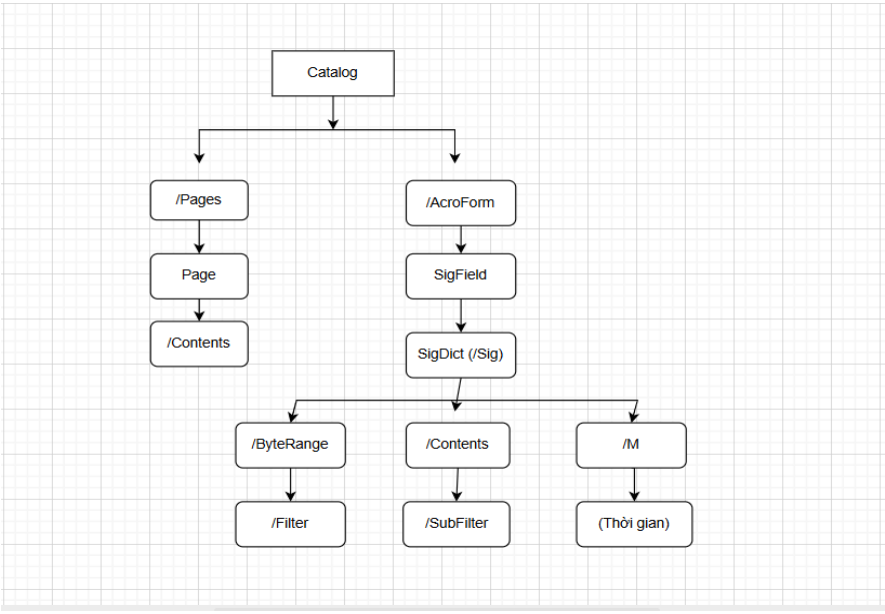
**Nghiên cứu: Cấu trúc PDF liên quan chữ ký và thời gian ký**

## 1. Cấu trúc PDF liên quan chữ ký

Trong một tệp PDF, chữ ký số được nhúng vào thông qua các đối tượng (objects) có cấu trúc phân cấp.
Các thành phần chính bao gồm:
- Catalog (Root): Gốc của toàn bộ cấu trúc tài liệu PDF.
- Pages Tree: Liên kết tới các trang của tài liệu.
- Page Object: Đại diện cho từng trang, chứa thông tin tài nguyên và nội dung.
- Resources: Danh sách các tài nguyên được dùng trong trang (phông chữ, hình ảnh, biểu mẫu...).
- Content Streams: Dòng nội dung của từng trang (chứa các lệnh vẽ, text,...).
- XObject: Đối tượng nhúng, có thể là hình ảnh hoặc biểu mẫu.
- AcroForm: Đối tượng chứa các trường biểu mẫu (form fields), bao gồm cả trường chữ ký.
- Signature Field (Widget): Là phần tử giao diện hiển thị vùng chữ ký.
- Signature Dictionary (/Sig): Chứa thông tin chữ ký số (người ký, thời gian, thuật toán, chứng chỉ...).
- /ByteRange: Xác định các byte của file được bảo vệ bởi chữ ký.
- /Contents: Chứa giá trị chữ ký mã hóa (PKCS#7/CMS).
- Incremental Updates: Cơ chế thêm nội dung hoặc chữ ký mới mà không ghi đè lên phần trước.
- DSS (Document Security Store): Lưu thông tin xác minh chữ ký (chứng chỉ, CRL, OCSP, timestamp) theo chuẩn PAdES.

**Sơ đồ quan hệ giữa các đối tượng:**



**2. Thời gian ký được lưu ở đâu?**

Trong tài liệu PDF, thông tin thời gian ký có thể được lưu ở nhiều vị trí khác nhau:

1. Trường /M trong Signature Dictionary:
   - Lưu thời gian ký dưới dạng chuỗi văn bản (text string).
   - Không có giá trị pháp lý vì không được xác thực bởi bên thứ ba.
2. Timestamp Token (RFC 3161) trong PKCS#7:
   - Là một thuộc tính (attribute) của cấu trúc chữ ký CMS (timeStampToken).
   - Được cung cấp bởi Time Stamping Authority (TSA), có giá trị pháp lý.
3. Document Timestamp Object (PAdES):
   - Là một dạng chữ ký đặc biệt áp dụng cho toàn bộ tài liệu (không gắn người ký).
   - Được dùng để đóng dấu thời gian cho tài liệu điện tử.
4. DSS (Document Security Store):
   - Có thể chứa thông tin timestamp, OCSP, CRL và dữ liệu xác minh khác.

**Khác biệt giữa /M và timestamp RFC3161:**

- /M chỉ là thông tin thời gian do phần mềm ký chèn vào, không được bảo vệ bởi cơ chế xác thực.
- Timestamp RFC3161 được tạo bởi bên thứ ba (TSA) và được ký số, đảm bảo giá trị pháp lý và xác thực thời gian.