

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN



CHỨNG THỰC ĐIỆN TỬ

BÀI TẬP LỚN

**Nghiên cứu các thiết bị phần cứng Hardware Token
(USB token, smart card, HSM), nguyên lý hoạt động
và mô phỏng triển khai**

Sinh viên thực hiện:

Phạm Anh Minh - AT160148

Trần Văn Sáng – AT160545

Giảng viên hướng dẫn: Nguyễn Thi Hồng Hà

Hà Nội, tháng 5 năm 2023

MỤC LỤC

Chương 1. Tổng quan về Hardware Token	1
1.1 Khái niệm	1
1.2 Token	2
1.2.1 Khái niệm token	2
1.2.2 Hard Token và Soft Token	3
1.2.3 Hard token	3
1.2.4 Soft token.....	3
1.2.5 Sự khác nhau Hard token và Soft token	4
1.3 Nguyên lý hoạt động Của Hardware Token	4
1.4 Vai trò và ứng dụng của Hardware Token	5
1.4.1 Vai trò của hardware token	5
1.4.2 Ứng dụng của hardware token.....	6
1.5 Tính năng của Hardware token.....	6
1.5.1 Tính bảo mật.....	7
1.5.2 Xác thực người dùng	7
1.5.3 Chống phishing.....	8
1.5.4 Tính di động	8
1.5.5 Khả năng tạo chữ ký số	9
1.5.6 Khả năng lưu trữ thông tin	10
1.5.7 Khả năng phát hiện nghi ngờ.....	10
Chương 2. USB Token, Smart Card và HSM.....	11
2.1 USB Token.....	12
2.1.1 Tổng quan.....	12
2.1.2 Tính pháp lý.....	13

2.1.3 Chức năng.....	14
2.1.4 Phân loại	15
2.1.4.1 Phân loại theo mục đích sử dụng.....	15
2.1.4.2 Phân loại theo cấu trúc và chức năng	16
2.1.5 Nguyên lý hoạt động	17
2.2 Smart Card.....	18
2.2.1 Tổng quan	18
2.2.2 Phân loại	21
2.2.2.1 Phân loại dựa trên công nghệ chip	21
2.2.2.2 Phân loại theo công nghệ đọc dữ liệu.....	23
2.2.3 Nguyên lý hoạt động	27
2.2.3.1 Lưu trữ Thông tin	27
2.2.3.2 Xử lý Thông tin	28
2.2.3.3 Giao tiếp với Thiết bị Bên ngoài	28
2.2.3.4 Bảo mật và Xác thực	32
2.2.4 Ứng dụng.....	35
2.2.5 Ưu điểm và hạn chế.....	37
2.3 HSM (Hardware Security Module)	39
2.3.1 Tổng quan	39
2.3.2 Chức năng.....	40
2.3.3 Phân loại	41
2.3.4 Nguyên lý hoạt động	43
2.3.5 Ứng dụng.....	44
Chương 3. Mô phỏng triển khai.....	46
3.1 Phần cứng	46
3.1.1 Module RFID RC522	46

3.1.1.1 Đặc điểm.....	47
3.1.1.2 Ứng dụng.....	47
3.1.1.3 Sơ đồ chân	47
3.1.2 Arduino UNO	49
3.2 Triển khai.....	50
3.2.1 Phần mềm	50
3.2.2 Kịch bản.....	51
3.2.2.1 Đọc thẻ.....	52
3.2.2.2 Xác thực 1 yếu tố.....	55
3.2.2.3 Xác thực 2 yếu tố với mật khẩu.....	57
Tài liệu tham khảo.....	61

DANH MỤC HÌNH ẢNH

Hình 1.1: Hardware Tokens.....	1
Hình 1.2: Soft Token	3
Hình 2.1: Chữ ký số.....	11
Hình 2.2: USB Token	12
Hình 2.3: Smart Card.....	19
Hình 2.4: Mô hình Smart Card	20
Hình 2.5: Kích thước tiêu chuẩn của Smart Card	20
Hình 2.6: Phân loại Smart Card dựa trên công nghệ chip.....	21
Hình 2.7: Phân loại Smart Card dựa trên công nghệ đọc dữ liệu.....	23
Hình 2.8: Tiếp điểm điện của Contact Smart Card	24
Hình 2.9: Máy đọc thẻ tiếp xúc	25
Hình 2.10: Thẻ thông minh không tiếp xúc.....	27
Hình 2.11: Công nghệ RFID	30
Hình 2.12: Ứng dụng của công nghệ NFC.....	31
Hình 2.13: HSM	39
Hình 2.14: Sự khác nhau giữa USB Token và HSM.....	40
Hình 2.15: Nguyên lý hoạt động HSM.....	43
Hình 3.1: Module RFID RC522	46
Hình 3.2: Cấu tạo chân module RFID RC522	48
Hình 3.3: Các chân của module RFID RC522	49
Hình 3.4: Arduino UNO nối với module RFID RC522	49
Hình 3.5: Arduino UNO	50
Hình 3.6: Cách nối chân module RFID RC522 và Arduino UNO	50
Hình 3.7: Chọn board Arduino Uno	51
Hình 3.8: Chạm thẻ vào module RFID RC522	52
Hình 3.9: Kết quả đọc thẻ RFID.....	54
Hình 3.10: Xác thực 1 yếu tố thành công.....	57
Hình 3.11: Xác thực 1 yếu tố thất bại.....	57
Hình 3.12: Xác thực 2 yếu tố thành công.....	59
Hình 3.13: Xác thực 2 yếu tố thất bại.....	60

LỜI NÓI ĐẦU

Hardware Token là một thiết bị phần cứng được sử dụng để xác thực người dùng trong các hệ thống bảo mật. Nó bao gồm các loại như USB Token, smartcard, và HSM. Thiết bị này hoạt động bằng cách lưu trữ các thông tin xác thực và sử dụng chúng để tạo ra các mã xác thực duy nhất mỗi khi người dùng đăng nhập vào hệ thống. Hardware Token là một giải pháp bảo mật hiệu quả cho các hệ thống yêu cầu tính xác thực cao.

Trong một hệ thống bảo mật, việc xác thực người dùng là một yếu tố vô cùng quan trọng, giúp đảm bảo tính toàn vẹn và bảo mật cho các thông tin nhạy cảm.

Với các giải pháp bảo mật truyền thống, phương pháp xác thực người dùng thường được thực hiện bằng mật khẩu hoặc mã PIN. Tuy nhiên, với sự phát triển của các công nghệ mới, các giải pháp bảo mật dựa trên phần cứng, như Hardware Token, đang trở thành một lựa chọn phổ biến hơn.

Hardware Token được thiết kế để lưu trữ thông tin xác thực của người dùng và sử dụng chúng để tạo ra các mã xác thực duy nhất mỗi khi người dùng đăng nhập vào hệ thống. Với cách thức hoạt động này, Hardware Token giúp đảm bảo tính xác thực cao và ngăn chặn các cuộc tấn công giả mạo danh người dùng.

Các loại Hardware Token phổ biến hiện nay bao gồm USB Token, smartcard, và HSM. USB Token thường được sử dụng trong các hệ thống phần mềm, trong khi smartcard và HSM thường được sử dụng trong các hệ thống phức tạp hơn, như các hệ thống tài chính hoặc hệ thống y tế.

Nghiên cứu về smart card là một trong những nhiệm vụ quan trọng trong việc triển khai các giải pháp bảo mật. Các tiêu chuẩn và quy trình giao tiếp, cấu trúc và thành phần, các thuật toán và giao thức bảo mật, cũng như các thách thức và rủi ro an ninh liên quan đến việc sử dụng smart card, đều là các lĩnh vực cần được nghiên cứu kỹ.

Tuy nhiên, với sự phát triển của các công nghệ mới, các giải pháp bảo mật dựa trên smart card cũng đang được cập nhật và phát triển. Ví dụ như tích hợp với công nghệ di động, các giải pháp dựa trên đám mây và phát triển của các thuật toán và giao thức bảo mật. Do đó, việc theo dõi các công nghệ mới và các xu hướng phát triển mới sẽ giúp cho việc triển khai các giải pháp bảo mật trở nên hiệu quả hơn.

Trong báo cáo bài tập lớn này, nhóm em đã trình bày tổng quan về hardware token, bao gồm các thông tin cơ bản, phân loại và chức năng của USB Token, Smart Card và HSM. Tuy nhiên, để giải quyết vấn đề bảo mật thông tin hiệu quả, nhóm em nhận thấy rằng Smart Card là thiết bị hiện nay đang phổ biến nhất trong số 3 thiết bị nêu trên. Vì vậy, nhóm em đã tập trung tìm hiểu về Smart Card và triển khai mô phỏng hoạt động của nó với module RFID RC522.

Trong phần 1 của báo cáo, nhóm em sẽ cung cấp cho độc giả tổng quan về Hardware Token, bao gồm các định nghĩa và mô tả về tính năng của nó. Phần 2 sẽ tập trung vào việc trình bày chi tiết về USB Token, Smart Card và HSM, trong đó tập trung vào Smart Card, thiết bị được nhóm em cho là phổ biến nhất và có tính ứng dụng cao trong cuộc sống hàng ngày. Cuối cùng, phần 3 sẽ mô phỏng triển khai đọc thông tin Smart Card, xác thực 1 yếu tố và 2 yếu tố sử dụng module RFID RC522, giúp độc giả hiểu rõ hơn về cách thức hoạt động của Smart Card và cách sử dụng nó để bảo vệ thông tin cá nhân.

Tóm lại, báo cáo của nhóm em sẽ cung cấp cho độc giả những kiến thức cơ bản về hardware token và tập trung vào việc giới thiệu Smart Card, thiết bị được sử dụng nhiều nhất hiện nay, và cách sử dụng nó để bảo vệ thông tin cá nhân của mình.

Chương 1. Tổng quan về Hardware Token

1.1 Khái niệm

Hardware Token là một loại thiết bị vật lý được sử dụng để cung cấp mã xác thực cho việc xác thực người dùng trong các hệ thống bảo mật thông tin. Nó là một phương tiện xác thực hai yếu tố, yêu cầu người dùng cung cấp cả thông tin đăng nhập (tên đăng nhập và mật khẩu) và mã xác thực từ thiết bị vật lý.

Có nhiều loại mã thông báo phần cứng khác nhau, bao gồm mã thông báo USB, smartcard và HSM (Mô-đun bảo mật phần cứng). Mỗi loại có đặc điểm riêng, tuy nhiên chúng đều hoạt động theo cùng một nguyên tắc chung: sử dụng mã xác thực tạm thời, được sinh ra bởi một thuật toán bảo mật, để xác thực người dùng.



Hình 1.1: Hardware Tokens

Một số ưu điểm của mã thông báo phần cứng bao gồm tính an toàn cao hơn so với các phương tiện xác thực khác như mật khẩu hoặc mã thông báo mềm, tính tiện dụng và dễ sử dụng, và khả năng tương thích với nhiều hệ thống bảo mật thông tin khác nhau.

Tuy nhiên, mã thông báo phân cứng cũng có những hạn chế như tính toán cơ động thấp, khi người dùng cần mang theo thiết bị vật lý để có thể sử dụng và chi phí cao hơn so với các phương tiện xác thực khác.

Trong tổ chức, mã thông báo phân cứng thường được sử dụng để bảo vệ các thông tin quan trọng như thông tin tài khoản ngân hàng, thông tin bệnh nhân trong các hệ thống y tế, thông tin khách hàng trong các hệ thống thương mại điện tử và other information information.

1.2 Token

1.2.1 Khái niệm token

Token là một dạng chữ kí điện tử, được mã hóa thành một dãy số duy nhất trên thiết bị. Mã token sẽ xuất hiện dưới dạng mã OTP ngẫu nhiên và chỉ sử dụng duy nhất một lần. Token thường được thấy trong các giao dịch trực tuyến giữa các doanh nghiệp và người được sử dụng để xác minh danh tính. Cũng vì mục đích bảo mật sau mỗi lần giao dịch, mã token sẽ được thay đổi ngẫu nhiên khác nhau hoàn toàn.

Hầu hết các doanh nghiệp khi thực hiện các giao dịch, nhất là giao dịch online thường áp dụng Token này, xem như mật khẩu bắt buộc mà bạn phải nhập cho mỗi lần bạn thực hiện giao dịch với mục đích bảo mật.

Xác nhận giao dịch bằng mã Token, doanh nghiệp đã được đảm bảo chính xác. Khi bạn đã xác nhận bằng mã Token này, đồng nghĩa với việc bạn đã ký kết vào hợp đồng giao dịch thay vì phải có giấy tờ chứng minh. Do đó, mã Token này có giá trị pháp lý giống như chữ ký của bạn.

Ưu điểm:

- Máy Token nhỏ gọn, bạn dễ dàng cầm đi mọi nơi
- Có tính bảo mật an toàn cao, không có trường hợp bạn mất tiền khi giao dịch
- Sử dụng máy Token dễ dàng, hiệu quả
- Mã OTP sử dụng một lần, dù có bị lộ thì mã OTP đó cũng bị vô hiệu hóa với các giao dịch sau đó

Nhược điểm:

- Để mua máy Token, bạn phải bỏ chi phí dao động từ 200.000 tới 400.000 đồng
- Mã Token này chỉ có hiệu lực trong thời gian ngắn 60 giây

- Các giao dịch giao dịch được thì phải có máy Token

1.2.2 Hard Token và Soft Token

Token được sử dụng rộng rãi trong nhiều lĩnh vực, đặc biệt về tài chính như ngân hàng, cơ quan thuế... Token hiện nay có hai loại căn bản là hard token và soft token

1.2.3 Hard token

Hard token được biết đến là một thiết bị khá nhỏ gọn và có thể giúp người sử dụng dễ dàng mang đi mọi nơi. Mã token này được dùng để xác thực thiết bị, giúp truy cập vào một tài sản kỹ thuật số nào đó. Ổ usb, thẻ, bàn phím RFID và thậm chí chìa khóa đều có thể là hard token.

Trong mỗi lần giao dịch, người dùng có thể dùng thiết bị này để lấy mã số, và để có được thiết bị này người dùng phải làm việc với ngân hàng nơi mở tài khoản ngân hàng trước đó.

1.2.4 Soft token

Soft token là một phần mềm hoặc ứng dụng cung cấp mã token khi giao dịch và được cài đặt sẵn trên máy tính, điện thoại hoặc các thiết bị di động khác. Khi giao dịch trực tuyến, phần mềm này tự động sinh ra các mã OTP.



Hình 1.2: Soft Token

1.2.5 Sự khác nhau Hard token và Soft token

Hard token và soft token là hai phương tiện xác thực khác nhau được sử dụng trong bảo mật thông tin. Dưới đây là một số điểm khác nhau giữa mã thông báo cứng và mã thông báo mềm:

1. Tính cơ động: Hard token là một thiết bị vật lý, do đó nó có tính cơ động thấp hơn so với soft token, vì bạn cần mang theo nó để có thể xác thực. Soft token là một ứng dụng phần mềm trên máy tính hoặc điện thoại thông minh, do đó nó có tính cơ động cao hơn và dễ dàng mang theo bất cứ nơi nào.

2. Độ an toàn: Hard token thường được xem là an toàn hơn so với soft token vì nó cung cấp một lớp bảo vệ vật lý. Tuy nhiên, nếu hard token bị đánh cắp hoặc mất, thì người dùng phải thực hiện các bước khác để cập nhật lại mã xác thực. Soft token có thể được bảo vệ bằng mật khẩu mạnh, tuy nhiên, nó có thể bị tấn công từ xa thông qua các lỗ hổng phần mềm.

3. Độ tin cậy: Hard token có độ tin cậy cao hơn so với soft token, vì nó không bị ảnh hưởng bởi lỗi phần mềm hoặc virus máy tính. Tuy nhiên, soft token có thể được cập nhật thường xuyên để giải quyết các lỗ hổng bảo mật.

4. Độ dễ sử dụng: soft token có mức độ dễ sử dụng cao hơn so với hard token, vì nó chỉ cần được cài đặt trên máy tính hoặc điện thoại di động và không cần phải mang theo một thiết bị vật lý. Tuy nhiên, việc sử dụng soft token có thể yêu cầu người dùng phải có kiến thức về phần mềm và bảo mật.

5. Chi phí: hard token có chi phí đầu tư ban đầu cao hơn so với soft token. Ngoài ra, nếu thiết bị bị hỏng hoặc bị mất, người dùng sẽ phải mua thiết bị mới để thay thế. Trong khi đó, hard token có chi phí đầu tư ban đầu thấp nhất và người dùng có thể tải xuống và cài đặt miễn phí trên nhiều thiết bị.

Cả hai loại token đều có những ưu điểm và nhược điểm riêng, và việc lựa chọn loại token phù hợp phụ thuộc vào nhu cầu và yêu cầu bảo mật của từng tổ chức hoặc người dùng.

1.3 Nguyên lý hoạt động Của Hardware Token

Các mã thông báo phân cứng, chẳng hạn như mã thông báo USB hoặc thẻ thông minh, thường hoạt động theo các bước sau:

B1: Người dùng cắm mã thông báo của thiết bị vào cổng USB hoặc thẻ đọc thẻ trên máy tính.

B2: Máy tính nhận diện và yêu cầu người dùng nhập mật khẩu để mở khóa mã thông báo thiết bị.

B3: Sau khi xác thực người dùng, mã thông báo thiết bị sẽ sinh ra một mã xác thực một lần (Mật khẩu một lần - OTP) dựa trên một thuật toán bảo mật được tích hợp sẵn trong mã thông báo.

B4: Người dùng sử dụng mã xác thực này để đăng nhập hoặc thực hiện các thao tác an toàn trên hệ thống.

B5: Sau khi sử dụng, mã xác thực sẽ tự hết hạn và không thể sử dụng lại.

Mã thông báo thiết bị cũng có thể tích hợp các tính năng bảo mật khác như mã hóa dữ liệu, chữ ký số hoặc chứng thực phần mềm.

Một số mã thông báo thiết bị còn được tích hợp với máy chủ chứng thực (Máy chủ xác thực) để tăng cường tính bảo mật. Khi người dùng đăng nhập vào hệ thống, mã thông báo thiết bị sẽ tương tác với máy chủ xác thực để kiểm tra tính hợp lệ của mã xác thực và đảm bảo rằng người dùng được phép truy cập vào hệ thống.

Tóm lại, mã thông báo phần cứng hoạt động bằng cách tạo mã xác thực một lần dựa trên các thuật toán bảo mật được tích hợp trong thiết bị và yêu cầu người dùng nhập mật khẩu để mở khóa thiết bị. Mã thông báo thiết bị cũng có thể tích hợp các tính năng bảo mật khác như mã hóa dữ liệu hoặc chứng thực phần mềm để đảm bảo tính an toàn và bảo mật.

1.4 Vai trò và ứng dụng của Hardware Token

1.4.1 Vai trò của hardware token

Hardware token đóng vai trò quan trọng trong sự phát triển của công nghệ và an ninh thông tin. Chúng được sử dụng rộng rãi trong các hệ thống bảo mật để cung cấp tính xác thực cao và đảm bảo tính bảo mật của thông tin.

Các thiết bị token giúp ngăn chặn việc truy cập trái phép vào hệ thống thông tin, bảo vệ thông tin nhạy cảm, chữ ký số, chứng thực, mã hóa và giải mã dữ liệu. Nó cũng giúp hạn chế sự lây lan của virus và phần mềm độc hại trên mạng.

Hardware token được sử dụng rộng rãi trong các lĩnh vực như tài chính, y tế, ngân hàng, chính phủ và các tổ chức lớn khác. Chúng giúp đảm bảo tính toàn vẹn của hệ thống thông tin và bảo vệ các thông tin quan trọng khỏi sự tấn công của hacker.

Hardware token cũng có vai trò quan trọng trong việc đáp ứng các tiêu chuẩn bảo mật quốc tế như PCI-DSS (Payment Card Industry Data Security Standard) hoặc HIPAA (Health Insurance Portability and Accountability Act). Các tiêu chuẩn này yêu cầu các tổ chức và doanh nghiệp phải cung cấp các phương tiện xác thực mạnh mẽ cho người dùng để đảm bảo tính bảo mật của thông tin.

