BÀI TẬP VỀ NHÀ AN TOÀN VÀ BẢO MẬT THÔNG TIN
CHỮ KÍ SỐ

Họ và tên: Nguyễn Thu Thảo
Mssv: K2225480106060
Lớp: K58KMT

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.

· **Catalog**

Là **điểm khởi đầu** của PDF, xác định root của tài liệu.

Liên kết tới cây Pages (/Pages) và form fields (/AcroForm) nếu có.

Vai trò: định hướng PDF reader truy xuất các trang và form fields.

· **Pages Tree**

Quản lý tất cả trang của PDF theo cấu trúc cây.

Mỗi node /Pages chứa:

/Kids: danh sách trang con

/Count: tổng số trang con

Vai trò: PDF reader duyệt từng trang dễ dàng.

· **Page Object**

Mỗi trang là object riêng, chứa thông tin layout và nội dung.

Chứa các trường quan trọng: /Contents (stream hiển thị nội dung), /Resources (font, hình ảnh).

Vai trò: xác định nội dung cụ thể của từng trang.

- **Resources**

  Chứa tài nguyên dùng chung trên trang: font, XObject (hình ảnh hoặc form XObject), màu sắc.

  Vai trò: tối ưu hóa, tránh lặp lại resources giữa các trang.

- **Content Streams**

  Stream chứa các lệnh hiển thị văn bản, hình ảnh, đồ họa.

  Không chứa chữ ký trực tiếp, nhưng có thể hiển thị vùng widget chữ ký.

- **XObject**

  Là các object con, thường dùng cho hình ảnh hoặc reusable form.

  Có thể dùng hiển thị logo hoặc biểu tượng chữ ký.

- **AcroForm**

  Quản lý tất cả **form fields**: text, checkbox, radio, signature.

  /SigFlags: chỉ ra PDF có signature field và cần validate chữ ký.

  Vai trò: tạo liên kết giữa form field (signature field) và signature dictionary.

- **Signature Field (Widget)**

  Là vùng hiển thị chữ ký trên trang PDF.

  Widget là annotation, liên kết tới page cụ thể.

  /V trỏ tới **Signature dictionary (/Sig)** chứa thông tin chữ ký.

- **Signature Dictionary (/Sig)**

  Chứa thông tin chữ ký số quan trọng:

    /Filter: thuật toán ký (ví dụ Adobe PPKLite)

    /SubFilter: chuẩn chữ ký (ví dụ PKCS#7 detached hoặc CAdES)

    /ByteRange: xác định vùng dữ liệu hash, **loại trừ /Contents**

    /Contents: blob chữ ký số PKCS#7 DER

/M: thời gian ký dạng text, không có giá trị pháp lý

- **/ByteRange và /Contents**

  /ByteRange: chỉ định các offset dữ liệu để hash, không bao gồm /Contents.

  /Contents: lưu chữ ký số PKCS#7.

  Hỗ trợ **incremental update**, giữ nguyên nội dung gốc.

- **Incremental Update**

  Thêm chữ ký mới hoặc cập nhật PDF mà không xóa dữ liệu cũ.

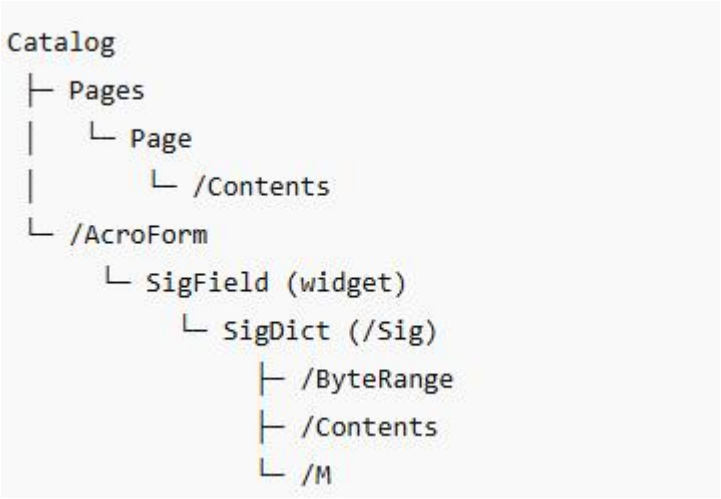
  Đảm bảo tính toàn vẹn và phát hiện chỉnh sửa.

