BÁO CÁO BÀI TẬP MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

Sinh viên thực hiện: Hứa Thị Thanh Hiền

MSSV: K225480106016

Lớp: 58KTPM

Môn học: An toàn và Bảo mật Thông tin

Giảng viên hướng dẫn: ThS. Đỗ Duy Cốp

Thời gian thực hiện: 24/10/2025 – 31/10/2025

I. GIỚI THIỆU CHUNG

Trong kỷ nguyên số, tài liệu điện tử được sử dụng rộng rãi trong các lĩnh vực hành chính, giáo dục và doanh nghiệp. Tuy nhiên, vấn đề tính xác thực và toàn vẹn dữ liệu là thách thức lớn.

Chữ ký số (Digital Signature) giúp bảo đảm rằng nội dung không bị thay đổi và người ký được xác minh rõ ràng.

Định dạng PDF (Portable Document Format) hỗ trợ chữ ký số theo chuẩn PDF 1.7 / PDF 2.0 và mở rộng PAdES (PDF Advanced Electronic Signatures) do ETSI ban hành.

II. CẤU TRÚC FILE PDF LIÊN QUAN CHỮ KÝ SỐ

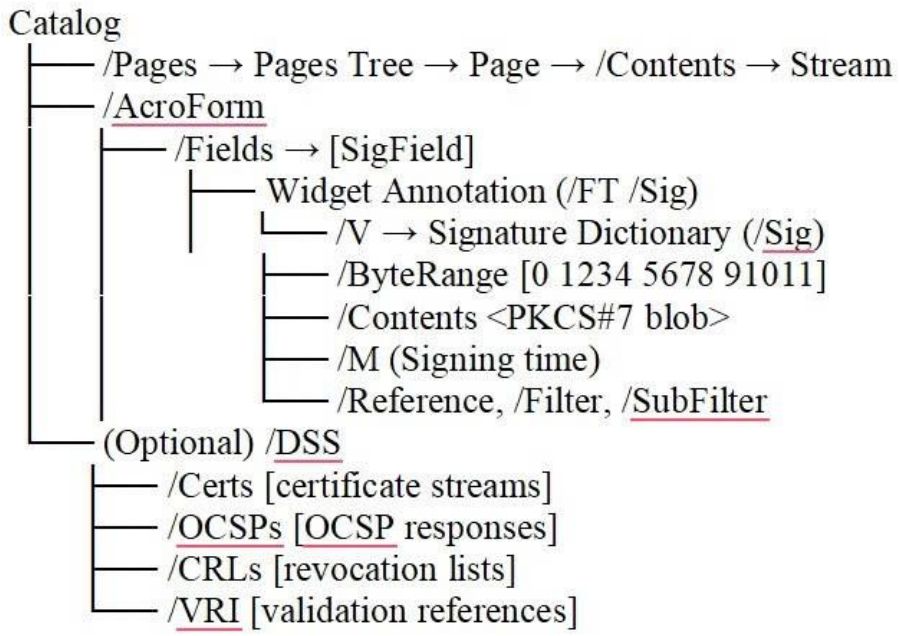
Một tài liệu PDF bao gồm các object (đối tượng**)** được tổ chức dạng cây, trong đó các thành phần chính có liên hệ chặt chẽ khi thực hiện ký điện tử.

1. Thành phần cơ bản của PDF

Thành phần	**Vai trò**
Catalog	Là đối tượng gốc (root) của tài liệu PDF, liên kết đến toàn bộ cây trang (Pages Tree) và AcroForm.
Pages tree	Quản lý danh sách các trang, cho phép trình đọc PDF xác định trang chứa chữ ký hiển thị.
Page object	Chứa nội dung, annotation (bao gồm widget của chữ ký).

Thành phần	Vai trò
Resources	Chứa các định nghĩa font, hình ảnh, và đối tượng đồ họa (XObject) được sử dụng trên trang.
Content Stream	Nơi lưu các lệnh vẽ, chữ, hoặc hình ảnh, định nghĩa bố cục trang.
XObject	Dùng để tái sử dụng đối tượng (như hình ảnh hoặc biểu mẫu).
AcroForm	Quản lý các trường biểu mẫu (Form Field), bao gồm Signature Field.
Signature Field (Widget)	Vị trí trên trang PDF dùng để hiển thị vùng chữ ký.
Signature Dictionary (/Sig)	Chứa thông tin người ký, thuật toán, thời gian và nội dung chữ ký.
ByteRange	Chỉ định vùng dữ liệu được ký – ngoại trừ vùng /Contents.
Contents	Chứa dữ liệu chữ ký PKCS#7 (ở dạng binary hoặc hex).
Incremental update	Cơ chế cập nhật từng lớp của PDF khi ký.
DSS (Document Security Store)	Lưu trữ chứng thư số, OCSP và CRL trong PAdES-LTV.

Sơ đồ object



- Chữ ký nằm trong Signature Dictionary, được tham chiếu từ AcroForm → SigField.
- Hash tính trên ByteRange, kết quả nhúng vào PKCS#7 tại /Contents.
- DSS (tùy chọn) lưu cert + OCSP/CRL → hỗ trợ xác thực dài hạn (LTV) sau khi cert hết hạn.

2. Các vị trí lưu thông tin thời gian trong PDF

Khi một file PDF được ký điện tử, thông tin về thời gian có thể được lưu ở nhiều cấp độ khác nhau, tùy thuộc vào mức độ tin cậy và chuẩn kỹ thuật áp dụng (PDF 1.7, PAdES, hoặc RFC 3161).

