Trường Đại học Bách Khoa Hà Nội

Viện Công nghệ Thông Tin và Truyền Thông

Đồ án Tốt nghiệp Đại học

THIẾT BỊ USB TOKEN

|  |  |
| --- | --- |
| Sinh viên thực hiện | Hoàng Viết Huy |
| Người hướng dẫn | ThS. Phạm Ngọc Hưng |

­­

Hà Nội, 04/2019

**PHIẾU GIAO NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP**

**1. Thông tin về sinh viên**

Họ và tên sinh viên: Hoàng Viết Huy

Điện thoại liên lạc: 0976986858 Email: hvhuybk@gmail.com.

Lớp: An toàn thông tin K59 Hệ đào tạo: Đại học chính quy

Thời gian làm ĐATN: Từ ngày 23/01/2019 đến 19/05/2019

**2. Mục đích nội dung của ĐATN**

* Tìm hiểu việc firmware cho dòng thiết bị tương ứng
* Xây dựng một ứng dụng Windows cho phép ký file bằng chữ ký từ thiết bị.

**3. Các nhiệm vụ cụ thể của ĐATN**

* Tìm hiểu việc lập trình firmware cho dòng thiết bị tương ứng.
* Tìm hiểu giao thức giao tiếp USB giữa vi điều khiển và PC Windows.
* Tìm hiểu lập trình Winform giao diện trên Windows
* Tìm hiểu phương pháp ký tài liệu bằng chữ ký điện tử.
* Tổng kết và đánh giá.

**4. Lời cam đoan của sinh viên:**

Tôi – Hoàng Viết Huy - cam kết ĐATN là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của *ThS Phạm Ngọc Hưng*.

Các kết quả nêu trong ĐATN là trung thực, không phải là sao chép toàn văn của bất kỳ công trình nào khác.

|  |  |
| --- | --- |
|  | *Hà Nội, ngày 24 tháng 05 năm 2018*  Tác giả ĐATN  *Hoàng Viết Huy* |

**5. Xác nhận của giáo viên hướng dẫn về mức độ hoàn thành của ĐATN và cho phép bảo vệ:**

|  |  |
| --- | --- |
|  | *Hà Nội, ngày 24 tháng 05 năm 2018*  Giáo viên hướng dẫn  *ThS Phạm Ngọc Hưng* |

**LỜI CẢM ƠN**

Để có thể hoàn thành đồ án tốt nghiệp này, em xin gửi lời cảm ơn chân thành nhất tới tập thể các thầy giáo, cô giáo trường Đại học Bách Khoa Hà Nội nói chung, viện Công nghệ thông tin và truyền thông nói riêng, đã đào tạo cho em những kiến thức, những kinh nghiệm quý báu trong suốt thời gian học tập và rèn luyện.

Em xin gửi lời cảm ơn tới thầy giáo, ThS. Phạm Ngọc Hưng - Giảng viên bộ môn Kỹ thuật máy tính, viện Công nghệ thông tin và truyền thông, trường Đại học Bách Khoa Hà Nội đã tận tình hướng dẫn em trong quá trình làm đồ án tốt nghiệp.

Tiếp theo, em xin gửi lời cảm ơn chân thành tới toàn thể các anh chị trong công ty An ninh mạng Viettel đã giúp đỡ rất nhiệt tình và tạo mọi điều kiện tốt nhất trong suốt quá trình em làm và hoàn thành đồ án tốt nghiệp tại công ty.

Cuối cùng là lời cảm ơn chân thành nhất tới những người thân thân trong gia đình, bạn bè đã luôn ở bên động viên, góp ý và tạo mọi điều kiện tốt nhất để tôi có thể hoàn thành đồ án tốt nghiệp này.

Tuy nhiên, do thời gian và kiến thức có hạn nên đồ án này chắc chắn không tránh khỏi những thiếu sót, em rất mong được sự đóng góp ý kiến của các thầy, các cô và toàn thể các bạn. Em xin chân thành cảm ơn.

