福建水务营收系统-安全设计

系统设计团队

2024年12月19日

1 福建水务营收系统安全设计文档

1.1 文档信息

项目信息	详情
项目名称	福建水务营收系统
文档类型	安全设计文档
技术框架	RuoYi-Vue-Pro + 达梦数据库 8.0+
文档版本	v1.0
编写日期	2024-12-19
文档状态	已完成

1.2 章节导航（精简）

安全设计概述

福建水务营收系统安全设计结合水务行业特点和国产化要求，构建全方位、多层次的安全防护体系。

1.2.1 安全目标

- **机密性**：确保敏感数据不被未授权访问
- **完整性**：防止数据被恶意篡改或损坏
- **可用性**：保障系统7×24小时稳定运行
- **可审计性**：完整记录系统操作审计轨迹
- **合规性**：满足行业监管要求

1.2.2 安全原则

- **纵深防御**：多层安全防护，避免单点故障
- **最小权限**：用户和应用仅具备必要的最小权限
- **默认安全**：系统默认采用最严格的安全配置
- **持续监控**：7×24小时安全监控和威胁检测
- **国产化优先**：优先采用国产安全产品和技术

1.2.3 总体安全架构

```
graph TB
    subgraph "外部威胁"
        THREAT1[网络攻击]
        THREAT2[恶意软件]
        THREAT3[数据泄露]
        THREAT4[内部威胁]
    end

    subgraph "安全防护层"
        subgraph "边界安全"
            WAF[Web应用防火墙]
            FW[网络防火墙]
            IPS[入侵防护系统]
            VPN[VPN网关]
        end

        subgraph "应用安全"
            AUTH[身份认证]
            AUTHZ[访问控制]
            AUDIT[操作审计]
            ENCRYPT[数据加密]
        end

        subgraph "数据安全"
            TDE[透明数据加密]
            RLS[行级安全]
            MASK[数据脱敏]
            BACKUP[安全备份]
        end

        subgraph "运维安全"
            MONITOR[安全监控]
            LOG[日志分析]
            ALERT[告警响应]
            PATCH[安全更新]
        end
    end

    subgraph "核心资产"
        APP[水务营收系统]
        DB[达梦数据库]
        FILE[文件存储]
        API[接口服务]
    end

    THREAT1 --> WAF
    THREAT2 --> FW
    THREAT3 --> IPS
    THREAT4 --> VPN

    WAF --> AUTH
    FW --> AUTHZ
    IPS --> AUDIT
    VPN --> ENCRYPT

    AUTH --> TDE
    AUTHZ --> RLS
    AUDIT --> MASK
    ENCRYPT --> BACKUP
```

```
    ENCRYPT --> BACKUP

    TDE --> MONITOR
    RLS --> LOG
    MASK --> ALERT
    BACKUP --> PATCH

    MONITOR --> APP
    LOG --> DB
    ALERT --> FILE
    PATCH --> API
```

达梦数据库安全

1.2.4 数据库安全架构

```
graph TB
    subgraph "达梦数据库安全特性"
        subgraph "身份认证"
            PWD[密码认证]
            CERT[证书认证]
            LDAP_AUTH[LDAP认证]
            KERBEROS[Kerberos认证]
        end

        subgraph "访问控制"
            RBAC_DB[基于角色的访问控制]
            RLS_DB[行级安全策略]
            CLS_DB[列级访问控制]
            SCHEMA[模式权限控制]
        end

        subgraph "数据加密"
            TDE_SM4[TDE透明加密<br/>SM4国密算法]
            SSL_SM[SSL传输加密<br/>SM2/SM3/SM4]
            FIELD_ENC[字段级加密]
            BACKUP_ENC[备份加密]
        end

        subgraph "审计监控"
            AUDIT_LOG[操作审计日志]
            LOGIN_LOG[登录审计]
            DDL_LOG[DDL操作记录]
            SECURITY_LOG[安全事件日志]
        end
    end

    PWD --> RBAC_DB
    CERT --> RLS_DB
    LDAP_AUTH --> CLS_DB
    KERBEROS --> SCHEMA

    RBAC_DB --> TDE_SM4
    RLS_DB --> SSL_SM
    CLS_DB --> FIELD_ENC
    SCHEMA --> BACKUP_ENC

    TDE_SM4 --> AUDIT_LOG
    SSL_SM --> LOGIN_LOG
    FIELD_ENC --> DDL_LOG
    BACKUP_ENC --> SECURITY_LOG
```

