文件更新补丁程序。
- 应定期检查镜像文件中关键组件是否被篡改，是否存在病毒、木马等恶意程序。
- 应确保部分数据损坏不会影响镜像文件的正常使用，损坏的数据应可恢复。
- 应保证镜像和快照文件具备容灾措施。

f) 虚拟机生命周期管理：
- 虚拟机销毁时，应彻底清除所有相关数据。
- 应按需处理业务系统在虚拟机中生成的应用数据，防止敏感数据泄露或非法恢复该虚拟机。
- 应限制对快照文件的访问，对快照文件的使用进行监测与审计，防止快照文件被非法窃取。

增强要求：

a) 虚拟化环境加固：
- 应对虚拟机管理器进行完整性检查，确保虚拟机管理器加载的功能模块的完整性和真实性。

b) 虚拟机生命周期管理：
- 应严格保证虚拟机迁移过程中重要数据的机密性和完整性。
- 应防止虚拟机的跨安全域迁移。

6.2.5 与外部系统连接安全

6.2.5.1 传输安全

金融机构与外部机构间的数据传输可采用专线、VPN、Internet方式，应符合下列安全要求。

基本要求：

a) 专线方式：
   - 专线传输敏感信息时，应对报文进行加密或对信道加密。
   - 在租用专线时，备份线路和主线应选用不同的电信运营商。

b) VPN 方式：
   - 应采用双因素验证方式对用户身份进行鉴别，例如，使用动态口令、客户端证书等验证方式。
   - 应严格限制具有 VPN 管理权限的用户，对增加、修改和删除用户的操作进行记录，并定期对相关记录进行审计。
   - 应建立 VPN 口令策略，对口令进行控制，设定口令复杂度要求及定期更换策略。
   - 应对 VPN 客户端按照“最小权限”的原则进行授权，并对 VPN 客户端的权限进行定期审查。
   - VPN 客户端应设置空闲超时时间限制，超过时间限制后应断开 VPN 连接。

c) Internet 方式：
   - 应使用安全传输通道进行通讯，传输关键数据时应进行双向认证。
   - 采用的安全协议应不包含已知的公开漏洞。
   - 传输会话应加入超时机制，并依据安全策略要求定时重新协商会话密钥。
   - 应采用固定 IP、域名、白名单、数字证书等方式，防止 DNS 欺骗、流量劫持等攻击。

6.2.5.2 数据安全

基本要求：

a) 金融机构应遵照有关法律法规和行业制度规定，严格遵照客户意愿和指令进行支付，不得泄露用户支付敏感信息。

b) 金融机构与外部机构应对发送的报文计算摘要或进行签名，保证数据报文的完整性，计算摘要或进行签名运算的数据应包含报文中的关键信息。

c) 金融机构与外部机构均应对发往对方的报文进行传输加密，加密信息应包括报文中的关键信息和客户敏感信息。

d) 金融机构与外部机构应拥有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，并使用符合国家密码主管部门要求的签名算法，对报文摘要数据进行规范化处理后，进行数字签名，保证交易行为的不可抵赖性。

e) 应依据《中国人民银行关于进一步加强银行卡风险管理的通知》等文件要求，对支付敏感信息的采集、展示、传输、存储、使用等环节制定保护策略，并定期开展支付敏感信息安全的内部审计。

6.3 安全管理规范

6.3.1 等级保护要求

网上银行系统应满足JR/T 0071“安全通用”中有关安全管理要求。网上银行系统采用云计算技术的，应满足JR/T 0071“云计算安全扩展要求”中有关安全管理要求。网上银行系统采用移动互联相关技术的，应满足JR/T 0071“移动互联安全扩展要求”中有关安全管理要求。

6.3.2 安全管理机构

基本要求：

a) 岗位设置：

- 应建立与金融机构发展战略相适应的网上银行信息安全保障及风险管理组织架构，建立由董事会、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调机制，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。
- 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，明确人员职责，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。
- 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，业务、技术、审计等各部门应明确本部门网上银行信息安全保障及风险管理职责，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。

b) 授权和审批：

- 应针对网上银行业务及技术规划、架构及策略、网上银行新产品推出、网上银行重要技术路线选择、网上银行系统重要变更操作、物理访问和网上银行系统接入等事项建立审批程序，应提交高级管理层审批，并按照审批程序执行审批过程，对重要活动建立逐级审批制度。