- **DSS (Document Security Store – theo PAdES)**

  Lưu thông tin bổ sung cho chữ ký: certificate chain, OCSP, CRL, timestamp.

  Hỗ trợ **Long Term Validation (LTV)**, giúp xác thực chữ ký lâu dài.

  Sơ đồ object tóm tắt:



  Giải thích sơ đồ :

- **Catalog**

  Là **object gốc** của PDF.

  Liên kết tới:

Pages: cây quản lý các trang PDF.

AcroForm: form fields (bao gồm các signature field nếu có).

- **Pages → Page → /Contents**

  Pages: quản lý toàn bộ các trang PDF.

  Page: từng trang riêng lẻ.

  /Contents: stream chứa lệnh vẽ nội dung trang (văn bản, hình ảnh, đồ họa).

  Chữ ký số không trực tiếp lưu trong /Contents, nhưng widget chữ ký có thể hiển thị trên trang này.

- **AcroForm → SigField (widget)**

  AcroForm quản lý tất cả form fields trong PDF.

  SigField: một **widget** trên trang, là vùng hiển thị chữ ký.

  Liên kết tới **SigDict (/Sig)**, nơi lưu trữ dữ liệu chữ ký số thực sự.

- **SigDict (/Sig)**

  Chứa toàn bộ thông tin chữ ký số.

  /ByteRange: xác định vùng dữ liệu PDF được hash, **loại trừ /Contents**.

  /Contents: lưu **blob PKCS#7** (chữ ký số thực sự, DER).

  /M: thời gian ký dưới dạng text, chỉ để hiển thị, **không có giá trị pháp lý**.

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 RFC3161.

Thời gian ký PDF được lưu ở đâu

/M trong Signature dictionary

Lưu thời gian ký **dưới dạng text**, ví dụ D:YYYYMMDDHHmmSSZ.

Mục đích: hiển thị thông tin thời gian ký trong PDF reader.

Lưu ý: chỉ là text, **không có giá trị pháp lý**, có thể bị chỉnh sửa mà không phát hiện.

Timestamp token (RFC3161) trong PKCS#7

Lưu trong **attribute** timeStampToken khi tạo chữ ký số (PKCS#7 detached hoặc CAdES).

Được **TSA (Time Stamping Authority) ký số**, đảm bảo **giá trị pháp lý và chứng thực thời gian**.

Vai trò: xác nhận chính xác thời điểm ký, **chống sửa đổi** nội dung PDF sau khi ký.

Document timestamp object (PAdES)

Là object riêng trong PDF theo chuẩn **PAdES**.

Lưu timestamp cho cả document hoặc cho một phần document, hỗ trợ **Long Term Validation (LTV)**.

Cho phép kiểm tra chữ ký sau nhiều năm mà không cần phụ thuộc certificate gốc còn hợp lệ hay không.

DSS (Document Security Store)

Nếu PDF hỗ trợ **LTV**, DSS sẽ lưu các timestamp và dữ liệu xác minh.

Bao gồm certificate chain, OCSP, CRL và timestamp, giúp kiểm tra chữ ký lâu dài.

Tiêu chí	/M (Signature Dictionary)	RFC3161 Timestamp
Loại dữ liệu	Text string (D:YYYYMMDDHHmmSSZ)	Digital token nhúng trong PKCS#7/CAdES
Cấu trúc	Chỉ chứa ngày giờ ký dưới	Signed structure: chứa ngày giờ,

	dạng text	hash của tài liệu, chữ ký số của TSA
Giá trị pháp lý	Không có giá trị pháp lý	Có giá trị pháp lý, được TSA ký số
Cơ chế bảo mật	Không được hash hay ký số, có thể chỉnh sửa	Được TSA ký số và kết hợp hash nội dung, thay đổi sẽ bị phát hiện
Liên kết với chữ ký số	Không liên kết trực tiếp với chữ ký số	Là attribute của chữ ký số, tích hợp vào PKCS#7/CAdES
Ứng dụng thực tế	Hiển thị cho người dùng ngày giờ ký, mục đích trình bày	Dùng trong hợp đồng điện tử, chứng từ ngân hàng, hồ sơ pháp lý, hỗ trợ LTV
Khả năng kiểm tra	Chỉ đọc trực tiếp từ PDF, không xác minh tính toàn vẹn	Có thể verify bằng public key của TSA, đảm bảo toàn vẹn và chứng thực thời điểm ký