

ICS 35.240.40

CCS A 11

团 体 标 准

T/NIFA 28—2023

网上银行服务 应用安全规范

Internet banking service—Specification for
application security

2023-11-10 发布

2023-11-10 实施

中国互联网金融协会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语与定义	1
4 缩略语	2
5 身份鉴别	2
5.1 身份鉴别技术要求	2
5.2 身份鉴别安全要求	6
6 交易安全性	8
6.1 抗抵赖机制	8
6.2 重放检测机制	8
6.3 防撞库及恶意查询	9
6.4 交易合法性检查	9
6.5 交易漏洞防范	10
7 数据安全性	10
7.1 传输数据的机密性保护	10
7.2 传输数据的完整性保护	11
7.3 存储数据的机密性保护	11
7.4 存储数据的完整性保护	11
7.5 页面展示信息的保护	11
7.6 与第三方合作时金融信息的保护	12
8 客户个人信息保护	12
8.1 客户个人信息的屏蔽保护	12
8.2 客户个人信息的访问控制	13
8.3 客户个人信息的使用限制	13
9 移动金融客户端安全	13
9.1 客户端程序安全保护	13
9.2 数据安全保护	14
9.3 其他安全要求	14
10 逻辑安全测评	15
10.1 身份鉴别测评	15
10.2 账户管理测试	18
10.3 金融交易测试	19
11 系统运营安全管理	21
11.1 配置管理	21
11.2 变更管理	21
11.3 风险管理	21
11.4 备份与恢复管理	21

附录 A（规范性）密码技术要求 23

参考文献..... 26

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、中国农业银行股份有限公司、中国民生银行股份有限公司、北京银行股份有限公司、北银金融科技有限责任公司、济宁银行股份有限公司、奇安信科技集团股份有限公司、长沙银行股份有限公司。

本文件主要起草人：单强、陆书春、朱勇、王新华、林松、国枫、蒋康定、王明月、邓康、袁丽欧、李晓、赵雪、赵重祺、张勇、杜宁波、陶振帅、赵晨阳、尹智清、廖植群、刘幸。

引 言

网上银行是支撑银行业服务客户的重要系统，网上银行服务降低了银行经营成本，提高了银行盈利能力，同时由于网上银行服务具有无时空限制的特性，有利于扩大客户群体，提升服务创新能力，向客户提供多种类、个性化的金融服务。网上银行服务的便利性和开放性也对其安全性提出了更高要求。

本文件通过整理分析网上银行系统应用安全技术问题和已发生的网上银行应用安全事件，有针对性地提出网上银行服务应用安全相关技术要求。

本文件旨在有效提升现有网上银行应用的安全技术水平，指导网上银行应用安全的设计工作，进一步提升网上银行应用的安全性，从而为客户提供更加安全的线上金融服务，最终促进网上银行服务的规范、健康发展。

网上银行服务 应用安全规范

1 范围

本文件规定了网上银行系统在设计方面的要求，包括密码技术、身份鉴别、访问控制、安全审计、数据安全性、客户个人信息保护、交易安全性、移动金融客户端安全、逻辑安全测评、系统运营安全等方面的相关规范要求。

本文件适用于中华人民共和国境内设立的银行业金融机构所提供的网上银行服务。

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 27912—2011 金融服务 生物特征识别 安全框架

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37036.1—2018 信息技术 移动设备生物特征识别 第1部分：通用要求

JR/T 0068—2020 网上银行系统信息安全通用规范

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

3 术语与定义

JR/T 0068—2020、JR/T 0092—2019和JR/T 0171—2020界定的以及下列术语和定义适用于本文件。

3.1

密钥 key

控制密码变换操作的符号序列。

注：加密、解密、密码校验函数计算、签名生成或签名验证。

[来源：GB/T 15843.1—2017，3.16]

3.2

对称加密算法 symmetric encryption algorithm

源发者和接收者使用同一秘密密钥进行变换的加密算法。

[来源：GB/T 15843.1—2017，3.34]

3.3

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。

[来源：GB/T 15843.1—2017，3.11]

3.4

双因素认证（2FA） two-factor authentication (2FA)

除静态密码外，采用动态密码、数字证书等技术，通过双重认证的方式加强身份管理的认证方式。

[来源：JR/T 0088.1—2012，2.43]

