BÀI TẬP VỀ NHÀ – MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

Chủ đề: Chữ ký số trong file PDF

Giảng viên: Đỗ Duy Cốp

Thời điểm giao: 2025-10-24 11:45

Đối tượng áp dụng: Toàn bộ sv lớp học phần 58KTPM

Hạn nộp: Sv upload tất cả lên github trước 2025-10-31 23:59:59

I. MÔ TẢ CHUNG

Sinh viên thực hiện báo cáo và thực hành: phân tích và hiện thực việc nhúng, xác

thực chữ ký số trong file PDF.

Phải nêu rõ chuẩn tham chiếu (PDF 1.7 / PDF 2.0, PAdES/ETSI) và sử dụng công cụ

thực thi (ví dụ iText7, OpenSSL, PyPDF, pdf-lib).

II. CÁC YÊU CẦU CỤ THỂ

1. CẤU TRÚC PDF LIÊN QUAN CHỮ KÝ (TÓM TẮT)

Các object liên quan chính:

Catalog (Root): entry /AcroForm trỏ tới AcroForm object.

Pages tree: Catalog → /Pages → Page objects.

Page object: contains /Contents, /Resources.

AcroForm: chứa /Fields — danh sách field, trong đó có Signature field (widget).

Signature Field (Widget): field type Sig (AcroForm field) — appearance (visual) optional.

Signature Dictionary (/Sig): chứa các entry quan trọng: /Filter, /SubFilter, /ByteRange, /Contents, /M, /Name, /Reference.

-
    -

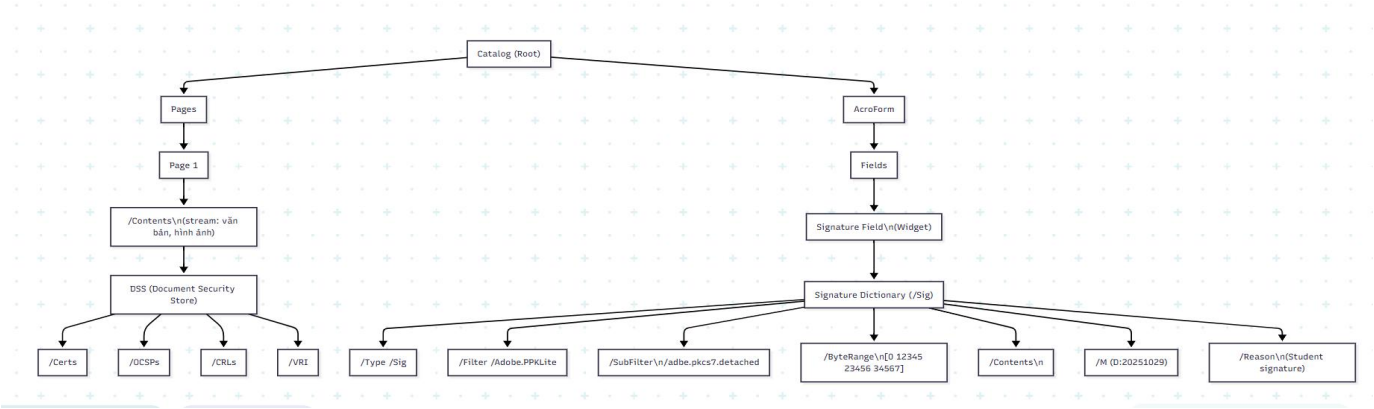
/Contents: chứa blob PKCS#7 (DER), thường hex-encoded hoặc binary in a string with reserved length.

/ByteRange: array of 4 integers [offset0, length0, offset1, length1] chỉ phần file được hash (khi ghi signature, vùng /Contents được loại trừ).

/M: signing time as text (human readable, không phải timestamp token).

Incremental update: việc thêm chữ ký thường ghi như incremental PDF update — nội dung mới appended ở cuối file; dùng để phát hiện sửa đổi.

DSS (Document Security Store) — PAdES: optional object chứa Certs, OCSP, CRL, và timestamp tokens để hỗ trợ LTV (Long-Term Validation).



2. THỜI GIAN KÝ ĐƯỢC LƯU Ở ĐÂU?

Các vị trí có thể lưu thông tin thời gian ký:

2.1 /M trong Signature dictionary

Dạng: text (ví dụ: D:20251024...Z) - chỉ là thông tin mô tả, không đảm bảo tính pháp lý cho timestamp.

2.2 Timestamp token (RFC 3161)

Được đưa vào như attribute timeStampToken trong PKCS#7 (signedAttributes) — đây là một timestamp do Time Stamping

Authority (TSA) cấp, có tính pháp lý và chống được replay (vì chứa hash của tệp và signature time).

2.3 Document timestamp object (PAdES)

PAdES định nghĩa cách nhúng document-level timestamp objects.

2.4 DSS

Nếu DSS chứa token timestamp, điều này hỗ trợ LTV.

Khác biệt /M vs RFC3161 timestamp

- **/M:** chỉ text lưu thời điểm; có thể do client tự gán; dễ bị giả mạo (phụ thuộc vào chữ ký để bảo vệ nhưng bản thân /M không đảm bảo).
- **RFC3161 timestamp token**: do TSA ký, chứa hash và thời gian; thường được chèn trong PKCS#7 signed attributes; có giá trị chứng thực thời gian mạnh hơn.

Hoang Duc Hoi
SDT: 0326559478
MSV: K225480106085
Ngày ký: 31/10/2025