**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

**NGUYỄN NGỌC NHUNG**

**ĐOÀN THỊ ÁNH DƯƠNG**

**ĐỒ ÁN MÔN MẬT MÃ HỌC**

**VĂN BẰNG ĐIỆN TỬ**

**SỬ DỤNG CHỮ KÝ SỐ VÀ MÃ QR**

**Electronic Certificate Using Digital Signature And QR Code**

**CỬ NHÂN NGÀNH AN TOÀN THÔNG TIN**

**TP. HỒ CHÍ MINH, 2023**

**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

**NGUYỄN NGỌC NHUNG – 21521248**

**ĐOÀN THỊ ÁNH DƯƠNG – 21521987**

**ĐỒ ÁN MÔN MẬT MÃ HỌC**

**VĂN BẰNG ĐIỆN TỬ**

**SỬ DỤNG CHỮ KÝ SỐ VÀ MÃ QR**

**Electronic Certificate Using Digital Signature And QR Code**

**CỬ NHÂN NGÀNH AN TOÀN THÔNG TIN**

**GIẢNG VIÊN HƯỚNG DẪN**

**NGUYỄN NGỌC TỰ**

**TP. HỒ CHÍ MINH, 2023**

**LỜI CẢM ƠN**

Kính gửi Thầy Nguyễn Ngọc Tự,

Chúng em xin gửi lời cảm ơn chân thành nhất đến Thầy về sự tận tâm và hướng dẫn chúng em nhiệt tình trong môn học Mật mã học. Nhờ sự hỗ trợ của Thầy, chúng em đã không chỉ nắm vững lý thuyết về các thuật toán mã hóa và giải mã mà còn biết cách áp dụng nó vào quá trình thực hiện đồ án. Qua đó, chúng em cũng đã hiểu rõ hơn về quy trình bảo mật thông tin và ý nghĩa của việc bảo vệ dữ liệu.

Sự tận tụy và sự hỗ trợ của Thầy đã tạo nên một môi trường học tập đầy cống hiến. Chúng em cũng xin bày tỏ lòng biết ơn đối với sự động viên và những lời khuyên quý giá từ Thầy trong quá trình làm đồ án. Thầy đã luôn sẵn lòng lắng nghe và giúp đỡ chúng em vượt qua những khó khăn.

Chúng em xin cam đoan sẽ tiếp tục áp dụng những kiến thức đã học từ Thầy vào công việc và cuộc sống hàng ngày. Sự hướng dẫn và đóng góp của Thầy sẽ mãi là nguồn động lực và định hướng cho chúng em trong tương lai.

Trân trọng,

Nguyễn Ngọc Nhung

Đoàn Thị Ánh Dương

**MỤC LỤC**

[Chương 1. MỞ ĐẦU 4](#_Toc138639482)

[Chương 2. PHÂN TÍCH HỆ THỐNG 4](#_Toc138639483)

[2.1. Ngữ cảnh 4](#_Toc138639484)

[2.2. Các bên liên quan 5](#_Toc138639485)

[2.3. Tài sản cần bảo vệ 5](#_Toc138639486)

[2.4. Các tính năng bảo mật cần xây dựng 6](#_Toc138639487)

[Chương 3. GIẢI PHÁP 6](#_Toc138639488)

[3.1. Tổng quan giải pháp 6](#_Toc138639489)

[3.2. Phân tích chi tiết 7](#_Toc138639490)

[3.2.1. Thuật toán Falcon 7](#_Toc138639491)

[3.2.2. Tạo cặp key 8](#_Toc138639492)

[3.2.3. Lưu trữ private key 9](#_Toc138639493)

[3.2.4. Phân phối public key 11](#_Toc138639494)

[3.2.5. Server để phân phối public key 12](#_Toc138639495)

[Chương 4. TRIỂN KHAI 17](#_Toc138639496)

[4.1. Tạo văn bằng từ mẫu PDF 17](#_Toc138639497)

[4.2. Tạo và phân phối key 21](#_Toc138639498)

[4.3. Ký văn bằng 22](#_Toc138639499)

[4.4. Xác thực 25](#_Toc138639500)

**DANH MỤC HÌNH**

[Hình 2.1. Phân tích ngữ cảnh 5](#_Toc138639445)

[Hình 2.2. Các bên liên quan 5](#_Toc138639446)

[Hình 2.3. Tài sản cần bảo vệ 6](#_Toc138639447)

[Hình 2.4. Các tính năng bảo mật cần xây dựng 6](#_Toc138639448)

[Hình 3.1. Tổng quan giải pháp 7](#_Toc138639449)

[Hình 3.2. Thuật toán Falcon 7](#_Toc138639450)

[Hình 3.3. Code tạo cặp key 9](#_Toc138639451)

[Hình 3.4. Code mã hoá và lưu trữ private key 10](#_Toc138639452)

[Hình 3.5. Nội dung file private-key.pem được lưu trữ 10](#_Toc138639453)

[Hình 3.6. Code đọc và giải mã private key 11](#_Toc138639454)

[Hình 3.7. Code lưu trữ public key 12](#_Toc138639455)

[Hình 3.8. Nội dung file public-key.pem được lưu trữ 12](#_Toc138639456)

[Hình 3.9. Truy cập domain nguyenhoangtuanh.id.vn 13](#_Toc138639457)

[Hình 3.10. Nội dung file ec-private-key.pem dùng để tạo văn bằng 13](#_Toc138639458)

[Hình 3.11. Nội dung file nguyenhoangtuanh.id.vn.crt 14](#_Toc138639459)

[Hình 3.12. Code tạo chứng chỉ X509 và server ở localhost port 8000 14](#_Toc138639460)

[Hình 3.13. Thiết lập kết nối TCP, stream ssl, xác thực chứng chỉ X509 và gửi public key 15](#_Toc138639461)

[Hình 3.14. Triển khai server trên Internet 16](#_Toc138639462)

[Hình 3.15. Code kết nối đến server và lấy nội dung public key 16](#_Toc138639463)

[Hình 4.1. Triển khai xác thực giấy chứng nhận tốt nghiệp cho trường đại học UIT 17](#_Toc138639464)

[Hình 4.2. Mẫu PDF để tạo văn bằng 18](#_Toc138639465)

[Hình 4.3. Tạo văn bằng từ mẫu PDF 19](#_Toc138639466)

[Hình 4.4. Văn bằng được tạo 20](#_Toc138639467)

[Hình 4.5. Giao diện dùng để ký giấy chứng nhận 21](#_Toc138639468)

[Hình 4.6. Chỉ định đường dẫn để lưu key 22](#_Toc138639469)

[Hình 4.7. Nhập password dùng để mã hoá private key 22](#_Toc138639470)

[Hình 4.8. Ký văn bằng đã được tạo 23](#_Toc138639471)

[Hình 4.9. Văn bằng sau khi ký và thêm QR Code 24](#_Toc138639472)

[Hình 4.10. Lấy public key trên server local 25](#_Toc138639473)

[Hình 4.11. Lấy public key trên Internet 26](#_Toc138639474)

**TÓM TẮT ĐỒ ÁN**

● Tóm tắt vấn đề nghiên cứu

Trong thời đại kĩ thuật số hiện đại, việc xác thực tính toàn vẹn và tính pháp lý của các văn bằng chứng chỉ là rất quan trọng. Một số văn bằng chứng chỉ có thể bị làm giả như một số hành vi:

- Sửa đổi thông tin: Kẻ gian có thể làm giả văn bằng chứng chỉ bằng cách sửa đổi thông tin trên văn bằng. Ví dụ, họ có thể thay đổi tên, ngành học, điểm số hoặc ngày cấp chứng chỉ để tạo ra một bằng giả mạo.

- Sử dụng chữ ký giả mạo: Kẻ gian có thể làm giả văn bằng chứng chỉ bằng cách tạo ra một chữ ký giả mạo. Họ có thể sao chép chữ ký của người đứng tên trên văn bằng hoặc tạo ra một chữ ký giả mạo để làm cho văn bằng trông chính xác như một văn bằng chính thức.

- Tạo văn bằng giả hoàn toàn: Kẻ gian có thể tạo ra một văn bằng giả hoàn toàn bằng cách sử dụng thiết bị và công nghệ để sao chép mẫu văn bằng chứng chỉ. Họ có thể tạo ra văn bằng giả mà không có sự tham gia hoặc chứng nhận từ bất kỳ tổ chức hoặc cơ quan nào.

- Mua bán văn bằng giả: Kẻ gian có thể mua bán văn bằng giả từ những nguồn không đáng tin cậy hoặc từ những người có kỹ năng làm giả văn bằng. Họ có thể mua văn bằng giả để sử dụng cho mục đích cá nhân hoặc lợi dụng văn bằng giả để xin việc, nâng cao địa vị xã hội hoặc lừa đảo.

