软件安全开发制度

Plain Text

安全编码原则
1. 保持简单，程序只实现指定的功能。
2. 坚持最小权限，把可能造成的危害降到最低。
3. 默认不信任，采用白名单机制，只放行已知的操作。
4. 永远不要相信用户的输入，对所有输入进行前台和后台两次检查。

2 常见WEB潜在问题
输入验证：嵌入到查询字符串、表单字段、cookie 和 HTTP 头中的恶意字符串的攻击。这些攻击包括命令执行、跨站点脚本(XSS)、SQL 注入和缓冲区溢出攻击。
身份验证：标识欺骗、密码破解、特权提升和未经授权的访问。
授权验证：访问保密数据或受限数据、篡改数据以及执行未经授权的操作。
配置管理：对管理界面进行未经授权的访问、具有更新配置数据的能力以及对用户帐户和帐户配置文件进行未经授权的访问。
敏感数据：泄露保密信息以及篡改数据。
会话管理：捕捉会话标识符，从而导致会话劫持及标识欺骗。
加密管理：访问保密数据或帐户凭据，或二者均能访问。
参数操作：路径遍历攻击、命令执行以及绕过访问控制机制，从而导致信息泄漏、特权提升和拒绝服务。
异常管理：拒绝服务和敏感的系统级详细信息的泄漏。
审核和记录：不能发现入侵迹象、不能验证用户操作，以及在诊断时出现困难。

3 页面组件安全防范
1. 页面标签必须关闭，属性值必须加引号。在页面中使用的标签不关闭，属性值不加引号往往成为被攻击点，攻击者很容易的利用这些漏洞进行注入。避免这些漏洞的出现可以提高被攻击的可能。
2. Form提交方式必须选用POST。Form默认的提交方式是Get，这种方式将表单中数据的按照variable=value的形式，使用“?”添加至Action所指向的URL后面，各个变量之间使用“&”连接。所要传递的信息量除受URL长度限制之外，信息内容都显示暴露。

4 敏感数据的安全防范
不能任意在Cookie、Session、ServletContext中存放数据，对于这些对象中存放的数据，必须有统一定义说明、Lifecycle的管理等。
对于敏感信息都必须保障其私密性。在页面显示、操作交互中不可避免的会有一些如用户的标识信息、密码、帐号信息。为保障这些数据不被曝露而提高安全性，我们要做到所有敏感信息必须进行加密处理，不能以明文的形式存在于任何网络、内存及其它持久化介质中(如：数据库、文件磁盘系统等)

5.加密标准
因系统使用 SpringBoot开发;密码加密使用 SpringSecurity中的BCryptPasswordEncoder对密码加密存储，BCryptPasswordEncoder 的特点是内置随机 slat，即便相同密码两次都会计算出不同容文，足够安全。
前后端之间使用RSA的方式来进行身份确认，前端敏感信息时，敏感信息使用与后端约定的 slat 值对密码进行加密，杜绝明文传输。服务配置文件敏感信息，统一使用 jasypt 密钥进行加密。杜绝明文配置呈现。系统方案中充分考虑系统过程中的安全性需要，提供完备的操作权限管理办法和完善的日志记录。本系统采用如下的安全策略和机制保障系统的安全性:系统提供完善的授权机制。根据不同的业务需要，采用不同的安全措施;对所有接触系统的人员进行权限等级设置，按其职责划定必须

的最小授权范围，详细限定各个权限等级操作人员所能执行的不同系统功能，防止与系统有关的人员非法修改程序和修改操作运行步骤来分割系统，防止超越权限使用系统，从而避免操作人员误操作或恶意操作而造成系统数据的破坏或丢失。

具备完善的应用系统日志，以检测和发现系统的故障差错或对系统的恶意侵害行为。本系统自动记录用户的登录活动和关键性操作，提供方便的发现并排除系统故障的功能。

文件信息，分布式文件存储，由于本次方案中不涉及大文件存储，所以文件信息直接存入 mongod服务器，暂不考虑搭建文件服务器。

定时数据备份。

系统补丁管理

由运维团队控制管理公司系统版本及系统补丁，更新内容由安全管理委员会成员。审核后交由运维团队排期处理。

评审需要确认处理等级，漏洞风险等级。

处理等级（处理时间）

【P1】主流程阻塞或用户核心期望<=1周内处理并发布

【P2】支线流程阻塞或用户期望内容<=4周内处理并发布

【P3】明显的UI展示或UE交互，对使用体验有影响

【P4】需要优化但不影响日常使用

漏洞风险等级

险实际的描述了此类问题导致的真正风险。

高危：可能导致公司商务或项目失败的风险

严重：会导致项目业务受损，并导致投诉

一般：会导致投诉并导致公司使用成本处理

较小：可以接受的风险，不会对公司业务项目产生影响

系统安全配置制度

1.系统安全性设计

整个系统的安全取决于系统运行物理环境的安全性、服务器及网络的安全性、操作系统的安全性、应用系统的安全性及应用数据的安全性等，通过设计实施整体的安全策略，对安全策略的实施结果进行评

