

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH
BỘ MÔN CÔNG NGHỆ THÔNG TIN



BÁO CÁO ĐỒ ÁN TỐT NGHIỆP

**ĐỀ TÀI: NGHIÊN CỨU CƠ CHẾ BẢO MẬT PACE VÀ EAC
ĐỂ XÂY DỰNG MÔ HÌNH XÁC THỰC ĐẢM BẢO AN TOÀN
THÔNG TIN TRÊN THẺ E-ID**

Giảng viên hướng dẫn: ThS. TRẦN PHONG NHÃ

Sinh viên thực hiện: VÕ KHẮC MẠNH

Lớp: CQ.61 CNTT

Khoá: 61

Tp. Hồ Chí Minh, năm 2024

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

BỘ MÔN: CÔNG NGHỆ THÔNG TIN

-----***-----

Mã sinh viên: 6151071071
Khóa: 61

Họ tên SV: VÕ KHẮC MẠNH
Lớp: CQ. 61.CNTT

1. Tên đề tài:

Nghiên cứu cơ chế bảo mật PACE và EAC để xây dựng mô hình xác thực đảm bảo an toàn thông tin trên thẻ e-ID.

2. Mục tiêu

Tìm hiểu cách thức hoạt động của thẻ danh tính điện tử e-ID, nghiên cứu hai hệ mật PACE và EAC đưa ra mô hình xác thực đảm bảo an toàn thông tin được lưu trữ trên thẻ và xây dựng mô hình mô phỏng quá trình đọc ghi thông tin lên thẻ e-ID.

3. Nội dung thực hiện

- Tìm hiểu về thẻ e-ID, cách lưu trữ dữ liệu trên thẻ, các mối nguy hiểm có thể bị tấn công trên thẻ
- Nghiên cứu tìm hiểu về hai hệ mật Password Authenticated Connection Establishment (PACE) và Extended Access Control (EAC)
- Nghiên cứu bài toán giả định gPACE-DH
- Đưa ra mô hình xác thực e-ID
- Xây dựng mô hình Iot mô phỏng quá trình đọc ghi dữ liệu lên thẻ e-ID

4. Công nghệ, công cụ và ngôn ngữ lập trình

- Thiết bị sử dụng: Module ESP 8266, Module RC522, Thẻ RFID Mirafe 1KB.
- Công cụ lập trình: Arduino IDE, Visual Studio Code
- Ngôn ngữ lập trình: C/C++, HTML, CSS, Bootstrap, Javascripts.

5. Các kết quả chính dự kiến

- Đưa ra được mô hình xác thực e-ID dựa trên hai cơ chế PACE và EAC
- Xây dựng mô hình mô phỏng quá trình đọc ghi dữ liệu lên thẻ e-ID

6. Giảng viên và cán bộ hướng dẫn

Họ tên: ThS. TRẦN PHONG NHÃ

Đơn vị công tác: Trường Đại học Giao thông Vận tải Phân hiệu tại TP. Hồ Chí Minh

Điện thoại: 0906 761 014

Email: tpnha@utc2.edu.vn

Ngày 20 tháng 03 năm 2024

Đã giao nhiệm vụ TKTN

Trưởng BM Công nghệ thông tin

Giảng viên hướng dẫn

Trần Phong Nhã

Trần Phong Nhã

Đã nhận nhiệm vụ TKTN

Sinh viên: Võ Khắc Mạnh

Điện thoại: 0374155521

Ký tên:

Email: 615107071@st.utc2.edu.vn

LỜI CẢM ƠN

Quãng thời gian làm đồ án vừa qua thật sự là một hành trình đáng trân trọng, mà từ đó em rút ra được nhiều bài học quý giá, đồng thời tích lũy những kinh nghiệm giá trị cho công việc của mình sau này. Điều quan trọng không chỉ là sự cố gắng của bản thân, mà còn là sự hỗ trợ và đồng hành đầy ý nghĩa từ mọi người xung quanh.

Để hoàn thành đề tài này trước tiên em xin cảm ơn đến thầy **ThS. Trần Phong Nhã** là giảng viên hướng dẫn, người đã tận tình hướng dẫn, chỉ bảo em trong suốt thời gian làm đồ án.

Em cũng xin chân thành gửi lời cảm ơn đến quý thầy, cô **Bộ môn Công nghệ thông tin – Phân hiệu Trường Đại học Giao thông Vận tải tại Thành phố Hồ Chí Minh** lời cảm ơn chân thành vì đã truyền đạt cho em những kiến thức không chỉ từ sách vở, mà còn những kinh nghiệm quý giá từ cuộc sống trong khoảng thời gian học tập tại trường.

Trong quá trình làm đồ án, với kiến thức của em vẫn còn hạn chế và nhiều bỡ ngỡ. Do vậy, những thiếu sót là điều chắc chắn không thể tránh khỏi, em rất mong nhận được những ý kiến đóng góp của thầy cô và các bạn để kiến thức của em được hoàn thiện hơn, phục vụ tốt hơn trong công tác thực tế sau này.

Sau cùng, em xin kính chúc Quý Thầy Cô trong **Bộ môn Công nghệ thông tin** lời chúc sức khỏe, luôn hạnh phúc và thành công hơn nữa trong công việc cũng như trong cuộc sống.

Em xin chân thành cảm ơn!

[illegible]

Giảng viên hướng dẫn

Trần Phong Nhã

MỤC LỤC

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP	i
LỜI CẢM ƠN	iii
NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN.....	iv
MỤC LỤC	v
DANH MỤC HÌNH ẢNH	viii
DANH MỤC BẢNG VIẾT TẮT	x
TỔNG QUAN.....	1
1. Lý do chọn đề tài	1
2. Mục tiêu và nhiệm vụ của đồ án.....	1
3. Bố cục đồ án	2
CHƯƠNG I. TỔNG QUAN VỀ THẺ DANH TÍNH ĐIỆN TỬ.....	3
1.1. Giới thiệu về thẻ danh tính điện tử.....	3
1.1.1. Lịch sử ra đời	3
1.1.2. Khái niệm về danh tính điện tử (e-Identity)	4
CHƯƠNG II. DỮ LIỆU TRÊN THẺ DANH TÍNH ĐIỆN TỬ	14
2.1 Dữ liệu và bảo vệ dữ liệu sinh trắc trên thẻ e-ID	14
2.1.1. Dữ liệu được lưu trữ trên thẻ e-ID	14
2.1.2. Xác thực đa yếu tố.....	14
2.1.3. Cơ chế xác thực trên thẻ e-ID	16
a. Xác minh mã PIN qua PACE	16
b. Xác thực lẫn nhau thông qua kiểm soát truy cập mở rộng (EAC)	16
c. Kiểm tra tính hợp lệ và đọc dữ liệu cá nhân	17
2.1.4. Kiểm tra và truy xuất dữ liệu trên thẻ e-ID.....	17
a. Khu vực kiểm tra bằng mắt (VIZ).....	17
b. Vùng đọc bằng máy (MRZ)	18

2.2 Quy trình truy xuất dữ liệu trên e-ID	20
2.2.1 Các giao thức mật mã được triển khai trên e-ID	22
2.3. Các kỹ thuật mật mã đảm bảo an toàn dữ liệu cho dữ liệu e-ID	25
2.3.1 Chữ ký số (<i>Digital Signature</i>)	25
2.3.2. Các chương trình mã hóa dữ liệu.....	28
CHƯƠNG III. CƠ CHẾ BẢO MẬT PACE, EAC VÀ MÔ HÌNH XÁC THỰC E-ID.....	30
3.1. Các vấn đề nguy hiểm tồn tại trên thẻ e-ID.....	30
3.2. Cơ chế bảo mật PACE và EAC	31
3.2.1. Cơ chế bảo mật PACE.....	31
3.2.2. Cơ chế bảo mật EAC	32
3.2.3. Mô hình thử nghiệm xác thực e-ID áp dụng cơ chế PACE và EAC	33
CHƯƠNG IV: XÂY DỰNG HỆ THỐNG IOT ĐỌC GHI DỮ LIỆU TRÊN THẺ RFID.....	42
4.1. Giới thiệu tổng quan mô hình.....	42
4.1.1. Ngôn ngữ và các công cụ lập trình	42
4.1.2 Giới thiệu thiết bị.....	42
a. ESP 8266	42
b. Modulee RFID RC522.....	43
c. Thẻ RFID Mifare 1KB	44
4.2. Mô tả hệ thống.....	47
4.2.1. Sơ đồ kết nối thiết bị.....	47
a. Sơ đồ các chân Pin được sử dụng.....	47
b. Sơ đồ đấu nối.....	48
4.2.2. Mô tả hoạt động và chức năng của mô hình.....	49
a. Hoạt động và chức năng Ghi dữ liệu	49
b. Hoạt động và chức năng Đọc dữ liệu.....	51

KẾT LUẬN VÀ KIẾN NGHỊ.....	53
Kết quả đạt được.....	53
Hạn chế	53
Hướng phát triển.....	53
TÀI LIỆU THAM KHẢO	54

DANH MỤC HÌNH ẢNH

Hình 1. Danh tính điện tử của công dân Việt Nam	5
Hình 2. Biểu tượng thẻ định danh điện tử	6
Hình 3. Mặt trước của thẻ e-ID	7
Hình 4. Mặt sau của thẻ e-ID	7
Hình 5. CCCD điện tử Việt Nam	8
Hình 6. Hộ chiếu điện tử Việt Nam.....	8
Hình 7. Ba kích thước của MRTD bao gồm MRP (kích thước TD3) với các vị trí được đề xuất cho tính năng xác minh tài liệu hỗ trợ của máy	10
Hình 8. Minh họa các kích thước ISO/IEC 7810 tính bằng milimet.....	11
Hình 9. Vùng đọc bằng mắt (VIZ) của thẻ e-ID	18
Hình 10. Tập hợp con các ký tự OCR-B từ [ISO 1073-2] để sử dụng trong tài liệu du lịch có thể đọc được bằng máy	18
Hình 11. Sơ đồ vùng đọc hiệu quả MRTD.....	19
Hình 12. Các giao thức mật mã	23
Hình 13. Hướng chữ kí được hiển thị.....	25
Hình 14. Mô tả giao thức gPACE-DH	32
Hình 15. Mô hình xác thực e-ID	35
Hình 16. Lược đồ PACE	36
Hình 17. Lược đồ TA	38
Hình 18. Lược đồ PA	39
Hình 19. Lược đồ CA	40
Hình 20. Module ESP8266 NodeMCU	42
Hình 21. Module RFID RC522 13.56MHz.....	43
Hình 22. Tổ chức bộ nhớ của thẻ RFID	46
Hình 23. Sơ đồ đấu nối.....	48
Hình 24. Hình ảnh mô hình được lắp ráp	48
Hình 25. Code chức năng ghi thông tin vào thẻ	49

Hình 26. Giao diện chức năng ghi thông tin vào thẻ.....	50
Hình 27. Dữ liệu được người dùng nhập vào và chờ ghi	50
Hình 28. Ghi dữ liệu thành công	51
Hình 29. Code hiện thông tin lên trang web	51
Hình 30. Giao diện chức năng đọc thẻ	52
Hình 31. Dữ liệu được đọc thành công	52

DANH MỤC BẢNG VIẾT TẮT

STT	Viết tắt	Diễn giải	Ý nghĩa
1	PACE	Password Authenticated Connection Establishment	Đây là một giao thức bảo mật được sử dụng để thiết lập kết nối bảo mật giữa các thiết bị thông qua việc xác thực bằng mật khẩu
2	EAC	Extended Access Control	Là một phương pháp kiểm soát truy cập mở rộng, cho phép quản lý và kiểm soát quyền truy cập chi tiết hơn đối với các tài nguyên và hệ thống.
3	e-ID	electronic Identification	Là hệ thống nhận dạng cá nhân sử dụng công nghệ điện tử để xác thực danh tính của cá nhân
4	CCCD	Căn Cước Công Dân	Thẻ căn cước công dân của Việt Nam
5	RFID	Radio Frequency Identification	Một công nghệ sử dụng sóng radio để tự động nhận diện và theo dõi các đối tượng có gắn thẻ RFID
6	NFC	Near Field Communication	Một công nghệ kết nối không dây cho phép các thiết bị tương tác với nhau khi chúng ở gần nhau, thường trong khoảng cách vài centimet.
7	MRTD		
8	VIZ	Visual Inspection Zone	Vùng kiểm tra bằng mắt
9	MRZ	Machine Readable Zone	Vùng được đọc bằng máy
10	DH	Diffie-Hellman	Là một phương pháp trao đổi khóa mật mã

11	DG1,2,3	Data Group1,2,3	Là nơi trữ các thông tin nhận dạng cơ bản của người sở hữu
12	SSL	Secure Sockets Layer	Là một giao thức bảo mật được phát triển ban đầu bởi Netscape vào những năm 1990
13	TLS	Transport Layer Security	Là phiên bản tiếp theo và là sự phát triển của SSL, được thiết kế để cải thiện các vấn đề bảo mật và hiệu suất của SSL
14	IS	Identity Scanner	Là các thiết bị được sử dụng để đọc thông tin từ thẻ e-ID, như hộ chiếu điện tử,... Chúng thường được sử dụng trong các ứng dụng xác thực, nhận dạng cá nhân và kiểm soát truy cập.
15	TA	Terminal Authentication	Xác thực thiết bị
16	PA	Passive Authentication	Xác thực thụ động

TỔNG QUAN

1. Lý do chọn đề tài

Trong thời đại kỷ nguyên số, định danh điện tử là một vấn đề mới ở Việt Nam. CCCD gắn chip chính thức được cấp thay thế cho CCCD cũ bắt đầu từ 01/01/2021. Yếu tố quan trọng trong việc quản lý dân số cùng với các chính sách về việc đơn giản hóa thủ tục hành chính của Chính phủ. Do đó, bảo mật thông tin trên thẻ trở thành mối quan tâm hàng đầu của người dân và doanh nghiệp khi thực hiện giao dịch điện tử, bao gồm cả dịch vụ công trực tuyến và các giao dịch khác trên mạng.

Chính phủ ban hành nghị định số 59/2022/NĐ-CP quy định về định danh và xác thực điện tử, có hiệu lực thi hành từ ngày 20/10/2022. Nghị định này quy định về danh tính điện tử, định danh điện tử, xác thực điện tử,... Nghị định này sẽ tạo cơ sở pháp lý cho việc cung cấp và sử dụng dịch vụ xác thực và định danh điện tử, đảm bảo an ninh thông tin trong các giao dịch điện tử. Điều này cũng giúp nâng cao hiệu quả của các công dịch vụ công quốc gia và hệ thống thông tin điện tử, góp phần hoàn thành mục tiêu xây dựng Chính phủ điện tử.

Phát triển thẻ căn cước công dân có gắn chip là bước đầu cho việc phát triển thẻ danh tính điện tử ở Việt Nam. Tuy nhiên, còn nhiều hạn chế và vấn đề cần giải quyết trong việc phát triển xác thực điện tử, đặc biệt là đảm bảo an toàn khi sử dụng thẻ danh tính điện tử.

Vì vậy, em chọn đề tài “Nghiên cứu cơ chế bảo mật PACE và EAC để xây dựng mô hình xác thực đảm bảo an toàn thông tin trên thẻ e-ID” để tập trung vào định danh và xác thực điện tử, đảm bảo truy cập an toàn và dễ dàng vào các dịch vụ công trực tuyến, giúp công dân, cơ quan tổ chức và doanh nghiệp bảo vệ thẻ danh tính của mình khỏi bị tấn công, đồng thời thúc đẩy quá trình chuyển đổi số của nước ta.

