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

**BÀI LÀM**

1.) Cấu trúc PDF liên quan chữ ký (Nghiên cứu)- Mô tả ngắn gọn: Catalog, Pages tree, Page object, Resources, Content streams, XObject, AcroForm, Signature field (widget), Signature dictionary (/Sig), /ByteRange, /Contents, incremental updates, và DSS (theo PAdES).- Liệt kê object refs quan trọng và giải thích vai trò của từng object trong lưu/truy xuất chữ ký

|  |  |
| --- | --- |
| Thành Phần | Vai Trò |
| Catalog | Gốc của tài liệu PDF, trỏ đến /Pages và /AcroForm. |
| Pages tree | Cấu trúc cây chứa tất cả các trang. |
| Page object | Đại diện 1 trang, có /Contents và /Resources. |
| Resources | Nơi lưu font, hình ảnh, form fields,... |
| Content streams | Dòng lệnh mô tả nội dung hiển thị (text, hình). |
| XObject | Các đối tượng nhúng như hình hoặc form. |
| AcroForm | Chứa các trường biểu mẫu (form fields), gồm chữ ký. |
| Signature field (Widget) | Field có loại /Sig, hiển thị vùng ký. |
| Signature dictionary (/Sig) | Nơi chứa dữ liệu chữ ký, có /Contents, /ByteRange, /M. |
| /ByteRange | 4 số xác định vùng dữ liệu được hash (bỏ qua vùng chứa chữ ký). |
| /Contents | Nơi chứa blob PKCS#7/CMS (chữ ký nhị phân). |
| Incremental update | Cơ chế ghi thêm phần chữ ký mà không thay đổi dữ liệu gốc. |
| DSS (Document Security Store) | Nơi lưu chứng chỉ, OCSP, CRL, timestamp (PAdES-LTV). |

* **sơ đồ object**

|  |
| --- |
|  |

2. Thời gian ký được lưu ở đâu?

* Nêu tất cả vị trí có thể lưu thông tin thời gian:
* /M trong Signature dictionary (dạng text, không có giá trị pháp lý).
* Timestamp token (RFC 3161) trong PKCS#7 (attribute timeStampToken).
* Document timestamp object (PAdES).
* DSS (Document Security Store) nếu có lưu timestamp và dữ liệu xác minh.
* Giải thích khác biệt giữa thông tin thời gian /M và timestamp RFC3161.
* **Các vị trí có thể lưu thông tin thời gian ký trong PDF có chữ ký số**

|  |  |  |
| --- | --- | --- |
| Vị trí lưu | Thuộc đối tượng | Mô tả & đặc điểm |
| /M | Trong Signature dictionary (/Type /Sig) | - Dạng text ISO-8601, ví dụ: /M (D:20251029T213000Z). - Do ứng dụng ký (signing software) tự ghi lại thời điểm ký. - Không có giá trị pháp lý, vì người ký có thể thay đổi thủ công. |
| timeStampToken (RFC 3161) | Bên trong PKCS#7/CMS (thuộc tính unsignedAttrs) | - Là chứng thực thời gian do TSA – Time Stamping Authority cấp. - Có giá trị pháp lý nếu TSA là tổ chức tin cậy. - Chứa dấu thời gian được ký bằng khóa riêng của TSA, đảm bảo “tài liệu đã tồn tại tại thời điểm đó”. |
| Document Timestamp Object | Đối tượng riêng trong PDF (theo PAdES) | - Cho phép gắn timestamp toàn tài liệu mà không cần chữ ký cá nhân. - Dùng để chứng thực thời điểm lưu hoặc bảo quản file (ví dụ LTV). |
| DSS (Document Security Store) | Mục /DSS ở cuối PDF (theo ETSI EN 319 142 / PAdES-LTV) | - Lưu trữ timestamp, chứng chỉ, OCSP, CRL phục vụ xác minh lâu dài (LTV – Long Term Validation). - Có thể chứa Document Timestamp và TimeStamp Token dùng để chứng minh tài liệu và chữ ký vẫn hợp lệ sau nhiều năm. |

* **So sánh /M và timestamp RFC 3161**

|  |  |  |
| --- | --- | --- |
| Tiêu chí | /M trong Signature dictionary | RFC 3161 Timestamp (timeStampToken) |
| Vị trí lưu | Trực tiếp trong /Sig dictionary của PDF | Bên trong PKCS#7/CMS (thuộc tính unsignedAttrs) |
| Cách tạo | Ứng dụng ký tự ghi thời gian hệ thống khi ký | Gửi hash tài liệu đến TSA (Time Stamping Authority) để nhận lại token đã được TSA ký |
| Chứng thực bởi bên thứ ba? | Không, chỉ là thông tin nội bộ | Có, được TSA ký bằng khóa riêng |
| Giá trị pháp lý | Không có | Có giá trị chứng minh thời điểm ký |
| Khả năng xác minh | Không thể kiểm tra tính chính xác | Có thể xác minh bằng chứng chỉ TSA và chữ ký TSA |
| Chuẩn tham chiếu | ISO 32000-1 / PDF 1.7 | RFC 3161 (IETF), ETSI EN 319 422 (PAdES) |

