**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**PHÂN HIỆU TẠI TP. HỒ CHÍ MINH**

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO ĐỒ ÁN TỐT NGHIỆP**

**ĐỀ TÀI:**

**NGHIÊN CỨU, TÌM HIỂU KỸ THUẬT MẬT MÃ BẢO ĐẢM AN TOÀN CHO THẺ ĐỊNH DANH DANH TÍNH ĐIỆN TỬ**

Sinh viên thực hiện:

Võ Khắc Mạnh – 6151071071

Lớp: CÔNG NGHỆ THÔNG TIN

Khoá:61

Tp. Hồ Chí Minh, năm 2024

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**PHÂN HIỆU TẠI TP. HỒ CHÍ MINH**

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO ĐỒ ÁN TỐT NGHIỆP**

**ĐỀ TÀI:**

**NGHIÊN CỨU, TÌM HIỂU KỸ THUẬT MẬT MÃ BẢO ĐẢM AN TOÀN CHO THẺ ĐỊNH DANH DANH TÍNH ĐIỆN TỬ**

Sinh viên thực hiện: Võ Khắc Mạnh

Võ Khắc Mạnh – 6151071071

Lớp: CÔNG NGHỆ THÔNG TIN

Khoá:61

Tp. Hồ Chí Minh, năm 2024

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH** Độc lập – Tự do – Hạnh phúc

# NHIỆM VỤ BÁO CÁO

**BỘ MÔN: CÔNG NGHỆ THÔNG TIN**

-------\*\*\*-------

**Mã sinh viên: 6151071071**  **Họ tên SV: VÕ KHẮC MẠNH Khóa:** **61**  **Lớp: CÔNG NGHỆ THÔNG TIN**

**1.Tên đề tài tốt nghiệp**

Nghiên cứu, tìm hiểu kỹ thuật mật mã đảm bảo an toàn cho thẻ định danh danh tính điện tử.

## **2.Nhiệm vụ tốt nghiệp**

## **3. Mục tiêu**

## **4. Yêu cầu công nghệ**

## **5. Nội dung**

## **6. Công nghệ, công cụ và ngôn ngữ lập trình**

## **7. Khảo sát**

## **8. Các kết quả chính dự kiến sẽ đạt được và ứng dụng**

|  |  |
| --- | --- |
|  | *TP. Hồ Chí Minh, ngày …… tháng 6 năm 2024*  **Sinh viên thực hiện**  *(Ký và ghi họ và tên)* |

# 

# LỜI CẢM ƠN

Quãng thời gian thực 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 tương lai sự nghiệp của mình. 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 hết em xin gửi 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, kiến thức của em vẫn còn hạn chế và nhiều bờ 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.

Em xin chân thành cảm ơn!

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!

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

|  |
| --- |
| ***Tp. Hồ Chí Minh, ngày ….… tháng ….… năm ….…***  **Giảng viên hướng dẫn** |

Mục Lục

# DANH MỤC THUẬT NGỮ VÀ TỪ VIẾT TẮT

DANH MỤC HÌNH ẢNH

MỞ ĐẦU

1.Lý do chọn đề tài

Trong thời đại kỷ nguyên số, định danh điện tử là yếu tố quan trọng để thực hiện các giao dịch điện tử và xây dựng chính phủ số. Chính phủ đang tập trung phát triển dịch vụ hành chính công trực tuyến để thúc đẩy cuộc cách mạng công nghiệp lần thứ tư. Do đó, bảo mật thông tin 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.

Bộ Thông tin và Truyền thông đã xây dựng một nghị định về định danh điện tử, đang lấy ý kiến từ công chúng và các bộ ngành liên quan. 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 cổng 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, tìm hiểu kỹ thuật mật mã bảo đảm an toàn cho thẻ định danh danh tính điện tử” 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 cơ quan tổ chức và doanh nghiệp bảo vệ hệ thống máy chủ web khỏi các cuộc tấn công, đồng thời thúc đẩy quá trình chuyển đổi số của nước ta.

