1) Cấu trúc PDF liên quan chữ ký (Nghiên cứu)- Mô tả ngắn gọn: Catalog, Pages tree, Page object, Resources, Content streams, XObject, AcroForm, Signature field (widget), Signature dictionary (/Sig), /ByteRange, /Contents, incremental updates, và DSS (theo PAdES).- Liệt kê object refs quan trọng và giải thích vai trò của từng object trong lưu/truy xuất chữ ký.- Đầu ra: 1 trang tóm tắt + sơ đồ object (ví dụ: Catalog → Pages → Page → /Contents ; Catalog → /AcroForm → SigField → SigDict)

- Các objects chính trong PDF:
  - **Catalog(Root):** đối tượng gốc của PDF, chứa các tham chiếu đến /Pages, có thể chứa thêm /AcroFrom (các from filed) và /DSS (Document Security Store cho PadEs).
  - **Pages tree →Page object :** Mỗi trang PDF có /Resources và /Contents (chứa nội dung hiện thị). Vùng hiển thị chữ ký(nếu có) thường là From XObject nằm trong /Resources và được tham chiếu qua /Annots.
  - **AcroForm:** Chứa danh sách các from field. Trường chữ ký (Signature field) nằm ở đây, là một "widget field" có kiểu /FT /Sig.
  - **Signature field (Widget):** Đối tượng đại diện cho trường chữ ký. Khi ký xong, nó sẽ tham chiếu đến Signature dictionary thông qua khóa /V.
  - Signature dictionary (/Sig): Nơi luu dữ liệu chữ ký thông tin meta:

    - /Type,/Sig: Xác định kiểu đối tượng.

    - /Filter và /SubFilter: quy định dạng

    - /Contents: Vùng byte chứa chữ ký PKCS#7/CMS hoặc CMS + timestamp

    - /ByteRange: mảng [start1 length1 start2 length2] chỉ định vùng dữ liệu được ký(loại trừ /Contents).

    - M: thời gian ký dạng text (không có giá trị pháp lý).

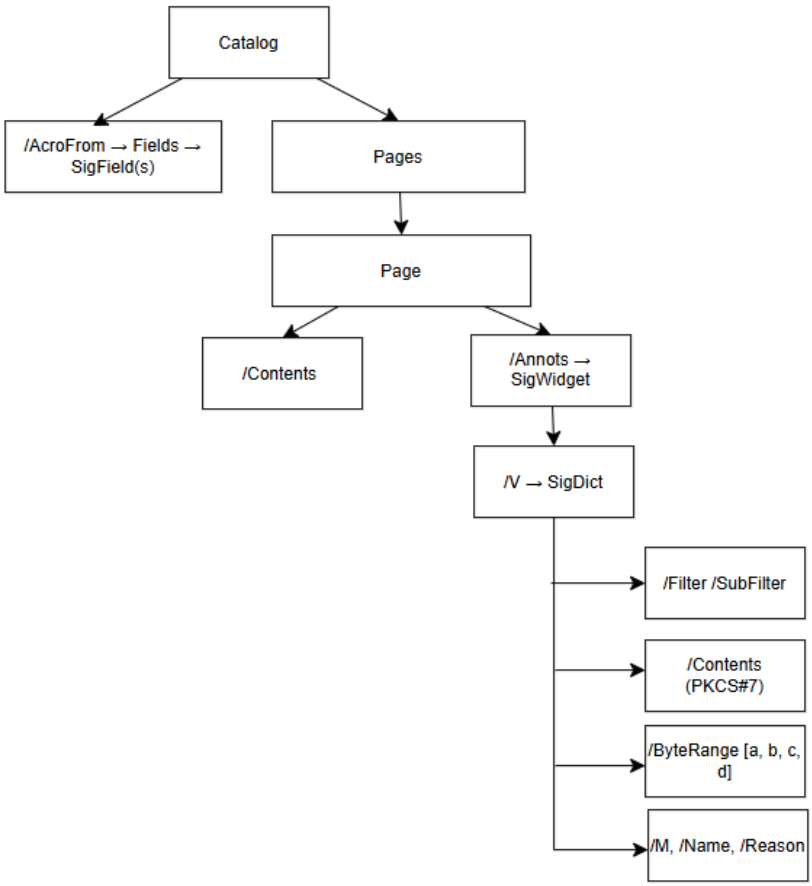
- /Name, /Reason, /Location: Thông tin người ký,lý do,nơi ký.