1.2.5 国产密码算法应用

1.2.5.1 传输加密

- 配置国密SSL连接，使用SM2/SM3/SM4算法套件
- 支持SM4-GCM-SM3和SM4-CCM-SM3加密套件
- 配置国产SM2证书和私钥文件
- 强制要求SSL连接，拒绝明文传输

1.2.5.2 透明数据加密

- 启用TDE透明数据加密，使用SM4算法
- 为敏感数据表配置列级加密
- 支持确定性加密和随机化加密
- 集成本地密钥管理系统(localkms)

1.2.6 行级安全策略

- 创建多租户行级安全策略，实现数据隔离
- 配置基于用户角色的数据访问控制
- 实现动态数据过滤和权限控制
- 支持复杂的安全策略表达式

1.2.7 数据脱敏策略

- 创建敏感数据脱敏函数和规则
- 为不同角色提供不同级别的数据视图
- 实现手机号、身份证号等敏感信息脱敏
- 支持动态脱敏和静态脱敏

应用系统安全

1.2.8 Spring Security安全配置

1.2.8.1 认证配置

- 使用国密SM3哈希算法进行密码加密
- 配置JWT身份验证过滤器
- 设置CSRF防护和HttpOnly Cookie
- 配置请求授权规则和无状态会话管理
- 启用方法级安全注解支持

1.2.8.2 多因素认证实现

- 生成随机验证码并缓存到Redis
- 设置验证码过期时间防止滥用
- 集成短信服务提供商发送验证码
- 实现验证码验证和及时清理机制

1.2.9 数据传输安全

1.2.9.1 HTTPS配置

- 启用HTTPS协议，使用SSL/TLS加密
- 配置国产密码算法套件支持
- 使用PKCS12格式的数字证书

- 支持TLSv1.2和TLSv1.3协议版本

1.2.9.2 银行文件传输安全约束

- 银行文件交换默认优先使用 `SFTP`；`FTP` 仅作为兼容能力保留，需在风险评估通过后启用。
- 文件传输凭据以 `credentialRef` 引用形式由环境配置或配置中心承接，不在正式文档、默认仓库配置样例或测试样本中写入明文密码、私钥、证书。
- 命中协议缺少 `host/port/username/credentialRef` 时必须立即阻断当前文件动作，避免以残缺配置尝试连接银行通道。
- 路径模板仅允许固定变量白名单，禁止自由表达式、脚本化拼装和未声明变量，防止目录逃逸与错误路由。
- 批次审计只保存最终实际使用的协议、目录、文件路径与文件名，不额外保存完整凭据快照，避免敏感配置在业务表中扩散。

