BÀI TẬP AN TOÀN VÀ BẢO MẬT THÔNG TIN

Sinh viên: Đậu Văn Khánh

MSSV: K225480106099

Lớp: K58KTP

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.

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.

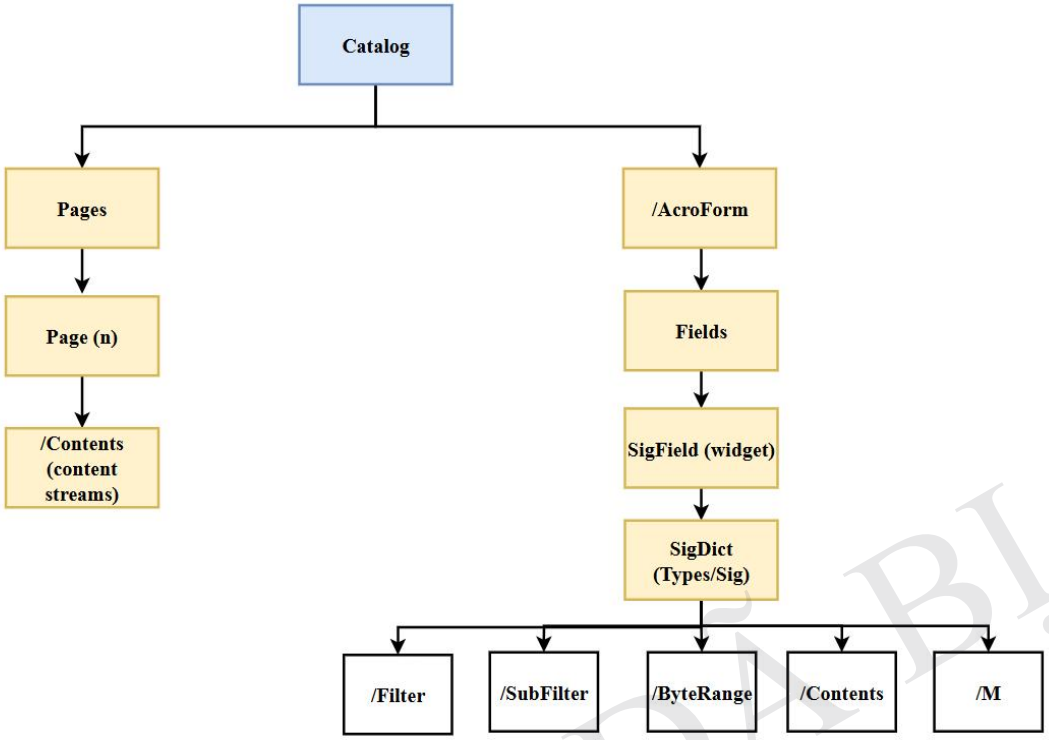
BÀI LÀM

1. Cấu trúc PDF liên quan chữ ký:

❖ Mô tả ngắn gọn các object:

- Catalog: root object của tài liệu. Thường tham chiếu tới /Pages và /AcroForm.
- Pages tree / Page object: chứa /Contents (content streams) và resources.
- Resources / Content streams / XObject: nội dung hiển thị.
- AcroForm: form-level dictionary; chứa Fields (form fields) và có thể có /SigFlags.
- Signature field (widget): một AcroForm field loại Sig (field dictionary) và widget annotation trên trang để hiển thị khung chữ ký.
- Signature dictionary (/Sig): Đối tượng chứa thông tin chữ ký, gồm: /Type /Sig, /Filter, /SubFilter (kiểu chữ ký), /ByteRange, /Contents (blob chữ ký PKCS#7), /M (thời gian ký), /Name, /Location.
- /ByteRange: mảng bốn số [start1 length1 start2 length2] xác định hai vùng dữ liệu trong file được hash (vùng giữa chứa /Contents placeholder).
- /Contents: chỗ chứa blob chữ ký (DER PKCS#7), thường được reserve kích thước cố định (ví dụ 8192 bytes) trong incremental update.
- Incremental updates: PDF có thể bổ sung object mới và xref bổ sung, cho phép chèn chữ ký mà không sửa nội dung cũ - cơ chế này cho phép phát hiện sửa đổi sau khi ký.
- DSS (Document Security Store): Lưu thông tin xác thực dài hạn (LTV) như chứng thư, OCSP/CRL và timestamp tokens.

❖ Sơ đồ object:



❖ Object refs quan trọng & vai trò:

- /AcroForm (Root obj): chứa danh sách field — cần để trình đọc biết chỗ signature fields.

- SigField (Field obj): định danh trường chữ ký (tên, vị trí hiển thị); widget annotation trên trang liên hệ tới form field này.

- SigDict (Signature dictionary): chứa metadata chữ ký và blob PKCS#7 trong /Contents — đây là object chính để lưu chữ ký.

- /ByteRange: thiết lập vùng file để compute digest (loại trừ vùng /Contents).

