i. Cấu trúc PDF liên quan chữ ký

Catalog (Root), Gốc của cây object; tham chiếu tới Pages và AcroForm

Pages tree, Cấu trúc phân cấp chứa các trang PDF

Page object, Mỗi trang có /Resources và /Contents

Resources, Font, hình ảnh, XObject

Content stream, Dòng lệnh vẽ nội dung trang

XObject, Đối tượng đồ họa (image, form)

AcroForm, Lưu metadata về các trường form (Field)

Signature field (widget), Trường chứa thông tin chữ ký (/FT /Sig)

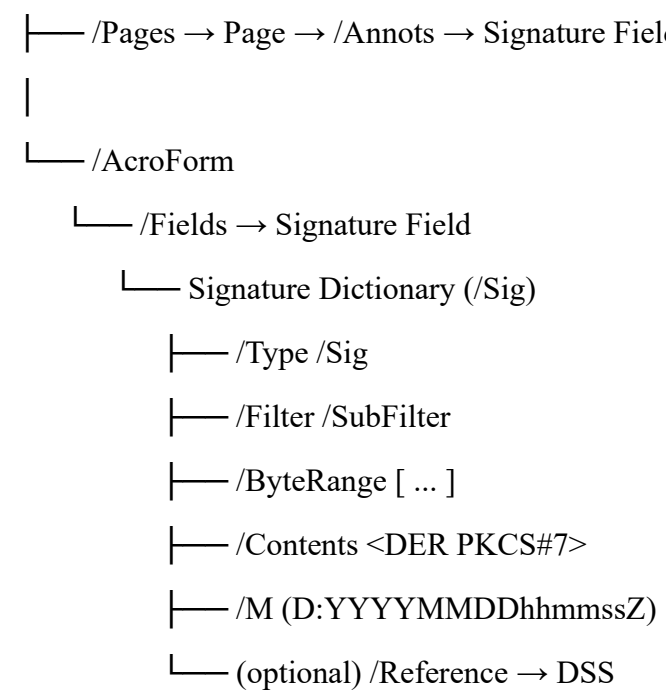
Signature dictionary (/Sig), Lưu nội dung chữ ký: /Filter, /SubFilter, /ByteRange, /Contents, /M

ByteRange, Mảng vị trí byte được tính hash

Contents, Blob chứa PKCS#7/CMS DER

Incremental update, Phần bổ sung khi ghi chữ ký, không sửa trực tiếp nội dung gốc

DSS (Document Security Store), Lưu dữ liệu LTV: chứng chỉ, CRL, OCSP, timestamp



ii. Thời gian ký được lưu ở đâu?

1. Thuộc tính /M trong Signature Dictionary3: /Sig
   - Không có giá trị pháp lý
2. Thuộc tính signingTime trong PKCS#7 (CMS SignedAttributes): Bên trong /Contents (blob PKCS#7 DER)
   - Có giá trị pháp lý cơ bản
3. Timestamp Token (RFC 3161): Attribute timeStampToken trong PKCS#7
   - Giá trị pháp lý cao
4. Document Timestamp (PAdES Part 4): Một chữ ký đặc biệt kiểu SubFilter /ETSI.RFC3161
   - Cao nhất (LTV)
5. DSS (Document Security Store)3/DSS Dictionary (tùy chọn trong PAdES-LTV)
   - Hỗ trợ xác minh lâu dài
6. Giải thích khác biệt giữa thông tin thời gian /M và timestamp RFC3161

Tiêu chí	**/M (Modification Date)**	**Timestamp RFC 3161**
Vị trí	Thuộc tính trong *Signature Dictionary* (/Sig)	Nằm trong gói **PKCS#7** (thuộc tính timeStampToken)
Nguồn	Do phần mềm ký tự ghi từ **đồng hồ máy tính** người ký	Do **TSA (Time Stamping Authority)** cấp, ký bằng khóa riêng của họ
Được bảo vệ bởi chữ ký?	có thể bị chỉnh sửa	được TSA ký, đảm bảo toàn vẹn
Độ tin cậy pháp lý	Thấp, chỉ để hiển thị thời gian ký	Cao, là bằng chứng pháp lý xác nhận thời điểm tài liệu tồn tại
Định dạng	Dạng text: D:YYYYMMDD	Dạng nhị phân ASN.1 theo chuẩn **RFC 3161**
Mục đích chính	Ghi chú thời gian ký do phần mềm đặt	Xác nhận thời gian ký thực tế và không thể chối bỏ