Vấn đề nghiên cứu chính trong đồ án này là tăng cường tính bảo mật và tính pháp lý của các văn bằng chứng chỉ thông qua việc áp dụng công nghệ chữ ký điện tử. Chữ ký điện tử không chỉ đảm bảo tính toàn vẹn của dữ liệu, mà còn giúp xác thực nguồn gốc của các văn bằng chứng chỉ, cung cấp sự chứng thực và công nhận pháp lý cho văn bằng, tạo ra sự tin tưởng và hỗ trợ trong các quy trình chứng thực và công nhận văn bằng.

● Hướng tiếp cận

- Sử dụng công nghệ chứng chỉ số và hệ thống PKI: Áp dụng công nghệ chứng chỉ số để xác thực và quản lý chữ ký điện tử trên các văn bằng chứng chỉ. Sử dụng hệ thống PKI để phát hành chứng chỉ, quản lý khóa công khai và đảm bảo nguồn gốc của chữ ký.

- Sử dụng thuật toán mã hóa mạnh: Áp dụng các thuật toán mã hóa mạnh chống máy tính lượng tử được NIST công bố như Dilithium, Falcon để mã hóa chữ ký điện tử và đảm bảo tính bảo mật của thông tin.

- Quản lý và xác thực chứng chỉ: Đảm bảo tính toàn vẹn và xác thực của chứng chỉ sử dụng trong quá trình tạo chữ ký điện tử. Quy trình này bao gồm kiểm tra chứng chỉ không hợp lệ và xác minh nguồn gốc của chứng chỉ.

- Kiểm tra tính toàn vẹn và xác thực của dữ liệu: Sử dụng khóa công khai để giải mã chữ ký, kiểm tra tính toàn vẹn của dữ liệu được ký. Điều này đảm bảo rằng dữ liệu không bị thay đổi sau khi được ký và có thể xác thực tính hợp lệ của chữ ký.

- Sử dụng mã QR chứa các thông tin trên văn bằng, cùng với chữ ký để bên xác thực thuận tiện trong việc theo dõi, đối chiếu văn bằng, chứng chỉ.

● Cách giải quyết vấn đề

- Xác định yêu cầu và mục tiêu của việc áp dụng chữ ký điện tử trên văn bằng chứng chỉ.

- Nghiên cứu và áp dụng các công nghệ chữ ký điện tử phù hợp, như chứng chỉ số và hệ thống PKI.

- Lựa chọn thuật toán mã hóa mạnh và triển khai các biện pháp bảo mật để đảm bảo tính toàn vẹn và tính bảo mật của chữ ký điện tử.

- Xây dựng quy trình quản lý chứng chỉ và xác thực nguồn gốc của chữ ký điện tử.

- Thiết kế và triển khai hệ thống chữ ký điện tử trên văn bằng chứng chỉ.

- Tiến hành kiểm tra và đánh giá tính hiệu quả và tính bảo mật của hệ thống chữ ký điện tử.

● Kết quả đạt được

- Xác thực danh tính: Chữ ký điện tử giúp xác thực danh tính của người ký văn bằng chứng chỉ, đảm bảo tính chính xác và đáng tin cậy của thông tin.

- Tính toàn vẹn: Chữ ký điện tử đảm bảo tính toàn vẹn của văn bằng chứng chỉ, ngăn chặn việc giả mạo hoặc thay đổi thông tin.

- Tính bảo mật: Áp dụng thuật toán chống máy tính lượng tử Falcon, hệ thống chữ ký điện tử đạt được tính bảo mật cao và khả năng chống lại các cuộc tấn công từ máy tính lượng tử.

- Quản lý chứng chỉ hiệu quả: Hệ thống quản lý chứng chỉ đảm bảo tính toàn vẹn và xác thực của chứng chỉ sử dụng trong quá trình tạo chữ ký điện tử.

# MỞ ĐẦU

Chữ ký điện tử trên các văn bằng chứng chỉ là một vấn đề quan trọng trong thời đại công nghệ số hiện nay. Việc chuyển đổi từ văn bằng chứng chỉ truyền thống sang văn bằng điện tử mang lại nhiều lợi ích, như tính tiện lợi, tiết kiệm thời gian và quản lý dễ dàng. Tuy nhiên, để đảm bảo tính toàn vẹn và xác thực của văn bằng điện tử, chữ ký điện tử đóng vai trò quan trọng. Vì vậy, chọn đề tài này nhằm tìm hiểu và nghiên cứu về cách áp dụng chữ ký điện tử trong lĩnh vực văn bằng chứng chỉ để đáp ứng nhu cầu của thế giới công nghệ hiện đại.

Mục đích của nghiên cứu là tìm hiểu và áp dụng chữ ký điện tử để xác thực và bảo vệ tính toàn vẹn của văn bằng chứng chỉ. Nghiên cứu nhằm xây dựng hệ thống chữ ký điện tử hiệu quả và bảo mật, từ đó đảm bảo tính tin cậy của thông tin trong văn bằng chứng chỉ điện tử.

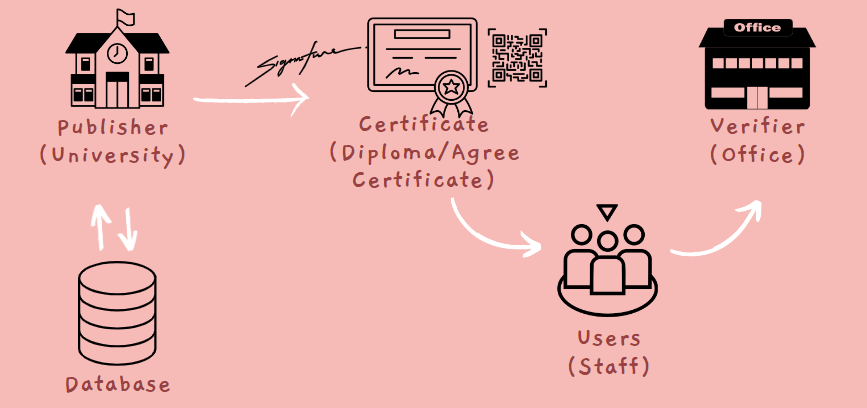
Đối tượng nghiên cứu của đề tài là các văn bằng chứng chỉ điện tử được cấp bởi các tổ chức, trường học hoặc cơ quan chứng nhận. Nghiên cứu tập trung vào việc áp dụng chữ ký điện tử để xác thực và bảo vệ tính toàn vẹn của các văn bằng chứng chỉ này.

Phạm vi nghiên cứu bao gồm các khía cạnh liên quan đến chữ ký điện tử trên văn bằng chứng chỉ, bao gồm các công nghệ và thuật toán sử dụng trong quá trình tạo chữ ký, quản lý chứng chỉ, và xác thực tính toàn vẹn của dữ liệu. Nghiên cứu sẽ tập trung vào các hướng tiếp cận và giải pháp hiện có để áp dụng chữ ký điện tử vào lĩnh vực văn bằng chứng chỉ, đồng thời đề xuất cách giải quyết các thách thức và vấn đề có thể phát sinh trong quá trình triển khai chữ ký điện tử trên văn bằng chứng chỉ.

# PHÂN TÍCH HỆ THỐNG

## 2.1. Ngữ cảnh

Một trường đại học cấp bằng tốt nghiệp cho các sinh viên của mình. Khi xin việc, nhà tuyển dụng yêu cầu sinh viên cung cấp bằng tốt nghiệp. Việc xác minh tính chính xác và nguồn gốc của văn bằng là rất quan trọng để đảm bảo rằng nhà tuyển dụng nhận được thông tin chính xác về quá trình học tập và thành tích của sinh viên. Trong thực tế, có rất nhiều văn bằng giả được tạo ra hiện nay. Điều này tạo ra nhu cầu cần có một phương pháp để nhà tuyển dụng có thể xác minh tính chính xác và nguồn gốc của văn bằng.



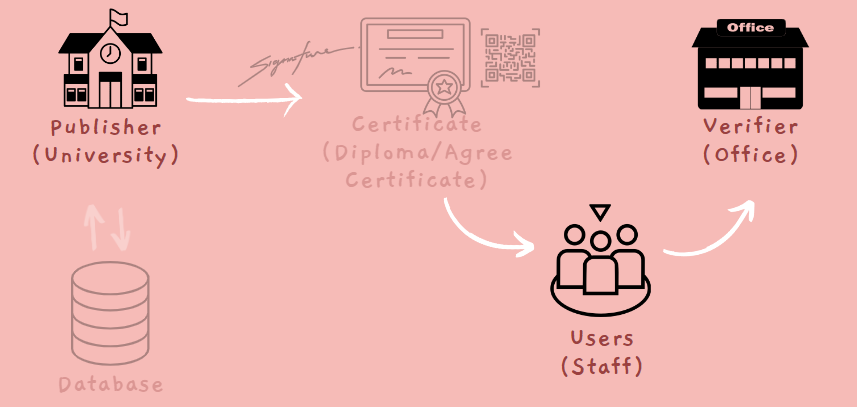
Hình 2.1. Phân tích ngữ cảnh

## 2.2. Các bên liên quan

- Trường đại học: Là tổ chức cấp bằng và cung cấp thông tin về học tập và thành tích của sinh viên. Trường đại học có trách nhiệm cung cấp thông tin chính xác về bằng cấp và quá trình học tập của sinh viên.