2. Mục tiêu và nhiệm vụ của đồ án

Nghiên cứu hai cơ chế bảo mật PACE và EAC. Đưa ra được mô hình xác thực e-ID dựa trên hai cơ chế bảo mật đó, xây dựng mô hình mô phỏng quá trình đọc ghi dữ liệu trên thẻ e-ID

3. Bố cục đồ án

TỔNG QUAN

CHƯƠNG 1: TỔNG QUAN VỀ THẺ DANH TÍNH ĐIỆN TỬ

CHƯƠNG 2: DỮ LIỆU TRÊN THẺ DANH TÍNH ĐIỆN TỬ

CHƯƠNG 3: HỆ MẬT ĐẢM BẢO AN TOÀN THÔNG TIN TRÊN THẺ DANH TÍNH ĐIỆN TỬ

CHƯƠNG 4: XÂY DỰNG HỆ THỐNG MÔ PHỎNG ĐỌC GHI DỮ LIỆU LÊN THẺ RFID

KẾT LUẬN VÀ KIẾN NGHỊ

TÀI LIỆU THAM KHẢO

CHƯƠNG I. TỔNG QUAN VỀ THẺ DANH TÍNH ĐIỆN TỬ

1.1. Giới thiệu về thẻ danh tính điện tử

1.1.1. Lịch sử ra đời

Thẻ danh tính điện tử (e-ID) đã phát triển từ nhu cầu về các phương pháp nhận dạng và xác thực danh tính đáng tin cậy và hiệu quả trong bối cảnh số hóa ngày càng tăng. Dưới đây là một cái nhìn tổng quan về lịch sử ra đời và phát triển của thẻ danh tính điện tử:

- **Thời Kỳ Đầu - Thẻ nhựa và mã vạch (1970s-1980s):**
 - 1970s: Các thẻ nhựa với mã vạch hoặc dải từ được sử dụng rộng rãi cho các mục đích nhận dạng cá nhân, như thẻ nhân viên hoặc thẻ ngân hàng.
 - 1980s: Hệ thống nhận dạng bằng thẻ thông minh (smart card) bắt đầu phát triển với các thẻ chứa chip vi mạch (integrated circuit chip), cho phép lưu trữ và xử lý dữ liệu trên thẻ.
- **Phát Triển Thẻ Thông Minh (1990s):**
 - 1991: Các tiêu chuẩn ISO/IEC 7816 cho thẻ thông minh được ban hành, tạo ra cơ sở cho việc phát triển các thẻ với khả năng lưu trữ và bảo mật cao hơn.
 - 1997: Thẻ thông minh bắt đầu được sử dụng rộng rãi ở Châu Âu, đặc biệt là trong các ứng dụng tài chính và viễn thông.
- **Sự Ra Đời của Thẻ Danh Tính Điện Tử (2000s)**
 - 2000s: Sự xuất hiện của thẻ danh tính điện tử, với việc các quốc gia như Estonia, Bỉ và Malaysia bắt đầu phát hành thẻ e-ID cho công dân của mình. Những thẻ này không chỉ lưu trữ thông tin cá nhân mà còn tích hợp chữ ký số và các chức năng bảo mật khác.
 - 2002: Estonia phát hành thẻ căn cước điện tử, một trong những thẻ e-ID tiên tiến nhất vào thời điểm đó, cho phép công dân truy cập các dịch vụ công trực tuyến và thực hiện các giao dịch điện tử an toàn.
 - 2004: Bỉ giới thiệu thẻ danh tính điện tử, được sử dụng cho các dịch vụ công với độ bảo mật cao.
- **Phổ Biến Toàn Cầu (2010s - Nay):**
 - 2010s: Nhiều quốc gia trên toàn thế giới bắt đầu triển khai thẻ danh tính điện tử như một phần của chiến lược Chính phủ điện tử và an

ninh mạng. Thẻ e-ID được sử dụng cho nhiều mục đích khác nhau, từ nhận dạng cá nhân, xác thực giao dịch trực tuyến, đến truy cập các dịch vụ công cộng và tư nhân.

- 2010: Malaysia phát hành thẻ MyKad, một thẻ đa chức năng tích hợp nhiều dịch vụ.
- 2013: Ấn Độ bắt đầu triển khai chương trình thẻ căn cước điện tử Aadhaar, một trong những hệ thống nhận dạng lớn nhất thế giới.
- 2020s: Với sự phát triển của công nghệ blockchain và sinh trắc học, thẻ e-ID ngày càng trở nên tiên tiến hơn, cung cấp các biện pháp bảo mật mới và tích hợp nhiều dịch vụ số.

- **Tại Việt Nam:**

- 2021: Việt Nam bắt đầu triển khai thẻ căn cước công dân gắn chip, với mục tiêu cung cấp một phương tiện nhận dạng an toàn và hiệu quả, tích hợp nhiều tiện ích và dịch vụ công trực tuyến.
- Nghị định về định danh điện tử: Bộ Thông tin và Truyền thông đã xây dựng các quy định và nghị định liên quan đến định danh điện tử, tạo cơ sở pháp lý cho việc sử dụng và phát triển thẻ danh tính điện tử

Tuy nhiên, việc triển khai và sử dụng thẻ danh tính điện tử cũng đối mặt với nhiều thách thức, bao gồm vấn đề bảo mật thông tin cá nhân và quyền riêng tư. Do đó, việc phát triển và quản lý thẻ danh tính điện tử đòi hỏi sự cân nhắc kỹ lưỡng về các vấn đề pháp lý và chính sách, cũng như việc áp dụng các biện pháp bảo mật hiệu quả để bảo vệ thông tin cá nhân của người dùng CCCD cũ.

1.1.2. Khái niệm về danh tính điện tử (e-Identity)

Danh tính điện tử hay danh tính số (e-Identity) là tập hợp các thông tin điện tử phục vụ việc xác định duy nhất một cá nhân, tổ chức.

Theo đó, danh tính điện tử của công dân Việt Nam bao gồm: Số định danh cá nhân, họ, tên đệm và tên, ngày, tháng, năm sinh, giới tính, ảnh chân dung và vân tay. Danh tính điện tử của người nước ngoài bao gồm: Số hộ chiếu hoặc số giấy tờ có giá trị đi lại quốc tế, họ, tên đệm và tên, ngày, tháng, năm sinh, giới tính, quốc tịch, ảnh chân dung và vân tay (nếu có).



Hình 1. Danh tính điện tử của công dân Việt Nam

Việc định danh, xác thực điện tử gồm nhiều hình thức như: Tài khoản/mật khẩu, thiết bị lưu mã (token), điện thoại di động và thẻ SIM. Định danh, xác thực điện tử cung cấp vai trò đặc biệt quan trọng trong hệ sinh thái số để đảm bảo truy cập an toàn và dễ dàng tới các dịch vụ công trực tuyến.

Nhận dạng điện tử (e-ID) là một giải pháp kỹ thuật số để chứng minh danh tính của công dân hoặc tổ chức. Chúng có thể được sử dụng để xem để truy cập các lợi ích hoặc dịch vụ do cơ quan chính phủ, ngân hàng hoặc các công ty khác cung cấp cho thanh toán di động, v.v. Ngoài xác thực và đăng nhập trực tuyến, nhiều dịch vụ nhận dạng điện tử cũng cung cấp cho người dùng tùy chọn để ký tài liệu điện tử bằng chữ ký kỹ thuật số.

1.1.3. Giới thiệu sơ lược về thẻ danh tính điện tử (e-ID)

Thẻ danh tính điện tử (e-ID card) là một loại thẻ nhận dạng kỹ thuật số được trang bị vi mạch điện tử, giúp xác thực danh tính của người sở hữu một cách an toàn và tiện lợi. Thẻ danh tính điện tử thường được chính phủ cấp phát và có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm xác thực danh tính, truy cập các dịch vụ trực tuyến của chính phủ và giao dịch điện tử.



Hình 2. Biểu tượng thẻ định danh điện tử

a. Cấu tạo của thẻ danh tính điện tử bao gồm:

- Vỏ thẻ
 - Chất liệu: Thẻ thường được làm từ nhựa bền, chẳng hạn như Polycarbonate hoặc PVC, để đảm bảo độ bền và khả năng chống chịu mài mòn.
 - Kích thước: Theo tiêu chuẩn quốc tế ISO/IEC 7810 ID-1 (85.60 mm × 53.98 mm).
- Vi mạch điện tử (chip)
 - Vi mạch: Chứa các dữ liệu cá nhân và sinh trắc học, cũng như các chứng chỉ số và khóa mã hóa.
 - Giao diện: Có thể giao tiếp với đầu đọc thẻ qua tiếp xúc hoặc không tiếp xúc. Một số thẻ có cả hai giao diện.
- Ống dây Antenna
 - Antenna: Được nhúng trong thẻ để hỗ trợ giao tiếp không tiếp xúc bằng cách truyền dữ liệu giữa thẻ và đầu đọc qua công nghệ RFID hoặc NFC.
- Các thành phần bảo mật
 - Chứng chỉ số: Được lưu trữ trong chip để xác thực danh tính và ký số.
 - Khóa mã hóa: Được sử dụng để bảo vệ dữ liệu trên thẻ và trong quá trình giao tiếp với đầu đọc.
- Dữ liệu in trên thẻ
 - Thông tin cá nhân: Tên, ngày sinh, quốc tịch, số thẻ, ngày phát hành và ngày hết hạn.
 - Ảnh chân dung: Ảnh khuôn mặt của người sở hữu thẻ.
 - Chữ ký số: Chữ ký của người sở hữu (nếu có).

b. Thẻ phải dựa trên các tiêu chuẩn như:

- ISO/IEC 14443-1: Đặc điểm vật lý
- ISO/IEC 14443-2: Giao diện RF (Radio Frequency Interface)
- ISO/IEC 14443-3: Giao thức chống xung đột và xử lý lệnh (Initialization and Anti-collision)
- ISO/IEC 14443-4: Giao thức truyền thông (Transmission Protocol)

Thẻ CCCD gắn chip điện tử, còn gọi là thẻ căn cước điện tử (e-ID) là một loại giấy tờ tùy thân của công dân Việt Nam, có thể đóng vai trò thiết bị nhận diện, xác thực danh tính và chìa khóa truy cập thông tin công dân trong hệ thống cơ sở dữ liệu quốc gia. Nó có giá trị chứng minh về căn cước công dân và cho phép người dùng tiếp cận nhiều dịch vụ vốn đòi hỏi hàng loạt giấy tờ khác nhau.

Thẻ CCCD gắn chip điện tử về cơ bản cũng giống như thẻ CCCD mã vạch. Tuy nhiên, trên thẻ không có các dòng trạng thái thể hiện mã vạch mà nó sẽ thay thế bằng chip điện tử dung lượng lớn. Thẻ CCCD gắn chip sẽ lưu trữ những đặc điểm nhận dạng bằng hình ảnh, vân tay và sinh trắc học.



Hình 5. CCCD điện tử Việt Nam



Hình 6. Hộ chiếu điện tử Việt Nam

Hộ chiếu điện tử (e-Passport) hay hộ chiếu sinh trắc học (Biometric Passport) có gắn chip chứa thông tin cá nhân và các đặc điểm nhận dạng được cài phía trong bìa để vừa tăng thêm giá trị bảo mật cho hộ chiếu (nhờ độ bảo mật cao hơn), giảm nguy cơ làm giả hoặc sửa đổi thông tin, vừa tương thích với các thiết bị kiểm tra hiện đại được trang bị ở các sân bay quốc tế.

1.2. Đặc điểm kĩ thuật của và các tiêu chuẩn của thẻ e-ID

1.2.1. Đặc điểm vật lí của MRTD

MRTD (Machine Readable Travel Document) là thuật ngữ dùng để chỉ các loại giấy tờ thông hành có thể đọc được bằng máy, chẳng hạn như hộ chiếu, thẻ căn

cước. Các tài liệu này được thiết kế theo các tiêu chuẩn quốc tế, cho phép máy móc đọc và trích xuất dữ liệu một cách tự động và nhanh chóng, đảm bảo tính chính xác và hiệu quả trong quá trình kiểm tra và xác thực thông tin cá nhân tại các cửa khẩu biên giới, sân bay và các điểm kiểm soát khác.

Các quốc gia và tổ chức phát hành có thể lựa chọn các tài liệu được sử dụng để sản xuất các thẻ của họ.

- **Kích thước và hình dạng:**

- Hộ chiếu tiêu chuẩn: Kích thước là 125mm x 88mm, giống với kích thước của sổ tay nhỏ.
- Thẻ căn cước: Kích thước là 85.60mm x 53.98mm, tương đương với kích thước của thẻ tín dụng.

- **Chất liệu:**

- Hộ chiếu: Bìa hộ chiếu thường được làm từ chất liệu giấy tổng hợp hoặc vật liệu nhựa có độ bền cao, giúp bảo vệ các trang bên trong. Các trang bên trong làm từ giấy đặc biệt chống giả mạo.
- Thẻ căn cước: Thường được làm từ nhựa Polycarbonate hoặc vật liệu tổng hợp khác, đảm bảo độ bền và khả năng chống mài mòn.

- **Dải quang học (Machine Readable Zone - MRZ):**

- MRZ: Là một dải chứa các ký tự có thể đọc bằng máy, thường nằm ở cuối trang nhận diện của hộ chiếu hoặc mặt sau của thẻ căn cước. MRZ chứa thông tin như tên, số hộ chiếu, quốc tịch, ngày sinh và ngày hết hạn.
- Định dạng MRZ: Được tiêu chuẩn hóa theo ICAO với hai hoặc ba dòng ký tự OCR-B, tùy thuộc vào loại tài liệu.

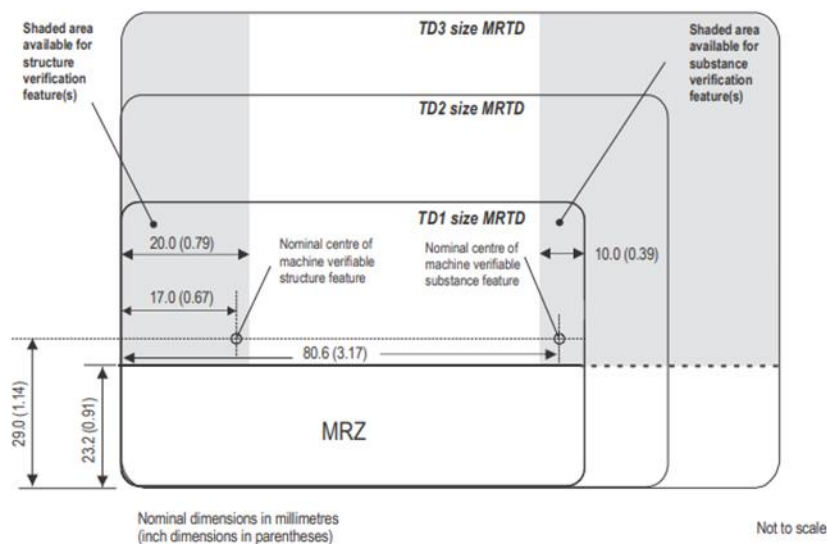
- **Chip điện tử (đối với e-Passport và e-ID):**

- Chip RFID: Nhiều MRTD hiện đại, như e-Passport và e-ID, tích hợp một chip RFID chứa dữ liệu sinh trắc học và thông tin cá nhân. Chip này giúp tăng cường bảo mật và chống làm giả.
- Dữ liệu sinh trắc học: Bao gồm ảnh khuôn mặt, dấu vân tay và/hoặc móng mắt, được lưu trữ trong chip để xác thực danh tính của người sở hữu.

- **Yếu tố bảo mật:**

- Hình mờ (Watermark): Các hộ chiếu và thẻ căn cước thường có hình mờ hoặc các yếu tố bảo mật nhìn thấy dưới ánh sáng đặc biệt để chống giả mạo.

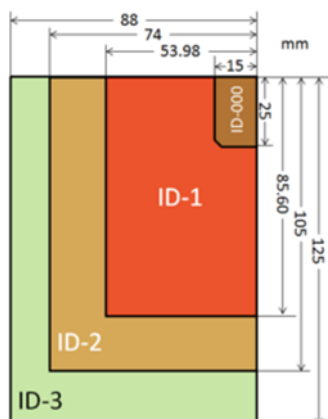
- In siêu mịn (Microprinting): Sử dụng in siêu mịn với các dòng chữ nhỏ khó sao chép.
- Mực chống giả mạo: Sử dụng mực UV, mực thay đổi màu sắc hoặc mực phát quang để tăng cường bảo mật.
- Hologram và lớp phủ bảo mật: Sử dụng các hình ảnh ba chiều và lớp phủ bảo mật đặc biệt để bảo vệ thông tin và chống giả mạo.
- Thông tin cá nhân và ảnh:
 - Trang dữ liệu cá nhân: Chứa thông tin cá nhân như tên, quốc tịch, ngày sinh, và ảnh chân dung của người sở hữu.
 - Ảnh chân dung: Được chụp theo tiêu chuẩn ICAO để đảm bảo khả năng nhận diện và xác thực sinh trắc học.



Hình 7. Ba kích thước của MRTD bao gồm MRP (kích thước TD3) với các vị trí được đề xuất cho tính năng xác minh tài liệu hỗ trợ của máy

1.2.2. Các thông số kỹ thuật của thẻ

- ID-1



Hình 8. Minh họa các kích thước ISO/IEC 7810 tính bằng milimet

Định dạng ID-1 chỉ định kích thước 85,60 x 53,98 mm ($3\frac{3}{8}$ in \times $2\frac{1}{8}$ in) và các góc tròn có bán kính 2,88–3,48 mm (khoảng $\frac{1}{8}$ in). Nó thường được sử dụng cho các loại thẻ thanh toán (thẻ ATM, thẻ tín dụng, thẻ ghi nợ, v.v.). Ngày nay nó cũng được sử dụng cho giấy phép lái xe và chứng minh thư cá nhân ở nhiều quốc gia, thẻ hệ thống thu phí tự động cho phương tiện giao thông công cộng, trong thẻ khách hàng thân thiết bán lẻ.

- ID-2

Định dạng ID-2 chỉ định kích thước 105 x 74 mm ($4\frac{1}{8}$ in \times $2\frac{15}{16}$ in). Kích thước này là định dạng A7. Ví dụ: định dạng ID-2 được sử dụng cho thị thực.

- ID-3

ID-3 chỉ định kích thước 125 x 88 mm ($4\frac{15}{16}$ in \times $3\frac{7}{16}$ in). Kích thước này là định dạng B7. Định dạng này thường được sử dụng cho các cuốn sổ hộ chiếu.

- ID-000

ID-000 chỉ định kích thước 25 x 15 mm (1 in \times $\frac{9}{16}$ in), với một góc hơi vát (3 mm hoặc $\frac{1}{8}$ in). Kích thước này được sử dụng cho định dạng "mini-SIM" của mô-đun nhận dạng thuê bao.