c) 沟通和合作：

- 应建立与相关金融机构、公安机关、电信公司的合作和沟通以及应急协调机制，有效处置DDoS、网络钓鱼等网络安全事件。
- 应加强与供应商、业界专家、专业安全公司、安全组织的合作与沟通，增强日常安全防护、突发事件处置、故障处理等方面的能力。

d) 审核和检查：

- 应制定安全审核和安全检查制度，规范安全审核和安全检查工作，按照制度要求进行安全审核和安全检查活动。应保证至少每年开展一次网上银行全面安全检查，检查内容至少包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
- 应制定安全检查方案并进行安全检查，形成安全检查汇总表和安全检查报告。
- 内部审计部门应至少每两年对网上银行开展一次审计，审计内容至少包括相关管理制度的完备性及其执行的有效性，相关操作流程的合理性与合规性，信息安全保障体系的完备性和有效性，信息安全风险管理、规划实施、信息系统运行的安全性，重要客户信息和交易数据的安全性，应急管理和外包管理的有效性以及其他重要信息安全保障的情况。
- 应制定针对违反和拒不执行安全管理措施规定行为的处罚细则。

6.3.3 安全管理制度

基本要求：

a) 应制定明确的网上银行系统总体安全保障目标、网上银行信息安全管理工作的总体方针和策略，将网上银行信息安全保障及信息安全风险管理纳入金融机构全面风险管理体系。

b) 应结合金融机构网上银行发展战略及业务特点，建立网上银行信息安全保障以及信息安全风险管理框架、策略及流程，制定针对网上银行系统设计与开发、测试与验收、运行与维护、备份与恢复、应急事件处置以及客户信息保密等的安全策略。应制定网上银行系统使用的网络设备、

主机设备、安全设备的配置和使用的安全策略。

c) 应建立贯穿网上银行业务运营、网上银行系统需求分析、可行性分析、设计、编码、测试、集成、运行维护以及评估、应急处置等过程，并涵盖安全制度、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。

d) 应做好网上银行相关的新产品(业务)设计以及主要技术路线选择等关键环节的深入论证工作，关注产品及技术路线的合规性、相关业务及技术规则的一致性和延续性以及产品间、系统间的关联性、依赖性，平衡客户体验和安全性，通过增加关键控制机制等措施防范潜在重大安全隐患，避免潜在的信息安全风险。

e) 应建立网上银行信息安全风险管理策略，至少包括风险评价和定级、风险偏好、容忍度及参数制定、风险控制、成本及效益评价、控制措施有效性评价策略等，应根据网上银行发展及检查审计结果，定期修订策略。

f) 应采取科学的分析方法开展覆盖风险识别及评价、风险监测及控制、审计和评估等过程的网上银行信息安全风险管理工作。

g) 在进行网上银行信息安全风险识别时，应明确保护对象，进行资产分类，识别、评估资产的重要性，综合分析其面临的内外部威胁，以及可被威胁利用的脆弱性，识别并评估已有的控制措施，准确界定由此产生影响的可能性，正确识别对国家安全、金融稳定、公众利益、金融机构声誉造成影响的信息安全风险。

h) 应制定安全风险分级标准，评定风险等级，针对不同的风险制定相应的可能性等级列表，对于已发现的风险应尽快修补或采取规避措施。

i) 应建立网上银行信息安全风险的持续监测机制，建立风险预警、报告、响应和处理机制，明确风险报告的内容、流程、主客体以及频率，建立符合金融机构实际状况的关键风险指标体系，实现信息安全风险监测的自动化，保证高级管理层和相关部门可及时获取网上银行信息安全风险变化，验证现有控制措施的有效性。

j) 应根据网上银行信息安全风险评估发现的不同等级风险，以及风险监测获取的风险变化情况，制定风险控制措施、应急处置及恢复方案以及相关的演练计划。

k) 对于衍生的网上银行信息安全风险以及未按计划达到的控制目标，应重新启动信息安全风险评估流程，制定和选择新的风险控制措施，对已接受的风险，定期进行再评估。

l) 应结合网上银行业务种类、发展规模以及信息安全新形势，关注与网上银行相关的新威胁以及隐患，调整风险控制措施以及风险评估方案。

m) 应每年至少开展一次对网上银行系统的信息安全风险评估及深度信息安全检测工作，评估方式不限于自评估和外部评估，自评估应由金融机构内独立于网上银行系统设计、开发、运行和管理的部门进行，外部评估机构应选择熟悉信息安全和金融行业相关标准、国家认证认可管理部门认可的专业机构，评估依据应覆盖本标准要求，并基于评估结果，妥善选择、实施整改措施。