- Sinh viên: Là người muốn xin việc và cung cấp bằng tốt nghiệp và các tài liệu liên quan. Sinh viên phải cung cấp thông tin chính xác về quá trình học tập và văn bằng của mình để nhà tuyển dụng xác minh.

- Nhà tuyển dụng, cơ quan: Là các tổ chức, doanh nghiệp, hoặc cơ quan tuyển dụng sinh viên. Nhà tuyển dụng cần xác minh tính chính xác và nguồn gốc của văn bằng để đảm bảo độ tin cậy của thông tin hồ sơ ứng viên.

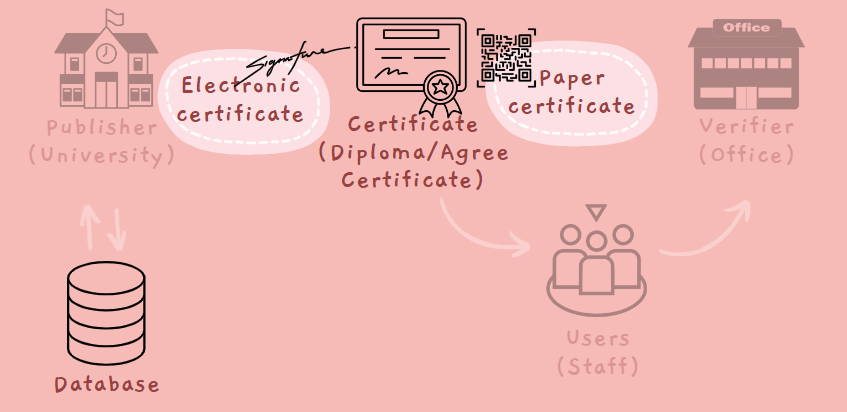


Hình 2.2. Các bên liên quan

## 2.3. Tài sản cần bảo vệ

- Database lưu trữ các văn bằng của trường: Đây là nơi lưu trữ thông tin về văn bằng của sinh viên, bao gồm thông tin cá nhân, chương trình học, và kết quả học tập.

- Văn bằng đã cung cấp cho sinh viên: Văn bằng được cung cấp ở hai dạng là bản mềm và bản cứng. Bản mềm thường là phiên bản điện tử của văn bằng, trong khi bản cứng là phiên bản giấy hoặc tài liệu in.



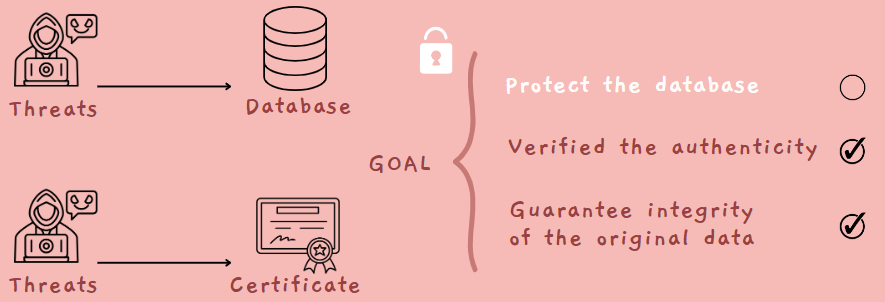
Hình 2.3. Tài sản cần bảo vệ

## 2.4. Các tính năng bảo mật cần xây dựng

- Bảo vệ database khỏi sự xâm nhập, tấn công từ bên ngoài.

- Đảm bảo nguồn gốc cho các văn bằng.

- Đảm bảo nội dung các văn bằng không bị chỉnh sửa.



Hình 2.4. Các tính năng bảo mật cần xây dựng

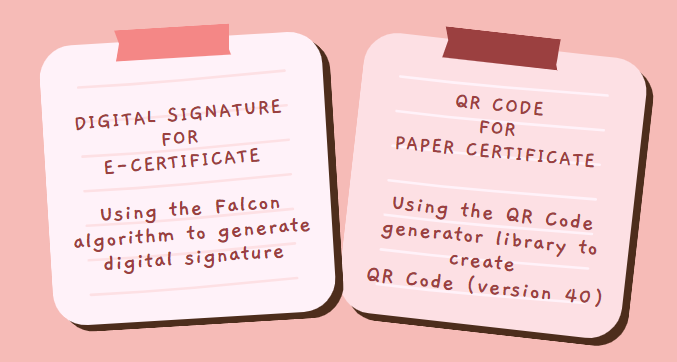
Nhóm chúng em chỉ đi phân tích giải pháp cho các tính năng 2 và 3.

# GIẢI PHÁP

## 3.1. Tổng quan giải pháp

- Sử dụng thuật toán Falcon để ký và xác thực chữ ký số: Falcon là một thuật toán chữ ký số có khả năng đảm bảo tính bảo mật và tính toàn vẹn của chữ ký. Sử dụng thuật toán Falcon để tạo ra chữ ký số cho văn bằng, đảm bảo rằng chữ ký không thể bị giả mạo và chỉ có thể được tạo ra bởi cơ quan có thẩm quyền.

- Bổ sung mã QR vào bản cứng để hiển thị thông tin sinh viên và chữ ký số: Bằng cách bổ sung mã QR vào bản cứng của văn bằng, người nhà tuyển dụng có thể dễ dàng quét mã QR để truy cập thông tin của sinh viên. Mã QR có thể chứa thông tin cá nhân, thông tin về văn bằng và chữ ký số được tạo bởi thuật toán Falcon. Nhờ có mã QR, nhà tuyển dụng có thể kiểm tra tính chính xác và nguồn gốc của văn bằng một cách nhanh chóng và thuận tiện.



Hình 3.1. Tổng quan giải pháp

## 3.2. Phân tích chi tiết

### 3.2.1. Thuật toán Falcon

A diagram of a flowchart

Description automatically generated with low confidence

Hình 3.2. Thuật toán Falcon

Trong lược đồ ký số Falcon hậu lượng tử, đầu tiên sẽ sử dụng lý thuyết Khung để xây dựng cho lược đồ ký số là dựa trên lưới (Khung GPV). Một khung này có thể được mô tả gồm các thành phần như sau:

- Khóa công khai: là một ma trận có hạng đầy đủ A (m > n) tạo ra một lưới q-ary Λ.

- Khóa bí mật: là một ma trận B tạo ra một lưới trực giao , ở đây là ký hiệu lưới trực giao của lưới Λ modulo q và lưới trực giao thỏa mãn tính chất: Với mọi x ∈ Λ và y ∈ , khi đó thỏa mãn điều kiện ⟨x, y⟩ = 0 mod q. Tương đương, các hàng của A và B trực giao thỏa mãn: B x At = 0.

- Thực hiện ký cho thông điệp m, chữ ký cho m là một giá trị nguyên ngắn s sao cho sAt = H(m), trong đó H : {0,1} → là một hàm băm. Khi đó, cho A, việc xác thực tính hợp lệ của chữ ký s được thực hiện đơn bằng cách kiểm tra s có là một giá trị nguyên ngắn (SIS) và thỏa mãn điều kiện sAt = H(m).

- Xác thực chữ ký: Quá trình tính toán kiểm tra tính hợp lệ của chữ ký có phần phức tạp hơn. Điều này, được thực hiện như sau:

(1) Đầu tiên, người dùng phải tính giá trị tiền ảnh C0 thỏa mãn C0At = H(m). Điều này hoàn toàn thực hiện được nhờ các công cụ tính toán đại số tuyến tính, bởi vì C0 không yêu cầu bắt buộc phải là ngắn và m ≥ n;

(2) Sau đó, B được sử dụng để tính vectơ đóng trực giao v ∈ gần với C0.Tính hợp lệ của chữ ký được xác định bằng s = c0 – v. Bởi vì, khi c0 và v đủ gần nhau (c0 – v đủ nhỏ), thì

sAt = c0At - vAt = c - 0 = H(m) (1)

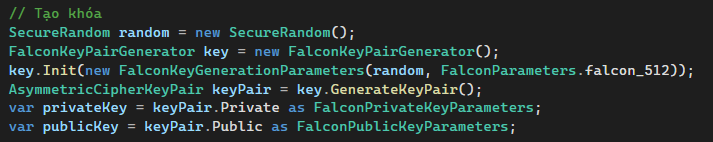
Suy ra, s là ngắn. Điều này, cho thấy với lược đồ chữ ký Falcon hướng tới ưu điểm là chữ ký phải đảm bảo là ngắn.

### 3.2.2. Tạo cặp key

- Sử dụng thuật toán Falcon, tạo cặp key gồm public key (khóa công khai) và private key (khóa bí mật).

- Key được tạo ngẫu nhiên với độ dài 512 bit, tuân theo chuẩn của thuật toán Falcon.

- Private key và pubic key sẽ được tạo 1 lần và lưu trữ trong hệ thống để tái sử dụng cho việc ký nhiều văn bằng. Nếu làm mất private key hoặc public key, người dùng sẽ phải thực hiện tạo lại private key và public key từ đầu.



