TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

Xây dựng hệ thống ký số nội bộ sử dụng công nghệ ký số từ xa

NGÔ SONG VIỆT HOÀNG
hoang.nsv183542@sis.hust.edu.vn

Ngành Khoa học máy tính

Giảng viên hướng dẫn: TS. Đỗ Bá Lâm _____

Chữ kí GVHD

Khoa: Khoa học máy tính

Trường: Công nghệ thông tin và Truyền thông

HÀ NỘI, 02/2023

LỜI CAM KẾT

Họ và tên sinh viên: Ngô Song Việt Hoàng
Điện thoại liên lạc: 0919408976
Email: hoangnsv.183542@sis.hust.edu.vn
Lớp: IT1-01
Hệ đào tạo: Đại học chính quy

Tôi – *Ngô Song Việt Hoàng* – cam kết Đồ án Tốt nghiệp (ĐATN) là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của *tiến sĩ Đỗ Bá Lâm*. Các kết quả nêu trong ĐATN là trung thực, là thành quả của riêng tôi, không sao chép theo bất kỳ công trình nào khác. Tất cả những tham khảo trong ĐATN – bao gồm hình ảnh, bảng biểu, số liệu, và các câu từ trích dẫn – đều được ghi rõ ràng và đầy đủ nguồn gốc trong danh mục tài liệu tham khảo. Tôi xin hoàn toàn chịu trách nhiệm với dù chỉ một sao chép vi phạm quy chế của nhà trường.

Hà Nội, ngày tháng năm

Tác giả ĐATN

Ngô Song Việt Hoàng

LỜI CẢM ƠN

Để hoàn thành được đồ án tốt nghiệp này, em xin gửi lời cảm ơn chân thành đến các thầy cô tại đại học Bách Khoa Hà Nội vì những bài giảng, những kiến thức được truyền tải trong các môn học đã giúp em có được nền tảng kiến thức vững vàng.

Đặc biệt, em xin gửi lời cảm ơn đến tiến sĩ Đỗ Bá Lâm, Trường Công nghệ thông tin và truyền thông, đại học Bách Khoa Hà Nội đã tận tình giúp đỡ, hướng dẫn trong suốt quá trình thực hiện đồ án. Em xin gửi lời cảm ơn đến các thành viên trong BKC Lab đã đồng hành giúp đỡ em trong quá trình làm đồ án.

Cuối cùng, Em xin gửi lời cảm ơn tới gia đình đã luôn là động lực phía sau giúp em có thể vững bước yên tâm học tập để em có được ngày hôm nay.

Em xin chân thành cảm ơn!

TÓM TẮT NỘI DUNG ĐỒ ÁN

Hiện nay hình thức ký tay trong các cơ quan tổ chức đang dần được thay thế bằng việc ký số. Với sự phổ biến của các tài liệu dưới dạng điện tử, việc sử dụng ký số sẽ đảm bảo tính pháp lý tương đương với chữ ký tay đồng thời giúp các tổ chức giảm tải thời gian cho việc xử lý văn bản hành chính. Chữ ký số sẽ đem đến sự an toàn và bảo mật thông tin nhờ vào công nghệ phía sau, chống được khả năng giả mạo cao hơn so với chữ ký tay. Nhận thấy được lợi ích của việc ký số, giải pháp ký số sử dụng USB hoặc SIM đã xuất hiện. Sau khi được triển khai trong thực tế, giải pháp đã phần nào cho thấy được tác dụng của việc ký số. Tuy nhiên, việc sử dụng USB hoặc SIM cho việc ký đã bộc lộ yếu điểm bao gồm chi phí cho một thiết bị để có thể ký được khá cao và sự bất tiện khi luôn phải mang theo thiết bị bên người khi ký.

Do những hạn chế của giải pháp ký số bằng USB hoặc SIM, hướng tiếp cận được lựa chọn trong đồ án tốt nghiệp là công nghệ ký số từ xa. Giải pháp này sẽ loại bỏ thiết bị như USB hoặc SIM bằng thiết bị phổ biến hơn với chúng ta như máy tính, máy tính bảng, điện thoại di động, ... Do đó, giải pháp này đã tiết kiệm được chi phí khi người dùng có thể ký được bằng các thiết bị quen thuộc sẵn có mà không cần phải mua thêm thiết bị mới để có thể ký số. Với việc sử dụng công nghệ ký số từ xa, người sử dụng sẽ có thể ký ở bất cứ đâu chỉ cần có kết nối internet. Trong đồ án tốt nghiệp này, em sẽ tiến hành phân tích và xác định các yêu cầu của một hệ thống ký số nội bộ sử dụng công nghệ ký số từ xa. Trong các phần tiếp theo, đồ án sẽ trình bày việc phân tích thiết kế để xây dựng các chức năng của hệ thống. Thông qua việc triển khai và đánh giá thử nghiệm, hệ thống đã chứng minh được tính hiệu quả trong việc ký số nội bộ làm qui trình số trong các tổ chức trở nên dễ dàng hơn.