Trong tương lai, hardware token cũng được kỳ vọng sẽ tiếp tục phát triển và cải tiến với các tính năng mới để đáp ứng nhu cầu ngày càng cao của người dùng.

1.4.2 Ứng dụng của hardware token

Hardware token có rất nhiều ứng dụng vào cuộc sống của chúng ta dưới đây là một số ứng dụng phổ biến thường thấy của hardware token:

- Xác thực truy cập mạng: Hardware token được sử dụng để xác thực người dùng khi truy cập vào mạng của tổ chức hoặc doanh nghiệp.
- Xác thực truy cập ứng dụng: Hardware token được sử dụng để xác thực người dùng khi truy cập vào các ứng dụng, dịch vụ trực tuyến như ngân hàng trực tuyến, thẻ tín dụng trực tuyến, email, v.v.
- Tạo chữ ký số: Hardware token có thể được sử dụng để tạo chữ ký số, cho phép người dùng ký và xác nhận tính toàn vẹn của các tài liệu hoặc giao dịch.
- Xác thực thẻ thanh toán: Hardware token có thể được sử dụng để xác thực các giao dịch thẻ thanh toán, bảo vệ thông tin thẻ của người dùng và ngăn chặn các hoạt động gian lận.
- Quản lý danh mục tài khoản: Hardware token có thể được sử dụng để lưu trữ danh mục tài khoản và thông tin đăng nhập, giúp người dùng truy cập nhanh chóng vào các tài khoản của mình mà không cần phải nhập lại thông tin đăng nhập.
- Xác thực thời gian thực: Một số loại hardware token có thể được sử dụng để cung cấp xác thực thời gian thực, đảm bảo tính toàn vẹn của thông tin và giao dịch.

1.5 Tính năng của Hardware token

Hardware token có một số tính năng:

1.5.1 Tính bảo mật

Hardware token được thiết kế để cung cấp tính bảo mật cao nhất cho thông tin và tài khoản của người dùng. Tính bảo mật của hardware token được coi là một trong những phương tiện bảo mật tốt nhất hiện nay. Dưới đây là một số tính năng bảo mật quan trọng của hardware token:

- Mã hóa đầu vào: Mã hóa đầu vào là một phương thức bảo mật quan trọng được sử dụng để bảo vệ thông tin người dùng. Mã hóa đầu vào có thể bao gồm mật khẩu hoặc các thông tin xác thực khác.

- Mã hóa dữ liệu: Hardware token được thiết kế để mã hóa và giải mã dữ liệu một cách an toàn và hiệu quả. Việc này giúp bảo vệ thông tin người dùng khỏi các cuộc tấn công từ bên ngoài.

- Chống lại tấn công phần mềm độc hại: Hardware token không phụ thuộc vào phần mềm trên máy tính, điều này làm cho chúng ít bị tấn công bởi phần mềm độc hại hoặc virus.

- Bảo vệ thông tin trên token: Tất cả thông tin trên hardware token đều được mã hóa, bảo vệ khỏi các cuộc tấn công từ bên ngoài.

- Khả năng xác thực cao: Hardware token được thiết kế để cung cấp mức độ xác thực cao cho người dùng, ngăn chặn việc sử dụng thông tin xác thực giả mạo hoặc lừa đảo.

- Khả năng phát hiện việc tấn công: Một số loại hardware token có khả năng phát hiện các cuộc tấn công và ngăn chặn việc truy cập trái phép vào hệ thống.

Tóm lại, tính bảo mật của hardware token là rất cao và chúng được sử dụng rộng rãi trong các ứng dụng yêu cầu mức độ bảo mật cao, như xác thực truy cập, tạo chữ ký số và quản lý danh mục tài khoản.

1.5.2 Xác thực người dùng

Hardware token sử dụng một số phương thức để xác thực người dùng, bao gồm sử dụng mã PIN hoặc mật khẩu. Tính xác thực người dùng của hardware token là một trong những tính năng quan trọng của nó. Hardware token được sử dụng để xác thực người dùng và cung cấp quyền truy cập vào các tài khoản, ứng dụng hoặc hệ thống.

Để xác thực người dùng, hardware token thường được kết hợp với một mã PIN (Personal Identification Number). Khi người dùng muốn truy cập vào tài khoản hoặc hệ

thông, họ sẽ cắm hardware token vào máy tính và nhập mã PIN của mình. Sau khi mã PIN được xác thực, token sẽ cung cấp cho người dùng một mã xác thực tạm thời (One-Time Password - OTP) hoặc chữ ký số để sử dụng để đăng nhập hoặc thực hiện các giao dịch an toàn khác.

Tính năng xác thực người dùng của hardware token là rất quan trọng trong việc bảo vệ thông tin cá nhân và các tài khoản quan trọng. Nó giúp ngăn chặn việc truy cập trái phép và đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào các tài khoản và thông tin quan trọng.

1.5.3 Chống phishing

Hardware token có thể giúp ngăn chặn các cuộc tấn công phishing bằng cách yêu cầu người dùng phải nhập mã PIN hoặc mật khẩu trực tiếp trên token, thay vì trên máy tính. Tính chống phishing của hardware token là một tính năng quan trọng giúp ngăn chặn các cuộc tấn công phishing.

Phishing là kỹ thuật tấn công mạng giả mạo trang web, email hoặc thông tin để lừa đảo người dùng để cung cấp thông tin cá nhân, thông tin đăng nhập hoặc thực hiện các giao dịch tài chính không an toàn. Tuy nhiên, với việc sử dụng hardware token, người dùng sẽ không còn phải lo lắng về việc các tài khoản và thông tin cá nhân của mình bị đánh cắp.

Vì hardware token chứa các thông tin đăng nhập và chứng chỉ số, người dùng không cần phải nhập thông tin này trực tiếp vào trình duyệt hoặc email, giúp ngăn chặn các phần mềm đánh cắp thông tin. Thay vào đó, người dùng chỉ cần cắm hardware token vào máy tính và nhập mã PIN để xác thực, sau đó token sẽ cung cấp cho người dùng một mã xác thực tạm thời (OTP) hoặc chữ ký số để sử dụng.

Với tính năng chống phishing của hardware token, người dùng có thể yên tâm sử dụng các tài khoản và thực hiện các giao dịch trực tuyến một cách an toàn và bảo mật hơn.

1.5.4 Tính di động

Hardware token nhỏ gọn và dễ dàng mang theo, cho phép người dùng truy cập vào các tài khoản của họ từ bất kỳ máy tính nào mà không cần cài đặt phần mềm trên máy

tính đó. Tính di động của hardware token là một tính năng quan trọng giúp người dùng sử dụng token một cách thuận tiện và linh hoạt hơn.

Với tính năng di động, người dùng có thể mang theo hardware token của mình bất cứ nơi đâu và sử dụng để truy cập vào các tài khoản hoặc hệ thống từ bất kỳ máy tính nào mà họ có thể truy cập được. Ngoài ra, nhiều loại hardware token như USB token hay smart card cũng được thiết kế nhỏ gọn, dễ dàng mang theo trong túi xách hoặc ví tiền.

Bên cạnh đó, tính di động của hardware token còn giúp người dùng có thể sử dụng token của mình trên các thiết bị di động như điện thoại thông minh hoặc máy tính bảng. Điều này giúp người dùng có thể truy cập vào các tài khoản của mình bất cứ lúc nào và bất cứ đâu mà không cần phải mang theo máy tính hay thiết bị đặc biệt nào khác.

Tính di động của hardware token cũng giúp ngăn chặn việc truy cập trái phép vào các tài khoản và hệ thống. Khi sử dụng token, người dùng có thể đảm bảo rằng chỉ có họ mới có thể truy cập vào tài khoản và thông tin của mình, ngay cả khi họ sử dụng các thiết bị hoặc mạng không an toàn.

1.5.5 Khả năng tạo chữ ký số

Một số loại hardware token có khả năng tạo ra chữ ký số, cho phép người dùng xác thực tính toàn vẹn của tài liệu hoặc giao dịch. Khả năng tạo chữ ký số là một trong những tính năng quan trọng của hardware token. Với khả năng này, người dùng có thể sử dụng hardware token để tạo và xác thực các chữ ký số cho các tài liệu, hợp đồng, giao dịch trực tuyến và các hoạt động khác.

Tùy thuộc vào loại hardware token, phương thức tạo chữ ký số có thể khác nhau. Ví dụ, với USB token, người dùng có thể sử dụng một ứng dụng tạo chữ ký số được cài đặt trên máy tính để tạo và quản lý các chữ ký số. Trong khi đó, với smart card, người dùng có thể sử dụng một ứng dụng tạo chữ ký số trên thẻ để tạo và quản lý các chữ ký số.

Trong quá trình tạo chữ ký số, hardware token sử dụng các thuật toán mật mã để tạo ra một chuỗi mã hóa duy nhất được gọi là chữ ký số. Chữ ký số này có thể được sử dụng để xác thực tính xác thực của người ký và tính toàn vẹn của tài liệu.

Từ đó, khả năng tạo chữ ký số của hardware token giúp tăng tính bảo mật và độ tin cậy trong các hoạt động trực tuyến và giao dịch điện tử.

1.5.6 Khả năng lưu trữ thông tin

Hardware token có khả năng lưu trữ thông tin như tên đăng nhập và mật khẩu, giúp người dùng truy cập nhanh chóng vào các tài khoản của mình. Các loại thông tin được lưu trữ trên hardware token bao gồm các chứng chỉ số, khóa riêng tư, mã PIN, các bản cập nhật phần mềm và các tệp tin khác liên quan đến việc xác thực và bảo mật thông tin.

Thông tin được lưu trữ trên hardware token được mã hóa bằng các thuật toán mật mã mạnh để đảm bảo tính bảo mật và an toàn. Người dùng cần nhập một mã PIN hoặc mật khẩu để truy cập vào các thông tin được lưu trữ trên hardware token.

Khả năng lưu trữ thông tin của hardware token giúp người dùng dễ dàng quản lý và truy cập các thông tin xác thực và bảo mật của họ một cách an toàn và tiện lợi. Đồng thời, nó cũng giúp ngăn chặn các cuộc tấn công truy cập trái phép vào các thông tin quan trọng của người dùng.

1.5.7 Khả năng phát hiện nghi ngờ

Một số loại hardware token có khả năng phát hiện các hoạt động bất thường hoặc nghi ngờ và cảnh báo cho người dùng. Khả năng phát hiện nghi ngờ của hardware token được thực hiện thông qua việc sử dụng các thuật toán phức tạp để giám sát và phân tích hành vi truy cập vào hệ thống của người dùng. Nếu hệ thống phát hiện ra các hoạt động truy cập không hợp lệ hoặc có nghi ngờ, nó sẽ tạm ngưng các hoạt động đó và yêu cầu người dùng xác nhận thông tin hoặc thực hiện các biện pháp bảo mật bổ sung để đảm bảo an toàn cho hệ thống.

Các hoạt động không hợp lệ có thể bao gồm đăng nhập không thành công, đăng nhập từ một địa điểm lạ hoặc sử dụng một thiết bị mới. Nếu các hoạt động này được phát hiện, hệ thống sẽ yêu cầu người dùng xác nhận thông tin hoặc sử dụng các phương pháp xác thực bổ sung như mã OTP (One-Time Password) để đảm bảo tính bảo mật của hệ thống.

Khả năng phát hiện nghi ngờ của hardware token là một tính năng quan trọng giúp đảm bảo tính bảo mật của hệ thống và tránh các cuộc tấn công truy cập trái phép.

Chương 2. USB Token, Smart Card và HSM

Chữ ký số được coi là giải pháp công nghệ thông minh giúp việc trao đổi thông tin trở nên dễ dàng, nhanh chóng và bảo mật hơn trong thời đại công nghệ số hiện nay. Sự phát triển của thị trường chữ ký số mở ra nhiều loại hình chữ ký số với tính năng và cách sử dụng khác nhau.

Ra đời đầu tiên trên thị trường, chữ ký số USB Token là loại chữ ký số truyền thống và hiện nay vẫn đang được phần đông các doanh nghiệp, cá nhân sử dụng để ký số chứng từ, tài liệu. Đặc trưng của chữ ký số USB Token là sử dụng một thiết bị phần cứng có hình dạng USB để lưu trữ khóa bí mật giúp tạo lập chữ ký số.



Hình 2.1: Chữ ký số

Quá trình ký số của chữ ký số USB Token yêu cầu sự kết nối của USB Token và máy tính nên không tránh khỏi một số bất cập như không thể ký số từ xa khi không có Token hay việc ký số bị giới hạn trên máy tính. Ngoài ra, chữ ký số USB Token cũng không đáp ứng được nhu cầu sử dụng nhiều người trên 1 Token. Tuy nhiên, ưu điểm

vượt trội của chữ ký số USB Token là dễ sử dụng và có độ bảo mật cao, khó có thể làm giả.

Chữ ký số Smartcard là loại chữ ký số được tích hợp trên sim do một số nhà mạng nghiên cứu và phát triển. Với chữ ký số Smartcard, người dùng có thể ký số nhanh chóng và linh động trên điện thoại di động. Ngoài ra còn một số loại Smart Card khác được ứng dụng rộng rãi trong các lĩnh vực xác thực, thanh toán,...

Chữ ký số HSM (Hardware security module) là một thiết bị phần cứng dùng để bảo vệ và quản lý các cặp khóa điện tử, giúp tăng tốc độ xác thực và mã hóa dữ liệu. Chữ ký số HSM được đánh giá có nhiều tính năng cao cấp hơn so với USB Token và Smartcard để đáp ứng nhu cầu hoạt động của các hệ thống lớn, có yêu cầu cao về hiệu năng và tính bảo mật.

Nhược điểm của chữ ký số HSM là giá thành khá cao và chỉ phù hợp với những doanh nghiệp lớn, có hệ thống quy mô lớn và cơ sở hạ tầng tốt. Ngoài ra, chữ ký số HSM cho phép nhiều người cùng ký số tại các điểm khác nhau nhưng thường giới hạn dưới 20 điểm truy cập ký số.

2.1 USB Token

2.1.1 Tổng quan

USB token là một thiết bị lưu trữ dữ liệu và cung cấp chức năng bảo mật và xác thực. Nó được sử dụng để bảo vệ và quản lý thông tin nhạy cảm, cung cấp tính năng xác thực hai yếu tố và bảo mật dữ liệu.



Hình 2.2: USB Token

USB token thường có hình dạng giống với USB flash drive, với một cổng USB để kết nối với máy tính hoặc các thiết bị hỗ trợ. USB token có bộ nhớ để lưu trữ các thông tin nhạy cảm như chứng chỉ số, khóa mã hóa, mật khẩu hoặc mã PIN. Thiết bị thường tích hợp một vi xử lý nhỏ để thực hiện các chức năng bảo mật và xác thực. USB token thường hỗ trợ các giao thức và tiêu chuẩn bảo mật như PKCS#11, RSA, AES, DES, ECC, và các giao thức xác thực như OTP (One-Time Password). USB token được sử dụng trong nhiều lĩnh vực như bảo mật thông tin cá nhân, xác thực người dùng, quản lý chứng chỉ số, mã hóa và giải mã dữ liệu, và bảo vệ quyền riêng tư. USB token cung cấp tính năng bảo mật như xác thực hai yếu tố, bảo vệ khóa riêng tư và thông tin nhạy cảm, và ngăn chặn truy cập trái phép vào dữ liệu. Các công cụ và phần mềm quản lý được cung cấp để quản lý và cấu hình USB token, bao gồm tạo và quản lý chứng chỉ số, xác thực người dùng và quản lý quyền truy cập.

USB token là một công cụ hữu ích để bảo mật thông tin và xác thực trong các hệ thống và ứng dụng khác nhau.

2.1.2 Tính pháp lý

Tính pháp lý của USB token phụ thuộc vào quốc gia và các quy định cụ thể trong lĩnh vực sử dụng:

1. Luật về bảo mật thông tin: Trong nhiều quốc gia, việc sử dụng USB token để bảo vệ thông tin nhạy cảm được quy định trong các luật về bảo mật thông tin. Các quy định này có thể yêu cầu việc sử dụng USB token để bảo vệ và xác thực truy cập vào dữ liệu nhạy cảm.

2. Chứng thực và chữ ký số: USB token thường được sử dụng để lưu trữ chứng chỉ số và khóa cá nhân để xác thực và chữ ký số. Việc sử dụng USB token cho mục đích này có thể tuân theo các quy định về chứng thực và chữ ký số trong quốc gia đó.

3. Quyền riêng tư và bảo vệ dữ liệu: USB token có thể được sử dụng để bảo vệ quyền riêng tư và bảo vệ dữ liệu cá nhân. Trong các quốc gia có quyền riêng tư và bảo vệ dữ liệu mạnh mẽ, việc sử dụng USB token để đảm bảo tính riêng tư và bảo vệ dữ liệu có thể tuân theo các quy định và quy tắc tương ứng.

4. Quy định về tiêu chuẩn và tuân thủ: USB token có thể phải tuân thủ các tiêu chuẩn và quy định cụ thể, chẳng hạn như các tiêu chuẩn về bảo mật thông tin, mã hóa

dữ liệu và giao tiếp. Các tiêu chuẩn này có thể được đề ra bởi các tổ chức quốc tế hoặc các cơ quan quốc gia có thẩm quyền.

5. Quy định ngành công nghiệp: Trong một số lĩnh vực như ngân hàng, y tế và chính phủ, việc sử dụng USB token có thể được quy định bởi các quy định ngành công nghiệp. Các quy định này đảm bảo tính an toàn và tuân thủ các tiêu chuẩn bảo mật cụ thể.

2.1.3 Chức năng

Xác thực người dùng: USB token được sử dụng để xác thực người dùng khi truy cập vào hệ thống hoặc ứng dụng. Người dùng cần cắm USB token và cung cấp thông tin xác thực bổ sung như mật khẩu PIN hoặc dấu vân tay để xác thực thành công.

Lưu trữ chứng chỉ số và khóa cá nhân: USB token thường có khả năng lưu trữ chứng chỉ số (như chứng chỉ số SSL, chứng chỉ số chữ ký số) và khóa cá nhân. Điều này cho phép người dùng thực hiện các hoạt động chữ ký số và xác thực bằng cách sử dụng khóa cá nhân lưu trữ trên USB token.

Bảo vệ dữ liệu: USB token có khả năng mã hóa và giải mã dữ liệu để bảo vệ thông tin nhạy cảm. Khi dữ liệu được gửi đi hoặc lưu trữ trên hệ thống, nó được mã hóa bằng khóa cá nhân lưu trữ trong USB token. Chỉ có USB token tương ứng mới có thể giải mã dữ liệu.

Giao tiếp an toàn qua USB: USB token giao tiếp với máy tính thông qua cổng USB. Thông tin truyền qua giao diện USB thường được mã hóa và bảo vệ bởi các phương thức bảo mật như TLS hoặc SSL. Điều này đảm bảo tính an toàn trong quá trình truyền thông và truy cập dữ liệu.

Đa dạng hóa ứng dụng: USB token có thể được sử dụng trong nhiều lĩnh vực và ứng dụng khác nhau. Chúng có thể được sử dụng trong ngân hàng trực tuyến, chữ ký số, truy cập mạng, mã hóa dữ liệu, điều khiển truy cập vật lý và nhiều ứng dụng khác yêu cầu tính bảo mật cao và xác thực người dùng.

Quản lý quyền truy cập: USB token có thể được sử dụng để quản lý quyền truy cập vào hệ thống hoặc dữ liệu. Chúng cho phép quản lý tập trung cấp phép và thu hồi quyền truy cập cho người dùng, đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào thông tin nhạy cảm.

USB token được coi là một phương tiện bảo mật và có độ tin cậy cao trong việc bảo vệ thông tin và đảm bảo tính an toàn của hệ thống.