Hình 3.3. Code tạo cặp key

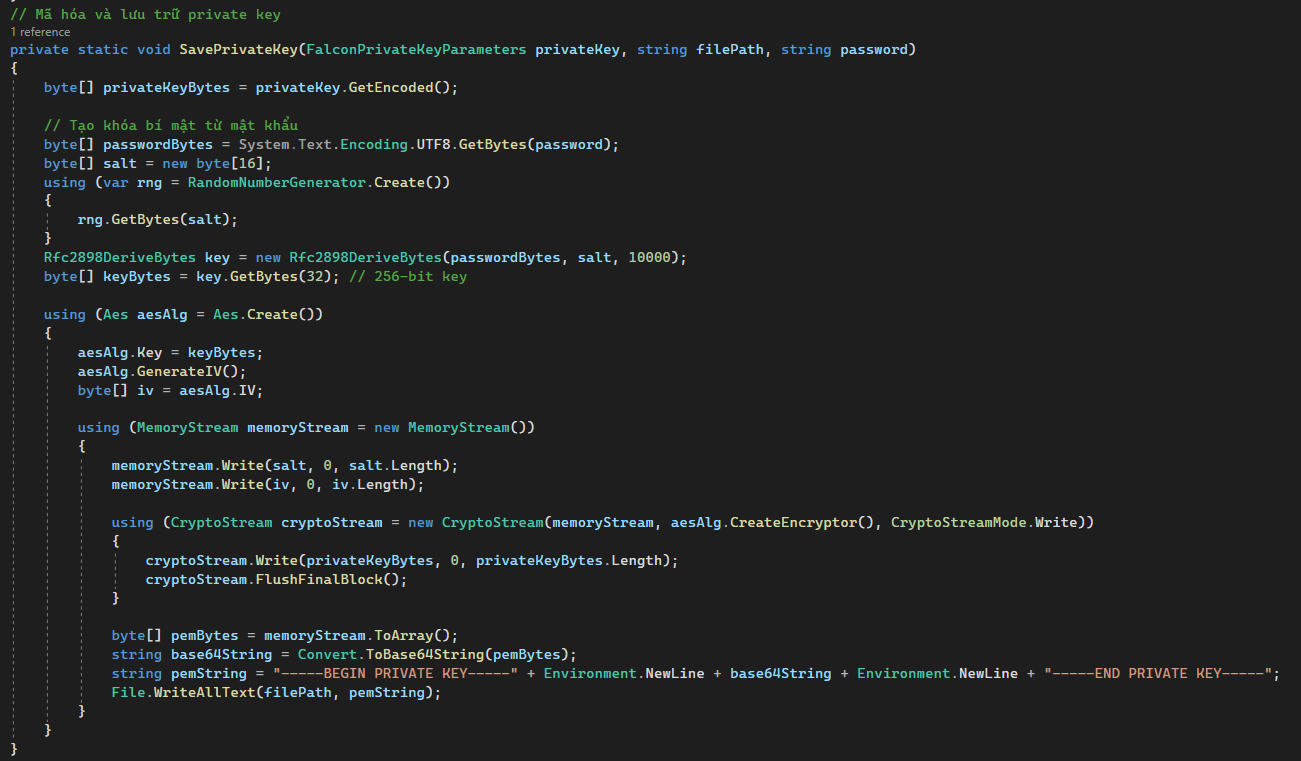
### 3.2.3. Lưu trữ private key

- Private key (khóa bí mật) là thông tin quan trọng và phải được bảo mật một cách cẩn thận.

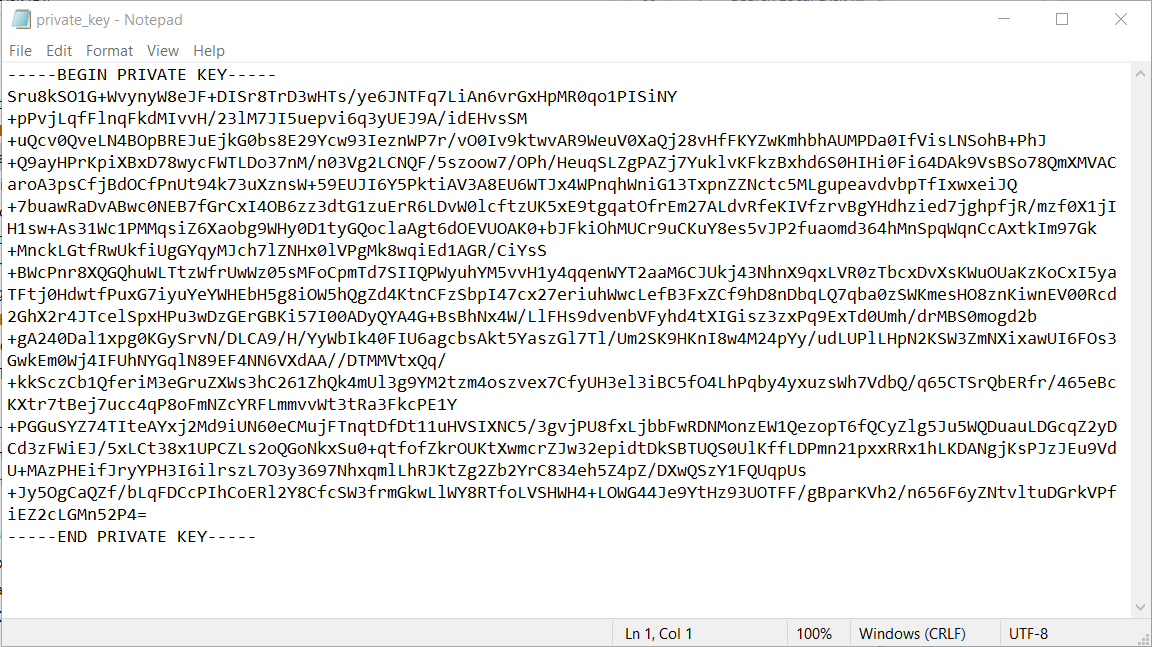
- Một mảng byte salt có độ dài 16 byte được tạo ngẫu nhiên bằng cách sử dụng lớp RandomNumberGenerator.

- Sử dụng Rfc2898DeriveBytes để tạo ra một khóa (AES-key) dựa trên mật khẩu (password) và salt đã được cung cấp. Trong đó, mật khẩu do người dùng nhập vào, mật khẩu này sẽ không được lưu lại trong hệ thống mà người dùng bắt buộc phải ghi nhớ. Salt là mảng byte đã được random trước đó. Chương trình sẽ tiến hành tạo khoá AES dựa trên số lần băm là 10000 lần.

- Private key sẽ được mã hoá bằng thuật toán AES với khoá đã tạo ở trên và iv được random. Sau đó các thông tin về salt, iv, private key sau khi mã hoá sẽ được chuyển sang dạng base64 và ghi vào file private-key.pem. File này được lưu ở trong thư mục do người dùng chỉ định.



Hình 3.4. Code mã hoá và lưu trữ private key



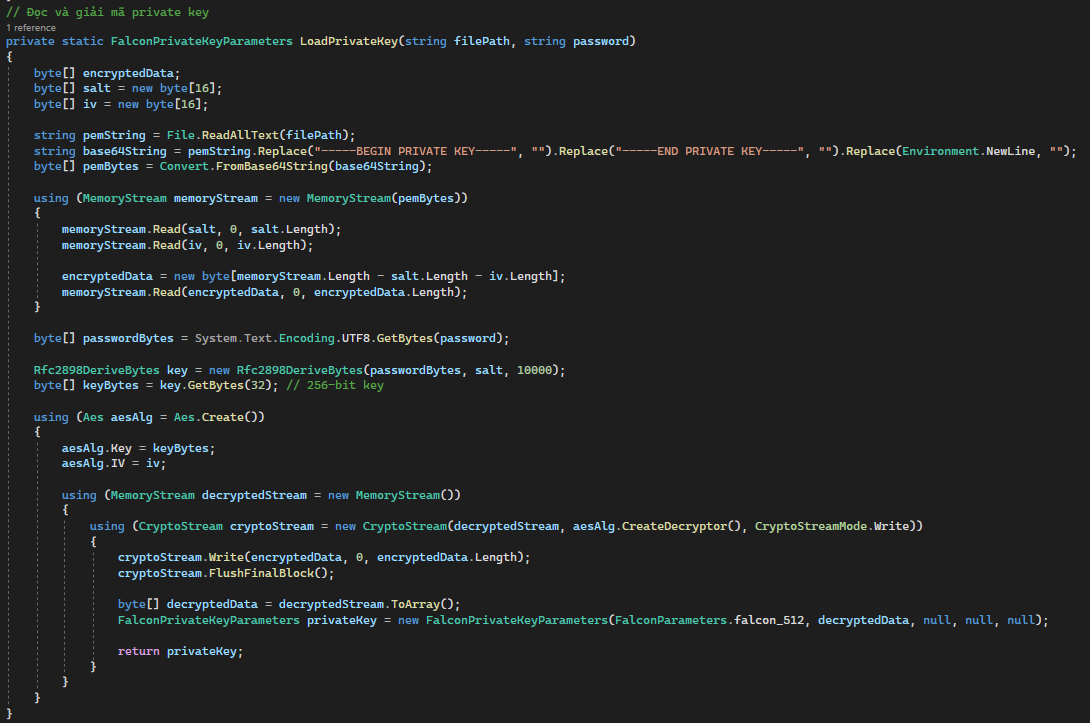
Hình 3.5. Nội dung file private-key.pem được lưu trữ

- Khi muốn sử dụng public key để ký, người dùng sẽ phải load public key lên từ thư mục đã lưu trước đó.