3.5

角色 role

一组预先确定的规则，规定在用户和对象之间许可的交互。

4 缩略语

下列缩略语适用于本文件。

MAC：消息认证码（Message Authentication Code）

OTP：一次性口令（One Time Password）

SDK：软件开发工具包（Software Development Kit）

VPN：虚拟专用网络（Virtual Private Network）

PIN：个人识别码（Personal Identification Number）

SSL：安全套接层（Secure Sockets Layer）

CVV：卡效验值（Card Verification Value）

CVN：卡效验号（Card Verification Number）

5 身份鉴别

5.1 身份鉴别技术要求

5.1.1 概述

身份鉴别按照实现方式可分为静态口令、第二信道设备（如手机动态验证码）、OTP设备（如软实现、硬件OTP）、数字证书（如软数字证书、硬数字证书）和生物特征识别等技术。

5.1.2 静态口令

5.1.2.1 生成要求

口令生成的要求如下：

- 长度不低于6个字符，宜采用8个字符以上的口令；
- 对于非设备绑定用户的账户，应采用非纯数字的口令，宜包含字母、数字、特殊字符混合输入，不宜出现连续6位数字或者身份证号、手机号中连续6位等弱口令；
- 对于手势密码等其他静态密码，应满足一定复杂度要求；
- 认证系统应能够对用户输入的口令强度进行分析，给出口令强度的反馈；
- 对于低强度的口令能够警示用户更换更高强度的口令。

5.1.2.2 使用要求

口令的使用应满足以下要求：

- a) 通过受理终端或支付客户端应用程序使用静态口令时，应采取屏蔽措施，避免出现口令明文；
- b) 应具备静态口令认证失败处理功能，可采取图形验证码、滑块验证、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；
- c) 应支持口令重置，在重置前，应在人脸识别、短信验证码、取款密码、设备指纹等认证方式中，采取至少两种方式进行身份认证。重置后的口令生成应遵守口令的输入要求；
- d) 口令在服务端验证过程中不应出现明文，应通过硬件密码设备加密后进行验证或存储；
- e) 口令应加密传输。

5.1.2.3 设备要求及安全要求

输入设备及安全措施应满足以下要求：

- a) 输入设备应具备一定的物理、逻辑安全机制，如应具备入侵检测机制，防止输入过程被监听，可安全存储敏感信息，具备完整的密钥体系；
- b) 在口令输入设备和读卡机之间传输 PIN 相关信息时，应有效地保护所传输的数据；
- c) 输入控件应具备一定的安全机制，防止非法用户采用键盘侦测手段获取密码；
- d) 在输入控件和终端程序间传输静态口令相关信息时，应有效地保护所传输的数据。

5.1.3 第二信道设备

5.1.3.1 生成要求

当用户使用第二信道设备接收到的动态验证码作为鉴别因子时，动态验证码的生成应满足以下要求：

- a) 动态验证码应随机生成，且长度不低于 6 个字符；
- b) 动态验证码应与交易实现一对一绑定；
- c) 动态验证码不应与交易信息绑定。

5.1.3.2 使用要求

使用第二信道设备接收到的动态验证码的要求如下：

- a) 应设定认证有效期，比如 60 秒，宜不超过 6 分钟；
- b) 应限制验证出错次数，若超过限制次数，则验证码失效或账户锁定；
- c) 重新获取验证码后，原先验证码自动失效。

5.1.3.3 设备要求及安全要求

传输信道宜与交易信息传输的信道相分离。

5.1.4 OTP 设备

5.1.4.1 生成要求

OTP 令牌作为鉴别因子，OTP 的生成应满足以下要求：

- a) 应使用经第三方专业安全测评机构检测通过的软件、OTP 令牌、客户端模块及后台支持系统；
- b) OTP 的长度应不少于 6 位，且应有复杂度要求；
- c) OTP 生成算法应经过国家密码主管部门认定。

5.1.4.2 使用要求

OTP的使用应满足以下要求：

- a) 应采取有效措施防范软件、OTP 令牌被中间人攻击，采取的措施包括但不限于通过客户端安全加固、软件加壳、代码混淆等；
- b) 不同业务中的 OTP 应各不相同，且使用后立即失效；
- c) 应具有激活尝试次数限制功能，当激活操作连续错误一定次数之后，将会被锁定一段时间，才可重新执行激活操作，避免恶意的穷举攻击。