Hà Nội ngày 23 tháng 5 năm 2012

Sinh viên: Hoàng Viết Huy

**TÓM TẮT NỘI DUNG ĐỒ ÁN TỐT NGHIỆP**

Hiện nay, công nghệ thẻ thông minh có thể tạo ra một môi trường an toàn để lưu trữ khóa bí mật và thực thi các thao tác mật mã. Thiết bị USB Token dựa trên công nghệ thẻ thông minh tạo ra môi trường lưu trữ và tính toán cách ly an toàn và không thể nhân bản được nên không thể bị sao chép hoặc làm giả.

Token được sử dụng để kê khai nộp thuế trực tuyến, kê khai hải quan điện tử, giao dịch ngân hàng điện tử, giao dịch chứng khoán điện tử, Cổng thông tin một cửa quốc gia, cơ quan hành chính… mà không phải in các tờ kê khai, đóng dấu đỏ của công ty và gần đây token còn được sử dụng để giao dịch trong lĩnh vực kê khai bảo hiểm xã hội điện tử.

Từ nhu cầu trên, và mong muốn mang lại một sản phẩm có ý nghĩa và có tính ứng dụng cao đã dẫn em đến ý tưởng xây dựng thiết bị USB Token có các chức năng an toàn, mà không phụ thuộc vào các thiết bị có sẵn trên thị trường, giúp giảm giá thành sản phẩm.

Với những lý do trên, em quyết định chọn đồ án tốt nghiệp của mình là “**Xây dựng thiết bị USB Token**”.

Mục tiêu chính của đồ án là nghiên cứu công nghệ nhúng, lập trình nhúng, xây dựng kịch bản giao tiếp thiết bị với Windows. Ứng dụng công nghệ này có thể dùng cho các việc sử dụng khóa riêng cho các yêu cầu như bảo đảm tính bí mật và tính toàn vẹn của dữ liệu. Ứng dụng USBTokenManager dùng để đảm bảo tính toàn vẹn dữ liệu bằng cách sử dụng khóa bí mật để ký chữ ký điện tử lên các file văn bản, để đảm bảo chữ ký này là duy nhất và không thể giả mạo.

Nội dung chính đồ án bao gồm :

**PHẦN I: NỀN TẢNG VÀ CÔNG NGHỆ PHÁT TRIỂN HỆ THỐNG**

Chương này tập trung đề cập đến thực trạng việc sử dụng Token CA và sự cần thiết về thiết bị Token CA. Các giải pháp đưa ra để giải quyết thực trạng này.

Chương này thực hiện khảo sát các công nghệ nhúng dùng trong thiết bị Token CA hiện có dùng để xác thực các thông tin cá nhân của người dùng như: thẻ RFID, thẻ từ, thẻ thông minh, thiết bị USB... Chương này cũng đề xuất giải pháp sẽ sử dụng lưu khóa bí mật: thiết bị USB. Cuối cùng là khảo sát các linh kiện cần thiết có thể sử dụng để xây dựng thiết bị USB.

**Chương II: Thiết kế và xây dựng phần cứng**

* Chương này tập trung vào đưa ra khảo sát các thiết bị phần cứng hiện tại và đề xuất công nghệ nhúng sử dụng:
* Phần đầu chương giới thiệu, khảo sát các công nghệ nhúng dùng trong thiết bị Token CA hiện có như: thẻ RFID, thẻ từ, thẻ thông minh, thiết bị USB.
* Tiếp theo, đề xuất giải pháp sẽ sử dụng lưu khóa bí mật: thiết bị USB
* Khảo sát các linh kiện cần thiết có thể sử dụng để xây dựng thiết bị USB.
* Cuối cùng là thiết kế mạch cho thiết bị.

**Chương II: Xây dựng giải pháp và thiết kế phần sụn (Firmware)**

* Phần đầu của chương này sẽ tập trung khảo sát giải pháp giao tiếp giữa thiết bị và ứng dụng Windows, sau đó đề xuất giải pháp giao tiếp sử dụng WinUSB.
* Phần tiếp theo của chương sẽ xây dựng kịch bản giao tiếp giữa firmware và ứng dụng Windows.

**Chương III: Xây dựng giải pháp và kịch bản giao tiếp giữa firmware và ứng dụng trên Windows**

Phần đầu của chương này sẽ tập trung khảo sát giải pháp giao tiếp giữa thiết bị và ứng dụng Windows, sau đó đề xuất giải pháp giao tiếp sử dụng WinUSB.

