TIÊU ĐỀ: BÁO CÁO KỸ THUẬT VÀ QUY TRÌNH TRIỂN KHAI

MODULE XÁC THỰC VÀ KÝ SỐ TÀI LIỆU

NGÀY: 8 tháng 11 năm 2025

BỞI: Nhóm Phát triển Lõi

PHIÊN BẢN: 1.0

PHẦN 1: TỔNG QUAN VỀ DỰ ÁN

1.1. Giới thiệu

Tài liệu này mô tả các yêu cầu kỹ thuật, kiến trúc hệ thống và quy trình triển khai cho "Module Ký số PAdES" (PDF Advanced Electronic Signatures). Mục tiêu của dự án là xây dựng một giải pháp cho phép người dùng ký và xác thực các tài liệu PDF bằng cách sử dụng cơ sở hạ tầng khóa công khai (PKI) tuân thủ các tiêu chuẩn ETSI và ISO 32000.

1.2. Mục tiêu

- Đảm bảo tính toàn vẹn (Integrity) của tài liệu sau khi ký.

- Đảm bảo tính xác thực (Authentication) của người ký.

- Đảm bảo tính chống chối bỏ (Non-repudiation).

- Hỗ trợ xác thực lâu dài (Long-Term Validation - LTV).

1.3. Phạm vi

Module này sẽ bao gồm hai chức năng chính:

1. Tạo chữ ký (Signing): Nhúng một chữ ký số hợp lệ vào tài liệu PDF.

2. Xác thực chữ ký (Verification): Kiểm tra tính hợp lệ của các chữ ký có trong tài liệu.

PHẦN 2: YÊU CẦU KỸ THUẬT

2.1. Yêu cầu mật mã

- Thuật toán băm: Phải hỗ trợ SHA-256 và SHA-512.

- Thuật toán ký: Phải hỗ trợ RSA với kích thước khóa tối thiểu 3072-bit.

- Đệm (Padding): Ưu tiên sử dụng RSASSA-PSS, hỗ trợ RSASSA-PKCS1-v1_5 để tương thích.

2.2. Yêu cầu định dạng (Tuân thủ PAdES - ETSI EN 319 142)

- Chữ ký phải được nhúng dưới dạng CAdES (CMS Advanced Electronic Signatures).

- Gói chữ ký (PKCS#7/CMS) phải ở dạng "detached" (chữ ký tách rời).

- Phải bao gồm các thuộc tính đã xác thực (authenticated attributes) như:

  - messageDigest (hash của tài liệu).

  - signingTime (thời gian ký).

  - contentType (cho biết đây là dữ liệu PDF).

2.3. Yêu cầu xác thực Lâu dài (LTV)

Để đảm bảo chữ ký có thể được xác thực nhiều năm trong tương lai (ngay cả khi chứng thư gốc hết hạn hoặc CA không còn tồn tại), hệ thống phải có khả năng nhúng các thông tin sau vào PDF (thông qua DSS - Document Security Store):

- Toàn bộ chuỗi chứng thư (Certificate chain).

- Thông tin thu hồi: Phản hồi OCSP (Online Certificate Status Protocol) hoặc CRL (Certificate Revocation List).

- (Tùy chọn) Dấu thời gian (Timestamp Token) từ một Cơ quan Dấu thời gian (TSA) tin cậy.

PHẦN 3: LUỒNG HOẠT ĐỘNG CHI TIẾT

3.1. Luồng tạo chữ ký (Signing Workflow)

Đây là các bước mà script phải thực hiện tuần tự:

1. (Chuẩn bị): Tải file PDF gốc, Private Key và Certificate Chain.

2. (Tạo Field): Phân tích cấu trúc PDF và chèn một đối tượng "Signature Field" (AcroForm) vào cấu trúc cây của tài liệu.

3. (Reserve): Dành riêng (reserve) một khoảng trống (ví dụ: 8192 bytes) cho nội dung chữ ký (/Contents).

4. (Xác định ByteRange): Xác định chính xác các khoảng byte của tài liệu sẽ được băm. Về cơ bản, đây là "toàn bộ file" *ngoại trừ* chính khoảng trống /Contents đã reserve ở bước 3.

5. (Tính Hash): Tính toán hash (ví dụ: SHA-256) trên các vùng ByteRange đã xác định.

6. (Tạo PKCS#7): Tạo một gói tin CMS/PKCS#7. Gói tin này chứa hash của tài liệu (từ bước 5), thời gian ký, chứng thư của người ký, và được ký bằng private key.

7. (Chèn chữ ký): Chuyển đổi gói tin PKCS#7 sang định dạng DER (hex), sau đó chèn nó vào đúng khoảng trống /Contents đã reserve.

8. (Lưu): Ghi lại tất cả các thay đổi này dưới dạng một "Incremental Update" (cập nhật tăng dần) vào cuối file PDF. Điều này đảm bảo file gốc không bị thay đổi.

3.2. Luồng xác thực (Verification Workflow)

1. (Đọc): Mở file PDF và tìm đối tượng Signature.

2. (Tách): Đọc /ByteRange và /Contents từ Signature dictionary. Tách gói tin PKCS#7 ra khỏi /Contents.

3. (Tính lại Hash): Tính lại hash của tài liệu dựa trên /ByteRange (giống hệt bước 5 của luồng ký).

4. (So sánh Hash): Giải mã gói tin PKCS#7, lấy ra 'messageDigest' bên trong và so sánh nó với hash vừa tính lại. Nếu không khớp, tài liệu đã bị thay đổi (lỗi toàn vẹn).

5. (Xác thực Chữ ký): Dùng public key (trong chứng thư) để xác thực chữ ký của gói PKCS#7.

6. (Kiểm tra Tin cậy): Xây dựng chuỗi chứng thư từ chứng thư người ký lên đến một CA gốc (Root CA) được tin tưởng.

7. (Kiểm tra Thu hồi): Kiểm tra thông tin OCSP/CRL (nếu có) để đảm bảo chứng thư vẫn hợp lệ tại thời điểm ký.