- Incremental update xref + trailer: nếu có thay đổi sau chữ ký, xref/trailer mới sẽ khác → phát hiện sửa đổi.

2. Thời gian ký được lưu ở đâu?

❖ Vị trí có thể lưu thông tin thời gian:

- /M trong Signature dictionary (dạng text, ví dụ D:20251026...). Không có giá trị pháp lý — chỉ là metadata.
- Timestamp token (RFC 3161) được nhúng trong PKCS#7/CMS (attribute timeStampToken hoặc separate attribute id-aa-signatureTimeStampToken trong CAdES). Timestamp RFC3161 do một TSA ký trên digest giúp chứng thực thời điểm.
- Document timestamp object (PAdES) — PDF có thể có đối tượng timestamp document-level (khác với signature field của signer) theo PAdES.
- DSS (Document Security Store): lưu trữ timestamp tokens (.tsr), chứng thư, OCSP/CRL responses phục vụ LTV.

❖ Khác biệt chính /M vs RFC3161 timestamp:

- /M: chỉ là chuỗi định dạng ngày giờ do signer ghi vào dictionary; có thể bị giả mạo (không được ký độc lập). Không đủ cho chứng thực thời điểm.
- RFC3161 timestamp: do một Time Stamping Authority (TSA) ký trên digest của PKCS#7/CMS (hoặc của dữ liệu), do đó là bằng chứng thời điểm độc lập và đáng tin cậy (nếu tin tưởng TSA).

3. Rủi ro bảo mật chữ ký số trong PDF

- **Tổng quan ngắn:** Chữ ký số trên PDF có thể rất an toàn nếu triển khai theo chuẩn (ví dụ PAdES) và thực hiện kiểm tra xác thực đầy đủ. Tuy nhiên có nhiều lớp rủi ro: từ việc sửa đổi nội dung PDF, dùng cập nhật gia tăng (incremental updates) để che thay đổi, đến sự yếu kém hoặc bị lộ của chứng thư và khoá riêng. Dưới đây tóm tắt các rủi ro chính, cách phát hiện và biện pháp giảm nhẹ.
- **Rủi ro bảo mật và giải pháp:**

- Incremental update lạm dụng: Nhiều lớp chữ ký che giấu thay đổi → Giải pháp: hạn chế incremental updates, kiểm tra modification_level.
- Metadata bị thay đổi: Tác giả, thời gian, title bị sửa mà không phá chữ ký → Giải pháp: ký toàn bộ document và metadata, tuân thủ PAdES.
- Thuật toán yếu: SHA-1, RSA nhỏ hoặc lỗi thời → Giải pháp: dùng SHA-256, RSA ≥2048-bit, kiểm tra policy ký.
- Tampering nội dung: Sửa /Contents hoặc vùng ByteRange → Giải pháp: kiểm tra full byte-range, dùng PAdES.
- Replay / incremental-update attack: Dùng chữ ký/timestamp cũ trên tài liệu sửa đổi → Giải pháp: kiểm tra lịch sử revision, xác thực timestamp RFC3161 và evidence PAdES-DSS.
- Time repudiation: Timestamp giả hoặc mất token → Giải pháp: dùng TSA tin cậy, lưu TimeStampToken (TST).
- Chứng thư thu hồi/hết hạn: Không kiểm tra CRL/OCSP → Giải pháp: xác thực OCSP/CRL hoặc nhúng responses trong PAdES-DSS.
- Lộ khóa riêng / side-channel: Khóa signer bị lộ → Giải pháp: dùng HSM/TPM, quản lý truy cập chặt.
- Vận hành & thuật toán yếu: Cấu hình sai, thiếu logging → Giải pháp: tuân thủ PAdES, audit và pen-test định kỳ.

Kết luận

Bài tập giúp sinh viên hiểu và thực hành quy trình tạo, nhúng và xác thực chữ ký số trong file PDF theo chuẩn PDF/PAdES, qua đó nắm rõ cấu trúc tài liệu, vị trí lưu chữ ký và thời gian ký, cùng cách sử dụng RSA, SHA-256 và PKCS#7 để đảm bảo tính toàn vẹn, xác thực và chống giả mạo.

Chữ ký số PDF duy trì tính toàn vẹn thông qua các thành phần AcroForm, SigDict và ByteRange, còn thông tin thời gian được lưu bằng thuộc tính /M hoặc token RFC3161. Để tăng độ tin cậy và ngăn ngừa nguy cơ sửa đổi hay giả mạo chứng thư, việc mở rộng xác minh bằng DSS và chuẩn PAdES nâng cao là cần thiết. Thử nghiệm các tệp original.pdf, signed.pdf, tampered.pdf cho thấy quy trình ký và kiểm chứng hoạt động chính xác, minh chứng cho tính hiệu quả của phương pháp.

Khánh

Dau Van Khanh
Lop: K58KTP
SDT: 0962213503
MSSV: K225480106099
Ngày ký: 29/10/2025

Đã chỉnh sửa ngày: 29/10/2025 21:26:09