1.2.9.3 敏感数据加密

- 采用国密SM4对称加密算法
- 实现统一的数据加密和解密服务
- 对身份证号、手机号等敏感信息加密存储
- 提供统一的异常处理和错误提示

1.2.10 接口安全防护

1.2.10.1 接口签名验证

- 基于时间戳、随机数和请求体生成签名
- 使用国密SM3哈希算法计算签名值
- 检查时间戳有效性防止重放攻击
- 实现客户端和服务端签名比对验证

1.2.10.2 接口限流防护

- 基于Redis实现分布式限流控制
- 支持按IP、用户、接口等维度限流
- 采用滑动窗口算法统计请求频率
- 超过限制时返回429状态码和错误提示

网络安全设计

1.2.11 网络拓扑安全

```
graph TB
    subgraph "外网区域"
        INTERNET[互联网]
        CDN[CDN加速]
        DNS[DNS服务]
    end

    subgraph "边界防护"
```

```
    WAF[Web应用防火墙<br/>国产WAF产品]
    FW_BORDER[边界防火墙<br/>安全审计]
    IPS[入侵防护系统<br/>威胁检测]
    DPI[深度包检测<br/>流量分析]
end

subgraph "DMZ区域"
    LB[负载均衡器<br/>SSL卸载]
    WEB1[Web服务器1]
    WEB2[Web服务器2]
    PROXY[反向代理]
end

subgraph "内网安全"
    FW_INTERNAL[内部防火墙]
    VLAN_APP[应用VLAN]
    VLAN_DB[数据库VLAN]
    VLAN_MGT[管理VLAN]
end

subgraph "应用层"
    APP1[应用服务器1]
    APP2[应用服务器2]
    APP3[应用服务器3]
end

subgraph "数据层"
    DB_MASTER[达梦主库]
    DB_SLAVE[达梦从库]
    REDIS[Redis集群]
end

subgraph "管理层"
    JUMP[跳板机]
    MONITOR[监控服务器]
    LOG[日志服务器]
end

INTERNET --> CDN
CDN --> DNS
DNS --> WAF
WAF --> FW_BORDER
FW_BORDER --> IPS
IPS --> DPI
DPI --> LB

LB --> WEB1
LB --> WEB2
WEB1 --> PROXY
WEB2 --> PROXY

PROXY --> FW_INTERNAL
FW_INTERNAL --> VLAN_APP
FW_INTERNAL --> VLAN_DB
FW_INTERNAL --> VLAN_MGT

VLAN_APP --> APP1
VLAN_APP --> APP2
```

```
    VLAN_APP --> APP3

    VLAN_DB --> DB_MASTER
    VLAN_DB --> DB_SLAVE
    VLAN_DB --> REDIS

    VLAN_MGT --> JUMP
    VLAN_MGT --> MONITOR
    VLAN_MGT --> LOG
```

1.2.12 防火墙策略配置

1.2.12.1 边界防火墙策略

- 允许HTTPS访问，开放443端口
- 允许HTTP重定向到HTTPS，开放80端口
- 禁止外部直接访问数据库端口
- 允许内网SSH管理，限制管理网段
- 默认拒绝所有其他入站连接

1.2.12.2 应用层防火墙策略

- 只允许来自DMZ区的应用访问
- 允许访问数据库服务器的指定端口
- 允许访问Redis缓存服务
- 允许DNS查询和时间同步
- 默认拒绝其他出站连接

1.2.13 入侵检测与防护

1.2.13.1 IDS/IPS规则配置

- 配置Web应用攻击检测规则
- 配置数据库直接访问告警规则
- 配置暴力破解攻击检测规则
- 设置基于流量特征的异常检测
- 配置威胁情报实时更新机制

数据安全设计

1.2.14 数据分类分级

1.2.14.1 数据分类标准

```
graph TB
    subgraph "数据分类"
        SECRET[机密级<br/>重要业务数据]
        INTERNAL[内部级<br/>一般业务数据]
        PUBLIC[公开级<br/>公开业务数据]
    end

    subgraph "水务业务数据"
        CUSTOMER[客户身份信息<br/>机密级]
        METER[水表计量数据<br/>内部级]
        BILLING[收费账务数据<br/>机密级]
        REPORT[统计报表数据<br/>内部级]
        CONFIG[系统配置数据<br/>内部级]
        LOG[日志审计数据<br/>内部级]
    end

    subgraph "保护措施"
        ENC_HIGH[强加密<br/>SM4+数字签名]
        ENC_MID[访问控制<br/>权限管理]
        ENC_LOW[公开访问<br/>无特殊保护]
    end

    SECRET --> ENC_HIGH
    INTERNAL --> ENC_MID
    PUBLIC --> ENC_LOW

    CUSTOMER --> SECRET
    BILLING --> SECRET
    METER --> INTERNAL
    REPORT --> INTERNAL
    CONFIG --> INTERNAL
    LOG --> INTERNAL
```