1.2.3. Cách thức hoạt động

Thẻ danh tính điện tử hoạt động dựa trên nhận dạng tần số vô tuyến (RFID). Đây là một công nghệ nhận dạng truyền dữ liệu thông qua việc sử dụng liên lạc không dây bằng sóng vô tuyến. RFID công nghệ lần đầu tiên được sử dụng trong Thế chiến II cho hệ thống nhận dạng bạn hay thù. RFID đã được sử dụng cho mục đích xác định một đối tượng hoặc một người. Cách truyền dữ liệu được thực hiện giữa một đầu đọc và một chip điện tử gắn vào một đồ vật hoặc một người. Hệ thống cho hộ chiếu điện tử (e-Passport) bao gồm một con chip, một đầu đọc, một ăng-ten và cơ sở hạ tầng khóa công khai (PKI).

Ở cấp độ cơ bản mỗi thẻ hoạt động theo một cách:

- Dữ liệu được lưu trữ trong chip RFID của thẻ chờ được đọc
- Ăng-ten của thẻ nhận được năng lượng từ ăng-ten của đầu đọc RFID.
- Sử dụng nguồn điện từ pin bên trong của nó hoặc năng lượng thu được từ trường điện từ của đầu đọc, thẻ sẽ gửi các sóng vô tuyến trở lại đầu đọc.

Người đọc thu nhận các sóng vô tuyến của thẻ và giải mã các tần số thành các dữ liệu có ý nghĩa

1.2.4. Mức độ an toàn của thẻ danh tính điện tử

Mức độ bảo đảm của danh tính điện tử được phân loại theo 03 mức độ: Thấp (Low), trung bình (Substantial), cao (High) được mô tả chi tiết dưới đây:

Mức độ bảo đảm	Mức độ bảo đảm bảo của danh tính điện tử (chứng minh danh tính khi đăng ký)	Mức độ xác thực
Thấp	Cung cấp danh tính từ cơ quan chức năng (từ xa hoặc trực tiếp)	Một yếu tố (mật khẩu hoặc mã pin)
Trung bình	Cung cấp danh tính (từ xa hoặc trực tiếp). Xác thực danh tính bởi cơ quan đăng ký	Nhiều yếu tố (điện thoại di động kết hợp với mã PIN)
Cao	Cung cấp giấy tờ danh tính trực tiếp tại cơ quan đăng ký. Xác thực danh tính sử dụng các nguồn chính thống và các tài liệu của cơ quan quản lý	Nhiều yếu tố. Phải truy nhập tới dữ liệu/khóa cá nhân trên các thiết bị vật lý. Có giải pháp mã hóa bảo vệ thông tin định danh cá nhân

Bảng: Mức độ đảm bảo danh tính điện tử

CHƯƠNG II. DỮ LIỆU TRÊN THẺ DANH TÍNH ĐIỆN TỬ

2.1 Dữ liệu và bảo vệ dữ liệu sinh trắc trên thẻ e-ID

2.1.1. Dữ liệu được lưu trữ trên thẻ e-ID

Con chip trên thẻ e-ID lưu trữ dữ liệu cá nhân của chủ sở hữu và đóng vai trò quan trọng trong việc bảo vệ và xác thực thông tin này. Thẻ e-ID sử dụng hai yếu tố để xác thực: "sở hữu" (thẻ e-ID) và "kiến thức" (mã PIN 6 chữ số). Chip của thẻ e-ID lưu trữ dữ liệu cá nhân và các khóa liên quan cần thiết cho quá trình xác thực. Để bắt đầu xác thực, chủ thẻ phải nhập mã PIN. Mã PIN này cũng được sử dụng để xác nhận sự đồng ý của chủ sở hữu đối với quá trình xác thực.

Con chip e-ID chứa một ứng dụng e-ID chuyên dụng, giúp lưu trữ an toàn dữ liệu cá nhân của chủ thẻ. Dữ liệu cá nhân được bảo mật trong ứng dụng e-ID và có thể được truyền đi trong quá trình xác thực. Hơn nữa, để kiểm tra tính hợp lệ của thẻ e-ID, mã thông báo thu hồi đặc biệt dành cho thẻ sẽ được so sánh với danh sách thu hồi của bên phụ thuộc. Thông tin về việc thẻ e-ID đã hết hạn hay chưa cũng sẽ được truyền đi như một phần của quá trình xác thực.

2.1.2. Xác thực đa yếu tố

Xác thực đa yếu tố sử dụng các loại thông tin khác nhau để xác nhận danh tính người dùng. Các yếu tố này bao gồm:

- Những gì bạn có: Như mã thông báo hoặc thẻ e-ID.
- Những gì bạn biết: Như mật khẩu hoặc mã PIN.
- Bạn là ai: Như dữ liệu sinh trắc học (quét móng mắt, dấu vân tay, nhận dạng khuôn mặt).

Việc sử dụng dữ liệu sinh trắc học giúp tăng cường bảo mật cho các giao dịch, bởi nó ngăn chặn người khác sử dụng ID của bạn. Các hệ thống ID như thẻ căn cước, hộ chiếu, và giấy phép lái xe thường sử dụng thông tin sinh trắc học như dấu vân tay hoặc ảnh để xác thực danh tính.

Nhiều hệ thống e-ID hiện nay cũng bắt đầu kết hợp dữ liệu sinh trắc học. Yêu cầu sinh trắc học khi hoàn tất giao dịch thêm một lớp bảo mật bằng cách liên kết e-ID với một cá nhân cụ thể. Ví dụ về dữ liệu sinh trắc học bao gồm:

- Dấu vân tay
- Dấu tay
- Nhận dạng tĩnh mạch ngón tay
- Nhận dạng khuôn mặt
- Nhận dạng móng mắt

Để tích hợp sinh trắc học vào e-ID, cần có cơ sở hạ tầng tổ chức và công nghệ để thu thập dữ liệu sinh trắc học khi đăng ký người dùng. Việc sử dụng sinh trắc học cũng yêu cầu công nghệ bổ sung, như máy quét dấu vân tay.

Một điểm trừ của việc sử dụng thông tin sinh trắc học là nó không thể thay đổi nếu bị xâm phạm (ví dụ: bạn không thể thay đổi dấu vân tay). Tuy nhiên, bảo mật từ sinh trắc học đến từ tính duy nhất của nó, không phải từ tính bí mật. Điều này nghĩa là sinh trắc học có thể ngăn ai đó sử dụng e-ID của người khác.

e-ID chuyển những nguyên tắc này vào thế giới kỹ thuật số. Các nguyên tắc cơ bản của nhận dạng điện tử qua e-ID dựa trên:

- Xác thực lẫn nhau giữa chip của thẻ e-ID và bên phụ thuộc (hoặc nhà cung cấp dịch vụ), có nghĩa là không chỉ chủ sở hữu e-ID xác thực qua e-ID cho bên phụ thuộc mà cả bên phụ thuộc xác thực trực tiếp vào chip e-ID
- Giao tiếp trực tiếp qua kênh truyền được bảo vệ từ đầu đến cuối an toàn giữa bên phụ thuộc và chip của e-ID

Nguyên tắc xác thực lẫn nhau cho phép cả hai bên giao tiếp:

- Có bằng chứng về danh tính của bộ phận đối ứng
- Thiết lập một kênh được bảo vệ từ đầu đến cuối đáng tin cậy và an toàn.

Là một phần của xác thực lẫn nhau, bên phụ thuộc phải chứng minh quyền truy cập vào dữ liệu liên quan. Chỉ có thể truy cập vào bất kỳ dữ liệu nào sau khi bên phụ thuộc xác thực thành công và xác minh các quyền truy cập tương ứng. Việc xác thực các bên liên lạc và phân quyền truy cập được thực hiện thông qua cơ sở hạ tầng khóa công khai chuyên dụng.

Tuy nhiên, không giống như các giao dịch như chữ ký, việc xuất trình thẻ e-ID không phải vĩnh viễn. Thay vào đó, quá trình nhận dạng là tạm thời và không thể được chứng minh cho bên thứ ba, thẻ e-ID cũng ánh xạ nguyên tắc này với nhận dạng điện tử. Vì dữ liệu cá nhân được lưu trữ an toàn trên chip của thẻ e-ID và được truyền qua kênh truyền đã xác thực, nên tính xác thực và tính toàn vẹn của dữ liệu được đảm bảo mà không cần phải ký vào dữ liệu. Do đó, không giống như các kế hoạch e-ID dựa trên chữ ký, bên phụ thuộc không nhận được bằng chứng nhận dạng vĩnh viễn. Từ quan điểm bảo vệ dữ liệu, điều này có lợi thế là bên phụ thuộc không thể chứng minh xác thực so với bên thứ ba.

2.1.3. Cơ chế xác thực trên thẻ e-ID

Cơ chế xác thực của e-ID được gọi là thủ tục xác thực chung. Nó bao gồm chuỗi các giao thức mật mã sau đây:

a. Xác minh mã PIN qua PACE

Giao thức PACE giúp xác minh rằng người dùng biết mã PIN của thẻ e-ID của họ và thiết lập một kênh liên lạc an toàn và bảo mật giữa thiết bị người dùng (như máy tính hoặc đầu đọc thẻ) và chip e-ID. Khi PACE được thực hiện thành công, tất cả giao tiếp tiếp theo giữa thiết bị người dùng và chip e-ID sẽ được mã hóa và bảo vệ bằng các khóa phiên mạnh, đảm bảo tính an toàn và toàn vẹn của thông tin trao đổi.

b. Xác thực lẫn nhau thông qua kiểm soát truy cập mở rộng (EAC)

Xác thực nhà cung cấp dịch vụ

Giao thức này cung cấp bằng chứng (dựa trên thử thách-phản hồi) về tính xác thực và quyền truy cập của bên phụ thuộc. Quyền truy cập của thiết bị đầu cuối được chỉ định thông qua chứng chỉ ủy quyền.

Cần có bằng chứng về quyền truy cập thông qua Xác thực đầu cuối đối với tất cả dữ liệu liên quan đến cá nhân và tài liệu được lưu trữ trong các ứng dụng của chip. Các quyền truy cập này chỉ có thể được thực hiện trong kênh được mã hóa bởi xác thực chip.

Xác thực khóa công khai thẻ e-ID

Bước này cung cấp bằng chứng về tính xác thực của dữ liệu được lưu trữ trên e-ID, đặc biệt là khóa công khai của chip. Vì mục đích này, khóa công khai của chip e-ID được nhà sản xuất thẻ ký bằng tài liệu PKI.

Xác thực tài liệu

Giao thức này cung cấp bằng chứng về việc sở hữu khóa cá nhân của e-ID (tương ứng với khóa công khai được xác minh trong quá trình Xác thực thụ động). Do đó, cùng với Xác thực thụ động, giao thức xác minh tính xác thực của e-ID. Hơn nữa, Xác thực chip thiết lập một kênh an toàn, được bảo vệ bằng mật mã từ đầu đến cuối giữa chip của e-ID và bên phụ thuộc. Chỉ sau khi kênh mã hóa đã được thiết lập, bên phụ thuộc mới có thể truy cập dữ liệu cá nhân hoặc liên quan đến tài liệu được lưu trữ trên chip e-ID.

c. Kiểm tra tính hợp lệ và đọc dữ liệu cá nhân

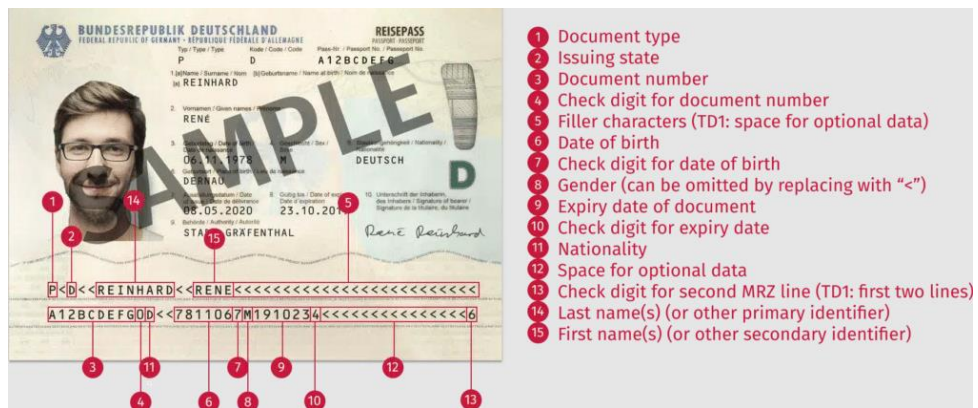
Nhà cung cấp dịch vụ kiểm tra tính hợp lệ của tài liệu, tức là tài liệu đó có bị thu hồi hay hết hạn sử dụng hay không. Nhà cung cấp dịch vụ có thể truy cập dữ liệu được lưu trữ trên e-ID theo quyền truy cập của họ và thực hiện các chức năng đặc biệt.

Khi kênh được xác thực, chủ thẻ cũng được xác thực. Hơn nữa, vì đường truyền được mã hóa, chỉ nhà cung cấp dịch vụ đã xác thực mới có thể đọc dữ liệu. Mỗi giao thức của quy trình xác thực chung đều có các mục tiêu bảo mật được xác định rõ ràng. Tính bảo mật của các giao thức được chứng minh trong các bằng chứng bảo mật mật mã.

2.1.4. Kiểm tra và truy xuất dữ liệu trên thẻ e-ID

a. Khu vực kiểm tra bằng mắt (VIZ)

Vùng kiểm tra trực quan của MRTD bao gồm các phần tử dữ liệu bắt buộc và tùy chọn được thiết kế cho hình ảnh kiểm tra. Các phần tử dữ liệu tùy chọn, cùng với các phần tử dữ liệu bắt buộc, phù hợp với yêu cầu của các quốc gia và tổ chức phát hành trong khi vẫn duy trì đủ tính đồng nhất để đảm bảo khả năng tương tác toàn cầu cho tất cả các MRTD.



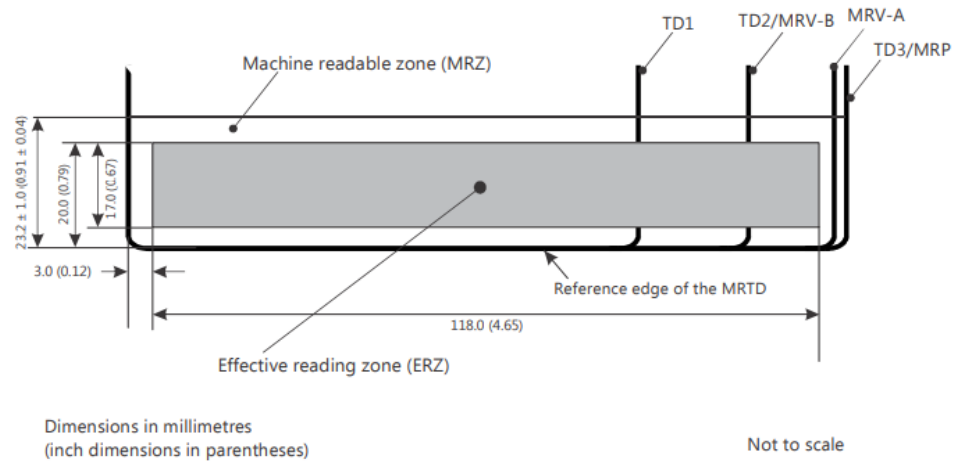
Hình 9. Vùng đọc bằng mắt (VIZ) của thẻ e-ID

b. Vùng đọc bằng máy (MRZ)

Vùng đọc máy (Machine Readable Zone - MRZ) trên thẻ căn cước điện tử (e-ID) là một khu vực chứa các thông tin cá nhân được mã hóa theo chuẩn quốc tế, giúp máy móc có thể đọc và trích xuất dữ liệu một cách tự động và nhanh chóng. MRZ thường nằm ở mặt sau hoặc dưới cùng của thẻ căn cước điện tử, tùy thuộc vào thiết kế của quốc gia phát hành.

0 1 2 3 4 5 6 7 8 9
A B C D E F G H I
J K L M N O P Q R
S T U V W X Y Z <

Hình 10. Tập hợp con các ký tự OCR-B từ [ISO 1073-2] để sử dụng trong tài liệu du lịch có thể đọc được bằng máy



Hình 11. Sơ đồ vùng đọc hiệu quả MRTD

Cấu trúc và định dạng của MRZ:

MRZ thường có định dạng chuẩn do Tổ chức Hàng không Dân dụng Quốc tế (ICAO) quy định trong tài liệu Doc 9303. Dưới đây là các yếu tố chính của MRZ:

Định dạng MRZ:

- Hai dòng ký tự (TD-1): Thường sử dụng cho thẻ căn cước và một số giấy tờ khác. Mỗi dòng có 30 ký tự.
- Ba dòng ký tự (TD-3): Thường sử dụng cho hộ chiếu. Mỗi dòng có 44 ký tự.

Thông tin trong MRZ:

- Dòng 1:
 - Ký tự bắt đầu: Loại tài liệu (ID cho thẻ căn cước).
 - Ký tự tiếp theo: Quốc gia phát hành (mã ba ký tự).
 - Họ và tên đầy đủ, được cách nhau bằng dấu "<<".
- Dòng 2:
 - Số thẻ căn cước.
 - Ký tự kiểm tra số thẻ.
 - Quốc tịch (mã ba ký tự).
 - Ngày sinh (định dạng YYMMDD).
 - Ký tự kiểm tra ngày sinh.
 - Giới tính (M/F).
 - Ngày hết hạn (định dạng YYMMDD).
 - Ký tự kiểm tra ngày hết hạn.
 - Ký tự kiểm tra toàn bộ MRZ (trong một số trường hợp).

