SIGNFLOW - QUY TRÌNH QUẢN LÝ TÀI LIỆU & CHỮ KÝ SỐ

Project: SignFlow

Role: Product Owner

Version: 1.0

Status: Draft

1. TỔNG QUAN (OVERVIEW)

Hệ thống SignFlow quản lý luồng ký duyệt tài liệu qua 3 lớp: **SENDER (Gửi) → CHECKER (Kiểm tra & Ký nháy) → MANAGER (Ký số pháp lý)**. Hệ thống tập trung tối đa vào tính toàn vẹn dữ liệu (Data Integrity), quản lý phiên bản chặt chẽ (Strict Versioning) và phát hiện giả mạo thông minh (Smart Tamper Detection).

Các nguyên tắc cốt lõi:

1. **Locking Mechanism:** Cơ chế khóa phiên bản khi đang review để tránh xung đột.
2. **Immutable History:** Mọi hành động đều được ghi Log và Timestamp, không thể sửa xóa.
3. **Smart Routing:** Lỗi ở đâu trả về đúng người chịu trách nhiệm ở đó.

2. CẤU TRÚC DỮ LIỆU BẢO MẬT (SECURITY DATA STRUCTURES)

2.1. File Metadata (Lưu trữ Database)

Mỗi phiên bản file upload lên sẽ đi kèm record metadata:

```
{
  "fileId": "UUID",
  "version": 1,
  "fileName": "hop_dong_a.pdf",
  "fileHash": "SHA-256 string",
  "uploadedBy": "SenderID",
  "uploadedAt": "ISO-8601 Timestamp",
  "status": "DRAFT | SUBMITTED | LOCKED_REVIEW | APPROVED | REJECTED | ...",
  "digitalFingerprint": "Unique Token generated by System"
}
```

2.2. Checker Internal Signature Block

Được gắn kèm (embedded) hoặc lưu rời (detached) tùy kiến trúc, nhưng logic bao gồm:

```
{
  "signerRole": "CHECKER",
  "signerId": "CheckerID",
  "targetFileHash": "SHA-256 of the Original File",
  "verdict": "APPROVE",
  "timestamp": "ISO-8601 Timestamp",
```

```
  "signatureValue": "RSA/ECDSA Signature string (Signed by Checker Private Key)"
}
```

2.3. Manager Signature Block

Internal (RSA):

```
{
  "signerRole": "MANAGER",
  "method": "INTERNAL_RSA",
  "targetFileHash": "SHA-256 of the Approved File",
  "timestamp": "ISO-8601 Timestamp",
  "signatureValue": "RSA Signature string"
}
```

External (CA/USB Token): Hệ thống sẽ trích xuất thông tin từ file PDF đã ký (PAdES) để lưu metadata:

- `Certificate Subject`, `Issuer`, `Serial Number`, `Signing Time`, `Validity Check Status`.

3. MA TRẬN TRẠNG THÁI & QUYỀN HẠN (STATE MACHINE)

Trạng thái (Status)	Checker Action	Sender Action	Mô tả chi tiết
DRAFT	*Không thấy file*	`Upload`, `Delete`	Sender mới tạo, chưa gửi đi.
SUBMITTED	`View`, `Start Review`	`Re-upload` (Overwrite)	File đã gửi. Nếu Checker chưa sờ vào, Sender được phép cập nhật version mới.
LOCKED_BY_CHECKER	`Approve`, `Reject`	⛔ **BLOCKED**	**QUAN TRỌNG:** Ngay khi Checker bấm "Review", trạng thái chuyển sang LOCKED. Sender không thể Re-upload để tránh Approve nhầm file.
REJECTED	*Read Only*	`Re-upload` (New Version)	Checker trả về. Sender phải up bản mới (Version N+1).
APPROVED (Perm-Lock)	*Read Only*	⛔ **BLOCKED**	Checker đã ký nháy. Version này bị khóa vĩnh viễn, chờ Manager.
MANAGER_PROCESSING	*Read Only*	⛔ **BLOCKED**	Manager đang xử lý (VD: Đang tải về để ký ngoài).
COMPLETED	*Read Only*	⛔ **BLOCKED**	Quy trình hoàn tất.