Bảo mật vật lý: USB token thường được thiết kế với vỏ bọc vật lý chắc chắn và khó bị phá hủy để ngăn chặn việc truy cập trái phép hoặc lấy cắp thông tin. Điều này đảm bảo rằng chỉ người dùng được ủy quyền mới có thể truy cập vào USB token.

Mật khẩu và thông tin xác thực: USB token thường yêu cầu người dùng cung cấp mật khẩu PIN hoặc dấu vân tay để xác thực và mở khóa. Điều này đảm bảo rằng người dùng cần phải có thông tin xác thực bổ sung để sử dụng USB token, ngăn chặn truy cập trái phép từ những người không có quyền.

Mã hóa dữ liệu: USB token có khả năng mã hóa dữ liệu để bảo vệ thông tin nhạy cảm. Dữ liệu được mã hóa bằng khóa cá nhân lưu trữ trong USB token, và chỉ USB token tương ứng mới có thể giải mã dữ liệu. Điều này đảm bảo rằng dữ liệu không thể bị đánh cắp hoặc truy cập trái phép khi nằm trong USB token.

Độ tin cậy và bền vững: USB token được thiết kế để có độ tin cậy cao và khả năng chống lại các cuộc tấn công phổ biến như lừa đảo, trộm cắp thông tin và tấn công từ chối dịch vụ (DoS). Ngoài ra, chúng thường có tính năng tự hủy nếu bị tấn công để ngăn chặn việc truy cập trái phép.

Quản lý và kiểm soát: USB token thường được quản lý bởi một hệ thống quản lý tập trung. Hệ thống này cho phép quản lý cấu hình, cung cấp quyền truy cập và thu hồi USB token khi không cần thiết. Điều này giúp đảm bảo rằng chỉ những người được ủy quyền mới có thể sử dụng USB token và truy cập vào hệ thống hoặc dữ liệu.

2.1.4 Phân loại

2.1.4.1 Phân loại theo mục đích sử dụng

USB token đang được sử dụng rộng rãi trong cuộc sống đặc biệt là được sử dụng trong các doanh nghiệp lên chúng có thể được phân loại theo các mục đích sử dụng khác nhau. Dựa vào các nhu cầu sử dụng khác nhau mà chúng được chia thành các usb token chính như:

USB token chứng thực (Authentication USB tokens): Loại USB token này được sử dụng để xác thực người dùng và cung cấp quyền truy cập vào hệ thống hoặc ứng dụng. Chúng thường yêu cầu người dùng cung cấp thông tin xác thực bổ sung như mật khẩu PIN hoặc dấu vân tay.

USB token chữ ký số (Digital Signature USB tokens): Loại USB token này được sử dụng để lưu trữ chứng chỉ số và khóa cá nhân để thực hiện chữ ký số và các hoạt động liên quan đến chứng thực. Chúng cho phép người dùng thực hiện chữ ký số và xác thực bằng cách sử dụng khóa cá nhân lưu trữ trên USB token.

USB token mã hóa (Encryption USB tokens): Loại USB token này cung cấp khả năng mã hóa và giải mã dữ liệu để bảo vệ thông tin nhạy cảm. Dữ liệu được mã hóa bằng khóa cá nhân lưu trữ trong USB token và chỉ có USB token tương ứng mới có thể giải mã dữ liệu.

USB token quản lý quyền truy cập (Access Management USB tokens): USB token này được sử dụng để quản lý quyền truy cập vào hệ thống hoặc dữ liệu. Chúng cho phép quản lý tập trung cấp phép và thu hồi quyền truy cập cho người dùng, đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào thông tin nhạy cảm.

USB token OTP (One-Time Password): Loại USB token này tạo ra các mã xác thực một lần (OTP) để xác thực người dùng. Mỗi mã OTP chỉ có thể sử dụng một lần duy nhất và có thời hạn hợp lệ giới hạn. Chúng thường được sử dụng để cung cấp lớp bảo mật bổ sung cho việc xác thực người dùng.

USB token mã hóa phần cứng (Hardware Encryption USB tokens): Loại USB token này tích hợp phần cứng mã hóa và khả năng lưu trữ dữ liệu an toàn. Chúng cung cấp mức bảo mật cao hơn bằng cách sử dụng chip mã hóa phần cứng riêng để mã hóa và giải mã dữ liệu.

2.1.4.2 Phân loại theo cấu trúc và chức năng

USB token tích hợp: Loại USB token này tích hợp các thành phần bảo mật và chức năng vào một thiết bị duy nhất. Thông thường, nó bao gồm vi xử lý, bộ nhớ, các khóa mã hóa và các thành phần quản lý bảo mật khác. USB token tích hợp có kích thước nhỏ gọn và dễ dàng mang theo.

USB token phi tích hợp: Loại USB token này được tách rời thành hai thành phần riêng biệt: một phần cứng USB (USB dongle) và một phần mềm điều khiển. USB dongle được cắm vào cổng USB của máy tính và kết nối với phần mềm điều khiển để thực hiện chức năng bảo mật. Phần mềm điều khiển thường cung cấp giao diện và tích hợp với ứng dụng hoặc hệ thống để quản lý và xác thực.

USB token dạng thẻ (Smart Card USB tokens): Loại USB token này tích hợp công nghệ thẻ thông minh (smart card) và giao tiếp thông qua giao diện USB. Thẻ thông minh chứa chip bảo mật và các ứng dụng liên quan, trong khi giao tiếp USB cung cấp khả năng kết nối và truyền dữ liệu giữa thẻ thông minh và máy tính. USB token dạng USB dongle: Loại USB token này có hình dạng giống một chiếc USB dongle hoặc USB flash drive. Chúng có kích thước nhỏ gọn và dễ dàng cắm vào cổng USB trên máy tính hoặc thiết bị. USB token dạng dongle thường tích hợp các tính năng bảo mật như mã hóa dữ liệu và xác thực người dùng.

USB token tích hợp màn hình (USB tokens with integrated display): Một số USB token được thiết kế với màn hình tích hợp để hiển thị các thông tin liên quan đến xác thực và giao tiếp với người dùng. Màn hình cho phép người dùng xem và xác nhận các thông tin như mã OTP hoặc dấu vân tay trên USB token trực tiếp.

USB token có tính năng mã hóa phần cứng (Hardware Encryption USB tokens): Loại USB token này tích hợp phần cứng mã hóa để bảo vệ dữ liệu. Chúng sử dụng chip mã hóa phần cứng riêng để thực hiện quá trình mã hóa và giải mã dữ liệu. Điều này cung cấp mức bảo mật cao hơn so với việc sử dụng phần mềm mã hóa trên máy tính.

USB token có tính năng chống sao chép (Copy Protection USB tokens): Loại USB token này được thiết kế để bảo vệ các ứng dụng, tệp tin hoặc nội dung trên USB token khỏi việc sao chép trái phép. Chúng sử dụng các công nghệ chống sao chép để đảm bảo rằng thông tin chỉ có thể truy cập và sử dụng trên USB token gốc.

2.1.5 Nguyên lý hoạt động

USB token hoạt động bằng cách kết hợp các thành phần phần cứng và phần mềm để cung cấp các tính năng bảo mật và xác thực:

Giao tiếp với máy tính: USB token kết nối với máy tính thông qua cổng USB. Khi được cắm vào, máy tính nhận diện USB token và thiết lập kết nối để truyền và nhận dữ liệu.

Xác thực người dùng: Khi sử dụng USB token, người dùng thường cần cung cấp thông tin xác thực như mật khẩu PIN hoặc dấu vân tay. Thông tin này được nhập vào máy tính thông qua giao diện người dùng hoặc phần mềm đặc biệt.

Mã hóa và giải mã dữ liệu: USB token có khả năng lưu trữ và xử lý khóa mã hóa. Khi người dùng muốn mã hóa dữ liệu, USB token sẽ sử dụng khóa mã hóa lưu trữ trong

nó để mã hóa thông tin trước khi truyền đi. Tương tự, khi nhận dữ liệu được mã hóa, USB token sẽ sử dụng khóa mã hóa để giải mã và hiển thị thông tin gốc.

Lưu trữ chứng chỉ và khóa cá nhân: Một trong các tính năng phổ biến của USB token là khả năng lưu trữ chứng chỉ số và khóa cá nhân. Chứng chỉ số được sử dụng để xác thực và chứng thực, trong khi khóa cá nhân được sử dụng để thực hiện các hoạt động như chữ ký số và mã hóa dữ liệu.

Bảo mật vật lý và phần mềm: USB token được thiết kế để đảm bảo tính an toàn và bảo mật. Vật lý, chúng có thể có vỏ bọc chắc chắn và khó bị phá hủy. Phần mềm, chúng thường đi kèm với các chương trình quản lý và ứng dụng để cung cấp các tính năng bảo mật và quản lý quyền truy cập.

Giao thức và tiêu chuẩn: USB token thường tuân thủ các giao thức và tiêu chuẩn bảo mật để đảm bảo tính tương thích và bảo mật. Ví dụ, các USB token chữ ký số thường tuân thủ tiêu chuẩn PKCS#11 và các USB token chứng thực thường sử dụng giao thức OTP hoặc FIDO.

2.2 Smart Card

2.2.1 Tổng quan

Thẻ thông minh, thẻ gắn chip, hay thẻ tích hợp vi mạch (tiếng Anh: integrated circuit card, viết tắt ICC) là loại thẻ bỏ túi thường có kích thước của thẻ tín dụng, bên trong chứa một mạch tích hợp có khả năng lưu trữ và xử lý thông tin. Nó có thể đóng vai trò như thẻ căn cước, thực hiện việc xác thực thông tin, lưu trữ dữ liệu hay dùng trong các ứng dụng thẻ. Có hai loại thẻ thông minh chính. Các thẻ nhớ (memory card) chỉ chứa các thành phần bộ nhớ bất biến (non-volatile memory), và có thể có một số chức năng bảo mật cụ thể. Thẻ vi xử lý chứa bộ nhớ khả biến (volatile memory) và các thành phần vi xử lý. Thẻ làm bằng nhựa, thường là PVC, đôi khi ABS. Thẻ có thể chứa một ảnh 3 chiều (hologram) để tránh các vụ lừa đảo.

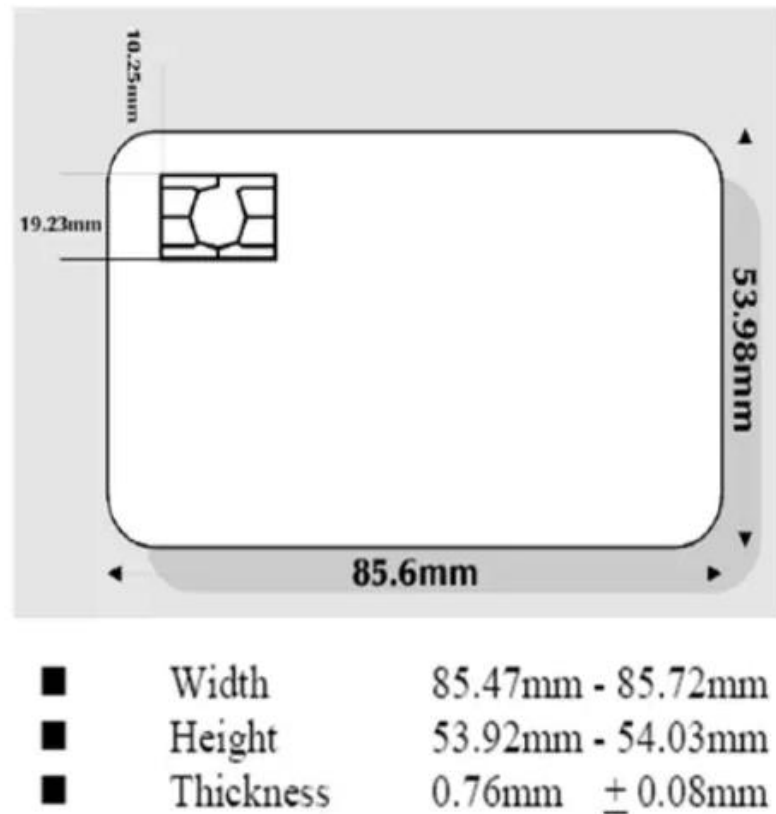
Thẻ thông minh còn được gọi nôm na là thẻ chip vì nó được tích hợp 1 con chip trên thẻ cho phép đáp ứng các nhu cầu về lưu trữ dữ liệu, bảo vệ dữ liệu, cũng như 1 số các nhu cầu về tính toán phức tạp (nhờ vào CPU trên chip). Thẻ chip được bảo mật tốt hơn thẻ từ. Vì ở thẻ từ, thông tin trên băng từ (magnetic stripe) hoàn toàn có thể bị đọc 1 cách bất hợp pháp. Ngoài ra thẻ từ cũng không cho phép thực hiện các phép tính toán mã hóa (cryptographic operations); nên không hỗ trợ các giao thức về authentication

cũng như không bảo đảm confidentiality và integrity của thông tin trên đường truyền; và vì vậy kém bảo mật hơn.



Hình 2.3: Smart Card

Một số ví dụ về thẻ chip: như SIM card là gần gũi với Việt Nam nhất; ngoài ra bankcard, transport card, identity card, passport, mã vạch trên hàng tiêu dùng ở các nước phát triển cũng có gắn chip.



Hình 2.4: Mô hình Smart Card

Thông thường có kích thước cỡ một thẻ tín dụng. Chuẩn ID-1 của ISO/IEC 7810 quy định là $85,60 \times 53,98$ mm. Một kích thước khác cũng khá thông dụng là ID-000 tức cỡ 25×15 mm. Cả hai kích thước này đều có bề dày là 0,76 mm.

Định dạng	Kích thước	Ứng dụng
ID - 1	85.60 x 53.98 mm	Hầu hết thẻ ngân hàng và các thẻ ID
ID - 2	105 x 74 mm	Thẻ Pháp và thẻ ID khác; thẻ visa
ID - 3	125 x 88 mm	Thẻ ID chính phủ Hoa Kỳ
ID – 000	25 x 15 mm	Thẻ SIM

Hình 2.5: Kích thước tiêu chuẩn của Smart Card

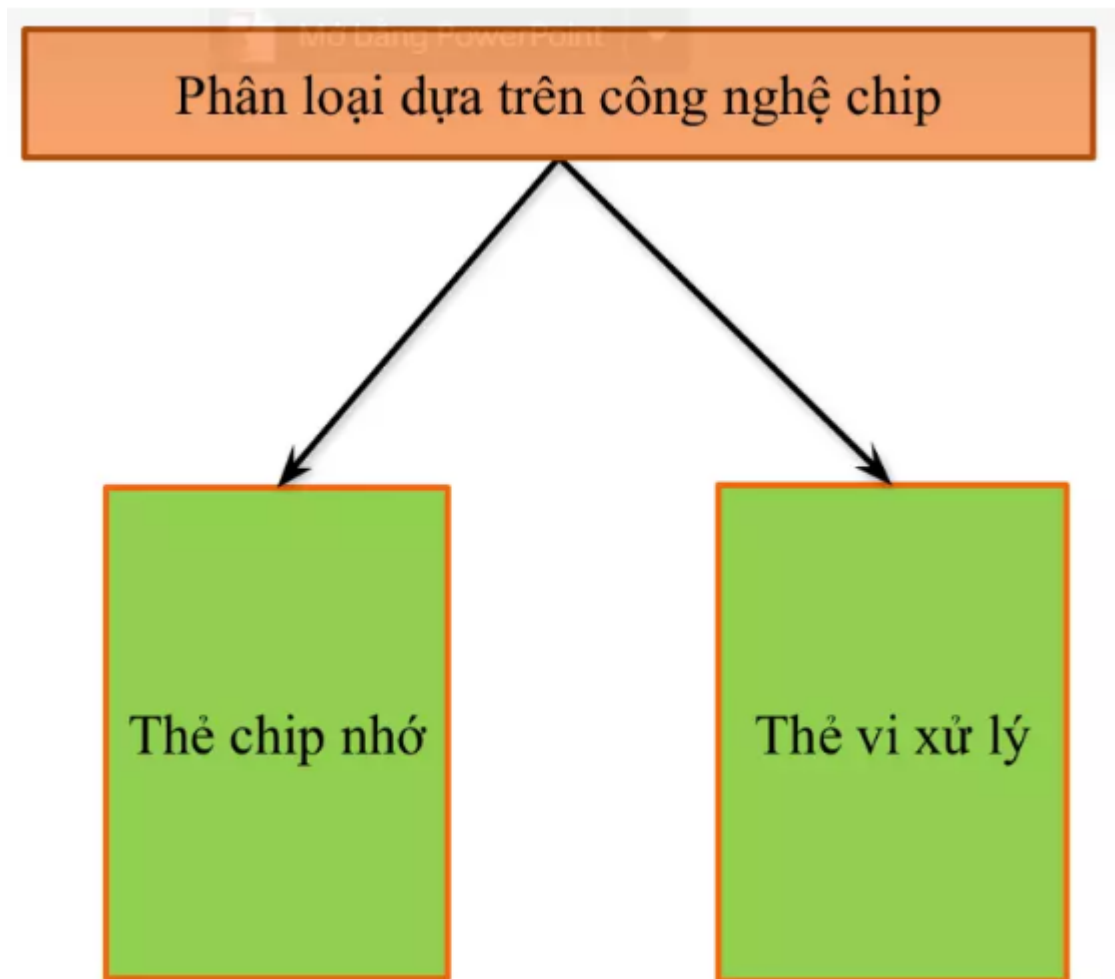
Smart Card chứa một hệ thống an ninh có các tính chất nhằm chống giả mạo (chẳng hạn, một vi xử lý chuyên dụng dùng cho bảo mật, một hệ thống an ninh quản lý file, các dấu hiệu có thể kiểm tra bằng mắt người) và có khả năng cung cấp các dịch vụ an ninh (chẳng hạn, bảo mật thông tin trong bộ nhớ). Tài nguyên trên thẻ được quản lý bởi một hệ thống quản trị trung tâm mà cho phép trao đổi thông tin và cấu hình cài đặt với thẻ

thông qua hệ thống an ninh nói trên. Dữ liệu trên thẻ được truyền đến hệ thống quản trị trung tâm nhờ vào các thiết bị đọc thẻ, chẳng hạn máy đọc vé, ATM,...

Ngoài khả năng lưu trữ dữ liệu, thẻ thông minh còn có khả năng xử lý dữ liệu tại chỗ, đây là điểm khác biệt so với thẻ từ.

2.2.2 Phân loại

2.2.2.1 Phân loại dựa trên công nghệ chip



Hình 2.6: Phân loại Smart Card dựa trên công nghệ chip

Thẻ chip nhớ (Memory Smart Cards)

Chứa từ 1 đến 4 Kb dữ liệu nhưng vì không có bộ xử lý nào được nhúng bên trong thẻ nên chúng hoàn toàn bị phụ thuộc vào đầu đọc thẻ. Thẻ chip nhớ giao tiếp với đầu đọc thẻ bằng một số giao thức đồng bộ, thường chỉ có một bộ nhớ chỉ đọc (EEPROM) có thể lập trình, xóa bằng tín hiệu điện. Thẻ chip nhớ không thể tái sử dụng.