估，及时采取修复补救措施，调整安全预防策略，综合动态地进行系统安全管理。

本系统的安全体系和一般信息系统的类似，也需要设计实施整体综合的安全策略，纳入总体安全体系，确保系统的安全运行。

由于本系统建立在商业银行现有的物理环境和网络环境中，环境安全性很好，并将不断完善优化，因此，有关本系统的安全设计的主要对象是系统自身的应用安全、数据安全、服务器操作系统和数据库的安全管理维护。

本系统与外联系统的数据传输安全严格遵循甲方外联网络相关技术规范。

本系统满足中国人民银行《金融行业信息系统信息安全等级保护测评指南》（JR/T 0072—2012）中第三级的要求，支持三级要求中的网络安全、主机安全、应用安全、数据安全。

网络安全要求：

1、保证主要网络和通信线路冗余；

2、保证网络各个部分的带宽满足业务高峰期需要；

3、加强网络访问控制；

主机安全要求：

1、具有身份认证与标识、鉴别功能；

2、控制用户对资源的访问权限;

应用安全要求：

1、对用户进行资源访问授权；

2、通信完整性，通过哈希值、摘要保证通信完整性；

3、通信保密性要求，通过专用的通信协议或加密的方式保证通信过程的加密性。

4、系统提供完整的交易日志；

数据安全要求：

1、保证数据完整性，保密性；

2、提供完备的和切实可行的数据备份与恢复方案，以及切换演练和应急切换步骤。

1.1 系统面临的安全威胁

本系统作为银行的管理系统，需要考虑系统及数据可能面临的以下安全威胁：

- 非人为因素：服务器意外断电、损坏、硬盘出错或损坏，网络中断等；
- 人为因素：操作失误，恶意攻击，病毒破坏等；
- 信息泄露、信息窃取、假冒、抵赖等；

- 系统软件安全漏洞。

1.2 系统安全方案

整个系统的安全取决于系统运行物理环境的安全性、服务器及网络的安全性、操作系统的安全性、应用系统的安全性及应用数据的安全性等，通过设计实施整体的安全策略，对安全策略的实施结果进行评估，及时采取修复补救措施，调整安全预防策略，综合动态地进行系统安全管理。

本系统需要设计实施整体综合的安全策略，纳入甲方总体安全体系，确保系统的安全运行。在系统实施过程中遵循以下方面的安全策略：

1.2.1 网路安全

本系统构建在企业内部网络，部署遵循企业网络架构，不同功能层/区之间的访问严格按照点对点进行访问控制。

网络中安装防火墙，进行访问检测、监测、控制、审查分析，阻止非法恶意攻击入侵，高级别的保护可以禁止一些服务，如视频流，Java、ActiveX、JavaScript脚本等，阻止恶意代码进入。

1.2.1.1 外联系统网络安全

本系统与外联系统的数据传输网络安全严格遵照执行外联网络建设相关规范的安全要求，同时复用已有的互联网连接及其安全控制措施：

- 外联单位业务主机必须通过安全控制设备（如防火墙）访问网络，外联单位系统必须与外联区的业务前置机进行数据交换，不得直接访问内部网。
- 在内网区部署一台内网数据中转服务器，由该服务器统一实现内网服务器与各业务前置机的数据交换，保障内网数据安全。
- 采取层次防护、区域控制的策略，通过边界防护和核心防护保护外联网络系统安全。
- 通过NAT技术，对外隐藏内部网络结构。
- 采用静态路由，限制外联单位访问。
- 同一个平台的多个业务流用ACL进行严格的隔离，使每一个业务流严格地按照规定的静态路由传输。
- 通过IDS系统对外联区进行入侵检测和行为审计。
- 对外联平台使用的网络设备、安全设备和服务器进行严格的访问控制，保障设备的运行安全。
- 定期分析、评估防火墙和IDS的日志，及时处理各级报警信息，并采取有效措施进行解决。对发现的恶意入侵事件应及时处理并立即上报。