2. Hướng tiếp cận đề tài và mục tiêu

3. Đối tượng và phạm vi đề tài

4. Phương pháp nghiên cứu

CHƯƠNG 1: TỔNG QUAN VỀ THẺ DANH TÍNH ĐIỆN TỬ

1.1. Giới thiệu về thẻ danh tính điện tử (e-ID)

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 và 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.
* **Công Nghệ và Tiêu Chuẩn Hiện Đại:**
* **Chip không tiếp xúc (Contactless chip):** Thẻ e-ID hiện đại thường sử dụng công nghệ RFID hoặc NFC để giao tiếp không tiếp xúc, thuận tiện hơn trong nhiều ứng dụng.
* **Chữ ký số và PKI:** Các thẻ e-ID tích hợp chữ ký số và hạ tầng khóa công khai (PKI) để đảm bảo tính toàn vẹn và xác thực của các giao dịch điện tử.
* **Tiêu chuẩn quốc tế:** Các tiêu chuẩn như ISO/IEC 14443 (giao tiếp không tiếp xúc) và ISO/IEC 7816 (giao tiếp tiếp xúc) giúp thẻ e-ID có khả năng tương thích và bảo mật cao hơn.

**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.

CMND cũ.

1.1.3. Khái niệm

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 1.1: 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 (" eID ") 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 kỹ thuật số chữ ký.

Thẻ danh tính điện tử (e-id card) là một thẻ nhận dạng vật lý có thể được sử dụng để nhận dạng hoặc xác thực cá nhân trực tuyến và ngoại tuyến. EIC là một thẻ thông minh ở định dạng ID-1 của thẻ ngân hàng thông thường, với thông tin nhận dạng được in trên bề mặt (chẳng hạn như chi tiết cá nhân và ảnh) và trong một vi mạch RFID nhúng, tương tự như trong hộ chiếu sinh trắc học. Con chip lưu trữ thông tin được in trên thẻ (chẳng hạn như tên và ngày sinh của chủ thẻ) và (các) ảnh của chủ thẻ. Một số ảnh có thể được chụp từ các góc độ khác nhau cùng với các biểu cảm khuôn mặt khác nhau, do đó cho phép hệ thống nhận dạng khuôn mặt sinh trắc học đo lường và phân tích cấu trúc tổng thể, hình dạng và tỷ lệ của khuôn mặt.  Nó cũng có thể lưu trữ dấu vân tay của chủ sở hữu. Thẻ có thể được sử dụng để xác thực trực tuyến, chẳng hạn như để xác minh độ tuổi hoặc cho các ứng dụng chính phủ điện tử. Một chữ ký điện tử, do một công ty tư nhân cung cấp, cũng có thể được lưu trữ trên chip.



CCCD gắn chíp điện tử và hộ chiếu điện tử là ví dụ cho thẻ danh tính điện tử:

Thẻ CCCD có 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.

Hộ chiếu điện tử (ePassport) hay hộ chiếu sinh trắc học ([*Biometric passport*](https://en.m.wikipedia.org/wiki/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 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. Cấu tạo và cách thức hoạt động của thẻ danh tính điện tử

Thẻ danh tính điện tử có dạng thẻ hình chữ nhật gồm dữ liệu về Quốc gia hoặc tổ chức phát hành nhập dữ liệu cá nhân liên quan đến chủ sở hữu tài liệu và dữ liệu liên quan đến việc ban hành và hiệu lực của thẻ.

A close-up of a computer id card

Description automatically generated

*Hình 1.2: Cấu tạo của thẻ danh tính điện tử*

Thẻ danh tính điện tử được tổ chức dựa trên cấu trúc của hộ chiếu thông thường, được chia thành hai thành phần: phần tài liệu vật lí là thẻ và phần vi mạch tích hợp RFIC (thể hiện dưới dạng chip không tiếp xúc).

1.2.1 Phần vật lý

**1. Kích Thước và Chất Liệu:**

* **Kích thước:** Theo tiêu chuẩn ID-1 của ISO/IEC 7810, kích thước thẻ CCCD là 85.60 x 53.98 mm.
* **Chất liệu:** Thẻ được làm từ nhựa Polycarbonate, một loại nhựa cứng có độ bền cao, chống gãy vỡ và chống mài mòn.

**2. Mặt Trước của Thẻ:**

* **Quốc huy:** Quốc huy Việt Nam ở góc trên bên trái.
* **Dòng chữ:** "CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM" và "Độc lập - Tự do - Hạnh phúc".
* **Tiêu đề:** "CĂN CƯỚC CÔNG DÂN" nằm ở giữa.
* **Ảnh chân dung:** Ảnh màu của người dân kích thước 20x30 mm.
* **Thông tin cá nhân:**
  + Số thẻ CCCD (Mã số định danh cá nhân).
  + Họ và tên.
  + Ngày, tháng, năm sinh.
  + Giới tính.
  + Quốc tịch.
  + Quê quán.
  + Nơi thường trú.
* **Ngày cấp và cơ quan cấp:** Ngày cấp thẻ và cơ quan phát hành thẻ.
* **Chữ ký của chủ thẻ:** Một phần của chữ ký của chủ thẻ.