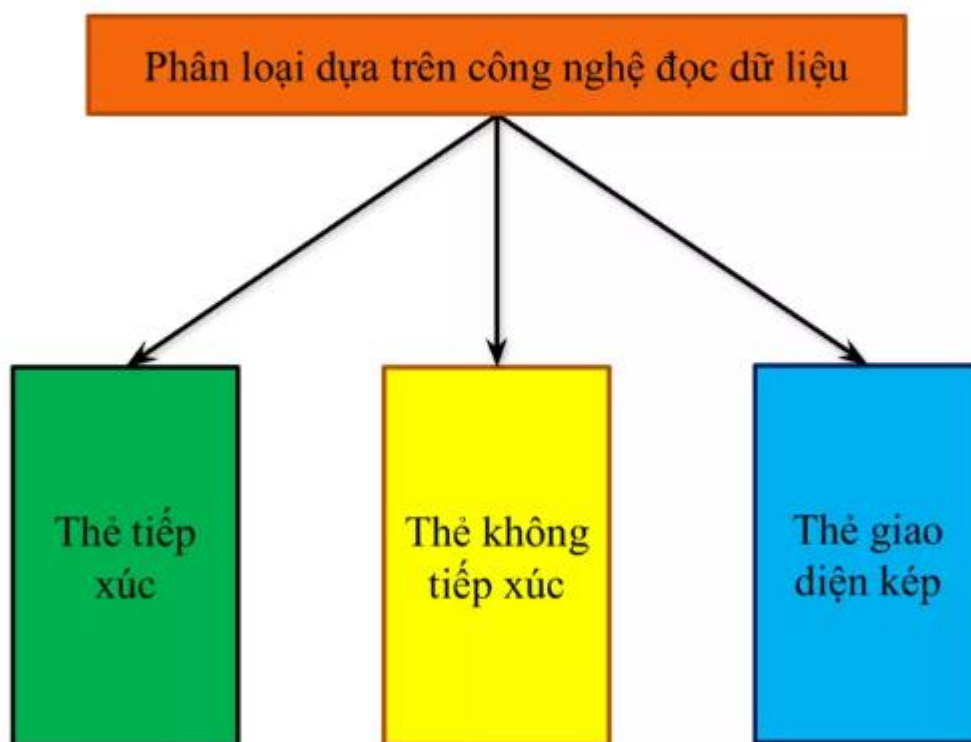
Memory Smart Card có thể lưu trữ, đọc và ghi dữ liệu vào chip. Dữ liệu có thể được ghi đè nhưng không thể sửa đổi vì thẻ không thể lập trình được. Các thẻ này được sử dụng hạn chế do dung lượng bộ nhớ thấp. Memory Smart Cards không bền và được sử dụng trong các sản phẩm dùng một lần. Các thẻ này có ba loại – thẻ nhớ thẳng, thẻ nhớ được bảo vệ và thẻ nhớ có giá trị lưu trữ.

Thẻ chip nhớ có ưu điểm là công nghệ đơn giản, dễ sản xuất, nhưng đó cũng chính là nhược điểm của nó, tính bảo mật không cao và rất dễ làm giả.

Thẻ chip vi xử lý (Microprocessor Smart Cards)

Thẻ chip vi xử lý là thẻ có chứa bộ xử lý bên trong nó, có khả năng bảo mật cao vượt trội và đa chức năng hơn nhiều. Các ứng dụng bên ngoài không thể trực tiếp truy cập vào dữ liệu trong thẻ. Thẻ chip vi xử lý kiểm soát, xử lý dữ liệu và truy cập bộ nhớ theo một tập hợp. Các điều kiện nhất định (mật khẩu, mã hóa,...) và theo sự chỉ dẫn của các thiết bị ngoại vi. Hiện tại nhiều thẻ chip vi xử lý có tính năng hỗ trợ mã hóa tích hợp. Các thẻ như vậy đặc biệt hữu ích cho các ứng dụng đòi hỏi cao về bảo mật dữ liệu.

2.2.2.2 Phân loại theo công nghệ đọc dữ liệu



Hình 2.7: Phân loại Smart Card dựa trên công nghệ đọc dữ liệu

Thẻ tiếp xúc (Contact Smart Card)

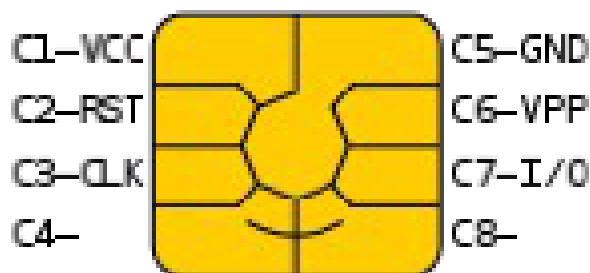
Loại thẻ thông minh có tiếp xúc có một diện tích tiếp xúc, bao gồm một số tiếp điểm mạ vàng, và có diện tích khoảng 1cm vuông. Khi được đưa vào máy đọc, con chip trên thẻ sẽ giao tiếp với các tiếp điểm điện tử và cho phép máy đọc thông tin từ chip và viết thông tin lên nó.

Các chuẩn ISO/IEC 7816 và ISO/IEC 7810 qui định:

- Hình dạng và kích thước vật lý
- Vị trí và hình dạng của các tiếp điểm điện tử
- Các đặc tính điện
- Các giao thức thông tin, bao gồm định dạng của các lệnh gửi đến thẻ và các đáp ứng từ thẻ.
- Độ tin cậy của thẻ
- Chức năng

- Thẻ không có pin; năng lượng làm việc sẽ được cấp từ máy đọc thẻ.

Mô tả các đặc tính điện:



Hình 2.8: Tiếp điểm điện của Contact Smart Card

C1 - Vcc: Điện áp cung cấp cho chip (thường là 5V, 3V hoặc 1.8V)

C2 - RST: Tín hiệu khởi động lại (reset) cho chip

C3 - CLK: Đồng hồ tín hiệu đầu vào (clock signal) để đồng bộ hóa giao tiếp giữa thẻ và máy đọc

C4 - AUX1: Tiếp điểm phụ 1, không được định nghĩa rõ ràng trong chuẩn ISO/IEC 7816 và có thể dùng cho các ứng dụng đặc biệt

C5 - GND: Mặt đất (ground) cho các mạch điện bên trong thẻ

C6 - Vpp: Điện áp lập trình (programming voltage), không còn được sử dụng trong các thẻ thông minh hiện đại.

C7 - I/O: Đường truyền dữ liệu vào/ra (input/output) giữa thẻ và máy đọc

C8 - AUX2: Tiếp điểm phụ 2, không được định nghĩa rõ ràng trong chuẩn ISO/IEC 7816 và có thể dùng cho các ứng dụng đặc biệt.

Lưu ý rằng không phải tất cả các tiếp điểm điện đều được sử dụng trong mọi trường hợp. Các tiếp điểm phổ biến nhất trong quá trình giao tiếp giữa thẻ và máy đọc bao gồm Vcc, RST, CLK, GND và I/O.

Máy đọc thẻ thông minh có tiếp xúc đóng vai trò trung gian liên kết giữa thẻ thông minh với một máy chủ, chẳng hạn, đó là một máy vi tính, một đầu cuối ở một điểm bán, hay một điện thoại di động.



Hình 2.9: Máy đọc thẻ tiếp xúc

Ví các chip trên thẻ thông minh dùng trong giao dịch tài chính cũng giống như các chip dùng trên SIM của điện thoại di động, chỉ khác cách lập trình và cách ghép vào miếng PVC có hình dạng khác nhau. Mặt khác, hiện nhu cầu dùng thẻ thông minh làm SIM là rất lớn cho nên các nhà sản xuất chip hiện đang tập trung vào việc sản xuất chip các chuẩn của điện thoại di động GSM/G3. Vì thế, mặc dầu EMV cho phép chip trên thẻ có thể gây tiêu hao một dòng khoảng 50mA từ máy đọc, hiện nay các chip đều chỉ tiêu hao chưa tới 6mA theo chuẩn của công nghiệp điện thoại. Điều này cho phép các máy đọc thẻ dùng trong giao dịch tài chính ngày càng nhỏ hơn và rẻ hơn, và tiến đến có thể trang bị cho mọi máy PC ở nhà một máy đọc thẻ cũng như phần mềm để bạn có thể mua sắm trên internet một cách dễ dàng và an ninh hơn.

Thẻ không tiếp xúc (Contactless Smart Card)

Một loại thẻ thứ hai là thẻ thông minh không tiếp xúc, đây là loại thẻ mà chip trên nó liên lạc với máy đọc thẻ thông qua công nghệ cảm ứng RFID (với tốc độ dữ liệu từ 36 đến 848 kbit/s). Những thẻ này chỉ cần đặt gần một anten để thực hiện quá trình truyền và nhận dữ liệu. Chúng thường được dùng trong các tình huống truyền nhận dữ liệu thật nhanh hay khi người chủ thẻ cần rảnh tay, chẳng hạn ở các hệ thống giao thông công cộng mà có thể sử dụng không cần rút thẻ ra khỏi ví.

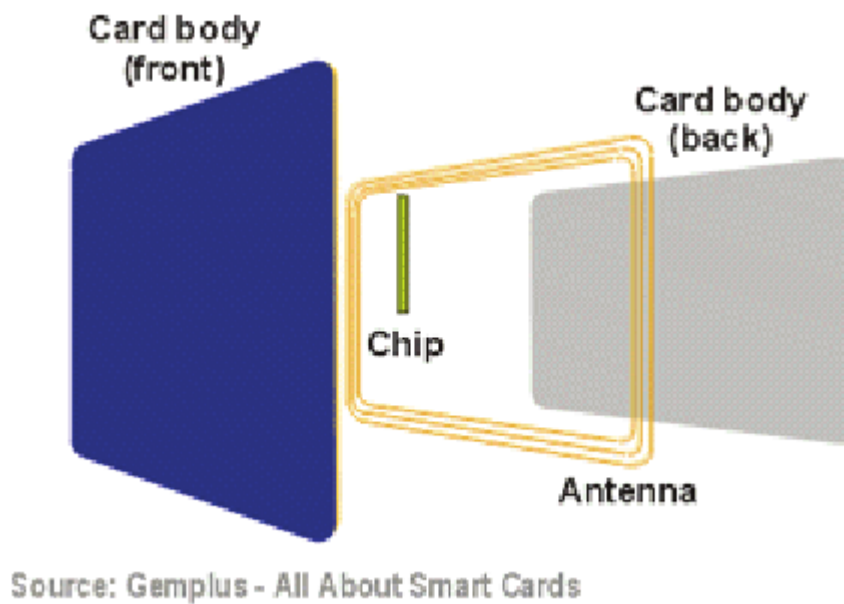
Chuẩn thông tin cho thị thông minh không tiếp xúc là ISO / IEC 14443, phát hành năm 2001, Nó qui định hai kiểu thẻ không tiếp xúc ("A" and "B"), cho phép liên lạc với khoảng cách lên đến 10 cm. Cũng có một vài chuẩn khác như ISO 14443 kiểu C, D, E và F mà đã bị loại bỏ bởi International Organization for Standardization. Một chuẩn khác của thẻ thông minh là ISO 15693, cho phép thông tin ở khoảng cách lên đến 50 cm.

Một số ví dụ của việc dùng thẻ thông minh không tiếp xúc là thẻ Octopus của Hong Kong, và thẻ Suica của Japan Rail; mà đã xuất hiện trước khi có chuẩn ISO / IEC 14443. Các hình sau cho thấy một số thẻ thông minh dùng trong giao thông công và ứng dụng thanh toán điện tử.

Một công nghệ không tiếp xúc có liên quan là RFID (radio frequency identification Xác nhận dựa vào tần số vô tuyến). Trong một số trường hợp cụ thể, nó có thể dùng trong những ứng dụng tương tự như thẻ thông minh không tiếp xúc, chẳng hạn dùng để thu phí cầu đường điện tử. Các thiết bị RFID thông thường không có chữa bệnh ghi được hay có bộ vi xử lý như thẻ thông minh.

Có loại thẻ gồm cả hai loại giao tiếp mà cho phép truy xuất bằng cách tiếp xúc và không tiếp xúc trên cùng một thẻ. Ví dụ như thẻ giao thông nhiều ứng dụng của Porto, BQT là Andante, mà dùng một chip cho cả tiếp xúc và không tiếp xúc,

Giống như thẻ thông minh có tiếp xúc, thẻ không tiếp xúc không có pin. Bên trong thẻ có một cuộn cảm mà có khả năng dờ một số tín hiệu vô tuyến, chỉnh lưu tín hiệu, và rồi dùng nó để cung cấp năng lượng cho chip trên thẻ.



Hình 2.10: Thẻ thông minh không tiếp xúc

2.2.3 Nguyên lý hoạt động

2.2.3.1 Lưu trữ Thông tin

Smart card lưu trữ thông tin trong chip tích hợp (IC) của nó. Các chip này thường được sản xuất bằng công nghệ bán dẫn, giống như những chip bạn tìm thấy trong máy tính và các thiết bị điện tử khác.

Dữ liệu được lưu trữ trên smart card có thể là các loại khác nhau, bao gồm dữ liệu cá nhân (như tên, địa chỉ, số định danh cá nhân), thông tin tài chính (như số tài khoản ngân hàng hoặc số thẻ tín dụng), hoặc thông tin liên quan đến quyền truy cập (như mã PIN hoặc chữ ký số).

Dung lượng lưu trữ của smart card phụ thuộc vào công nghệ và kích thước của chip IC. Một số smart card có khả năng lưu trữ chỉ vài kilobyte dữ liệu, trong khi những thẻ khác có thể lưu trữ nhiều megabyte.

Dữ liệu được lưu trữ trên smart card thường được bảo mật bằng cách sử dụng các thuật toán mã hóa. Điều này ngăn chặn việc truy cập không được phép vào dữ liệu. Trong nhiều trường hợp, smart card cung cấp cơ chế để quản lý dữ liệu được lưu trữ. Điều này có thể bao gồm việc cập nhật dữ liệu, xóa dữ liệu, hoặc thực hiện các thao tác khác trên dữ liệu.

2.2.3.2 Xử lý Thông tin

Smart card không chỉ đơn thuần là thiết bị lưu trữ, mà còn có khả năng xử lý thông tin nhờ việc tích hợp một vi xử lý nhỏ (microprocessor) bên trong chip của nó. Đây chính là điểm tạo nên sự thông minh của smart card so với các loại thẻ thông thường khác. Cách mà smart card xử lý thông tin bao gồm:

- **Xác thực:** Smart card có thể thực hiện các thuật toán xác thực để chứng minh tính xác thực của thẻ hoặc người dùng. Ví dụ, một smart card có thể yêu cầu người dùng nhập mã PIN và sau đó xác minh mã PIN này trước khi cho phép truy cập vào dữ liệu trên thẻ.
- **Mã hóa/ Giải mã:** Smart card có thể thực hiện các thuật toán mã hóa để bảo vệ dữ liệu trên thẻ và dữ liệu truyền đi từ thẻ. Điều này đặc biệt quan trọng khi thẻ được sử dụng trong các giao dịch tài chính hoặc khi truy cập vào các hệ thống yêu cầu bảo mật cao.
- **Xử lý giao dịch:** Trong một số ứng dụng, smart card còn có thể thực hiện các giao dịch phức tạp. Ví dụ, một smart card sử dụng cho giao dịch tài chính có thể tự động thực hiện các thao tác như kiểm tra số dư, trừ tiền, cập nhật thông tin giao dịch, v.v.
- **Thực hiện lệnh:** Smart card có thể nhận và thực hiện các lệnh từ một thiết bị bên ngoài, như một máy đọc thẻ. Lệnh này có thể yêu cầu thẻ thực hiện các hành động như đọc dữ liệu, ghi dữ liệu, thực hiện xác thực, v.v.

2.2.3.3 Giao tiếp với Thiết bị Bên ngoài

Contact smart card

Contact smart card giao tiếp với thiết bị bên ngoài (thông thường là một máy đọc thẻ) thông qua một bộ gồm 8 chân tiếp xúc kim loại được chuẩn hóa và đặt ở giữa thẻ. Các chân này, khi thẻ được chèn vào máy đọc, kết nối với các chân tương ứng trên máy đọc, tạo ra một đường truyền dữ liệu.

Đây là các chân tiếp xúc và mục đích của chúng:

Vcc: Để cung cấp năng lượng cho thẻ.

RST: Để khởi động lại hoặc thiết lập lại thẻ.

CLK: Đưa ra tín hiệu đồng hồ để đồng bộ hóa truyền dữ liệu.

GND: Đất hoặc điểm tham chiếu cho năng lượng.

Vpp: Được sử dụng trong một số thẻ để cung cấp điện áp lập trình cao (không còn được sử dụng nhiều nữa).

I/O: Đây là kênh truyền dữ liệu chính giữa thẻ và máy đọc.

C4, C8: Các chân này có thể được sử dụng cho các chức năng phụ hoặc đặc biệt (tùy thuộc vào loại thẻ).

Quá trình giao tiếp bắt đầu khi thẻ được chèn vào máy đọc. Máy đọc sẽ cung cấp điện năng cho thẻ thông qua chân Vcc và đất (GND), sau đó thiết lập lại thẻ bằng cách sử dụng chân RST. Máy đọc sau đó sẽ gửi một chuỗi các lệnh đến thẻ thông qua chân I/O, và thẻ sẽ trả lời bằng cách gửi dữ liệu trở lại qua cùng một chân.

Cả máy đọc và thẻ đều phải tuân theo một giao thức giao tiếp đặc biệt, thường là T=0 hoặc T=1 theo chuẩn ISO/IEC 7816. Giao thức này quy định cách dữ liệu được truyền đi và nhận lại, bao gồm các định dạng dữ liệu, thời gian truyền, và cách xử lý lỗi.

Contactless smart card

Contactless smart card giao tiếp với máy đọc thông qua một kỹ thuật không dây gọi là giao tiếp từ xa gần (NFC - Near Field Communication). Thay vì cần phải chèn thẻ vào máy đọc, người dùng chỉ cần đặt thẻ gần máy đọc (thường không cách xa hơn 10 cm).

Quá trình giao tiếp giữa thẻ không tiếp xúc và máy đọc bao gồm các bước sau:

1. Khi thẻ đặt gần máy đọc, máy đọc sẽ tạo ra một trường điện từ.
2. Thẻ không tiếp xúc chứa một ăng-ten nhỏ kết nối với một mạch tích hợp. Khi thẻ được đặt trong trường điện từ, năng lượng từ trường điện từ sẽ tạo ra dòng điện trên ăng-ten, cung cấp năng lượng cho mạch tích hợp.
3. Máy đọc sau đó sẽ gửi một yêu cầu, hoặc lệnh, đến thẻ. Điều này được thực hiện bằng cách thay đổi trường điện từ, tạo ra một tín hiệu RF (tần số vô tuyến) mà thẻ có thể phát hiện và giải mã.
4. Thẻ trả lời bằng cách thay đổi sự cản trở của ăng-ten, tạo ra thay đổi trong trường điện từ mà máy đọc có thể phát hiện - một kỹ thuật được gọi là load modulation.

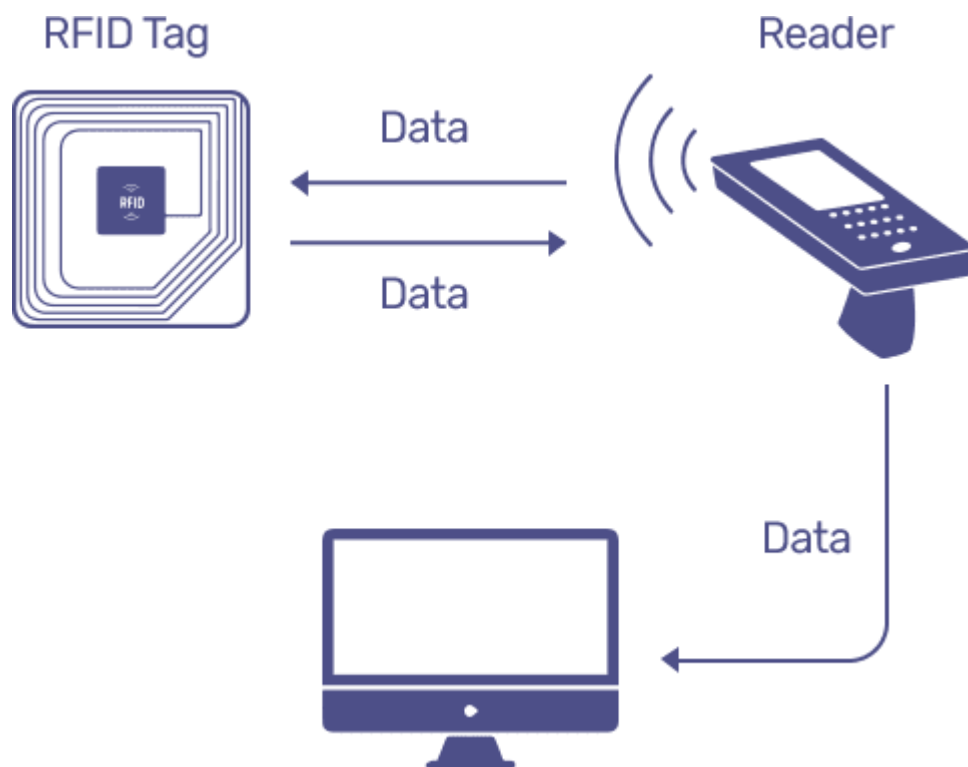
Máy đọc và thẻ không tiếp xúc cũng tuân theo một giao thức giao tiếp cụ thể, thường là ISO/IEC 14443 hoặc ISO/IEC 15693. Giao thức này quy định cách dữ liệu

được truyền đi và nhận lại, bao gồm các định dạng dữ liệu, thời gian truyền, và cách xử lý lỗi.

