BÀI TẬP SỐ 2. AN TOÀN VÀ BẢO MẬT THÔNG TIN

Họ tên: Phương Thị Ánh Nguyệt

Mssv: K225480106098

CÁC YÊU CẦU CỤ THỂ

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).

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

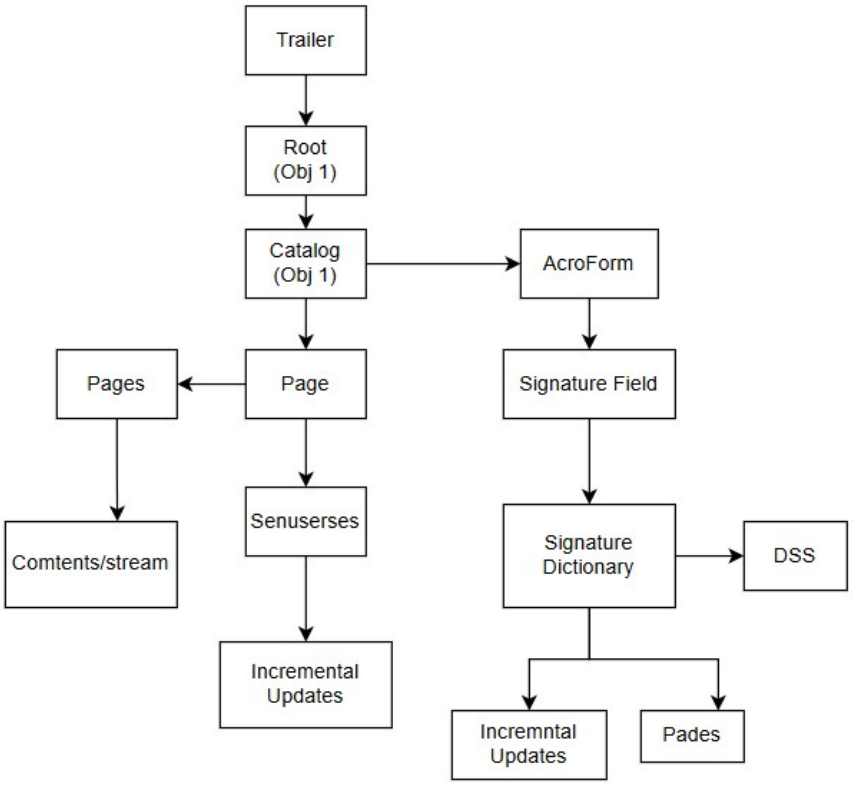
1. Cấu trúc PDF liên quan chữ ký.

Các thành phần chính:

Object / Thành phần	Vai trò trong tài liệu PDF và quy trình ký
Catalog (/Root)	Là điểm khởi đầu (entry point) của cấu trúc tài liệu PDF. Từ đây có thể truy cập đến /Pages, /AcroForm, và các cấu trúc chữ ký.
Pages tree (/Pages)	Là cây phân cấp chứa toàn bộ các trang PDF. Mỗi node /Pages có thể chứa danh sách /Kids (các trang con) và tổng số trang /Count.
Page object (/Page)	Đại diện cho từng trang. Chứa /Resources, /Contents (dòng lệnh vẽ nội dung), /Annots (annotation – bao gồm chữ ký nếu là widget).

Resources	Tập hợp các tài nguyên dùng trên trang (font, ảnh, XObject, v.v). Chữ ký dạng hình ảnh hoặc stamp dùng /XObject trong /Resources.
Content streams (/Contents)	Chứa lệnh vẽ (PDF graphics operators) – hiển thị văn bản, hình, chữ ký hình ảnh. Không liên quan trực tiếp đến chữ ký số nhưng là phần được băm hash trong ByteRange.
XObject	Là đối tượng nhúng (như ảnh PNG/JPG hoặc Form XObject). Trong vùng hiển thị chữ ký, ảnh chữ ký tay hoặc khung nền được chèn như XObject.
AcroForm	Là đối tượng chứa mô tả toàn bộ biểu mẫu (form fields) của PDF, trong đó có Signature fields.
Signature field (Widget Annotation)	Một trường biểu mẫu đặc biệt, có type /Sig hoặc /Widget. Dùng để chứa chữ ký số hoặc làm vị trí hiển thị stamp.
Signature dictionary (/Sig)	Là object chính chứa dữ liệu chữ ký (metadata, thời gian ký, lý do, vị trí, algorithm, và vùng /ByteRange, /Contents).

