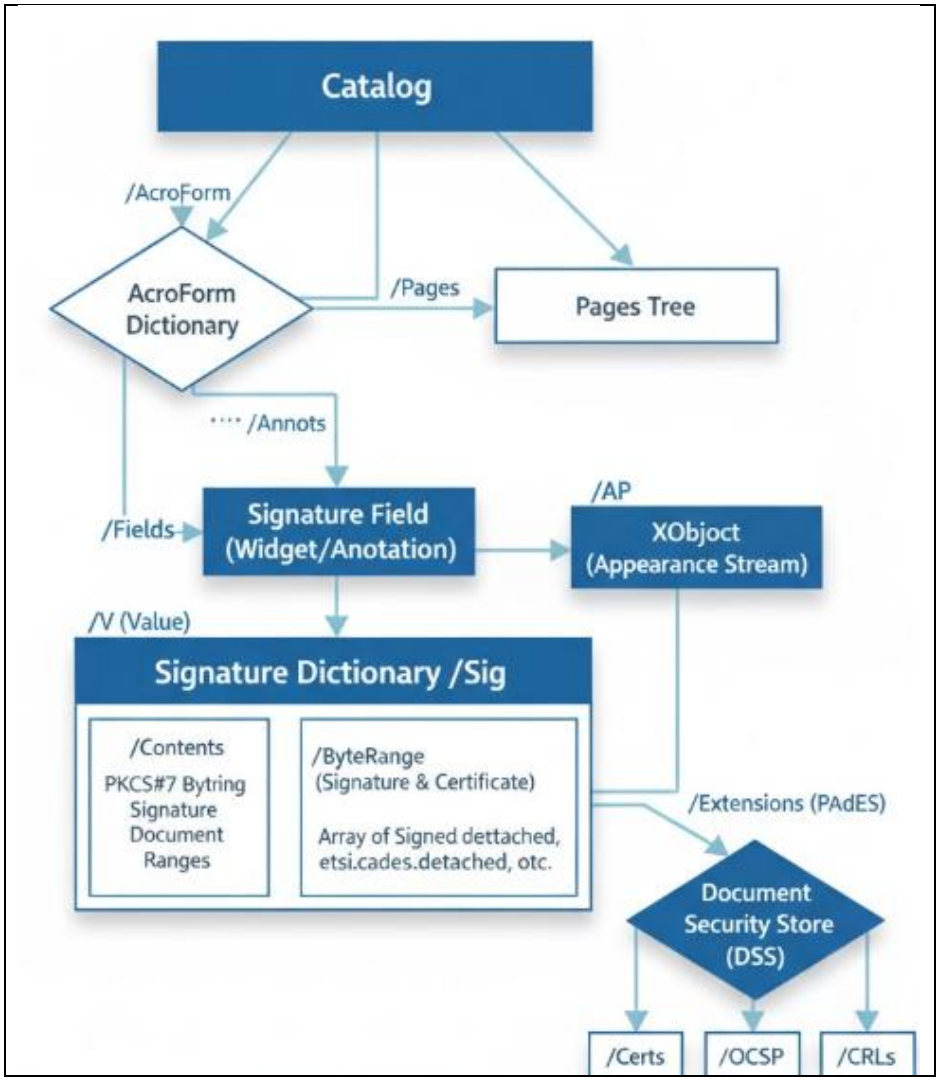
BÀI TẬP VỀ NHÀ – MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

BÀI LÀM

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

Thành Phần	Vai Trò
Catalog	Gốc của tài liệu PDF, trỏ đến /Pages và /AcroForm.
Pages tree	Cấu trúc cây chứa tất cả các trang.
Page object	Đại diện 1 trang, có /Contents và /Resources.
Resources	Nơi lưu font, hình ảnh, form fields,...
Content streams	Dòng lệnh mô tả nội dung hiển thị (text, hình).
XObject	Các đối tượng nhúng như hình hoặc form.
AcroForm	Chứa các trường biểu mẫu (form fields), gồm chữ ký.
Signature field (Widget)	Field có loại /Sig, hiển thị vùng ký.
Signature dictionary (/Sig)	Nơi chứa dữ liệu chữ ký, có /Contents, /ByteRange, /M.
/ByteRange	4 số xác định vùng dữ liệu được hash (bỏ qua vùng chứa chữ ký).
/Contents	Nơi chứa blob PKCS#7/CMS (chữ ký nhị phân).
Incremental update	Cơ chế ghi thêm phần chữ ký mà không thay đổi dữ liệu gốc.
DSS (Document Security Store)	Nơi lưu chứng chỉ, OCSP, CRL, timestamp (PAdES-LTV).

❖ **sơ đồ object**



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.

❖ **Các vị trí có thể lưu thông tin thời gian ký trong PDF có chữ ký số**

Vị trí lưu	Thuộc đối tượng	Mô tả & đặc điểm

/M	Trong Signature dictionary (/Type /Sig)	- Dạng text ISO-8601, ví dụ: /M (D:20251029T213000Z). - Do ứng dụng ký (signing software) tự ghi lại thời điểm ký. - Không có giá trị pháp lý, vì người ký có thể thay đổi thủ công.
timeStampToken (RFC 3161)	Bên trong PKCS#7/CMS (thuộc tính unsignedAttrs)	- Là chứng thực thời gian do TSA – Time Stamping Authority cấp. - Có giá trị pháp lý nếu TSA là tổ chức tin cậy. - Chứa dấu thời gian được ký bằng khóa riêng của TSA, đảm bảo "tài liệu đã tồn tại tại thời điểm đó".
Document Timestamp Object	Đối tượng riêng trong PDF (theo PAdES)	- Cho phép gắn timestamp toàn tài liệu mà không cần chữ ký cá nhân. - Dùng để chứng thực thời điểm lưu hoặc bảo quản file (ví dụ LTV).
DSS (Document Security Store)	Mục /DSS ở cuối PDF (theo ETSI EN 319 142 / PAdES-LTV)	- Lưu trữ timestamp, chứng chỉ, OCSP, CRL phục vụ xác minh lâu dài (LTV – Long Term Validation). - Có thể chứa Document Timestamp và TimeStamp Token dùng để chứng minh tài liệu và chữ ký vẫn hợp lệ sau nhiều năm.

❖ **So sánh /M và timestamp RFC 3161**

Tiêu chí	/M trong Signature dictionary	RFC 3161 Timestamp (timeStampToken)

Vị trí lưu	Trực tiếp trong /Sig dictionary của PDF	Bên trong PKCS#7/CMS (thuộc tính unsignedAttrs)
Cách tạo	Ứng dụng ký tự ghi thời gian hệ thống khi ký	Gửi hash tài liệu đến TSA (Time Stamping Authority) để nhận lại token đã được TSA ký
Chứng thực bởi bên thứ ba?	Không, chỉ là thông tin nội bộ	Có, được TSA ký bằng khóa riêng
Giá trị pháp lý	Không có	Có giá trị chứng minh thời điểm ký
Khả năng xác minh	Không thể kiểm tra tính chính xác	Có thể xác minh bằng chứng chỉ TSA và chữ ký TSA
Chuẩn tham chiếu	ISO 32000-1 / PDF 1.7	RFC 3161 (IETF), ETSI EN 319 422 (PAdES)