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-li

II. CÁC YÊU CẦU CỤ THỂ

1) Cấu trúc PDF liên quan chữ ký (Nghiên cứu)

Catalog, Pages tree, Page object, Resources, Content streams, XObject, AcroForm, Signature field (widget), Signature dictionary (/S
Đầu ra: 1 trang tóm tắt + sơ đồ object (Catalog → Pages → Page → /Contents; Catalog → /AcroForm → SigField → SigDict).

2) Thời gian ký được lưu ở đâu?

+ /M trong Signature dictionary (dạng text, không phải bằng chứng pháp lý).
+ Timestamp token (RFC3161) trong PKCS#7 (attribute timeStampToken).
+ Document timestamp object (PAdES).
+ DSS (Document Security Store) nếu có lưu timestamp và dữ liệu xác minh.
Giải thích: /M chỉ là metadata, RFC3161 là token TSA (bằng chứng thời điểm).

3) Các bước tạo và lưu chữ ký trong PDF (tóm tắt)

1. Chuẩn bị file PDF gốc.
2. Tạo Signature field (AcroForm), reserve vùng /Contents (ví dụ 8192 bytes).
3. Xác định /ByteRange (loại trừ vùng /Contents khỏi hash).
4. Tính hash (SHA-256/512) trên vùng ByteRange.
5. Tạo PKCS#7/CMS detached hoặc CAdES (include messageDigest, signingTime, certificate chain).
6. Chèn blob DER PKCS#7 vào /Contents đúng offset; ghi incremental update.
7. (LTV) Cập nhật DSS với Certs, OCSPs, CRLs, VRI.