n) 在选择外部评估机构时，并对其加强安全管理，签订保密协议或在相关服务协议中明确保密条款。

o) 应按照国家及行业网络安全等级保护工作有关要求，开展网上银行系统网络安全等级测评及整改工作。

p) 金融机构如提供跨境网上银行服务，应依据国家与行业主管、监管部门有关法律法规、监管要求，充分考虑境内外法律法规、监管要求等的差异性，在深入评估相关风险的基础上，妥善选择相应的安全控制措施。

q) 应主动跟踪行业主管、监管部门与信息安全行业技术组织（例如，国家互联网应急中心等）发布的安全公告、漏洞通知等信息，并及时采取安全检查、修复漏洞、调整系统配置、加强安全管理等应对手段，以保障网上银行系统不受已知安全漏洞的影响。

r) 应指定或授权专门的部门或人员负责安全管理制度的制定。

增强要求：

应梳理与网上银行相关的信息资产，划定其安全级别，并制定与安全级别相对应的保护措施。

6.3.4 安全管理人员

基本要求：

a) 应具有员工岗位调动或离职的安全管理制度，应取回各种工作证件、钥匙、徽章等以及金融机构提供的软硬件设备，避免系统账号、设备配置信息、技术资料及相关敏感信息等泄漏。

b) 应建立网上银行相关的员工培训机制，制定明确的培训计划，对网上银行相关管理人员、业务操作人员、开发设计人员、运维人员、风险管理人员、审计人员等进行安全意识教育培训以及岗位技能在职专业培训，培训方式不限于内部培训或参加第三方机构的专业培训，培训内容应关注网上银行相关的信息安全法律法规、监管要求、标准规范、网上银行的关键技术、业务操作风险、网络安全攻防、社会工程学等，以保持相关人员与工作岗位相匹配的安全意识与专业能力。每年的专业培训应覆盖所有信息科技人员，关键岗位人员的人均培训时间不低于 48 个学时。

c) 应对培训的开展情况和效果进行监督，对安全教育和培训的情况和结果进行记录并归档保存。

d) 应建立外来人员管理制度，在外来人员访问网上银行相关的区域、系统、设备、信息等内容时，提出书面申请并获得批准后应由专人陪同或监督，并登记备案，必要时签署保密协议。对允许被外部人员访问的系统和网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。

e) 针对长期或临时聘用的技术人员和承包商，尤其是从事敏感性技术相关工作的人员，应制定严格的审查程序，包括身份验证和背景调查，并签署保密协议。

f) 金融机构采用外部服务时，应与服务提供方签订安全保密协议，明确服务提供方不得进行任何未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息。

6.3.5 安全建设管理

基本要求：

a) 安全方案设计：
   - 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，组织相关部门和有关安全技术专家对其合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

b) 产品采购和使用：
   - 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

c) 自行软件开发：
   - 在应用系统上线前，应对程序代码进行代码复审，识别可能的后门程序、恶意代码、逻辑缺陷和安全漏洞。
   - 应严格控制对生产版本源代码的访问，避免代码泄露。全部或部分源代码如需交由本机构开发者之外的第三方使用或进行再次开发时，需执行严格的审批流程、明确相关责任并与第三方签署保密协议。
   - 应对生产库源代码版本进行控制，保证当前系统始终为最新的稳定版本。
   - 应对源代码管理系统的访问日志进行审计，对异常行为进行识别。

d) 外包软件开发：
   - 不得将信息科技管理责任外包，应合理谨慎监督外包职能的履行。

- 实现金融机构客户资料与外包服务商其他客户资料的有效隔离，确保在中止外包协议时收回或销毁外包服务商保存的所有客户资料。
- 按照“必需知道”和“最小授权”原则对外包服务商相关人员授权，并签署保密协议。
- 严格控制外包服务商再次对外转包，采取有效措施确保商业银行相关信息的安全。
- 建立恰当的应急措施以应对外包服务商在服务中可能出现的重大缺失。尤其需要考虑外包服务商的重大资源损失，重大财务损失和重要人员的变动，以及外包协议的意外终止等情况。若需要外包人员进入进行现场实施时，应对外包人员的背景、能力和经验进行审查，并应事先提交计划操作内容，金融机构人员应在现场陪同外包人员，核对操作内容并记录，涉及敏感操作（例如，输入用户口令等）应由金融机构人员进行操作，外包人员不得查看、复制或带离任何敏感信息。
- 外包服务商应建立对缺陷的通报、跟踪机制。