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI 1

1.1 Đặt vấn đề 1

1.2 Mục tiêu và phạm vi đề tài 2

1.3 Định hướng giải pháp 2

1.4 Bố cục đồ án 3

CHƯƠNG 2. CÔNG NGHỆ SỬ DỤNG 4

2.1 Tổng quan về công nghệ ký số từ xa 4

2.1.1 Hệ mã hóa bất đối xứng 4

2.1.2 Chữ ký số 4

2.1.3 Public Key Infrastructure 5

2.1.4 Chuẩn eIDAS và chữ ký số từ xa 6

2.1.5 Các công nghệ tích hợp trong ký số từ xa 7

2.2 Hardware Security Module 8

2.3 Softhsm 9

2.4 Hệ quản trị cơ sở dữ liệu Mongodb 9

2.5 Framework cho phát triển phía server 10

2.6 React 10

2.7 Docker 11

2.8 Kubernetes 11

2.9 Time-based one-time password 13

CHƯƠNG 3. KHẢO SÁT VÀ PHÂN TÍCH YÊU CẦU 14

3.1 Phân tích hiện trạng 14

3.1.1 Phân tích dưới góc nhìn người dùng 14

3.1.2 Khảo sát một số sản phẩm sẵn có 14

3.1.3 Kết quả 14
3.2 Tổng quan chức năng 16
3.2.1 Biểu đồ use case tổng quát 16
3.2.2 Biểu đồ use case phân rã quản lý chứng thư 17
3.2.3 Biểu đồ use case phân rã quản lý chữ ký 17
3.2.4 Quy trình nghiệp vụ đơn ký 18
3.2.5 Quy trình nghiệp vụ đồng ký 19
3.3 Đặc tả chức năng 20
3.3.1 Đặc tả use case đơn ký 20
3.3.2 Đặc tả use case đồng ký 21
3.3.3 Đặc tả use case xác thực tài liệu đã ký 21
3.3.4 Đặc tả use case cấp mới chứng thư 22
3.3.5 Đặc tả use case thu hồi chứng thư 22
3.3.6 Đặc tả use case cập nhật chứng thư 23
3.3.7 Đặc tả use case Đăng nhập 23
3.3.8 Đặc tả use case Đăng ký 24
3.4 Yêu cầu phi chức năng 24
CHƯƠNG 4. TRIỂN KHAI VÀ ĐÁNH GIÁ 25
4.1 Thiết kế kiến trúc 25
4.1.1 Lựa chọn kiến trúc phần mềm 25
4.1.2 Thiết kế tổng quan 28
4.1.3 Thiết kế chi tiết gói 29
4.2 Thiết kế chi tiết 30
4.2.1 Thiết kế giao diện 30
4.2.2 Thiết kế lớp 32
4.2.3 Thiết kế cơ sở dữ liệu 36

4.3 Xây dựng ứng dụng 38
4.3.1 Thư viện và công cụ sử dụng 38
4.3.2 Kết quả đạt được 38
4.3.3 Minh họa các chức năng chính 38
4.4 Triển khai 45
4.4.1 Cách thức triển khai 45
4.4.2 Qui trình triển khai 46
4.4.3 Kiểm thử tương thích 47
4.4.4 Đánh giá hiệu năng 48
CHƯƠNG 5. CÁC ĐÓNG GÓP NỔI BẬT 51
5.1 Softhsm 51
5.1.1 Đặt vấn đề 51
5.1.2 Giải pháp 51
5.2 Xử lý tài liệu PDF khi ký 53
5.2.1 Đặt vấn đề 53
5.2.2 Giải pháp 53
5.2.3 Kết quả 53
5.3 Chứng thư công cộng 54
5.3.1 Đặt vấn đề 54
5.3.2 Giải pháp 54
5.3.3 Kết quả 59
CHƯƠNG 6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 60
6.1 Kết luận 60
6.2 Kinh nghiệm, kỹ năng đạt được 60
6.3 Hướng phát triển 61
TÀI LIỆU THAM KHẢO 63