RFID và NFC

Công nghệ NFC (Near Field Communication) và RFID (Radio Frequency Identification) đều liên quan đến việc truyền tải dữ liệu không dây và đều được sử dụng trong một số loại smart card.

RFID là viết tắt của Radio Frequency Identification. Công nghệ này cho phép truyền tải dữ liệu từ xa thông qua sóng vô tuyến giữa một thiết bị đọc và một "tag" hoặc "chip" RFID, không cần thiết bị đọc phải nhìn thấy trực tiếp thẻ. Thẻ RFID thường được dùng trong các ứng dụng quản lý hàng tồn kho, quản lý vận tải, và theo dõi sản phẩm, nhưng cũng có thể được tích hợp vào smart card.



Hình 2.11: Công nghệ RFID

Trong ngữ cảnh smart card, thẻ RFID được sử dụng để giữ và truyền dữ liệu. Ví dụ, một thẻ ID nhân viên có thể chứa thông tin về người sở hữu và truyền dữ liệu đó đến một thiết bị đọc để kiểm soát truy cập.

NFC hay Near Field Communication là một công nghệ không dây cho phép trao đổi thông tin giữa hai thiết bị ở khoảng cách rất ngắn, thường là ít hơn 10 cm. Điều này khác với RFID, mà có thể hoạt động ở khoảng cách xa hơn nhiều.

NFC thường được sử dụng trong các ứng dụng như thanh toán di động hoặc vé điện tử. Smart card sử dụng NFC có thể chứa thông tin thanh toán, và khi chúng được đặt gần một thiết bị đọc NFC (ví dụ, một thiết bị đọc thẻ tín dụng tại cửa hàng), thông tin thanh toán được truyền từ thẻ đến thiết bị đọc.



Hình 2.12: Ứng dụng của công nghệ NFC

Mỗi công nghệ này đều có ưu và nhược điểm riêng. RFID có thể hoạt động ở khoảng cách xa, nhưng thông thường chỉ cho phép truyền tải dữ liệu một chiều - từ thẻ đến thiết bị đọc. Trong khi đó, NFC hoạt động ở khoảng cách ngắn hơn, nhưng cho phép giao tiếp hai chiều, làm cho nó lý tưởng cho các ứng dụng như thanh toán di động, nơi thông tin cần được trao đổi giữa hai thiết bị.

Vậy, smart card, đặc biệt là loại không tiếp xúc (contactless), thường sử dụng công nghệ RFID hoặc NFC để giao tiếp không dây với các thiết bị khác. Loại thẻ này có thể được sử dụng trong nhiều ứng dụng khác nhau, từ việc kiểm soát truy cập đến việc thanh toán không tiếp xúc.

2.2.3.4 Bảo mật và Xác thực

Lưu trữ an toàn

Dữ liệu lưu trữ trên smart card thường được mã hóa bằng cách sử dụng các thuật toán mã hóa mạnh mẽ. Điều này đảm bảo rằng dữ liệu không thể được đọc mà không có khóa giải mã thích hợp. Để truy cập vào dữ liệu trên smart card, thường cần phải chứng thực bằng một mã PIN hoặc một cơ chế chứng thực biometric. Điều này ngăn người không có quyền truy cập vào dữ liệu. Smart card thường được thiết kế để chống lại các cố gắng truy cập vô hiệu hoá, chẳng hạn như cố gắng phá vỡ vật lý card để lấy dữ liệu. Nhiều smart card cũng bao gồm các biện pháp để tự hủy nếu họ phát hiện cố gắng truy cập trái phép. Smart card thường được thiết kế để an toàn lưu trữ và xử lý dữ liệu nhạy cảm. Ví dụ, họ có thể được thiết kế để thực thi mã chỉ nếu nó đã được ký bởi một nhà cung cấp tin cậy, ngăn chặn việc tấn công bằng mã độc. Smart card thường được thiết kế để an toàn lưu trữ và xử lý dữ liệu nhạy cảm. Ví dụ, họ có thể được thiết kế để thực thi mã chỉ nếu nó đã được ký bởi một nhà cung cấp tin cậy, ngăn chặn việc tấn công bằng mã độc.

Mã hóa

Mã hóa trong smart card đề cập đến việc sử dụng thuật toán để chuyển đổi dữ liệu thành một dạng không thể đọc được nếu không có khóa giải mã. Dữ liệu sau khi được mã hóa được gọi là ciphertext. Đây là một phương thức quan trọng để đảm bảo tính bảo mật của thông tin lưu trữ trên smart card.

Smart card thường sử dụng hai loại chính của mã hóa:

- Mã hóa đối xứng: Trong mã hóa đối xứng, cùng một khóa được sử dụng để mã hóa và giải mã dữ liệu. Một ví dụ phổ biến về thuật toán mã hóa đối xứng là AES (Advanced Encryption Standard). Điểm mạnh của mã hóa đối xứng là nhanh và hiệu quả, nhưng yêu cầu phân phối khóa an toàn.
- Mã hóa bất đối xứng: Trong mã hóa bất đối xứng, hai khóa được sử dụng - một khóa công khai để mã hóa dữ liệu và một khóa bí mật để giải mã. Ví dụ phổ biến về thuật toán mã hóa bất đối xứng bao gồm RSA, DSA và ECC. Mã hóa bất đối xứng có thể cung cấp một cấp độ bảo mật cao hơn nhưng cũng tiêu tốn nhiều tài nguyên hơn.

Smart card cũng thường hỗ trợ các hoạt động mã hóa khác như tạo chữ ký số và xác thực nguồn gốc của thông tin. Trong mô hình sử dụng phổ biến, thông tin quan trọng như khóa bí mật và mã PIN được lưu trữ trong smart card sau khi được mã hóa. Khi cần truy cập vào thông tin này, người dùng cung cấp mã PIN hoặc một hình thức chứng thực khác, sau đó smart card thực hiện quá trình giải mã.

Trong mô hình sử dụng phổ biến, thông tin quan trọng như khóa bí mật và mã PIN được lưu trữ trong smart card sau khi được mã hóa. Khi cần truy cập vào thông tin này, người dùng cung cấp mã PIN hoặc một hình thức chứng thực khác, sau đó smart card thực hiện quá trình giải mã.

Xác thực

Xác thực trong smart card liên quan đến việc đảm bảo rằng người dùng hay hệ thống mà smart card đang giao tiếp với là hợp lệ và có quyền truy cập vào dữ liệu hoặc thực hiện các giao dịch cụ thể.

Trong nhiều trường hợp, xác thực diễn ra bằng cách yêu cầu người dùng nhập một mã PIN hoặc mật khẩu. Điều này thường được gọi là xác thực dựa trên cái gì người dùng biết. Mã PIN hoặc mật khẩu này sau đó được so sánh với giá trị được lưu trữ trên smart card. Nếu giá trị này khớp, quyền truy cập sẽ được cấp phép.

Trong một số trường hợp, smart card có thể yêu cầu một hình thức xác thực khác, như xác thực dựa trên cái gì người dùng có (ví dụ: smart card) hoặc xác thực dựa trên cái gì người dùng là (biometrics như dấu vân tay hay khuôn mặt).

Smart card cũng có thể được sử dụng trong quá trình xác thực hai yếu tố (2FA). Trong trường hợp này, người dùng cần cung cấp hai hình thức xác thực khác nhau - ví dụ: một cái gì đó họ biết (mã PIN) và một cái gì đó họ có (smart card).

Ngoài ra, smart card cũng thường thực hiện xác thực với máy chủ hoặc hệ thống mà nó đang giao tiếp thông qua quá trình trao đổi khóa và mã hóa. Điều này giúp ngăn chặn việc giả mạo và đảm bảo rằng thông tin được truyền an toàn giữa smart card và hệ thống.

Chống tấn công phân tích

Các tấn công phân tích điện năng (power analysis attacks) dựa trên việc quan sát mức tiêu thụ điện năng trong quá trình xử lý thông tin để xác định dữ liệu bên trong

smart card. Smart card chống lại loại tấn công này bằng cách sử dụng các kỹ thuật như "masking" (che giấu) và "blinding" (làm mù) để làm mờ sự biến động của tiêu thụ điện năng.

Smart card chống lại các tấn công phá vỡ vật lý, như việc thâm nhập vào chip bằng cách sử dụng vật liệu bảo vệ chống lại sự thâm nhập vật lý và phát hiện vi phạm tích hợp. Một số smart card còn có cấu trúc phần cứng đặc biệt để làm hỏng chip khi cố gắng mở ra.

Các tấn công phân tích tần số đồng hồ dựa trên việc điều chỉnh tần số đồng hồ của smart card để gây ra lỗi và từ đó lấy được thông tin nhạy cảm. Để chống lại điều này, một số smart card có chức năng điều chỉnh độ nhảy của việc thay đổi tần số đồng hồ.

Smart card còn chống lại việc lấy thông tin thông qua phương pháp phụ như tiếng ồn điện từ, bằng cách sử dụng kỹ thuật che giấu thông tin và chống nhiễu.

Tất cả các kỹ thuật này giúp giảm thiểu rủi ro của việc thông tin bị đánh cắp từ smart card thông qua các tấn công phần cứng. Tuy nhiên, cũng nên lưu ý rằng không có hệ thống nào là hoàn toàn an toàn, và những kỹ thuật này chỉ làm tăng khó khăn cho kẻ tấn công, chứ không phải lúc nào cũng ngăn chặn hoàn toàn được mọi tấn công.

Chứng thực thiết bị

Chứng thực thiết bị smart card đề cập đến việc xác minh danh tính của smart card và đảm bảo rằng nó là thiết bị hợp lệ, không bị giả mạo hoặc thay đổi. Điều này thường được thực hiện thông qua một quy trình chứng thực hai chiều, trong đó cả smart card và thiết bị đọc thẻ (reader) đều phải chứng minh rằng chúng là hợp lệ.

Trong quá trình này, thiết bị đọc thẻ sẽ yêu cầu smart card cung cấp bằng chứng về danh tính của nó, thường là thông qua việc sử dụng một chìa khóa bí mật nằm trong smart card. Smart card sẽ sau đó tạo ra một chữ ký số hoặc mã hóa một thông điệp sử dụng chìa khóa bí mật này. Nếu thiết bị đọc thẻ có thể giải mã hoặc xác minh chữ ký số sử dụng chìa khóa công khai tương ứng, thì danh tính của smart card được xác nhận.

Ngược lại, thiết bị đọc thẻ cũng cần phải chứng minh danh tính của nó với smart card. Điều này đảm bảo rằng chỉ các thiết bị đọc thẻ hợp lệ mới có thể truy cập vào dữ liệu trên smart card. Quá trình này thường giống với quá trình chứng thực smart card, nhưng ngược lại.

Thực thi mã an toàn

Trong smart card, thực thi mã an toàn thường liên quan đến việc sử dụng phần cứng và phần mềm để đảm bảo rằng chỉ mã được ủy quyền mới được thực thi trên smart card:

Isolation (Cô lập): Smart card thường sử dụng một hệ điều hành đặc biệt cho phép chạy nhiều ứng dụng một cách độc lập với nhau. Điều này đảm bảo rằng việc thực thi mã của một ứng dụng không thể ảnh hưởng đến hoạt động của các ứng dụng khác hoặc dẫn đến vi phạm bảo mật.

Digital Signature (Chữ ký số): Mã thực thi thường được ký số bởi nhà cung cấp hoặc nhà sản xuất smart card. Trước khi mã được thực thi, smart card sẽ kiểm tra chữ ký số này để đảm bảo rằng mã không bị thay đổi kể từ khi nó được ký và rằng nó đến từ một nguồn đáng tin cậy.

Secure Boot (Khởi động an toàn): Trong quá trình khởi động, smart card sẽ kiểm tra sự toàn vẹn và chữ ký số của hệ điều hành và các ứng dụng của nó. Nếu bất kỳ điều gì không phù hợp, smart card sẽ từ chối khởi động hoặc thực thi các ứng dụng đó.

Access Control (Kiểm soát truy cập): Smart card sử dụng các cơ chế kiểm soát truy cập phức tạp để ngăn chặn việc truy cập không được phép vào mã thực thi. Ví dụ, một ứng dụng không thể đọc hoặc ghi vào vùng nhớ của một ứng dụng khác.

Encryption (Mã hóa): Mã thực thi có thể được mã hóa để ngăn chặn việc đọc hoặc sửa đổi bất hợp pháp.

2.2.4 Ứng dụng

An ninh cho máy tính

Trình duyệt web Mozilla Firefox có thể dùng thẻ thông minh để lưu trữ chứng nhận dùng cho việc duyệt web một cách an ninh. Một vài hệ thống mã hóa đĩa, chẳng hạn như FreeOTFE, có thể dùng thẻ thông minh để giữ các khóa mã một cách an ninh, và cũng để thêm một lớp nữa cho việc mã hóa các phần quan trọng nhất của đĩa cần bảo mật. Thẻ thông minh cũng được dùng cho việc xác nhận và cho phép truy cập đến các máy tính mà không cần phải sử dụng thêm một phương tiện nào khác như mật khẩu,...

Tài chính

Các ứng dụng của thẻ thông minh trong lĩnh vực tài chính bao gồm: thẻ tín dụng hay thẻ ATM, thẻ đổ xăng, SIM cho điện thoại di động, thẻ truyền hình cho các kênh phải trả tiền, các thẻ dùng cho điện thoại công cộng hoặc giao thông công cộng. Thẻ thông minh cũng có thể dùng như ví điện tử. Chip trên thẻ thông minh có thể được nạp sẵn một số tiền mà có thể dùng tiêu xài tại các trạm đỗ xe và các máy bán hàng tự động. Một số ví dụ như Proton, Geldkarte, Chipknip và Mon€o. Thẻ Geldkarte của Đức cũng có thêm tính năng kiểm tra tuổi của người mua để cho phép mua thuốc lá tại các máy bán hàng tự động hay không.

Dùng cho thẻ chứng minh hoặc các thẻ tương tự

Một ứng dụng đang ngày càng phát triển rất nhanh đó là dùng trong các thẻ chứng minh nhân dân kỹ thuật số. Trong ứng dụng này, thẻ thông minh được dùng như một bằng chứng để xác minh. Một ví dụ thường gặp nhất là sử dụng thẻ thông minh cùng với một PKI. Thẻ thông minh sẽ lưu trữ một chứng nhận số đã mã hóa từ PKI cùng với các thông tin liên quan và cần thiết về người chủ thẻ. Các hệ thống hiện có như thẻ ra vào dùng chung (CAC) của Bộ quốc phòng Mỹ, và hệ thống chứng minh nhân dân tại nhiều nước áp dụng cho toàn thể công dân của họ. Khi dùng chung với các đặc trưng sinh trắc học, thẻ thông minh có độ tin cậy và an ninh tăng gấp hai đến ba lần.

Hệ thống giấy phép lái xe dùng thẻ thông minh đầu tiên trên thế giới được giới thiệu vào năm 1995 tại Mendoza, một tỉnh của Argentina. Mendoza là nơi có tỉ lệ tai nạn giao thông cao, số người vi phạm giao thông nhiều và tỉ lệ đóng phạt lại thấp. Giấy phép lái xe dùng thẻ thông minh sẽ lưu trữ và cập nhật thông tin vi phạm và số tiền phạt chưa đóng của tài xế. Nó cũng lưu thông tin cá nhân, loại và số giấy phép cũng như hình chụp của người chủ thẻ. Ngoài ra các thông tin cần thiết cho cấp cứu như nhóm máu, dị ứng, và sinh trắc học (dấu tay) cũng được lưu vào trong chip nếu người chủ thẻ yêu cầu. Chính phủ Argentina cho biết hệ thống mới này đã giúp họ thu hồi hơn 10 triệu USD tiền phạt trên một.

Trường hợp Ấn Độ, năm 1999 Gujarat là tiểu bang đầu tiên đưa vào sử dụng smart card license system Lưu trữ 2009-04-10 tại Wayback Machine. Hiện nay, chính phủ Gujarat đã phát hành 5 triệu giấy phép lái xe dùng thẻ thông minh đến công dân của họ.

Về cơ bản, đây là loại thẻ nhựa theo chuẩn ISO/IEC 7810 có khả năng lưu trữ và kiểm tra thông tin về chủ thẻ.

Thẻ thông minh đã và đang được quảng cáo như một phương tiện phù hợp cho các nhiệm vụ xác minh cá nhân, bởi chúng được thiết kế và chế tạo nhằm tránh giả mạo. Chip được nhúng trên thẻ thông minh thường được cài thêm một số thuật toán bảo mật. Thông tin về giải thuật bên trong chỉ có thể biết được nếu biết chính xác thời gian và dòng điện tiêu thụ của việc mã hóa và giải mã. Một số nghiên cứu cũng đã đưa ra tính khả thi của việc tấn công lấy cắp thông tin trên thẻ và cũng đã đưa ra nhiều biện pháp đối phó.

Bắt đầu từ năm 2009 toàn bộ dân số của Tây Ban Nha và Bỉ sẽ có thẻ chứng minh nhân dân số. Các thẻ này có hai chức năng: xác minh và chữ ký điện tử. Chữ ký này được công nhận hợp pháp. Ngày càng có nhiều quốc gia sử dụng thẻ chứng minh nhân dân số như là bằng chứng hợp pháp cho nhiều dịch vụ khác nhau.

Thẻ thông minh được dùng rộng rãi để bảo vệ các kênh truyền hình số có thu phí. Về tổng quan, xem mã hóa truyền hình, và để có một ví dụ đặc biệt nhằm hiểu thẻ thông minh làm việc như thế nào trong trường hợp này nên xem VideoGuard.

2.2.5 Ưu điểm và hạn chế

Ưu điểm

Bảo mật cao: Smart card có khả năng mã hóa dữ liệu và thực hiện các chức năng bảo mật nâng cao như xác thực hai yếu tố, ngăn chặn sao chép hoặc sửa đổi thông tin trên thẻ.

Dung lượng lưu trữ: Mặc dù kích thước nhỏ gọn, smart card có thể lưu trữ một lượng dữ liệu khá lớn.

Tính linh hoạt: Smart card có thể được sử dụng cho nhiều mục đích khác nhau, từ chứng minh thực thể cá nhân (như thẻ ID hoặc thẻ lái xe) đến việc thực hiện giao dịch tài chính (như thẻ tín dụng hoặc thẻ ATM).

Tuân thủ tiêu chuẩn: Hầu hết các smart card tuân thủ theo một số tiêu chuẩn quốc tế, giúp đảm bảo sự tương thích giữa các thiết bị và hệ thống khác nhau.

Khả năng chống gian lận: Do cách thức hoạt động và các cơ chế bảo mật, smart card khá khó bị tấn công và gian lận so với các hình thức chứng thực truyền thống khác.

Độ bền: Smart card thường rất bền và có thể chịu đựng được việc sử dụng hàng ngày.