Sơ đồ liên kết



2. Thời gian kí được lưu.

Các vị trí có thể lưu thông tin thời gian:

Vị trí lưu	Mô tả	Tính pháp lý
1. Trường /M trong Signature Dictionary	Là một trường trong cấu trúc chữ ký của PDF (Signature Dictionary), chứa thời gian do phần mềm ký ghi lại (thường theo giờ hệ thống máy tính). Ví dụ: /M (D:20251030 154230+07'00').	Không có giá trị pháp lý – vì có thể bị thay đổi hoặc bị ảnh hưởng bởi thời gian hệ thống.
2. Timestamp Token (RFC 3161) trong PKCS#7/CMS	Là một thuộc tính (attribute) trong đối tượng chữ ký, có tên timeStampToken. Đây là dấu thời gian điện tử được chứng thực bởi TSA (Time Stamping Authority) – một bên thứ ba tin cậy.	Có giá trị pháp lý, vì được ký bởi TSA và xác nhận thời điểm tài liệu đã tồn tại.
3. Document Timestamp Object (PAdES)	Là dạng chữ ký đặc biệt chỉ chứa timestamp, không chứa thông tin người ký. Nó chứng thực rằng tài liệu đã tồn tại tại thời điểm cụ thể.	Có giá trị pháp lý (nếu TSA uy tín).
4. DSS – Document Security Store	Là nơi lưu trữ các thông tin xác minh trong tài liệu PDF: chứng thư số, OCSP, CRL, và cả timestamp (nếu có).	Bổ trợ xác minh sau này (giúp chứng minh chữ ký vẫn hợp lệ khi chứng thư hết hạn).

Khác biệt giữa thông tin thời gian /M và timestamp RFC 3161

Tiêu chí	/M trong Signature Dictionary	Timestamp RFC 3161 (timeStampToken)
Nguồn gốc thời gian	Do máy tính của người ký ghi lại.	Do máy chủ TSA (Time Stamping Authority) – bên thứ ba tin cậy cung cấp.
Được ký bảo vệ không?	Không được ký, có thể bị thay đổi.	Được ký bởi TSA, không thể thay đổi nếu không làm sai chữ ký.

Giá trị pháp lý	Không có – chỉ tham khảo.	Có – chứng minh được thời điểm tài liệu đã tồn tại.
Mức độ tin cậy	Thấp – phụ thuộc vào thời gian hệ thống máy người ký.	Cao – do TSA quản lý đồng hồ chuẩn (theo UTC, NTP, GPS, v.v.).
Chuẩn kỹ thuật	PDF Specification (ISO 32000)	RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol)
Ứng dụng chính	Hiển thị thời gian ký trong phần mềm (Adobe, Foxit, v.v.)	Chứng thực thời điểm ký hoặc tồn tại của tài liệu phục vụ xác minh pháp lý.

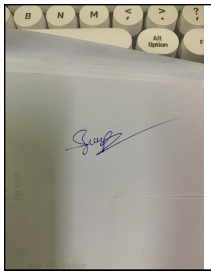
3. Rủi ro bảo mật

Khái niệm "rủi ro bảo mật" rủi ro bảo mật là khả năng một mối đe dọa (threat) khai thác được điểm yếu (vulnerability) trong hệ thống, gây thiệt hại cho tài sản thông tin hoặc dịch vụ.

Các nhóm rủi ro bảo mật phổ biến

- Rủi ro về con người (Human Risk)
  - Nhân viên chia sẻ mật khẩu, lộ thông tin nội bộ.
  - Thiếu đào tạo về an toàn thông tin → bị lừa đảo (phishing).
  - Lợi dụng quyền truy cập nội bộ để đánh cắp dữ liệu.
- Rủi ro kỹ thuật (Technical Risk)
  - Lỗ hổng phần mềm (bug, zero-day, lỗi cấu hình).
  - Tấn công mạng: malware, ransomware, DDoS, SQL injection, XSS.
  - Kênh truyền không an toàn: HTTP không mã hóa, Wi-Fi công cộng.
  - Xử lý sai trong mã hóa/chữ ký số: dùng thuật toán yếu, không kiểm timestamp, không xác thực TSA.
- Rủi ro vật lý (Physical Risk)
  - Thiết bị chứa dữ liệu bị mất cắp hoặc phá hoại.
  - Hệ thống máy chủ bị hỏng do cháy, lũ, mất điện.
  - Camera, USB, ổ cứng bị truy cập trái phép.
- Rủi ro tổ chức & quy trình (Organizational Risk)
  - Không có chính sách bảo mật hoặc sao lưu.
  - Phân quyền sai, cấp quyền vượt mức.

- Không kiểm tra định kỳ nhật ký, không giám sát sự kiện bảo mật.



Phuong Anh Nguyet
SDT: 0366771009
MSSV: K225480106098
Ngày ký: 31/10/2025