e) 测试验收：

- 系统上线前，应清除系统中与测试有关的代码及数据。
- 系统上线前，应进行严格的代码安全测试。若应用程序为委托外部机构开发时，金融机构应要求外部开发机构自行对交付版本应用程序进行安全测试，金融机构对交付版本的应用程序源代码进行安全审计。
- 金融机构应建立对应用程序及源代码进行定期安全检测的机制。

6.3.6 安全运维管理

基本要求：

a) 环境管理：

- 机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰。
- 应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。
- 弱电井应留有足够的可扩展空间。

b) 资产管理：

- 应制定资产的分类原则、方法与标识的基本要求，对信息资产与文档化资产的使用、传输（或传递）、存储等方面提出相应的安全管理要求。
- 应梳理网上银行系统的信息资产，制定资产清单并定期进行盘点。资产清单应包括责任部门、使用部门、重要程度、所处位置等内容。
- 应做好公共文件存储区文档的访问权限管理。
- 应对文档化的资产实行有效期管理，对于超过保密期限的文档降低保密级别，对已经失效的文档定期清理，并严格执行文档管理制度中的销毁和监销规定。
- 应定期对代码仓库、文件共享等网站进行检索，对非授权公开的源代码等敏感文件资产应进行删除处理。

c) 介质管理：

- 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理措施应与本地相同。
- 应根据介质使用期限及时转储数据。

d) 设备管理：

- 应建立标准化的设备配置文档。
- 应加强对高权限终端的管理措施，例如，网络管理员、系统管理员、安全管理员等特权用户使用的终端，以及运维终端、内网扫描终端等。

e) 监控管理和安全管理中心：
- 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，建立监测指标和监测模型，有效监测、预警网上银行安全事件（风险），形成记录并妥善保存，保存期限应不小于6个月。
- 应及时采取控制措施，消除监测到的安全威胁。
- 应建立网络与信息系统运行监测日报、周报、月报或季报制度，统计分析运行状况。
- 应按重要程度进行分级报警，对重要报警应主动及时通知相关人员处置。
- 应制定网上银行系统运行维护的服务管理规范以及相应的控制措施，包括事件处理、问题处理、变更管理等，明确岗位、职责、处理流程、升降级标准、处理时间、所需资源以及流程间的关联和衔接等，及时预警、响应和处置运行监测中发现的问题，发现重大隐患和运行事故应及时协调解决。

f) 网络安全管理：
- 应指定专人对网络进行管理，配备AB岗专（兼）职网络管理员，负责运行日志、网络监控记录的日常维护和报警信息分析、处理工作，并与负责网络设备配置更改的人员职责分离。设备维护记录应至少妥善保存6个月。
- 应对日志记录或外发中断、日志文件损坏等异常事件进行分析。
- 建立健全网络安全运行维护档案，及时发现和解决网络异常情况。
- 应实现设备的最小服务配置，并定期离线备份配置文件。
- 应根据安全策略控制便携式和移动式设备的网络接入。
- 应定期对系统进行漏洞扫描，及时修补发现的系统安全漏洞。
- 应定期检查网络设备的软件，并在需要更新前对现有的重要文件进行备份。

g) 系统安全管理：
- 应根据业务需求和系统安全分析确定系统的访问控制策略。
- 应建立系统容量规划，对设备运行关键指标进行日常监控与分析，注意监控、分析业务高峰时段业务压力对系统的影响，合理设计、适时调整容量参数，及时提出、实施设备扩容。

h) 恶意代码防范管理：
- 应限制在可以访问生产服务器的终端上使用U盘、移动硬盘等移动存储设备，如需使用移动存储设备，应在接入前进行病毒检查。
- 应定期对病毒事件日志进行分析。