Phần tiếp theo của chương sẽ xây dựng kịch bản giao tiếp giữa firmware và ứng dụng Windows.

**Chương IV: Xây dựng giao diện và demo một ứng dụng chữ ký điện tử.**

* Chương này tập trung vào việc đánh giá kết quả đạt được, đưa ra phương hướng phát triển cho hệ thống sau khi kết thúc đồ án và phần kết luận.

**MỤC LỤC**

[**PHIẾU GIAO NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP 2**](#_Toc515323278)

[**LỜI CẢM ƠN 3**](#_Toc515323279)

[**TÓM TẮT NỘI DUNG ĐỒ ÁN 4**](#_Toc515323280)

[**MỤC LỤC 5**](#_Toc515323281)

[**DANH MỤC CÁC BẢNG 7**](#_Toc515323282)

[**DANH MỤC HÌNH VẼ 8**](#_Toc515323283)

[**DANH MỤC CÁC TỪ VIẾT TẮT VÀ THUẬT NGỮ 9**](#_Toc515323284)

[**PHẦN I: NỀN TẢNG VÀ CÔNG NGHỆ PHÁT TRIỂN HỆ THỐNG 10**](#_Toc515323285)

[1.1. Tổng quan 10](#_Toc515323286)

[1.1.1. Các vấn đề, khó khăn hiện tại 10](#_Toc515323287)

[1.1.2. Mục tiêu cần đạt được 11](#_Toc515323288)

[1.1.3. Lựa chọn và định hướng thiết kế 12](#_Toc515323289)

[1.2. Yêu cầu về thiết bị 13](#_Toc515323290)

[1.3. Công nghệ sử dụng 13](#_Toc515323291)

[1.3.1. Framework ASP.NET MVC 13](#_Toc515323292)

[1.3.2. Hệ quản trị CSDL SQL Server 15](#_Toc515323293)

[**PHẦN II: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 16**](#_Toc515323294)

[2.1. Mô hình vận hành của hệ thống mới 16](#_Toc515323295)

[2.2. Phân rã chức năng 17](#_Toc515323296)

[2.3. Usecase tổng quan 18](#_Toc515323297)

[2.3.1. Mô hình Use case tổng quan hệ thống 18](#_Toc515323298)

[2.4. Phân tích yêu cầu chức năng của hệ thống 20](#_Toc515323299)

[2.4.1. Chức năng đăng nhập (login): 20](#_Toc515323300)

[2.4.2. Chức năng tạo mới người dùng 21](#_Toc515323301)

[2.4.3. Chức năng quản lý đơn nhập kho (PO) 23](#_Toc515323302)

[2.4.4. Chức năng quản lý đơn xuất kho (PL) 25](#_Toc515323303)

[2.4.5. Chức năng nhập kho (Receipt) 26](#_Toc515323304)

[2.4.6. Chức năng xuất kho (Issue) 27](#_Toc515323305)

[2.4.7. Chức năng xuất báo cáo 28](#_Toc515323306)

[2.4.8. Chức năng quản lý vật tư 29](#_Toc515323307)

[2.5. Thiết kế hệ thống 33](#_Toc515323308)

[2.5.1. Sơ đồ thực thể liên kết 33](#_Toc515323309)

[2.5.2. Thiết kế CSDL 34](#_Toc515323310)

[2.5.3. Biểu đồ lớp 39](#_Toc515323311)

[2.5.4. Triển khai MVC 39](#_Toc515323312)

[2.5.5. Thiết kế giao diện 41](#_Toc515323314)

[**PHẦN III: CÀI ĐẶT VÀ TRIỂN KHAI HỆ THỐNG 44**](#_Toc515323315)

[3.1. Thông tin sản phẩm 44](#_Toc515323316)

[3.2. Triển khai cơ sở dữ liệu 45](#_Toc515323317)

[3.3. Giao diện chức năng 45](#_Toc515323319)

[3.3.1. Trang chủ 45](#_Toc515323320)

[3.3.2. Đăng nhập 46](#_Toc515323321)