Hạn chế

Một nhược điểm của thẻ thông minh là khả năng hư hỏng. Thẻ nhựa mà chip đặt trên nó là khá dẻo, dễ uốn, và do đó chip càng lớn thì càng dễ bị gãy. Thẻ thông minh thường được bỏ trong ví, đây là một môi trường khá khắc nghiệt đối với chip điện tử. Tuy nhiên, đối với một số hệ thống ngân hàng lớn, chi phí quản lý bảo hành thẻ có thể chấp nhận được so với chi phí giảm giả mạo và lừa đảo. Dùng thẻ thông minh cho giao thông công cộng cũng có một chút rủi ro về quyền tự do cá nhân, bởi vì với hệ thống như vậy thì người quản lý giao thông có thể dò theo hành trình của cá nhân. Ở Phần Lan, bộ phận Bảo vệ Dữ Liệu Ombudsman cấm người quản lý giao thông của YTV thu thập các thông tin như vậy, mặc dầu trong hợp đồng với YTV người chủ thẻ có quyền yêu cầu YTV cung cấp cho họ lịch trình đi mà YTV đã tính tiền cho họ. Những thông tin về lịch trình từng được dùng trong việc truy tìm thủ phạm trong vụ đánh bom Myyrmanni.

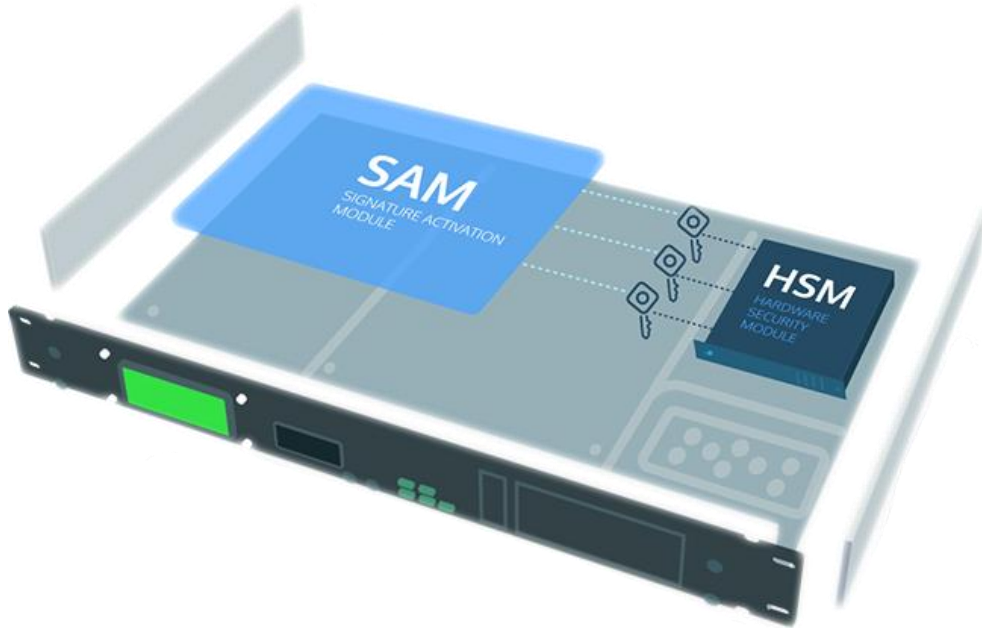
Thẻ thông minh dùng để xác nhận khách hàng là một trong những cách an ninh nhất, có thể dùng trong những ứng dụng như giao dịch ngân hàng qua internet, nhưng mức độ an ninh không thể đảm bảo 100%. Trong trường hợp giao dịch ngân hàng qua internet, nếu PC bị nhiễm bởi các phần mềm xấu, mô hình an ninh sẽ bị phá vỡ. Phần mềm xấu có thể viết đè lên thông tin (cả thông tin đầu vào từ bàn phím và thông tin đầu ra màn hình) giữa khách hàng và ngân hàng. Nó có thể sẽ sửa đổi giao dịch mà khách hàng không biết. Có những phần mềm xấu như vậy, chẳng hạn như Trojan. Silentbanker). Các ngân hàng như Fortis Dexia ở Bỉ dùng một thẻ thông minh chung với một máy đọc thẻ không nối mạng nhằm giải quyết vấn đề trên. Khách hàng nhập một thông tin đánh giá từ trang web của ngân hàng, PIN của họ, và tổng số tiền giao dịch vào một máy đọc thẻ, máy đọc thẻ sẽ trả lại một chữ ký 8 chữ số. Chữ ký này sẽ được khách hàng nhập bằng tay vào PC và được kiểm chứng bởi ngân hàng.

Bên cạnh việc chạy đua kỹ thuật cũng là sự thiếu hẳn một chuẩn thống nhất về chức năng và an ninh của thẻ thông minh. Để giải quyết vấn đề này, dự án ERIDANE đã được khởi động bởi The Berlin Group để phát triển một "khung chức năng và an ninh cho những thiết bị bán lẻ đầu cuối dùng thẻ thông minh".

2.3 HSM (Hardware Security Module)

2.3.1 Tổng quan

HSM (Hardware Security Module) là một thiết bị phần cứng được sử dụng để cung cấp bảo mật mạnh mẽ và quản lý khóa cho các ứng dụng và hệ thống. HSM thường được sử dụng trong các lĩnh vực như bảo mật thông tin, chữ ký số, thanh toán điện tử và quản lý quyền truy cập.



Hình 2.13: HSM

HSM có tính năng và khả năng bảo mật cao hơn so với phần mềm mã hóa thông thường trên máy tính, vì chúng sử dụng một phần cứng chuyên dụng để thực hiện các hoạt động bảo mật. HSM thường được thiết kế để bảo vệ các khóa mã hóa và thực hiện các hoạt động như mã hóa, giải mã, tạo chữ ký số và xác thực.

SỰ KHÁC NHAU GIỮA 2 THIẾT BỊ KÍ SỐ



USB TOKEN

Ký trên Desktop, Laptop có cổng USB

Người dùng bắt buộc phải luôn mang theo thiết bị bên mình.

Tại một thời điểm chỉ 1 người có quyền sử dụng, không thể phân quyền rộng rãi

Ký số lần lượt và tốc độ ký chậm, khoảng 4-5 hóa đơn/phút.

Cần cài đặt Tool, Java hỗ trợ để kết nối USB.

Phù hợp với doanh nghiệp quy mô nhỏ.



HSM

Ký trên Desktop, Laptop và mọi thiết bị di động.

Người dùng không phải mang theo thiết bị ký số như USB Token.

Nhiều bộ phận có thể thực hiện ký số cùng lúc, phân quyền sử dụng cho các bộ phận liên quan dễ dàng.

Ký số tốc độ cao và ký đồng thời đảm bảo nguyên tắc số hóa đơn cùng đây, liên tục theo trình tự thời gian, tốc độ lên đến 1.500 hóa đơn/giây.

Không cần cài đặt Tool, Java, ít bị lỗi khi ký hóa đơn.

Phù hợp cho tất cả các loại hình và quy mô doanh nghiệp.

Hình 2.14: Sự khác nhau giữa USB Token và HSM

2.3.2 Chức năng

Các chức năng chính của HSM bao gồm:

1. Quản lý khóa: HSM có khả năng tạo, lưu trữ và quản lý các khóa mã hóa. Chúng bảo đảm an toàn cho khóa bằng cách lưu trữ chúng trong phần cứng bảo mật và thực hiện các hoạt động quản lý khóa như tạo khóa, quản lý vòng đời khóa và hủy bỏ khóa.

2. Mã hóa và giải mã: HSM cung cấp khả năng mã hóa và giải mã dữ liệu bằng cách sử dụng khóa mã hóa được lưu trữ trong phần cứng. Chúng hỗ trợ các thuật toán mã hóa mạnh như AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), DES (Data Encryption Standard) và ECC (Elliptic Curve Cryptography).

3. Tạo và xác thực chữ ký số: HSM có khả năng tạo chữ ký số và xác thực chữ ký số trên dữ liệu. Điều này đảm bảo tính toàn vẹn và xác thực của dữ liệu và đảm bảo rằng chữ ký số không bị giả mạo.

4. Xác thực người dùng: HSM có thể được sử dụng để xác thực người dùng trước khi cho phép truy cập vào các khóa và dữ liệu quan trọng. Chúng hỗ trợ các phương pháp xác thực như mật khẩu PIN, dấu vân tay và thẻ thông minh.

5. Bảo mật vật lý: HSM được thiết kế với các biện pháp bảo mật vật lý như vỏ bọc chắc chắn, cảm biến va đập và chống nước.

HSM được sử dụng trong nhiều lĩnh vực, bao gồm ngân hàng, tài chính, thẻ tín dụng, chứng khoán, điện toán đám mây và các hệ thống mạng lớn. Việc sử dụng HSM giúp đảm bảo tính bảo mật, sự toàn vẹn và tính khả dụng của dữ liệu và hoạt động mật mã.

2.3.3 Phân loại

HSM (Hardware Security Module) có thể được phân loại theo các tiêu chí khác nhau, bao gồm:

Dựa trên cấu trúc vật lý:

HSM ở dạng chân trời (Rack-mounted HSM): Được cài đặt trong một rack server và tích hợp vào hạ tầng hệ thống tổ chức.

HSM ở dạng thẻ (Card-based HSM): Có kích thước nhỏ gọn và có thể được cài đặt trực tiếp trên các thiết bị như máy tính hoặc thiết bị mạng.

Dựa trên mục đích sử dụng:

- HSM chữ ký số (Signature HSM): Tập trung vào việc tạo và quản lý chữ ký số, hỗ trợ các hoạt động như ký số, xác thực chữ ký số và quản lý chứng chỉ số.
- HSM mã hóa (Encryption HSM): Tập trung vào việc mã hóa và giải mã dữ liệu, cung cấp các thuật toán mã hóa mạnh mẽ và quản lý khóa mã hóa.

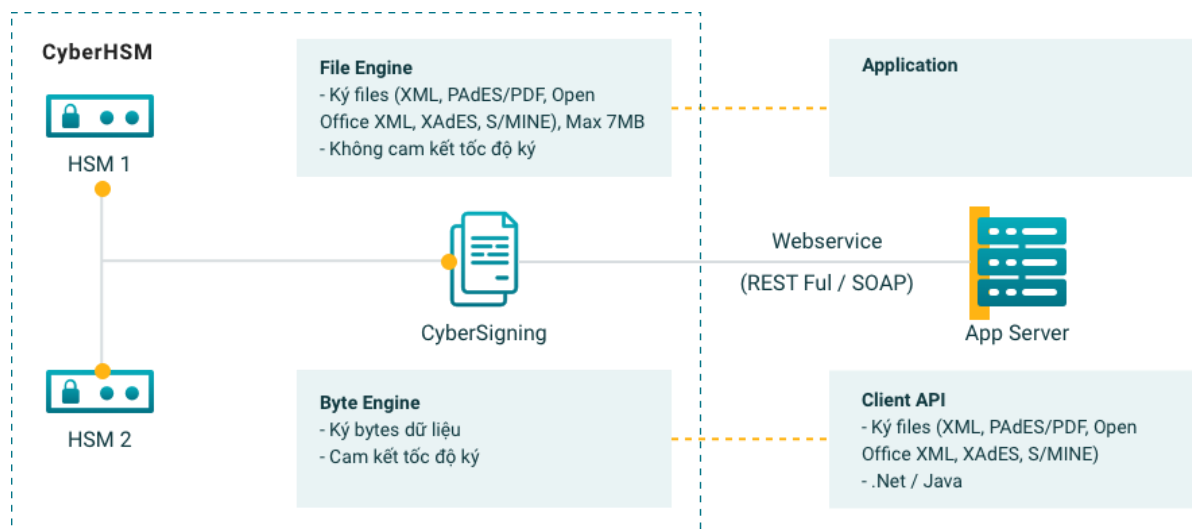
- HSM chứng thực (Authentication HSM): Tập trung vào việc xác thực người dùng và hệ thống, cung cấp chức năng như quản lý mã OTP (One-Time Password), xác thực hai yếu tố và hỗ trợ giao thức FIDO (Fast Identity Online).
- HSM tổ chức (Enterprise HSM): Cung cấp một loạt các chức năng bảo mật cho tổ chức, bao gồm quản lý khóa, chứng thực, mã hóa và chữ ký số.

Dựa trên hiệu suất và khả năng:

- HSM cấp doanh nghiệp (Enterprise-grade HSM): Có khả năng xử lý cao và hỗ trợ cho các hệ thống quy mô lớn và tải trọng cao.
- HSM cấp tập trung (Centralized HSM): Thiết kế để quản lý nhiều HSM từ một trung tâm quản lý duy nhất, giúp tối ưu hóa việc triển khai và quản lý các HSM.

2.3.4 Nguyên lý hoạt động

Nếu như trước đây khi tiến hành các giao dịch, ký kết hợp đồng, kê khai giấy tờ,... các cá nhân/ doanh nghiệp đều phải ký tay, xác nhận chữ ký tay hoặc đóng dấu mất rất nhiều thời gian, công sức thì giờ đây chữ ký số đã hoàn toàn xóa bỏ những bất tiện đó.



Hình 2.15: Nguyên lý hoạt động HSM

Về tổng quan, nguyên lý hoạt động của chữ ký số HSM khá tương tự như USB Token.

Để chữ ký số HSM có thể vận hành, chúng ta cần sử dụng thiết bị phần cứng HSM có chứa cặp khóa (khóa công khai và khóa bí mật) để xác nhận danh tính người dùng. Dữ liệu được mã hóa trong HSM được bảo mật an toàn, không thể nhân bản, sao chép hay làm giả.

Tuy nhiên, nếu như chữ ký số USB Token chỉ được sử dụng như một loại hình offline, phải cắm USB token vào máy tính mới có thể thực hiện ký số, thì chữ ký số HSM lại linh hoạt hơn khi có thể phát huy tính năng ở môi trường trực tuyến.

Cụ thể, khi sử dụng chữ ký số HSM, người dùng sẽ được đăng ký và tạo lập một tài khoản tương tự như các trang mạng xã hội thông thường, sau đó thực hiện ký số online qua mạng.

Chính vì tính năng ưu việt này, cá nhân hay doanh nghiệp không cần mang theo HSM bên người mà vẫn có thể thực hiện ký số.

2.3.5 Ứng dụng

Chữ ký số HSM có những đặc tính ưu việt, đáp ứng nhu cầu ký số của nhiều doanh nghiệp và đảm bảo quy định của pháp luật. Tuy nhiên thiết bị này đặc biệt phù hợp với các đối tượng sau đây:

Ngân hàng và tài chính: HSM được sử dụng để bảo vệ và quản lý các khóa mật mã và dữ liệu nhạy cảm trong các hoạt động tài chính, bao gồm thanh toán điện tử, chuyển tiền và giao dịch trực tuyến.

Ngành công nghiệp thẻ tín dụng: HSM được sử dụng để bảo vệ thông tin thẻ tín dụng và thực hiện các chức năng bảo mật như chứng thực, mã hóa và giải mã trong các giao dịch thẻ tín dụng.

Chứng khoán và giao dịch tài chính: HSM được sử dụng để bảo vệ khóa mật mã và chứng chỉ số trong các hoạt động chứng khoán và giao dịch tài chính, bao gồm xác thực và ký số các hợp đồng và tài liệu quan trọng.

Cơ quan chính phủ: HSM được sử dụng trong các cơ quan chính phủ để bảo vệ thông tin nhạy cảm, đảm bảo tính bí mật và xác thực trong việc xử lý thông tin quan trọng và các giao dịch quốc gia.

Công nghệ thông tin và bảo mật: HSM được sử dụng trong lĩnh vực công nghệ thông tin và bảo mật để bảo vệ và quản lý khóa mật mã, chứng chỉ số, chữ ký số và các dữ liệu quan trọng khác. Nó cung cấp các chức năng mã hóa, giải mã, chứng thực và xác thực để đảm bảo tính bảo mật của hệ thống và dữ liệu.

Các ứng dụng IoT (Internet of Things): HSM được sử dụng để bảo vệ các thiết bị và dữ liệu trong môi trường IoT, nơi nhiều thiết bị kết nối và truyền dữ liệu. Nó giúp đảm bảo tính toàn vẹn, bảo mật và xác thực trong việc trao đổi thông tin giữa các thiết bị.

Cloud computing và dịch vụ web: HSM được sử dụng để bảo vệ và quản lý các khóa và dữ liệu mật mã trong môi trường đám mây và dịch vụ web. Nó giúp đảm bảo tính bảo mật của dữ liệu và hoạt động mã hóa.

HSM (Hardware Security Module) có nhiều ứng dụng quan trọng trong lĩnh vực bảo mật và mã hóa thông tin. Dưới đây là một số ứng dụng chính của HSM:

- Quản lý khóa mật mã: HSM được sử dụng để quản lý các khóa mật mã, bao gồm tạo, lưu trữ và quản lý quyền truy cập vào khóa. HSM bảo vệ tính bí mật

và toàn vẹn của khóa mật mã bằng cách lưu trữ chúng trong môi trường bảo mật và thực hiện các chức năng kiểm soát truy cập nghiêm ngặt.

- **Chứng thực và xác thực:** HSM cung cấp chức năng chứng thực và xác thực để đảm bảo tính xác thực và bảo mật của người dùng, ứng dụng hoặc hệ thống. Nó hỗ trợ các phương pháp xác thực như OTP (One-Time Password), xác thực hai yếu tố và hỗ trợ giao thức FIDO (Fast Identity Online).
- **Mã hóa và giải mã phần cứng:** HSM cung cấp khả năng thực hiện mã hóa và giải mã phần cứng. Việc sử dụng mã hóa phần cứng giúp bảo vệ dữ liệu khỏi các cuộc tấn công mã độc và lạm dụng lỗ hổng phần mềm.
- **Chữ ký số và chứng chỉ số:** HSM hỗ trợ việc tạo và xác thực chữ ký số và chứng chỉ số. Điều này giúp xác định tính hợp lệ của dữ liệu được ký số và chứng chỉ số được sử dụng trong quá trình chứng thực và mã hóa.
- **Thanh toán điện tử và giao dịch tài chính:** HSM được sử dụng trong ngành ngân hàng và tài chính để bảo vệ các giao dịch thanh toán điện tử và giao dịch tài chính. Nó đảm bảo tính bảo mật của thông tin tài chính, xác thực giao dịch và bảo vệ khỏi các hình thức gian lận.
- **Quản lý quyền truy cập:** HSM được sử dụng để quản lý quyền truy cập vào tài nguyên và dữ liệu quan trọng. Nó hỗ trợ việc xác định và kiểm soát quyền truy cập của người dùng và ứng dụng, đảm bảo tính bảo mật và tuân thủ chính sách bảo mật.

Chương 3. Mô phỏng triển khai

3.1 Phần cứng

3.1.1 Module RFID RC522



Hình 3.1: Module RFID RC522

RC522 là một Mô-đun RFID đa giao tiếp cho Arduino và Vi điều khiển. RC522 được gọi là MFRC-522 do vi điều khiển bán dẫn NFX của nó. Mô-đun cho phép các nhà phát triển giao tiếp nó với bất kỳ vi điều khiển dựa trên SPI, I2C và UART nào khác. Nó đi kèm với một thẻ RFID và fob khóa bao gồm 1KB bộ nhớ.

Mô-đun RC522 hoạt động trên tần số 13.56 MHz và nó có thể hoạt động như một đầu đọc và ghi cho thẻ UID / RFID. Các thẻ RFID giao tiếp với mô-đun ở khoảng cách

ngắn với tần số vô tuyến do kỹ thuật cảm ứng lẫn nhau. Trong hầu hết các sản phẩm bảo mật và thương mại, mô-đun có hiệu quả vì nó có thể phát hiện được các lỗi và sự cố với Thẻ RFID.

Thẻ RFID là một thiết bị lưu trữ bộ nhớ có bộ nhớ trị giá 1KB. Bộ nhớ này được chia thành 16 cung (0-15), trong đó mỗi khu vực được chia thành 4 khối (0,1,2,3). Mỗi khối là 16 byte. Như vậy $4 \text{ khối} \times 16 \text{ byte} \times 16 \text{ cung} = 1024 \text{ byte}$ là 1KB.