Ví dụ về MRZ trên thẻ căn cước điện tử (TD-1):

IDVNM<NGUYEN<<THI<MINH<HANH<<<<<<<<<<<<<<<<<
1234567890VNM8101014F2501012<<<<<<<<<<<<<00

Dòng 1:

- ID: Loại tài liệu (ID cho thẻ căn cước).
- VNM: Quốc gia phát hành (Việt Nam).
- NGUYEN<<THI<MINH<HANH: Họ và tên đầy đủ.

Dòng 2:

- 1234567890: Số thẻ căn cước.
- VNM: Quốc tịch (Việt Nam).
- 810101: Ngày sinh (01 tháng 01 năm 1981).
- F: Giới tính (Nữ).
- 250101: Ngày hết hạn (01 tháng 01 năm 2025).

Lợi ích của MRZ trên thẻ căn cước điện tử:

- **Tốc độ và hiệu quả:** Giúp các hệ thống kiểm tra danh tính tự động đọc và xử lý thông tin nhanh chóng.
- **Giảm thiểu lỗi:** Giảm thiểu lỗi do nhập liệu thủ công, đảm bảo tính chính xác của thông tin.
- **Tính toàn cầu:** Theo chuẩn ICAO, MRZ có thể được đọc bởi các hệ thống kiểm tra danh tính trên toàn thế giới.

Vùng đọc máy (MRZ) là một phần quan trọng của thẻ căn cước điện tử, giúp cải thiện tính hiệu quả và độ tin cậy của quá trình xác thực danh tính tại các điểm kiểm soát an ninh và trong các giao dịch điện tử.

2.2 Quy trình truy xuất dữ liệu trên e-ID

Quy trình truy xuất dữ liệu trên chip để xác thực hệ thống kiểm tra bao gồm các bước sau. Nếu PACE (phần chương III) không được hỗ trợ bởi hệ thống kiểm tra, Bước 1 và 2 bị bỏ qua.

B1. Đọc EF.CardAccess (cần thiết)

Nếu PACE được hỗ trợ bởi eMRTD, thì chip eMRTD phải cung cấp các tham số được sử dụng cho PACE trong tệp EF.CardAccess.

Nếu EF.CardAccess có sẵn, hệ thống kiểm tra sẽ đọc tệp EF.CardAccess (Tệp EF.CardAccess có trong tệp chính là bắt buộc nếu PACE được hỗ trợ bởi eMRTD chip và SHALL chứa các SecurityInfos liên quan được yêu cầu cho PACE) để xác

định các tham số (tức là mật mã đối xứng, thuật toán thỏa thuận khóa, miền tham số và ánh xạ) được hỗ trợ bởi chip eMRTD. Hệ thống kiểm tra có thể chọn bất kỳ thông số.

Nếu tệp EF.CardAccess không có sẵn hoặc không chứa các tham số cho PACE, hệ thống kiểm tra NÊN cố gắng đọc eMRTD với Kiểm soát Truy cập Cơ bản (bỏ qua Bước 4).

B2. PACE (Tùy chọn)

Bước này được khuyến cáo nếu PACE được chip eMRTD hỗ trợ.

- Hệ thống kiểm tra nên lấy khóa K_{π} từ MRZ. Có thể sử dụng CAN thay vì MRZ nếu CAN được nhận biết trên hệ thống kiểm tra.
- Chip eMRTD SHALL chấp nhận MRZ làm mật khẩu cho PACE.
- Hệ thống kiểm tra và chip eMRTD xác thực lẫn nhau bằng cách sử dụng K_{π} và lấy các khóa phiên $K_{S_{Enc}}$ và $K_{S_{MAC}}$ (Giao thức PACE được mô tả trong Phần chương III)

Nếu thành công, chip eMRTD thực hiện những việc sau:

- Nó sẽ bắt đầu nhấn tin an toàn.
- Nó sẽ cấp quyền truy cập vào dữ liệu ít nhạy cảm hơn (ví dụ: DG1, DG2, DG14, DG15, ...)
- Nó sẽ hạn chế quyền truy cập để yêu cầu nhấn tin an toàn.

B3. Chọn Ứng dụng eMRTD (cần thiết)

B4. Kiểm soát truy cập cơ bản (tùy chọn)

Bước này là bắt buộc nếu kiểm soát truy cập chip được thực thi bởi chip eMRTD và PACE chưa được đã sử dụng. Nếu PACE được thực hiện thành công hoặc nếu eMRTD không thực thi Kiểm soát truy cập chip, điều này bước bị bỏ qua.

- Hệ thống kiểm tra NÊN lấy các Khóa Truy cập Cơ bản của Tài liệu (K_{Enc} và K_{MAC}) từ MRZ.

- Hệ thống kiểm tra và chip eMRTD xác thực lẫn nhau bằng Quyền truy cập Cơ bản về Tài liệu

Khóa và lấy khóa phiên KS_{Enc} và KS_{MAC} .

Nếu thành công, chip eMRTD thực hiện những việc sau:

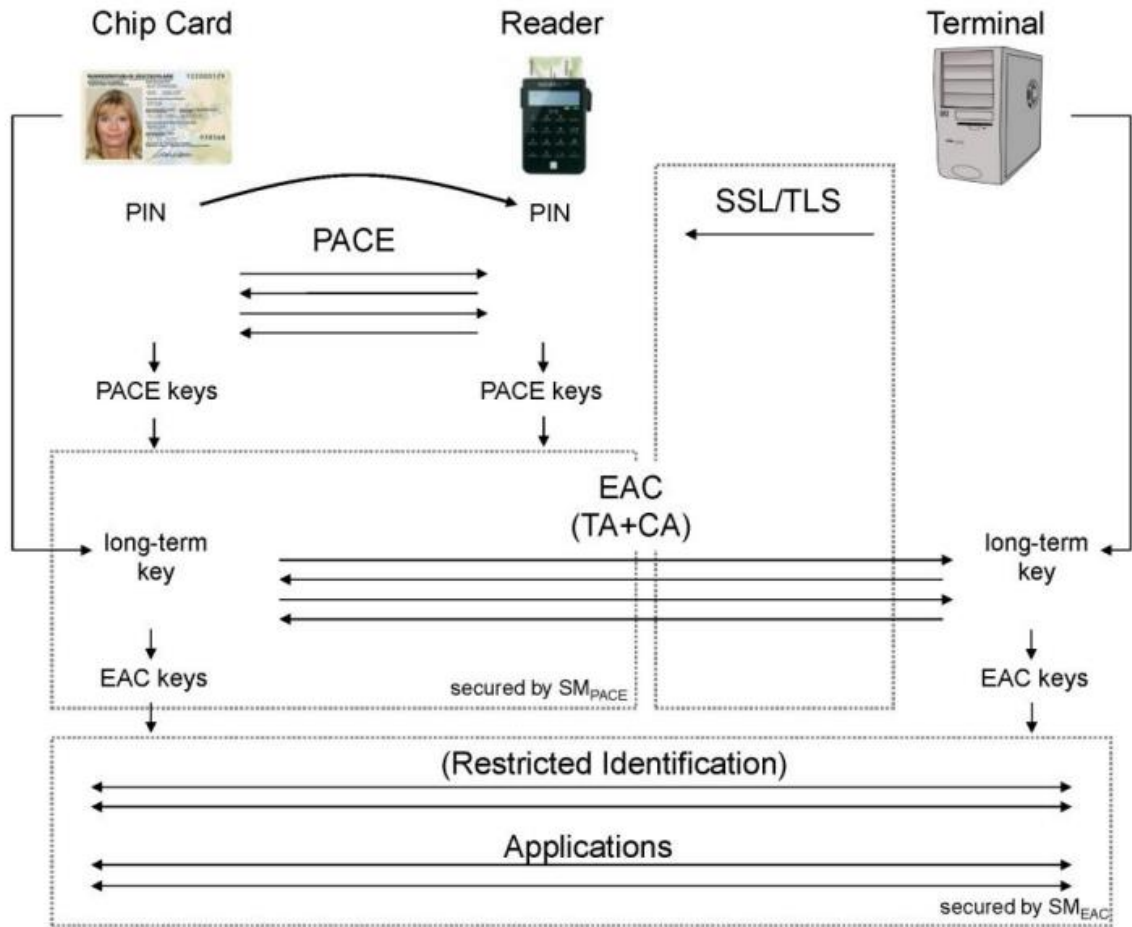
- Nó sẽ bắt đầu Nhấn tin an toàn.
- Nó sẽ cấp quyền truy cập vào dữ liệu ít nhạy cảm hơn (ví dụ: DG1, DG2, DG14, DG15, ...)
- Nó sẽ hạn chế quyền truy cập để yêu cầu Nhấn tin an toàn.

Hệ thống kiểm tra phải xác minh tính xác thực của nội dung tệp EF.CardAccess sử dụng DG14.

2.2.1 Các giao thức mật mã được triển khai trên e-ID

Các giao thức mật mã được triển khai trên thẻ e-ID xây dựng giao tiếp tương ứng giữa thẻ chip và đầu đọc thẻ hoặc thiết bị đầu cuối. Mô tả tổng quan về tất cả các giao thức đồ họa có liên quan.

Về cơ bản, giao thức tạo ra một khóa Diffie – Hellman an toàn từ một mật khẩu entropy thấp - mã PIN cho thẻ e-ID của Đức - mà chủ sở hữu phải nhập vào đầu đọc hoặc được truyền qua đầu đọc của máy- vùng có thể đọc được. Khóa Diffie – Hellman (đã băm) này sau đó được sử dụng để bảo mật thông tin liên lạc thông qua giao thức an toàn mà mô tả bên dưới.



Hình 12. Các giao thức mật mã

Giao thức kiểm soát truy cập mở rộng (EAC) ban đầu được đề xuất bởi Văn phòng Bảo mật Thông tin Liên bang Đức (BSI) cho hệ chiếu điện tử (ePASS). Nó cung cấp một thiết lập khóa an toàn giữa thẻ chip và thiết bị đầu cuối, sử dụng cơ sở hạ tầng khóa công khai. Phiên bản mới của EAC được trình bày trong luận án này (với một số đơn giản hóa nhỏ nhằm mục đích trình bày, nhưng không vi phạm các đặc tính bảo mật của giao thức tổng thể). EAC phục vụ mục đích hạn chế quyền truy cập vào dữ liệu nhạy cảm được lưu trữ trên thẻ chip (ví dụ: dấu vân tay, móng mắt,...). Các BSI đã tích hợp EAC trong thẻ nhận dạng điện tử (e-ID) của Đức để bảo vệ toàn bộ dữ liệu cá nhân được ghi lại.

Giao thức EAC bao gồm hai giai đoạn: giao thức xác thực đầu cuối (TA) là giao thức phản hồi thử thách trong đó thiết bị đầu cuối ký một thử thách ngẫu nhiên

(và một khóa công khai tạm thời) bằng khóa ký được chứng nhận của nó, và giao thức xác thực chip (CA), trong đó cả hai bên lấy khóa Diffie – Hellman từ khóa tạm thời của thiết bị đầu cuối và khóa tĩnh, được chứng nhận của chip và cuối cùng chip sẽ tính mã xác thực thông báo để xác thực.

Giao thức nhắn tin bảo mật (SM) như được chỉ định trong xây dựng một kênh bảo mật bảo toàn tính toàn vẹn từ đầu đến cuối, kênh này yêu cầu khóa bí mật được chia sẻ bởi thẻ chip và đầu đọc hoặc thiết bị đầu cuối tương ứng và cho phép các bên giao tiếp một cách an toàn qua một kênh chữa bệnh nội bộ. Đặc biệt, SM cung cấp tính bảo mật và tính xác thực cho các tin nhắn được trao đổi. Nó sử dụng mô hình Encrypt-thenAuthenticate triển khai một kênh an toàn nếu các khóa đầu vào được phân bổ đồng nhất.

Giao thức nhắn tin an toàn được chạy hai lần. Đầu tiên, các thông điệp giữa thẻ chip và đầu đọc thẻ được bảo mật bằng khóa phiên do PACE thu được. Thứ hai, các khóa có được bằng cách chạy EAC đóng vai trò là đầu vào cho SM để cung cấp bảo mật đầu cuối. Biểu thị giao thức SM bằng SMPACE với đầu vào là các khóa PACE, và SMEAC biểu thị giao thức chạy cho các khóa EAC.

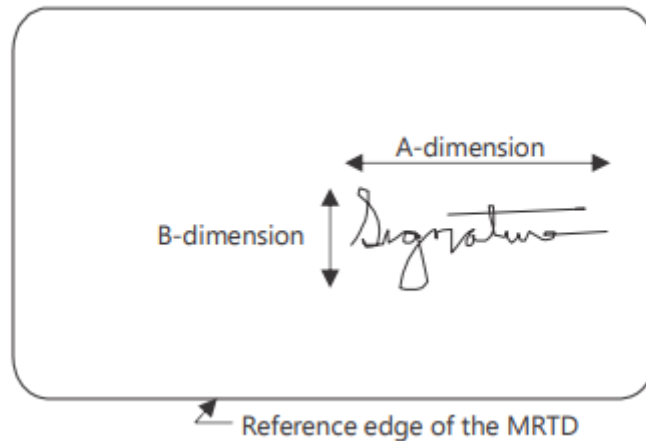
Nhận dạng bị hạn chế. Thiết kế tổng thể của thẻ nhận dạng bao gồm một giao thức khác, được gọi là nhận dạng hạn chế (RI). Trong giao thức tùy chọn này, chủ thẻ có thể sử dụng các bút danh theo miền cụ thể để tương tác với các nhà cung cấp dịch vụ sao cho (a) nhà cung cấp dịch vụ có thể nhận ra các bút danh của các thẻ riêng lẻ và sử dụng thông tin này cho dịch vụ (khả năng liên kết theo miền cụ thể) và (b) các nhà cung cấp dịch vụ khác nhau không thể liên kết các tương tác của một người dùng trong các miền tương ứng của họ (ẩn danh giữa nhiều miền).

Giao thức nhận dạng hạn chế được chạy ngay sau khi một kênh bảo mật được xây dựng giữa thẻ chip và nhà cung cấp dịch vụ tương ứng bằng cách chạy SMEAC. Sau đó, bất kỳ ứng dụng thẻ nào cũng có thể được chạy miễn là liên lạc liên quan được bảo mật và bí mật.

2.3. Các kỹ thuật mật mã đảm bảo an toàn dữ liệu cho dữ liệu e-ID

2.3.1 Chữ ký số (Digital Signature)

Chữ ký (kỹ thuật số) cho phép một bên cung cấp bằng chứng có thể xác minh công khai rằng một tin nhắn nhất định được nó chấp thuận. Nó là chất tương tự kỹ thuật số của một chữ ký viết tay. Đại khái là bất kỳ ai có thể sản xuất chữ ký thay mặt cho một bên phải biết tài liệu bí mật tương ứng của bên đó.



Hình 13. Hướng chữ kí được hiển thị

Điều này cung cấp một phương tiện đảm bảo tính xác thực của dữ liệu. Chữ ký điện tử là các công cụ quan trọng trong các giao thức trao đổi khóa, nơi các bên có thể xác minh rằng đối tác trong một phiên là đối tác hợp pháp. Định nghĩa sau chụp chữ ký điện tử chính thức.

Sơ đồ chữ ký (kỹ thuật số) bao gồm ba thuật toán PPT (SKGen, Sig, SVf) được định nghĩa như sau:

- Key Generation: Khi nhập thông số bảo mật 1^λ , thuật toán xác suất SKGen xuất ra một cặp khóa (sk, pk) trong đó sk (tương ứng pk) biểu thị chữ ký (tương ứng xác minh công khai) khóa.
- Signature: Khi nhập một phím ký sk và một thông báo m, thuật toán xác suất sig xuất ra một chữ ký σ

- Verification: Khi nhập khóa xác minh pk , một tin nhắn m và một chữ ký σ , thuật toán xác định SVf xuất ra 1 (= hợp lệ) hoặc 0 (= không hợp lệ).

Các bước bạn đề cập liên quan đến cơ chế của hệ thống chữ ký số, một thành phần quan trọng của PKI. Dưới đây là giải thích chi tiết về từng bước trong quy trình này:

Bước 1: Key Generation (Tạo khóa)

- Nhập thông số bảo mật λ : Thông số bảo mật λ là một giá trị đầu vào để xác định mức độ bảo mật của hệ thống. Thông số này thường liên quan đến kích thước của khóa (ví dụ: λ có thể là 2048 bit, 3072 bit, v.v.). Một giá trị λ lớn hơn sẽ cung cấp mức độ bảo mật cao hơn nhưng cũng yêu cầu tính toán nhiều hơn.
- **Thuật toán xác suất SKGen**: Đây là thuật toán tạo khóa, sử dụng thông số bảo mật λ để sinh ra một cặp khóa.
 - $sksk$ (private key - khóa riêng): Khóa riêng được giữ bí mật và sử dụng để tạo chữ ký số.
 - $pkpk$ (public key - khóa công khai): Khóa công khai được phân phối rộng rãi và sử dụng để xác minh chữ ký số.

Bước 2: Signature (Tạo chữ ký)

- **Nhập khóa ký $sksk$ và thông báo mm** :
 - $sksk$: Khóa riêng của người ký.
 - mm : Thông báo hoặc dữ liệu mà bạn muốn ký.
- Thuật toán xác suất sig: Thuật toán này sử dụng khóa riêng $sksk$ và thông báo mm để tạo ra chữ ký số σ .
 - Chữ ký σ : Kết quả đầu ra là chữ ký số, là một đoạn mã hóa duy nhất xác định rằng thông báo mm đã được ký bởi chủ sở hữu khóa riêng $sksk$.