i) 密钥管理：
- 对于所有用于加密客户数据的密钥，金融机构应制定并实施全面的密钥管理流程，包括：密钥生成、密钥分发、密钥存储、密钥更换、密钥销毁、知识分割以及双重控制密钥、防止未授权的密钥更换、更换已被知晓或可能被泄露的密钥、收回过期或失效的密钥等。
- 应在安全环境中进行关键密钥的备份工作，并设置遇紧急情况下密钥自动销毁功能。
- 各类密钥应定期更换，对已泄露或怀疑泄露的密钥应及时废除，过期密钥应安全归档或定期销毁。

j) 变更管理：
- 在网上银行系统投产及系统的升级、改造等重大变更前，应经过科学的规划、充分的论证和严格的技术审查，并在事后及时进行总结评价。

6.3.7 业务连续性与灾难恢复

基本要求：

a) 业务运行连续性：

- 应制定网上银行业务连续性策略及计划。
- 应将网上银行业务连续性管理整合到组织的流程和架构中，明确指定相关部门负责业务连续性的管理。
- 应制定员工在网上银行业务连续性方面的培训计划和考核标准。
- 应定期或在网上银行系统发生显著变化时，测试并更新网上银行业务连续性计划与过程，以确保其持续有效。
- 应避免机房采用的多路市电输入均来自于同一个变电站，应对 UPS 等重要设备的报警日志进行及时审核和处理。
- 应提供冗余通信线路，并选择与主用通信线路不同的电信运营商和不同的物理路径。
- 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或分布式多副本存储技术，以避免单一部件故障影响设备运行的风险。
- 应梳理并维护关键的设备部件、备件清单，采取有效的措施防止因单个设备部件出现故障，导致冗余设备无法正常启用或切换的风险。

b) 备份与恢复管理：

- 应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。
- 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存，明确规定备份数据的保存期，做好备份数据的销毁审查和登记工作，应定期导出网上银行系统业务日志文件，并加以明确标识，日志文件应至少妥善保存 6 个月。
- 应定期执行恢复程序，检查并测试各份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。
- 为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。
- 应在金融机构统一的灾难恢复策略下建立完善的网上银行系统灾难恢复体系，开展灾难恢复需求分析、策略及计划制定、灾备系统建设及演练等工作，并根据实际情况对其进行分析和改进，确保各环节的正确性以及灾难恢复体系的有效性。
- 对于同城数据备份中心，应保证可以接管所有核心业务的运行，与生产中心直线距离应满足 JR/T 0071“数据备份恢复”中有关安全技术要求；对于异地数据备份中心，与生产中心直线距离应满足 JR/T 0071“数据备份恢复”中有关安全技术要求。

6.3.8 安全事件与应急响应

基本要求：

a) 安全事件处置：

- 对于重大信息安全事件，各单位相关人员应注意保护事件现场，采取必要的控制措施。
- 应定期对本机构及同业发生的网上银行信息安全事件及风险进行深入研判、分析，评估现有控制措施的脆弱性，及时整改发现的问题。

b) 应急管理：

- 应建立业务和技术部门协调配合的网上银行信息安全事件的应急处置机制，在任何场景下，选择处置方案应充分考虑可能消耗的时间，探索采用事故现场远程视频会议等多种手

段缩短供应商等参与方的响应时间，优先保障业务恢复、账务正确以及数据安全，对于网络和信息安全事件导致的账务差错或异常交易的处理，应严格按照程序做好转人工处理等应急操作。

- 应建立应用系统紧急补丁（应急方案）的开发、发布流程，以备必要时提供紧急补丁或应急方案进行处理，以修补重要安全漏洞。
- 应建立应急预案演练制度，定期组织有业务部门参与的桌面演练和生产系统实战演练，定期对双机热备系统进行切换演练，备份系统与生产系统的切换要至少每年演练一次。演练应考虑不同的中断场景，例如单个或部分业务、系统中断、机房整体供电或网络中断等场景。针对 DDoS、网络钓鱼等重要安全威胁，定期开展有相关单位、部门参与的联合演练。