3.1.1.1 Đặc điểm

- RFID RC522 sử dụng cảm ứng lẫn nhau để kích hoạt thẻ và 13.56MHz để truyền dữ liệu.
- Thẻ RFID có thể sử dụng từ cả hai phía của mô-đun ở mức tối đa 5cm.
- Chỉ cần 3.3V để kích hoạt thiết bị.
- Chế độ ngủ tự động của nó làm cho nó ít mô-đun tiêu thụ điện năng hơn.
- Mô-đun có ba loại giao tiếp. Do đó, nó có thể sử dụng được với hầu hết mọi bộ vi điều khiển hoặc thiết bị trên thị trường.
- Thẻ và đầu đọc RFID (RC522) có thể truyền dữ liệu lên đến 10Mb / s.

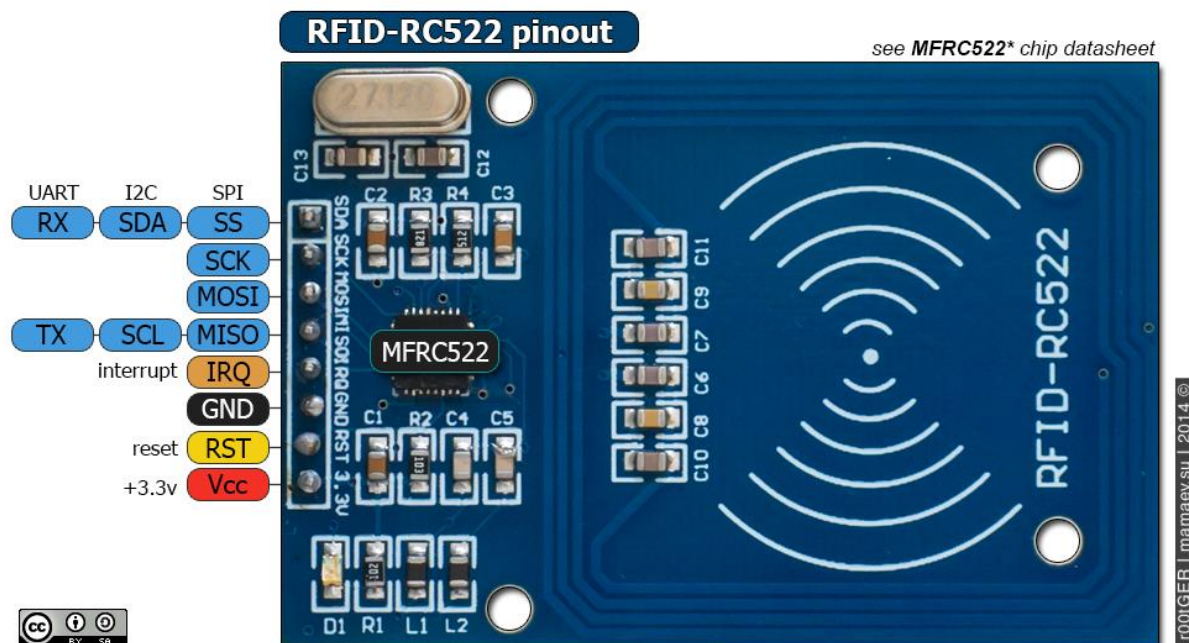
3.1.1.2 Ứng dụng

- RFID có hầu hết việc sử dụng như một thiết bị bảo mật.
- Ở một số công ty, các thiết bị sử dụng với các mặt hàng mua sắm.
- Một số sân bay cũng đã bắt đầu sử dụng RFID để xác định và theo dõi túi xách và các vật dụng khác.
- Hệ thống chấm công hoặc đỗ xe cũng sử dụng RFID để giữ an toàn cho hệ thống.

3.1.1.3 Sơ đồ chân

Trong mô-đun này, chỉ có hai loại chân. Vì vậy, cái đầu tiên là sức mạnh và cái thứ hai là chân giao tiếp. Do đó, thiết bị có thể có chip vi điều khiển trên chính nó nhưng nó chỉ làm cho nó hoạt động như một RFID. Bộ vi điều khiển tích hợp sẽ không làm cho mô-đun trở thành một thiết bị độc lập.

Tất cả các chân của Đầu đọc thẻ RFID MFRC / RC522 là:



Hình 3.2: Cấu tạo chân module RFID RC522

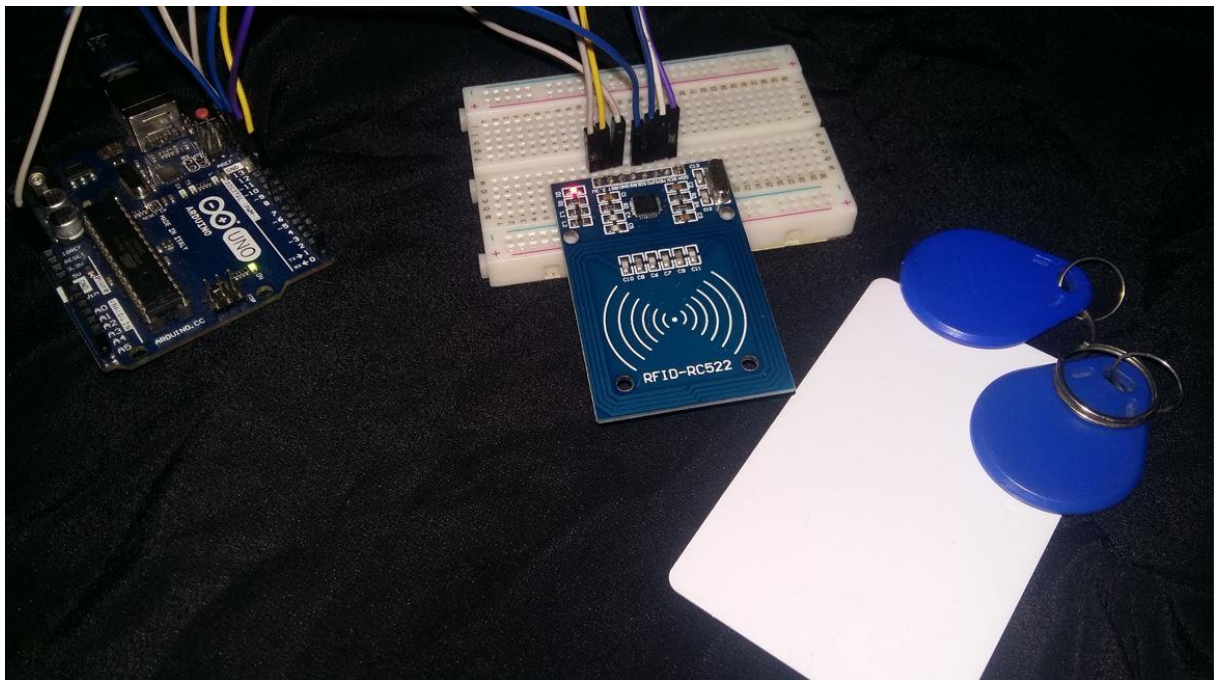
Chân	Mô tả
VCC	Các chân nguồn là VCC. Trong một số phiên bản của RC522, chân này được ký hiệu là 3V3 trên mô-đun thay vì VCC.
RST	Đây là chân đặt lại cho mô-đun. Do đó, nó sẽ đặt lại thiết bị trong trường hợp có lỗi khi thiết bị không đưa ra bất kỳ phản hồi nào.
GND	Ground giúp tạo ra điểm chung với mọi thiết bị bên ngoài, ví dụ như Nguồn điện, Bộ vi điều khiển hoặc Arduino.
IRQ	Thiết bị có thể chuyển sang chế độ ngủ để tiết kiệm năng lượng. Vì vậy, IRQ giúp đánh thức nó.
MISO	Chân này kết nối với Arduino / Vi điều khiển để giao tiếp SPI. Tuy nhiên, nó chuyển dữ liệu từ mô-đun sang Arduino. Chân MISO cũng có thể sử dụng cho các chức năng khác thay vì SPI. Nó cũng có thể giao tiếp với I2C cho xung đồng hồ và UART Serial để truyền dữ liệu từ mô-đun.
MOSI	MOSI là chân nhập dữ liệu cho mô-đun RFID trong giao tiếp SPI
SCK	Các chân SCK giúp gửi xung đồng hồ trong giao tiếp SPI.

SS	<p>Chân SS là một con chip cho phép pin trong giao tiếp SPI. Do đó, nó nhận được tín hiệu khi Master (Arduino) phải thực hiện giao tiếp SPI.</p> <p>Chân SS trong RFID có thể sử dụng làm chân thứ hai (SDA) để giao tiếp I2C.</p> <p>Nó cũng nhận dữ liệu trong quá trình giao tiếp UART.</p>
----	--

Hình 3.3: Các chân của module RFID RC522

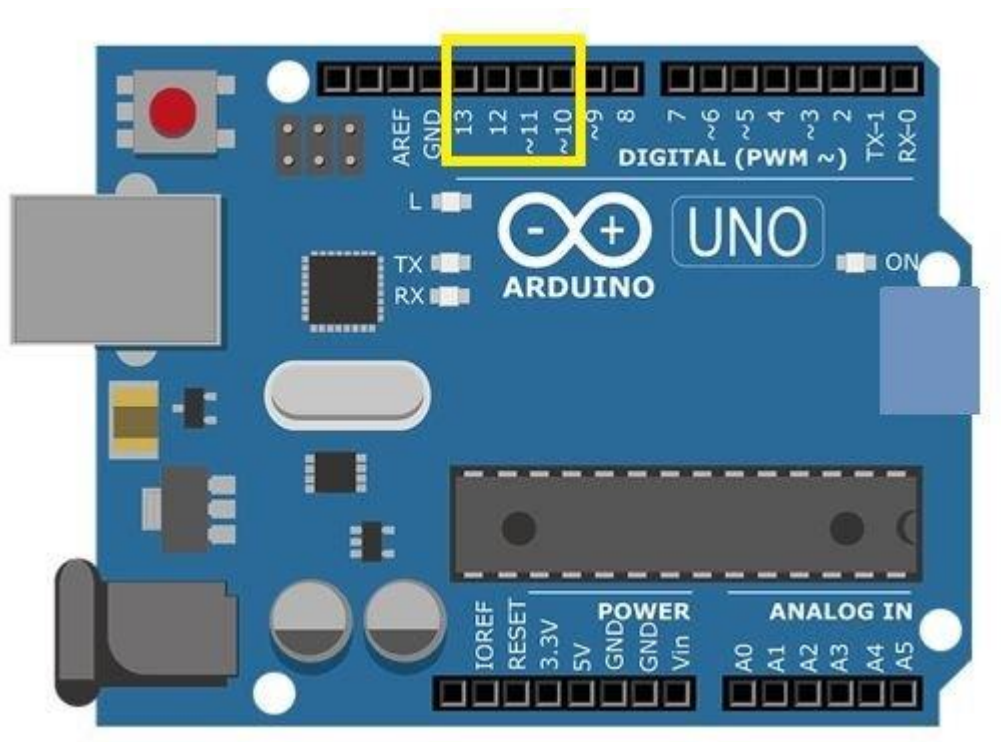
3.1.2 Arduino UNO

Như chúng ta đã thấy ở trên, mô-đun RC522 có 8 thiết bị đầu cuối mà chúng ta sẽ kết nối với Arduino UNO. Vì RC522 yêu cầu điện áp hoạt động trong phạm vi 2.5-3.3V, do đó đầu cuối VCC của mô-đun RC522 sẽ chung với chân 3.3V của Arduino UNO. Tương tự như vậy, cả hai thiết bị sẽ có điểm chung.



Hình 3.4: Arduino UNO nối với module RFID RC522

Giao tiếp SPI giúp giao tiếp với mô-đun đầu đọc RFID, phổ biến trong mọi bộ vi điều khiển. Vì vậy, chúng tôi sẽ sử dụng giao diện SPI của Arduino UNO. Dưới đây, bạn có thể xem các chân SPI của Arduino UNO.



Hình 3.5: Arduino UNO

Cách kết nối giữa 2 thiết bị:

Module RFID RC522	Arduino UNO
3V3	3V3
RST	Chân 9
GND	GND
IRQ	Không được kết nối
MISO	Chân 12
MOSI	Chân 11
SCK	Chân 13
SDA	Chân 10

Hình 3.6: Cách nối chân module RFID RC522 và Arduino UNO

3.2 Triển khai

3.2.1 Phần mềm

IDE: Arduino IDE version 2.1.0

Thư viện cài đặt:

- RFID: <https://github.com/miguelbalboa/rfid>

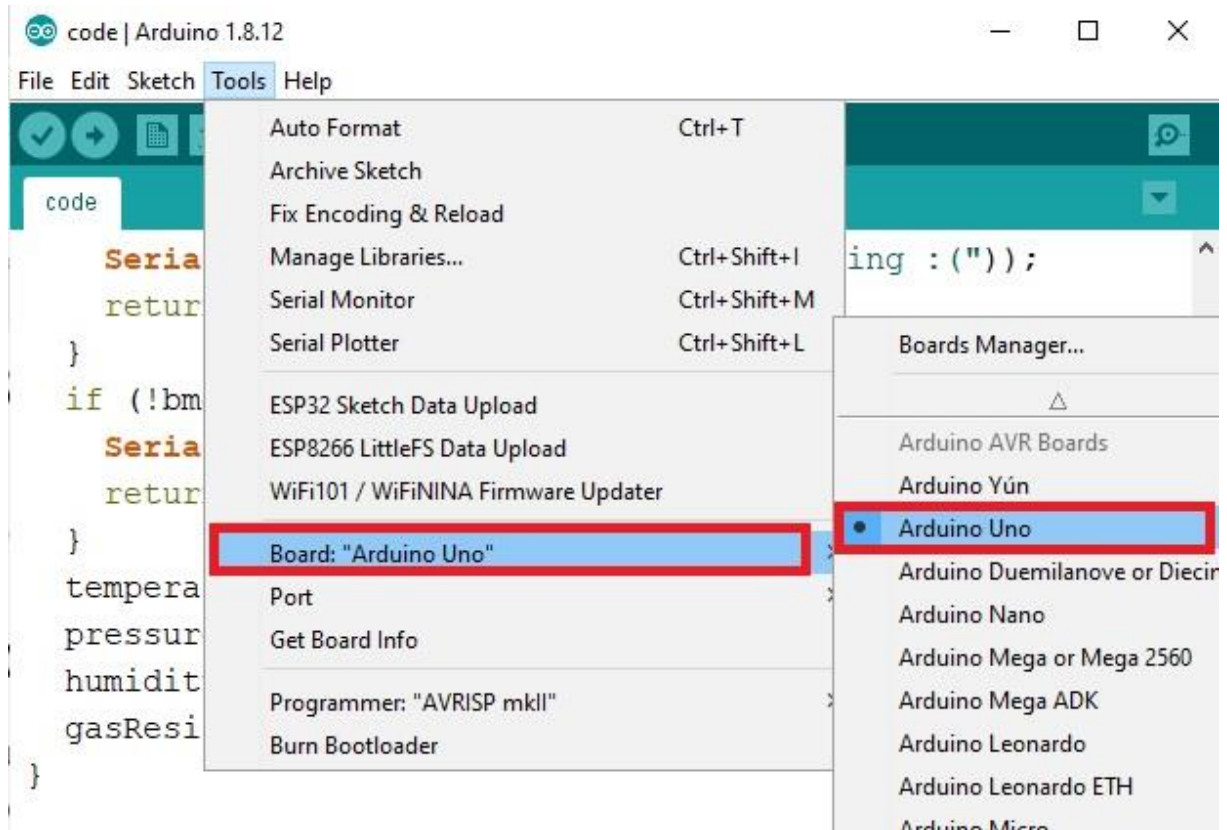
- SPI: <https://github.com/PaulStoffregen/SPI>

Ngôn ngữ lập trình: C/C++

3.2.2 Kịch bản

Các bước thực hiện chung:

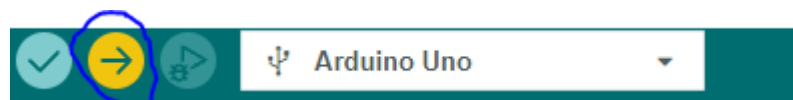
1. Chọn board Arduino Uno



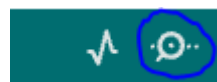
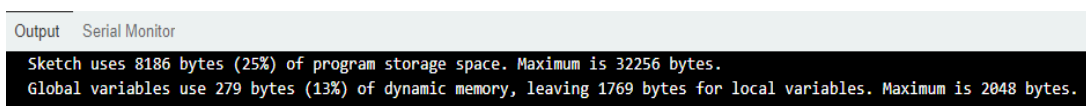
Hình 3.7: Chọn board Arduino Uno

2. Chèn đoạn code

3. Upload code

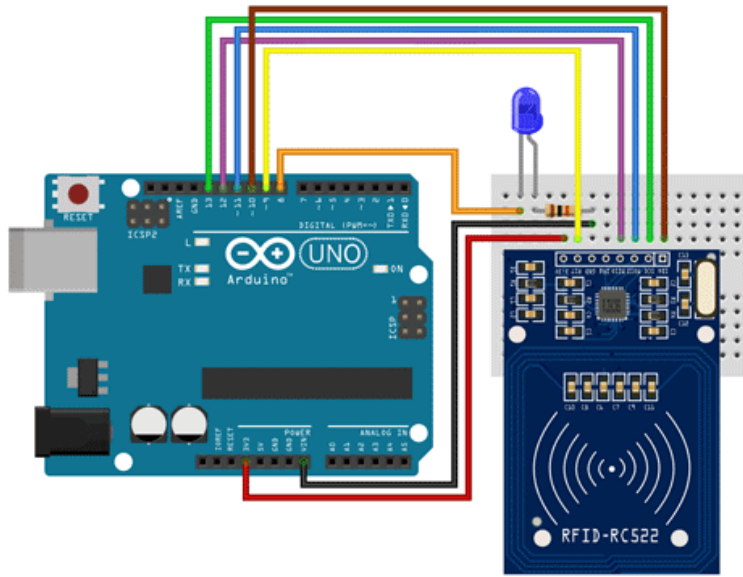


Output:



4. Chọn Serial Monitor để chạy code

5. Chạm thẻ vào module RFID RC522



Hình 3.8: Chạm thẻ vào module RFID RC522

6. Xem kết quả tại tab Serior Monitor

3.2.2.1 Đọc thẻ

Bây giờ sau khi lắp ráp mô-đun đầu đọc RFID RC522 và bảng Arduino UNO, tiến hành phác thảo ví dụ từ thư viện MFRC522 để đọc thẻ RFID.

Mở Arduino IDE và đi tới File > Examples > MFRC522 > DumpInfo. Mã chương trình sau sẽ mở ra. Bản phác thảo ví dụ này sẽ hiển thị thông tin về thẻ RFID.

Code

```
1. #include <SPI.h>
2. #include <MFRC522.h>
3.
4. #define RST_PIN      9           // Configurable, see typical pin layout above
5. #define SS_PIN       10          // Configurable, see typical pin layout above
6.
7. MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance
8.
9. void setup() {
10.     Serial.begin(9600);          // Initialize serial communications with the PC
11.     while (!Serial);             // Do nothing if no serial port is opened (added for
    Arduinos based on ATMEGA32U4)
12.     SPI.begin();                 // Init SPI bus
13.     mfrc522.PCD_Init();          // Init MFRC522
14.     delay(4);                   // Optional delay. Some board do need more time after
    init to be ready, see Readme
```

```

15.   mfr522.PCD_DumpVersionToSerial(); // Show details of PCD - MFRC522 Card Rea
    der details
16.   Serial.println(F("Scan PICC to see UID, SAK, type, and data blocks..."));
17. }
18.
19. void loop() {
20.   // Reset the loop if no new card present on the sensor/reader. This saves the
    entire process when idle.
21.   if ( ! mfr522.PICC_IsNewCardPresent() ) {
22.     return;
23.   }
24.
25.   // Select one of the cards
26.   if ( ! mfr522.PICC_ReadCardSerial() ) {
27.     return;
28.   }
29.
30.   // Dump debug info about the card; PICC_HaltA() is automatically called
31.   mfr522.PICC_DumpToSerial(&(mfr522.uid));
32. }

```

Giải thích

Trong đoạn code trên, chúng ta sử dụng thư viện SPI và MFRC522 để làm việc với module đọc thẻ RFID RC522.