**3. Mặt Sau của Thẻ:**

* **Thông tin lưu trữ bằng mã vạch:** Mã vạch hai chiều (QR code) lưu trữ thông tin cá nhân.
* **Thông tin lưu trữ bằng chip điện tử:** Thẻ CCCD tích hợp chip điện tử lưu trữ các thông tin chi tiết và dữ liệu sinh trắc học của chủ thẻ.
* **Vùng dữ liệu có thể đọc bằng máy (MRZ):** Một phần nhỏ dành cho vùng dữ liệu có thể đọc bằng máy theo chuẩn ICAO để thuận tiện cho việc kiểm tra tự động tại các điểm kiểm soát.

**4. Chip Điện Tử:**

A text on a white background

Description automatically generated

*Hình 1.4 Mô tả MRZ*

1.2.2 Phần vi mạch tích hợp tần số radio (RFIC)

* **Chức năng:** Chip điện tử trên thẻ CCCD lưu trữ các thông tin cá nhân, dữ liệu sinh trắc học (vân tay, ảnh khuôn mặt, chữ ký điện tử), và các thông tin liên quan khác. Chip này giúp tăng cường bảo mật và thuận tiện trong việc xác minh danh tính.
* **Chuẩn giao tiếp:** Thẻ sử dụng chuẩn giao tiếp không tiếp xúc (ISO/IEC 14443) và chuẩn giao tiếp tiếp xúc (ISO/IEC 7816) cho phép thẻ được đọc bởi các đầu đọc thích hợp.

Chip được đưa vào Thẻ e-ID phải tuân theo chuẩn ISO/IEC 14443, trong đó chỉ ra khoảng cách đọc được chính xác trong khoảng 10cm.

**ISO/IEC 14443-1: Đặc điểm vật lý**

* **Nội dung:** Xác định các đặc điểm vật lý của thẻ không tiếp xúc, bao gồm:
  + Kích thước và hình dạng của thẻ.
  + Chất liệu của thẻ.
  + Độ bền và khả năng chịu nhiệt độ, độ ẩm.
  + Các đặc điểm cơ học như độ cứng và tính linh hoạt của thẻ.

**2. ISO/IEC 14443-2: Giao diện RF (Radio Frequency Interface)**

* **Nội dung:** Quy định về các đặc điểm của giao diện RF giữa thẻ và đầu đọc, bao gồm:
  + Tần số hoạt động: 13.56 MHz.
  + Cơ chế điều chế và mã hóa dữ liệu.
  + Các tham số kỹ thuật của tín hiệu RF, như biên độ, tần số và chu kỳ làm việc.
  + Đặc điểm của sóng mang và cách thức truyền năng lượng từ đầu đọc đến thẻ.

**3. ISO/IEC 14443-3: Giao thức chống xung đột và xử lý lệnh (Initialization and Anti-collision)**

* **Nội dung:** Xác định các quy trình và giao thức để đảm bảo thẻ và đầu đọc có thể giao tiếp mà không bị xung đột, bao gồm:
  + Cơ chế khởi tạo kết nối giữa thẻ và đầu đọc.
  + Quy trình chống xung đột: Cho phép đầu đọc xác định và giao tiếp với một thẻ duy nhất trong trường hợp có nhiều thẻ trong phạm vi hoạt động.
  + Các lệnh cơ bản để bắt đầu phiên làm việc và xác định danh tính thẻ.

**4. ISO/IEC 14443-4: Giao thức truyền thông (Transmission Protocol)**

* **Nội dung:** Quy định giao thức truyền thông giữa thẻ và đầu đọc sau khi quá trình khởi tạo và chống xung đột đã hoàn tất, bao gồm:
  + Các quy tắc trao đổi dữ liệu giữa thẻ và đầu đọc.
  + Cơ chế truyền dữ liệu: Định dạng các khung dữ liệu, cách thức phát hiện và sửa lỗi.
  + Quản lý phiên giao dịch: Đảm bảo dữ liệu được truyền đi một cách liên tục và không bị gián đoạn.

