**TRƯỜNG ĐẠI HỌC NÔNG LÂM THÀNH PHỐ HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**Môn: An toàn thông tin**

**Tên đề tài:** **Digital Signature**

Nhóm sinh viên:

19130206 Nguyễn Lê Thành

19130120 Cao Huy Tấn Lộc

19130029 Nguyễn Hữu Đạo

**Ngày 03 Tháng 01 Năm 2023**

MỤC LỤC

[I. GIỚI THIỆU: 2](#_Toc123672770)

[II. CÁC PHẦN CHÍNH: 3](#_Toc123672771)

[1. Work Flow: 3](#_Toc123672772)

[2. Tool ký 4](#_Toc123672773)

[a) Các bước kết nối: 4](#_Toc123672774)

[b) Màn hình đăng nhập: 4](#_Toc123672775)

[d) Màn hình tạo key pair và certificate: 4](#_Toc123672776)

[e) Màn hình ký hóa đơn PDF: 4](#_Toc123672777)

[3. Chức năng thanh toán xác thực người dùng trên website: 4](#_Toc123672778)

[a) Trình tự xác thực 4](#_Toc123672779)

[b) Màn hình tạo certificate và public key 4](#_Toc123672780)

[c) Màn hình quản lý certificate và public key 4](#_Toc123672781)

[III. TÀI LIỆU THAM KHẢO: 4](#_Toc123672782)

# I. GIỚI THIỆU:

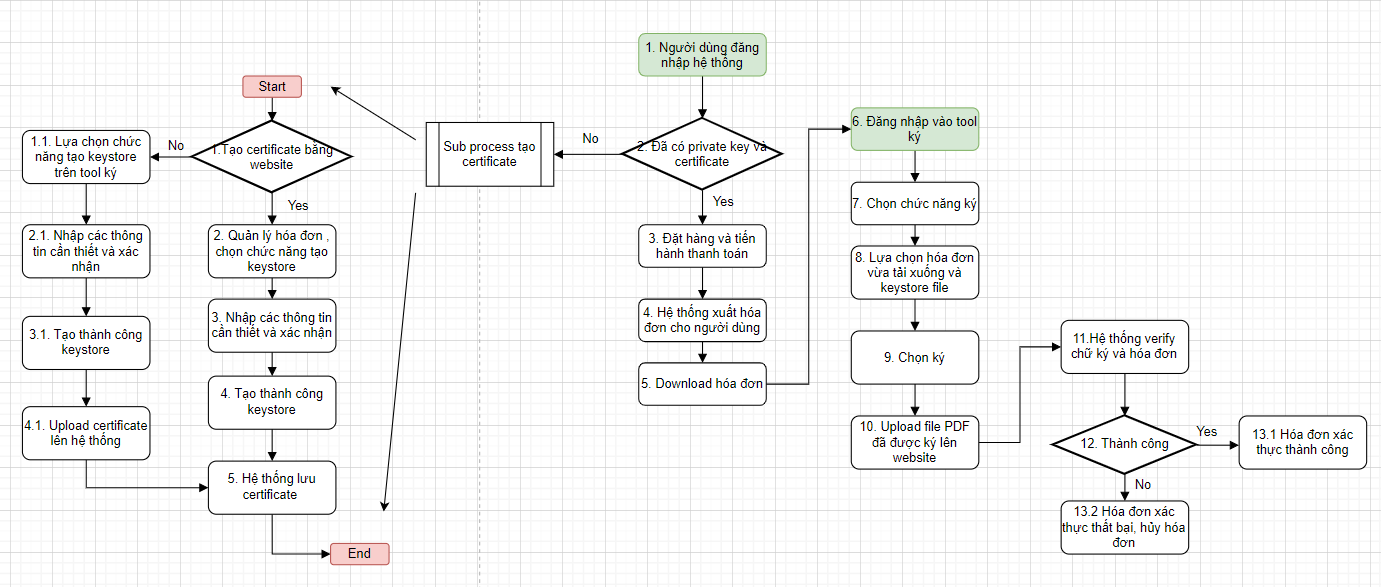
Với sự phát triển của Internet và ứng dụng di động, các nền tảng thương mại càng có cơ sở để phát triển mạnh mẽ. Hiện nay tính bảo mật trong các giao dịch là vấn đề đáng lo ngại. Vì vậy để đảm bảo an toàn trong việc thực hiện các giao dịch điện tử như nộp thuế qua mạng, kê khai hải quan, mua sắm điện tử và quản lý bảo mật các thông tin khách hàng thì việc sử dụng chữ ký số là vô cùng cần thiết. Thông qua việc sử dụng chữ ký số này sẽ giúp xác thực được người gửi tài liệu đối với các giao dịch điện tử qua internet và đảm bảo rằng nội dung gốc của tài liệu đó không bị thay đổi sữa chữa. Vì vậy nhóm chúng em đã áp dụng chữ ký điện tử vào giai đoạn xác thực hóa đơn, đảm bảo rằng danh tính của người mua hàng, không phải người khác do người khác giả mạo rồi mua hàng cũng như đảm bảo tính toàn vẹn của hóa đơn khi được chuyển giao trên đường truyền internet.