DANH MỤC HÌNH VẼ

Hình 2.1 Các thành phần của chữ ký số [2] 4
Hình 2.2 Vòng đời của chứng thư số [3] 5
Hình 2.3 Các thành phần trong PKI [4] 6
Hình 2.4 Kiến trúc của mô hình ký số từ xa theo chuẩn eIDAS [7] . . . 7
Hình 2.5 Card PCI [8] 8
Hình 2.6 Thiết bị HSM trong thực tế [9] 9
Hình 2.7 Kiến trúc của docker [13] 11
Hình 2.8 Kiến trúc của K8s [15] 12
Hình 2.9 Cách hoạt động của TOTP [16] 13

Hình 3.1 Biểu đồ use case tổng quan 16
Hình 3.2 Biểu đồ use case phân rã quản lý chứng thư 17
Hình 3.3 Biểu đồ use case phân rã quản lý chữ ký 17
Hình 3.4 Biểu đồ hoạt động quá trình đơn ký tài liệu 18
Hình 3.5 Biểu đồ hoạt động quá trình đồng ký tài liệu 19

Hình 4.1 Các thành phần trong SOA [17] 25
Hình 4.2 Kiến trúc ứng dụng 26
Hình 4.3 Thiết kế gói tổng quan 28
Hình 4.4 Thiết kế chi tiết gói 29
Hình 4.5 Thiết kế chi tiết gói của dịch vụ ký 30
Hình 4.6 Thiết kế giao diện đơn ký chưa có tài liệu 30
Hình 4.7 Thiết kế giao diện đơn ký đã có tài liệu tải lên 31
Hình 4.8 Thiết kế giao diện các tài liệu đã ký 31
Hình 4.9 Thiết kế nhóm lớp cho dịch vụ ký 32
Hình 4.10 Thiết kế lớp cho dịch vụ hsm pki 33
Hình 4.11 Thiết kế lớp cho dịch vụ hsm token 33
Hình 4.12 Biểu đồ tuần tự cho dịch vụ ký 34
Hình 4.13 Biểu đồ tuần tự cho dịch vụ xác thực tài liệu 35
Hình 4.14 Biểu đồ tuần tự cho dịch vụ cấp chứng thư 36
Hình 4.15 Giao diện khi chọn đơn ký 39
Hình 4.16 Giao diện khi chọn vẽ chữ ký 39
Hình 4.17 Giao diện khi chọn tải lên chữ ký 39
Hình 4.18 Giao diện khi chọn tải file để ký 40
Hình 4.19 Giao diện tùy chọn chèn ký 40
Hình 4.20 Giao diện totp 41

Hình 4.21 Giao diện khi ký thành công 41
Hình 4.22 Giao diện khi chọn đồng ký 42
Hình 4.23 Giao diện khi tạo đồng ký cho một tài liệu 43
Hình 4.24 Giao diện khi tạo đồng ký cho một tài liệu 43
Hình 4.25 Giao diện khi người dùng được mời tạo đồng ký 44
Hình 4.26 Mô hình triển khai trên môi trường thử nghiệm 45
Hình 4.27 Mô hình triển khai trên môi trường thực tế 45
Hình 4.28 Quá trình thực hiện build tự động trên môi trường staging . . . 46
Hình 4.29 Quá trình thực hiện deploy tự động trên môi trường staging . . 46
Hình 4.30 Biểu đồ thời gian phản hồi với 10 người dùng đồng thời 48
Hình 4.31 Biểu đồ thời gian phản hồi với 100 người dùng đồng thời . . . 49
Hình 4.32 Biểu đồ thời gian phản hồi với 200 người dùng đồng thời . . . 49
Hình 4.33 Biểu đồ thời gian phản hồi với 500 người dùng đồng thời . . . 50

Hình 5.1 Luồng cấp chứng thư và sinh khóa 52
Hình 5.2 Luồng ký tài liệu 52
Hình 5.3 Sử dụng Itext kết hợp với chữ ký từ Softhsm ký ẩn 53
Hình 5.4 Sử dụng Itext kết hợp với chữ ký từ Softhsm ký hiện 54
Hình 5.5 Luồng tích hợp với API VNPT 55
Hình 5.6 HTTP Body của API lấy access token 56
Hình 5.7 Các trường dữ liệu trả về 56
Hình 5.8 Các trường dữ liệu trả về 57
Hình 5.9 HTTP Body của API Lấy thông tin Certificate của khách hàng 57
Hình 5.10 Các trường dữ liệu trả về 57
Hình 5.11 HTTP Body của API ký hash 58
Hình 5.12 Kết quả ký với chứng thư công cộng 59