4. Các bước tạo và lưu chữ ký số

1. Chuẩn bị: PDF gốc, private RSA key, certificate.
2. Tạo Signature Field: thêm /FT=/Sig vào /AcroForm, reserve /Contents (vd: 8192 bytes).
3. Xác định /ByteRange: chọn vùng hash, loại trừ /Contents.
4. Tính hash: SHA-256 hoặc SHA-512 trên ByteRange.
5. Tạo PKCS#7/CAdES: ký hash bằng RSA, bao gồm messageDigest, signingTime, certificate chain; tùy chọn thêm timestamp RFC3161.
6. Chèn chữ ký: ghi PKCS#7 vào /Contents, dùng incremental update.
7. (Tùy chọn) LTV/DSS: thêm Certs, OCSP, CRL, VRI để xác thực lâu dài.

Đầu ra: PDF gốc (original.pdf), PDF đã ký (signed.pdf), script thực hiện.

**5. Rủi ro chính và biện pháp giảm thiểu**

1. **Rò rỉ private key**
   * *Rủi ro*: Kẻ xấu dùng key giả mạo chữ ký.
   * *Giảm thiểu*: Lưu key offline, dùng key thử nghiệm; không upload key thật lên GitHub; dùng HSM hoặc phần mềm quản lý khóa.
2. **Padding oracle / lỗi RSA**
   * *Rủi ro*: Kỹ thuật tấn công khai thác padding RSA, làm giả chữ ký.
   * *Giảm thiểu*: Dùng RSA-PSS thay PKCS#1 v1.5; chọn key ≥ 2048-bit, hash SHA-256 trở lên.
3. **Replay / ký lại tài liệu cũ**
   * *Rủi ro*: Kẻ tấn công tái sử dụng chữ ký hợp lệ trên tài liệu khác.
   * *Giảm thiểu*: Dùng timestamp RFC3161 và lưu chứng chỉ trong DSS/LTV; kiểm tra incremental update.
4. **Sửa đổi nội dung PDF sau khi ký**
   * *Rủi ro*: Chữ ký bị vô hiệu nếu PDF bị thay đổi.
   * *Giảm thiểu*: Dùng incremental update đúng, kiểm tra /ByteRange, validate hash.
5. **Chứng chỉ không tin cậy / hết hạn**
   * *Rủi ro*: Không xác thực được chữ ký hoặc bị từ chối.
   * *Giảm thiểu*: Dùng chain CA tin cậy, kiểm tra OCSP/CRL, cập nhật DSS.
6. **Mất tính hợp pháp về thời gian**
   * *Rủi ro*: Thời gian ký /M không có giá trị pháp lý.
   * *Giảm thiểu*: Dùng RFC3161 timestamp token, lưu trong PKCS#7 hoặc DSS.

**6. Khuyến nghị kỹ thuật**

* Thuật toán mạnh: RSA ≥ 2048-bit, SHA-256+, ECC/PSS nếu được
* Bảo vệ private key, không upload lên GitHub
* Sử dụng timestamp hợp pháp và LTV/DSS
* Tuân theo chuẩn PDF 1.7/2.0 và ETSI PAdES
* Kiểm tra chữ ký đầy đủ: hash, signature, chain, OCSP/CRL, incremental update

**7. Minh họa File đính kèm**

**Thư mục CHU\_KI\_SO chứa các file sau:**

|  |  |
| --- | --- |
| **File** | **Nội dung / Vai trò** |
| cert.pem | Certificate public dùng ký số |
| private.pem | Private key RSA dùng ký (key thử nghiệm) |
| public.pem | Public key tương ứng với private key |
| chuki.py | Script tạo chữ ký và chèn vào PDF |
| CHU\_KI\_SO\_BTVN1.pdf | PDF gốc hoặc PDF đã ký bài tập 1 |
| CHU\_KI\_SO\_BTVN2.pdf | PDF gốc hoặc PDF đã ký bài tập 2 |
| signature\_image\_template.png | Hình ảnh chữ ký dùng chèn vào PDF (visual) |
| signature\_image\_stamp.png | Hình ảnh stamp chữ ký/tem |
| signature.bin | File lưu chữ ký PKCS#7 dạng nhị phân |
| temp\_visual.pdf | PDF tạm thời để hiển thị chữ ký trước khi ký chính thức |
| unsigned.pdf | PDF đã chuẩn bị signature field nhưng chưa ký |