**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BỘ MÔN CÔNG NGHỆ PHẦN MỀM**

**MAI VĂN TUẤN – 1612781**

**CHÂU XUÂN TUẤN – 1712868**

**NGUYỄN THỌ TUẤN – 1712878**

**LÊ VĂN – 1712897**

**HOÀNG MINH VŨ - 1712918**

# XÂY DỰNG HỆ THỐNG KÝ KẾT VĂN BẢN TRỰC TUYẾN

**THỰC TẬP DỰ ÁN TỐT NGHIỆP CỬ NHÂN CNTT**

**CHƯƠNG TRÌNH CHÍNH QUY**

**Tp. Hồ Chí Minh, tháng 03/2022**

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

**KHOA CÔNG NGHỆ THÔNG TIN**

**MAI VĂN TUẤN – 1612781**

**CHÂU XUÂN TUẤN – 1712868**

**NGUYỄN THỌ TUẤN – 1712878**

**LÊ VĂN – 1712897**

**HOÀNG MINH VŨ - 1712918**

# XÂY DỰNG HỆ THỐNG KÝ KẾT VĂN BẢN TRỰC TUYẾN

THỰC TẬP DỰ ÁN TỐT NGHIỆP CỬ NHÂN CNTT

CHƯƠNG TRÌNH CHÍNH QUY

**GIÁO VIÊN HƯỚNG DẪN**

TS. NGÔ HUY BIÊN

Tp. Hồ Chí Minh, tháng 03/2022

# NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

…….....

…….....

…….....

Tp. HCM, ngày … tháng … năm 2021
Giáo viên hướng dẫn

# NHẬN XÉT CỦA GIÁO VIÊN PHẢN BIỆN

…….....

…….....

…….....

…….....

…….....

…….....

…….....

…….....

…….....

…….....

…….....

…….....

…….....

Tp. HCM, ngày … tháng … năm 2021
Giáo viên phản biện

# LỜI CẢM ƠN

Để hoàn thành Thực tập dự án tốt nghiệp này, đầu tiên chúng tôi xin gửi lời cảm ơn đến Khoa Công nghệ Thông tin - Trường Đại học Khoa học Tự nhiên, xin cảm ơn ban quản trị của nhà trường và toàn thể quý Thầy Cô giảng dạy. Các bài giảng của thầy cô trang bị cho chúng tôi những kiến thức, nền tảng vững chắc và quý báu trong những năm học vừa qua.

Đặc biệt, chúng tôi xin chân thành gửi lời cảm ơn đến thầy Ngô Huy Biên, thầy đã trực tiếp hướng dẫn, tận tình giải đáp thắc mắc, góp ý về nội dung, tạo điều kiện thoải mái và đưa ra những định hướng trong quá trình thực hiện Thực tập dự án tốt nghiệp.

Trong quá trình thực hiện Thực tập dự án tốt nghiệp, do những hạn chế về kinh nghiệm nên khó có thể tránh khỏi những thiếu sót và hạn chế. Vì vậy, chúng tôi hi vọng thầy cô và người đọc sẽ đưa ra những phản hồi, những đóng góp giúp đề tài dự án trở nên hoàn thiện hơn.

Cuối cùng, chúng tôi xin kính gửi đến thầy cô một lời cảm ơn sâu sắc, chúc các thầy cô sẽ gặp nhiều thành công trong cuộc sống.

*Thành phố Hồ Chí Minh, ngày ..... tháng 03 năm 2022*

*Nhóm sinh viên thực hiện*

**Mai Văn Tuấn**

**Châu Xuân Tuấn**

**Nguyễn Thọ Tuấn**

**Lê Văn**

**Hoàng Minh Vũ**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

ĐỀ CƯƠNG ĐỒ ÁN TỐT NGHIỆP

# XÂY DỰNG HỆ THỐNG KÝ KẾT VĂN BẢN TRỰC TUYẾN

***(BUILDING E-SIGNATURE SYSTEM)***

## 1 THÔNG TIN CHUNG

**Người hướng dẫn:**

TS. Ngô Huy Biên (Khoa Công nghệ Thông tin)

**Nhóm sinh viên thực hiện:**

1. Mai Văn Tuấn (MSSV: 1612781)
2. Châu Xuân Tuấn (MSSV: 1712868)
3. Nguyễn Thọ Tuấn (MSSV: 1712878)
4. Lê Văn (MSSV: 1712897)
5. Hoàng Minh Vũ (MSSV: 1712918)

**Loại đề tài:** Ứng dụng

**Thời gian thực hiện:** Từ *09/2021* đến 0*3/2022*

# 2 NỘI DUNG THỰC HIỆN

## 2.1 Giới thiệu về đề tài

Hiện nay, khi mà mọi vấn đề trong cuộc sống đều có thể giải quyết bằng ứng dụng công nghệ và số hóa thông tin. Chữ ký điện tử được sử dụng rộng rãi và nhiều người biết đến, cụ thể trong các giao dịch điện tử. Các ứng dụng hiện có trên thị trường rất đa dạng, với nhiều tính năng kèm theo và có thể mang nặng tính chất kinh doanh quảng cáo. Bên cạnh đó, chức năng và nhu cầu của người sử dụng không nhiều, các hệ thống chữ ký điện tử phổ biến hầu hết tập trung vào thị trưởng Mỹ và nước ngoài. Dẫn đến bất cập không hỗ trợ ngôn ngữ tiếng việt, nhiều chức năng thừa và không được sử dụng tại quốc gia Việt Nam, yêu cầu thẻ thanh toán trực tuyến quốc tế khi đăng ký, bản quyền giá cao khi quy đổi ngoại tệ tiền Việt Nam. Vì thế chúng tôi muốn tạo ra một hệ thống ký kết văn bản trực tuyến, tập trung thị trường trong nước, ưu tiên sự tối giản, nhanh gọn. Tên là VTSign – Hệ thống ký kết văn bản trực tuyến (Building e-signature system).

## 2.2 Mục tiêu đề tài

**Thiết kế, xây dựng, kiểm thử, và triển khai hệ thống.**

- Back-end: Cung cấp các API bao gồm: cho phép người dùng đăng ký, và thanh toán chi phí sử dụng dịch vụ, cho phép người quản trị quản lý người sử dụng dịch vụ, xử lý việc quản lý và ký kết văn bản, cung cấp các báo cáo cho admin về quá trình truy cập và báo cáo cho người dùng về quá trình truy cập, dung lượng sử dụng của từng người dùng sử dụng, dung lượng sử dụng của tài khoản. Áp dụng Microservices, mô phỏng, thiết kế, thực hiện, báo cáo kết quả các kịch bản kiểm thử khả năng tải mong muốn (load tests), khả năng chịu tải tối đa (stress tests), khả năng xâm nhập hệ thống (penetration testing).
- Front-end: Các giao diện kết nối với các tính năng tương ứng với back-end, đơn giản dễ dàng thao tác và phù hợp với nhiều đối tượng người dùng sử dụng.