- Tiến hành chuyển dữ liệu từ base64 thành mảng byte, lấy dữ liệu cho salt, iv, và private key đã mã hoá.

- Dựa trên mật khẩu người dùng cung cấp để giải mã. Mật khẩu này chính là mật khẩu đã được dùng để tạo privatekey. Nếu mật khẩu người dùng cung cấp không trùng khớp, private key được giải mã sẽ không chính xác.

- Trả về một đối tượng FalconPrivateKeyParameters được khởi tạo bằng mảng byte private key đã được giải mã.

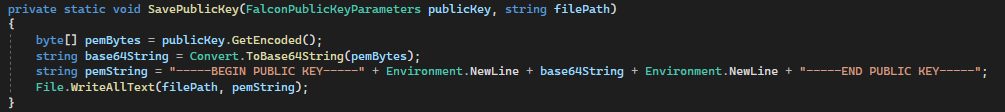


Hình 3.6. Code đọc và giải mã private key

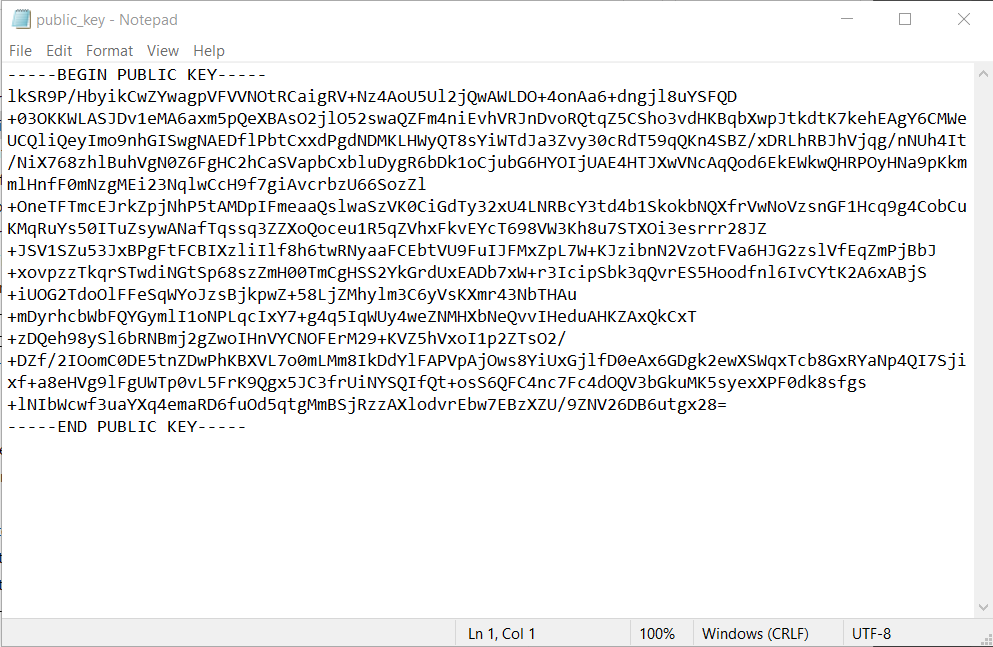
### 3.2.4. Phân phối public key

- Public key (khoá công khai) được phân phối cho các bên liên quan, bao gồm cả sinh viên và nhà tuyển dụng.

- Public key sẽ được chuyển thành định dạng base64 và lưu trong file public-key.pem, file này nằm chung thư mục với private key.



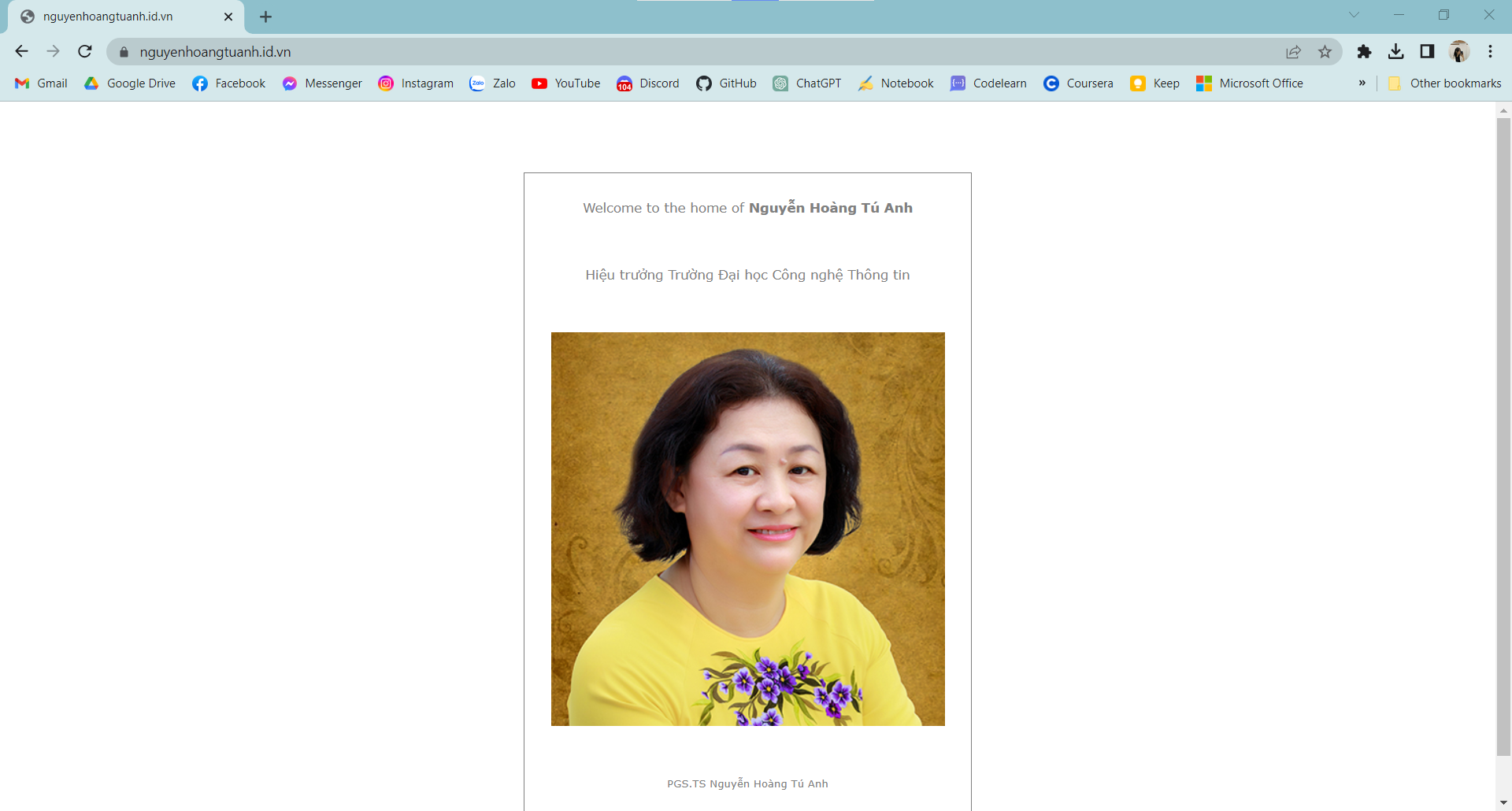
Hình 3.7. Code lưu trữ public key



Hình 3.8. Nội dung file public-key.pem được lưu trữ

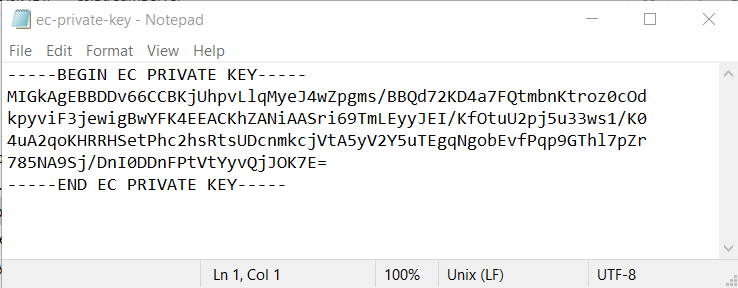
### 3.2.5. Server để phân phối public key

- Đăng ký 1 domain và tạo web hosting cho domain đó. Ở đây, nhóm chúng em đã đăng ký domain nguyenhoangtuanh.id.vn.