Bước 3: Verification (Xác minh chữ ký)

- **Nhập khóa xác minh $pkpk$, tin nhắn mm và chữ ký σ :**
 - $pkpk$: Khóa công khai tương ứng với khóa riêng $sksk$ đã sử dụng để ký thông báo.
 - mm : Thông báo hoặc dữ liệu đã được ký.
 - σ : Chữ ký số đã được tạo.
- **Thuật toán xác định SVf:** Thuật toán này kiểm tra xem chữ ký σ có hợp lệ cho thông báo mm với khóa công khai $pkpk$ hay không.
 - Đầu ra 1 (hợp lệ): Nếu chữ ký σ hợp lệ, tức là nó thực sự được tạo bởi khóa riêng tương ứng với khóa công khai $pkpk$, thuật toán trả về 1.
 - Đầu ra 0 (không hợp lệ): Nếu chữ ký σ không hợp lệ, thuật toán trả về 0, nghĩa là chữ ký không khớp hoặc không được tạo bởi khóa riêng tương ứng với khóa công khai $pkpk$.

Quy trình tổng thể

Bước 1: Tạo khóa: Một người dùng hoặc hệ thống tạo ra một cặp khóa công khai và khóa riêng.

Bước 2: Ký thông báo: Người dùng sử dụng khóa riêng của mình để ký một thông báo, tạo ra chữ ký số.

Bước 3: Xác minh chữ ký: Một bên thứ ba có thể sử dụng khóa công khai để xác minh tính hợp lệ của chữ ký trên thông báo.

Ví dụ cụ thể:

Bước 1: Tạo khóa

Alice muốn gửi thông báo một cách an toàn. Cô ấy sử dụng thuật toán SKGen để tạo cặp khóa (khóa riêng $sksk$ và khóa công khai $pkpk$).

Bước 2: Ký thông báo

Alice có thông báo mm muốn ký. Cô ấy sử dụng khóa riêng $sksk$ và thuật toán sig để tạo chữ ký số $\sigma\sigma$.

Bước 3: Xác minh chữ ký

Bob nhận được thông báo mm và chữ ký $\sigma\sigma$ từ Alice. Anh ấy sử dụng khóa công khai $pkpk$ của Alice và thuật toán SVf để kiểm tra tính hợp lệ của chữ ký $\sigma\sigma$.

Nếu thuật toán trả về 1, Bob biết rằng thông báo mm thực sự được ký bởi Alice. Nếu thuật toán trả về 0, Bob biết rằng có gì đó không đúng với chữ ký.

Kết luận

Quy trình này giúp đảm bảo tính toàn vẹn và xác thực của thông tin trong các giao dịch số. Khóa riêng và khóa công khai cùng chữ ký số tạo nên một hệ thống bảo mật mạnh mẽ để chống lại việc giả mạo và lừa đảo.

Yêu cầu xác minh tính chính xác, tức là người xác minh phải luôn chấp nhận chữ ký xác thực. Chính thức hơn, đối với bất kỳ tham số bảo mật nào λ , bất kỳ $(sk, pk) \leftarrow \text{SKGen}(1^\lambda)$, đối với bất kỳ thông điệp m , bất kỳ chữ ký nào $\sigma \leftarrow \text{Sig}(sk, m)$, chúng tôi phải có $\text{SVf}(pk, m, \sigma) = 1$. Từ sơ đồ chữ ký, yêu cầu không người ngoài nào có thể giả mạo chữ ký của người ký. Về mặt hình thức, thuộc tính này được gọi là không thể chống lại được các cuộc tấn công theo thông điệp được lựa chọn một cách thích ứng (unf-cma).

2.3.2. Các chương trình mã hóa dữ liệu

Các chương trình mã hóa cho phép người dùng gửi tin nhắn đến người nhận qua một kênh liên lạc không an toàn trong khi vẫn giữ được tính bảo mật của tin nhắn. Nói một cách dễ hiểu, việc mã hóa một thông điệp không tiết lộ bất kỳ thông tin nào về thông điệp và chỉ người biết khóa bí mật tương ứng mới có thể khôi phục được bản rõ đã được mã hóa. Các giao thức liên quan đến thẻ e-ID sử dụng các sơ đồ mã hóa đối xứng, trong đó cả mã hóa thông điệp và giải mã mật mã đều yêu cầu khóa bí mật. Định nghĩa sau đây nắm bắt các sơ đồ mã hóa đối xứng một cách chính thức.

Sơ đồ mã hóa đối xứng một lược đồ mã hóa đối xứng bao gồm ba thuật toán thời gian đa thức $E = (\text{KGen}, \text{Enc}, \text{Dec})$ được định nghĩa như sau:

Kgen (Key Generation): Thuật toán KGen tạo ra một khóa bí mật dùng cho cả quá trình mã hóa và giải mã. Khóa này cần được giữ bí mật và chỉ chia sẻ giữa các bên giao tiếp an toàn.

Enc (Encryption): Thuật toán Enc nhận đầu vào là bản rõ và khóa bí mật, sau đó tạo ra bản mã bằng cách áp dụng các phép biến đổi mã hóa dựa trên khóa bí mật.

Dec (Decryption): Thuật toán Dec nhận đầu vào là bản mã và khóa bí mật, sau đó khôi phục lại bản rõ bằng cách áp dụng các phép biến đổi ngược lại của mã hóa dựa trên khóa bí mật.

Kgen sẽ tạo ra khóa bí mật k .

Enc sử dụng khóa k để mã hóa bản rõ m thành bản mã c

Dec sử dụng khóa k để giải mã bản mã c thành bản rõ m

Sơ đồ mã hóa đối xứng đảm bảo rằng chỉ có những ai sở hữu khóa bí mật k mới có thể mã hóa và giải mã thông tin một cách an toàn. Việc bảo mật của sơ đồ này phụ thuộc hoàn toàn vào việc giữ bí mật khóa k .

CHƯƠNG III. CƠ CHẾ BẢO MẬT PACE, EAC VÀ MÔ HÌNH XÁC THỤ E-ID

3.1. Các vấn đề nguy hiểm tồn tại trên thẻ e-ID

Vấn đề bảo mật thông tin lưu trong thẻ nhớ không cần tiếp xúc của hộ chiếu điện tử chủ yếu liên quan đến những nguy cơ chính của công nghệ RFID. Theo các tài liệu nghiên cứu của tác giả Ari Juels, David Molnar và David Wagner, có 5 nguy cơ mất an toàn/bảo mật thông tin đối với công nghệ RFID như sau:

- ***Clandestine Tracking***: nguy cơ này liên quan đến định danh của một thẻ RFID. Việc xác định được ID của một thẻ nhớ không cần tiếp xúc có thể cho phép những nghe lén xác định được nguồn gốc của chủ sở hữu và một số thông tin cá nhân quan trọng khác.
- ***Skimming and Cloning***: nguy cơ này liên quan đến khả năng nhân bản và sao chép dữ liệu từ chip RFID. Kẻ xấu có thể sao chép thông tin từ e-ID và tạo bản sao, điều này rất nguy hiểm.
- ***Eavesdropping***: nguy cơ nghe lén phức tạp luôn được coi là nguy cơ có tính nguy hiểm nhất trong an toàn, bảo mật hộ chiếu điện tử. Nguy cơ diễn ra trong quá trình đọc dữ liệu từ thẻ nhớ không cần tiếp xúc đến máy đọc. Lý do chủ yếu xuất phát từ khả năng những thông tin được truyền bằng công nghệ RFID giữa chip-reader có thể bị nghe lén trong một khoảng cách nhất định (khoảng vài mét).
- ***Biometric Data-Leakage***: nguy cơ lộ dữ liệu sinh trắc. Nguy cơ này liên quan mật thiết đến vấn đề đảm bảo an toàn đối với những dữ liệu sinh trắc nói riêng và những dữ liệu được lưu trong chip nói chung của các thẻ nhớ không cần tiếp xúc.
- ***Cryptographic Weaknesses***: liên quan đến cách thông tin được bảo vệ trong chip RFID. Đảm bảo sự an toàn của dữ liệu trong chip là một phần quan trọng để đối phó với các nguy cơ khác.

3.2. Cơ chế bảo mật PACE và EAC

3.2.1. Cơ chế bảo mật PACE

PACE là một giao thức trao đổi khóa dựa trên mật khẩu, và nó có những tính chất bảo mật nhất định như sau:

- Sử dụng các công cụ mã hóa và băm an toàn: PACE sử dụng các công cụ mã hóa và hàm băm được coi là an toàn để bảo vệ thông tin. Điều này đảm bảo rằng dữ liệu truyền qua mạng là an toàn và không thể bị đánh cắp hoặc chỉnh sửa.
- Lý tưởng trong mô hình tiên tri ngẫu nhiên và mật mã lý tưởng: PACE được thiết kế để hoạt động trong mô hình lý tưởng, có nghĩa là nó cung cấp mức độ bảo mật cao trong môi trường lý tưởng. Điều này giúp đảm bảo rằng giao thức hoạt động đúng cách và không bị tấn công một cách dễ dàng.
- Xác thực tin nhắn M không dễ bị tấn công: PACE được thiết kế để ngăn chặn các cuộc tấn công như xâm nhập hoặc làm giả tin nhắn M một cách hiệu quả. Điều này giúp đảm bảo rằng dữ liệu truyền đi là tin cậy và không bị thay đổi.
- Khó khăn trong giải bài toán gPACE-DH: Giả định rằng việc giải quyết bài toán gPACE-DH là khó, nghĩa là không dễ dàng để tính toán một giá trị cụ thể từ một giá trị khác. Điều này làm tăng tính bảo mật của giao thức, bảo vệ khỏi các cuộc tấn công từ việc giải quyết bài toán này.

Tóm lại, PACE được thiết kế để cung cấp mức độ bảo mật cao và ngăn chặn các cuộc tấn công từ việc tiếp cận, xâm nhập hoặc làm giả dữ liệu trao đổi giữa các thiết bị.

Để chứng minh tính bảo mật, một giả định lý thuyết số mới được đưa ra, được gọi là phần tử DH được chọn dựa trên mật khẩu chung (gPACE-DH) vấn đề liên quan đến giả định DH. Nó cho phép suy luận về bảo mật của giao thức PACE độc lập với sự lựa chọn tương ứng cho Map2Point. Vấn đề gPACE-DH ghi lại thực tế là trong PACE, đối thủ có thể trực tiếp chọn các giá trị đầu vào như y_C và y_T hoặc đối thủ có thể gián tiếp thông qua quá trình ánh xạ vào trình tạo nhóm G , bao gồm việc chọn giá trị nonce và các giá trị tạm thời trong Map2point. Giả định gPACE-DH được thiết kế để bảo vệ giao thức PACE bằng cách đảm bảo rằng ngay cả khi đối thủ có khả

năng can thiệp vào quá trình tính toán, họ vẫn không thể dự đoán hoặc tính toán được khóa cuối cùng. Điều này làm cho khóa phiên trở nên ngẫu nhiên và bảo mật trước mọi nỗ lực tấn công của đối thủ. Đặc biệt, điều này có nghĩa là giá trị DH được bấm, xác định (các) khóa phiên, trông ngẫu nhiên với một đối thủ và do đó, đối thủ không thể giành chiến thắng trong mô hình BPR bằng cách phân biệt khóa phiên với chìa khóa lấy mẫu. Về mặt hình thức, gPACE-DH được định nghĩa như sau.

Bài toán DH phần tử được chọn dựa trên mật khẩu là (t, N, Q, ϵ) -hard (đối với Map2Point) nếu đối với bất kỳ thuật toán nào $A = (A0, A1, A2)$ chạy trong thời gian t , xác suất mà thử nghiệm sau trả về 1 nhiều nhất là $1N + \epsilon$.

gPACE-DH

Map2Point, $N, Q, A(\lambda)$

pick authenticated group parameters $G = (a, b, p, q, g, \lambda)$ $(s1, \dots, sn, st) \leftarrow_R A0(G, N)$ with $s1, \dots, sn$ pairwise distinct pick $yT \leftarrow_R Z_q$ and $k \leftarrow_R [N]$

let g be the local output of the honest party in an run of Map2Point(sk),

where $A1(st)$ controls the other party (updating state information st).

$(YC, K1, \dots, KQ) \leftarrow A2(state, g^yT)$

Return 1

iff $YC \neq 0$ and $Ki = Y^yT C$ for some $i \in [Q]$.

Hình 14. Mô tả giao thức gPACE-DH

3.2.2. Cơ chế bảo mật EAC

Giao thức Kiểm soát Truy cập Mở rộng (EAC) bởi Văn phòng Bảo mật Thông tin Liên bang Đức (BSI), dành cho thẻ định danh điện tử. Nó có nghĩa là cung cấp thiết lập khóa an toàn giữa thẻ chip và một thiết bị đầu cuối, sử dụng cơ sở hạ tầng khóa công khai. Phiên bản mới nhất của EAC, được đề nghị cho thẻ ID, được trình bày trong đồ án này (với một số đơn giản hóa một chút để trình bày, nhưng không thay đổi thuộc tính bảo mật của giao thức tổng thể). EAC cho phép thiết bị đầu cuối truy cập dữ liệu nhạy cảm trên thẻ (ví dụ: dấu vân tay được lưu trữ). BSI tích hợp

EAC trong thẻ ID của Đức để đảm bảo bảo vệ đầy đủ tất cả những gì đã ghi dữ liệu cá nhân.

Giao thức EAC bao gồm hai giai đoạn: Xác thực đầu cuối (TA) là một giao thức phản hồi thử thách trong đó thiết bị đầu cuối ký một thử thách ngẫu nhiên (và một khóa công khai tạm thời) bằng khóa ký được chứng nhận của nó và Chip Xác thực (CA), trong đó cả hai bên lấy khóa Diffie – Hellman từ khóa tạm thời của thiết bị đầu cuối và khóa được chứng nhận tĩnh của chip, trong lần thứ hai phần chip kết thúc bằng cách tính toán và gửi mã xác thực tin nhắn để xác thực.

Lưu ý rằng giao thức trao đổi khóa EAC chỉ là một thành phần trong khung bảo mật cho chứng minh nhân dân và hộ chiếu. Một giao thức phụ khác là thiết lập kết nối được xác thực bằng mật khẩu (PACE) đảm bảo trao đổi khóa an toàn giữa thẻ và đầu đọc (giữa thẻ và thiết bị đầu cuối). Giao thức PACE được thực thi đầu tiên, và sau đó giao tiếp giữa thẻ và thiết bị đầu cuối được bảo mật thông qua giao thức EAC. Lưu ý rằng đầu đọc và thiết bị đầu cuối phải cũng được kết nối an toàn thông qua, chẳng hạn, SSL / TLS, trước các khóa trong EAC giao thức được bắt nguồn bởi chip và thiết bị đầu cuối.

3.2.3. Mô hình thử nghiệm xác thực e-ID áp dụng cơ chế PACE và EAC

Mô hình xác thực e-ID

Tiến hành xây dựng mô hình xác thực e-ID tích hợp cả hai cơ chế PACE và EAC. Mô hình này bao gồm các bước chính sau:

Bước 1: Người mang thẻ danh tích điện tử chiếu xuất trình cho cơ quan kiểm tra, cơ quan tiến hành thu nhận các đặc tính sinh trắc học từ người xuất trình thẻ.

Bước 2: Kiểm tra các đặc tính bảo mật trên thẻ thông qua các đặc điểm an ninh truyền thống đã biết: thủy ấn, dải quang học, lớp bảo vệ ảnh...