6.4 业务运营安全规范

6.4.1 业务申请及开通

基本要求：

a) 应遵守相关法律法规，严格落实《中国人民银行关于进一步加强银行卡风险管理的通知》、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）、《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85 号）等相关规定，严格落实关于账户实名制、账户分类管理等相关规定，确保网上银行系统业务设施的安全稳定运行。

b) 通过网上银行渠道开立个人 II、III类银行结算账户时，应严格落实《中国人民银行关于改进个人银行账户服务加强账户管理的通知》（银发〔2015〕392 号）、《中国人民银行关于落实个人银行账户分类管理制度的通知》（银发〔2016〕302 号）、《中国人民银行关于改进个人银行账户分类管理有关事项的通知》（银发〔2018〕16 号）等文件相关要求。

c) 金融机构应充分考虑并采取有效技术措施防范网上银行资金类交易开通的安全风险。个人网银资金类交易的开通应由客户本人到柜台申请，申请时，金融机构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或同等安全级别认证方式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金融机构能有效识别转入、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。

d) 网上银行资金类业务关闭后，重新申请开通该功能，应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，核实客户身份和交易开通意愿。

e) 企业网银开通应由本企业人员到柜台申请，金融机构应审查其申请材料的真实性、完整性和合规性。

f) 企业网银客户加挂账户可通过柜台或通过使用专用安全机制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。重置智能密码钥匙的密码应到柜台办理。

g) 通过手机终端访问网上银行的资金类交易开通应有效验证客户身份，客户应通过柜台或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，金融机构应采取包含电子签名验证在内的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，核实客户身份和交易开通意愿。

h) 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金融机构设置，金融机构应强制客户首次登录时修改初始密码。

i) 客户重置登录密码及支付密码且保留资金类交易权限时，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申请。通过网上银行渠道申请时，金融机构应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。

j) 申请客户数字证书时，应验证公钥的有效性，对证书签名请求采取安全保护措施。

k) 下载客户数字证书时，应对客户身份进行认证。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。

l) 客户申请智能密码钥匙作为数字证书载体或其他安全设备时，应持有效身份证件到柜台办理。例如，申请基于 SE、TEE 技术构建的新型智能密码钥匙，其支付初始额度不能超过新型智能密码钥匙原申请渠道的额度上限，并应引导客户通过柜台、传统智能密码钥匙辅助认证等渠道办理额度提升。

m) 金融机构应采取将安全设备序列号与客户信息进行绑定等措施，如涉及数字证书应在客户下载证书时将其作为客户身份认证因素之一，以防止证书被非授权下载。如安全设备丢失，应持有效证件到柜台重新办理，将原有安全设备和客户绑定关系解除。

n) 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金融机构客服电话等办理，金融机构应核实客户信息、网银账户信息并对预留手机号码进行验证。

6.4.2 业务安全交易机制

6.4.2.1 身份认证

基本要求：

a) 金融机构应按照审慎原则，采取有效、可靠的身份认证手段，保证资金类交易安全。

b) 应采取交易验证强度与交易额度相匹配的技术措施，提高交易的安全性。高风险业务应组合选用下列三类要素对交易进行验证：一是客户知悉的要素，例如，静态密码等；二是仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；三是客户本人生物特征要素，例如，指纹、虹膜等。应确保采用的要素相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或者泄露。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金融机构能有效识别转入、转出方为同一客户账户的。

c) 采用数字证书、电子签名作为支付交易验证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、JR/T 0118—2015 等有关规定，确保数字证书的唯一性、完整性及交易的抗抵赖性。

d) 采用一次性密码作为支付交易验证要素的，应将一次性密码有效期严格限制在最短的必要时间内。

e) 使用企业网银进行资金类交易时，应至少使用硬件承载的数字证书等方式进行身份认证。

f) 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，避免设置易猜解的简单密码（例如，连续或相同字母数字、键盘顺序、常见单词短语等），与常用软件（例如，社交软件）、网站（例如，社交平台、论坛）、与客户个人信息相似度过高的用户名和密码组合。

g) 客户登录网上银行或登录后执行资金类交易时，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，并引导客户采取隔日登录、密码重置等措施进行有关锁定状态解除操作。对于大数据分析认定的高风险行为，应通过短信或电话等可靠的方式通知客户。

h) 金融机构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，金融机构应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。