安装Windows系统的统一外联平台主机按照行业规定安装相关安全软件，并确保能够及时升级病毒库和系统补丁。

1.2.1.2 服务器及客户端系统安全

为避免单点故障，应用服务器、数据库服务器等需采用集群或HA配置。

对于服务器操作系统，进行相应的安全配置维护管理，及时打补丁，安装反病毒程序，定期查杀病毒，根据实际情况及时进行安全策略调整，定期进行有关系统的数据备份。

对于数据库系统，进行相应的安全配置维护管理，根据实际情况及时进行安全策略调整，定期进行数据库系统的有关备份。

由于客户端计算机用途很开放，很容易受到病毒感染、恶意攻击等，可能会进一步影响到服务器，因此，对客户端计算机也要采取安全措施，进行相应的安全配置管理，如设置有效的系统密码，设置较高的浏览器级别，及时打补丁，安装反病毒程序，定期查杀病毒，根据实际情况及时采取安全措施。

1.2.1.3 终端准入机制

系统具备终端准入机制，只能允许已经注册认证的合法终端才能够访问系统服务。

系统根据IP设置接入应用的黑白名单。

1.2.2 主机安全

1.2.2.1 身份认证与标识、鉴别

系统提供完备的权限管理、用户认证、密钥管理方案。

系统支持多种柜员认证机制，目前已在使用的有密码、指纹。

系统支持用户认证失败超过指定次数后的锁定机制，用户锁定后需要主管用户对其进行解锁，用户忘记密码可以向高级别柜员申请重置密码。

用户密码认证支持有效期，超过有效期后，会要求用户修改密码

系统可控制用户登陆地点，通过机构下可使用IP地址范围，限定不在IP地址范围内终端不得登陆。

平台可采用SSL加密传输的方式，用户和服务方之间在网络上传输的所有数据全部用会话密钥加密，直到用户退出系统为止，而且每次会话所使用的加密密钥都是随机产生的。

➢ 鉴别机制（采用用户名和口令机制）

• 输入口令字时以“*”回显；

• 用户的口令是以密文方式存在数据库中；

• 用户认证通过后，如果在一定时间内（该时间可以通过配置文件设定）无操作，需要重新认证；

➢ 鉴别失败处理

• 当用户连续鉴别错误次数超过门限条件时（该次数可以通过配置文件设定），将该用户锁定，该用户必须通过管理员解锁；

• 返回有限的失败信息(“用户名或密码错”）；

➢ 应用系统中的口令规范

• 系统限制口令长度至少六位；

• 口令存储的密码技术使用与密码支持按本页密码支持的要求；

• 系统初始化用户时，默认密码为指定字符串，用户第一次登录系统时强制要求修改初始密码；

• 强制口令一定期限内（此期限是在参数中定义的）更新，默认为30天；

1.2.2.2 资源利用

本系统能够对应用系统的最大并发会话连接数进行限制；

1.2.3 应用系统安全

1.2.3.1 访问控制

➢ 访问控制机制

• 系统权限控制以角色为权限集合，控制用户权限；

• 粗粒度控制“系统功能（菜单）”访问权限；

• 细粒度控制数据权限，如：“页面表单元素（文本框、下拉框、按钮等）”操作权限、列表一条数据的查看、修改、删除权限；

➢系统支持用户会话超时失效，自动退出功能。

1.2.3.2 安全审计

系统提供完善的日志管理体系。系统对用户登录情况，如登录用户、进入时间、操作功能项等进行自动记录； 对于数据录入、数据提交、任务开始和数据分析等应用处理的时间、数据范围、 执行情况等也自动记录日志，以便出问题时跟踪追查审计。

系统对请求的数据报文都记录接受时间，响应时间，接口报文，操作员，请求成功标识等信息，便于追踪请求数据的正确性及及时找出错误原因。

➢ 安全审计机制

• 系统具有机构、用户、交易的安全控制审计机制；

•系统通过身份及密码验证、操作日志登记及查询、交易日志登记及查询、交易复核及授权、交易权限配置等机制，保证系统的安全。系统在客户端登陆,服务端会签发一个token发送给客户端，客户端将token存储在cookie里，后面客户端访问服务端都需要带着token去访问，服务端首先要对客户端token进行验证，通过后才允许访问。