5.1.4.3 设备要求及安全要求

输入设备及安全措施的要求如下：

- a) 应采取有效措施保证种子密钥数据在整个生命周期的安全；
- b) 软件 OTP 令牌可使用 PIN 码、生物特征信息等方式进行保护；
- c) 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、复制等；
- d) 对于硬件 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；
- e) 对于硬件 OTP，令牌加密芯片应具备抵抗旁路攻击的能力；
- f) 对于硬件 OTP，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；
- g) 对于硬件 OTP，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。

5.1.5 数字证书

5.1.5.1 文件证书

5.1.5.1.1 生成要求

文件证书生成应满足JR/T 0068“文件证书”中有关安全技术的要求，同时应满足以下要求：

- a) 文件证书对应私钥的存储应与终端设备信息绑定，防范私钥被非法复制到其他设备上使用；
- b) 针对移动终端用户，文件证书应与移动终端的 IMEI、IMSI、MEID、ESN 等设计用于唯一标识移动终端的信息绑定，防范证书被非法复制到其他移动终端使用。

5.1.5.1.2 使用要求

使用文件证书应满足以下要求：

- a) 文件证书的发放宜使用离线或 VPN 专线方式，确需通过公共网络发放的，应提供一次性下载链接，且传输过程中的证书是加密的；
- b) PIN 码连续输入错误次数达到上限，证书软件应被锁定。

5.1.5.1.3 设备要求及安全要求

输入设备及安全措施应满足以下要求：

- a) 签名密钥应由软件模块内部生成，产生、使用、存储、销毁等过程中的任何时间均不以明文方式出现在内存中，签名密钥、非对称加密密钥、对称密钥等密钥信息均不以明文方式存储在非易失性存储器上；
- b) 使用密码技术保护私钥，应将签名私钥保存在签名验签服务器、密码机、智能密码钥匙等密码设备中；
- c) 密码模块应鉴别并验证操作员的角色或身份，以确保其是否有权执行对应的服务；
- d) 采用验证码对关键操作（如签名）进行保护，防范穷举攻击；

- e) 文件证书软件模块具备软件完整性检测与关键功能自测试功能。

5.1.5.2 智能密码钥匙

5.1.5.2.1 生成要求

应能够支持一个或多个应用，并能提供和保持不同应用之间的安全性。

5.1.5.2.2 使用要求

使用智能密码钥匙应满足以下要求：

- a) 应能够保证一个应用不会影响另一个应用的安全操作；
- b) 如智能密码钥匙不具备确认功能，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；
- c) 证书存储介质应能够自动识别与客户端的连接状态，宜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言提示、屏幕显示提醒等功能；
- d) 如智能密码钥匙不具备确认功能，交易过程中应使用双因素认证，以防范远程挟持。

5.1.5.2.3 设备要求及安全要求

输入设备及安全措施应满足JR/T 0068中有关安全技术要求，同时应满足以下要求：

- a) 应使用通过第三方专业测评机构安全检测的证书存储介质；
- b) 应采取有效措施防范证书存储介质被远程挟持；
- c) 证书存储介质应采用具有密钥生成和数字签名运算能力的安全芯片，保证敏感操作在存储介质的安全芯片内实施；
- d) 证书存储介质的主文件应受到安全机制保护，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；
- f) 参与密钥、PIN 码运算的随机数应在证书存储介质内生成，其随机性指标应符合国家密码主管部门的要求；
- 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。

5.1.6 生物特征识别

5.1.6.1 概述

本文件中用于用户身份识别的生物特征识别模态包括但不限于：

- a) 人脸识别；
- b) 指纹识别；
- c) 声纹识别；
- d) 虹膜识别；
- e) 静脉识别。

5.1.6.2 技术要求

基于生物特征识别技术的用户身份识别应满足GB/T 27912—2011的要求。此外，还遵循如下要求：

- a) 根据个人信息分级分类管理的要求,对身份鉴别过程中涉及到的敏感生物特征信息的收集、传输、存储、使用、委托处理、共享、转让、公开披露应遵循 GB/T 35273—2020 以及 JR/T 0171—2020 中的相关要求;
- b) 应充分评估所使用的生物特征识别技术的特点及存在的风险,按照 GB/T 37036.1—2018 的要求合理的选择远程模式或本地模式;
- c) 处理高安全需求业务时(如网络支付等)应采取适当的措施检测呈现攻击手段并具备相应的处理机制,防止恶意伪造攻击,检测和处理的呈现攻击手段要求如下:
 - 1) 形状包括但不限于 2D、3D 等方式;
 - 2) 载体包括但不限于图像、视频、头模、指纹膜等方式;
 - 3) 材质包括但不限于纸质、电子、硅胶等方式。
- d) 应具备有效的安全机制,确保生物特征样本采集、质量判断、呈现攻击检测、生物特征项提取和传输过程中,用户生物特征数据的机密性和完整性;
- e) 宜结合可信环境实现生物特征识别。