**Lợi ích và ứng dụng của ISO/IEC 14443:**

* **Tương Thích Quốc Tế:** Đảm bảo rằng thẻ không tiếp xúc có thể hoạt động với các đầu đọc khác nhau trên toàn thế giới.
* **Bảo Mật Cao:** Hỗ trợ các giao thức bảo mật để bảo vệ thông tin cá nhân và tài chính.
* **Ứng Dụng Rộng Rãi:** Sử dụng trong nhiều lĩnh vực như hộ chiếu điện tử, thẻ căn cước, thẻ tín dụng, vé điện tử, và các hệ thống thanh toán không tiếp xúc.
* **Tiện Lợi:** Cho phép giao tiếp nhanh chóng và thuận tiện mà không cần tiếp xúc vật lý.

**Các công nghệ liên quan:**

* **RFID (Radio Frequency Identification):** Công nghệ sử dụng sóng radio để truyền dữ liệu giữa thẻ và đầu đọc.
* **NFC (Near Field Communication):** Một tập hợp con của RFID, cho phép giao tiếp ở khoảng cách ngắn (dưới 10 cm) và thường được sử dụng trong các thiết bị di động và hệ thống thanh toán.

ISO/IEC 14443 là tiêu chuẩn quan trọng đảm bảo sự hoạt động hiệu quả và an toàn của các hệ thống thẻ không tiếp xúc, góp phần vào sự phát triển của các giải pháp nhận dạng và thanh toán hiện đại.

**1.2.3 Đặc điểm vật lí của MRTD**

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.

1. **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.

1. **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.

1. **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.

1. **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 mống mắt, được lưu trữ trong chip để xác thực danh tính của người sở hữu.

1. **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.

1. **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.

A diagram of a card

Description automatically generated

*Hình 1.5 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.*

1.2.4 Các thông số kỹ thuật của thẻ

**A diagram of a rectangular object with numbers and lines

Description automatically generated with medium confidence**

*Hình 1.6 Minh họa các kích thước ISO / IEC 7810 tính bằng milimét*

Tiêu chuẩn xác định bốn kích thước thẻ: ID-1, ID-2, ID-3 và ID-000.

* ID-1

Định dạng ID-1 chỉ định kích thước 85,60 x 53,98 mm (3+3 ⁄ 8 in × 2+1 ⁄ 8 in) và các góc tròn có bán kính 2,88–3,48 mm (khoảng1 ⁄ 8 in). Nó thường được sử dụng cho[các loại thẻ thanh toán](https://en.wikipedia.org/wiki/Payment_cards) ([thẻ ATM](https://en.wikipedia.org/wiki/Automated_teller_machine) , thẻ[tín dụng](https://en.wikipedia.org/wiki/Credit_card) ,[thẻ ghi nợ](https://en.wikipedia.org/wiki/Debit_card) , v.v.). Ngày nay nó cũng được sử dụng cho[giấy phép lái xe](https://en.wikipedia.org/wiki/Driving_licence) và chứng minh thư cá nhân ở nhiều quốc gia,[thẻ hệ thống thu phí tự động](https://en.wikipedia.org/wiki/Automated_fare_collection_system) 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+1 ⁄ 8 in × 2+15 ⁄ 16 in). Kích thước này là định dạng[A7.](https://en.wikipedia.org/wiki/ISO_216)Ví dụ: định dạng ID-2 được sử dụng cho[thị thực](https://en.wikipedia.org/wiki/Visa_(document)).

* ID-3

ID-3 chỉ định kích thước 125 x 88 mm (4+15 ⁄ 16 in × 3+7 ⁄ 16 in). Kích thước này làđịnh dạng[B7 .](https://en.wikipedia.org/wiki/ISO_216)Định dạng này thường được sử dụng cho các[cuốn sổ hộ chiếu](https://en.wikipedia.org/wiki/Passport) .

* ID-000

ID-000 chỉ định kích thước 25 x 15 mm (1 in × 9 ⁄ 16 in), với một góc hơi vát (3 mm hoặc 1 ⁄ 8 in). Kích thước này được sử dụng cho định dạng " [mini-SIM](https://en.wikipedia.org/wiki/Mini-SIM) " của [mô-đun nhận dạng thuê bao](https://en.wikipedia.org/wiki/Subscriber_identity_module) .

