BÀI TẬP VỀ NHÀ – MÔN:
AN TOÀN VÀ BẢO MẬT THÔNG TIN
Chủ đề: Chữ ký số trong file PDF

1) Cấu trúc PDF liên quan chữ ký (Nghiên cứu)

Object quan trọng	Vai trò trong lưu/truy xuất chữ kí
Catalog	Object gốc của file PDF.Thường trỏ đến AcroForm nếu có chữ kí số.
AcroForm	Từ điển(Dictionary) chứ tất cả các trường biểu mẫu (Form fields),bao gồm cả trường chữ kí số
Pages Tree	Cấu trúc cây chứa tất cả các trang. Gồm /Kids (các Page object con) và /Count
Page Object	Mỗi trang cụ thể, chứa tham chiếu đến /Contents (dòng lệnh vẽ), /Resources, /Annots
Resources	Danh sách tài nguyên (font, hình ảnh, XObject, form…).
Content Streams	Dòng lệnh mô tả nội dung hiển thị của trang (text, hình ảnh, vector).
XObject	Đối tượng đồ họa có thể tái sử dụng (ví dụ logo, biểu mẫu, tem chữ ký).
Signature Field (Widget)	Trường hiển thị chữ ký trên trang PDF.Chứa tham chiếu đến từ điển chữ ký.
Signature Dictionary	Đối tượng chứa thông tin chữ ký: /Type /Sig, /Filter, /SubFilter,

(/Sig)	/ByteRange, /Contents, /M, /Name, /Reference.
/ByteRange	Mảng 4 phần tử xác định các vùng dữ liệu (byte) trong file PDF được dùng để tính hàm băm (hash). Vùng này loại trừ chính vùng chứa chữ ký (/Contents).
/Contents	Nơi lưu chữ ký nhị phân PKCS#7/CMS (thường 8–16 KB vùng dự trữ).
Incremental Update	Cơ chế thêm chữ ký mà không ghi đè file gốc — mỗi lần ký thêm là một incremental update mới.
DSS (Document Security Store)	Cấu trúc trong PAdES lưu chứng chỉ, OCSP, CRL, VRI giúp xác minh lâu dài (LTV – Long Term Validation).

Object refs quan trọng

Root (Catalog)	Liên kết toàn bộ cấu trúc tài liệu.
/AcroForm	Danh sách các trường form, trong đó có trường chữ ký.
/SigField	Trường biểu mẫu thể hiện vùng ký.
/SigDict	Lưu thông tin chữ ký, hash, chứng chỉ, thời gian ký.
/Contents	Dữ liệu chữ ký (PKCS#7/CMS blob).
/ByteRange	Dùng để xác định vùng dữ liệu đã được ký.
/DSS	Lưu chứng chỉ và thông tin xác minh cho xác thực dài hạn.

2. Thời gian ký trong PDF

Các vị trí có thể lưu thời gian ký

Vị trí	Mô tả	Giá trị pháp lý
/M trong **Signature dictionary**	Chuỗi ngày tháng (dạng D:YYYYMMDDHHmmSS+TZ). Do phần mềm ký tự ghi.	✗ Không có giá trị pháp lý.
Timestamp token (RFC 3161) trong **PKCS#7/CMS**	Thuộc tính timeStampToken trong thuộc tính có chữ ký. Gắn bởi TSA (Time Stamping Authority).	✓ Có giá trị pháp lý, xác nhận thời điểm ký.
Document Timestamp Object (PAdES)	Một chữ ký đặc biệt (SubFilter=ETSI.RFC3161) áp dụng cho toàn tài liệu, không cần private key người ký.	✓ Pháp lý cao, thường dùng cho lưu trữ lâu dài.
DSS (Document Security Store)	Có thể lưu thêm timestamp và thông tin xác minh (OCSP/CRL).	✓ Dùng cho xác thực lâu dài (LTV).

Khác biệt giữa /M và timestamp RFC 3161

So sánh	/M	Timestamp RFC3161
Nguồn gốc	Phần mềm ký tự ghi	Do cơ quan TSA phát hành
Định dạng	Chuỗi text trong PDF	Chứng chỉ số (PKCS#7/CMS Attribute)
Mức độ tin cậy	Thấp (có thể sửa được)	Cao, xác minh bằng khóa TSA
Mục đích	Hiển thị thời gian ký	Chứng minh thời điểm ký hợp lệ
Giá trị pháp lý	Không có	Có, theo chuẩn eIDAS/PAdES