4. QUY TRÌNH CHI TIẾT (DETAILED WORKFLOW)

Giai đoạn 1: Khởi tạo & Gửi (Sender Layer)

1. **Upload:** SENDER upload file `V1`. Hệ thống tính `Hash(V1)`.
2. **Submit:** Chuyển trạng thái sang `SUBMITTED`.
3. **Re-upload (Optional):** Nếu trạng thái vẫn là `SUBMITTED`, SENDER có thể upload `V2` (ghi đè logic hoặc tăng version tùy policy, nhưng hash sẽ thay đổi).

Giai đoạn 2: Kiểm tra & Ký nháy (Checker Layer)

1. **Locking (Critical):** CHECKER bấm nút **"Review/Start Check"**.
   - Hệ thống kiểm tra Hash hiện tại.
   - Chuyển trạng thái sang `LOCKED_BY_CHECKER`.
   - SENDER bị vô hiệu hóa nút Upload.
2. **Validation:**
   - CHECKER xem file trên PDF Viewer.
   - **Decision:**
     - **Reject:** Nhập lý do -> Trạng thái `REJECTED` -> Mở khóa cho SENDER upload `V_new`.
     - **Approve:**
       - Hệ thống yêu cầu CHECKER xác thực (Password/OTP).
       - Hệ thống dùng Private Key của CHECKER tạo `Internal Signature`.
       - Gắn chữ ký vào file hoặc Metadata.
       - Trạng thái chuyển sang `APPROVED`. Hash của file (kèm chữ ký Checker) được chốt lại làm `InputHash` cho Manager.

Giai đoạn 3: Ký số pháp lý (Manager Layer)

Phương án A: Ký nội bộ (Internal RSA)

1. MANAGER xem file.
2. Hệ thống chạy **Auto-Integrity Check 1**: So sánh Hash hiện tại với Hash lúc CHECKER approve. Nếu sai -> **Báo lỗi giả mạo**.
3. MANAGER bấm "Sign".
4. Hệ thống ký bằng Private Key của Manager.
5. Trạng thái `COMPLETED`.

Phương án B: Ký bên ngoài (External CA/USB Token)

1. MANAGER tải file (`File_For_Sign.pdf`) về máy. Trạng thái chuyển `MANAGER_PROCESSING`.
2. MANAGER cắm USB Token, ký offline ra file `File_Signed.pdf`.
3. MANAGER upload `File_Signed.pdf` lên hệ thống.
4. **Hệ thống thực hiện xác thực nghiêm ngặt (Validation Pipeline):**
   - **B1: Verify CA:** Check tính hợp lệ của Certificate (Expiration, Revocation, Trusted Root).
   - **B2: Verify Signature:** Chữ ký số trên file có khớp với nội dung file không.

- **B3: Verify Content Integrity (Quan trọng):**
  - Hệ thống so sánh nội dung gốc của `File_Signed.pdf` (trừ phần chữ ký mới thêm vào) có khớp với `File_For_Sign.pdf` ban đầu không.
  - *Lưu ý:* Nếu Manager sửa nội dung PDF rồi mới ký -> Hash content thay đổi -> **Reject hành động upload.**

5. QUY TRÌNH XỬ LÝ GIẢ MẠO & NGOẠI LỆ (EXCEPTION & TAMPER HANDLING)

Hệ thống sử dụng cơ chế **"Smart Routing Error"** để trả về đúng người chịu trách nhiệm.

Kịch bản 1: Giả mạo nội dung file (File Integrity Violation)

- **Phát hiện:** Khi chuyển từ SENDER -> CHECKER hoặc CHECKER -> MANAGER. Hệ thống tính Hash lại và thấy khác với Hash trong DB.
- **Nguyên nhân:** Có can thiệp vào Database hoặc File Storage trái phép; hoặc lỗi truyền tải.
- **Hành động hệ thống:**
  1. Block quy trình ngay lập tức.
  2. Tự động chuyển trạng thái về `REJECTED_SYSTEM_ERROR`.
  3. Gửi thông báo cho SENDER: "File đã bị thay đổi không hợp lệ, vui lòng upload lại".
  4. Log lại sự cố mức độ `CRITICAL`.