5.1.7 手机号认证

手机号认证是移动运营商提供,通过基于SIM卡进行手机号认证,采用“通信网关取号”及SIM卡识别等技术实现的一种移动互联网身份认证方法,具体要求如下:

- a) 应保障用户实名手机号并完成相关注册或登记;
- b) 验证时应有移动数据网络信号覆盖;
- c) 一键授权应用场景下,应具备授权页面,经用户授权后方可获得手机号码,适用于移动金融客户端的注册、登录等场景;
- d) “本机号码校验”应用场景下,本机号码校验不返回号码,仅返回待校验号码与本机号码是否一致的结果;
- e) 宜具备相关机制保障手机终端为手机号所有者所有并使用。

5.2 身份鉴别安全要求

身份鉴别攻击过程中,攻击者通过获取用户所持有能够用以证明其身份的鉴别因子,假扮成合法的注册用户,在通过身份鉴别后造成危害。表1列出了身份鉴别过程中常见的安全威胁以及相应的防范措施。

表 1 身份鉴别过程中常见的安全威胁以及相应的防范措施要求

安全威胁	描述	攻击示例	防范目标与措施
在线猜测/字典攻击	攻击者通过不断猜测可能的验证信息来重复登录尝试	攻击者通过尝试猜测用户的用户名和常用密码来登录一个网上银行	防范目标:让攻击者没有更多先验知识的情况下,仅通过重复尝试猜测来攻击变得不可行。
暴力破解	也称为“蛮力破解”或“穷举攻击”,是一种特殊的字典攻击。在暴力破解中所使用的字典是字符串的全集,对可能存在的的所有组合进行猜测,直至得到正确的信息为止	攻击者通过穷举的方式来试图获取到正确的密码	防范措施:限制失败尝试次数、登录失败后设置等待时间、要求验证对象通过公开的图灵测试机制(如滑块验证)来防范机器人猜测等
键盘监听	通过对用户的实体或虚	按键记录软件以木马方式	防范目标:让攻击者无法通过植

安全威胁	描述	攻击示例	防范目标与措施
	拟键盘进行监听，获取用户输入信息	植入用户的计算机后，可以偷偷地记录下用户的每次按键动作，从而窃取用户输入的口令，并按预定的计划把收集到的信息通过电子邮件等方式发送出去	入程序的方式进行键盘等输入设备的监听 防范措施：客户端安装必要的杀毒软件并定期查杀；客户端使用定制的加密动态键盘，打乱键位；增加反录屏和截屏机制
钓鱼攻击（假冒网页）	注册用户被引诱与一个假冒的验证方进行交互，并被其欺骗泄露了所持有的验证信息、敏感个人数据或者凭证密钥等，攻击者在获得这些数据后可假扮成注册用户与真正的验证方进行交互并通过其验证	一个注册用户收到了一封邮件并被引导到了一个假冒的网上银行，在该假冒网上银行上登录时泄露了其用户名和密码	防范目标：让实施假扮的攻击者无法成功获取凭证密钥或者认证有效验证值，用以后续假扮注册用户进行攻击。 防范措施：使用个性化的设置来提示用户是否遇到了伪冒服务器，例如用户自行设定的登录前提示语、登录后欢迎词等；使用基于密码学原理的安全鉴权机制等
网域欺骗	注册用户在尝试连接一个合法的验证方时，被攻击者通过修改 DNS 或路由表的方式引导到攻击者的网上银行	通过 DNS 污染的方式，注册用户在登录一个合法网上银行时被引到了一个假冒网上银行，在该假冒网上银行上登录时泄露了其用户名和密码	
窃听攻击	攻击者通过监听认证协议报文，来获取可以用于后续假扮注册用户的信息	攻击者通过监听获取了在传输过程中的用户密码或者密码哈希值	防范目标：让攻击者即使录制了注册用户与身份认证服务提供方之间的通讯报文，也无法从中分析出能够让攻击者假扮成注册用户的有效信息。 防范措施：使用受保护的安全通讯协议如 TLS 等
重放攻击	攻击者通过重复使用此前获取的报文信息来假扮注册用户到验证方进行验证	攻击者在此前的一个实际验证会话中获取了注册用户的口令或者口令哈希值，并在后续使用该信息尝试再到验证方进行验证	防范目标：防止攻击者通过记录并重放此前的成功验证协议报文，来通过后续的身份认证过程。 防范措施：在通讯协议中使用随机数或者挑战值
会话劫持	攻击者将其自身嵌入到注册用户与验证方的通讯会话流程中，面对注册用户可模仿成验证方，反之面对验证方可模仿成注册用户	攻击者通过窃听手段拿到用于标识 HTTP 请求的验证值，并非法使用该验证值伪装成注册用户，达到攻击目的	防范目标：将认证跟数据传输绑定起来，防止攻击者参与到数据传输会话中而没有被检测到。 防范措施：通过为每次验证会话都生成单独的会话密钥用于会话数据传输

