**Báo cáo: Chữ ký số trong PDF**

## 1) Cấu trúc PDF liên quan chữ ký

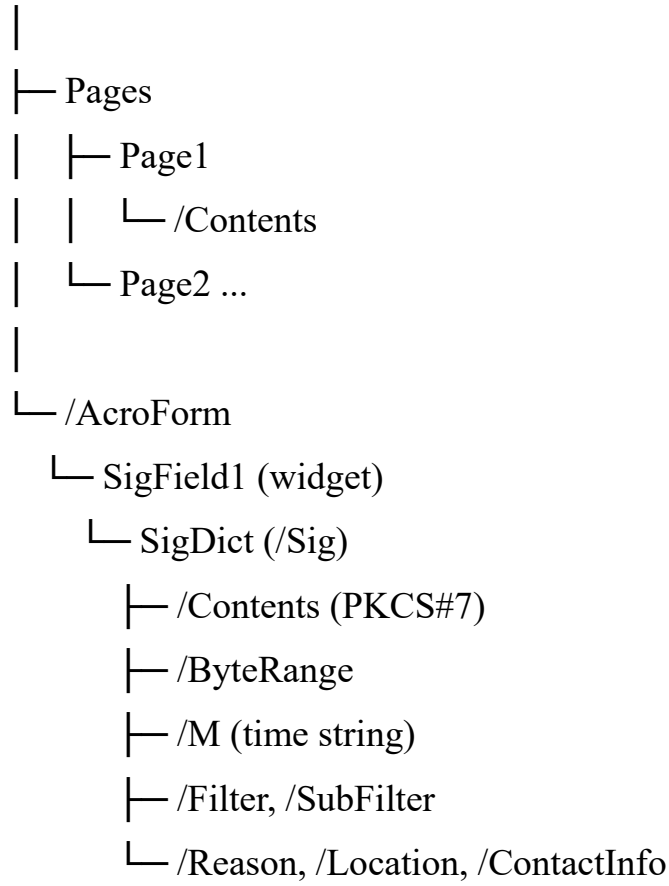
### Mô tả các thành phần chính

- **Catalog (/Catalog)**
  Là root object của PDF, chứa các tham chiếu quan trọng tới:
  - /Pages: Cây quản lý tất cả trang.
  - /AcroForm: Form chứa fields (bao gồm signature field).
  - /Metadata: Dữ liệu mô tả PDF.
- **Pages tree (/Pages)**
  Quản lý tất cả các trang PDF theo cấu trúc cây (tree).
  Mỗi nút có thể chứa danh sách con (/Kids) và tổng số trang (/Count).
- **Page object (/Page)**
  Đại diện một trang PDF, chứa:
  - /Resources: Font, hình ảnh, XObject.
  - /Contents: Content stream chứa dữ liệu hiển thị (text, hình ảnh, vector).
- **Resources (/Resources)**
  Chứa thông tin dùng chung cho trang:
  - Fonts, XObjects (hình ảnh hoặc reusable forms), Color Spaces.
- **Content streams (/Contents)**
  Chứa nội dung hiển thị của trang PDF. Đây là phần dữ liệu mà chữ ký sẽ ký (được xác định bởi /ByteRange).
- **XObject (/XObject)**
  Là object nhúng hình ảnh hoặc form tái sử dụng. Có thể là ảnh bitmap hoặc template form.
- **AcroForm (/AcroForm)**
  Là form của PDF, chứa tất cả form fields:
  - Signature fields (/SigField) dùng để nhúng chữ ký số.
  - Text fields, checkbox, radio button khác.