如通过网上银行系统开展网上支付业务，还应满足以下条款：

a) 网上银行系统接受商户或非银行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。

b) 应对网上银行系统和商户、非银行支付机构的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。

6.4.2.2 交易流程

基本要求：

a) 金融机构应充分考虑、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) 应为客户提供银行卡交易安全锁服务，并落实《中国人民银行办公厅关于强化银行卡磁条交易安全管理的通知》（银办发〔2017〕120 号）等文件的相关要求。

c) 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交易信息不被篡改，例如，使用挑战应答型动态口令令牌产生的交易密码、发送包含确认信息的短信验证码、在智能密码钥匙内完成确认等。

d) 资金类交易中，如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。

e) 金融机构应采取有效措施鉴别客户身份，保证支付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。

f) 提交交易请求时，应上送终端相关信息，例如，计算机终端可提交设备 CPU ID、硬盘序列号、浏览器指纹等；移动终端设备可提交 IMEI、IMSI、MEID、ESN 等。后台服务器应对编号信息和登记信息进行一致性验证。如对交易数据签名，签名数据应包含此类信息。

g) 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。

h) 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。

i) 应在账户资金汇总页面明确显示包含所有子账户资金、在途资金等在内的全部资金状况。

j) 金融机构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，应使用其他身份认证方式进一步确认客户身份。

k) 对于资金类等高风险业务，金融机构应在确保客户联系方式有效的前提下，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，及时告知客户其资金变化情况。

l) 应对交易过程进行风险识别与干预，防范潜在的非法交易、欺诈交易。

m) 对于大数据分析认定的高风险交易，应进行附加交易验证，进一步校验交易发起者的真实身份。
n) 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，包括但不限于采用数字证书、电子签名等技术手段。
o) 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。条码支付业务应按照《条码支付安全技术规范（试行）》等文件要求，根据不同的风险防范能力设置相应的交易限额。

6.4.2.3 交易监控

基本要求：

a) 金融机构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) 应建立基于高风险交易特点和用户行为特征等的风险评估模型，并根据风险等级实施差异化风险防控。
d) 应通过交易行为分析、机器学习等技术不断优化风险评估模型，结合生物探针、相关客户行为分析等手段，建立并完善反欺诈规则，实时分析交易数据，根据风险高低产生报警信息，实现欺诈行为的侦测、识别、预警和记录，提高欺诈交易拦截成功率，切实提升交易安全防护能力。
e) 应建立风险交易监控系统，对具备频次异常、账户非法、批量交易、用户习惯偏离、用户特征偏离、非法更正交易、报文重复、金额异常、扫库或撞库等特征的请求，以及外部欺诈、身份冒用、套现、洗钱等异常情况进行有效监控，对于风险较大、可疑程度较高的交易，应采取精准识别、实时拦截等措施。
f) 对监测到的可疑或异常交易建立报告、复核、查结机制。应开展人工分析，识别攻击源头、进行影响分析并及时采取拦截措施，防止集中性风险事件发生。
g) 应对存在异常交易的终端和商户，采取调查核实、风险提示、延迟结算、拒绝服务等风险防控措施。
h) 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。
i) 针对疑似发生支付敏感信息泄露的客户，应通过灰名单、登录之后强制修改密码、附加验证等措施保证客户账户的资金安全。
j) 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、处置并妥善留存违规行为线索和证据。
k) 风险交易监控系统应能够不断更新反欺诈规则，建立和完善风险信息库，及时从主管部门、公安机关、银行卡清算组织等获取黑名单等风险信息。

增强要求：

金融机构的风险交易监控系统应能够实现与各金融机构、主管部门和公安机关等机构间的信息共享和信息交换。

6.4.3 外部机构业务合作

金融机构通过网上银行系统与外部机构开展业务合作时，应遵循如下安全要求。

基本要求：

a) 金融机构应建立与外部机构业务合作的风险管理机制，明确技术、业务等相关部门职责，制定风险管理制度，建立安全技术标准，规范系统接入，并加强对业务开展情况的动态管理。

b) 金融机构与外部机构应在合作协议中明确交易验证、信息保护、差错处理、风险赔付等方面的权利、义务和违约责任，切实保障持卡人资金安全和信息安全。

c) 金融机构在与外部机构进行业务来往时，应采取有效的技术措施鉴别发生交易的银行卡账户对应的客户身份。

d) 金融机构应保证与外部机构建立一次签约、多次支付的业务合作关系的账户具有至少一种账户变动即时通知技术方式（通知信息中的内容应至少包括外部机构名称、交易金额、交易时间等信息）。

e) 金融机构应评估外部机构的技术风险承受能力，保证客户与外部机构相关的账户关联、业务类型、交易限额（包括单笔支付限额和日累计支付限额）应与其技术风险承受能力相匹配。