**Viết 80 trang Đồ án.**

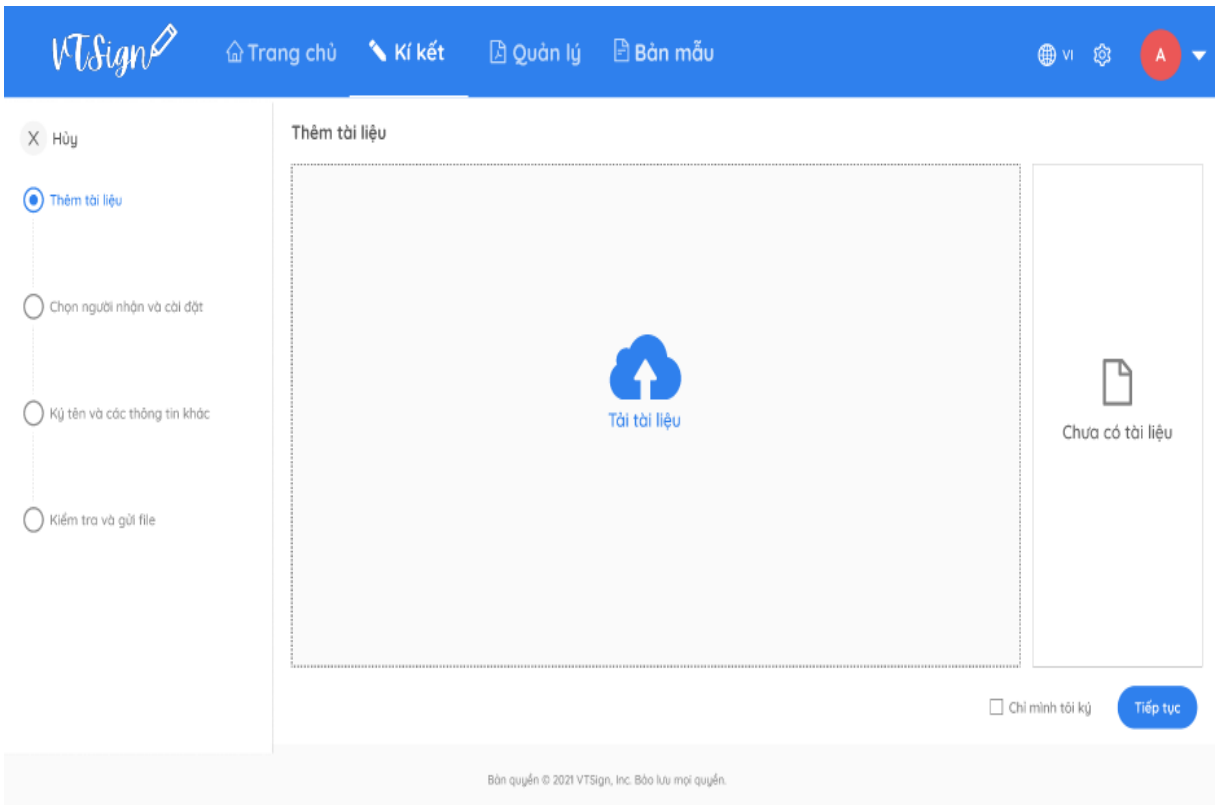
## 2.3 Phạm vi của đề tài

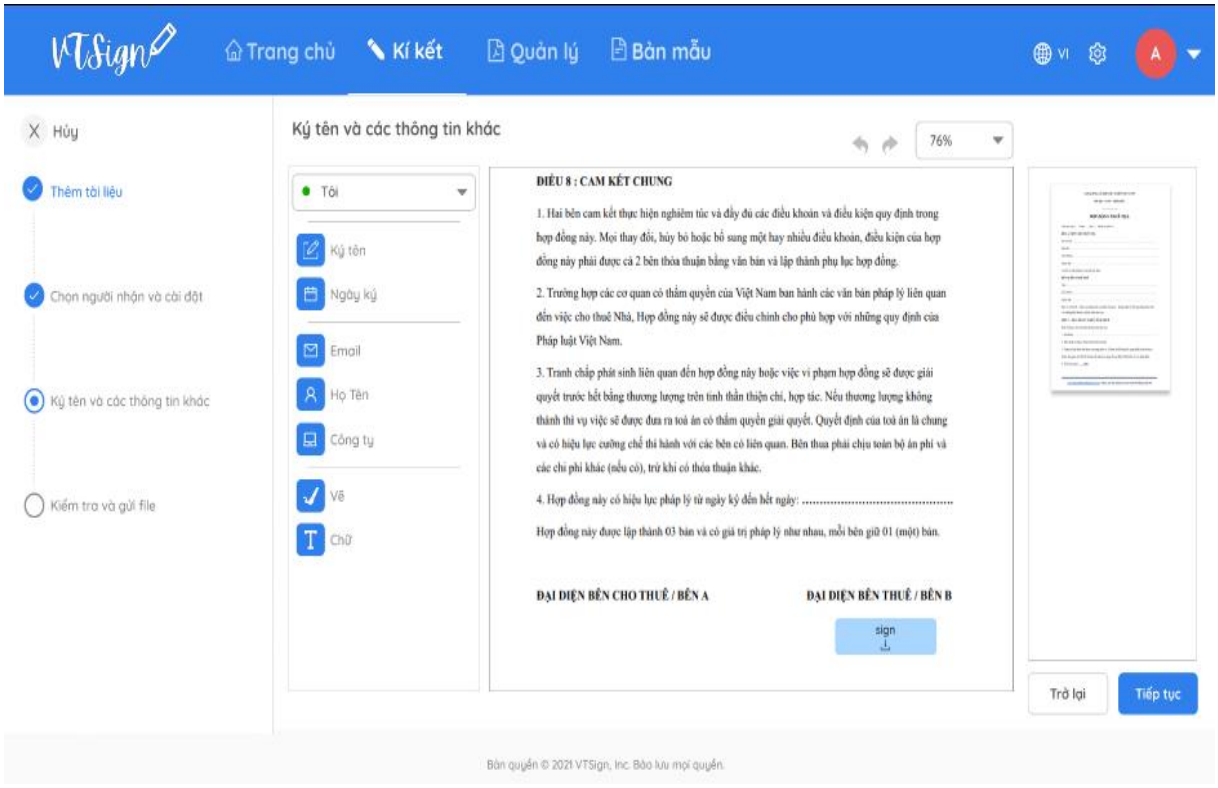
**Các tính năng không thực hiện**

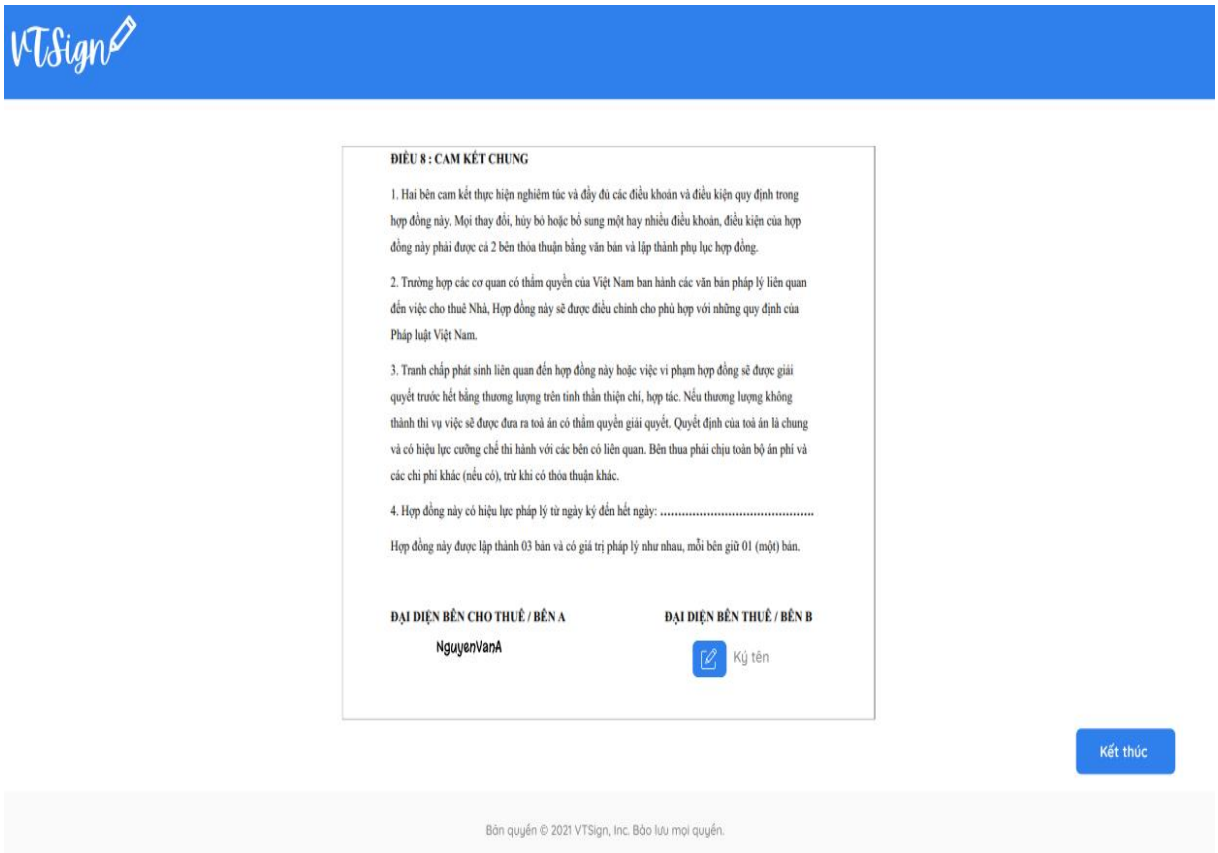
- Các chức năng tự động hóa được thiết lập riêng. Thanh toán trực tuyến thông qua ngân hàng. Bản quyền và giới hạn sử dụng.
- Đồng bộ vào trên các phần mềm bên thứ ba ví dụ như Dropbox, Word, Adobe. Triển khai trên tất cả nền tảng khác.
- Chức năng phức tạp chuyên môn cao như công chứng và chống giả mạo, mã hóa tài liệu và bảo mật cao. Chức năng kiểm toán thống kê đánh giá đặc thù.
- Giao diện có nhiều tùy chọn thay đổi như quốc gia và vùng, ngôn ngữ. Tùy chọn ẩn hay hiện mục và các chức năng trên hệ thống.
- Thêm các thương hiệu logo được cá nhân hóa. Xác định các loại chữ ký được phép. Hệ thống live chat trò chuyện trực tiếp trên hệ thống.

## 2.4 Cách tiếp cận dự kiến

***Bản mẫu:** demo các trang chức năng chính của website.

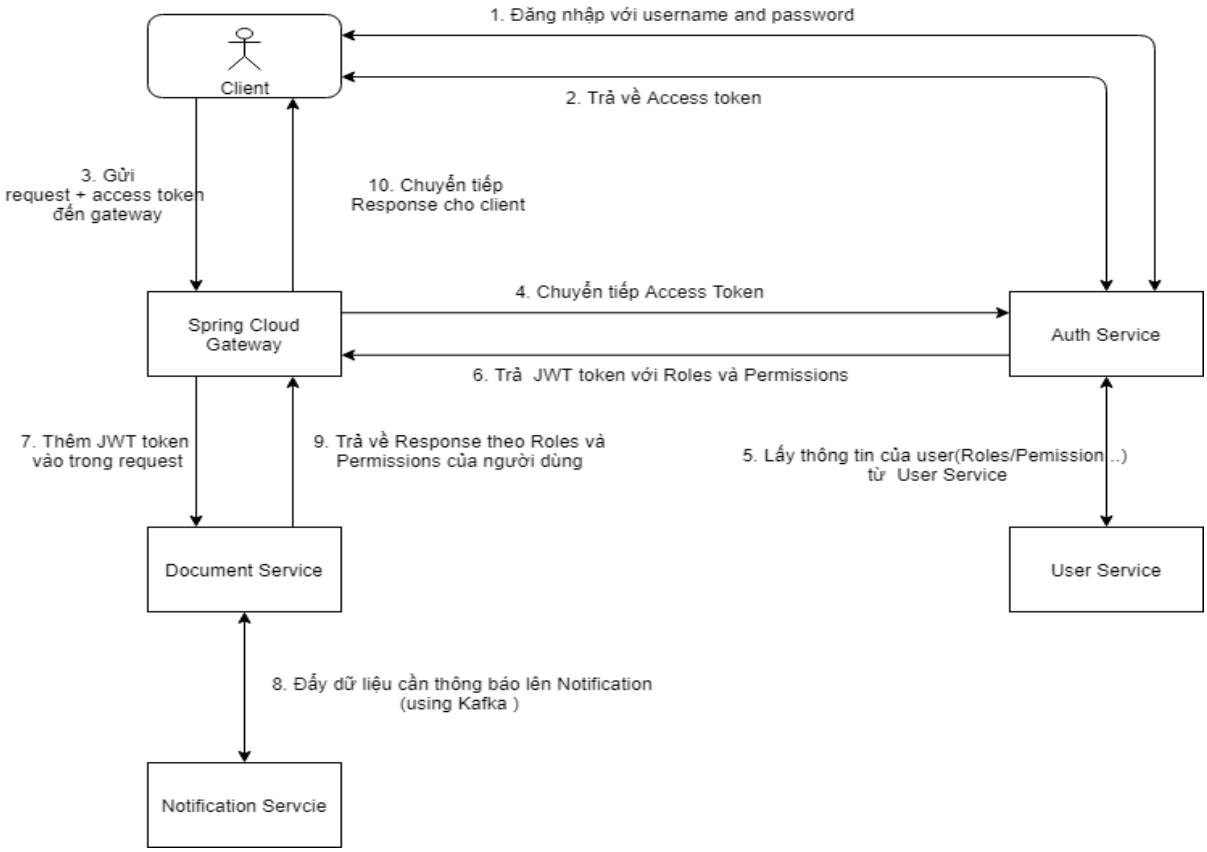



VTSign
Trang chủ
Kí kết
Quản lý
Bản mẫu
VI
A
Hủy
Thêm tài liệu
Chọn người nhận và cài đặt
Ký tên và các thông tin khác
Kiểm tra và gửi file
Ký tên và các thông tin khác
76%
Tôi
Ký tên
Ngày ký
Email
Họ Tên
Công ty
Vẽ
Chữ
ĐIỀU 8 : CAM KẾT CHUNG
1. Hai bên cam kết thực hiện nghiêm túc và đầy đủ các điều khoản và điều kiện quy định trong hợp đồng này. Mọi thay đổi, hủy bỏ hoặc bổ sung một hay nhiều điều khoản, điều kiện của hợp đồng này phải được cả 2 bên thỏa thuận bằng văn bản và lập thành phụ lục hợp đồng.
2. Trường hợp các cơ quan có thẩm quyền của Việt Nam ban hành các văn bản pháp lý liên quan đến việc cho thuê Nhà, Hợp đồng này sẽ được điều chỉnh cho phù hợp với những quy định của Pháp luật Việt Nam.
3. Tranh chấp phát sinh liên quan đến hợp đồng này hoặc việc vi phạm hợp đồng sẽ được giải quyết trước hết bằng thương lượng trên tinh thần thiện chí, hợp tác. Nếu thương lượng không thành thì vụ việc sẽ được đưa ra toà án có thẩm quyền giải quyết. Quyết định của toà án là chung và có hiệu lực cưỡng chế thi hành với các bên có liên quan. Bên thua phải chịu toàn bộ án phí và các chi phí khác (nếu có), trừ khi có thỏa thuận khác.
4. Hợp đồng này có hiệu lực pháp lý từ ngày ký đến hết ngày: .....
Hợp đồng này được lập thành 03 bản và có giá trị pháp lý như nhau, mỗi bên giữ 01 (một) bản.
ĐẠI DIỆN BÊN CHO THUÊ / BÊN A
ĐẠI DIỆN BÊN THUÊ / BÊN B
sign
Trở lại
Tiếp tục
Bản quyền © 2021 VTSign, Inc. Bảo lưu mọi quyền.


VTSign
ĐIỀU 8 : CAM KẾT CHUNG
1. Hai bên cam kết thực hiện nghiêm túc và đầy đủ các điều khoản và điều kiện quy định trong hợp đồng này. Mọi thay đổi, hủy bỏ hoặc bổ sung một hay nhiều điều khoản, điều kiện của hợp đồng này phải được cả 2 bên thỏa thuận bằng văn bản và lập thành phụ lục hợp đồng.
2. Trường hợp các cơ quan có thẩm quyền của Việt Nam ban hành các văn bản pháp lý liên quan đến việc cho thuê Nhà, Hợp đồng này sẽ được điều chỉnh cho phù hợp với những quy định của Pháp luật Việt Nam.
3. Tranh chấp phát sinh liên quan đến hợp đồng này hoặc việc vi phạm hợp đồng sẽ được giải quyết trước hết bằng thương lượng trên tinh thần thiện chí, hợp tác. Nếu thương lượng không thành thì vụ việc sẽ được đưa ra toà án có thẩm quyền giải quyết. Quyết định của toà án là chung và có hiệu lực cưỡng chế thi hành với các bên có liên quan. Bên thua phải chịu toàn bộ án phí và các chi phí khác (nếu có), trừ khi có thỏa thuận khác.
4. Hợp đồng này có hiệu lực pháp lý từ ngày ký đến hết ngày: .....
Hợp đồng này được lập thành 03 bản và có giá trị pháp lý như nhau, mỗi bên giữ 01 (một) bản.
ĐẠI DIỆN BÊN CHO THUÊ / BÊN A
NguyenVanA
ĐẠI DIỆN BÊN THUÊ / BÊN B
Ký tên
Kết thúc
Bản quyền © 2021 VTSign, Inc. Bảo lưu mọi quyền.