安全威胁	描述	攻击示例	防范目标与措施
中间人攻击	攻击者将其自身放置在注册用户与验证方之间，获取并修改通讯报文中内容。一般而言，攻击者会同时面向注册用户模仿成验证方和面向验证方模仿成注册用户	攻击者通过侵入路由表转发注册用户与验证方之间的报文。转发报文时，攻击者使用自己的公钥代替验证方的公钥，注册用户被其欺骗后，攻击者就可解密获得注册用户的密码等敏感信息	弱级别中间人攻击的防范目标：应提供措施供注册用户判断其是否在与真实的验证方之间进行通讯。但攻击者仍有可能获得注册用户的验证值用于假扮注册用户并能通过验证方验证； 强级别中间人攻击的防范目标：应能完全避免注册用户向攻击者泄露可以供攻击者用于假扮注册用户的任何信息，让攻击者能够利用该信息假扮注册用户通过验证方验证； 防范措施：使用安全的通讯协议如 TLS 并使用经过国家安全认证的 CA 机构颁发的 SSL 证书
客户端运行环境攻击	攻击者利用终端环境的脆弱性对应用运行环境进行篡改或攻击	攻击者通过定制 ROM 进行摄像头劫持，可绕过客户端人脸识别采集功能	防范目标：加强终端环境监测能力，异常环境下主动退出程序； 防范措施：在客户端建立风险感知和处置能力，在合规的前提下充分采集端点环境数据，通过服务端实时风控系统对风险环境进行交易处置（弹窗提醒、阻断交易、退出程序等）

6 交易安全性

6.1 抗抵赖机制

应用系统中如涉及资金转移、开户类的交易，交易提交方应采用以下任一种方式：

- 交易提交方在交易数据中应附加发送原发者身份、发送位置、发送日期和时间等，确保发送方无法否认交易；
- 交易接收方应能够将凭证/存折打印签名等方式作为交易的接收证据；
- 交易提交方采用数字签名技术对交易数据进行数字签名：
 - 客户或第三方用私钥签名，并将签名后数据、签名证书发送给接收方；
 - 系统接收方使用发送方公钥验证签名数据，并保留签名数据以便于审计；
 - 签名数据中可要求使用时间戳加随机码方式，保证签名数据并非事前签名，而是事中签名。

6.2 重放检测机制

在部分交易中，重复提交会导致安全风险，应控制重复提交。当重复交易次数，即重放次数超过规定次数时，应断开该用户的连接并记录日志。对于直接或间接涉及资金变化的交易，至少应选用方式c至方式e中的某一种，以防范重复交易。

- 客户端界面控制：客户端提交交易后采取按钮灰显、遮罩等措施防止客户重复提交；

- b) 服务端控制：包括但不限于使用乐观锁、分布式锁、防重表等技术手段保证服务接口的幂等性；
- c) 简单重放检测机制：如采用计数器、时间标记、验证码等，通过与时间、计数器、验证码比较或与列表匹配检测重放，可防止交易重复提交；
- d) 基于数字签名技术的重放检测机制：采用基于数字签名技术，应通过数字签名数据中的交易次序信息用于标识唯一的一次交易请求，服务器端程序验证签名信息时，应首先验证交易次序信息的有效性，再验证签名的合法性，防止交易重复提交；
- e) 基于动态密码技术的重放检测机制：对于采用动态密码技术进行交易控制时，应在动态密码系统中增加防止重放检测机制，动态密码认证一次有效，认证后动态密码应失效。