[3.3.3. Quản lý người dùng 47](#_Toc515323322)

[3.3.4. Quản lý quyền hạn 48](#_Toc515323323)

[3.3.5. Quản lý đơn đặt hàng 49](#_Toc515323324)

[3.3.6. Quản lý công ty 51](#_Toc515323326)

[3.3.7. Quản lý chi nhánh 52](#_Toc515323327)

[3.3.8. Quản lý kiện hàng 53](#_Toc515323328)

[3.3.9. Quản lý vật tư 54](#_Toc515323329)

[**PHẦN IV: KẾT LUẬN 55**](#_Toc515323330)

[**DANH MỤC TÀI LIỆU THAM KHẢO 56**](#_Toc515323331)

**DANH MỤC CÁC BẢNG**

[Bảng 1. Bảng mô tả UC chức năng đăng nhập 21](#_Toc515323451)

[Bảng 2. Bảng mô tả các bước sử dụng chức năng đăng nhập 21](#_Toc515323452)

[Bảng 3. Bảng mô tả UC tạo mới người dùng 22](#_Toc515323453)

[Bảng 4. Bảng mô tả các bước sử dụng chức năng đăng ký 22](#_Toc515323454)

[Bảng 5. Bảng mô tả UC thêm mới PO 24](#_Toc515323455)

[Bảng 6. Bảng mô tả các bước sử dụng chức năng thêm mới PO 24](#_Toc515323456)

[Bảng 7. Bảng mô tả UC thêm mới PL 26](#_Toc515323457)

[Bảng 8. Bảng mô tả các bước sử dụng chức năng thêm mới PL 26](#_Toc515323458)

[Bảng 9. Bảng mô tả UC chức năng nhập kho 27](#_Toc515323459)

[Bảng 10. Bảng mô tả các bước sử dụng chức năng nhập kho 27](#_Toc515323460)

[Bảng 11. Bảng mô tả UC chức năng xuất kho 28](#_Toc515323461)

[Bảng 12. Bảng mô tả các bước sử dụng chức năng xuất kho 29](#_Toc515323462)

[Bảng 13. Bảng mô tả UC chức năng xuất báo cáo 29](#_Toc515323463)

[Bảng 14. Bảng mô tả các bước sử dụng chức năng xuất kho 30](#_Toc515323464)

[Bảng 15. Bảng mô tả UC thêm mới vật tư 30](#_Toc515323465)

[Bảng 16. Bảng mô tả các bước sử dụng chức năng thêm mới PL 31](#_Toc515323466)

[Bảng 17. Bảng mô tả UC sửa vật tư 32](#_Toc515323467)

[Bảng 18. Bảng mô tả các bước sử dụng chức năng sửa vật tư 32](#_Toc515323468)

[Bảng 19. Bảng Công ty 35](#_Toc515323469)

[Bảng 20. Bảng Chi nhánh 35](#_Toc515323470)

[Bảng 21. Bảng Nhân viên 36](#_Toc515323471)

[Bảng 22. Bảng Quyền hạn 36](#_Toc515323472)

[Bảng 23. Bảng Chi tiết quyền hạn 36](#_Toc515323473)

[Bảng 24. Bảng Module quyền hạn 37](#_Toc515323474)

[Bảng 25. Bảng Vị trí lưu kho 37](#_Toc515323475)

[Bảng 26. Bảng Trạng thái vị trí 37](#_Toc515323476)

[Bảng 27. Bảng Kiện hàng 38](#_Toc515323477)

[Bảng 28. Bảng Trạng thái kiện hàng 38](#_Toc515323478)

[Bảng 29. Bảng Vật tư 38](#_Toc515323479)

[Bảng 30. Bảng Đơn nhập hàng 38](#_Toc515323480)

[Bảng 31. Bảng Chi tiết đơn nhập hàng 39](#_Toc515323481)

[Bảng 32. Bảng Đơn xuất vật tư 39](#_Toc515323482)

[Bảng 33. Bảng Chi tiết đơn xuất nhập tư 39](#_Toc515323483)