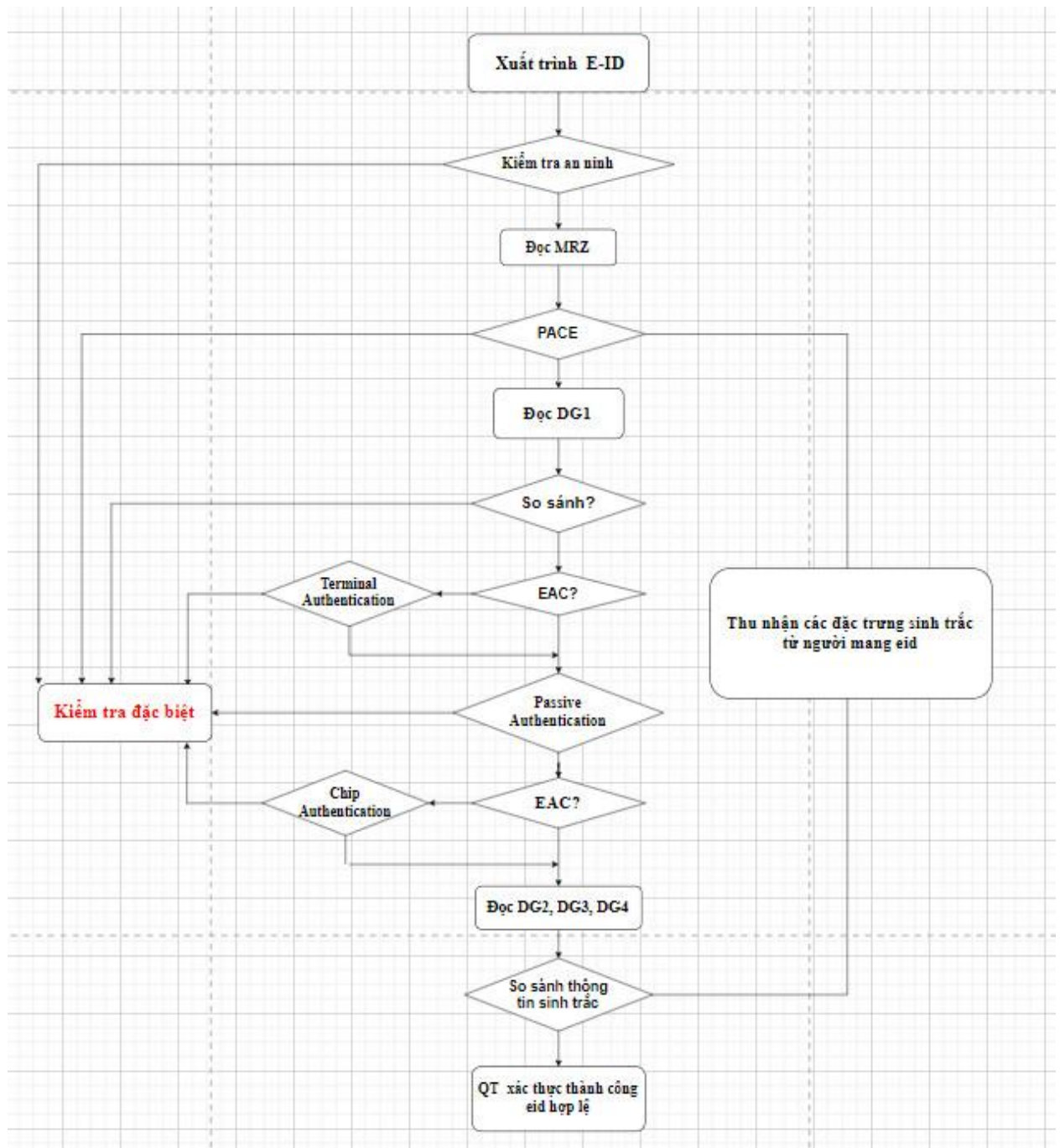
Bước 3: IS và RFID thực hiện quá trình PACE. Sau khi PACE thành công, IS có thể đọc các thông tin trong chip ngoại trừ DG3, DG4 (ảnh vân tay và móng mắt), mọi thông tin trao đổi giữa đầu đọc và chip được truyền thông báo bảo mật, mã hoá sau đó là xác thực theo cặp khoá (KENC, KMAC) có được từ quá trình PACE.

Bước 4: Tiến hành quá trình TA để chứng minh quyền truy cập của đầu đọc đến phần dữ liệu DG3, DG4.

Bước 5: Thực hiện PA để kiểm tra tính xác thực và toàn vẹn của các thông tin lưu trong chip thông qua kiểm tra chữ ký trong SOD bằng khoá công khai của cơ quan cấp e-ID. Việc trao đổi khoá thông qua chứng chỉ số theo mô hình khuyến cáo của ICAO.

Bước 6: Tiến hành CA để chứng minh được tính nguyên gốc của chip đồng thời cung cấp khoá phiên mạnh cho truyền thông bảo mật.

Bước 7: IS đối sánh dữ liệu sinh trắc thu nhận được trực tiếp từ người xuất trình e-ID với dữ liệu sinh trắc lưu trong chip. Nếu quá trình đối sánh thành công và kết hợp với các chứng thực trên, cơ quan kiểm tra e-ID có đủ điều kiện để tin tưởng e-ID là xác thực và người mang e-ID đúng là con người mô tả trong e-ID. Nếu cơ quan kiểm tra e-ID không triển khai EAC thì IS đó không có quyền truy cập DG3 và DG4. Thông tin sinh trắc học duy nhất dùng để đối sánh chỉ là ảnh khuôn mặt.



Hình 15. Mô hình xác thực e-ID

Giải thích mô hình với cơ chế PACE và EAC:

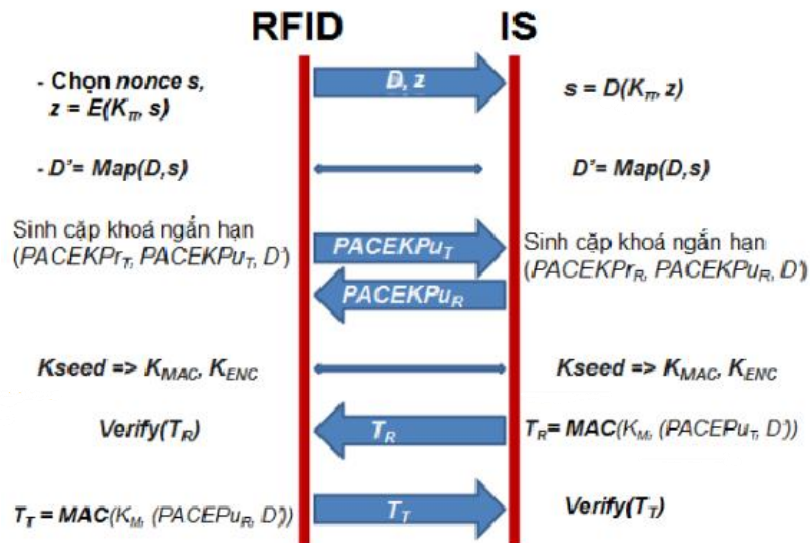
Bước 1. Kiểm tra an ninh Công dân mang e-ID xuất trình thẻ cho hệ thống kiểm duyệt (IS). Trước tiên e-ID cần phải trải qua một số bước kiểm tra an ninh nghiệp vụ truyền thống tại các điểm xuất/nhập cảnh như dùng lớp kim loại bảo vệ để

tạo hiệu ứng lồng Faraday nhằm chống khả năng đọc thông tin trong chip RFID ngoài ý muốn của người mang e-ID hay dùng thủy ấn để bảo vệ booklet...

Bước 2. PACE thiết lập các thông báo bảo mật giữa chip RFID và IS, sử dụng mật khẩu đơn giản, theo các bước như lược đồ sau:

- Chip RFID sinh ra ngẫu nhiên s , mã hoá s sử dụng $K_\pi : z = E(K_\pi, s)$ với $K_\pi = \text{SHA-1}(\pi||3)$ và gửi bản mã z cùng các tham số miền tỉnh D đến cho IS.
- IS khôi phục lại bản rõ $s = D(K_\pi, z)$ sử dụng mật khẩu chung π .
- Cả RFID và IS cùng thực hiện các bước sau:
 - Tính các tham số miền tỉnh D' dựa trên D và s : $D' = \text{Map}(D, s)$
 - Thực hiện giao thức thoả thuận khoá DiffieHellman dựa trên D' và khoá chia sẻ.
 - $K = \text{KA}(\text{PACEKPrT}, \text{PACEKPrR}, D') = \text{KA}(\text{PACEKPrR}, \text{PACEKPrT}, D')$

Trong suốt quá trình thoả thuận khoá DH, mỗi bên phải kiểm tra rằng hai khoá công khai PACEKPrR và PACEKPrT là khác nhau. Từ đó cả hai bên tính cả khoá phiên K_{MAC} và K_{ENC} . RFID tính thẻ xác thực $T_T = \text{MAC}(K_M, (\text{PACEKPrR}, D'))$ và gửi đến cho IS thẩm định. IS tính thẻ xác thực $T_R = \text{MAC}(K_M, (\text{PACEKPrT}, D'))$ và gửi đến cho RFID thẩm định.



Hình 16. Lược đồ PACE

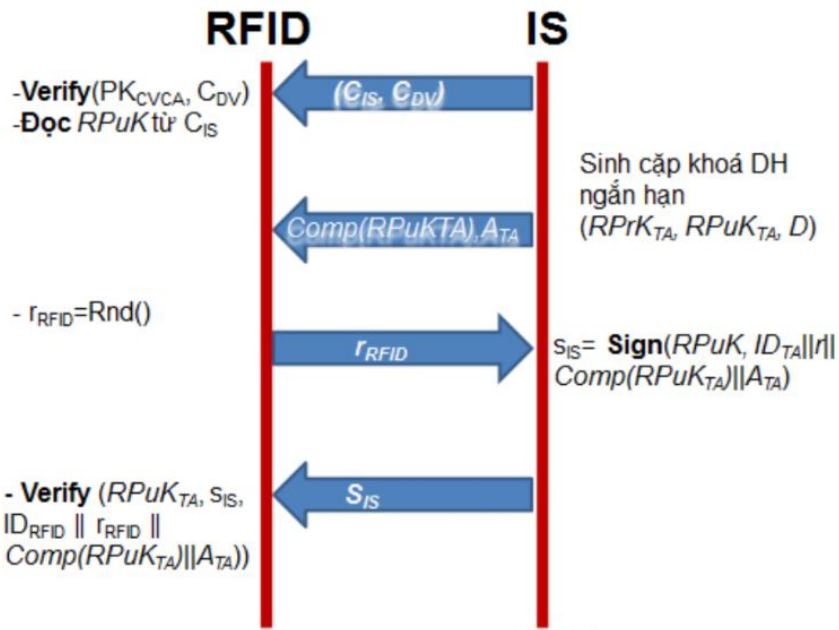
Bước 3: Đọc vùng dữ liệu DG1

Sau khi PACE thành công, hệ thống xác thực e-ID sẽ tiến hành đọc vùng dữ liệu DG1 trong chip RFID của e-ID và so sánh với những dữ liệu hệ thống đã đọc được từ vùng MRZ. Nếu dữ liệu trùng nhau thì chuyển sang bước 4, nếu không thì chuyển qua bước kiểm tra đặc biệt.

Bước 4: Xác thực đầu đọc

TA cho phép chip RFID thẩm định liệu đầu đọc có được quyền truy cập vào vùng dữ liệu nhạy cảm hay không (ảnh vân tay, ảnh mống mắt, ...). Các bước trong TA như sau:

- IS gửi chuỗi chứng chỉ đến chip gồm CIS và CDV.
- RFID kiểm chứng các chứng chỉ này sử dụng PKCVCA và trích khoá công khai của đầu đọc RPuK.
- IS sinh ra cặp khoá DH ngắn hạn trên miền D: RPrKTA, RPuKTA. Sau nó gửi $\text{Comp}(\text{RPuKTA})$ và dữ liệu ATA đến cho RFID.
- RFID gửi thách đố ngẫu nhiên rRFID đến IS.
- IS trả lời bằng chữ ký
$$sIS = \text{Sign}(\text{RPuK}, \text{IDTA} || r || \text{Comp}(\text{RPuKTA}) || \text{ATA})$$
- Chip kiểm tra chữ ký nhận được từ IS bằng khoá RPuKTA
$$\text{Verify}(\text{RPuKTA}, sIS, \text{IDRFID} || rRFID || \text{Comp}(\text{RPuKTA}) || \text{ATA}))$$



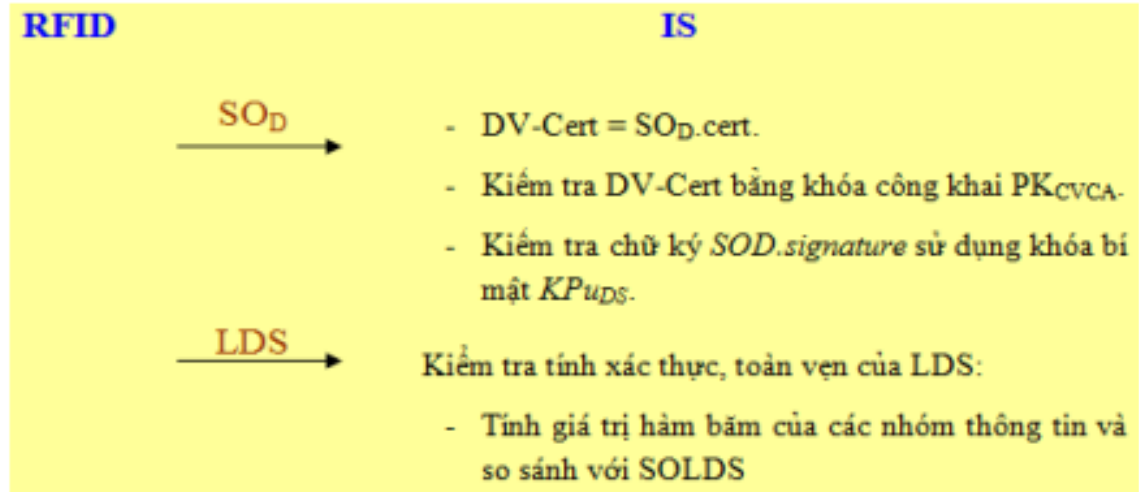
Hình 17. Lược đồ TA

Bước 5: Xác thực thụ động

Quá trình PA cho phép kiểm tra tính xác thực và toàn vẹn thông tin lưu trong chip RFID thông qua việc kiểm tra chữ ký lưu trong SOD bằng khóa công khai của cơ quan cấp e-ID. Việc trao đổi khóa công khai thông qua chứng chỉ số được thực hiện theo mô hình khuyến cáo của ICAO. Thực hiện thành công quá trình PA cùng với CA trong cơ chế EAC thì có thể khẳng định chắc chắn chip trong e-ID là nguyên gốc.

- Đọc SOD từ chip RFID.
- Lấy chứng chỉ DV-Cert từ SOD vừa đọc ở trên.
- Kiểm tra DV-Cert từ khóa công khai PKCVCA có được từ PKD hoặc từ cơ sở dữ liệu được trao đổi trực tiếp giữa các quốc gia thông qua đường công hàm.
- Kiểm tra chữ ký số SOD.signature sử dụng khóa bí mật KPuDS của DV. Bước này nhằm khẳng định thông tin SOLDS đúng là được tạo ra bởi cơ quan cấp e-ID và SOLDS không bị thay đổi.
- Đọc các thông tin cần thiết từ LDS.

- Tính hàm băm cho các thông tin ở bước 4, sau đó so sánh với SOLDS. Qua bước này mới khẳng định được nhóm dữ liệu là xác thực và toàn vẹn.

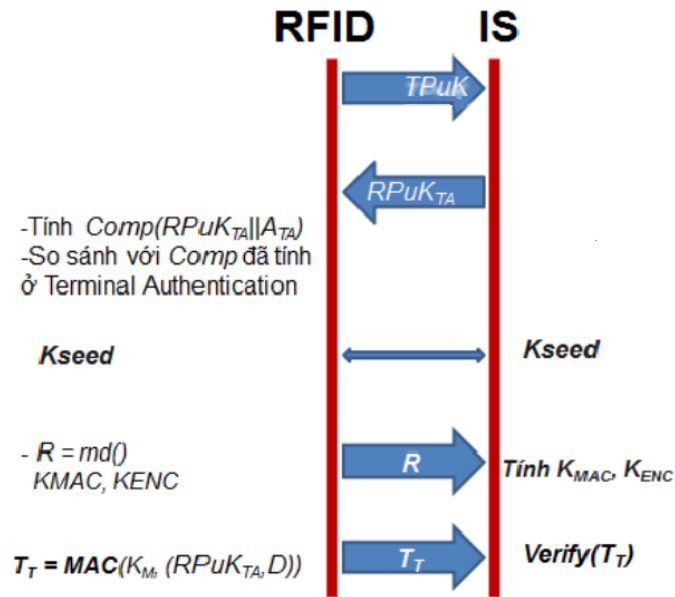


Hình 18. Lược đồ PA

Bước 6: Xác thực chip

CA thiết lập thông báo bảo mật giữa chip MRTD và IS dựa trên cặp khoá tĩnh được lưu trữ trên chip. CA thay thế cơ chế AA mà ICAO đã đưa ra và cung cấp các khoá phiên mạnh. Các bước tiến hành trong CA như sau:

- RFID gửi cho IS khoá công khai (TPuK).
- IS gửi khoá công khai ngắn hạn RPuKTA đã được sinh ra trong TA đến cho RFID.
- RFID tính $Comp(RPuKTA)$ và dữ liệu ATA. Nó sẽ so sánh giá trị Comp này với giá trị nó nhận được từ TA.
- RFID và IS có đủ thông tin chia sẻ để tính khoá Kseed.
- RFID sinh ra chuỗi ngẫu nhiên (R). Các khoá phiên được tính: $KMAC = SHA1(Kseed || R || 2)$ và $KENC = SHA-1(Kseed || R || 1)$.
- RFID tính: $TT = MAC(KMAC, (RPuKTA, D))$. RFID gửi R và TT đến cho IS. 7) IS sử dụng R để tính các khoá phiên từ Kseed. Sau đó nó thẩm định thẻ bài xác thực TT.



Hình 19. Lược đồ CA

Bước 7: Đối sánh đặc trưng sinh trắc

Hệ thống kiểm duyệt có quyền truy cập vào các vùng dữ liệu DG2, DG3, DG4 và tiến hành đọc các dữ liệu sinh trắc của người sở hữu e-ID (ảnh khuôn mặt, dấu vân tay, móng mắt) được lưu trong chip RFID. Cùng lúc đó, bằng các thiết bị chuyên dụng, cơ quan kiểm tra sẽ tiến hành thu nhận các đặc tính sinh trắc học như ảnh khuôn mặt, vân tay, móng mắt...từ công dân. Sau đó, hệ thống sẽ thực hiện quá trình trích chọn đặc trưng của các đặc tính sinh trắc, tiến hành đối chiếu và đưa ra kết quả. Nếu cả ba dữ liệu sinh trắc thu được trực tiếp từ người dùng khớp với dữ liệu thu được từ chip RFID thì cơ quan kiểm tra xác thực có đủ điều kiện để tin tưởng e-ID điện tử đó là đúng đắn và người mang e-ID là hợp lệ

Ngoài ra, với việc sử dụng hệ mật dựa trên đường cong Elliptic (ECC) - hệ mật được đánh giá có độ an toàn cao trong khi kích thước khoá nhỏ, thời gian tính toán nhanh và rất phù hợp để triển khai trên các thiết bị tính toán có năng lực xử lý yếu. Đây là điều kiện tiên quyết đảm bảo hiệu năng của mô hình xác thực.