#include <SPI.h> và **#include <MFRC522.h>**: Đây là lệnh để nạp các thư viện cần thiết để làm việc với module RFID RC522 thông qua giao tiếp SPI.

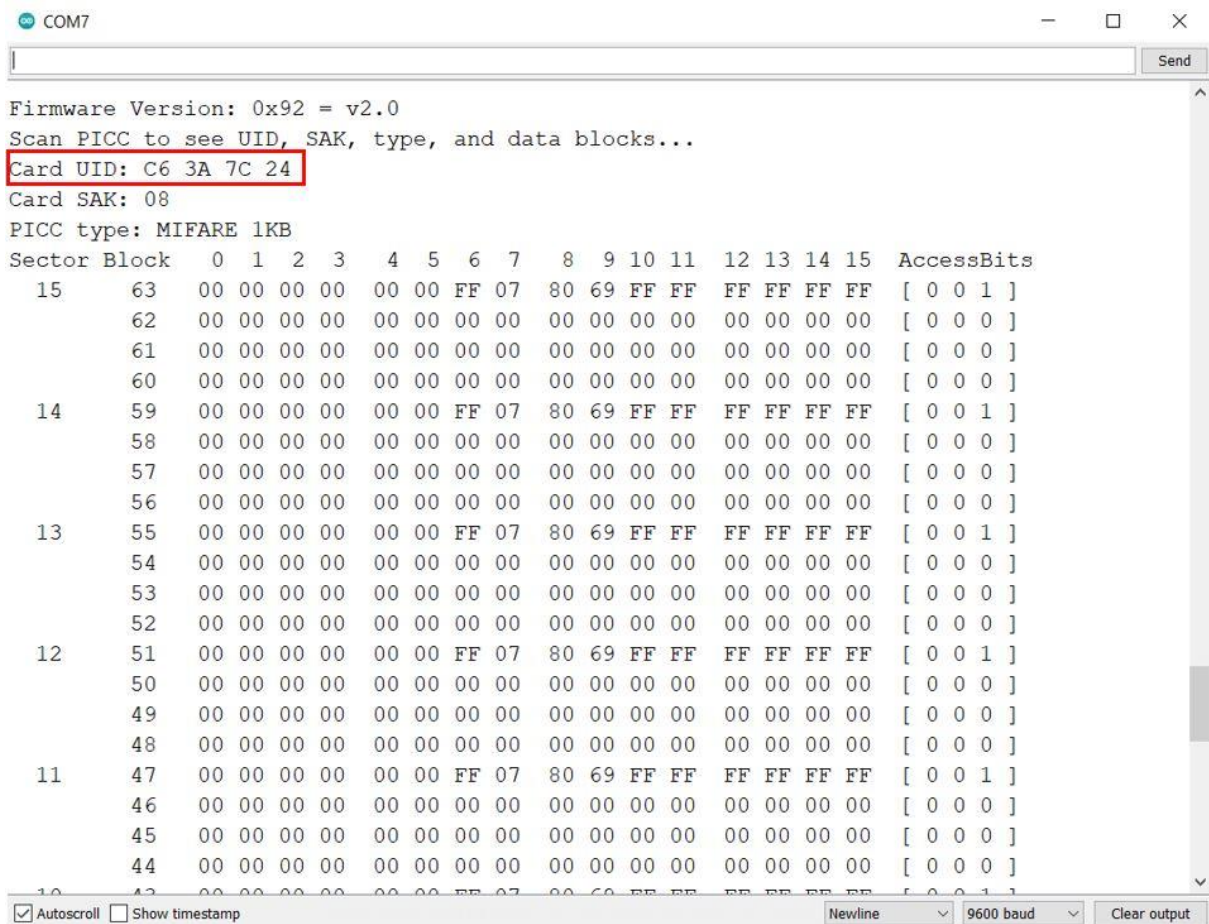
#define RST_PIN 9 và **#define SS_PIN 10**: Đây là khai báo các chân kết nối giữa Arduino và module RC522. Chúng có thể được cấu hình lại theo mạch cụ thể.

MFRC522 mfr522(SS_PIN, RST_PIN): Đây là khởi tạo một đối tượng MFRC522 với các chân kết nối đã được khai báo ở trên

void setup(): Hàm này được gọi một lần duy nhất khi Arduino khởi động. Trong hàm này, chúng ta thiết lập giao tiếp serial, giao tiếp SPI, khởi tạo module RC522 và hiển thị thông tin chi tiết về module RC522 lên serial monitor.

void loop(): Hàm này được thực thi lặp lại. Trong hàm này, chúng ta kiểm tra xem có thẻ RFID mới nào được đặt lên module hay không. Nếu có, chúng ta đọc thông tin của thẻ và hiển thị lên serial monitor bằng cách sử dụng hàm **mfr522.PICC_DumpToSerial()**. Sau khi đọc thông tin, thẻ sẽ được hủy bằng cách gọi hàm **mfr522.PICC_HaltA()** tự động.

Kết quả



```
COM7
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: C6 3A 7C 24
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 [ 0 0 0 ]
      61  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 [ 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 [ 0 0 0 ]
      57  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 [ 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 [ 0 0 0 ]
      53  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 [ 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 [ 0 0 0 ]
      49  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      48  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
11      47  00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]
      46  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      45  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      44  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
10      43  00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]
      42  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      41  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      39  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      38  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      37  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      36  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      35  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      34  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      33  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      32  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      31  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      29  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      28  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      27  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      26  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      25  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      24  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      23  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      22  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      21  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      19  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      18  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      17  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      16  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      15  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      14  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      13  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      12  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      11  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      09  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      08  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      07  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      06  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      05  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      04  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      03  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      02  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      01  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
      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 3.9: Kết quả đọc thẻ RFID

Các thông số được cung cấp là thông tin cụ thể về thẻ thông minh MIFARE 1KB. Dưới đây là giải thích chi tiết về các thông số:

1. Card UID (Unique Identifier): C6 3A 7C 24

Card UID là mã duy nhất được gắn vào thẻ và được sử dụng để định danh duy nhất cho thẻ trong hệ thống. Mỗi thẻ MIFARE 1KB có một UID riêng, không trùng lặp với các thẻ khác.

2. Card SAK (Select Acknowledge): 08

Card SAK là một byte trong trường dữ liệu của thẻ và thông báo cho thiết bị đọc về khả năng và chức năng hỗ trợ của thẻ MIFARE 1KB. SAK được sử dụng để xác định loại thẻ và tính năng của thẻ trong quá trình giao tiếp.

3. PICC type: MIFARE 1KB

PICC (Proximity Integrated Circuit Card) là thuật ngữ được sử dụng để chỉ thẻ thông minh. Trong trường hợp này, PICC type cho biết loại thẻ là MIFARE 1KB. Đây

là một loại thẻ thông minh có dung lượng lưu trữ 1 kilobyte và thuộc công nghệ MIFARE được phát triển bởi NXP Semiconductors. Thẻ MIFARE 1KB được sử dụng rộng rãi trong các ứng dụng như thẻ đôi tác, thẻ thông qua, thẻ thanh toán và nhiều ứng dụng khác.

Tóm lại, thông số trên cung cấp thông tin về một thẻ thông minh MIFARE 1KB cụ thể, bao gồm Card UID (mã duy nhất của thẻ), Card SAK (thông tin về chức năng hỗ trợ của thẻ) và loại thẻ (MIFARE 1KB).

3.2.2.2 Xác thực 1 yếu tố

Dựa vào UID đã đọc được ở trên, xác thực thẻ với UID có sẵn:

Code

```
1. #include <SPI.h>
2. #include <MFRC522.h>
3.
4. #define SS_PIN 10
5. #define RST_PIN 9
6. MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance.
7.
8. void setup()
9. {
10.   Serial.begin(9600); // Initiate a serial communication
11.   SPI.begin(); // Initiate SPI bus
12.   mfrc522.PCD_Init(); // Initiate MFRC522
13.   Serial.println("Approximate your card to the reader...");
14.   Serial.println();
15.
16. }
17. void loop()
18. {
19.   // Look for new cards
20.   if ( ! mfrc522.PICC_IsNewCardPresent())
21.   {
22.     return;
23.   }
24.   // Select one of the cards
25.   if ( ! mfrc522.PICC_ReadCardSerial())
26.   {
27.     return;
28.   }
29.   //Show UID on serial monitor
30.   Serial.print("UID tag :");
31.   String content= "";
32.   byte letter;
33.   for (byte i = 0; i < mfrc522.uid.size; i++)
34.   {
35.     Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
36.     Serial.print(mfrc522.uid.uidByte[i], HEX);
37.     content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
38.     content.concat(String(mfrc522.uid.uidByte[i], HEX));
39.   }
40.   Serial.println();
41.   Serial.print("Message : ");
42.   content.toUpperCase();
```



```

43.   if (content.substring(1) == "90 BD DB 20") //change here the UID of the car
      d/cards that you want to give access
44.   {
45.       Serial.println("Authorized access");
46.       Serial.println();
47.       delay(3000);
48.   }
49.
50.   else {
51.       Serial.println(" Access denied");
52.       delay(3000);
53.   }
54. }

```

Giải thích

#include <SPI.h> và ***#include <MFRC522.h>***: Đây là lệnh để nạp các thư viện cần thiết để làm việc với module đọc thẻ RFID RC522 thông qua giao tiếp SPI.

#define SS_PIN 10 và ***#define RST_PIN 9***: Đây là khai báo các chân kết nối giữa Arduino và module RC522. Chúng có thể được cấu hình lại theo mạch cụ thể.

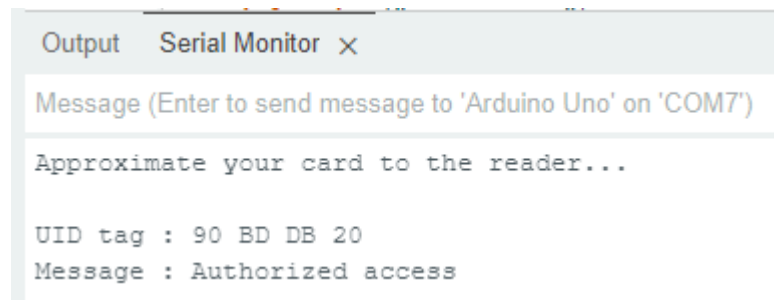
MFRC522 mfrc522(SS_PIN, RST_PIN): Đây là khởi tạo một đối tượng MFRC522 với các chân kết nối đã được khai báo ở trên.

void setup(): Hàm này được gọi một lần duy nhất khi Arduino khởi động. Trong hàm này, chúng ta thiết lập giao tiếp serial, giao tiếp SPI và khởi tạo module RC522. Đồng thời, chúng ta hiển thị thông báo "Approximate your card to the reader..." lên serial monitor.

void loop(): Hàm này được thực thi lặp lại. Trong hàm này, chúng ta kiểm tra xem có thẻ RFID mới nào được đặt lên module hay không. Nếu có, chúng ta đọc thông tin của thẻ, hiển thị UID lên serial monitor và so sánh với giá trị ***"90 BD DB 20"***. Nếu giá trị UID trùng khớp, hiển thị thông báo ***"Authorized access"*** lên serial monitor và đợi 3 giây. Ngược lại, hiển thị thông báo ***"Access denied"*** lên serial monitor và đợi 3 giây.

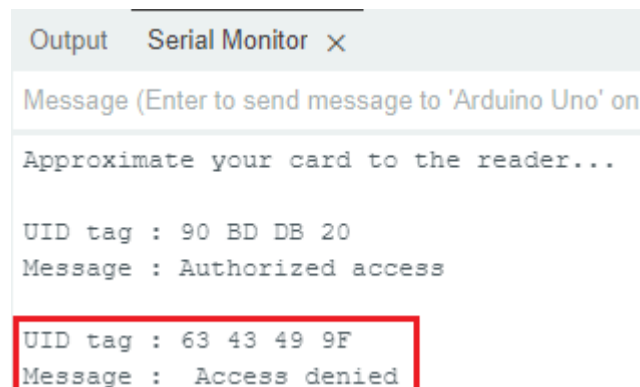
Kết quả

UID thẻ trùng khớp, xác thực thành công:



Hình 3.10: Xác thực 1 yếu tố thành công

Sử dụng 1 thẻ khác, xác thực không thành công:



Hình 3.11: Xác thực 1 yếu tố thất bại

3.2.2.3 Xác thực 2 yếu tố với mật khẩu

Dựa vào đoạn code trên, bây giờ thêm chức năng xác thực bằng mật khẩu. Như vậy để xác thực thành công, cần dùng đúng thẻ đã nhập UID và mật khẩu đã cài đặt.

Code

```

1. #include <SPI.h>
2. #include <MFRC522.h>
3.
4. #define SS_PIN 10
5. #define RST_PIN 9
6. MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance.
7.
8. #define PASSWORD "1234" // Mật khẩu được đặt là "1234"
9.
10. void setup()
11. {
12.   Serial.begin(9600); // Khởi tạo giao tiếp serial
13.   SPI.begin(); // Khởi tạo bus SPI
14.   mfrc522.PCD_Init(); // Khởi tạo MFRC522
15.   Serial.println("Approximate your card to the reader...");
16.   Serial.println();
17. }
18.
19. void loop()

```



```

20. {
21.     // Tìm kiếm thẻ mới
22.     if (!mfr522.PICC_IsNewCardPresent())
23.     {
24.         return;
25.     }
26.
27.     // Chọn một trong các thẻ
28.     if (!mfr522.PICC_ReadCardSerial())
29.     {
30.         return;
31.     }
32.
33.     // Hiển thị UID trên serial monitor
34.     Serial.print("UID tag: ");
35.     String content = "";
36.     for (byte i = 0; i < mfr522.uid.size; i++)
37.     {
38.         Serial.print(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " ");
39.         Serial.print(mfr522.uid.uidByte[i], HEX);
40.         content.concat(String(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " "));
41.         content.concat(String(mfr522.uid.uidByte[i], HEX));
42.     }
43.     Serial.println();
44.
45.     // Kiểm tra mật khẩu
46.     Serial.print("Enter password: ");
47.     while (Serial.available() <= 0); // Đợi người dùng nhập mật khẩu
48.     String password = Serial.readStringUntil('\n'); // Đọc dữ liệu từ Serial
49.     password.trim(); // Xóa khoảng trắng đầu và cuối chuỗi
50.
51.     if (password == PASSWORD) // So sánh mật khẩu nhập vào với mật khẩu đúng
52.     {
53.         Serial.println("Authorized access");
54.         Serial.println();
55.         delay(3000);
56.     }
57.     else
58.     {
59.         Serial.println("Access denied");
60.         delay(3000);
61.     }
62. }

```

Giải thích

#include <SPI.h> và **#include <MFRC522.h>**: Đây là thư viện cần thiết để sử dụng module MFRC522.

#define SS_PIN 10 và **#define RST_PIN 9**: Định nghĩa chân kết nối của module MFRC522 với Arduino.

MFRC522 mfr522(SS_PIN, RST_PIN): Khởi tạo một đối tượng MFRC522 để tương tác với module.

#define PASSWORD "1234": Định nghĩa mật khẩu cho việc xác thực.

Serial.begin(9600): Khởi tạo giao tiếp Serial với baud rate 9600 để giao tiếp với Serial Monitor.

SPI.begin(): Khởi tạo bus SPI để giao tiếp với module MFRC522.

mfrfc522.PCD_Init(): Khởi tạo module MFRC522.

mfrfc522.PICC_IsNewCardPresent(): Kiểm tra xem có thẻ mới được đặt lên module hay không.

mfrfc522.PICC_ReadCardSerial(): Đọc dữ liệu từ thẻ và lưu trữ nó trong đối tượng MFRC522.

Serial.print("UID tag: ") và *Serial.print(mfrfc522.uid.uidByte[i], HEX)*: Hiển thị UID (Unique Identifier) của thẻ lên Serial Monitor dưới dạng mã HEX.

Serial.print("Enter password: ") và *Serial.readStringUntil('\n')*: Yêu cầu người dùng nhập mật khẩu từ Serial Monitor và đọc dữ liệu được nhập vào.

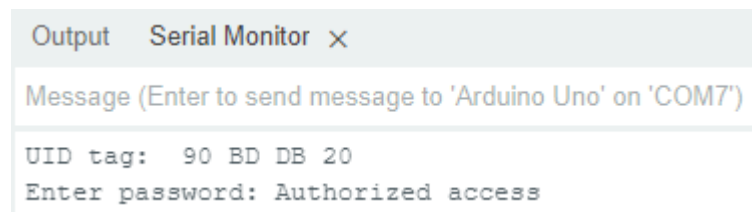
password.trim(): Xóa các khoảng trắng đầu và cuối chuỗi mật khẩu.

if (password == PASSWORD): So sánh mật khẩu nhập vào với mật khẩu đã được định nghĩa.

Nếu mật khẩu nhập vào trùng khớp với mật khẩu đã được định nghĩa, thông báo "Authorized access" sẽ được hiển thị và chương trình sẽ chờ 3 giây trước khi tiếp tục. Ngược lại, thông báo "Access denied" sẽ được hiển thị và chương trình cũng sẽ chờ 3 giây trước khi tiếp tục.

Kết quả

Trường hợp 1: đúng thẻ, đúng mật khẩu, xác thực thành công

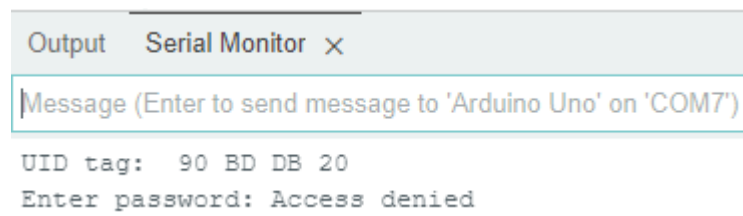


Hình 3.12: Xác thực 2 yếu tố thành công

Trường hợp 2: đúng thẻ, sai mật khẩu, xác thực thất bại

Trường hợp 3: sai thẻ, đúng mật khẩu, xác thực thất bại

Trường hợp 4: sai thẻ, sai mật khẩu, xác thực thất bại



Hình 3.13: Xác thực 2 yếu tố thất bại

Tài liệu tham khảo

- [1] RFC 4226: “HOTP: An HMAC-Based One-Time Password Algorithm”, IETF, D. M'Raihi (VeriSign), M. Bellare (UCSD), F. Hoornaert (Vasco), D. Naccache (Gemplus), O. Ranen (Aladdin), December 2005.
- [2] RFC 6238: “TOTP: Time-Based One-Time Password Algorithm”, IETF, ISSN: 2070 – 1721, D. M'Raihi (Verisign, Inc.), S. Machani (Diversinet Corp.), M. Pei (Symantec), J. Rydell (Portwise, Inc.), May 2021.
- [3] <https://pinonote.wordpress.com/2018/11/27/thuat-toan-hmac-based-one-time-password-algorithm-hotp-va-time-based-one-time-password-totp-trong-google-authenticator/>
- [4] <https://viblo.asia/p/tong-quan-ve-the-thong-minh-smart-card-eW65GryRlDO>
- [5] <https://randomnerdtutorials.com/security-access-using-mfrc522-rfid-reader-with-arduino/>
- [6] <https://circuitdigest.com/microcontroller-projects/interfacing-rfid-reader-module-with-arduino>
- [7] <https://mecsuvn.com/ho-tro-ky-thuat/modun-doc-rfid-rc522-voi-arduino.w6o>
- [8] <https://github.com/miguelbalboa/rfid>
- [9] <https://github.com/PaulStoffregen/SPI>