1.2.14.2 数据保护策略

- **机密级数据**：强加密存储，严格访问控制
- **内部级数据**：权限控制，审计日志记录
- **公开级数据**：无特殊保护要求
- **敏感字段**：单独加密，支持查询需求

1.2.15 数据备份与恢复安全

1.2.15.1 备份加密策略

- 使用国产密码算法加密备份文件
- 生成备份文件完整性校验码
- 实现备份文件的安全传输
- 定期验证备份文件的完整性

1.2.15.2 数据恢复流程

- 验证备份文件完整性和真实性

- 在隔离环境中进行恢复测试
- 验证恢复数据的完整性和一致性
- 记录详细的恢复过程和验证结果

1.2.16 数据销毁与清理

1.2.16.1 安全数据销毁

- 实现安全的数据删除和物理清除
- 记录数据销毁的审计日志
- 定期清理历史数据和临时文件
- 确保已删除数据无法被恢复

运维安全设计

1.2.17 安全监控体系

1.2.17.1 安全监控架构

```
graph TB
    subgraph "数据采集层"
        AGENT1[系统日志采集]
        AGENT2[应用日志采集]
        AGENT3[数据库日志采集]
        AGENT4[网络流量采集]
    end

    subgraph "数据处理层"
        KAFKA[消息队列<br/>Kafka集群]
        STREAM[流处理<br/>Flink/Storm]
        ETL[数据清洗<br/>Logstash]
    end

    subgraph "存储分析层"
        ES[Elasticsearch<br/>日志存储]
        SIEM[安全信息事件管理<br/>SIEM平台]
        AI[智能分析<br/>机器学习]
    end

    subgraph "可视化层"
        DASHBOARD[监控仪表盘<br/>Grafana]
        ALERT[告警系统<br/>AlertManager]
        REPORT[安全报告<br/>自动生成]
    end

    AGENT1 --> KAFKA
    AGENT2 --> KAFKA
    AGENT3 --> KAFKA
    AGENT4 --> KAFKA

    KAFKA --> STREAM
    STREAM --> ETL
    ETL --> ES

    ES --> SIEM
    SIEM --> AI
    AI --> DASHBOARD

    DASHBOARD --> ALERT
    ALERT --> REPORT
```

1.2.17.2 安全事件检测规则

- **暴力破解检测**：失败登录次数阈值告警
- **异常数据访问**：大量数据查询行为监控
- **权限提升检测**：管理员权限变更告警
- **异常时间访问**：非工作时间访问行为监控

1.2.18 漏洞管理

1.2.18.1 漏洞扫描策略

- 定期进行系统漏洞扫描

- 执行Web应用安全测试
- 进行数据库安全评估
- 生成漏洞扫描报告和修复建议

1.2.18.2 补丁管理流程

```
graph LR
    DISCOVER[漏洞发现] --> ASSESS[风险评估]
    ASSESS --> PLAN[补丁计划]
    PLAN --> TEST[测试验证]
    TEST --> DEPLOY[生产部署]
    DEPLOY --> VERIFY[部署验证]
    VERIFY --> DOCUMENT[文档记录]

    subgraph "评估标准"
        HIGH[高危<br/>24小时内]
        MEDIUM[中危<br/>7天内]
        LOW[低危<br/>30天内]
    end

    ASSESS --> HIGH
    ASSESS --> MEDIUM
    ASSESS --> LOW
```

1.2.19 应急响应预案

1.2.19.1 安全事件分级

级别	描述	响应时间	处理措施
P0	系统完全不可用，数据泄露	15分钟	立即启动应急预案，通知管理层
P1	核心功能受影响，安全风险高	30分钟	启动应急预案，组建应急小组
P2	部分功能受影响，安全风险中等	2小时	安排专人处理，定期汇报
P3	轻微影响，安全风险较低	8小时	正常工作时间处理