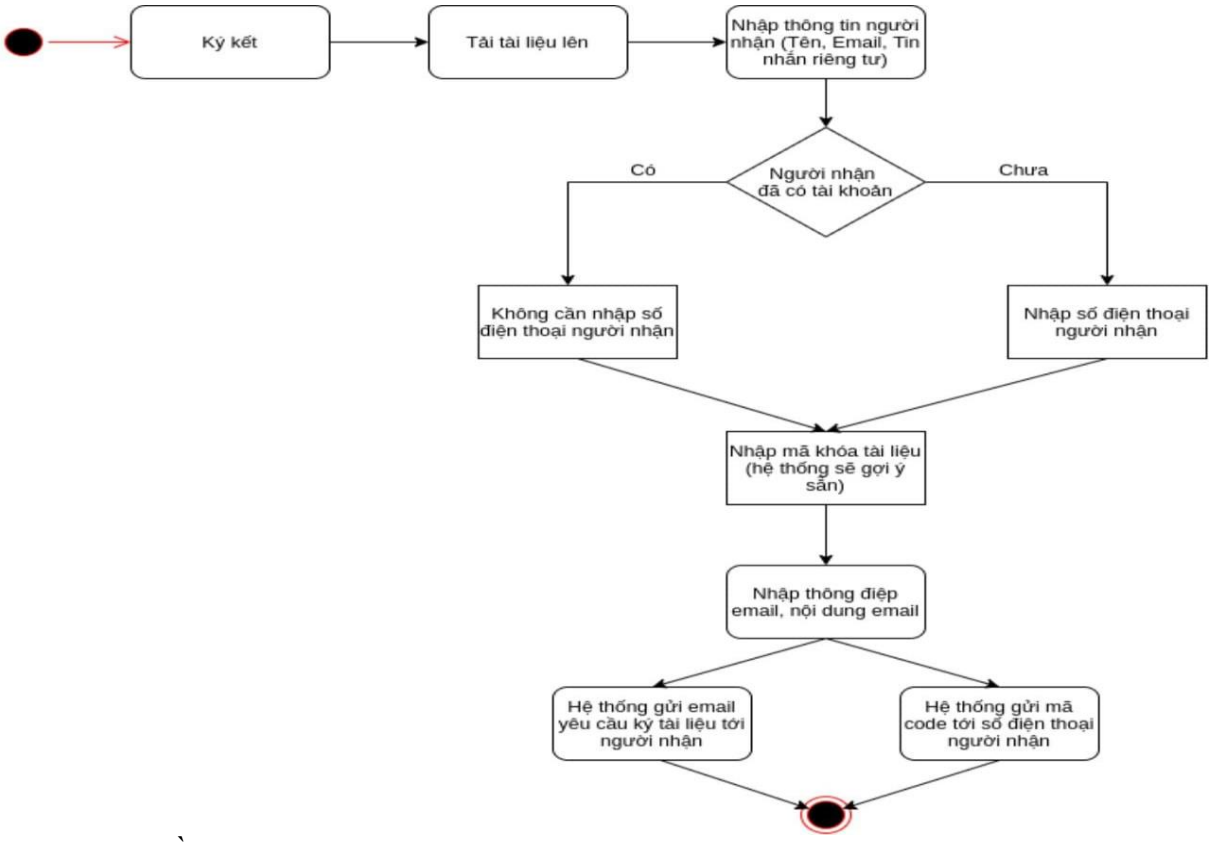
***Kiến trúc:**

Kiến trúc Process:

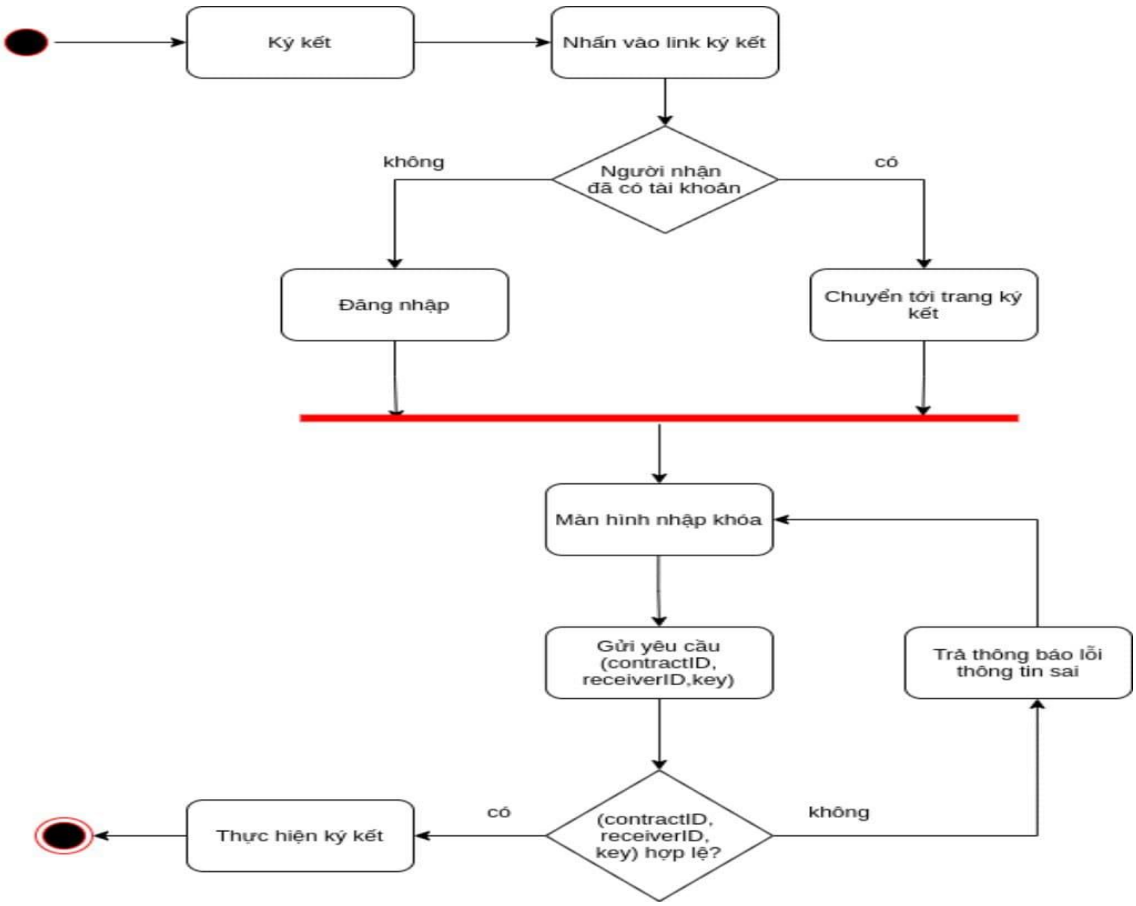



- Hình trên thể hiện quy trình khi thực hiện yêu cầu thì yêu cầu sẽ đi qua các service. Yêu cầu được gửi lên từ user (đã có tài khoản) thông qua phải có AccessToken. Sau đó Spring Cloud Gateway sẽ gửi AccessToken lên AuthService và lấy roles và permissions. Tạo ra Access Token mới và trả về cho gateway gắn vào request và tiếp tục đến service đích. Người chưa có tài khoản cần đăng ký, đăng nhập để có Access Token.

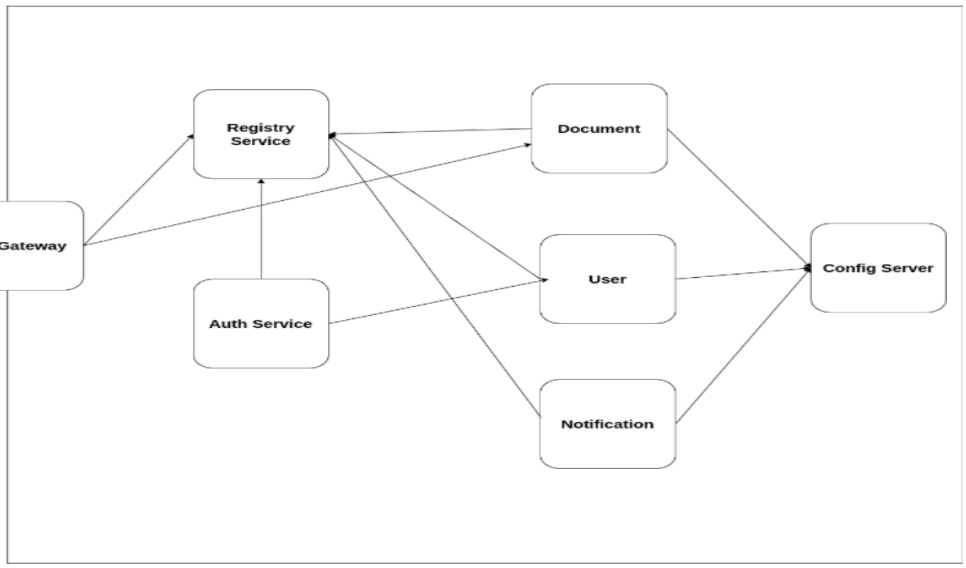
- Mô tả luồng gửi tài liệu:




- Mô tả luồng ký tài liệu:



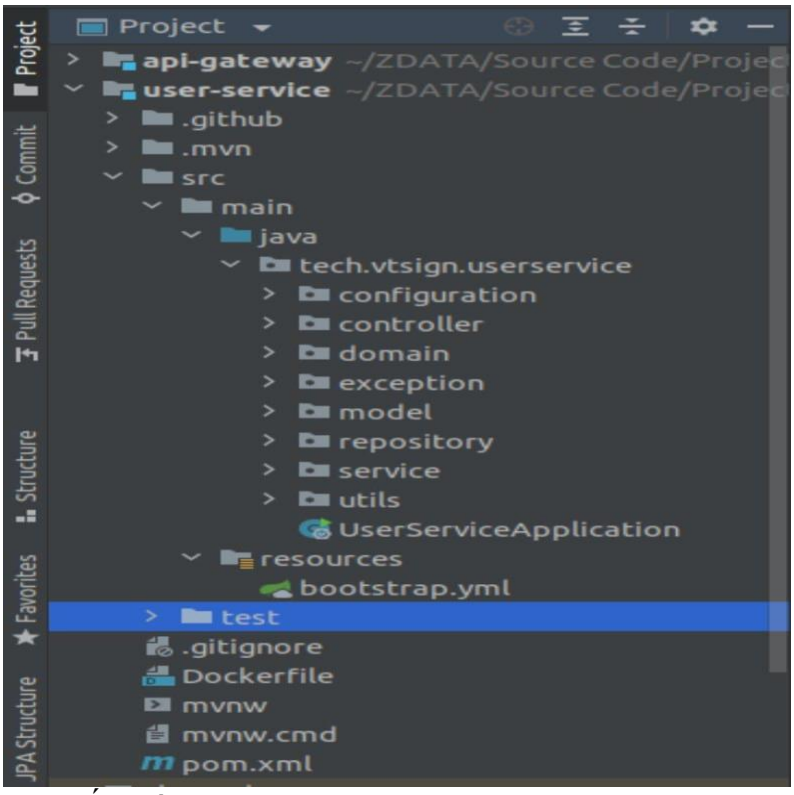
Kiến trúc Logical:




- Logical view của nhóm thể hiện cấu trúc và tổ chức thiết kế giữa các service trong hệ thống, logical view được dùng để phân tích và thiết kế.

- Miêu tả các lớp đối tượng và mối quan hệ, gửi thông điệp cho nhau để cung cấp các thiết lập cấu hình được cài sẵn.

Kiến trúc Development:



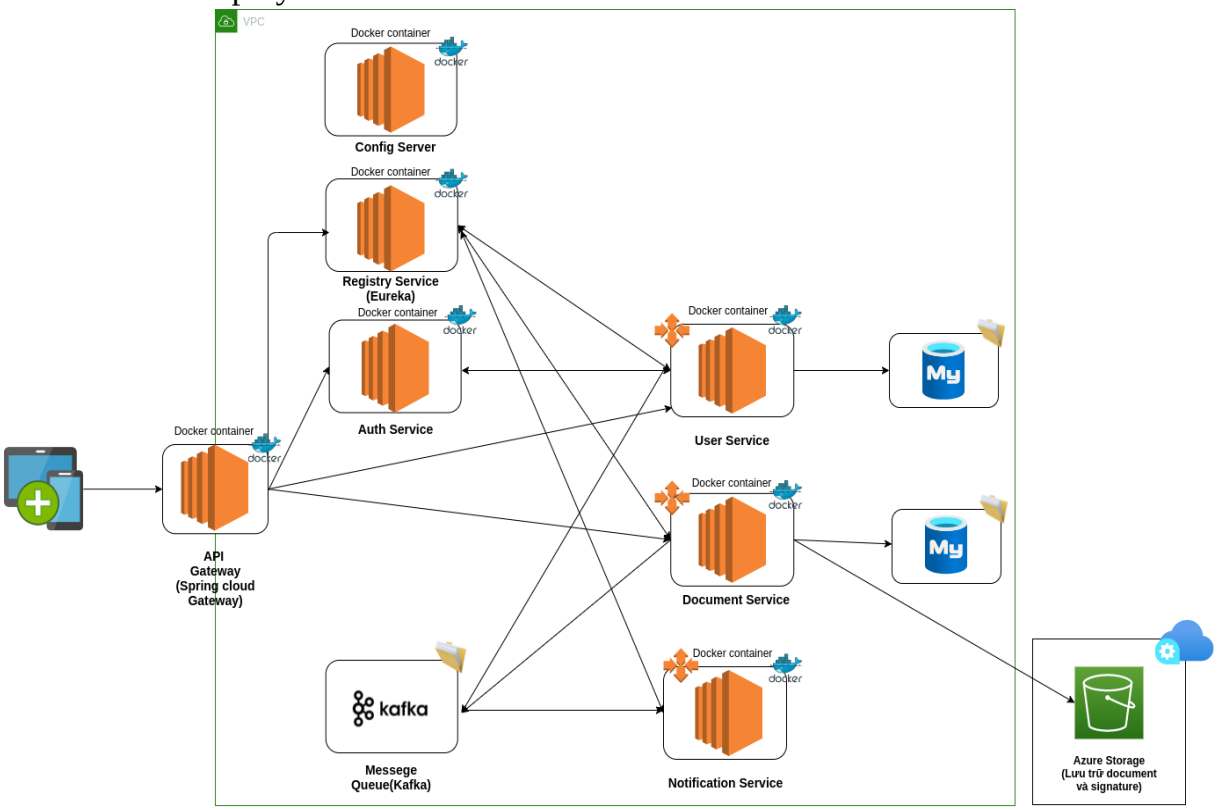

- Phát triển theo kiến trúc microservices
- Mỗi service backend gồm có các packages chính sau:

+ configuration: Các cấu hình cho service
+ controller: Tiếp nhận các yêu cầu gửi tới
+ domain: Transfer dữ liệu với database
+ exception: Xử lý các lỗi và ngoại lệ
+ model: Transfer dữ liệu với các services khác
+ repository: Thao tác dữ liệu với database
+ service: Xử lý logic
+ utils: Các hàm xử lý tiện ích
+ test: Viết các unit test
+ resources: chứa các file cấu hình biến môi trường cho service

