TRƯỜNG ĐẠI HỌC KỸ THUẬT CÔNG NGHIỆP

KHOA ĐIỆN TỬ

BỘ MÔN. KỸ THUẬT ĐIỆN TỬ

BÀI TẬP 2

AN TOÀN BẢO MẬT THÔNG TIN

Sinh viên: Vũ Lân

Lớp: K58KTP

MSSV : K225480106036

Thái Nguyên – 2025

BÁO CÁO BÀI TẬP 02 – CHỮ KÝ SỐ PDF

Sinh viên thực hiện: Vũ Lân
Ngày hoàn thành: 30/10/2025
Môi trường thực hiện: Windows 11 + Visual Studio 2022 + .NET 8.0
Thư viện chính: iText7 + BouncyCastle + OpenSSL

I. MÔ TẢ CẤU TRÚC HỆ THỐNG

1. Mục tiêu bài tập

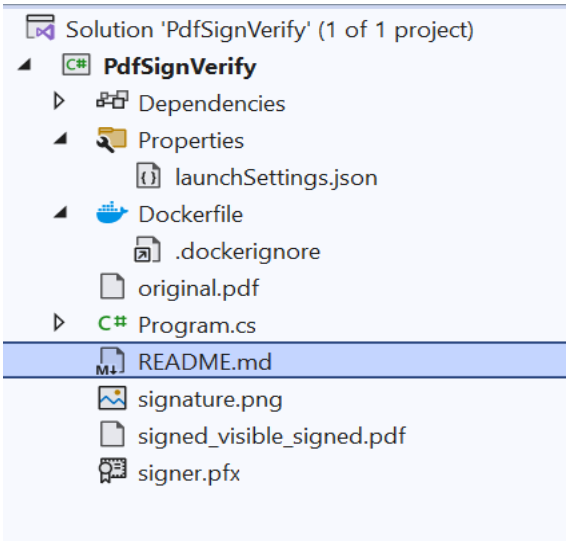
Xây dựng chương trình thực hiện ký số (Digital Signature) trên file PDF, hiển thị chữ ký tay, gắn thông tin người ký, đồng thời xác thực chữ ký theo chuẩn PAdES (ETSI EN 319 142).
Kết quả sau khi chạy chương trình:

- Tạo file PDF có chữ ký hiển thị.
- Chữ ký hợp lệ, có thể xác minh bằng iText7 hoặc Adobe Acrobat.
- Khi chỉnh sửa file sau khi ký, chữ ký sẽ bị vô hiệu hóa.

2. Kiến trúc chương trình

Cấu trúc thư mục dự án:

- **Program.cs:** Mã nguồn chính ký và xác thực.
- **signer.pfx:** Chứng chỉ số và khóa bí mật cá nhân.
- **signature.png:** Hình ảnh chữ ký tay "Vũ Lân" hiển thị trên PDF.
- **original.pdf:** Tài liệu gốc.
- **signed_visible_signed.pdf:** File đã ký số.
- **tampered.pdf:** Bản đã bị chỉnh sửa để kiểm tra cảnh báo.



II. THỜI GIAN KÝ VÀ KẾT QUẢ THỰC NGHIỆM

1. Tạo chứng chỉ ký số

Sử dụng **OpenSSL**, sinh khóa RSA 3072 bit và chứng chỉ tự ký:

```
openssl genrsa -out key.pem 3072
openssl req -new -x509 -key key.pem -out cert.pem -days 365 ^
  -subj "/C=VN/ST=HN/L=HN/O=VuLan/OU=IT/CN=Vu Lan"
openssl pkcs12 -export -out signer.pfx -inkey key.pem -in cert.pem -passout pass:1234
```

Dùng file signer.pfx gộp cả 2, định dạng PKCS#12 bắt buộc có trong project

```
// CẤU HÌNH MẶC ĐỊNH
// ==========================
const string SignatureImage = "signature.png";
const string OriginalPdf = "original.pdf";
const string SignedPdf = "signed_visible_signed.pdf";
const string PfxFile = "signer.pfx";
const string PfxPassword = "1234"; // đổi nếu khác
```

2. Ký số file PDF

Chọn đúng thư mục chứa project: cd "E:\chukyso2\PdfSignVerify\PdfSignVerify"