1.2.5 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 (WWII) cho hệ thống nhận dạng, bạn hay thù (IFF). 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. RFID hệ thống cho Hộ chiếu được Kích hoạt (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 vi mạch 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 thích các tần số dữ liệu là có ý nghĩa.

1.3 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 trong Bảng 1 dưới đây:

*Bảng 1-1: Mức độ đảm bảo danh tính điện tử*

|  |  |  |
| --- | --- | --- |
| **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 |

1.5 Tiêu chí chuẩn quy định của thẻ chip

Hiện nay, bộ tiêu chuẩn TCVN 11689 (ISO/IEC 14443) về *Thẻ định danh - Thẻ mạch tích hợp không tiếp xúc - Thẻ cảm ứng* gồm các tiêu chuẩn:

* + TCVN 11689-1:2016 (ISO/IEC 14443-1:2016), Phần 1: Đặc tính vật lý
  + TCVN 11689-2:2016 (ISO/IEC 14443-2:2016), Phần 2: Giao diện tín hiệu và công suất tần số radio
  + TCVN 11689-3:2016 (ISO/IEC 14443-3:2016), Phần 3: Khởi tạo và chống va chạm
  + TCVN 11689-4:2016 (ISO/IEC 14443-4:2016), Phần 4: Giao thức truyền dẫn.

sử dụng đồng thời nhiều giao diện vật lý, thì mối quan hệ giữa các sự việc xảy ra trên các giao diện vật lý khác nhau không thuộc phạm vi của tiêu chuẩn này.

## **1.6 Kết luận chương 1**

Qua chương 1, Quy định về định danh, xác thực điện tử tạo thành một bước tiến quan trọng đối với tầm nhìn về Thị trường kỹ thuật số duy nhất cho quốc gia, thúc đẩy chuyển đổi số trong khu vực công và tư nhân. Điều quan trọng cần hiểu là không giống như luật bắt buộc và hạn chế hành vi; định danh, xác thực điện tử là phương thức hỗ trợ, thiết lập các tiêu chuẩn được pháp luật công nhận cho thương mại điện tử và dịch vụ công.

Danh tính điện tử giúp khẳng định chính xác danh tính số hợp pháp của người thực hiện giao dịch, nâng cao độ bảo mật và tin tưởng giữa cả người dân, chính quyền và doanh nghiệp (DN) trên môi trường số. Thẻ định danh điện tử hứa hẹn tạo ra giá trị kinh tế bằng cách thúc đẩy tăng cường hòa nhập, mang lại khả năng tiếp cận hàng hóa và dịch vụ nhiều hơn; tăng cường quy trình hóa, giúp giảm gian lận danh tính, duy trì quyền hạn và tăng tính minh bạch và thúc đẩy số hóa, thúc đẩy tính năng động và dễ sử dụng của các dịch vụ được cung cấp.

CHƯƠNG 2: DỮ LIỆU TRÊN THẺ DANH TÍNH ĐIỆN TỬ

## 2.1. Dữ liệu và bảo vệ dữ liệu sinh trắc trên chip

### 2.1.1. Dữ liệu được lưu trữ

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 lẫn nhau**

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 mống 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
* Hình học bàn tay
* Nhận dạng tĩnh mạch ngón tay
* Nhận dạng khuôn mặt
* Nhận dạng mống 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.

Ví dụ: một người có thể chia sẻ mã PIN nhưng không thể chia sẻ dấu vân tay. Thông tin sinh trắc học đặc biệt hữu ích khi được thu thập bằng phần cứng an toàn trong môi trường được kiểm soát để ngăn những kẻ tấn công giả mạo (tức là gửi sai) dữ liệu sinh trắc học. Mặc dù các cuộc tấn công giả dạng là hợp lý trong nhiều điều kiện khác nhau, nhưng sinh trắc học có thể bổ sung một lớp bảo mật khác cho hệ thống e-ID.

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 eI-D 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 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 và
* 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 eID không dẫn đến bằng chứng nhận dạng vĩnh viễn trong thế giới thực. Thay vào đó, quá trình nhận dạng là tạm thời và không thể được chứng minh cho bên thứ ba, thẻ eID 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 eID và được truyền qua kênh 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 eID 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.

**2.1.2. Cơ chế xác thực**

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:

1. **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.

.

1. **Xác thực lẫn nhau thông qua Kiểm soát truy cập mở rộng**

* **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.

1. **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.