- Một số file và thư mục khác:

+ github: thư mục viết các cấu hình chạy hệ thống CI/CD tự động với Github Actions
+ Dockerfile: cấu hình để xây dựng docker image để tiện hơn cho việc triển khai
+ pom.xml: quản lý các thư viện phụ thuộc

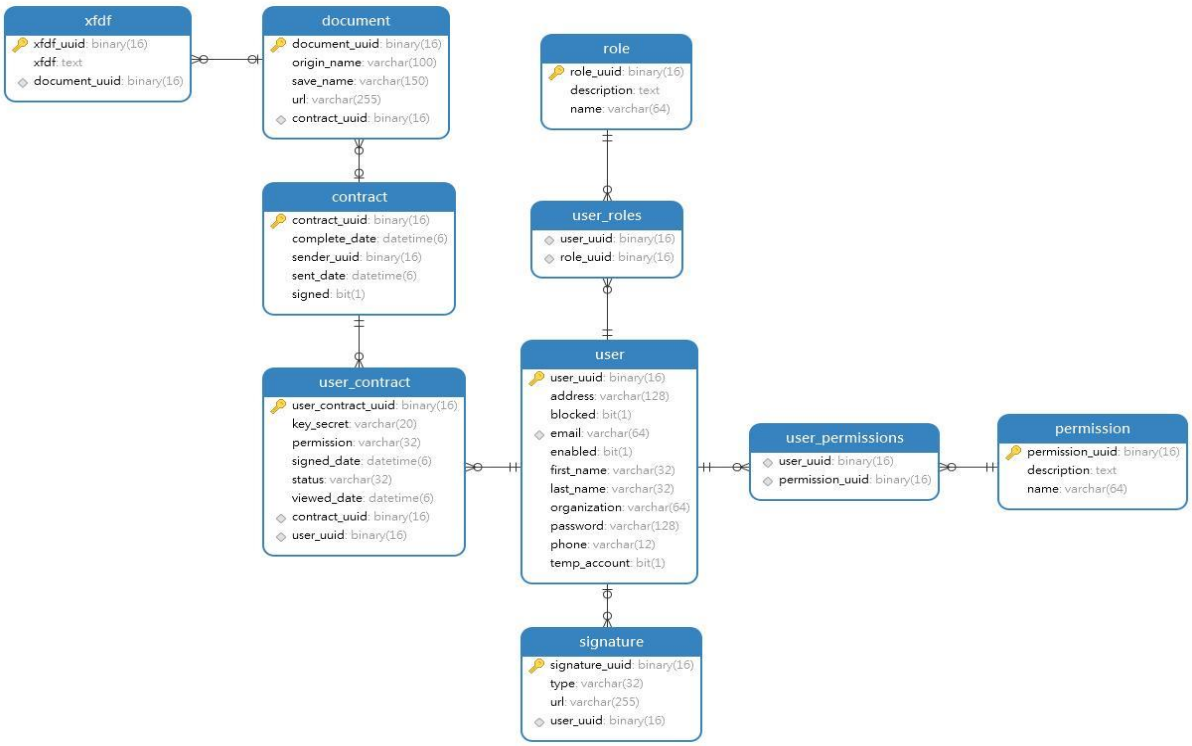
Kiến trúc Deployment:



- Thể hiện cách triển khai hệ thống trên quy trình thực tế
- Hệ thống phát triển theo hướng microservices:

+ Mỗi service có thể có nhiều thể hiện (instance), được triển khai bên trong các Docker Container và kết nối tới một database độc lập.
+ Hệ quản trị CSDL được sử dụng là MySQL.
+ Api Gateway sử dụng Spring Cloud Gateway để nhận các yêu cầu từ người dùng.
+ Các service đăng ký với nhau thông qua Registry Service (sử dụng Eureka Server), có thể gọi nhau bằng service-id.
+ Message Queue sử dụng Kafka.
+ Config Server sử dụng Spring Cloud Config Server để cấu hình các service trên Github repository.
+ Tài liệu được lưu trữ trên Microsoft Azure Storage.
+ Có thể triển khai trên các hệ thống máy chủ chạy độc lập với nhau (loosely coupled)
+ Docker Image của mỗi service được build và đẩy lên Docker Hub một cách tự động thông qua hệ thống build tự động (Github Actions).

***Mô hình dữ liệu:**



***Các mục tiêu kiểm thử:**

- Load, Stress testing: Apache Jmeter là một dự án Apache có thể được sử dụng như một công cụ kiểm tra tải để phân tích và đo lường hiệu suất của nhiều loại dịch vụ, tập trung vào các ứng dụng web.
- Penetration Testing: Nmap - Network Mapper là một công cụ bảo mật được phát triển bởi Gordon Lyon. Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật.

***Dự kiến phương pháp so sánh, đánh giá hệ thống:**

**Bảng so sánh các tính năng ký kết cơ bản của 4 hệ thống**

| Tính năng | SignNow | AdobeSign | DocuSign | VTSign |
|---|---|---|---|---|
| Gửi tài liệu cần ký | ✓ | ✓ | ✓ | ✓ |
| Mời ký số lượng lớn | ✓ | ✓ | ✓ | ✓ |
| Chỉnh sửa tài liệu trước khi gửi | ✓ | ✓ | ☒ | ☒ |
| Tạo các mẫu có thể sử dụng lại | ✓ | ✓ | ✓ | ✓ |
| Thêm thương hiệu được cá nhân hóa | ✓ | ✓ | ✓ | ☒ |
| Gửi lời mời qua liên kết | ✓ | ✓ | ✓ | ✓ |
| Ký kết trực tiếp | ✓ | ☒ | ☒ | ✓ |
| Xác định các loại chữ ký được phép | ✓ | ☒ | ☒ | ☒ |
| Trò chuyện trực tiếp | ✓ | ✓ | ☒ | ☒ |
| Bảo vệ mối đe dọa nâng cao | ✓ | ☒ | ✓ | ✓ |
| Quản lý tài liệu có thời hạn | ✓ | ☒ | ✓ | ✓ |

**Bảng ưu điểm khuyết điểm của 4 hệ thống**

| Hệ thống | Ưu điểm | Khuyết điểm |
|---|---|---|
| **SignNow** | - Đăng nhập/đăng ký nhanh bằng tài khoản Facebook, Google.<br>- Hệ thống sử dụng eSignature đơn giản, giao diện hiện đại | - Hỗ trợ ít ngôn ngữ, tập trung thị trường nước ngoài.<br>- Giao diện trình duyệt chưa có chế độ nền tối. |

| | | |
|---|---|---|
| | dễ sử dụng, có LiveChat hỗ trợ khách hàng.<br>- Bản dùng thử không giới hạn nhiều chức năng, bản quyền giá hợp lý, phù hợp nhiều đối tượng. | - Không dùng phương pháp Digital Signature, bảo mật còn hạn chế. |
| **DocuSign** | - Sử dụng phương pháp định danh Self-Signed Digital Signature, không đòi hỏi người dùng trả tiền mua Chứng thực (Certificate).<br>- Sử dụng các công nghệ mã hóa và bảo mật dữ liệu, thông báo qua tin nhắn (SMS Delivery).<br>- Phù hợp với các công ty quy mô lớn, đặt nặng về bảo mật chuyên môn.<br>- Nhiều công cụ hỗ trợ kèm theo, đáp ứng nhiều tiêu chuẩn bảo mật. | - Không có đăng nhập/đăng ký nhanh bằng tài khoản Facebook, Google.<br>- Hệ thống nặng, truy cập chậm ở khu vực Việt Nam, không có LiveChat.<br>- Không được chỉnh sửa tài liệu trước khi gửi và ký kết trực tiếp.<br>- Hỗ trợ ít ngôn ngữ, tập trung thị trường Mỹ, bản quyền giá cao. |
| **AdobeSign** | - Sử dụng phương pháp Digital Signature, đòi hỏi người dùng trả tiền mua 1 Chứng thực (Certificate).<br>- Đồng bộ và cá nhân hóa với phần mềm liên quan của Adobe. | - Đăng nhập/đăng ký phức tạp, hệ thống khá chậm và tải nhiều thông tin và thông báo.<br>- Giao diện cũ khó nhìn, nhiều tính năng thừa và khó sử dụng, Không ký trực tiếp. |

| | | |
|---|---|---|
| | | - Bản quyền và phí sử dụng cao, bản dùng thử nhiều ràng buộc chức năng. |
| **VTSign** | - Hệ thống xử lý và hiển thị nhanh, không hiện các thông báo gây nhiễu.<br>- Bảo mật tài liệu, xác thực người dùng bằng email và số điện thoại cá nhân.<br>- Giao diện thao tác đơn giản dễ sử dụng, phù hợp nhiều lứa tuổi.<br>- Hỗ trợ ngôn ngữ tiếng việt, bản quyền sử dụng phù hợp người Việt Nam. | - Không có đăng nhập/đăng ký nhanh bằng tài khoản Facebook, Google.<br>- Không chỉnh sửa tài liệu trước khi gửi, không LiveChat, không hỗ trợ nhiều ngôn ngữ.<br>- Phù hợp với người dùng cá nhân, các tổ chức nhỏ, không chuyên môn cao. |

**Đánh giá**

- Các hệ thống trên thị trường rất đa dạng, với nhiều tính năng kèm theo. Thực tế chức năng và nhu cầu của người sử dụng không nhiều, các hệ thống phổ biến đa số tập trung vào thị trưởng Mỹ và nước ngoài. Dẫn đến bất cập không hỗ trợ ngôn ngữ tiếng việt, nhiều chức năng thừa và không được sử dụng tại Việt Nam, yêu cầu thẻ thanh toán trực tuyến quốc tế khi đăng ký, bản quyền giá cao khi quy đổi ngoại tệ tiền Việt Nam.
- Qua so sánh, đánh giá hệ thống của nhóm với các hệ thống tương tự. Các thành viên nhóm đã đưa ra thống nhất tổng quan về hệ thống VTSign. Thực hiện đúng các kế hoạch đề ra theo các mục 2.2 Mục tiêu đề tài và 2.3 Phạm vi của đề tài.

***Danh sách các công nghệ, công cụ sử dụng:**

- Mô hình Kanban: để thiết kế và triển khai đồ án.
- Kiến trúc Microservice: một kỹ thuật phát triển phần mềm, với nhiều lợi ích mang lại về khả năng mở rộng và bảo trì.
- Trello: để chia việc theo danh sách và các thẻ (kiểu Kanban).
- Figma: thiết kế giao diện bản mẫu các chức năng, luồng hệ thống.
- ReactJs: một thư viện JavaScript front-end mã nguồn mở miễn phí.
- Material-UI: một thư viện các React Component.
- Intellij: một IDE Java để phát triển các phần mềm máy tính.
- Visual Studio Code: một trình biên tập mã được phát triển bởi Microsoft.
- Postman: công cụ thao tác với APT như call và test API
- PhpMyAdmin: quản lý Cơ sở dữ liệu
- Microsoft Azure: quản lý, lưu trữ các tài liệu của user
- Github: một dịch vụ cung cấp kho lưu trữ mã nguồn
- Digitalocean: thiết lập quản lý các Cloud máy chủ chạy các Service.

## 2.5 Kết quả dự kiến của đề tài

- Hệ thống ký kết văn bản trực tuyến hoàn chỉnh với các chức năng đặt ra.
- Mã nguồn ứng dụng, trang website hệ thống ký kết văn bản VTSign.
- Tài liệu báo cáo chi tiết mà nhóm đã tìm hiểu trong suốt quá trình thực hiện đồ án. Kinh nghiệm tích lũy đạt được khi thực hiện một đồ án thực tế.