6.3 防撞库及恶意查询

在涉及输入用户身份信息（例如用户名、手机号、卡号、证件号、密码等）且后台需要验证身份信息的一致性（例如是否已注册、用户名/密码是否匹配、姓名/证件号/卡号是否匹配）等情况下，应具有防范撞库攻击、恶意查询的措施，具体要求如下：

- a) 图形验证码技术及要求：
 - 1) 图形验证码应由服务器端随机生成，客户端不应包含图形验证码文本内容，且宜由数字和字母组成。当验证失败超过一定次数时，可采用汉字验证码等方式增加自动识别的难度；
 - 2) 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，防范验证码被攻击程序自动识别；
 - 3) 具有使用时间限制并仅能使用一次。
- b) 其他验证码技术：
 - 1) 滑块验证码；
 - 2) 动态语义验证；
 - 3) 必要时可根据用户多维环境因素建立分级模型，精确区分可信、可疑和恶意用户，并使用不同的验证方式。
- c) 限制终端交易频率：限制一定时间内的交易执行次数。考虑到不同终端可能存在相同的内网 IP、外网 IP，为了避免控制范围的扩大化，宜以设备 ID 为维度进行交易频度的限制，设备 ID 可由不同的硬件信息或软件信息组合而成，不宜单独以 IP 为维度进行限制；
- d) 可信终端检查：用户通过可信方式成功认证后，应用系统建立用户可信终端列表，限制用户只能从可信的终端执行相关交易，若检测到终端存在操作系统重装或初始化操作后，应将终端设置为不可信状态；
- e) 动态验证码：限定使用动态验证码才能执行交易，如手机短信验证码、电子密码器验证码；
- f) 数字签名技术：限定使用数字签名技术才能执行交易，如 U 盾。

对于不涉及资金变动交易或资金变动交易需要结合其他认证手段的应用系统，至少应采取上述任意一种方式；对于用户名及静态密码登录后可直接执行资金变动交易的应用系统，至少应采用方式 c 至方式 e 中的一种。

6.4 交易合法性检查

交易合法性检查及漏洞防范的要求如下：

- a) 合法性检查范围包括所有外部提交的交易要素，如前端提交、接口传入的需增删改的要素、交易的检索要素、业务/技术标识等；
- b) 合法性检查内容应包括参数的合法性（类型、长度、格式、上下限边界、参数之间的匹配关系等）、用户权限合法性等技术及业务类规则；

- c) 应在服务端采用参数化查询、存储过程等预编译方式分离数据库指令及参数，防范 SQL 注入攻击；
- d) 对于解析 XML 报文的场景，服务端应禁用 XML 解析组件的外部实体引用功能，防范 XML 外部实体引用攻击（XXE）；如果不能禁用，则应对 XML 报文中的外部实体引用内容进行数据合法性检查；
- e) 对交易请求逻辑顺序进行合理控制。在涉及多个步骤的业务交易中，在每个步骤中，后台应确认相关权限，并对上一步骤的流程作出判断。在进行关键交易请求时，服务器应对前面流程中的认证合法性进行校验，应避免绕过前面认证流程，防止流程跳跃或认证绕过，防止发生垂直越权；
- f) 通过互联网或专线对外服务且用户可上传文件的应用系统，应采取以下措施对上传的文件进行合法性检查：
 - 1) 上传文件应保存在 WEB 程序目录之外的其他目录并禁止在服务器端执行，禁止被不必要的账户访问；
 - 2) 应严格限定上传文件类型，并在服务端对上传文件进行检查，优先通过白名单方式仅允许上传必要的文件类型，禁止上传可执行文件及脚本；
 - 3) 应对用户提交的文件名进行检查，禁止包含非法字符，上传后应修改文件名；
 - 4) 上传文件大小应有最大值限制；
 - 5) 接收文件的服务器宜部署杀毒软件对文件内容进行扫描。