Ngoài ra, mô hình nêu trên hoàn toàn đáp ứng được những yêu cầu đặt ra đối với e-ID như: đảm bảo tính chân thực (quy trình rõ ràng), tính không thể nhân bản (sử dụng CA và PA), tính nguyên vẹn và xác thực (PA và PKI), tính liên kết công

dân e-ID (sử dụng ba đặc trưng sinh trắc có độ xác thực cao nhất), kiểm soát được truy cập (PACE và EAC).

Mặc dù mô hình xác thực e-ID này, được xây dựng dựa trên những đặc tả trong phiên bản thế hệ thứ ba, khắc phục hầu hết các nguy cơ kém an toàn của e-ID thế hệ thứ nhất và thứ hai, tuy nhiên nó vẫn tồn tại nhược điểm liên quan đến vấn đề hết hạn của đầu đọc.

CHƯƠNG IV: XÂY DỰNG HỆ THỐNG IOT ĐỌC GHI DỮ LIỆU TRÊN THẺ RFID

4.1. Giới thiệu tổng quan mô hình

4.1.1. Ngôn ngữ và các công cụ lập trình

Ngôn ngữ lập trình sử dụng:

- Dùng ngôn ngữ lập trình C/C++ để xây dựng phía server trên module ESP8266
- Websocket dùng HTML, CSS, Javascripts và Bootstrap để xây dựng

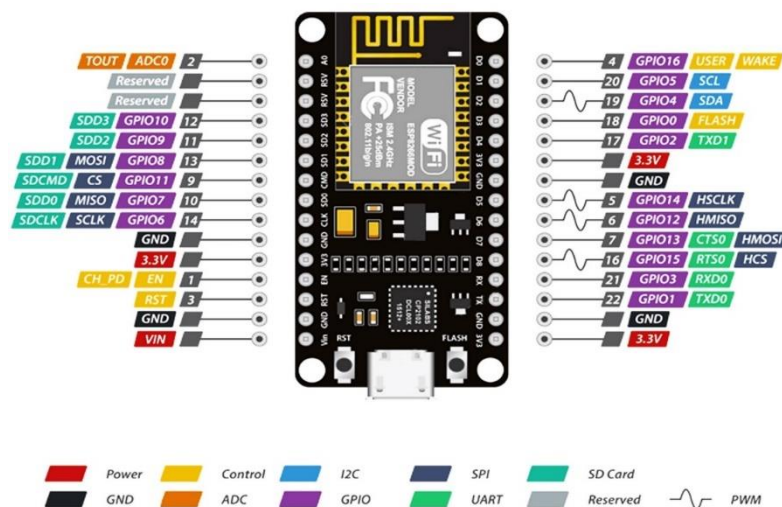
Công cụ lập trình:

- IDE Arduino
- Visual Studio

4.1.2 Giới thiệu thiết bị

a. ESP 8266

- **Vi xử lý mạnh mẽ:** Chip ESP8266 được tích hợp vi xử lý Tensilica L106 32-bit RISC với tần số hoạt động lên đến 160 MHz, cung cấp đủ sức mạnh để xử lý các tác vụ phức tạp.
- **Bộ nhớ:** ESP8266 có bộ nhớ flash từ 512KB đến 4MB và RAM 50KB để lưu trữ và chạy các chương trình.
- **GPIO:** ESP8266 có các chân GPIO (General Purpose Input/Output) cho phép nó tương tác với các thiết bị ngoại vi khác như cảm biến, relay, và các module khác.
- **Giao tiếp:** Nó hỗ trợ nhiều giao tiếp như UART, SPI, I2C, PWM, và ADC.



Hình 20. Module ESP8266 NodeMCU

Các ứng dụng phổ biến của ESP8266:

- Điều khiển thiết bị thông qua Wi-Fi: Điều khiển đèn, quạt, cửa ra vào từ xa qua internet.
- Giám sát và thu thập dữ liệu: Sử dụng các cảm biến để thu thập dữ liệu môi trường (nhiệt độ, độ ẩm, ánh sáng, v.v.) và gửi về máy chủ.
- Thiết bị nhà thông minh: Tích hợp trong các thiết bị nhà thông minh như công tắc thông minh, ổ cắm thông minh, và camera giám sát.
- Hệ thống báo động: Xây dựng các hệ thống báo động an ninh có thể gửi thông báo qua internet.

ESP8266 có thể được lập trình thông qua nhiều ngôn ngữ lập trình và môi trường phát triển khác nhau, bao gồm Arduino IDE, Lua (NodeMCU), và MicroPython, giúp người dùng dễ dàng triển khai và phát triển các ứng dụng khác nhau.

b. Modulee RFID RC522

RFID RC522 là một module đọc/ghi RFID sử dụng công nghệ tần số vô tuyến để giao tiếp với thẻ RFID. RC522 là một module phổ biến trong các dự án Arduino và các hệ thống nhúng khác do dễ sử dụng và giá thành thấp. Dưới đây là một số thông tin chi tiết về module này:



Hình 21. Module RFID RC522 13.56MHz

Đặc điểm kỹ thuật của RFID RC522:

1. Tần số hoạt động: RC522 hoạt động ở tần số 13.56 MHz, đây là tần số chuẩn cho các ứng dụng RFID.
2. Giao tiếp: Module này giao tiếp với vi điều khiển thông qua giao thức SPI, nhưng cũng hỗ trợ I2C và UART.

3. Khoảng cách đọc: Khoảng cách đọc của RC522 khoảng 0-5 cm, tùy thuộc vào loại thẻ và điều kiện môi trường.
4. Điện áp hoạt động: RC522 hoạt động với điện áp 3.3V, do đó cần cẩn thận khi kết nối với các vi điều khiển hoạt động ở 5V như Arduino để tránh hư hỏng.
5. Các chân kết nối:
 - VCC: Nguồn cấp (3.3V)
 - GND: Ground
 - RST: Reset
 - IRQ: Ngắt
 - MISO/SCL/TX: Dữ liệu ra (Master In Slave Out)
 - MOSI/SDA/RX: Dữ liệu vào (Master Out Slave In)
 - SCK: Clock (SPI Clock)
 - SS/SDA: Slave Select (SPI Chip Select)

Ứng dụng của RFID RC522:

- Hệ thống kiểm soát truy cập: Dùng trong các hệ thống cửa ra vào, thang máy để quản lý việc truy cập.
- Quản lý kho hàng: Gắn thẻ RFID vào các sản phẩm để theo dõi và quản lý hàng tồn kho.
- Thanh toán điện tử: Sử dụng thẻ RFID cho các hệ thống thanh toán không tiếp xúc.
- Theo dõi tài sản: Gắn thẻ RFID vào tài sản để dễ dàng theo dõi và quản lý.

c. Thẻ RFID Mifare 1KB

Thẻ RFID MIFARE 1KB là loại thẻ sử dụng công nghệ RFID với chip MIFARE Classic, được thiết kế và sản xuất bởi NXP Semiconductors. Đây là một trong những loại thẻ RFID phổ biến nhất cho các ứng dụng yêu cầu bảo mật và lưu trữ dữ liệu vừa phải, như kiểm soát truy cập, vé điện tử, và thanh toán không tiếp xúc. Dưới đây là một số đặc điểm và thông tin chi tiết về thẻ MIFARE 1KB:

Đặc điểm kỹ thuật của thẻ MIFARE 1KB:

1. Dung lượng bộ nhớ: Thẻ MIFARE Classic 1KB có tổng dung lượng bộ nhớ là 1024 bytes, được chia thành 16 khối (sector), mỗi khối gồm 4 block, mỗi block chứa 16 bytes.

2. Tần số hoạt động: Thẻ hoạt động ở tần số 13.56 MHz, phù hợp với tiêu chuẩn ISO/IEC 14443A.
3. Bảo mật: Thẻ hỗ trợ cơ chế bảo mật thông qua hai khóa A và B cho mỗi sector, cho phép kiểm soát truy cập đọc/ghi dữ liệu trên thẻ.
4. Khoảng cách đọc: Khoảng cách đọc của thẻ thường là 0-10 cm, tùy thuộc vào điều kiện môi trường và thiết bị đọc.
5. Tốc độ truyền dữ liệu: Tốc độ truyền dữ liệu giữa thẻ và đầu đọc là 106 kbit/s.

Ứng dụng của thẻ MIFARE 1KB:

- Kiểm soát truy cập: Sử dụng trong các hệ thống quản lý ra vào như cửa từ, thang máy, và các khu vực hạn chế.
- Vé điện tử: Sử dụng làm vé cho các phương tiện giao thông công cộng, công viên giải trí, và sự kiện.
- Thanh toán không tiếp xúc: Sử dụng trong các hệ thống thanh toán nhanh tại cửa hàng, máy bán hàng tự động.
- Quản lý thành viên: Sử dụng trong các phòng gym, thư viện, và các tổ chức để quản lý thành viên.

Tổ chức bộ nhớ trên thẻ RFID

Trên thẻ RFID, bộ nhớ được tổ chức thành các khối dữ liệu gọi là "sector" và "block". Các thẻ RFID thường có một số sector và mỗi sector chứa một số block. Cấu trúc tổ chức bộ nhớ này thường áp dụng cho các thẻ sử dụng công nghệ MIFARE.

Cấu trúc tổ chức bộ nhớ trên thẻ RFID:

Sector (Phân đoạn):

Mỗi sector là một phân vùng dữ liệu độc lập.

Mỗi sector có thể chứa nhiều block.

Số lượng sector trên một thẻ RFID có thể khác nhau, thường từ 1 đến 16 hoặc hơn tùy theo loại thẻ.

Firmware Version: 0x91 = v1.0
 Scan PICC to see UID, SAK, type, and data blocks...
 Card UID: E7 45 D6 19
 Card SAK: 08
 PICC type: MIFARE 1KB

Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	AccessBits
15	63	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	[0 0 1]
	62	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	61	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
14	59	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	[0 0 1]
	58	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	57	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	56	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
13	55	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	[0 0 1]
	54	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	53	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	52	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
12	51	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	[0 0 1]
	50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]

☒ Autoscroll ☐ Show timestamp Newline 9600 baud Clear output

Hình 22. Tổ chức bộ nhớ của thẻ RFID

Block (Khối):

Mỗi sector chứa nhiều block dữ liệu.

Trên thẻ MIFARE, mỗi sector thường có 4 block dữ liệu.

Các block được đánh số từ 0 đến 3. Block có số 3 thường là block trailer chứa các thông tin quản lý như khóa truy cập (Access bits) và các khóa (Key A và Key B).

Trailer Block (Block trailer):

Là block cuối cùng trong mỗi sector (với chỉ số là 3).

Chứa thông tin quản lý sector như Access bits và các khóa (Key A và Key B).

Thông thường, để truy cập vào một sector, bạn cần phải xác thực bằng một trong các khóa (Key A hoặc Key B) được lưu trong block trailer.

Ví dụ:

Thẻ MIFARE Classic 1K có 16 sector và mỗi sector có 4 block.

Ví dụ về cấu trúc tổ chức bộ nhớ trên thẻ MIFARE Classic 1K:

Sector 0: Block 0, Block 1, Block 2, Block 3 (trailer block)

Sector 1: Block 4, Block 5, Block 6, Block 7 (trailer block)

...

Sector 15: Block 60, Block 61, Block 62, Block 63 (trailer block)

Quản lý quyền truy cập (Access bits):

Mỗi block trailer chứa các Access bits, quy định quyền truy cập vào sector và các block trong đó.

Access bits quản lý quyền đọc (Read) và ghi (Write) cho Key A và Key B.

Sử dụng trong ứng dụng thực tế:

Thẻ RFID được sử dụng rộng rãi trong các hệ thống điều khiển truy cập, thẻ khách, thanh toán không tiếp xúc, và các ứng dụng IoT.

Các dữ liệu quan trọng như thông tin cá nhân, thông tin truy cập và các thông tin đặc biệt khác có thể được lưu trữ trong các sector và được bảo vệ bằng các khóa xác thực.

Lưu ý:

Mỗi loại thẻ RFID có thể có cấu trúc bộ nhớ khác nhau, điều này phụ thuộc vào tiêu chuẩn và loại thẻ cụ thể.

Việc sử dụng các khóa (Key A và Key B) đúng cách là rất quan trọng để đảm bảo an ninh và bảo vệ dữ liệu trên thẻ RFID.

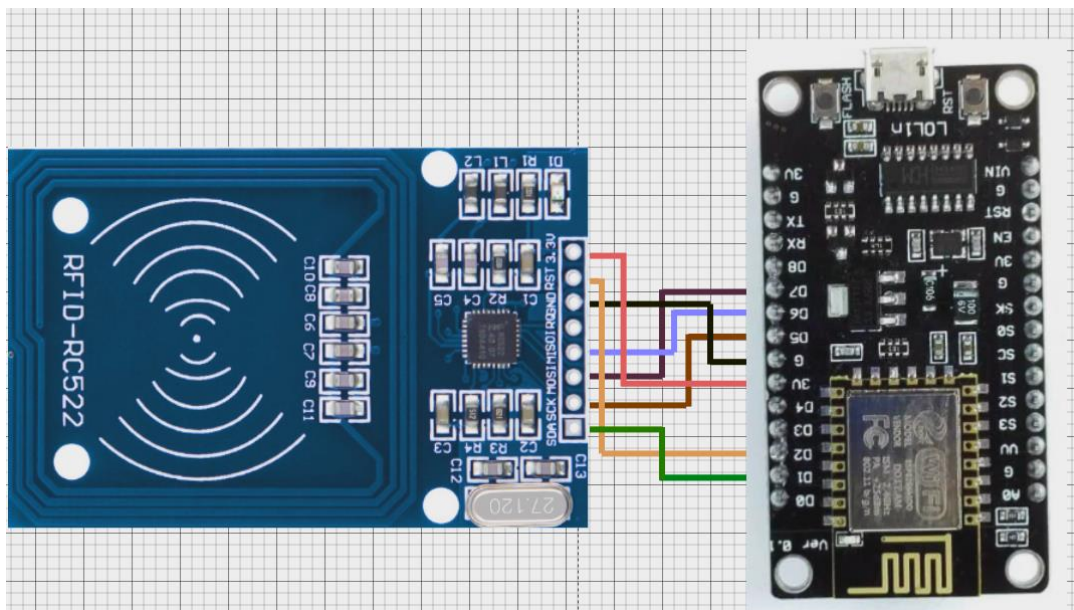
4.2. Mô tả hệ thống

4.2.1. Sơ đồ kết nối thiết bị

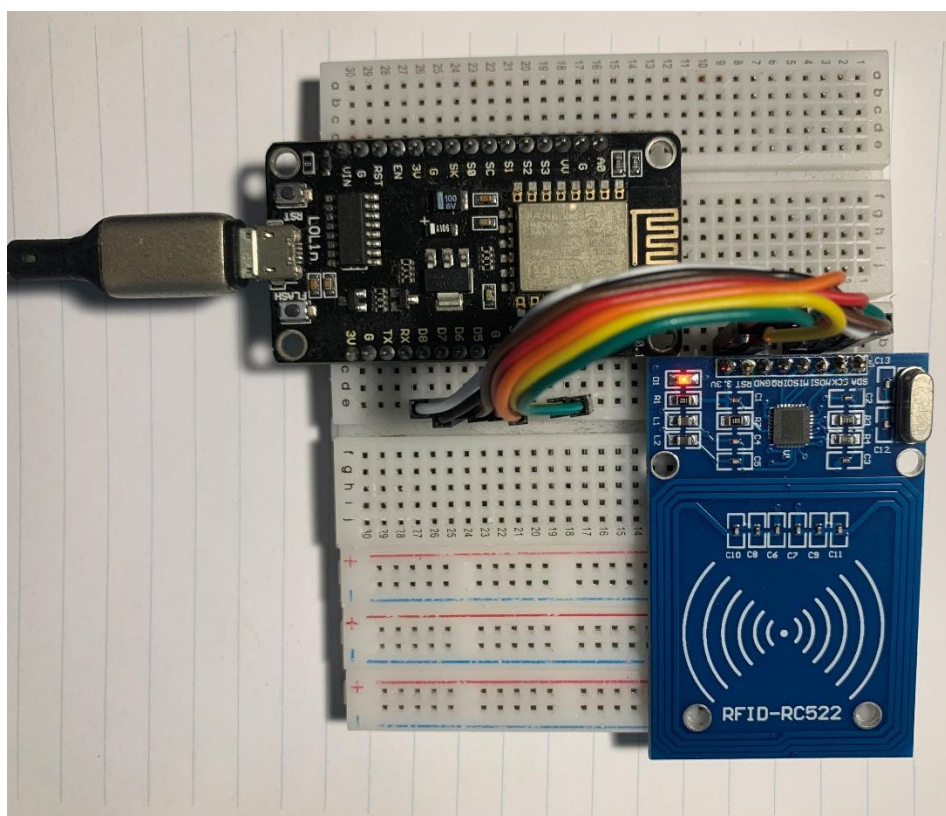
a. Sơ đồ các chân Pin được sử dụng

	RFID-RC522	ESP8266
Signal	Pin	Pin
RST/Reset	RST	4 (D2)
SPI SS	SDA(SS)	5 (D1)
SPI MOSI	MOSI	D7
SPI MISO	MISO	D6
SPI SCK	SCK	D5