## 2.6 Kế hoạch thực hiện

| Thời gian | Công việc | Người thực hiện |
|---|---|---|
| 15/08/2021<br>–<br>31/08/2021 | - Liên hệ giảng viên hướng dẫn xem xét, bàn luận để thống nhất nhận thực hiện đề tài.<br>- Tìm hiểu thêm về đề tài. Nghiên cứu quy trình thực hiện đồ án của giảng viên hướng dẫn.<br>- Nộp đơn đăng ký thực tập dự án tốt nghiệp. | Tất cả thành viên |

| | | |
|---|---|---|
| 01/09/2021<br>–<br>30/09/2021 | - Giai đoạn khởi tạo dự án, khảo sát thị trường với các hệ thống tương tự.<br>- Chuẩn bị bản mẫu Prototype và Proof of Concept.<br>- Khởi tạo và hoàn thành chương 1 báo cáo. Khởi tạo đề cương chi tiết, kế hoạch sơ bộ. | Tất cả thành viên |
| 01/10/2021<br>–<br>31/10/2021 | - Thiết kế luồng hoạt động dự kiến của hệ thống.<br>- Tìm hiểu và lựa chọn các công cụ, công nghệ, thư viện hỗ trợ xây dựng hệ thống.<br>- Cập nhật chương 2 báo cáo và đề cương. | Tất cả thành viên |
| 01/11/2021<br>–<br>30/11/2021 | - Tổ chức mã nguồn, thiết kế giao diện trang chủ và đăng nhập.<br>- Hoàn tất khái niệm chương 2, cập nhật chương 5 và đề cương. Gửi giảng viên góp ý để chỉnh sửa tài liệu.<br>- Hoàn tất và nộp đề cương chi tiết cho khoa 10/11. | Tất cả thành viên |
| 01/12/2021<br>–<br>31/12/2021 | - Phát triển thiết kế kiến trúc hệ thống. Triển khai CI/CD. Xây dựng các chức năng đã đặt ra.<br>- Thực hiện triển khai chức năng xử lý dữ liệu người dùng trên máy khách - chủ.<br>- Hoàn tất cơ bản giao diện hệ thống. Triển khai phiên bản thử nghiệm.<br>- Hoàn tất chương 5, cập nhật chương 4 và thảo luận với giảng viên. | Tất cả thành viên |
| 01/01/2022<br>–<br>31/01/2022 | - Tiếp tục xử lý các vấn đề còn lại của hệ thống, đánh giá chung và cải tiến.<br>- Hoàn tất chương 4, cập nhật chương 3 và thảo luận với giảng viên. | Tất cả thành viên |
| 01/02/2022<br>–<br>28/02/2022 | - Thực hiện kiểm thử, triển khai phiên bản chính thức đầu tiên.<br>- Hoàn tất chương 3, cập nhật làm xong chương 2, kiểm tra toàn bộ báo cáo.<br>- Chuẩn bị và nộp đơn đăng ký bảo vệ đồ án 23/02. | Tất cả thành viên |
| 01/03/2021<br>–<br>Thời gian còn lại | - Cập nhật, kiểm tra hệ thống và máy chủ lần cuối. Hoàn tất báo cáo đề tài.<br>- Thực hiện chỉnh sửa báo cáo đề tài lần cuối. Chuẩn bị tài liệu buổi bảo vệ đề tài. | Tất cả thành viên |

# Tài liệu

[1] N. X. Sơn, Chữ kỳ điện tử và ứng dụng. PhD thesis, Trường Đại học Bách Khoa Hà Nội, 2015.

[2] J. Katz, Digital signatures. Springer Science & Business Media, 2010.

[3] C. Richardson, Microservices patterns: with examples in Java. Simon and Schuster, 2018.

[4] X. WANG, Y. WANG, and F. WANG, "The implement of a pair of secret key of digital signature algorithm by using java programming language," Journal of Logistical Engineering University, vol. 3, 2006.

[5] C. Adams and S. Lloyd, Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional, 2003.

| | |
|---|---|
| **XÁC NHẬN CỦA** | ***TP.Hồ Chí Minh, ngày 10 / tháng 11 / năm 2021*** |
| **GIẢNG VIÊN HƯỚNG DẪN** | **NHÓM SINH VIÊN THỰC HIỆN** |
| *(Ký và ghi rõ họ tên)* | *(Ký và ghi rõ họ tên)* |

# MỤC LỤC

# DANH SÁCH CÁC HÌNH

# DANH SÁCH CÁC BẢNG

# DANH MỤC CÁC TỪ VIẾT TẮT

| STT | Ký hiệu | Diễn giải |
|---|---|---|
| 1 | FAQ | Frequently Asked Questions |
| 2 | e-Signature | Electronic Signature |
| 3 | PKI | Public key Infrastructure |
| 4 | CA | Certificate Authority |

# TÓM TẮT BÁO CÁO

Báo cáo đề tài tốt nghiệp là tài liệu chính của thực tập dự án tốt nghiệp, nội dung của báo cáo sẽ đề cập tới các kiến thức, kỹ thuật liên quan trong quá trình thực hiện đồ án. Báo cáo bao gồm các phần như sau:

Chương 1 – Giới thiệu: Giới thiệu về đề tài, trình bày lý do xây dựng hệ thống ký kết văn bản trực tuyến. Trình bày nhận xét 3 hệ thống ký kết văn bản tiêu biểu. Mô tả chi tiết các chức năng chính của hệ thống. Nêu ra mục tiêu, phạm vi phát triển đề tài về hệ thống của nhóm.

Chương 2 – Lý thuyết nền tảng: Trình bày các khái niệm về Chữ ký số, Chữ ký điện tử. Tìm hiểu các quy trình ký kết văn bản trong đời sống thực, bằng máy tính. Bên cạnh đó đề cập đến phương pháp ký kết văn bằng bằng Chữ ký số, bằng cách định danh.

Chương 3 – Giải pháp đề tài:

Chương 4 – Cài đặt và triển khai:

Chương 5 – Tổng kết và đánh giá: Phần này sẽ liệt kê các kiến thức mà nhóm đạt được trong quá trình thực hiện luận văn, sản phẩm và những chức năng thu được từ quá trình thực hiện. Trong chương này còn so sánh ứng dụng của luận văn với một số ứng dụng hiện có trên thị trường, phương hướng phát triển trong tương lai trong ứng dụng.

# Chương 1

# GIỚI THIỆU

## 1.1 Giới thiệu đề tài

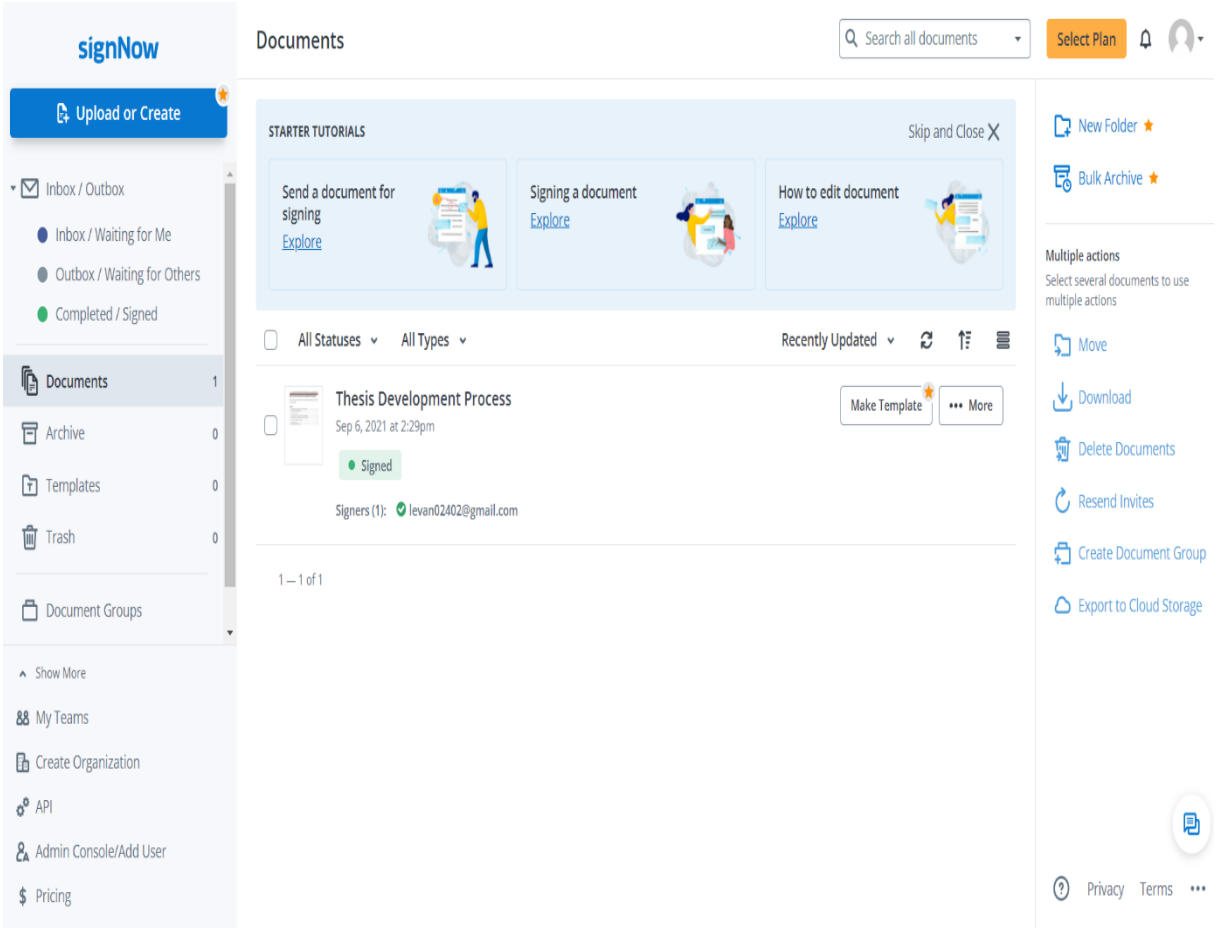
Hiện nay, khi mà mọi vấn đề trong cuộc sống đều có thể giải quyết bằng ứng dụng công nghệ và số hóa thông tin. Chữ ký điện tử được sử dụng rộng rãi và nhiều người biết đến, cụ thể trong các giao dịch điện tử. Các ứng dụng hiện có trên thị trường rất đa dạng, với nhiều tính năng kèm theo và có thể mang nặng tính chất kinh doanh quảng cáo. Bên cạnh đó, chức năng và nhu cầu của người sử dụng không nhiều, các hệ thống chữ ký điện tử phổ biến hầu hết tập trung vào thị trưởng Mỹ và nước ngoài. Dẫn đến bất cập không hỗ trợ ngôn ngữ tiếng việt, nhiều chức năng thừa và không được sử dụng tại quốc gia Việt Nam, yêu cầu thẻ thanh toán trực tuyến quốc tế khi đăng ký, bản quyền giá cao khi quy đổi ngoại tệ tiền Việt Nam. Vì thế chúng tôi muốn tạo ra một hệ thống ký kết văn bản trực tuyến, tập trung thị trường trong nước, ưu tiên sự tối giản, nhanh gọn. Tên là VTSign – Hệ thống ký kết văn bản trực tuyến (Building e-signature system).

## 1.2 Khảo sát thị trường

### 1.2.1 "SignNow" do airSlate Inc phát triển

**Giới thiệu**

SignNow là nhà cung cấp công nghệ chữ ký điện tử được phát triển tại Hoa Kỳ. Nền tảng phần mềm dưới dạng dịch vụ của công ty cho phép các cá nhân và doanh nghiệp ký, quản lý tài liệu từ bất kỳ máy tính nào. Sản phẩm được cung cấp miễn phí trên các thiết bị iPhone, iPad và Android, cho phép tải lên tài liệu từ tài khoản email, máy ảnh hoặc Dropbox của điện thoại thông minh và nhấn để chèn chữ ký.

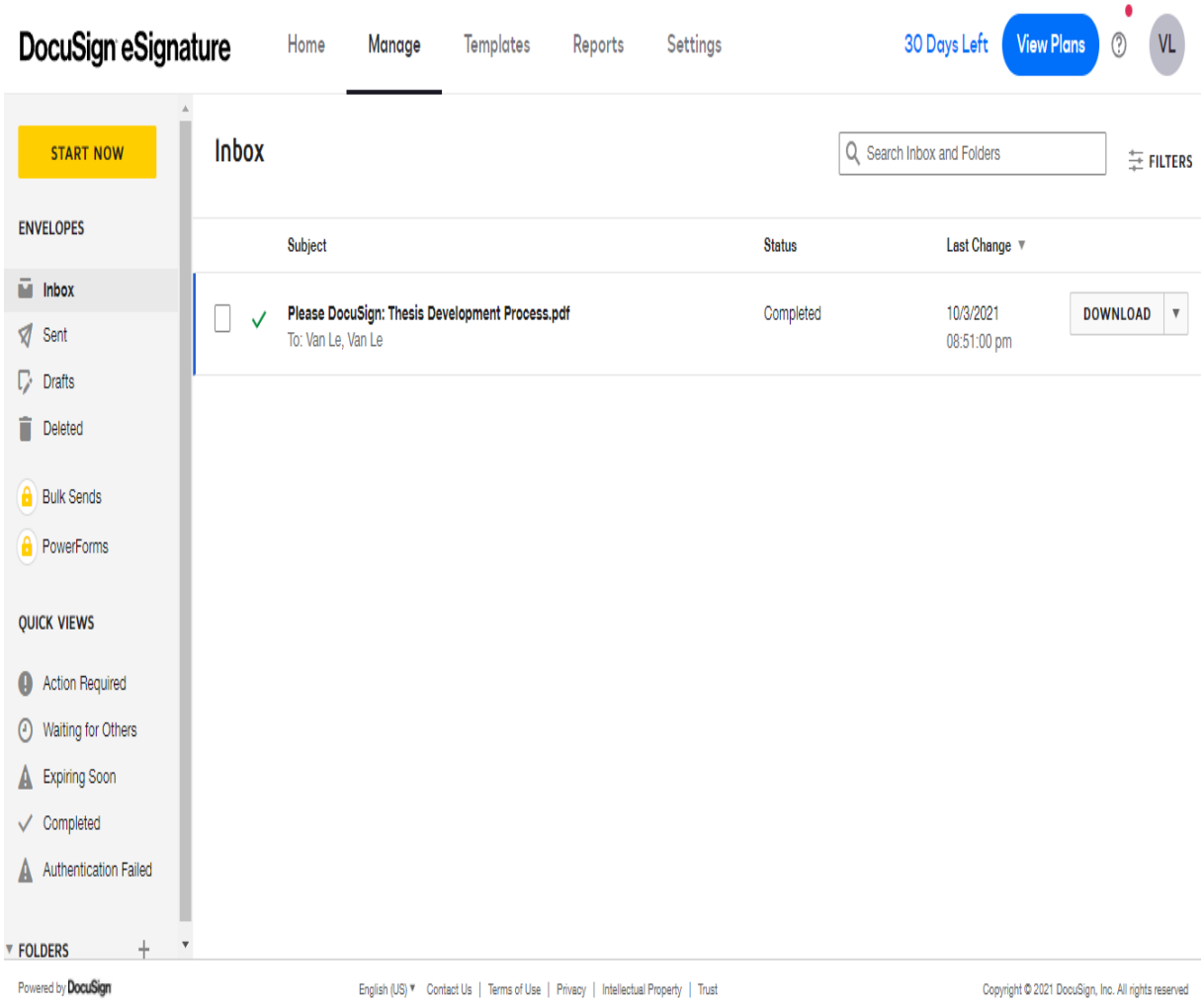



Hình 1-1: Màn hình sau khi đăng nhập hệ thống SignNow [1]

### 1.2.2 "DocuSign" do DocuSign Inc phát triển

**Giới thiệu**

DocuSign là hãng công nghệ tiên phong và đứng số 1 trong mảng chữ ký điện tử trên thế giới. Cung cấp giải pháp e-signature cho 500.000 doanh nghiệp và hàng trăm triệu người dùng tại 180 quốc gia toàn cầu. Cung cấp chữ ký an toàn và đơn giản cho các văn bản điện tử và thu thập chữ ký từ những tài liệu khác. Ứng dụng loại bỏ hết sự phức tạp, chi phí và thiếu an toàn trong in ấn, fax, scan các tài liệu cho việc ký kết.