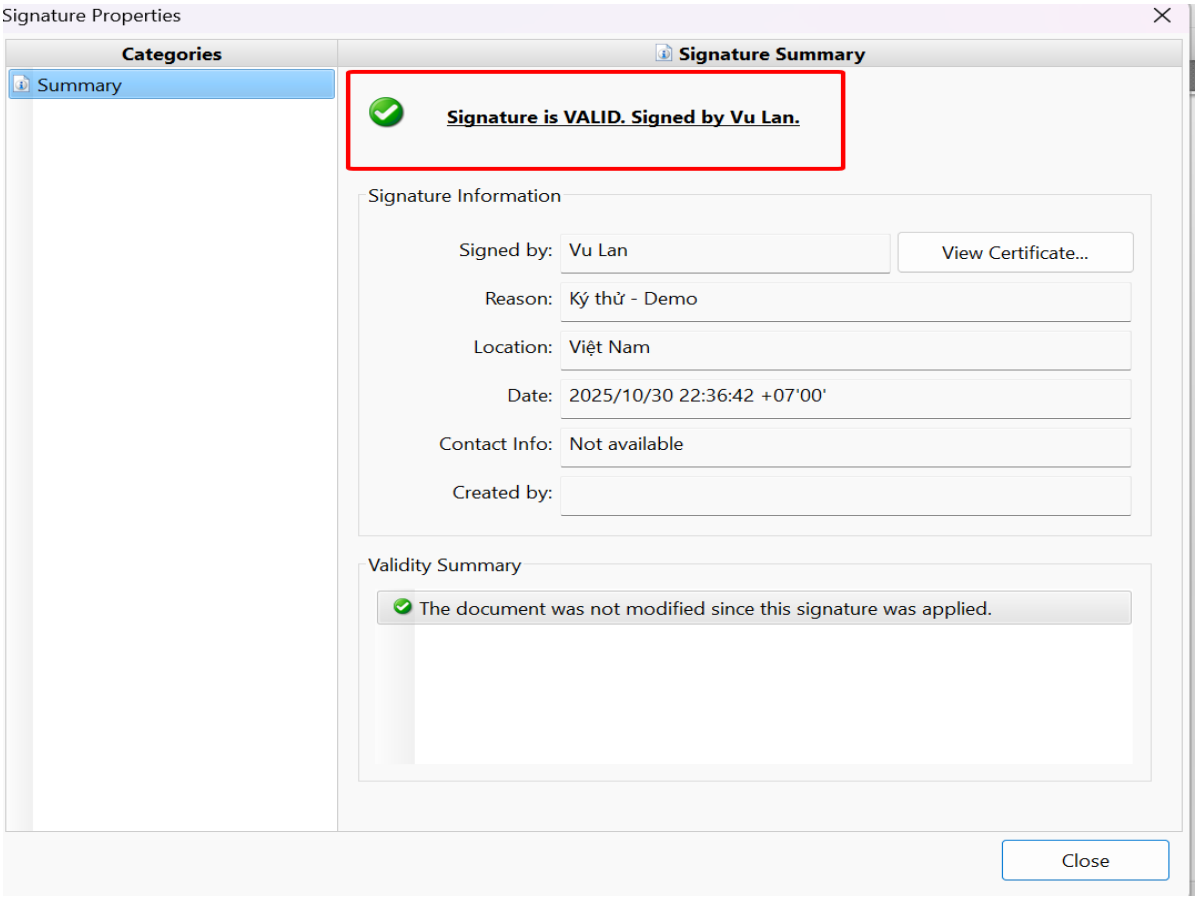
Chạy : dotnet run sign

Kết quả hiển thị:

```
PS E:\chukyso2\PdfSignVerify> cd "E:\chukyso2\PdfSignVerify\PdfSignVerify"
>> dotnet run sign
>>
Using launch settings from E:\chukyso2\PdfSignVerify\PdfSignVerify\Properties\launchSettings.json...
 Đã thêm chữ ký hiển thị vào PDF
 Đã ký số thành công: signed_visible_signed.pdf
 Hoàn tất ký PDF!
```

Ngi ký: V Lân
Ngày ký: 2025-10-30

Chứng chỉ tin cậy:



III. PHÂN TÍCH RỦI RO BẢO MẬT

3.1. Nguy cơ bảo mật

- Rò rỉ khóa riêng (private key): Nếu file signer.pfx bị sao chép, người khác có thể giả mạo chữ ký "Vũ Lân". -> Mất tính xác thực, chữ ký mất giá trị pháp lý.
- Chỉnh sửa sau khi ký: Dữ liệu PDF bị thay đổi sau khi ký, vượt ngoài vùng ByteRange.-> Chữ ký bị vô hiệu, cảnh báo "Document has been altered".
- Không có Timestamp (dấu thời gian): Thời gian ký phụ thuộc vào máy người ký, không có chứng thực thời gian chuẩn.-> Giảm giá trị pháp lý của chữ ký.
- Thuật toán yếu (SHA1, RSA nhỏ): Một số hệ thống cũ dùng thuật toán dễ bị tấn công.-> Có thể giả mạo hoặc phá vỡ tính toàn vẹn.
- Chứng chỉ hết hạn hoặc bị thu hồi: Khi chứng chỉ hết hạn mà không gia hạn hoặc kiểm tra CRL/OCSP-> Chữ ký không còn hợp lệ.

3.2. Giải pháp đề xuất

- Bảo vệ file `signer.pfx` bằng mật khẩu mạnh và lưu trữ ngoại tuyến.
- Sử dụng **Timestamp Authority (TSA)** để chứng thực thời gian ký.

- Chuyển sang **PAdES-LTV (Long-Term Validation)** nếu cần hiệu lực lâu dài.
- Kiểm tra định kỳ CRL/OCSP để phát hiện chứng chỉ thu hồi.
- Dùng thuật toán SHA256 trở lên, khóa ≥ 2048 bit.