Đồ án kết hợp việc sử dụng các chức năng ở website cũng như chức năng ký ở tool ký được mở thông qua USB.

Để tìm hiểu kĩ hơn về các kỹ thuật, các chức năng của bài đồ án. Mời thầy và các bạn cùng tiếp tục đọc và tìm hiểu sâu hơn ở các phần tiếp theo.

# II. CÁC PHẦN CHÍNH:

## 1. Work Flow:



[*https://app.diagrams.net/#G1YgafLTsy4Vgq08OPnwJrLc1onrF\_qi2E*](https://app.diagrams.net/#G1YgafLTsy4Vgq08OPnwJrLc1onrF_qi2E)

**Các bước thực hiện:**

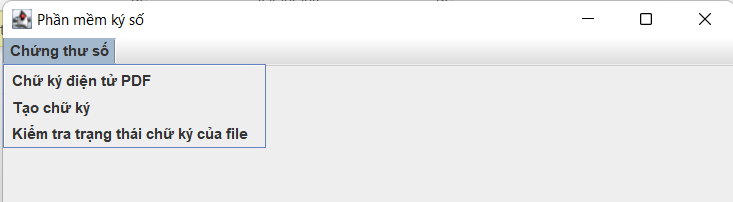
1. Người dùng đăng nhập vào website.
2. Nếu người dùng đã có private key và certificate rồi thì tiến hành bước tiếp theo.
3. Người dùng đặt hàng và tiến hành thành toán.
4. Hệ thống xuất hóa đơn cho người dùng.
5. Người dùng tải hóa đơn về máy của mình.
6. Đăng nhập vào tool ký.
7. Chọn chức năng ký của tool
8. Lựa chọn file hóa đơn vừa tải xuống và file keystore (private key và certificate)
9. Chọn nút ký
10. Người dùng upload file pdf đã được ký lên website
11. Hệ thống validate file pdf.
12. Nếu thành công thì hóa đơn xác thực thành công, nếu không hóa đơn xác thực thất bại và hủy hóa đơn.

**Luồng phụ:** Tạo keystore khi người dùng chưa có private key và certificate hoặc người dùng muốn tạo cặp khóa khác cho bản thân:

* 1. Người dùng sử dụng website để tạo cặp key mới và certificate:
     1. Lựa chọn quản lý hóa đơn và chọn chức năng tạo keystore.
     2. Nhập các thông tin cần thiết và xác nhận
     3. Hệ thống thông báo tạo keystore thành công
     4. Hệ thống lưu certificate của người dùng để sử dụng cho lần validate sau.
  2. Người dùng sử dụng tool ký để tạo cặp key mới và certificate:
     1. Lựa chọn chức năng tạo keystore trên tool ký.
     2. Nhập các thông tin cần thiết và xác nhận.
     3. Tạo thành công keystore.
     4. Người dùng upload certificate lên hệ thống.
     5. Hệ thống lưu lại certificate của người dùng để sử dụng cho lần validate sau.

## 2. Tool ký:

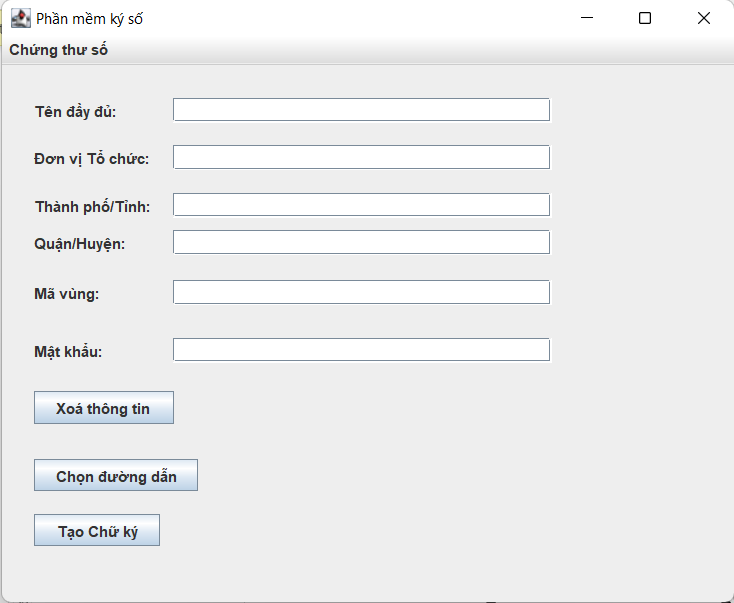
### a) Màn hình bắt đầu:



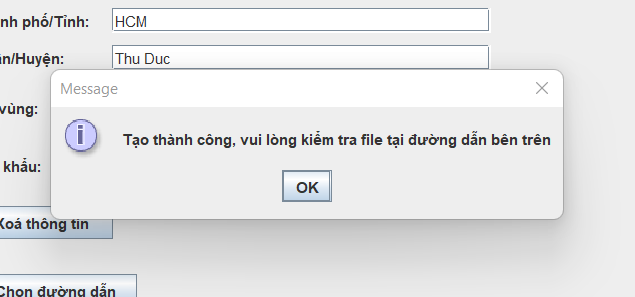
### b) Màn hình tạo key pair và certificate:

Người dùng được yêu cầu nhập các thông tin để tạo private key và certificate.