Mục tiêu của việc ghi nhận thời gian ký là:

- Chứng minh thời điểm người ký thực hiện chữ ký.
- Bảo đảm tính pháp lý nếu chứng thư số hết hạn sau này.
- Hỗ trợ xác minh toàn vẹn tài liệu tại một thời điểm cụ thể.

1.1. Thời gian /M trong Signature Dictionary

- Thuộc tính /M nằm trong Signature Dictionary (/Sig).
- Dạng lưu trữ: D:YYYYMMDDHHmmSS+07'00' (theo chuẩn PDF ISO 32000).

- Đây là thời gian mà phần mềm ký (ví dụ iText, OpenSSL, PyPDF) tự động lấy từ đồng hồ của máy tính người ký.
- Dữ liệu này không có giá trị pháp lý, vì người dùng có thể chỉnh lại thời gian hệ thống rồi ký.

1.2. Thời gian trong Timestamp Token (RFC 3161)

- Là một dạng chữ ký số độc lập, được tạo bởi TSA (Time Stamping Authority).
- Khi ký, người ký gửi hash của tài liệu đến TSA → TSA gắn "con dấu thời gian" (timeStampToken) và ký lại.
- Thông tin này được nhúng vào khối PKCS#7 (thuộc tính unsignedAttributes → timeStampToken).
- Thời gian này có giá trị pháp lý, vì do bên thứ ba đáng tin cậy xác nhận.

1.3. Document Timestamp Object (PAdES)

- Là loại chữ ký đặc biệt trong chuẩn ETSI EN 319 142 (PAdES).
- Dùng để đóng dấu thời gian toàn bộ tài liệu mà không có người ký cụ thể.
- Được sử dụng trong chữ ký dạng "Document Timestamp" (subFilter /ETSI.RFC3161).
- Giúp xác minh tài liệu vẫn nguyên vẹn sau thời điểm xác nhận.

1.4. DSS (Document Security Store)

- Là phần mở rộng trong PAdES-LTV (Long-Term Validation).
- Lưu trữ timestamp, chứng thư, OCSP và CRL để có thể xác minh lâu dài, ngay cả khi chứng thư của người ký đã hết hạn.

Tiêu chí	/M	Timestamp RFC3161
Nguồn thời gian	Đồng hồ hệ thống máy ký	Máy chủ TSA (độc lập, được chứng thực)

Tiêu chí	/M	Timestamp RFC3161
Định dạng dữ liệu	Văn bản ISO 8601 (D:YYYYMMDDHHmmSS)	ASN.1 DER nhị phân
Vị trí lưu trữ	Trong Signature Dictionary (/M)	Trong PKCS#7 → timeStampToken
Tính pháp lý	Không có	Có giá trị pháp lý
Mục đích	Hiển thị thời gian ký cho người dùng	Làm bằng chứng xác nhận tài liệu tồn tại tại thời điểm ký
Khả năng làm giả	Dễ bị thay đổi (vì phụ thuộc đồng hồ máy)	Hầu như không thể, vì TSA ký bằng khóa riêng được chứng nhận

Rủi ro bảo mật

Loại rủi ro	Mô tả chi tiết	Hậu quả có thể xảy ra
1. Lộ private key	Private key của người ký bị đánh cắp hoặc lưu trữ không an toàn.	Kẻ tấn công có thể giả mạo chữ ký hợp lệ trên tài liệu khác.
2. Padding Oracle Attack	Lỗ hổng trong cơ chế RSA PKCS#1 v1.5 cho phép giải mã hoặc ký giả mạo.	Toàn bộ hệ thống ký số bị phá vỡ, phải đổi cặp khóa mới.
3. Replay Attack	Kẻ tấn công tái sử dụng chữ ký cũ (PKCS#7 blob) gắn vào tài liệu khác.	Tài liệu giả có chữ ký hợp lệ nhưng nội dung sai lệch.
4. Tampering Incremental Update	Chỉnh sửa file PDF sau khi ký bằng cách thêm lớp update mới.	Người nhận không phát hiện nội dung bị thêm vào.

Loại rủi ro	Mô tả chi tiết	Hậu quả có thể xảy ra
5. Fake Timestamp / TSA giả mạo	Timestamp không đến từ TSA thật hoặc không có chứng thư xác thực.	Thời gian ký không đáng tin cậy, chữ ký mất giá trị pháp lý.
6. Hash Collision (SHA-1)	Sử dụng thuật toán hash yếu (SHA-1) dễ bị tạo file có hash trùng.	Chữ ký vẫn "hợp lệ" về mặt kỹ thuật nhưng sai nội dung.
7. Xác minh chứng thư không đầy đủ	Không kiểm tra OCSP/CRL hoặc chain đến root CA.	Có thể xác thực nhầm chứng thư bị thu hồi hoặc hết hạn.

III. Kết luận

Qua bài thực hành "Chữ ký số trong file PDF", em đã hiểu rõ:

- Cấu trúc PDF liên quan đến chữ ký số (Catalog, AcroForm, Signature Field, Signature Dictionary).
- Quy trình tạo và xác thực chữ ký bằng RSA – SHA256 theo chuẩn PDF 1.7 / PAdES.
- Cách lưu thời gian ký qua /M và timestamp RFC3161, cùng ý nghĩa pháp lý của chúng.
- Các rủi ro bảo mật như lộ khóa, tấn công replay, chỉnh sửa incremental update và cách phòng tránh.

Sinh viên ký