Câu 1. Cấu trúc PDF liên quan đến chữ ký số

1) Cấu trúc tổng quát của file PDF

File PDF gồm nhiều object được quản lý qua xref table và trailer:

```
%PDF-1.7
1 0 obj  ← Catalog
2 0 obj  ← Pages
3 0 obj  ← Page
4 0 obj  ← Contents
xref
trailer
%%EOF
```

Thành phần chính:

Thành phần	Vai trò
Header	Khai báo phiên bản PDF
Body	Chứa các object (Catalog, Pages, Fonts, Images...)
XRef Table	Bảng chỉ vị trí object
Trailer	Metadata, /Root, /Info
StartXRef & EOF	Đánh dấu kết thúc file

2) Cấu trúc khi có chữ ký số

Khi ký, PDF không sửa nội dung cũ mà thêm incremental update, gồm các object mới:

- AcroForm: biểu mẫu chứa trường ký.
- Signature Field (Widget): vùng hiển thị chữ ký.
- Signature Dictionary (/Sig): dữ liệu chữ ký (PKCS#7 hoặc CAdES).
- DSS (Document Security Store): chứa chứng chỉ, OCSP, CRL, timestamp phục vụ LTV (PAdES).

Sơ đồ mối liên hệ object:

Catalog

├── /Pages → /Page → /Contents

└── /AcroForm

  └── /Fields

└── Signature Field (Widget)

├── /FT /Sig

├── /Rect (...)

└── /V → Signature Dictionary

3) Vai trò các thành phần trong quá trình ký

Thành phần	Vai trò
Catalog	Nút gốc của tài liệu
AcroForm	Danh sách trường ký
Signature Field	Vùng ký hiển thị trên trang
Signature Dictionary (/Sig)	Chứa dữ liệu ký: /Filter, /SubFilter, /M, /ByteRange, /Contents
/ByteRange	Xác định vùng byte được hash (trừ vùng chứa chữ ký)
/Contents	Blob PKCS#7/CAdES (hash, cert, timestamp)
DSS	Lưu dữ liệu xác minh lâu dài

PDF ký số tuân theo chuẩn PAdES (ETSI EN 319 142) dựa trên PDF 1.7/2.0, cho phép xác thực tính toàn vẹn và chống sửa đổi sau khi ký.

Câu 2. Thời gian ký được lưu ở đâu trong PDF

PDF có thể chứa thời gian ở nhiều vị trí khác nhau — không phải vị trí nào cũng có giá trị pháp lý:

Vị trí lưu	Nơi chứa	Đặc điểm	Giá trị pháp lý
/M	Signature Dictionary	Dạng text, lấy từ máy người ký	Không
signingTime	Thuộc tính trong PKCS#7	Bị hash bảo vệ, nhưng không có chứng thực TSA	⚠ Tham khảo
timeStampToken	RFC 3161 trong PKCS#7	Có chữ ký TSA xác nhận thời điểm tồn tại tài liệu	Có
Document Timestamp Object	Chuẩn PAdES	Timestamp toàn bộ file, do TSA cấp	Có
DSS	Vùng xác minh lâu dài	Lưu Certs, OCSP, CRL, timestamp	Hỗ trợ LTV

So sánh nhanh:

Tiêu chí	/M	RFC 3161 Timestamp
Nguồn thời gian	Máy người ký	Máy chủ TSA
Có được ký bảo vệ không	Không	Có
Có thể sửa được không	Có	Không
Giá trị pháp lý	Không	Có
Chuẩn liên quan	PDF 1.7	RFC 3161, PAdES

Kết luận

- PDF có nhiều mốc thời gian, nhưng chỉ timestamp của TSA (RFC 3161 hoặc PAdES) có giá trị chứng thực.
- Thuộc tính /M chỉ để hiển thị, không được bảo vệ bởi chữ ký nên không có giá trị pháp lý.
- Các hệ thống chuyên nghiệp (hóa đơn, hợp đồng điện tử) luôn phải gắn timestamp hợp lệ từ TSA để đảm bảo giá trị pháp lý và xác minh lâu dài (LTV).