**DANH MỤC HÌNH VẼ**

[Hình 1. Minh họa nhập hàng hiện thời bằng phương pháp thủ công 11](#_Toc515323408)

[Hình 2. Mô hình MVC 14](file:///C:\Users\CUONGBK\Downloads\BaocaoDATN_NguyenVanCuong_20135181.docx#_Toc515323409)

[Hình 3. Mô hình hoạt động với website 17](#_Toc515323410)

[Hình 4. Sơ đồ phân rã chức năng 18](#_Toc515323411)

[Hình 5. Sơ đồ Use case tổng quan hệ thống 19](#_Toc515323412)

[Hình 6. Sơ đồ use case Cấu hình 20](file:///C:\Users\CUONGBK\Downloads\BaocaoDATN_NguyenVanCuong_20135181.docx#_Toc515323413)

[Hình 7. Sơ đồ Use case báo cáo 20](#_Toc515323414)

[Hình 8. Biểu đồ hoạt động chức năng đăng nhập 22](#_Toc515323415)

[Hình 9. Biểu đồ hoạt động chức năng tạo mới người dùng 23](#_Toc515323416)

[Hình 10. Biểu đồ tuần tự chức năng quản lý đơn nhập kho và quản lý nhập kho 24](#_Toc515323417)

[Hình 11. Biểu đồ hoạt động chức năng thêm mới PO 25](#_Toc515323418)

[Hình 12. Biểu đồ tuần tự chức năng quản lý đơn xuất kho và quản lý xuất kho 26](#_Toc515323419)

[Hình 13. Hình biểu đồ hoạt động chức năng thêm mới PL 27](#_Toc515323420)

[Hình 14. Hình biểu đồ hoạt động chức năng nhập kho 28](#_Toc515323421)

[Hình 15. Hình biểu đồ hoạt động chức năng nhập kho 29](#_Toc515323422)

[Hình 16. Biểu đồ chức năng xuất báo cáo 30](#_Toc515323423)

[Hình 17. Hình biểu đồ hoạt động chức năng thêm mới vật tư 32](#_Toc515323424)

[Hình 18. Hình biểu đồ hoạt động chức năng sửa vật tư 34](#_Toc515323425)

[Hình 19. Sơ đồ thực thể liên kết 35](#_Toc515323426)

[Hình 20. Các lớp Models 41](file:///C:\Users\CUONGBK\Downloads\BaocaoDATN_NguyenVanCuong_20135181.docx#_Toc515323427)

[Hình 21. Các lớp controllers 41](file:///C:\Users\CUONGBK\Downloads\BaocaoDATN_NguyenVanCuong_20135181.docx#_Toc515323428)

[Hình 22. Một số Views 41](file:///C:\Users\CUONGBK\Downloads\BaocaoDATN_NguyenVanCuong_20135181.docx#_Toc515323429)

[Hình 23. Giao diện Trang chủ 42](#_Toc515323430)

[Hình 24. Giao diện Danh sách đơn đặt hàng 42](#_Toc515323431)

[Hình 25. Giao diện Nhập kho 43](#_Toc515323432)

[Hình 26. Giao diện Quản lý kiện hàng 43](#_Toc515323433)

[Hình 27. Giao diện In barcode kiện hàng 44](#_Toc515323434)

[Hình 28. Giao diện Quản lý công ty 44](#_Toc515323435)

[Hình 29. Triển khai cơ sở dữ liệu 46](#_Toc515323436)

[Hình 30. Trang chủ 46](#_Toc515323437)

[Hình 31. Đăng nhập 47](#_Toc515323438)

[Hình 32. Danh sách người dùng 48](#_Toc515323439)

[Hình 33. Thêm mới người dùng 48](#_Toc515323440)

[Hình 34. Danh sách quyền hạn 49](#_Toc515323441)

[Hình 35. Quản lý quyền hạn chi tiết 50](#_Toc515323442)

[Hình 36. Danh sách đơn đặt hàng 50](#_Toc515323443)

[Hình 37. Tạo mới đơn đặt hàng 51](#_Toc515323444)

[Hình 38. Danh sách công ty 52](#_Toc515323445)

[Hình 39. Thêm mới công ty 53](#_Toc515323446)