- **Signature field (/SigField)**
  Là field widget dành cho chữ ký số, chứa tham chiếu đến **Signature dictionary** (/Sig).
- **Signature dictionary (/Sig)**
  Object quan trọng chứa thông tin chữ ký:
  - /Filter và /SubFilter: Xác định chuẩn chữ ký (ví dụ: adbe.pkcs7.detached cho chữ ký PKCS#7).
  - /ByteRange: Xác định vùng byte trong PDF được ký.
  - /Contents: Dữ liệu chữ ký PKCS#7 hoặc CMS.
  - /M: Thời gian ký dạng text (không pháp lý, chỉ để hiển thị).
  - /Reason, /Location, /ContactInfo: Thông tin mô tả lý do ký và người ký.
- **Incremental updates**
  Khi ký PDF, dữ liệu mới được append vào cuối file, không thay đổi nội dung đã ký trước đó.
  Điều này giúp chữ ký trước vẫn hợp lệ, đồng thời hỗ trợ nhiều chữ ký trên cùng file.
- **DSS (Document Security Store, theo PAdES)**
  Theo chuẩn PAdES, DSS lưu trữ các dữ liệu hỗ trợ xác minh lâu dài:
  - Certificate chains, CRL, OCSP responses.
  - Timestamp tokens.
  - Hỗ trợ xác minh chữ ký số ngay cả khi các CA hoặc TSA ban đầu không còn tồn tại.

**Sơ đồ object tham khảo**

Catalog




**2) Thời gian ký (Signing Time)**

**Các vị trí lưu thông tin thời gian**

- **/M trong Signature dictionary**
  - Dạng text, ví dụ: (D:20251030153000+07'00').
  - Chỉ biểu diễn thời gian ký, **không có giá trị pháp lý**.
  - Chỉ phục vụ hiển thị và báo cáo nội bộ.
- **Timestamp token (RFC 3161) trong PKCS#7**
  - Lưu trong /Contents dưới dạng attribute timeStampToken.
  - Có giá trị pháp lý, được ký bởi TSA (Time Stamp Authority).
  - Xác thực thời gian ký chính xác, dùng trong chứng thực pháp lý và long-term validation.

- **Document timestamp object (PAdES)**
  - Timestamp toàn document, không chỉ cho một chữ ký.
  - Hỗ trợ việc ký số nhiều lần và xác minh chữ ký lâu dài.
- **DSS (Document Security Store)**
  - Nếu DSS lưu timestamp và dữ liệu xác minh (certificates, CRL, OCSP), có thể xác thực chữ ký lâu dài mà không cần truy vấn CA/TSA gốc.

**So sánh /M vs RFC3161 timestamp**

| **Thuộc tính** | **/M** | **RFC3161 Timestamp** |
|---|---|---|
| Dạng lưu | Text trong PDF | Token số hóa (PKCS#7) |
| Giá trị pháp lý | Không | Có, xác thực bởi TSA |
| Bảo mật chống sửa | Thấp | Cao (token ký bởi TSA) |
| Phục vụ xác minh lâu dài | Không | Có |

**3) Rủi ro bảo mật liên quan chữ ký PDF**

- **Chữ ký chỉ bảo vệ vùng byte đã ký:**
  Nội dung khác trong PDF có thể append qua incremental update mà không bị ảnh hưởng chữ ký trước nếu không kiểm tra toàn bộ /ByteRange.
- **Thông tin thời gian /M có thể bị thay đổi:**
  Vì chỉ là text, không được ký riêng, nên không đảm bảo tính xác thực.

- **Phụ thuộc vào TSA tin cậy:**
  Timestamp RFC3161 chỉ có giá trị pháp lý nếu TSA đáng tin cậy. TSA bị xâm nhập làm giảm giá trị pháp lý.
- **Xác minh chữ ký lâu dài phụ thuộc DSS:**
  Nếu thiếu CRL, OCSP, hoặc dữ liệu DSS lỗi, chữ ký có thể không xác minh được trong tương lai.
- **Chữ ký không bảo vệ metadata hoặc font/resources:**
  Một số object PDF như fonts nhúng hoặc metadata có thể bị sửa mà không ảnh hưởng chữ ký nếu không nằm trong /ByteRange.

NGUYEN HOANG VIET
SDT: 0359621318
MSV: K225480106074
Ngày ký: 30/10/2025