

福建水务营收系统-报装CA电子签章补充

系统设计团队

2024年12月19日

- 1 福建水务营收系统报装电子签章设计补充说明
 - 1.1 章节导航（精简）
 - 1.2 文档定位与边界
 - 1.3 集成架构与交互边界
 - 1.4 接口清单与字段约定
 - 1.4.1 接口清单
 - 1.4.2 字段约定（最小集）
 - 1.5 流程约束与状态管理
 - 1.5.1 签章状态机
 - 1.5.2 关键约束
 - 1.6 异常补偿与重试机制
 - 1.7 安全与合规控制
 - 1.8 运维监控与发布管理
 - 1.8.1 监控指标
 - 1.8.2 发布与变更

1 福建水务营收系统报装电子签章设计补充说明

1.1 章节导航（精简）

- 文档定位与边界
- 集成架构与交互边界
- 接口清单与字段约定
- 流程约束与状态管理
- 异常补偿与重试机制
- 安全与合规控制
- 运维监控与发布管理

1.2 文档定位与边界

本文件是 01_Detailed_Design.md 中 INST-002 工程管理 下“合同签署与电子签章能力”的专项补充文档，重点补充：

- 泛微 CA 接口对接边界与字段约定；

- 2. 签章任务状态流转、异常补偿和运维观测点；
- 3. 合规与审计约束落地要求。

权威边界：

- 报装业务主流程以 01_Detailed_Design.md 为准；
- CA 方案总览可参考 ../04_Appendix/03_CA_Integration_Summary.md ；
- 安全控制通用要求以 ../03_Technical_Design/04_Security_Design.md 为准。

1.3 集成架构与交互边界

```
flowchart LR
    subgraph INST[报装业务系统]
        A[合同管理]
        B[签章任务中心]
        C[回执处理]
        D[档案归档]
    end

    subgraph CA[泛微 CA 电子签章平台]
        E[身份认证接口]
        F[签章接口]
        G[时间戳接口]
        H[存证接口]
    end

    A --> B
    B --> E
    B --> F
    B --> G
    B --> H
    F --> C
    G --> C
    H --> C
    C --> D
```

边界说明：

- 报装系统负责合同上下文、签署方信息、业务状态回写与档案归档；
- 泛微 CA 负责身份认证、签章执行、时间戳与存证；
- 回执成功后才允许进入“归档完成”状态。

1.4 接口清单与字段约定

1.4.1 1. 接口清单

接口方向	业务接口编号	对接接口名称	关键输入	关键输出
报装系统 → CA	IF-INST-003	合同签署发起	合同ID、签署方、签署位置、业务流水号	签章任务ID、受理状态
报装系统 → CA	IF-INST-003	身份认证调用	用户标识、认证类型、认证要素	认证结果、认证凭证
报装系统 → CA	IF-INST-003	时间戳申请	签章摘要哈希、请求时间	时间戳令牌、签发时间
报装系统 → CA	IF-INST-003	存证申请	签章后文档摘要、元数据	存证ID、存证状态
CA → 报装系统	IF-INST-004	签章结果回执	任务ID、签章状态、凭证编号、失败原因	回写结果、重试标记

1.4.2 2. 字段约定（最小集）

字段	说明	约束
biz_trace_id	业务追踪ID	必填；同一签署流程全链路唯一
contract_id	合同ID	必填；与报装申请单关联
sign_task_id	签章任务ID	回执必填；用于幂等去重
sign_status	签署状态	必填；INIT/PROCESSING/SUCCESS/FAILED
evidence_id	存证ID	成功场景必填
error_code	异常码	失败场景必填
error_message	异常描述	失败场景必填；可审计
callback_time	回执时间	必填；用于超时判断

1.5 流程约束与状态管理

1.5.1 1. 签章状态机

```
stateDiagram-v2
    [*] --> INIT
    INIT --> PROCESSING: 发起签署
    PROCESSING --> SUCCESS: 回执成功
    PROCESSING --> FAILED: 回执失败
    FAILED --> PROCESSING: 人工重试/系统重试
    SUCCESS --> ARCHIVED: 完成归档
    ARCHIVED --> [*]
```

1.5.2 2. 关键约束

- 1. 签章发起前必须完成合同正文固化与版本锁定；
- 2. 同一 `sign_task_id` 回执必须幂等处理，禁止重复更新业务状态；
- 3. 失败回执需记录错误码并进入补偿队列，不允许静默丢失；
- 4. 归档完成前，合同状态不得标记为“签署完成可生效”。

1.6 异常补偿与重试机制

异常类型	检测方式	处理策略	人工介入条件
网络超时	请求超时/连接异常	指数退避重试（最多3次）	连续失败或超时超过阈值
CA受理失败	返回失败码	写入补偿队列并通知业务端	失败码为不可恢复类
回执丢失	超时未回执	主动查询 + 重放回执校验	超过最大等待窗口
数据校验失败	字段缺失/签名不匹配	拒绝入库并告警	连续出现同类异常

补偿要求：

- 所有补偿任务必须带 `biz_trace_id`；
- 重试与人工补录均写入审计日志；
- 重试成功后需自动回补主流程状态。

1.7 安全与合规控制

- 1. 传输安全：CA 对接链路统一使用 HTTPS，回执启用签名校验；
- 2. 身份安全：签署方认证结果需与报装业务实名信息一致；
- 3. 数据安全：合同摘要、签章凭证、存证编号需防篡改存储；
- 4. 审计留痕：签章发起、回执处理、补偿重试、人工干预均需审计；
- 5. 合规要求：执行《电子签名法》及项目安全设计文档中关于日志留痕、访问控制和数据保护要求。

1.8 运维监控与发布管理

1.8.1 1. 监控指标

指标	说明	建议阈值
签章成功率	成功任务 / 总任务	日均 ≥ 99%
回执时延P95	发起到回执耗时	≤ 5 秒
补偿队列积压	待补偿任务数	告警阈值按租户配置
幂等冲突次数	重复回执冲突数	连续异常触发告警

1.8.2 2. 发布与变更

1. 涉及 CA 字段或签名算法变更，需先更新本补充文档与接口设计文档；
2. 发布前执行联调清单：签署成功、签署失败、回执重放、超时补偿；
3. 发布后至少观察一个完整业务周期，确认签章成功率与回执时延稳定。