[Hình 40. Danh sách chi nhánh 53](#_Toc515323447)

[Hình 41. Thêm mới chi nhánh 54](#_Toc515323448)

[Hình 42. Danh sách kiện hàng 54](#_Toc515323449)

[Hình 43. Danh sách vật tư 55](#_Toc515323450)

**DANH MỤC CÁC TỪ VIẾT TẮT VÀ THUẬT NGỮ**

|  |  |  |
| --- | --- | --- |
| **Số thứ tự** | **Từ viết tắt** | **Ý nghĩa** |
| 1 | ĐATN | **Đ**ồ **Á**n **T**ốt **N**ghiệp |
| 2 | OS | **O**perating **S**ystem – Hệ điều hành |
| 3 | PO | **P**urchase **O**rder – Đơn đặt hàng |
| 4 | PL | **P**ick **L**ist – Đơn lấy hàng |
| 5 | WMS | **W**arehouse **M**anagement **S**ystem |
| 6 | CSDL | **C**ơ **S**ở **D**ữ **L**iệu |
| 7 | LTV | **L**ập **T**rình **V**iên |
| 8 | SQL | **S**tructured **Q**uery **L**anguage |
| 9 | UC | **U**se **C**ase |
| 10 | RDBMS | **R**elational **D**atabase **M**anagement **S**ystem |

**1**

**PHẦN I: GIỚI THIỆU ĐỀ TÀI**

Trong chương này sẽ giới thiệu tổng quan, mục tiêu cần đạt được, về đề tài.

## Tổng quan

USB (Universal Serial Bus) là một chuẩn kết nối tuần tự đa dụng trong máy tính. USB sử dụng để kết nối các thiết bị ngoại vi với máy tính, chúng thường được thiết kế dưới dạng các đầu cắm cho các thiết bị tuân theo chuẩn cắm-và-chạy mà với tính năng cắm nóng thiết bị (nối và ngắt các thiết bị không cần phải khởi động lại hệ thống).

Giao tiếp USB được ứng dụng trong nhiều thiết bị với giao thức đã được chuẩn hóa. Tuy nhiên, với các nhu cầu riêng biệt, thì yêu cầu cần các giao thức không theo chuẩn là nhu cầu cần thiết. Từ đó, việc hiểu về cách thức giao tiếp USB là rất quan trọng để có thể tùy chỉnh theo từng nhu cầu.

Giao thức được tùy biến có nhiều ứng dụng khác nhau, điển hình là lưu trữ khóa bí mật dùng để bảo đảm tính bí mật và tính toàn vẹn dữ liệu.

Vì vậy, trong phạm vi đồ án này em sẽ đề xuất sử dụng sản phầm sử dụng giao tiếp USB để có thể sản xuất thiết bị nhỏ hơn, giá thành rẻ hơn, cùng với đó là tính mềm dẻo tốt hơn. Với những ưu điểm vừa nêu, thì thiết bị có thể áp dụng cho nhiều sản phẩm tùy biến theo mục đích của doanh nghiệp. Ví dụ có thể tùy biến thiết bị USB như một phần xác thực giao dịch thư điện tử, email, tham gia đầu tư chứng khoán trực tuyến, mua bán hàng hóa online, thanh toán online, chuyển tiền trực tuyến mà không sợ bị mất cắp tiền như với đối với dùng các tài khoản VISA, Master. Bên cạnh đó, còn có thể dùng trong kê khai, nộp thuế trực tuyến với cơ quan hải quan hoặc tương lai gần có thể sử dụng trong chính phủ điện tử.

## Mục tiêu cần đạt được

Theo tìm hiểu một số công ty lớn sử dụng USB làm thiết bị CA, em nhận thấy các công ty đang phụ thuộc khá nhiều vào các nhà sản xuất phần cứng (Independent Hardware Vendor - IHV) ví dụ nổi tiếng nhất như SecureMetric.Việc phụ thuộc vào các nhà phát triển phần cứng với cộng với việc đặt số lượng lớn giúp chi phí nghiên cứu và giá thành giảm xuống. Việc này mang lại lợi ích kinh tế trước mắt, tuy nhiên, việc đó cũng làm chúng ta phụ thuộc vào công nghệ của các công ty này. Thay vì việc tùy biến thiết bị theo ý muốn, chúng ta cố gắng ép mình theo khả năng của thiết bị.