b. Sơ đồ đấu nối



Hình 23. Sơ đồ đấu nối



Hình 24. Hình ảnh mô hình được lắp ráp

4.2.2. Mô tả hoạt động và chức năng của mô hình

a. Hoạt động và chức năng Ghi dữ liệu

Chức năng này cho phép người dùng có thể điền thông tin vào các ô input, sau khi nhấn nút thêm thì sẽ hiển một dòng thông báo “đưa thẻ lại gần đầu đọc”. Sau khi thẻ được đưa lại gần đầu đọc. Dữ liệu sẽ được ghi vào thẻ và hiện trạng thái SUCCESS.

```
//Function Set Info to card
void set_info_to_card(card_info_t* card_info, MFRC522::MIFARE_Key* auth_key, msg_response_t* msg_resp) {
    MFRC522::StatusCode status;
    byte buffer[18] = {0};
    byte size = sizeof(buffer);
    status = auth_sector_with_keyA(SECTOR, auth_key);
    if (status != MFRC522::STATUS_OK) {
        strncpy(msg_resp->reason, "authentication Key wrong", 50);
        goto EXIT;
    }
    status = del_info_to_card(NAME_BLOCK, auth_key);
    if (status != MFRC522::STATUS_OK) {
        strncpy(msg_resp->reason, "Del block 'name' failed", 50);
        goto EXIT;
    }
    status = (MFRC522::StatusCode) mfr522.MIFARE_Write(NAME_BLOCK, (byte*)card_info->name, 16);
    if (status != MFRC522::STATUS_OK) {
        Serial.print(F("MIFARE_Write() 'name' failed: "));
        Serial.println(mfr522.GetStatusCodeName(status));
        strncpy(msg_resp->reason, "MIFARE_Write() 'name' failed", 50);
        goto EXIT;
    }
    // set cccd
    status = del_info_to_card(CCCD_BLOCK, auth_key);
    if (status != MFRC522::STATUS_OK) {
        strncpy(msg_resp->reason, "Del block 'cccd' failed", 50);
        goto EXIT;
    }
    status = (MFRC522::StatusCode) mfr522.MIFARE_Write(CCCD_BLOCK, (byte*)card_info->cccd, 16);
    if (status != MFRC522::STATUS_OK) {
        Serial.print(F("MIFARE_Write() 'cccd' failed: "));
        Serial.println(mfr522.GetStatusCodeName(status));
        strncpy(msg_resp->reason, "MIFARE_Write() 'cccd' failed", 50);
        goto EXIT;
    }
    // set plates
    status = del_info_to_card(PLATES_BLOCK, auth_key);
    if (status != MFRC522::STATUS_OK) {
        strncpy(msg_resp->reason, "Del block 'plates' failed", 50);
        goto EXIT;
    }
    status = (MFRC522::StatusCode) mfr522.MIFARE_Write(PLATES_BLOCK, (byte*)card_info->plates, 16);
    if (status != MFRC522::STATUS_OK) {
        Serial.print(F("MIFARE_Write() 'plates' failed: "));
        Serial.println(mfr522.GetStatusCodeName(status));
        strncpy(msg_resp->reason, "MIFARE_Write() 'plates' failed", 50);
        goto EXIT;
    }
}
EXIT:
    msg_resp->err_code = status;
}
```

Hình 25. Code chức năng ghi thông tin vào thẻ

Ở hàm `set_info_to_card` này sẽ thực hiện các bước chính như sau:

- Xác thực sector trên thẻ RFID bằng khóa KeyA để có quyền truy cập vào các block dữ liệu.
- Xóa dữ liệu hiện có trong các block được chỉ định trước ghi dữ liệu mới
- Ghi các thông tin đã được người dùng điền vào vào các block tương ứng
- Kiểm tra và xử lý lỗi trong quá trình xác thực, xóa và ghi dữ liệu. Nếu có lỗi, hàm sẽ lưu thông báo lỗi và mã lỗi vào biến `msg_resp`

Giao diện của chức năng ghi dữ liệu

The screenshot shows a web application interface with three tabs: 'GIỚI THIỆU', 'GHI DỮ LIỆU', and 'ĐỌC DỮ LIỆU'. The 'GHI DỮ LIỆU' tab is active. In the center, there is a modal form titled 'Nhập Thông Tin'. The form contains four input fields: 'Name:', 'License:', 'CCCD:', and 'Authentication (KeyA):'. Below these fields is a green 'Thêm' (Add) button. Underneath the button is a section titled 'Trạng thái' (Status) which contains a large, empty rectangular box. At the bottom of this section is a pink 'Xóa' (Delete) button.

Hình 26. Giao diện chức năng ghi thông tin vào thẻ

This screenshot shows the same 'GHI DỮ LIỆU' interface as Figure 26, but with data entered into the form. The 'Name' field is filled with 'Nguyễn Nam Tran', 'License' with '10071999', 'CCCD' with '12993288127', and 'Authentication (KeyA)' with 'FF-FF-FF-FF-FF-FF'. The green 'Thêm' button is now highlighted. In the 'Trạng thái' section, the large box now contains the text '23:56:36 Sun Jun 16 2024' and 'Đưa thẻ cần ghi, lại gần cảm biến' (Bring the card to be written close to the sensor). The pink 'Xóa' button remains at the bottom.

Hình 27. Dữ liệu được người dùng nhập vào và chờ ghi

Hình 28. Ghi dữ liệu thành công

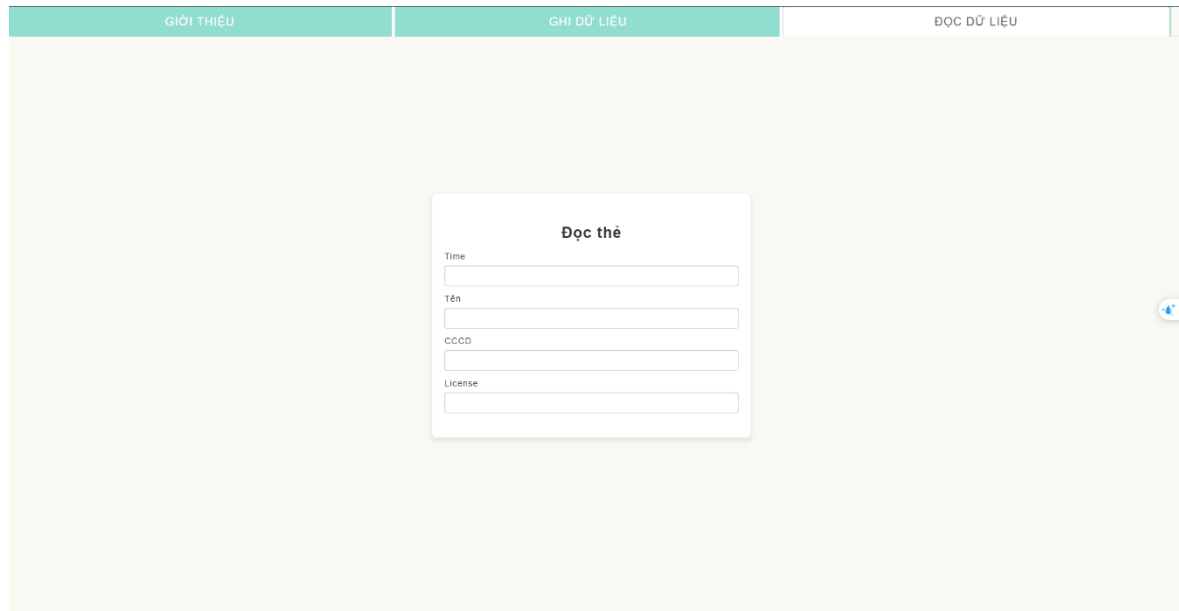
b. Hoạt động và chức năng Đọc dữ liệu

Chức năng này khi người dùng đưa thẻ lại gần đầu đọc thẻ thì dữ liệu được lưu ở trên thẻ sẽ được hiển thị lên màn hình. Khi đưa thẻ khác vào đọc, dữ liệu sẽ tự động được thay thế bằng dữ liệu mới.

```
// Function Show info from card
void show_info_from_card(card_info_t* card) {
    String out;
    int size_msg = strlen("type") + strlen("card_info")      +
                  strlen("card_uid") + strlen("name")        +
                  strlen("cccd") + strlen("license_plate")  +
                  sizeof(*card) + 30;
    Serial.print(F("Size of msg: "));
    Serial.println(size_msg);
    DynamicJsonDocument doc(size_msg);
    doc["type"] = "card_info";
    doc["card_uid"] = card->uid;
    doc["name"] = card->name;
    doc["cccd"] = card->cccd;
    doc["license_plate"] = card->plates;
    serializeJson(doc, out);
    ws.broadcastTXT(out);
}
```

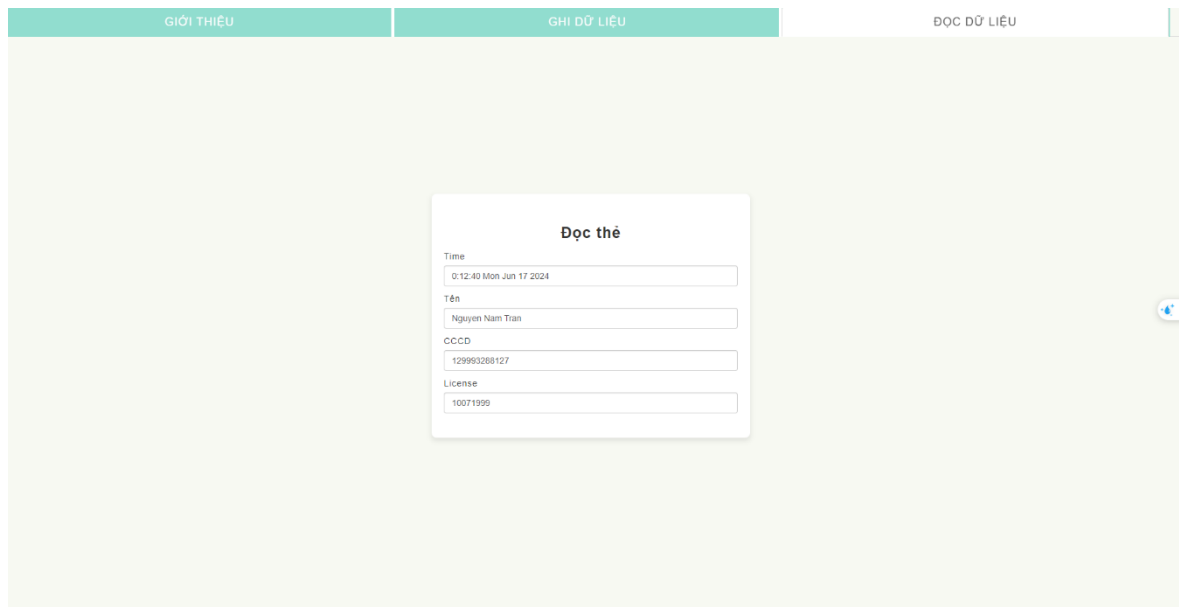
Hình 29. Code hiện thông tin lên trang web

Đoạn code này có chức năng thu thập thông tin từ thẻ RFID, sau đó tạo một thông điệp JSON chứa thông tin đó và phát nó qua WebSocket để hiển thị thông tin lên trang web



The screenshot shows a web application interface with a navigation bar at the top. The bar has three tabs: 'GIỚI THIỆU', 'GHI DỮ LIỆU', and 'ĐỌC DỮ LIỆU'. The 'ĐỌC DỮ LIỆU' tab is active. Below the navigation bar, there is a large light green area. In the center of this area is a white form titled 'Đọc thẻ'. The form contains four input fields: 'Time', 'Tên', 'CCCD', and 'License'. All fields are currently empty.

Hình 30. Giao diện chức năng đọc thẻ



The screenshot shows the same web application interface as Figure 30, but now the 'Đọc thẻ' form contains data. The 'Time' field is filled with '0:12:40 Mon Jun 17 2024', the 'Tên' field with 'Nguyễn Nam Tran', the 'CCCD' field with '129993268127', and the 'License' field with '10071999'.

Hình 31. Dữ liệu được đọc thành công

KẾT LUẬN VÀ KIẾN NGHỊ

Kết quả đạt được

- Về đề án

Nội dung trình bày bám sát mục tiêu đề ra của đề án “Nghiên cứu cơ chế bảo mật PACE và EAC để xây dựng mô hình xác thực đảm bảo an toàn thông tin trên thẻ e-ID”. Trình bày được dữ liệu và bảo vệ dữ liệu sinh trắc trên chip. Các giao thức mật mã đảm bảo an toàn cho dữ liệu trên thẻ e-ID. Trình bày chi tiết về hai cơ chế bảo mật PACE và EAC và áp dụng đưa ra mô hình xác thực e-ID. Ngoài ra xây dựng mô hình đọc ghi thẻ mô phỏng e-ID.

- Về bản thân

Sau khi hoàn thành đề án, em đã hoàn thiện được cho mình những kỹ năng về đọc tài liệu từ các nguồn Quốc tế, các bài báo cáo khoa học và kỹ thuật. Kỹ năng làm việc độc lập, sắp xếp công việc thời gian hợp lý và quý giá hơn là đã trang bị cho mình những kiến thức về an toàn và bảo mật thông tin cụ thể là hai cơ chế bảo mật PACE và EAC của đề tài này.

Hạn chế

Do điều kiện có hạn về cơ sở vật chất cũng như thời gian, em đã tiến hành thử nghiệm mô hình trên theo hướng kiểm thử quy trình xác thực với thẻ dữ liệu mô phỏng. Các phần liên quan đến những bước cần xử lý xác thực sinh trắc học và trên thẻ e-ID thật sẽ được thử nghiệm trong thời gian tới.

Hướng phát triển

Trong thời gian tới sẽ tích hợp thêm các module xác thực nhân tố sinh trắc học và thiết bị thực tế. Phát triển mô hình để được sử dụng rộng rãi trong xã hội. Được thử nghiệm trên các mô hình tiêu chuẩn với hi vọng sẽ được nghiên cứu sâu hơn, hướng đến sản xuất e-ID cho công dân Việt Nam mà không phải phụ thuộc vào sản phẩm nước ngoài.

TÀI LIỆU THAM KHẢO

- [1] N. Viết Tuyền, Bồ Quốc Bảo, Tống Văn Luyên, *Giáo trình mạng máy tính*, Nhà xuất bản KH&KT, 2013. Truy cập vào ngày 18/04/2024.
- [2] TS. Nguyễn Hữu Hòa, ThS Nguyễn Thị Thùy Linh. *Bảo mật hệ thống và an ninh mạng*, Nhà xuất bản Đại học Cần Thơ, 2017. Truy cập vào ngày 22/04/2024.
- [3] Đỗ Mạnh Hùng, *Giáo trình lập trình mạng*, Nhà xuất bản Thống kê, 2020 Truy cập vào ngày 23/04/2024.
- [4] Bjarne Stroustrup, *The C++ Programming Language*, Nhà xuất bản Addison-Wesley, 2013. Truy cập vào 25/04/2024.
- [5] P.T. Long, N.N. Hoa, “Mô hình xác thực hộ chiếu điện tử”, tại Hội thảo Quốc gia “Một số vấn đề chọn lọc trong CNTT, 06/2008, Huế, Việt Nam. Truy cập vào 28/04/2024.
- [6] Lê Mỹ hà, Phạm Quang Huy, *Lập trình IoT với Arduino*, Nhà xuất bản Thanh niên, 2017. Truy cập vào 29/04/2024.
- [7] Lucjan Hanzlik, Mirosław Kutylowski, *Chip Authentication for E-Passports: PACE with Chip Authentication Mapping v2*, Wrocław University of Science and Technology, Poland ISC 2016 Honolulu. Truy cập vào 30/04/2024.
- [8] Dr. Jens Bender, Dr. Dennis Kugler, *Introducing the PACE solution*. Truy cập vào 03/05/2024.
- [9] Laurel C Sadler, Jesse Kovach, *Radio-Frequency Identification (RFID) MultiReader/Integrated Sensor Architecture (ISA)*, Publisher Software Documentation. Truy cập vào 02/05/2024.
- [10] *Basic Access Control and Extended Access Control in ePassports*, 18th Meeting of the Technical Advisory Group on Machine Readable Travel Documents Truy cập vào ngày 07/05/2024.
- [11] Anupam Datta, *SSL/TLS*, 18733: Applied Cryptography. Truy cập vào ngày 10/05/2024.
- [12] ICAO Security and Facilitation, *Access to ePassport chip*. Truy cập vào ngày 15/05/2024.
- [13] ESP8266 Technical Reference Documentation. Truy cập vào ngày 25/05/2024

[14] Arduino Documentation: <https://docs.arduino.cc/software/ide/> . Truy cập vào ngày 27/05/2024

[15] Module RC522 Documentation: <https://mecu.vn/ho-tro-ky-thuat/module-doc-rfid-rc522.65B> . Truy cập vào ngày 27/05/2024

[16] Thông tư quy định về mẫu thẻ căn cước công dân của Bộ công an, số: 06/2021/TT-BCA, Hà Nội, ngày 23 tháng 01 năm 2021. Truy cập ngày 28/05/2024.