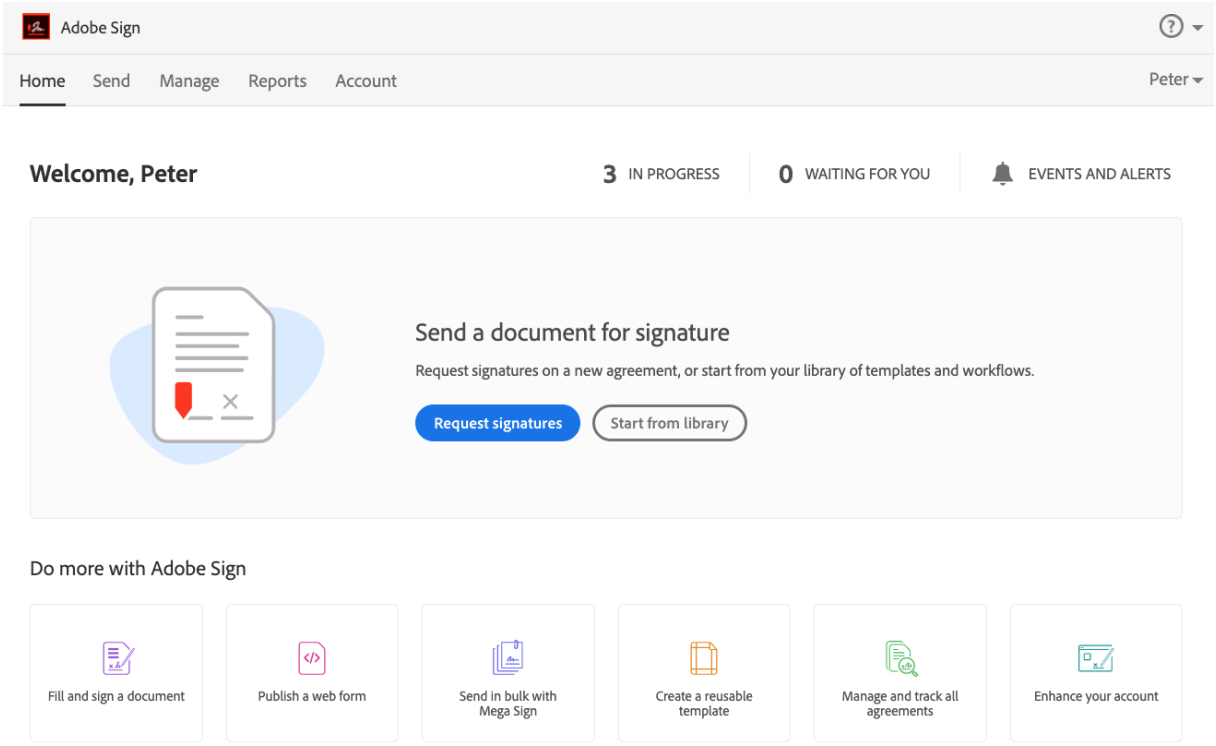



Hình 1-2: Màn hình sau khi đăng nhập hệ thống DocuSign [2]

### 1.2.3 "AdobeSign" do Adobe Inc phát triển

**Giới thiệu**

AdobeSign là một dịch vụ dựa trên đám mây cho phép một cá nhân hoặc tổ chức gửi, bảo mật, theo dõi và quản lý các chữ ký điện tử có quy trình (từ khi gửi tài liệu cho đến khi kết thúc bằng chữ ký). Dịch vụ này nhằm thay thế chữ ký giấy và mực in vật lý bằng một giải pháp thay thế điện tử hoàn toàn tự động. AdobeSign được phát triển bởi nền tảng EchoSign.




Hình 1-3: Màn hình sau khi đăng nhập hệ thống AdobeSign [3]

### 1.2.4 So sánh nhận xét 4 hệ thống ký kết văn bản

Bảng 1-1 So sánh các tính năng ký kết cơ bản của 4 hệ thống

| Tính năng | SignNow | AdobeSign | DocuSign | VTSign |
|---|---|---|---|---|
| Gửi tài liệu cần ký | ✓ | ✓ | ✓ | ✓ |
| Mời ký số lượng lớn | ✓ | ✓ | ✓ | ✓ |
| Chỉnh sửa tài liệu trước khi gửi | ✓ | ✓ | ☒ | ☒ |
| Tạo các mẫu có thể sử dụng lại | ✓ | ✓ | ✓ | ✓ |
| Thêm thương hiệu được cá nhân hóa | ✓ | ✓ | ✓ | ☒ |
| Gửi lời mời qua liên kết | ✓ | ✓ | ✓ | ✓ |
| Ký kết trực tiếp | ✓ | ☒ | ☒ | ✓ |
| Xác định các loại chữ ký được phép | ✓ | ☒ | ☒ | ☒ |
| Trò chuyện trực tiếp | ✓ | ✓ | ☒ | ☒ |
| Bảo vệ mối đe dọa nâng cao | ✓ | ☒ | ✓ | ✓ |
| Quản lý tài liệu có thời hạn | ✓ | ☒ | ✓ | ✓ |

Bảng 1-2 Ưu điểm và khuyết điểm của 4 hệ thống ký kết

| Hệ thống | Ưu điểm | Khuyết điểm |
|---|---|---|
| **SignNow** | - Đăng nhập/đăng ký nhanh bằng tài khoản Facebook, Google.<br>- Hệ thống sử dụng eSignature đơn giản, giao diện hiện đại dễ sử dụng, có LiveChat hỗ trợ khách hàng.<br>- Bản dùng thử không giới hạn nhiều chức năng, bản quyền giá hợp lý, phù hợp nhiều đối tượng. | - Hỗ trợ ít ngôn ngữ, tập trung thị trường nước ngoài.<br>- Giao diện trình duyệt chưa có chế độ nền tối.<br>- Không dùng phương pháp Digital Signature, bảo mật còn hạn chế. |
| **DocuSign** | - Sử dụng phương pháp định danh Self-Signed Digital Signature, không đòi hỏi người dùng trả tiền mua Chứng thực (Certificate).<br>- Sử dụng các công nghệ mã hóa và bảo mật dữ liệu, thông báo qua tin nhắn (SMS Delivery).<br>- Phù hợp với các công ty quy mô lớn, đặt nặng về bảo mật chuyên môn.<br>- Nhiều công cụ hỗ trợ kèm theo, đáp ứng nhiều tiêu chuẩn bảo mật. | - Không có đăng nhập/đăng ký nhanh bằng tài khoản Facebook, Google.<br>- Hệ thống nặng, truy cập chậm ở khu vực Việt Nam, không có LiveChat.<br>- Không được chỉnh sửa tài liệu trước khi gửi và ký kết trực tiếp.<br>- Hỗ trợ ít ngôn ngữ, tập trung thị trường Mỹ, bản quyền giá cao. |

| | | |
|---|---|---|
| **AdobeSign** | - Sử dụng phương pháp Digital Signature, đòi hỏi người dùng trả tiền mua 1 Chứng thực (Certificate).<br>- Đồng bộ và cá nhân hóa với phần mềm liên quan của Adobe. | - Đăng nhập/đăng ký phức tạp, hệ thống khá chậm và tải nhiều thông tin và thông báo.<br>- Giao diện cũ khó nhìn, nhiều tính năng thừa và khó sử dụng, Không ký trực tiếp.<br>- Bản quyền và phí sử dụng cao, bản dùng thử nhiều ràng buộc chức năng. |
| **VTSign** | - Hệ thống xử lý và hiển thị nhanh, không hiện các thông báo gây nhiễu.<br>- Bảo mật tài liệu, xác thực người dùng bằng email và số điện thoại cá nhân.<br>- Giao diện thao tác đơn giản dễ sử dụng, phù hợp nhiều lứa tuổi.<br>- Hỗ trợ ngôn ngữ tiếng việt, bản quyền sử dụng phù hợp người Việt Nam. | - Không có đăng nhập/đăng ký nhanh bằng tài khoản Facebook, Google.<br>- Không chỉnh sửa tài liệu trước khi gửi, không LiveChat, không hỗ trợ nhiều ngôn ngữ.<br>- Phù hợp với người dùng cá nhân, các tổ chức nhỏ, không chuyên môn cao. |

## 1.3 Lý do lựa chọn đề tài

Hiện nay, xã hội và công nghệ đang ngày càng phát triển không ngừng, kéo theo nhu cầu rất cao của con người hiện đại. Tần suất xử lý các công việc và tác vụ ngày càng lớn, luôn yêu cầu phải áp dụng công nghệ và số hóa mọi thứ có thể, chúng tôi muốn tạo ra một hệ thống ký kết văn bản trực tuyến trong việc quản lý thao tác thực hiện chữ ký điện tử vào các giao dịch và hợp đồng. Trong quá trình thực hiện đề tài, các thành viên nhóm cũng có cơ hội kiểm tra xem tự mình có thể thực hiện một dự án thực tế từ khi bắt đầu đến khi kết thúc hay không. Đồng thời đánh giá được khả năng sẽ hợp với vai trò

nào trong một dự án thực tế giúp ích cho các dự án thương mại sau khi tốt nghiệp. Nâng cao kỹ năng giải quyết vấn đề, kỹ năng tự nghiên cứu và tìm hiểu, viết tài liệu báo cáo một cách bài bản. Đồ án tốt nghiệp này là sự tổng hợp và ứng dụng các kiến thức của nhóm tích lũy được trong suốt thời gian học tập và nghiên cứu tại trường. Quá trình thực hiện đề tài cũng hỗ trợ chúng tôi làm quen với mô hình quản lý dự án Kanban. Bên cạnh đó, các hệ thống chữ ký điện tử nổi tiếng trên thị trường rất nhiều, các chức năng thừa ít sử dụng, kèm theo tính chất kinh doanh quảng cáo sản phẩm đặc thù riêng của mỗi công ty. Tập trung nhiều vào thị trường nước ngoài, với người Việt Nam nói riêng hay người dùng cơ bản nói chung rất khó sử dụng thành thạo và nhanh chóng. Vì thế kết quả hướng tới của nhóm là tạo ra được một hệ thống đơn giản dễ sử dụng, tiếp cận được với nhiều người hơn.

## 1.4 Mục tiêu thực hiện

**Thiết kế, xây dựng, kiểm thử, và triển khai hệ thống.**

- Back-end: Cung cấp các API bao gồm: cho phép người dùng đăng ký, và thanh toán chi phí sử dụng dịch vụ, cho phép người quản trị quản lý người sử dụng dịch vụ, xử lý việc quản lý và ký kết văn bản, cung cấp các báo cáo cho admin về quá trình truy cập và báo cáo cho người dùng về quá trình truy cập, dung lượng sử dụng của từng người dùng sử dụng, dung lượng sử dụng của tài khoản. Áp dụng Microservices, mô phỏng, thiết kế, thực hiện, báo cáo kết quả các kịch bản kiểm thử khả năng tải mong muốn (load tests), khả năng chịu tải tối đa (stress tests), khả năng xâm nhập hệ thống (penetration testing).
- Front-end: Các giao diện kết nối với các tính năng tương ứng với back-end, đơn giản dễ dàng thao tác và phù hợp với nhiều đối tượng người dùng sử dụng.

**Viết 80 trang Đồ án.**

## 1.5 Yêu cầu chức năng

Nhóm đề xuất các chức năng mà một hệ thống ký kết văn bản trực tiếp cần phải đáp ứng như sau. Bao gồm người gửi, người nhận, hành động thực hiện và mô tả.