### Dữ liệu và cách lưu trữ dữ liệu trên chip

### 2.1.1 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.

A black letters and numbers

Description automatically generated

Hình 2.5. 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

A diagram of a machine reading zone

Description automatically generated

Hình 2.6. Sơ đồ vùng đọc hiệu quả MRTD

**Quy trình 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 Kπ và lấy các khóa phiên KSEnc và KSMAC (Giao thức PACE được mô tả trong Phần chương III)

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

• Nó sẽ bắt đầu Nhắn 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 Nhắn 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 (KEnc và KMAC) 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 KSEnc và KSMAC.

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

• Nó sẽ bắt đầu Nhắn 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 Nhắn tin an toàn.

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

## Các giao thức mật mã được triển khai trên eID

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 eID 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.

A diagram of a computer security system

Description automatically generated

*Hình 2.7: Các giao thức mật mã*

Giao thức kiểm soát truy cập mở rộng. Giao thức Kiểm soát truy cập mở rộng (EAC) ban đầu được đề xuất vào năm 2005 bởi Văn phòng Bảo mật Thông tin Liên bang Đức (BSI) cho hộ 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 khuyến nghị và giới thiệu vào tháng 11 năm 2010 cho thẻ ID của Đức, 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). Các BSI đã tích hợp EAC trong thẻ nhận dạng điện tử (eID) 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.

## **Các kỹ thuật mật mã đảm bảo an toàn cho dữ liệu eID**

### **Chữ ký kỹ thuật số**

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.

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 1λ, 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:

**1. Key Generation (Tạo khóa)**

* Nhập thông số bảo mật 𝜆*λ*: Thông số bảo mật 𝜆*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*λ* có thể là 2048 bit, 3072 bit, v.v.). Một giá trị 𝜆*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*λ* để sinh ra một cặp khóa.
  + 𝑠𝑘*sk* (private key - khóa riêng): Khóa riêng được giữ bí mật và sử dụng để tạo chữ ký số.
  + 𝑝𝑘*pk* (public key - khóa công khai): Khóa công khai được phân phối rộng rãi và sử dụng để xác minh chữ ký số.

**2. Signature (Tạo chữ ký)**

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

**3. Verification (Xác minh chữ ký)**

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

**Quy trình tổng thể**

1. Tạo khóa: Một người dùng hoặc hệ thống tạo ra một cặp khóa công khai và khóa riêng.
2. Ký thông báo: Người dùng sử dụng khóa riêng của mình để ký một thông báo, tạo ra chữ ký số.
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 𝑠𝑘*sk* và khóa công khai 𝑝𝑘*pk*).
* Bước 2: Ký thông báo
  + Alice có thông báo 𝑚*m* muốn ký. Cô ấy sử dụng khóa riêng 𝑠𝑘*sk* và thuật toán sig để tạo chữ ký số 𝜎*σ*.
* Bước 3: Xác minh chữ ký
  + Bob nhận được thông báo 𝑚*m* và chữ ký 𝜎*σ* từ Alice. Anh ấy sử dụng khóa công khai 𝑝𝑘*pk* của Alice và thuật toán SVf để kiểm tra tính hợp lệ của chữ ký 𝜎*σ*.
  + Nếu thuật toán trả về 1, Bob biết rằng thông báo 𝑚*m* 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) ← SKGen (1λ), đối với bất kỳ thông điệp m, bất kỳ chữ ký nào σ ← Sig (sk, m), chúng tôi phải có SVf (pk, m, σ) = 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).

### **Lược đồ mã hoá**

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 đại khái, 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 eID 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 = (KGen, Enc, Dec) được định nghĩa như sau:

CHƯƠNG 3: KỸ THUẬT MẬT MÃ ĐẢM BẢO AN TOÀN CHO THẺ DANH TÍNH ĐIỆN TỬ (eid card)

Các vấn đề nguy hiểm và nguy cơ bị tấn công trên thẻ

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 [7], 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.