Mật khẩu người dùng bắt buộc nhập vào phải >= 6 kí tự.

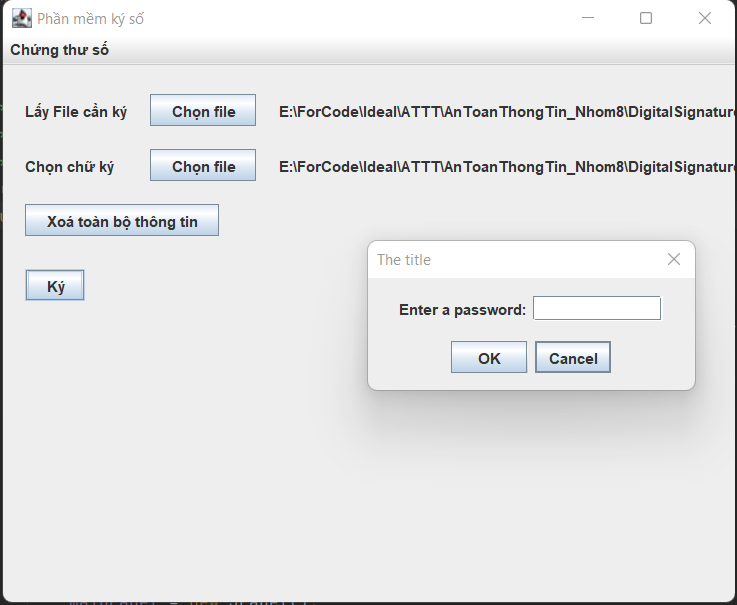


Sau khi nhập đầy đủ thông tin, người dụng click vào button Tạo chữ ký. Nếu tạo thành công, pop-up thông báo tạo thành công sẽ được hiển thị.



Và file key store cũng được hiển thị 

### c) Màn hình ký hóa đơn PDF:

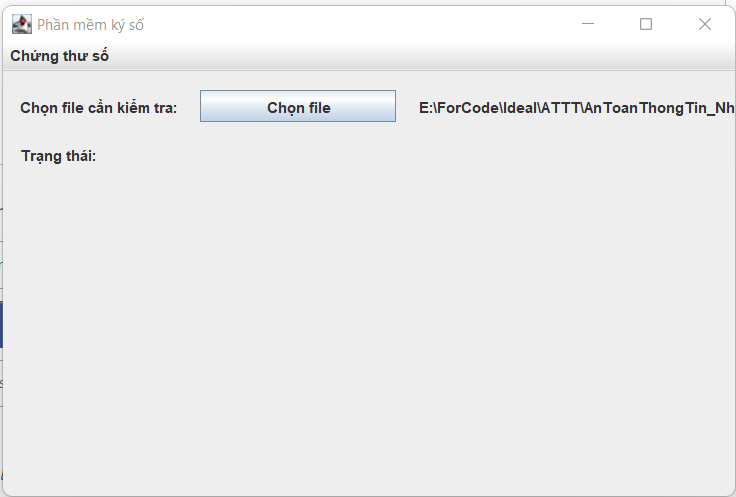


Người dùng chọn đến đường dẫn của file hóa đơn cần ký, sau đó chọn đường dẫn đến file keyStoreFile ở bên trên để thực hiện ký. Cuối cùng bấm ký để tiến hành ký vào file pdf. Tool pop-up yêu cầu người dùng nhập mật khẩu của file chữ ký đã lựa chọn ở bên trên.

Sau khi nhập đúng mật khẩu và ký thành công sẽ có pop-up thông báo cho người dùng.

d) Màn hình kiểm tra file đã được ký hay chưa:

Trước khi upload file hóa đơn đã được ký lên cho website xử lý thì người dùng cũng có thể kiểm tra lại liệu file pdf đó đã được ký chính xác hay chưa bằng cách chọn file cần kiểm tra và chọn nút kiểm tra. Nếu kiểm tra thành công thì sẽ hiện thị trạng thái là đã được ký, còn không thì chưa được ký.



## 3. Chức năng thanh toán xác thực người dùng trên website:

### a) Trình tự xác thực

### b) Màn hình tạo certificate và public key

### c) Màn hình quản lý certificate và public key

# III. TÀI LIỆU THAM KHẢO:

*https://itextpdf.com/sites/default/files/2018-12/digitalsignatures20130304.pdf*