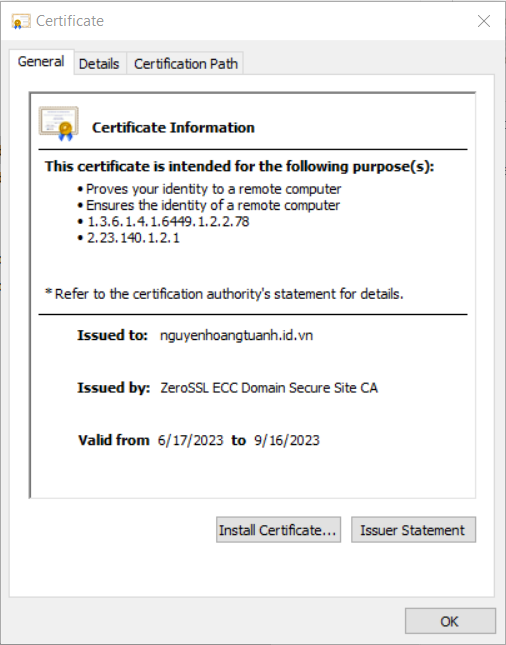
Hình 3.9. Truy cập domain nguyenhoangtuanh.id.vn

- Dùng openssl để tạo file .key và .csr



Hình 3.10. Nội dung file ec-private-key.pem dùng để tạo văn bằng

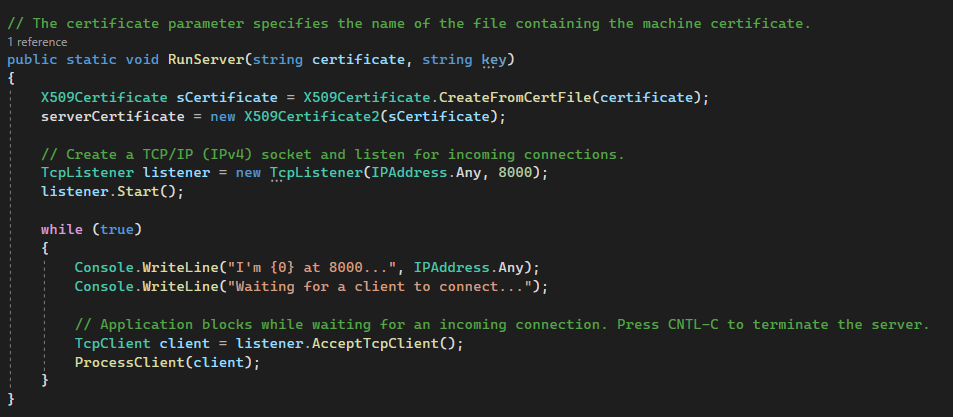
- Dùng Zerossl để tạo file .crt từ file .key và .csr



Hình 3.11. Nội dung file nguyenhoangtuanh.id.vn.crt

- Sử dụng openssl để tạo file .pfx

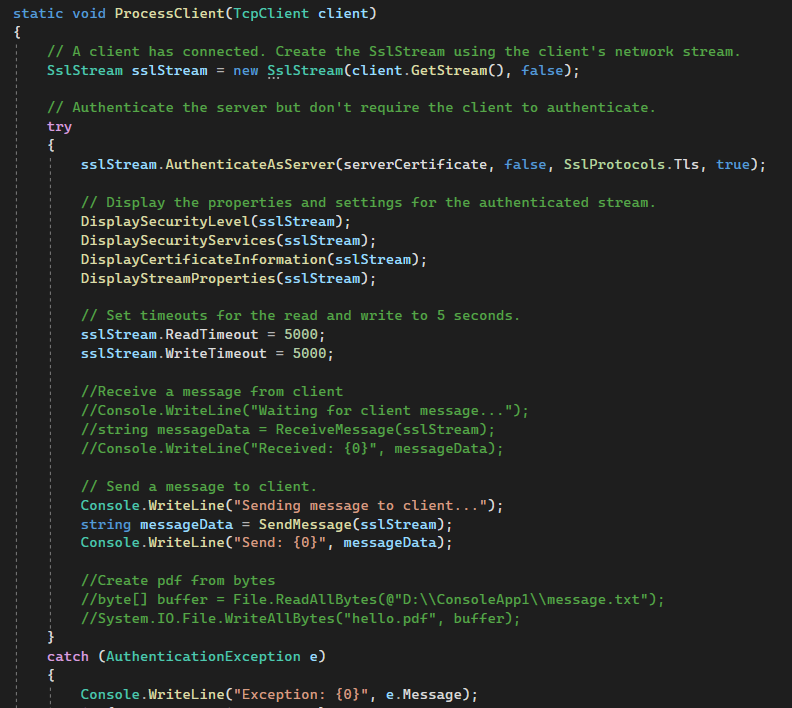
- Tạo một server ở localhost port 8000 và tạo văn bằng từ các file đã tạo trước đó.



Hình 3.12. Code tạo chứng chỉ X509 và server ở localhost port 8000

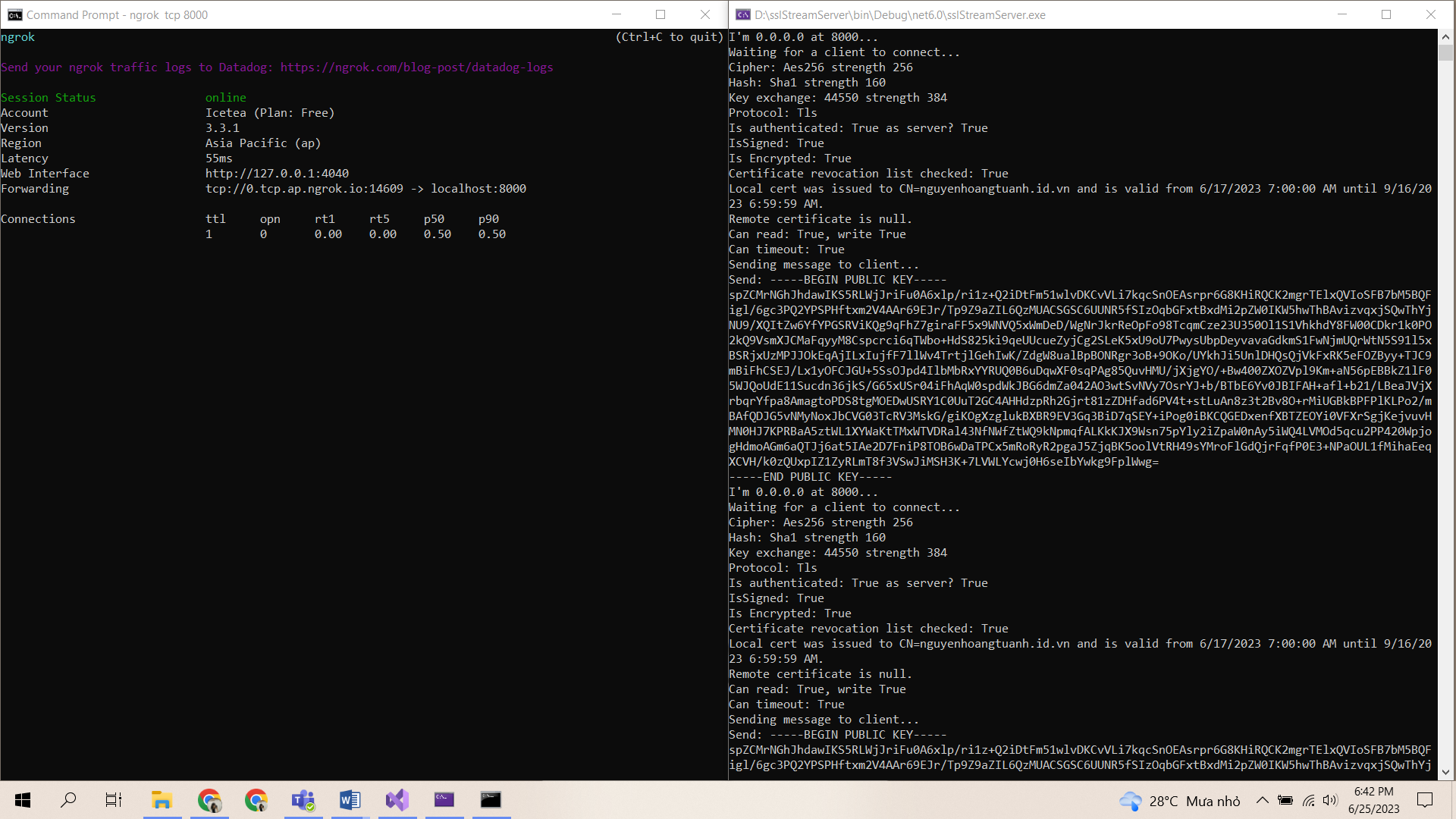
- Khi client kết nối tới server thì thiết lập một stream ssl, tiến hành xác thực chứng chỉ X509 ở phía server và hiển thị các thông tin xác thực lên console.