## **Cơ chế mật mã giao thức PACE và EAC**

**Bảo mật của 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:

1. **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.
2. **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.
3. **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.
4. **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, đưa ra một giả định lý thuyết số mới, 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 đóng góp vào đầu vào của DH hoặc trực tiếp, thông qua yC (tương ứng. yT), hoặc gián tiếp, thông qua ánh xạ vào trình tạo nhóm gˆ bao gồm sự lựa chọn của nonce s và các giá trị tạm thời trong Map2Point. Do đó, vấn đề gPACE-DH nói rằng không có đối thủ hiệu quả nào có thể tính toán giá trị DH cuối cùng ngay cả khi đối thủ có tác động mạnh đến DH tương ứng chấp hành. Đặc biệt, điều này có nghĩa là giá trị DH được băm, 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 + ε.

|  |
| --- |
| gPACE-DH  Map2Point,N,Q,A (λ)  pick authenticated group parameters G = (a, b, p, q, g, λ) (s1, . . . ,sn,st) ←R A0(G, N) with s1, . . . ,sn pairwise distinct pick yT ←R Zq and k ←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, . . . , KQ) ← A2(state, gˆ yT )  Return 1  iff YC ≠ 0 and Ki = Y yT C for some i ∈ [Q]. |

**Bảo mật của EAC**

Giao thức Kiểm soát Truy cập Mở rộng (EAC) được đề xuất vào năm 2005 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.

## Mô hình xác thực Eid thử nghiệm ứng dụng cơ chế PACE và EAC

Mô hình xác thực Eid

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

B1: 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.

B2: Kiểm tra các đặc tính bảo mật trên thẻ thông qua các đặc điểm an ninh truyền thống đã biết: thuỷ ấn, dải quang học, lớp bảo vệ ảnh…

B3: 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 mống 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.

B4: Tiến hành quá trình TA để chứng mình quyền truy cập của đầu đọc đến phần dữ liệu DG3, DG4.

B5: 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 eID. Việc trao đổi khoá thông qua chứng chỉ số theo mô hình khuyến cáo của ICAO.

B6: Tiến hành CA để chứng minh được tính nguyên gốc của chip đồng thời cung cấp khoá phiên mạnh cho truyền thông báo bảo mật.

B7: IS đối sánh dữ liệu sinh trắc thu nhận được trực tiếp từ người xuất trình eID 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 eID có đủ điều kiện để tin tưởng eID là xác thực và người mang eID đúng là con người mô tả trong eID. Nếu cơ quan kiểm tra eID 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.

A diagram of a data flow

Description automatically generated

*Hình 3.1: Mô hình xác thực Eid*

Giải thích mô hình với cơ chế PACE và EAC

**1.** Kiểm tra an ninh Công dân mang eID xuất trình thẻ cho hệ thống kiểm duyệt (IS). Trước tiên EID 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 eID hay dùng thủy ấn để bảo vệ booklet…

**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 Kπ : z = E(Kπ, s) với Kπ = SHA-1(π||3) và gửi bản mã z cùng các tham số miền tĩnh D đến cho IS.
* IS khôi phục lại bản rõ s = D(Kπ, z) sử dụng mật khẩu chung π.
* Cả RFID và IS cùng thực hiện các bước sau:
* Tính các tham số miền tĩnh D’ dựa trên D và s: D’ = Map(D,s)
* Thực hiện giao thức thoả thuận khoá DiffieHellman dựa trên D’ và khoá chia sẻ.
* K=KA(PACEKPrT,PACEKPuR,D’)= KA(PACEKPrR,, PACEKPuT, D’ )

Trong suốt quá trình thoả thuận khoá DH, mỗi bên phải kiểm tra rằng hai khoá công khai PACEKPuR và PACEKPuT là khác nhau. Từ đó cả hai bên tính cá khoá phiên KMAC và KENC. RFID tính thẻ xác thực TT = MAC(KM, (PACEPuR, D’)) và gửi đến cho IS thẩm định. IS tính thẻ xác thực TR = MAC(KM, (PACEPuT, D’)) và gửi đến cho RFID thẩm định.

A diagram of a rfid

Description automatically generated

*Hình 3.2: Lược đồ PACE*

1. **Đọc vùng dữ liệu DG1**

Sau khi PACE thành công, hệ thống xác thực eID sẽ tiến hành đọc vùng dữ liệu DG1 trong chip RFID của EID 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.

1. **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:

1. IS gửi chuỗi chứng chỉ đến chip gồm CIS và CDV.

2. RFID kiểm chứng các chứng chỉ này sử dụng PKCVCA và trích khoá công khai của đầu đọc RPuK.

3. IS sinh ra cặp khoá DH ngắn hạn trên miền D: RPrKTA, RPuKTA. Sau nó gửi Comp(RPuKTA) và dữ liệu ATA đến cho RFID

4. RFID gửi thách đố ngẫu nhiên rRFID đến IS.

5. IS trả lời bằng chữ ký sIS=Sign(RPuK,IDTA||r||Comp(RPuKTA)||ATA)

6. Chip kiểm tra chữ ký nhận được từ IS bằng khoá RPuKTA Verify(RPuKTA, sIS, IDRFID || rRFID || Comp(RPuKTA)||ATA))

A diagram of a rfid

Description automatically generated

*Hình 3.2: Lược đồ TA*

1. **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 eID. 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 eID là nguyên gốc.