f) 金融机构应将与外部机构的合作业务纳入本机构业务运营风险监测系统的监控范围，采取技术手段对商户和客户在本机构的账户资金活动情况进行实时监控，对达到风险标准的应组织核查。特别是对其中大额、异常的资金收付，应做到逐笔监测、认真核查、及时预警、及时控制。

g) 金融机构应对客户通过外部机构进行的交易建立自动化的交易监控机制和风险监控模型，及时发现和处置异常行为。

h) 金融机构应完整地保留在与外部机构开展各项业务时的各类数据、指令、日志等信息。所保存的内容应在相关法律法规规定的期限内妥善保管，便于事后检查和审计。不得留存非本机构的支付敏感信息，确有必要留存的，应取得客户本人及账户管理机构的授权并进行加密或不可逆变换。

i) 金融机构在与外部机构建立关联业务时，应采用多因素身份认证方式，直接鉴别客户身份，取得客户授权，并保存记录。应采取有效的技术措施保证交易指令的安全性，对于支付类交易应要求外部机构提供必要的订单信息，以用于客户进行交易确认，保障支付交易安全。

j) 金融机构应对交易的唯一性进行检查，防止重复支付；通过可靠的数字签名等机制保证交易信息的真实性、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。

k) 金融机构在资金拨付前，应与外部机构校验、确认支付相关信息，防止支付或订单信息被篡改、重放、替换等。

l) 金融机构应要求、督促外部机构识别客户所购买的商品类别，并根据商品类别对应的不同风险，采取有效的技术措施保障交易安全，降低交易风险。

m) 金融机构应要求外部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。

n) 如外部机构参与支付敏感信息的处理，金融机构应要求、监督外部机构，禁止其存储客户的支付敏感信息，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。

6.4.4 客户培训及权益保护

基本要求：

a) 金融机构应切实加强客户培训和风险提示，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，在网上银行新产品（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。

b) 金融机构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，提示客户牢记金融机构官方网站地址和呼叫中心号码。

c) 金融机构应向客户印发通俗、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培训栏目。在显著位置或关键操作界面，宜提醒客户注意防范各类诈骗。

d) 金融机构应按照相关法律法规要求，制定网上银行系统隐私政策。

e) 金融机构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，避免设置与常用软件（例如，社交软件）、网站（例如，社交平台、论坛）、与客户个人信息相似度过高的用户名和密码组合，避免将本人网上银行支付敏感信息告知他人，避免将本人的网上银行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断开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，注意对网上银行的支付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，建立有效的问题处置机制，及时通过金融机构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、纠纷处理及舆情应对机制，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金融机构声誉。

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，可能影响服务的系统重要升级或变更等重大事项。

参 考 文 献

[1] GB/T 14394—2008 计算机软件可靠性和可维护性管理

[2] GB 17859—1999 计算机信息系统 安全保护等级划分准则

[3] GB/T 18336.1—2015 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

[4] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能组件

[5] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保障组件

[6] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[7] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

[8] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

[9] GB/T 22239 信息安全技术 网络安全等级保护基本要求

[10] GB/T 22240—2019 信息安全技术 信息系统安全等级保护定级指南

[11] GB/T 25058—2019 信息安全技术 网络安全等级保护实施指南

[12] GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

[13] GB/T 28448 信息安全技术 网络安全等级保护测评要求

[14] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

[15] GB/T 35273—2017 信息安全技术 个人信息安全规范

[16] 中国人民银行关于进一步加强银行业金融机构信息安全保障工作的指导意见（银发〔2006〕123号），2006-04-18

[17] 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），2009-04-27

[18] 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），2009-08-03

[19] 中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知（银发〔2011〕17号），2011-01-21

[20] 中国人民银行关于银行业金融机构信息系统安全等级保护定级的指导意见（银发〔2012〕163号），2012-06-29

[21] 中国人民银行关于加强银行卡业务管理的通知（银发〔2014〕5号），2014-01-08

[22] 中国银监会 中国人民银行关于加强商业银行与第三方支付机构合作业务管理的通知（银监发〔2014〕10号），2014-04-09

[23] 中国人民银行办公厅关于开展支付安全风险专项排查工作的通知（银办发〔2018〕146号），2018-08-14

[24] 中国人民银行关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知（银发〔2019〕237号），2019-09-27