6.5 交易漏洞防范

交易漏洞防范的要求如下：

- a) 对于通过互联网及专线对外服务的 BS 应用系统，应对用户提交参数进行检测，过滤存在危害的字符，防范跨站脚本攻击（Cross-site scripting, XSS）；
- b) 对于通过互联网及专线对外服务的 BS 应用系统，如果涉及资金转移、客户信息/协议调整的交易，相关页面应采取与客户二次交互，防范客户会话信息被窃取后，攻击者利用跨站请求伪造攻击（CSRF）伪造交易报文，在客户不知情的情况下完成恶意交易；
- c) BS 应用系统如使用 cookie 且 cookie 中包含登录后的会话标识，应设置 cookie 的 HTTP only 属性，对于采用 HTTPS 连接的，应设置 cookie 的 secure 属性；
- d) BS 应用系统中服务端如涉及调用其他服务端 URL 资源且该 URL 地址可被前端查看，应采用服务器端拼接跳转地址或别名映射等安全方式防范 URL 跳转漏洞，不应将跳转的目的 IP、端口和路径直接在 URL 中显示，避免服务端信息暴露而被利用。

7 数据安全性

7.1 传输数据的机密性保护

应用系统数据传输时，采取以下方式保证通信数据传输的机密性：

- a) 应用系统数据通过内网传输时，应在应用层采用对称密码算法或非对称密码算法，对传输的用户密码等鉴别信息和密钥（不含公钥），及银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等支付敏感信息进行机密性保护；
- b) 应用系统数据通过内网传输时，应在应用层采用对称密码算法或非对称密码算法，对传输的银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等支付敏感信息进行机密性保护；

- c) 应用系统数据通过专线网络对外传输时，对于由本行主导制定通信规则的情况，应选用对称密码算法或非对称密码算法对传输的银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等支付敏感信息以及个人身份信息进行机密性保护；
- d) 应用系统数据通过互联网传输时，应使用 HTTPS 等加密通信协议，并选用对称密码算法或非对称密码算法，对传输的银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等支付敏感信息以及个人金融信息进行机密性保护；
- e) 应用系统数据传输时，采用的对称密码算法中的对称密钥、非对称密码算法中的非对称密钥，都应由客户端与服务端通过随机数生成与内置种子等方式协商生成，数据传输过程中不应涉及生成后的对称密钥、非对称密钥的传输。

7.2 传输数据的完整性保护

应用系统数据传输时，采取以下方式保证敏感信息的完整性：

- a) 协商应用通讯报文格式：应结合应用和业务特点，通信双方协商专门的通讯报文格式，接收方通过验证通信数据中各字段是否符合报文格式要求，检查其完整性是否遭到破坏；
- b) 应通过业务规则来检查数据完整性是否遭到破坏，内容包括但不限于：
 - 1) 统计交易记录总数，并将记录总数附在传输数据后，接收方做验证；
 - 2) 统计文件总数，并将文件总数附在传输数据后，接收方做验证。
- c) 发送方对传输的敏感信息采用密码技术计算校验码，接收方对校验值做验证，检查其完整性是否遭到破坏；
- d) 应在客户端和服务端进行数据完整性校验，防止数据包被替换、字段被篡改。

7.3 存储数据的机密性保护

存储数据机密性保护的要求如下：

- a) 应采取访问控制机制，确保客户信息、账户信息和密码信息等各类敏感信息不被授权以外的任何用户或授权用户以任何未经授权的方式访问；
- b) 中间环节应用系统的服务器和终端设备中不应存放本行和合作单位的客户鉴别信息（如密码、PIN、磁道信息、CVV、CVV2、CVN、CVN2 等）；
- c) 应对系统中的各类密码、密钥加密存放；
- d) 对于涉及商业秘密和敏感信息的电子文件，应结合业务部门需求，使用电子文件安全控制系统进行加密和授权；
- e) 密钥的生成、存放、销毁宜在加密机中进行。

7.4 存储数据的完整性保护

存储数据完整性保护的要求如下：

- a) 可采用操作系统、数据库和存储系统提供的系统级完整性机制保证重要数据的完整性，若数据库采用透明加密方式，对应用层是透明的，不足以满足存储完整性和机密性要求，需配合应用层字段校验和加密等措施有效应对 SQL 注入、拖库、DBA 篡改数据等攻击；
- b) 可根据重要数据的业务关系，检查其完整性是否遭到破坏，如账务的总分核对等；
- c) 存储时可对重要数据采用密码技术计算校验码，检查时重新计算并核对，如密码等数据在使用时也应进行核对，以检查其完整性是否遭到破坏。

7.5 页面展示信息的保护

页面展示信息的要求如下：

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/385013342314011120>