1) Đọc SOD từ chip RFID.

2) Lấy chứng chỉ DV-Cert từ SOD vừa đọc ở trên.

3) 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.

4) 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 eID và SOLDS không bị thay đổi.

5) Đọc các thông tin cần thiết từ LDS.

6) 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.

**A yellow background with black text

Description automatically generated**

*Hình 3.3: Lược đồ PA*

1. 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:

1) RFID gửi cho IS khoá công khai (TPuK).

2) IS gửi khoá công khai ngắn hạn RPuKTA đã được sinh ra trong TA đến cho RFID.

3) RFID tính Comp(RPuKTA) và dữ liệu ATA. Nó sẽ so sánh giá trị Comp này với giá trị nó nhận được từ TA.

4) RFID và IS có đủ thông tin chia sẻ để tính khoá Kseed.

5) RFID sinh ra chuỗi ngẫu nhiên (R). Các khoá phiên được tính: KMAC = SHA1(Kseed||R||2) và KENC = SHA-1(Kseed||R||1).

6) 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.

**A diagram of a rfid

Description automatically generated**

*Hình 3.4: Lược đồ CA*

1. **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 hộ chiếu (ảnh khuôn mặt, dấu vân tay, mống 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, mống 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 hộ chiếu điện tử đó là đúng đắn và người mang hộ chiếu 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 EID như: đảm bảo tính chân thực (quy trình rõ rang); tính không thể nhân bản (sử dụng CA và PA); tính nguyên vẹn và xác thực (PA và PKI), tính liên kết công dân-EID (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 eID 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 EID 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.

**XÂY DỰNG HỆ THỐNG IOT ĐỌC GHI DỮ LIỆU TRÊN THẺ RFID**

**4.1 Giới thiệu tổng quan mô hình**

**4.1.1 Công nghệ và các công cụ lập trình**

**4.1.2 Giới thiệu thiết bị**

**ESP8266**

ESP8266 là một vi điều khiển tích hợp Wi-Fi được sản xuất bởi công ty Espressif Systems. Đây là một trong những module Wi-Fi phổ biến nhất hiện nay do tính năng mạnh mẽ và giá thành phải chăng, thường được sử dụng trong các dự án IoT (Internet of Things). Dưới đây là một số đặc điểm chính của ESP8266:

1. **Kết nối Wi-Fi**: ESP8266 có khả năng kết nối mạng Wi-Fi, cho phép nó truyền và nhận dữ liệu qua internet.
2. **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.
3. **Bộ nhớ**: ESP8266 có bộ nhớ flash từ 512KB đến 4MB và RAM 50KB để lưu trữ và chạy các chương trình.
4. **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.
5. **Giao tiếp**: Nó hỗ trợ nhiều giao tiếp như UART, SPI, I2C, PWM, và ADC.

**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.

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:

**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.

**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.

4.2 Mô tả hệ thống

4.3 Cách thức hoạt động

**KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

**Kết quả đạt được**

Nội dung trình bày bám sát mục tiêu đề ra của đồ án “Nghiên cứu, tìm hiểu kỹ thuật mật mã bảo đảm an toàn cho thẻ danh tính điện tử”. Việc sử dụng e-ID đã minh chứng ưu việt trong việc cấp phát và kiểm soát hộ chiếu. Phân tích các thế hệ e-ID giúp chúng ta hiểu rõ ưu và nhược điểm, từ đó đề xuất giải pháp phù hợp.

Dù e-ID thế hệ thứ nhất vẫn còn được sử dụng, nhưng thế hệ thứ ba với những cải tiến về an ninh, an toàn khẳng định tiềm năng ứng dụng cao. Tuy nhiên, vấn đề về tuổi thọ đầu đọc ở thế hệ này cần được giải quyết. Những thử nghiệm trong mô hình đề xuất hy vọng sẽ là nền tảng cho 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.

**Hướng phát triển**

Mục tiêu của đồ án 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

**TÀI LIỆU THAM KHẢO**