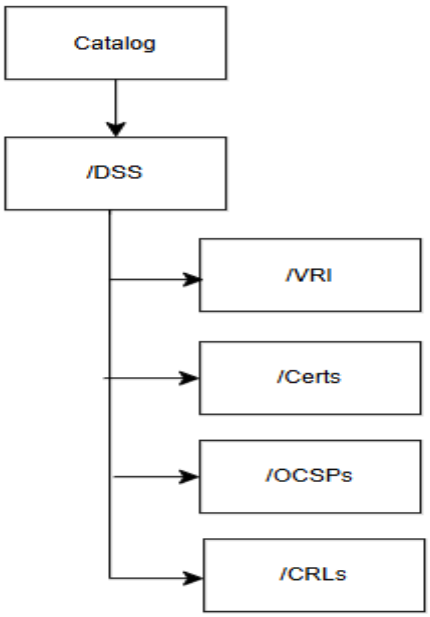
- **/Contents vs. /ByteRange** : /ByteRange cho biết vùng dữ liệu được băm, /Contents là vùng bị loại trừ để chèn chữ ký sau khi băm.
- **Incremental updates**: PDF cho phép " ghi thêm phần mới" mà không thay đổi dữ liệu cũ. Khi ký ,PDF sẽ ghi một incremental update; nhờ đó ta có thể phát hiện sửa đổi sau khi ký.
- **XObject (From Xobject):** dùng để hiện thị chữ ký trên trang.
- **DSS (Document Security Store):** vùng lưu trữ thông tin xác minh dài hạn(LTV) như chứng chỉ, OCSP, CRL, timestamp.

➢ Các object refs quan trọng

- **Catalog (Root)**: chứa /AcroForm và liên kết tới pages; entry bắt đầu của traversal.
- **AcroForm**: chứa /Fields (mảng SigField refs) và /SigFlags.
- **SigField (Widget annotation)**: vị trí visual trên Page, tham chiếu tới SigDict qua /V sau khi signed.
- **Signature dictionary (SigDict)**: *chứa* /Contents (PKCS#7), /ByteRange, /M, /Filter, /SubFilter (ví dụ /adbe.pkcs7.detached), /Name, /Location.
- **Page**:chứa /Annots array (với widget ref) và /Contents (appearance XObject có thể reference tới SigField appearance).
- **/Contents (Signature placeholder in SigDict)**: vùng nhúng blob DER PKCS#7.
- **DSS / VRI (PAdES)**: chứa hỗ trợ xác thực lâu dài: certs, ocspResponses, crls, vri entries referencing signature byte ranges.
- **Incremental update (xref/trailer of appended revision)**: chứa new objects (SigDict, updated AcroForm field V pointer) appended — cho phép detection of post-sign changes.

❖ Sơ đồ quan hệ object





2) Thời gian ký được lưu ở đâu?- Nêu tất cả vị trí có thể lưu thông tin thời gian: + /M trong Signature dictionary (dạng text, không có giá trị pháp lý). + Timestamp token (RFC 3161) trong PKCS#7 (attribute timeStampToken). + Document timestamp object (PAdES). + DSS (Document Security Store) nếu có lưu timestamp và dữ liệu xác minh.- Giải thích khác biệt giữa thông tin thời gian /M và timestamp RFC

- /M trong Signature dictionary (dạng text, không có giá trị pháp lý)
  + Chuỗi text kiểu (D:20251027...).
  + Không được bảo vệ bằng chữ ký, có thể chỉnh sửa → không có giá trị pháp lý.
- Thuộc tính signingTime trong PKCS#7/CMS
  + Nằm trong SignedAttributes, được bao phủ bởi chữ ký → có giá trị pháp lý.
- RFC 3161 Timestamp Token (TST)
  + Token do TSA (Time Stamp Augthority) cấp, xác nhận thời điểm tồn tại của dữ liệu.
  + Được nhúng trong PKCS#7 dưới dạng timeStampToken (unsigned attribute).
  + Cung cấp bằng chứng mạnh mẽ hơn về thời gián ký.
- Document Timestamp (PAdES)
  + Một dạng chữ ký đặc biệt áp dụng cho toàn bộ tài liệu, thường dùng trong xác thực dài hạn (LTV).
- DSS (Document Security Store)
  + Có thế chứa thêm timestamp và dữ liệu xác minh để lưu lâu dài.

➢ Khác biệt giữa /M và RFC3161 timestamp

- /M: chỉ là text → dễ bị sửa, không ràng buộc mật mã.
- RFC3161 timestamp: do TSA cấp, có chữ ký riêng → bằng chứng hợp pháp về thời điểm tài liệu tồn tại.

3) Các bước tạo và lưu chữ ký trong PDF (đã có private RSA)- Viết script/code thực hiện tuần tự:

1. Chuẩn bị file PDF gốc.

2. Tạo Signature field (AcroForm), reserve vùng /Contents (8192 bytes).

3. Xác định /ByteRange (loại trừ vùng /Contents khỏi hash).

4. Tính hash (SHA-256/512) trên vùng ByteRange.

5. Tạo PKCS#7/CMS detached hoặc CAdES:- Include messageDigest, signingTime, contentType.- Include certificate chain.- (Tùy chọn) thêm RFC3161 timestamp token.

6. Chèn blob DER PKCS#7 vào /Contents (hex/binary) đúng offset.

7. Ghi incremental update.

8. (LTV) Cập nhật DSS với Certs, OCSPs, CRLs, VRI.- Phải nêu rõ: hash alg, RSA padding, key size, vị trí lưu trong PKCS#7.- Đầu ra: mã

SĐT: 0383792082
Ngày ký: 31/10/2025 00:26:20
Location: VIỆT NAM

NGUYỄN THỊ LINH