Dựa trên các phân tích đánh giá trên, ta nhận thấy với việc sử dụng thiết bị của các nhà cung cấp thiết bị, khả năng tùy biến thiết bị của chúng ta sẽ thấp, và nếu tiếp tục công nghệ nhúng của chúng ta sẽ khó phát triển mạnh hơn nếu không làm chủ được công nghệ. Với ứng dụng được tùy biến từ những phần nhỏ nhất, từ thiết bị đến firmware và ứng dụng giao tiếp, việc tùy biến thiết bị sau này sẽ đơn giản hơn, và phù hợp hơn với nhu cầu của từng bài toán cụ thể.

Mục tiêu được đặt ra ở đây là cần làm chủ công nghệ, từ thiết bị, firmware và ứng dụng. Trên cơ sở đó, tạo nên ứng dụng dùng để làm thiết bị USB Token dùng để xác thực chủ thể cụ thể.

## Lựa chọn và định hướng thiết kế

Từ yêu cầu nêu ra bên trên, em tập trung nghiên cứu tìm các thiết bị có giá thành rẻ, kèm theo có EEPROM kèm theo. Từ đó, quyết định chọn vi điều khiển dòng LPC1833 có 16kB bộ nhớ EEPROM dùng để lưu thông tin.

Tiếp theo, chọn kỹ thuật giao tiếp USB với firmware của thiết bị, em chọn sử dụng công nghệ WinUSB trên Windows thay vì sử dụng User-mode framework ( UMDF) hay kernel-mode driver framework (KMDF). Việc lựa chọn này giúp tiết kiệm thời gian phát triển, đồng thời đảm bảo có thể sử dụng đầy đủ tính năng cần cung cấp. Giải thích việc lựa chọn này sẽ được giải thích chi tiết trong Chương 3.

Giao diện ứng dụng trên Windows, sử dụng thư viện Winform trên nền .Net Framework. Việc lựa chọn Winform giúp giao diện ưa nhìn, tiết kiệm thời gian phát triển, và dễ tiếp cận. Ứng dụng trên Windows tương tác với thư việc SQLite cho phép tương tác với cơ sở dữ liệu chữ ký số để sử dụng.

Từ yêu cầu xây dựng thiết bị với giá thành rẻ nhưng vẫn đảm bảo các yếu tố về an toàn và bảo mật, đồ án đề ra giải pháp nghiên cứu và phát triển thiết bị USB Token từ các linh kiện có giá thành rẻ. Ngoài ra xây dựng thuật toán cho phép lưu trữ khóa bí mật trên thiết bị một cách an toàn và khó để có thể tìm ra khóa bí mật nếu thiết bị bị mất. Cùng với đó là ứng dụng trên Windows cho phép giao tiếp với thiết bị, hoạt động trên các máy tính sử dụng Windows. Cuối cùng là giao diện để người dùng sử dụng các chức năng của thiết bị.

## Bố cục đồ án

Phần còn lại của báo cáo đồ án tốt nghiệp này được tổ chức như sau.

Chương 1 Trình bày về giới thiệu, đặt vấn đề, các mục tiêu cần đạt được, lựa chọn giải pháp cho mục tiêu của đồ án này.

Chương 2: Trình bày về việc xây dựng, và thiết kế thiết bị, firmware giao tiếp thiết bị.

Chương 3 Trình bày việc xây dựng ứng dụng giao tiếp với driver , kịch bản giao tiếp với thiết bị.

Chương 4: Ứng dụng giao tiếp với USB tạo USB Token. Xây dựng demo giao tiếp giữa thiết bị và ứng dụng.

**PHẦN IV: KẾT LUẬN**

**DANH MỤC TÀI LIỆU THAM KHẢO**

[1] Giới thiệu về ASP.NET MVC <https://www.asp.net/>, truy cập tháng 5/2018

[2] Giới thiệu về SQL Server <https://en.wikipedia.org/wiki/Microsoft_SQL_Server>, truy cập tháng 5/2018