•系统提供重要信息变更登记机制，系统会登记修改前后的信息要素，供查询或审计使用。

•系统提供详细的交易日志及报文日志，同时提供数据库变更日志，确保数据安全性。同时提供数据一致性检查的功能。

•系统对于交易数据和日志，系统具有完善的防篡改机制，防止对数据和交易日志文件进行直接修改。系统对于前端请求后端的机制进行了相关类名，方法，数据进行加密处理，无法对前端数据进行篡改。系

统通讯层可以对报文中的敏感字段进行加密处理，如密码等，以防密码信息泄露，同时通讯层可以对报文进行md5计算，然后将计算的值放入报文头中，系统得到报文之后对报文体在进行md5计算，然后将计算的值跟报文头中的md5值进行比较，以确保报文未被篡改，保证数据传输的安全性。

•系统在数据库层和应用层，进行严格的操作权限控制，防止对数据和交易日志文件进行直接修改。

➢ 日志产生

• 系统后台可配置产生功能调试日志，如：访问功能相关的SQL语句；

• 系统记录用户登录日志；

• 可配置记录用户菜单访问日志

• 可配置记录系统功能日志：系统可配置性记录用户的功能操作日志，日志记录包括操作时间、操作用户、操作对象、操作用户IP等。

1.2.3.3 密码支持

系统采用MD5加密方式，加密页面关键跳转信息，如：访问后台方法名，跳转路径等；

1.2.2.4 加密方案

系统的安全机制基于可插拔式开发，具有很强的独立性，可以通过简单安全适配器开发，达到适配不同的安全产品的目的，故可以替换不同的安全产品（如通讯加密、PIN加密等），使用农发行的加密方案。

1.2.3.5 加密算法支持

系统符合人民银行、银监会等监管部门有关加密算法的最新规定及要求，支持国密算法，包括：SM1对称加密算法，SM2公钥算法，SM3密码杂凑算法，其中SM1对称加密算法，加密强度为128位，采用硬件实现；SM2为国家密码管理局公布的公钥算法，其加密强度为256位；SM3密码杂凑算法，杂凑值长度为32字节。

1.2.3.6 交易日志

系统对所有系统操作提供日志记录，包括但不限于变更类操作的用户、发生时间、具体操作动作和变更内容，并提供日志管理功能，包括但不限于友好的日志查询与管理界面、日志记录策略的设置以及日志的安全性的保障。

系统提供对新增类数据审计日志、变更类数据审计日志的查询。

系统提供日志导出功能。

系统提供多维度的安全性保障措施：

1)日志记录中包含了时间戳字段，避免被非法篡改。

2)日志表本身也可以配置登记变更日志的策略，可以达到双重保障。

3)日志中的敏感数据支持字段级配置化加密。

4)日志表中的数据可以配置数据清理策略，将历史数据的持久化纳入全行级数据生命周期管理中。

1.2.4 数据安全设计

1.2.4.1 数据备份策略

系统产品在实施过程中将提供完备的和切实可行的数据备份与恢复方案，以及切换演练和应急切换步骤。

数据备份策略：

数据库运行在归档日志模式，可以联机在线进行备份，不影响数据库的访问。数据表采用定期归档、备份策略：

定期（如：每个月进行）将数据表进行清理，将过期数据导入归档数据库，并对归档库进行备份；

同时，对在线库进行定期（全备可以定为每月）全备，并结合每天增量备份的方式；

归档、备份时不影响系统运行。

一般性数据恢复时首先确定恢复数据和时点，并从备份数据中先恢复全量备份，再恢复之后的增量备份，完成恢复。

对于灾难性恢复，则通过恢复最近一次的数据备份及源系统数据进行数据追补。日常备份最小时间间隔不大于1 天，以保障灾难发生时数据丢失小于24小时的RPO目标。

备份数据异地保存，并配置灾备软硬件环境，每日备份数据预先恢复到灾备环境，当灾难发生时，只需要做切换工作，以保障业务中断不超过4小时的RTO目标。

备份时间点

备份时间应该避开数据处理繁忙时间段，可在每天批处理完成后进行备份。

1.2.4.2 数据传输安全

系统支持数据存储、数据传输、密钥管理等方面的安全功能。系统与其他系统间的数据交互，采用数据接口文件方式进行，系统之间数据库不互相开放。与其他系统间批量数据文件传输通过企业数据集成平台进行，传输过程中建议对数据进行压缩、加密，实现数据安全可控传输。

用户客户端与WEB、应用服务器间支持采用HTTPS协议，对数据传输过程进行加密。