Kịch bản 2: Giả mạo chữ ký Checker (Checker Signature Forgery)

- **Phát hiện:** Khi MANAGER mở file. Hệ thống verify chữ ký của CHECKER thất bại (do Public Key không giải mã được hoặc Hash trong chữ ký không khớp Hash file).
- **Nguyên nhân:** Hacker giả mạo chữ ký Checker hoặc Checker Key bị lộ/thay đổi.
- **Hành động hệ thống:**
  1. Trả hồ sơ về cho **CHECKER** (Không trả về Sender vì file gốc có thể vẫn đúng).
  2. Trạng thái: `FLAGGED_CHECKER_SIG`.
  3. Yêu cầu CHECKER kiểm tra và ký lại (Re-sign).

Kịch bản 3: Manager upload file ký ngoài sai (Wrong File/Fake File)

- **Phát hiện:** MANAGER upload file đã ký, nhưng nội dung bên dưới chữ ký không khớp bản gốc (Hash mismatch).
- **Hành động hệ thống:**
  1. Từ chối nhận file (Upload Failure).
  2. Hiển thị lỗi: "Nội dung file đã bị thay đổi so với bản Checker duyệt. Vui lòng chỉ ký số, không chỉnh sửa nội dung."
  3. Giữ nguyên trạng thái `APPROVED` (chờ Manager ký lại đúng file).

Kịch bản 4: Sender cố tình Re-up khi đang Review (Race Condition)

- **Phát hiện:** Sender gọi API upload khi status = `LOCKED_BY_CHECKER`.

- **Hành động:** API trả về `409 Conflict`. Thông báo: "Tài liệu đang được Checker xem xét. Không thể cập nhật lúc này."

6. LƯU ĐỒ LUỒNG DỮ LIỆU (DIAGRAMS)

6.1. State Machine Diagram

```
stateDiagram-v2
    [*] --> Draft
    Draft --> Submitted: Sender Upload
    Submitted --> Submitted: Sender Re-upload (Version N+1)

    Submitted --> Locked_Review: Checker clicks "Review"
    note right of Locked_Review
      FILE LOCKED
      Sender cannot upload
    end note

    Locked_Review --> Rejected: Checker Deny
    Rejected --> Submitted: Sender Upload New Version

    Locked_Review --> Approved: Checker Sign (Internal)

    Approved --> Completed: Manager Sign (Internal)
    Approved --> Processing_Ext: Manager Download

    Processing_Ext --> Completed: Manager Upload Signed File (Valid)
    Processing_Ext --> Processing_Ext: Upload Invalid (Error Msg)

    Completed --> [*]
```

6.2. Tamper Detection Routing

```
graph TD
    A[Start Validation Phase] --> B{Check File Hash Integrity?}

    B -- No (Hash Mismatch) --> C[Route to: SENDER]
    C --> C1[Action: Request Re-upload]
    C --> C2[Log: Integrity Breach]

    B -- Yes --> D{Check Checker Signature?}

    D -- Invalid --> E[Route to: CHECKER]
    E --> E1[Action: Request Re-sign]
    E --> E2[Log: Signature Invalid]

    D -- Valid --> F{Check Manager CA/Sig?}

    F -- Invalid/Revoked --> G[Route to: MANAGER]
    G --> G1[Action: Alert Certificate Error]

    F -- Valid --> H[SUCCESS / COMPLETED]
```

7. YÊU CẦU PHI CHỨC NĂNG (NON-FUNCTIONAL REQUIREMENTS)

1. **Audit Trail:**
    - Bắt buộc ghi log IP, UserAgent, Geolocation (nếu có) cho hành động KÝ.
    - Log không được phép xóa (Append only).
2. **Performance:**
    - Hash check phải thực hiện < 1s cho file 10MB.
    - Lock mechanism phải là Atomic Operation (xử lý tranh chấp DB).
3. **Storage:**
    - Lưu trữ riêng biệt từng Version (V1, V2, V3...) không ghi đè vật lý để phục vụ tra soát.

End of Specification