Bảng 1-3: Mô tả chi tiết các chức năng của hệ thống

| STT | Đối tượng | Hành động | Mô tả |
|---|---|---|---|
| 1 | Khách hàng xem trang web | Tạo tài khoản cá nhân | Lưu trữ thông tin cá nhân, đăng nhập vào hệ thống |
| 2 | Người đã có tài khoản | Đăng nhập tài khoản | Bắt đầu sử dụng tài khoản và các chức năng trong hệ thống |
| 3 | Người đã có tài khoản | Tạo chữ ký cá nhân | Để thực hiện việc ký kết văn bản, yêu cầu bắt buộc |
| 4 | Người đã có tài khoản | Tạo tài liệu, tải lên các tài liệu để ký kết | Để những bên liên quan có thể cùng ký lên tài liệu |
| 5 | Chủ tài liệu | Nhập thông tin người nhận gồm họ và tên, email | Gửi tài liệu đúng người nhận |
| 6 | Chủ tài liệu | Cài đặt quyền cho người nhận | Tùy chọn có người nhận có thể ký và có người nhận chỉ được phép xem tài liệu |
| 7 | Chủ tài liệu | Ký tài liệu đã tải lên | Ký tên vào tài liệu đã tải lên |
| 8 | Chủ tài liệu | Cài đặt tài liệu | Đánh đánh dấu chỗ người nhận cần ký và các thông tin khác |
| 9 | Chủ tài liệu | Gửi lời nhắn cho các đối tác qua email | Để có thể thông báo về tài liệu cho người nhận |
| 10 | Người nhận tài liệu | Nhận được email có chứa đường dẫn đến tài liệu cần ký | Xem được tài liệu cần ký trực tiếp |
| 11 | Người nhận tài liệu | Đăng nhập trước khi ký tài liệu | Đảm bảo việc xác thực người ký tài liệu |

| | | | |
|---|---|---|---|
| 12 | Người nhận tài liệu | Ký tài liệu được nhận | Ký tên lên tài liệu đối tác gửi |
| 13 | Người nhận tài liệu | Nhận email xác nhận đã ký tài liệu | Để có thể xem lại tài liệu đã vừa ký |
| 14 | Chủ tài liệu | Nhận được email thông báo đối tác đã ký tài liệu | Biết được trạng thái tài liệu của người gửi đã được ký |
| 15 | Người đã có tài khoản | Quản lý các tài liệu của tài khoản gồm các tài liệu đã ký, cần ký, đã xóa | Để có thể quản lý các tài liệu của chủ tài khoản |
| 16 | Người đã có tài khoản | Xem tổng quát các tài liệu yêu cầu về số lượng | Có cái nhìn tổng quát và có thể truy cập tới những tài liệu đó dễ dàng |
| 17 | Thanh tra | Mọi thay đổi đều phải ghi lại | Để thanh tra lại mọi thay đổi |
| 18 | Nhà quản trị hệ thống | Nhận được thông báo ngay khi hệ thống gặp sự cố | Để kịp thời xử lý nhanh chóng |
| 19 | Người đã có tài khoản | Tùy chỉnh chữ ký, tải lên chữ ký | Tạo chữ ký theo ý thích của chủ tài khoản và sử dụng chúng khi cần ký văn bản |
| 20 | Người đã có tài khoản | Tạo bản mẫu | Tạo bản cho riêng và lưu trữ lại để sử dụng chúng khi cần |
| 21 | Người đã có tài khoản | Đăng xuất | Để đảm bảo không ai có thể sử dụng tài khoản khi không dùng đến |
| 22 | Người đã có tài khoản | Thay đổi Thông tin tài khoản | Chủ tài khoản thay đổi các thông tin của mình khi cần |

| | | | |
|---|---|---|---|
| 23 | Người đã có tài khoản | Quản lý các bản mẫu đã tạo như sửa, xóa | Điều chỉnh lại bản mẫu khi cần |
| 24 | Người đã có tài khoản | Tải tài liệu đã hoàn thành xuống máy tính | Tải tài liệu lưu trữ trên thiết bị hoặc in ra giấy nếu cần |
| 25 | Khách hàng xem trang web | Thông tin giới thiệu website | Khách hàng biết đucợ được trang web hỗ trợ mình những gì |
| 26 | Khách hàng xem trang web | Chuyên mục FAQ | Khách hàng tìm kiếm nhanh những giải pháp cho vấn đề thường gặp |
| 27 | Khách hàng xem trang web | Thông tin liên hệ của website | Khách hàng tìm được thông tin liên lạc khi cần sự hỗ trợ |

## 1.6 Phạm vi đề tài

**Các tính năng không thực hiện**

- Các chức năng tự động hóa được thiết lập riêng. Thanh toán trực tuyến thông qua ngân hàng. Bản quyền và giới hạn sử dụng.
- Đồng bộ vào trên các phần mềm bên thứ ba ví dụ như Dropbox, Word, Adobe. Triển khai trên tất cả nền tảng khác.
- Chức năng phức tạp chuyên môn cao như công chứng và chống giả mạo, mã hóa tài liệu và bảo mật cao. Chức năng kiểm toán thống kê đánh giá đặc thù.
- Giao diện có nhiều tùy chọn thay đổi như quốc gia và vùng, ngôn ngữ. Tùy chọn ẩn hay hiện mục và các chức năng trên hệ thống.
- Thêm các thương hiệu logo được cá nhân hóa. Xác định các loại chữ ký được phép. Hệ thống live chat trò chuyện trực tiếp trên hệ thống.

# Chương 2

# LÝ THUYẾT NỀN TẢNG

## 2.1 Các khái niệm liên quan tới Chữ ký số Chữ ký điện tử

### 2.1.1 Chữ ký số - Digital signatures

**Định nghĩa**

- Chữ ký số là một loại của chữ ký điện tử (electronic signatures), một tập hợp các ký tự (characters) được thêm vào cuối tài liệu hoặc phần nội dung của thông điệp (message) bằng cách áp dụng các thuật toán mật hóa (cryptographic algorithms) để xác nhận hoặc thể hiện tính hợp lệ và bảo mật. Được sử dụng để xác định người đưa ra thông điệp và tính xác thực tài liệu không bị sửa đổi so với bản gốc [7].

**Các thành phần**

- Key generation: khóa công khai và khóa cá nhân tương quan của người dùng.
- Signing: tin nhắn tương ứng được ký bởi người dùng bằng khóa riêng của họ.
- Verification: chữ ký cho một thông điệp (message) được cung cấp dựa trên khóa công khai được xác minh.
- Hash Function: hàm băm đại diện cho một tập hợp các số và chữ cái được tạo ra từ một thuật toán được sử dụng bởi phần mềm chữ ký điện tử là duy nhất cho một tài liệu. Xây dựng theo một chiều (one-way), không thể đảo ngược (reversed) để tìm các tệp khác sử dụng các giá trị tương tự.
- Key cryptology: đại diện cho phương pháp mật mã (cryptographic) được sử dụng để tạo tập hợp các khóa công khai và riêng tư được liên kết với một tài liệu.
- Public Key Infrastructure (PKI): cơ sở hạ tầng khóa công khai là một tập hợp các yêu cầu cho phép tạo ra chữ ký số. Thông qua PKI, mỗi giao dịch chữ ký số bao gồm một cặp khóa: khóa riêng tư và khóa công khai. Khóa riêng tư không được chia sẻ và chỉ được sử dụng bởi người ký để ký điện tử vào các tài liệu. Khóa công khai có sẵn và được sử dụng bởi những người cần xác thực chữ ký điện tử của người ký.

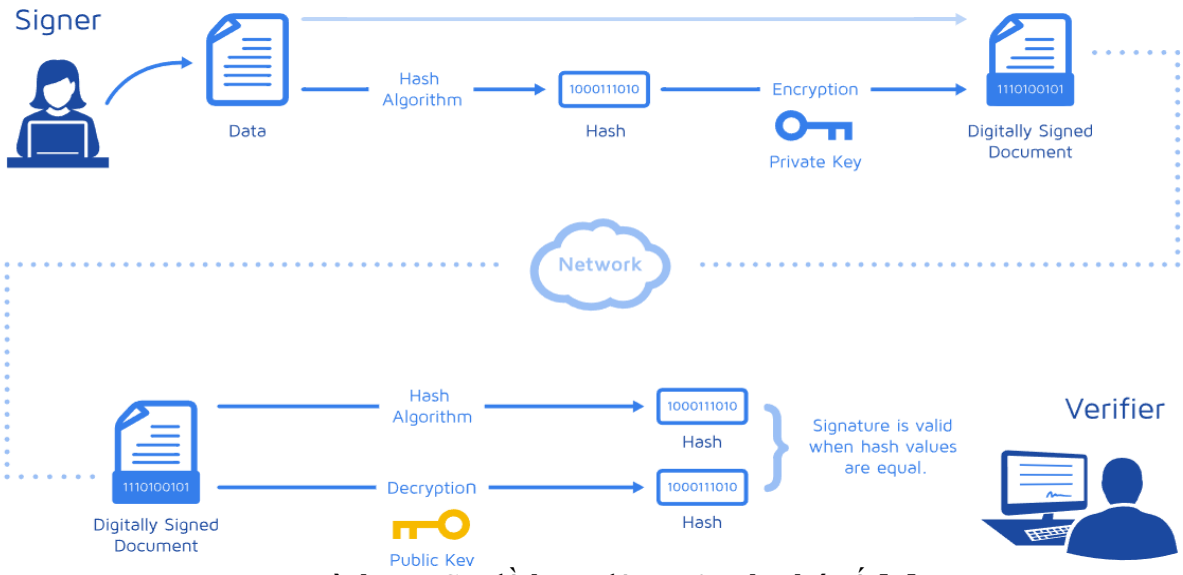
PKI thực thi các yêu cầu bổ sung, như Tổ chức phát hành chứng chỉ (Certificate Authority - CA), chứng chỉ số, phần mềm đăng ký người dùng cuối và các công cụ để quản lý, gia hạn và thu hồi khóa và chứng chỉ.

- Certificate Authority (CA): chữ ký số dựa trên các khóa công khai và riêng tư. Các khóa đó phải được bảo vệ để đảm bảo an toàn và tránh bị giả mạo hoặc sử dụng với mục đích xấu. Khi gửi hoặc ký một tài liệu, cần đảm bảo rằng tài liệu và khóa được tạo một cách an toàn và đang sử dụng khóa hợp lệ. Nhà cung cấp dịch vụ tin cậy CA là các tổ chức bên thứ ba đã được chấp nhận rộng rãi là đáng tin cậy để đảm bảo bảo mật khóa và có thể cung cấp các chứng chỉ kỹ thuật số cần thiết. Cả người gửi và người nhận ký tài liệu phải đồng ý sử dụng một CA nhất định.

**Cách thức hoạt động**

- Chữ ký điện tử, giống như chữ ký viết tay, là duy nhất cho mỗi người ký. Các nhà cung cấp giải pháp chữ ký số phải tuân theo một giao thức cụ thể, được gọi là PKI. PKI yêu cầu nhà cung cấp sử dụng một thuật toán toán học để tạo ra hai dãy mã số, được gọi là khóa. Một khóa là công khai và một khóa là riêng tư [2].
- Khi người ký ký điện tử vào một tài liệu, chữ ký được tạo bằng cách sử dụng khóa riêng của người ký, khóa này luôn được người ký lưu giữ an toàn. Thuật toán toán học hoạt động giống như một mật mã, tạo ra dữ liệu khớp với tài liệu đã ký, được gọi là hàm băm và mã hóa dữ liệu đó. Dữ liệu được mã hóa kết quả là chữ ký điện tử. Chữ ký cũng được đánh dấu bằng thời gian mà tài liệu được ký. Nếu tài liệu thay đổi sau khi ký, chữ ký điện tử sẽ mất hiệu lực [2].
- Để bảo vệ tính toàn vẹn của chữ ký, PKI yêu cầu các khóa phải được tạo, tiến hành và lưu một cách an toàn, yêu cầu các dịch vụ của Tổ chức phát hành chứng chỉ CA đáng tin cậy. Các nhà cung cấp chữ ký số đáp ứng các yêu cầu của PKI về an toàn chữ ký số [2].

- Tùy hệ thống ký kết sẽ đòi hỏi mỗi người dùng phải trả tiền mua 1 chứng chỉ từ một CA tin cậy như hệ thống Adobe Acrobat hoặc bằng cách định danh tự thiết lập CA cho riêng mình như hệ thống DocuSign (Self-Signed Digital Signature). Các hệ thống ký kết văn bản phổ biến hiện nay đều hỗ trợ các CA nổi bật dựa vào tổ chức hay khu vực bao gồm OpenTrust được sử dụng rộng rãi ở các nước thuộc Liên minh Châu Âu, SAFE-BioPharma là chứng chỉ xác thực mà các tổ chức khoa học đời sống hay sử dụng.




Hình 2-1 Sơ đồ hoạt động của chữ ký số [2].

Bước 1: Hệ thống tạo ra cặp chìa khóa (key pair) cho từng tài khoản của người dùng.

Bước 2: Người gửi sẽ ký và tải (upload) tài liệu lên hệ thống.

Bước 3: Sử dụng thuật toán SHA256 để mã hóa tài liệu thành bản tóm tắt (digest).

Bước 4: Hệ thống tiếp tục dùng bản tóm tắt (digest) và khóa riêng tư (private key) của người gửi để tiến hành tạo thành chữ ký số (digital signature).