- Sau khi quá trình xác thực thành công, server sẽ lấy dữ liệu từ file public-key.pem là file lưu public key. Server gửi dữ liệu đến client và quay lại chờ kết nối từ các client khác.



Hình 3.13. Thiết lập kết nối TCP, stream ssl, xác thực chứng chỉ X509 và gửi public key

- Vì server được triển khai trên local, nên để các client khác có thể truy cập được, chúng em dùng ngrok để tạo một liên kết từ địa chỉ private thành một địa chỉ public trên internet.



Hình 3.14. Triển khai server trên Internet

- Về phía client, sau khi kết nối đến server cũng sẽ thiết lập một stream ssl, tiến hành xác thực ở phía client và nhận dữ liệu public key, Chương trình thực hiện chuyển dữ liệu từ base64 thành mảng byte và trả về đối tượng FalconPublicKeyParameters.



Hình 3.15. Code kết nối đến server và lấy nội dung public key

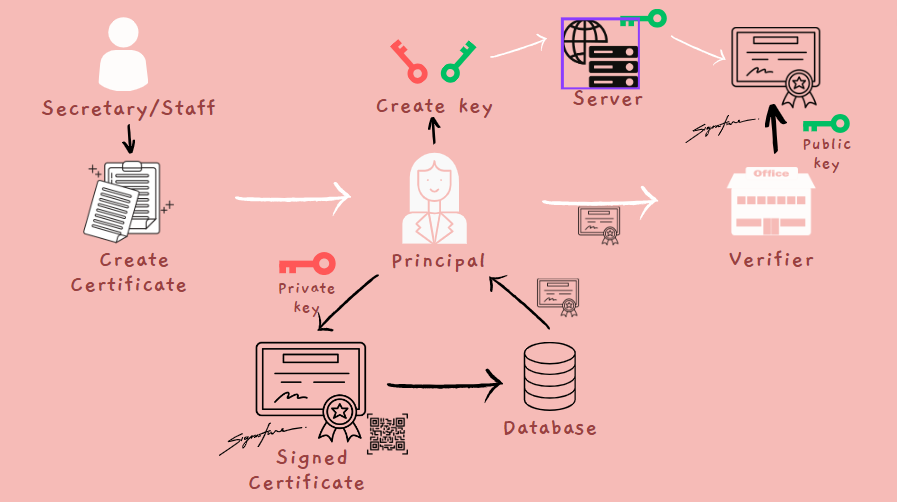
# TRIỂN KHAI

Triển khai mô hình tạo và xác thực giấy chứng nhận tốt nghiệp cho trường đại học UIT, người ký giấy chứng nhận tốt nghiệp là PGS.TS Nguyễn Hoàng Tú Anh.

- Một nhân viên sẽ tiến hành tạo giấy chứng nhận từ một mẫu PDF và dữ liệu của sinh viên.

- Giấy chứng nhận sau khi tạo xong sẽ chuyển cho hiệu trưởng là cô Tú Anh để ký. Để có thể ký được, trước tiên cô Tú Anh phải tạo một cặp key và lưu lại key. Sau khi đã tạo key, cô Tú Anh sẽ dùng private key của mình để ký giấy chứng nhận và lưu nó vào database. Giấy chứng nhận có thể được lấy ra từ database và chuyển đến nơi cần xác nhận.

- Đồng thời, public key cũng sẽ được đưa lên server để những ai muốn xác nhận có thể kết nối tới server và lấy public key.



Hình 4.1. Triển khai xác thực giấy chứng nhận tốt nghiệp cho trường đại học UIT

## 4.1. Tạo văn bằng từ mẫu PDF

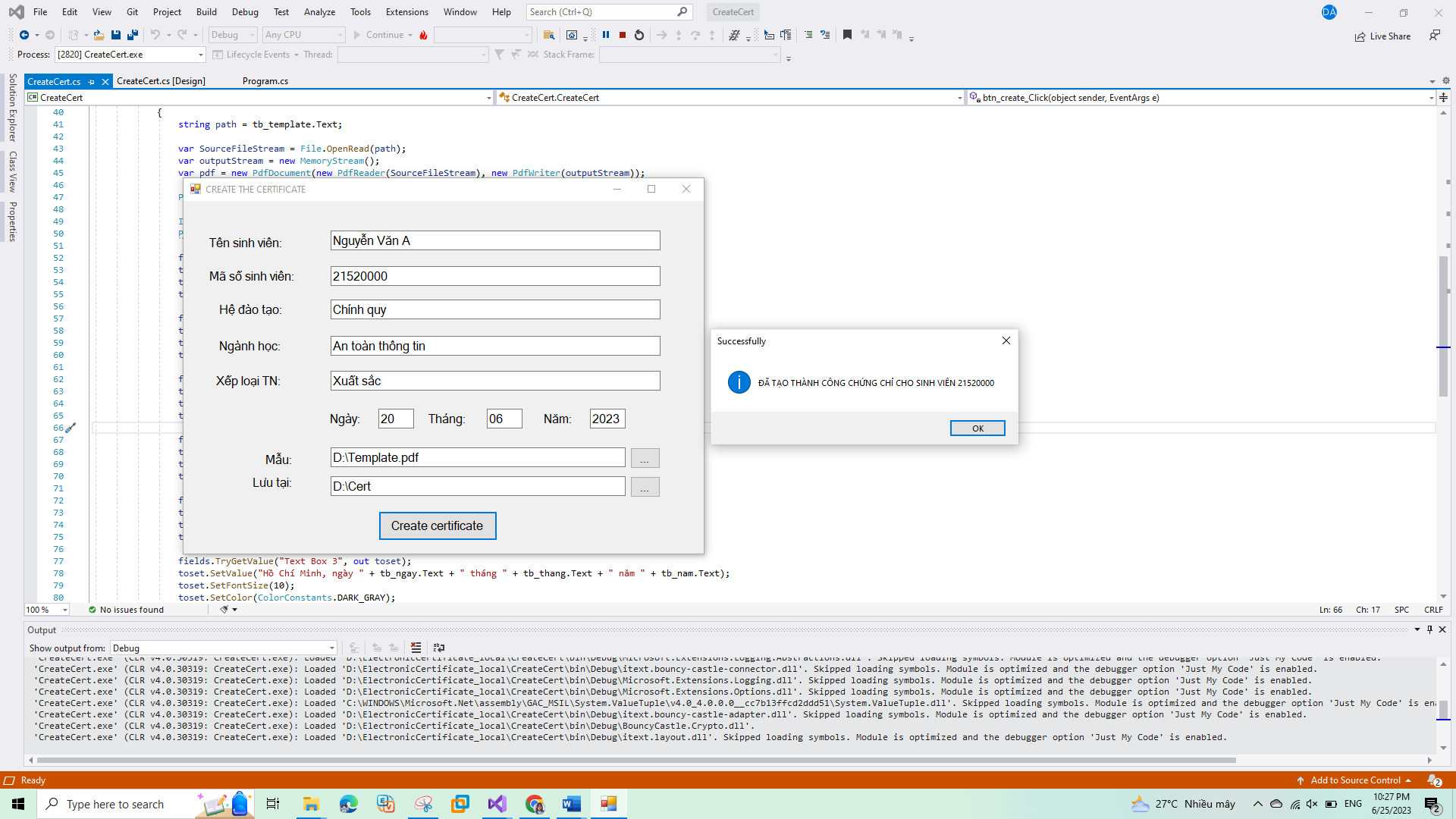
- Mẫu PDF để tạo văn bằng:

A picture containing text, screenshot

Description automatically generated

Hình 4.2. Mẫu PDF để tạo văn bằng

- Tạo văn bằng từ mẫu này:



Hình 4.3. Tạo văn bằng từ mẫu PDF

- Văn bằng được tạo:

A picture containing text, screenshot, design

Description automatically generated

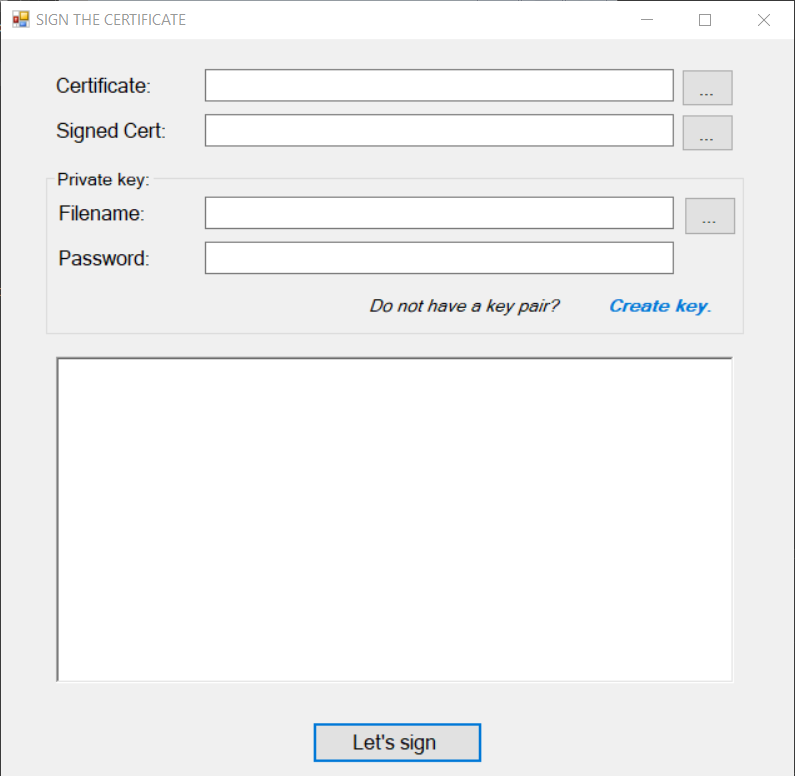
Hình 4.4. Văn bằng được tạo

- Mô tả:

Sử dụng Windows Forms C# và sử dụng thư viện iText để tạo và điền dữ liệu vào các form field trong tệp PDF mẫu. Trong quá trình xử lý, ứng dụng sử dụng lớp PdfDocument của iText để đọc tệp PDF mẫu và tạo tệp PDF kết quả. Lớp PdfAcroForm được sử dụng để truy cập và điền dữ liệu vào các trường form trong tệp PDF. Các trường form được truy cập thông qua phương thức GetAllFormFields(), sau đó dữ liệu được gán vào các trường form bằng cách sử dụng phương thức SetValue().Cuối cùng, tệp PDF kết quả được lưu trữ dưới dạng một mảng byte và được ghi vào đường dẫn được chỉ định.

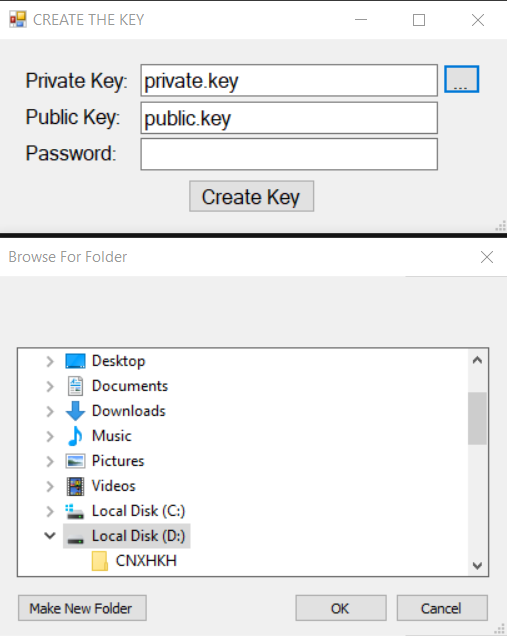
## 4.2. Tạo và phân phối key

- Để có thể ký văn bằng, trước tiên phải có cặp key (private key và public key tương ứng), nhấn vào Create key để tạo key.



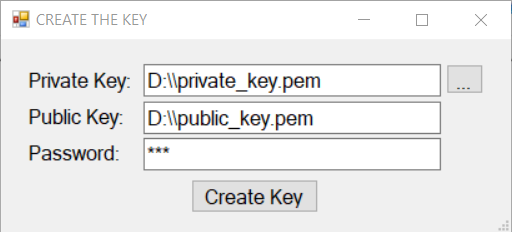
Hình 4.5. Giao diện dùng để ký giấy chứng nhận

- Chỉ định đường dẫn để lưu key.

****

Hình 4.6. Chỉ định đường dẫn để lưu key

- Chọn một password và nhập vào chương trình, người dùng cần ghi nhớ password đã nhập.



Hình 4.7. Nhập password dùng để mã hoá private key

- Nhấn Create Key để tiến hành tạo key. Sau khi tạo key xong, người dùng có thể dùng key để ký các văn bằng.

## 4.3. Ký văn bằng

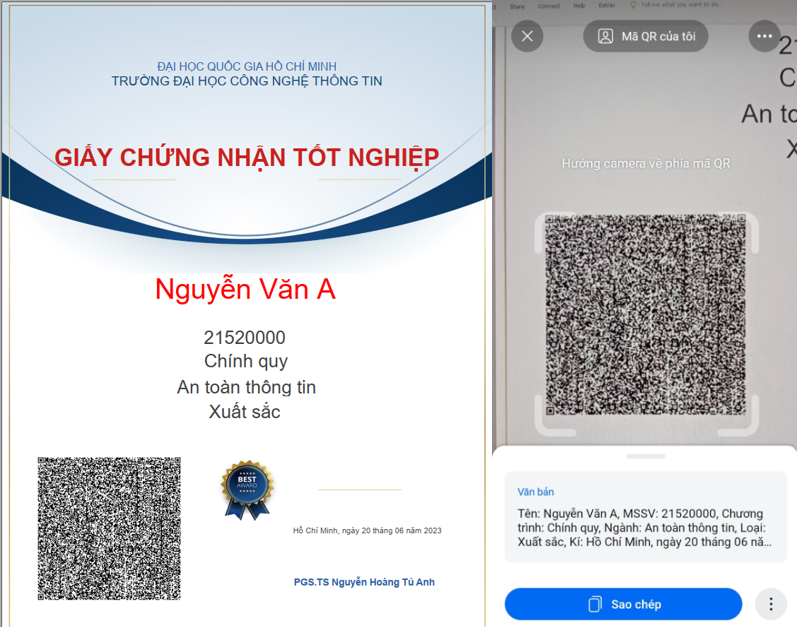
- Ký văn bằng đã được tạo:

A picture containing text, electronics, screenshot, software

Description automatically generated

Hình 4.8. Ký văn bằng đã được tạo

- Văn bằng sau khi thêm chữ ký và QR code:



Hình 4.9. Văn bằng sau khi ký và thêm QR Code

- Mô tả:

+ Sử dụng Windows Forms ngôn ngữ lập trình C# và sử dụng thư viện iText để lấy thông tin cần ký, và ghi thông tin chữ ký sau khi ký từ các thông tin của văn bằng, sử dụng Bouncy Castle để ký các thông tin của văn bằng sử dụng Private key Falcon từ file PEM cùng với password, và thư viện Net.Codecrete.QrCodeGenerator để hỗ trợ tạo QR version 40 chứa các thông tin trên văn bằng và chữ ký của các thông tin trên (hỗ trợ bản cứng cho văn bằng).

+ Đầu tiên, ứng dụng cho phép người dùng chọn tệp PDF văn bằng, tệp Private key và thư mục đích để lưu tệp PDF đã ký. Sau đó, ứng dụng sử dụng thư viện iText để đọc thông tin từ tệp PDF văn bằng. Các form field trong tệp PDF được truy cập bằng cách sử dụng lớp PdfAcroForm và phương thức GetAllFormFields(). Dữ liệu từ các trường form được sử dụng để tạo chữ ký.

+ Tiếp theo, ứng dụng sử dụng thư viện Bouncy Castle để đọc và giải mã Private key từ tệp PEM. Sau khi có chữ ký và khóa riêng, ứng dụng sử dụng lớp FalconSigner từ thư viện Bouncy Castle để tạo chữ ký. Dữ liệu cần ký là một chuỗi được mã hóa từ các trường form trong tệp PDF văn bằng. Sau khi có chữ ký, ứng dụng sử dụng thư viện Net.Codecrete.QrCodeGenerator để tạo mã QR từ các thông tin trong văn bằng. Cuối cùng, ứng dụng sử dụng thư viện iText để chèn chữ ký và mã QR vào tệp PDF văn bằng. Tệp PDF đã ký được lưu trữ trong thư mục đích được chỉ định.

## 4.4. Xác thực

- Public key được lấy từ server triển khai trên mạng local:

A screenshot of a computer

Description automatically generated

Hình 4.10. Lấy public key trên server local

- Public key được lấy từ server triển khai trên mạng Internet:

A screenshot of a computer

Description automatically generated

Hình 4.11. Lấy public key trên Internet

**TÀI LIỆU THAM KHẢO**

1. Ahmed, H. A., & Jang, J. W. (2018, January). Document certificate authentication system using digitally signed QR code tag. In Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication (pp. 1-5).

2. Arief, A. T., Wirawan, W., & Suprapto, Y. K. (2019, August). Authentication of printed document using quick response (QR) code. In 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA) (pp. 228-233). IEEE.

3. Sintyaningrum, D. E., & Ashar, M. (2021, October). The Encryption of Electronic Professional Certificate by Using Digital Signature and QR Code. In 2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE) (pp. 19-24). IEEE.

**PHÂN CÔNG CÔNG VIỆC**

|  |  |
| --- | --- |
| Phân tích hệ thống | Nhung & Dương |
| Tạo văn bằng | Dương |
| Tạo key, bảo mật private key, phân phối public key | Nhung |
| Server phân phối public key | Nhung |
| Ký văn bằng | Dương |
| Xác thực văn bằng | Dương |
| Trình bày báo cáo đồ án | Nhung |