1.2.19.2 应急响应流程

```
graph TB
    INCIDENT[安全事件发生] --> DETECT[事件检测]
    DETECT --> REPORT[事件上报]
    REPORT --> ASSESS[影响评估]
    ASSESS --> RESPONSE[应急响应]

    subgraph "应急响应措施"
        ISOLATE[系统隔离]
        PRESERVE[证据保全]
        RECOVER[系统恢复]
        INVESTIGATE[调查分析]
    end

    subgraph "后续处理"
        LESSON[经验总结]
        IMPROVE[流程改进]
        TRAIN[培训加强]
        DOC[文档更新]
    end

    RESPONSE --> ISOLATE
    RESPONSE --> PRESERVE
    RESPONSE --> RECOVER
    RESPONSE --> INVESTIGATE

    INVESTIGATE --> LESSON
    LESSON --> IMPROVE
    IMPROVE --> TRAIN
    TRAIN --> DOC
```

安全管理制度

1.2.20 安全组织架构

1.2.20.1 安全管理组织

```
graph TB
    CEO[总经理<br/>安全最高责任人]
    CISO[信息安全负责人<br/>CISO]

    subgraph "安全管理委员会"
        IT_DIR[IT总监]
        SECURITY_DIR[安全总监]
        COMPLIANCE[合规负责人]
        LEGAL[法务负责人]
    end

    subgraph "安全执行团队"
        SEC_ADMIN[安全管理员]
        SYS_ADMIN[系统管理员]
        DBA[数据库管理员]
        NET_ADMIN[网络管理员]
    end

    subgraph "业务安全责任人"
        BUS_OWNER[业务负责人]
        DATA_OWNER[数据负责人]
        USER_ADMIN[用户管理员]
    end

    CEO --> CISO
    CISO --> IT_DIR
    CISO --> SECURITY_DIR
    CISO --> COMPLIANCE
    CISO --> LEGAL

    IT_DIR --> SEC_ADMIN
    IT_DIR --> SYS_ADMIN
    IT_DIR --> DBA
    IT_DIR --> NET_ADMIN

    SECURITY_DIR --> BUS_OWNER
    SECURITY_DIR --> DATA_OWNER
    SECURITY_DIR --> USER_ADMIN
```

1.2.21 安全管理制度

1.2.21.1 人员安全管理

- **入职安全审查**：对关键岗位人员进行背景调查
- **安全培训**：定期进行信息安全意识培训
- **权限管理**：建立权限申请、审批、回收流程
- **离职管理**：离职人员权限及时回收，签署保密协议

1.2.21.2 系统建设安全管理

- **安全需求分析**：项目立项阶段进行安全需求分析
- **安全设计评审**：设计阶段进行安全架构评审
- **安全测试**：上线前进行安全渗透测试

- **安全验收**：系统上线前进行安全验收

1.2.21.3 系统运维安全管理

- **变更管理**：所有系统变更都需要安全评估
- **备份管理**：定期备份，异地存储，加密保护
- **监控管理**：7×24小时安全监控
- **应急管理**：建立应急响应机制

1.2.22 合规管理

1.2.22.1 法律法规合规

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》
- 《关键信息基础设施安全保护条例》

1.2.22.2 行业标准合规

- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
- GB/T 32918《信息安全技术 SM2椭圆曲线公钥密码算法》
- GB/T 32905《信息安全技术 SM3密码杂凑算法》

1.2.22.3 合规检查清单

- [ ] 年度安全评估报告
- [ ] 安全管理制度建立
- [ ] 安全技术措施落实
- [ ] 安全培训记录完整
- [ ] 应急预案演练记录
- [ ] 安全事件处置记录
- [ ] 第三方安全服务合同

总结

福建水务营收系统安全设计结合达梦数据库的安全特性，建立了全方位、多层次的安全防护体系。通过技术防护、管理制度、人员培训等多重措施，确保系统安全稳定运行，满足水务行业的安全要求。

本安全设计方案的核心特点： 1. **国产化安全**：采用达梦数据库和国密算法 2. **纵深防御**：网络、应用、数据多层安全防护 3. **持续改进**：建立安全监控和应急响应机制 4. **管理规范**：完善的安全管理制度和流程