Bước 5: Người nhận xác nhận danh tính với hệ thống để nhận được tài liệu + khóa công khai (public key) + chữ ký số (digital signature) của người gửi.

Bước 6: Hệ thống giải mã chữ ký điện tử của người nhận cung cấp bằng khóa công khai (public key) → bản tóm tắt (digest) 1 ( nếu không giải mã được thì chữ ký điện tử này là giả mạo).

Bước 7: Hệ thống cũng mã hóa tài liệu của người gửi → bản tóm tắt (digest) 2.

Bước 8: Hệ thống so sánh 2 bản tóm tắt (digest) 1 và 2 để chứng thực.

### 2.1.2 Chữ ký điện tử - Electronic Signatures

- Chữ ký điện tử là một phần dữ liệu đề cập đến dữ liệu điện tử khác và được sử dụng để xác minh người ký tài liệu, rằng danh tính của người ký đã được xác minh và tài liệu đó không thay đổi sau khi chữ ký được thêm vào. Các phương pháp khác nhau để ghi lại chữ ký gồm nhập tên của người ký vào khung chỗ ký bằng cách sử dụng máy tính hoặc ứng dụng di động để chụp ảnh chữ ký viết tay, xác minh qua email, bằng ID công ty hoặc mã PIN điện thoại [8].

### 2.1.3 Sự khác biệt giữa chữ ký số và chữ ký điện tử

Bảng 2-1: So sánh chữ ký điện tử và chữ ký số

| | **Chữ ký số** | **Chữ ký điện tử** |
|---|---|---|
| **Tính chất** | Được mã hóa và chứng thực danh tính người ký. | Biểu tượng, hình ảnh, quy trình được đính kèm với tin nhắn hoặc tài liệu chứng thực danh tính của người ký và hành động. |
| **Tính năng** | Bảo mật một tài liệu | Xác minh một tài liệu |
| **Tiêu chuẩn** | Sử dụng các phương thức mã hoá mật mã dựa trên PKI và đảm bảo danh tính người ký, tính toàn vẹn dữ liệu. | Không phụ thuộc vào các tiêu chuẩn. Không sử dụng mã hóa. |
| **Xác thực** | Kỹ thuật số dựa trên chứng chỉ. | Xác thực danh tính người ký thông qua email, mã pin |
| **Bảo mật** | Độ an toàn bảo mật cao, khó có thể được giả mạo hoặc thay đổi. | Chữ ký dễ bị giả mạo. |

| | | |
|---|---|---|
| **Độc quyền** | Được xác nhận bởi bất kỳ người nào mà không cần phần mềm xác minh độc quyền. | Trong các trường hợp, chữ ký điện tử không được ràng buộc về mặt pháp lý và sẽ yêu cầu phần mềm độc quyền để xác nhận chữ ký điện tử. |
| **Xác nhận** | Được xác nhận bởi các cơ quan chứng nhận hoặc nhà cung cấp dịch vụ tin cậy. | Không có quy trình xác nhận cụ thể rõ ràng nào. |

## 2.2 Ký kết văn bản trong đời sống thực

### 2.2.1 Quy trình ký kết

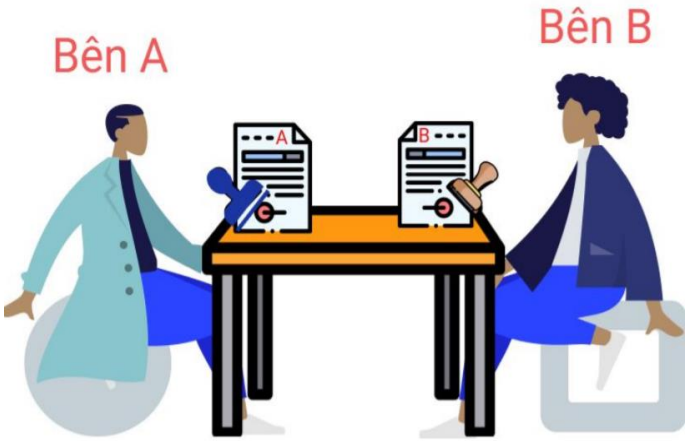
Bước 1: Bên A và bên B đều được chuẩn bị 1 văn bản / hợp đồng cho mỗi bên, cùng với con dấu (nếu có). Cả 2 sẽ hẹn một ngày gặp mặt để ký kết văn bản / hợp đồng.


Hình 2-2 Tiến trình ký kết văn bản đời sống thực – Bước 1

Bước 2: Bên A và bên B ký lên văn bản / hợp đồng của mình.

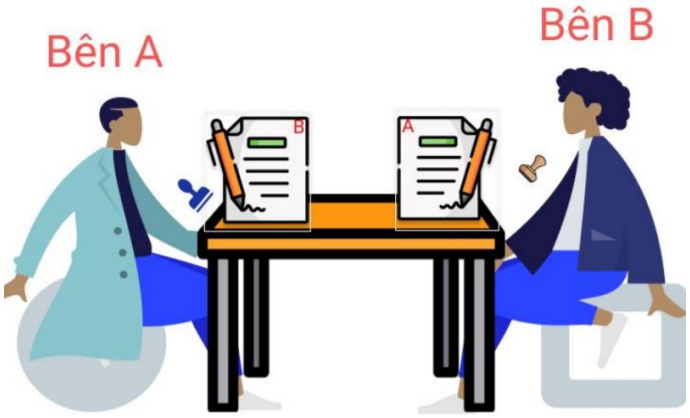

Hình 2-4 Tiến trình ký kết văn bản đời sống thực – Bước 2

Bước 3: Bên A và bên B đóng dấu lên văn bản / hợp đồng của mình.




Hình 2-3 Tiến trình ký kết văn bản đời sống thực – Bước 3

Bước 4: Bên A và bên B ký tên lên văn bản / hợp đồng của đối tác.




Hình 2-5 Tiến trình ký kết văn bản đời sống thực – Bước 4

Bước 5:  Bên A và bên B đóng dấu lên văn bản / hợp đồng của đối tác.


Hình 2-7 Tiến trình ký kết văn bản đời sống thực – Bước 5

Bước 6: Văn bản / hợp đồng sẽ được mang đến văn phòng công chức và 1 số giấy tờ theo yêu cầu. Công chứng viên kiểm tra xem đã đầy đủ giấy tờ theo yêu cầu hay chưa.


Hình 2-6 Tiến trình ký kết văn bản đời sống thực – Bước 6

Bước 7: Công chứng viên sẽ đóng dấu lên văn bản / hợp đồng đó để hoàn tất. Văn bản / hợp đồng này đã có hiệu lực pháp lý.


Hình 2-8 Tiến trình ký kết văn bản đời sống thực – Bước 7

### 2.2.2 Các vấn đề và tình huống xảy ra

### 2.2.3 Các phương pháp xử lý

- Vị trí địa lý của bên A và bên B xa nhau: Xử lý bằng cách thống nhất địa điểm thuận tiện cho cả 2 bên, ví dụ như ở giữa vị trí bên A và bên B, địa điểm lý tưởng phù hợp nhu cầu của cả 2, bên A tới trực tiếp bên B hoặc ngược lại.
- Thời gian ký kết toàn bộ quá trình lâu: Xử lý bằng các cách cử người đại diện như luật sư để thay thế xử lý, chuẩn bị tài liệu đầy đủ và thống nhất 2 bên chắc chắn để không gặp vấn đề phát sinh, mọi bước thực hiện đều được tính tới.
- Hủy hoặc soạn lại văn bản / hợp đồng: Xử lý bằng cách bàn bạc lại văn bản / hợp đồng từ đầu, hoặc có phương án dự phòng như văn bản / hợp đồng thay thế, thống nhất được với nhau thông qua luật sư.
- Thủ tục và chờ đợi văn phòng công chứng lâu: Xử lý bằng cách đặt lịch hẹn trước với phòng công chứng, hoặc làm việc thảo luận với công chứng viên trước đó, sắp xếp thời gian hợp lý để đến.

## 2.3 Ký kết văn bản bằng máy tính

### 2.3.1 Quy trình ký kết

### 2.3.2 Các vấn đề và tình huống xảy ra

### 2.3.3 Các phương pháp xử lý

- Người dùng không biết sử dụng máy tính hoặc hệ thống ký kết: Xử lý bằng cách đào tạo thực hành bởi công ty tổ chức. Hệ thống ký kết văn bản trên thị trường đều có hướng dẫn sử dụng và thao tác đơn giản dễ tiếp cận.
- Bảo mật, an toàn và chứng thực tài liệu: Xử lý bằng cách lựa chọn hệ thống ký kết tin cậy và phổ biến. Áp dụng phương pháp Chữ ký số (Digital Signature) hoặc Chữ ký điện tử (Electronic Signature).
- Nhiều hệ thống ký kết văn bản trên thị trường: Xử lý bằng cách lựa chọn hệ thống uy tín giá cả bản quyền phù hợp nhu cầu. Thống nhất được giữa bên A và bên B và sử dụng cho toàn bộ công ty hoặc tổ chức.

## 2.4 Phương pháp ký kết văn bản bằng Digital Signature

### 2.4.1 Hoạt động

### 2.4.2 Ưu điểm

### 2.4.3 Khuyết điểm

## 2.5 Phương pháp ký kết văn bản bằng cách định danh

### 2.5.1 Hoạt động

### 2.5.2 Ưu điểm

### 2.5.3 Khuyết điểm

# Chương 3
# GIẢI PHÁP ĐỀ TÀI

# Chương 4
# CÀI ĐẶT VÀ TRIỂN KHAI

# Chương 5

# TỔNG KẾT VÀ ĐÁNH GIÁ

## 5.1 Kiến thức thu được

Trong thời gian thực hiện khóa luận, nhóm đã học tập cải thiện bổ sung được thêm nhiều kiến thức. Các kiến thức chuyên môn, kinh nghiệm làm việc nhóm, xử lý các vấn đề gặp phải, giải quyết mâu thuẫn, trao đổi và phát triển dự án, bao gồm:

- Kỹ năng trình bày báo cáo và viết tài liệu một cách bài bản khoa học. Thực hiện đúng các quy chuẩn đề ra. Trích dẫn tài liệu tham khảo cụ thể theo chuẩn, khả năng tổng hợp các kiến thức trên các sách, bài báo về đề tài.
- Khả năng làm việc nhóm, giao tiếp giữa các thành viên. Kỹ năng lên kế hoạch cụ thể theo từng quá trình, phân chia nhiệm vụ hợp lý phù hợp với khả năng của từng thành viên trong nhóm.
- Áp dụng phương pháp quản lý công việc bằng mô hình Kanban, sử dụng công cụ Trello xuyên suốt quá trình thực hiện. Tổng quát rõ ràng công việc, bao gồm các cột tương ứng với trạng thái quá trình đang thực hiện.
- Tinh thần trách nhiệm công việc được giao, thử sức ở nhiều vai trò khác nhau khi xây dựng hệ thống gồm quản lý dự án, kiểm thử, thiết kế giao diện. Tác phong chuyên nghiệp, trình bày báo cáo cho trưởng nhóm và giảng viên hướng dẫn.
- Học hỏi và áp dụng kiến trúc microservice, mô hình CI/CD, thiết kế giao diện sử dụng thư viện mã nguồn mở JavaScript. Khái niệm và kiến thức liên quan đến chữ ký điện tử, chữ ký số, chuẩn hash và thuật toán mã hóa. Quá trình và chức năng đầy đủ của một hệ thống ký kết văn bản.
- Khả năng học hỏi công nghệ và kiến thức mới, kỹ năng viết mã nguồn, tìm kiếm và sửa lỗi, bảo trì và nâng cấp. Kinh nghiệm khắc phục lỗi khi gặp sự cố và triển khai sản phẩm cho người dùng cuối.

## 5.2 Sản phẩm thu được

### 5.2.1 Môi trường phát triển

### 5.2.2 Môi trường triển khai

### 5.2.3 Hiệu năng hệ thống

### 5.2.4 Các chức năng đã cài đặt

### 5.2.5 So sánh chức năng với các hệ thống khác trên thị trường

## 5.3 So sánh kết quả thu được với mục tiêu ban đầu

## 5.4 Định hướng phát triển và nghiên cứu

### 5.4.1 Khả năng mở rộng

### 5.4.2 Cải thiện chức năng

### 5.4.3 Nâng cấp giao diện

### 5.4.4 Sử dụng trên nhiều nền tảng

## 5.5 Lời kết

# PHỤ LỤC 1

# TÀI LIỆU THAM KHẢO


[1] "signNow: eSign PDF with Electronic Signature Online," airSlate Inc, 2021. [Online]. Available: https://www.signnow.com/. [Accessed 04 October 2021].

[2] "DocuSign | #1 in Electronic Signature and Agreement Cloud," DocuSign Inc, 2021. [Online]. Available: https://www.docusign.com/. [Accessed 04 October 2021].

[3] "E-signatures & digital signing software - Adobe," Adobe Inc, 2021. [Online]. Available: https://www.adobe.com/sign.html. [Accessed 04 October 2021].

[4] J. Katz, Digital signatures, Springer Science & Business Media, 2010.

[5] D. Pinkas, Integris, J. Ross and N. Pope, Electronic Signature Formats for long term electronic signatures, The Internet Society, 2001.

[6] Adams, Carlisle, Lloyd and Steve, Understanding PKI: concepts, standards, and deployment considerations, Addison-Wesley Professional, 2003.