PDF là định dạng dựa trên object, với cấu trúc cây. Các object chính liên quan đến chữ ký số bao gồm:

Catalog (/Root): Object gốc của PDF, chứa tham chiếu đến Pages tree và AcroForm. Vai trò: Làm trung tâm lưu trữ metadata, bao gồm /AcroForm cho form fields như signature.

Pages tree: Cấu trúc cây các trang (/Pages), chứa Page objects. Vai trò: Tổ chức nội dung trang, nhưng chữ ký thường không ảnh hưởng trực tiếp trừ khi visible signature (widget annotation trên Page).

Page object: Đại diện một trang, chứa /Resources, /Contents. Vai trò: Nếu signature visible, Signature field (widget) được thêm vào /Annots của Page.

Resources: Dictionary chứa font, XObject (images/forms). Vai trò: Hỗ trợ render widget signature nếu có appearance stream.

Content streams: Dữ liệu hiển thị trang (operators như text, path). Vai trò: Không trực tiếp liên quan chữ ký, nhưng hash bao gồm chúng.

XObject: Object bên ngoài (Form XObject cho appearance). Vai trò: Sử dụng cho appearance của signature widget.

AcroForm: Dictionary trong Catalog, chứa /Fields (mảng fields). Vai trò: Quản lý form fields, bao gồm Signature field.

Signature field (widget): Một field trong /Fields, là annotation trên Page. Vai trò: Đại diện vị trí visible signature, chứa tham chiếu đến Signature dictionary.

Signature dictionary (/Sig): Dictionary trong Signature field, chứa /Filter (e.g., Adobe.PPKLite), /SubFilter (adbe.pkcs7.detached), /ByteRange, /Contents. Vai trò: Lưu metadata chữ ký.

/ByteRange: Mảng chỉ vùng bytes được hash (loại trừ /Contents). Vai trò: Xác định phạm vi tính hash.

/Contents: Hex string chứa PKCS#7/CMS blob (DER encoded). Vai trò: Lưu chữ ký thực tế.

Incremental updates: Cập nhật PDF bằng cách append bytes mới mà không overwrite. Vai trò: Cho phép thêm chữ ký mà giữ nguyên nội dung cũ, dễ kiểm tra tamper.

DSS (Document Security Store): Dictionary trong Catalog (/DSS), chứa /Certs, /OCSPs, /CRLs, /VRI. Vai trò: Lưu dữ liệu xác minh LTV (Long-Term Validation) để xác thực offline.

Object refs quan trọng và vai trò:

Catalog (ref 1 0): Lưu AcroForm và DSS.

AcroForm (ref e.g., 10 0): Lưu SigField.

SigField (ref e.g., 11 0): Lưu SigDict.

SigDict (ref e.g., 12 0): Lưu /ByteRange, /Contents.

DSS (ref e.g., 20 0): Lưu certs cho LTV.

Sơ đồ object (text-based):

textCatalog → /AcroForm → SigField (widget) → SigDict (/Sig) → /ByteRange, /Contents

Catalog → Pages → Page → /Annots → Widget (if visible)

Catalog → /DSS → /Certs, /OCSPs, /CRLs, /VRI (per signature)

2. Thời Gian Ký Được Lưu Ở Đâu?

Thông tin thời gian ký có thể lưu ở nhiều vị trí, nhưng độ tin cậy khác nhau:

/M trong Signature dictionary: Lưu dạng text (e.g., D:20251031000000+07'00'). Vai trò: Thời gian báo cáo bởi signer, không có giá trị pháp lý vì có thể giả mạo.

Timestamp token (RFC 3161) trong PKCS#7: Lưu trong attribute timeStampToken (unsigned attrs của SignerInfo). Vai trò: Thời gian trusted từ TSA (Time Stamping Authority), chống backdating.

Document timestamp object (PAdES): Một signature đặc biệt chỉ chứa timestamp, không cert. Vai trò: Bảo vệ toàn bộ document, bao gồm signatures trước, cho LTV.

DSS: Lưu timestamp và dữ liệu xác minh (OCSP responses chứa thời gian). Vai trò: Hỗ trợ xác thực dài hạn.

C