BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH : CÔNG NGHỆ THÔNG TIN

Sinh viên : Trần Minh Quang

Giảng viên hướng dẫn: TS Hồ Văn Canh

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

TÌM HIỂU VẤN ĐỀ BẢO MẬT THÔNG TIN TRÊN HỆ THỐNG ATM (Automatic Teller Machine)

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

NGÀNH: CÔNG NGHỆ THÔNG TIN

Sinh viên : Trần Minh Quang

Giảng viên hướng dẫn: TS Hồ Văn Canh

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên: Trần Minh Quang **Mã SV**: 1712112002

Lớp : CT2201M **Ngành** : Công nghệ thông tin

Tên đề tài: Tìm hiểu vấn đề bảo mật thông tin trên hệ thống ATM (Automatic Teller Machine)

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

…….

…….

…….

…….

…….

…….

2. Các tài liệu, số liệu cần thiết

…….

…….

…….

…….

…….

…….

…….

…….

…….

3. Địa điểm thực tập tốt nghiệp

…….

LỜI CẢM ƠN

Trong lời đầu tiên của báo cáo Đồ án tốt nghiệp "Nghiên cứu, tìm hiểu hệ thống rút tiền tự động ATM và vấn đề ATTT cho hệ thống" này, em muốn gửi lời cảm ơn và biết ơn chân thành nhất của mình tới tất cả những người đã hỗ trợ, giúp đỡ em về kiến thức cũng như tinh thần trong quá trình thực hiện Đề án.

Trước hết em xin gửi lời cảm ơn đến TS Hồ Văn Canh, người thầy đã hướng dẫn em rất nhiều trong suốt quá trình tìm hiểu và hoàn thành đồ án này từ lý thuyết đến ứng dụng của hệ thống ATM.

Đồng thời em cũng xin chân thành cảm ơn các thầy cô trong bộ môn cũng như các thầy cô trong trường đã trang bị cho em những kiến thức cơ bản cần thiết để em có thể hoàn thành tốt đồ án này.

Cuối cùng em xin gửi lời cảm ơn đến gia đình, bạn bè, người thân đã giúp đỡ động viên em rất nhiều trong quá trình học tập và làm Đồ án Tốt Nghiệp.

Do thời gian có hạn, kiến thức còn nhiều hạn chế nên Đồ án thực hiện chắc chắn không tránh khỏi những thiếu sót nhất định. Em rất mong nhận được ý kiến đóng góp của thầy cô và các bạn để em có thêm kinh nghiệm và tiếp tục hoàn thiện Đồ án của mình.

Em xin chân thành cảm ơn!

Hải Phòng, ngày tháng năm 2022

Sinh viên thực hiện

Trần Minh Quang

DANH MỤC NHỮNG TỪ VIẾT TẮT ATM

ATM: Automatic Teller Machine

BIN: Bank Identification Number

CVK: Card Verification Keys

CD: Check Digitp

CSDL: Cơ sở dữ liệu

DES: Data Encryption Standard

3DES: Triple DES

EMV: Europay, MasterCard, Visa

EPP: Encrypt PIN Pad

HSM: Hardware Security Module

ISO: International Organization for Standardization

KME (MEK): Message Encryption Keys

LMK: Local Master Keys

MD: Message Digest Algorithm

MAC: Message Authentication Code

PC: Personal Computer

POS: Point Of Service

PIN: Personal Identification Number

PAN: Primary Account Number

PVV: VISA PIN Verification Keys

PVK: PIN Verification Keys

RSA: Rivest, Shamir And Adleman

TMK: Terminal Master Keys

WK: Working Keys

LỜI MỞ ĐẦU

Ngày nay, công nghệ ATM đang được ứng dụng rộng rãi trên phạm vi toàn thế giới và cả ở Việt Nam. Khái niệm máy rút tiền ATM cũng không còn xa lạ trong cuộc sống của ngọời dân Việt Nam. Những tiện ích mà các dịch vụ thẻ mang lại đã góp phần từng bước thay đổi thói quen qua sử dụng tiền mặt của người dân, giảm chi phí xã hội, nâng cao khả năng quản lý tiền tệ của Nhà nước cũng như góp phần hữu ích vào việc tạo dựng nền móng cho sự hình thành một nền thương mại điện tử còn non trẻ của nước ta.

Tuy nhiên, một vấn đề bức xúc cũng được đặt ra là làm thế nào để đảm bảo an toàn tuyệt đối cho hệ thống và cả người dùng, chống lại mọi sự gian lận, ăn cắp tài khoản … của người dùng.

Với các vấn đề như trên, em chọn đề tài là "Nghiên cứu, tìm hiểu hệ thống rút tiền tự động ATM và vấn đề ATTT của hệ thống" nhằm mục đích nghiên cứu cơ chế hoạt động, độ an toàn và tính bảo mật của hệ thống ATM, phân tích đánh giá, ọu nhọợc điểm của công nghệ hiện tại đang sử dụng, nhằm mục tiêu đề ra giải pháp tối ưu hơn giúp cho tính bảo mật và an toàn của hệ thống được nâng cao.

Ngoài các phần mở đầu, lời cảm ơn, tài liệu tham khảo, luận văn gồm có 5 chương và phần kết luận.

Chương 1. Tổng quan về máy ATM và hệ thống thanh toán tự động ATM.

Chương 2. Hệ thống thanh toán ATM cho thẻ từ và thẻ chip.

Chương 3. Cơ chế bảo mật và an toàn thông tin trên hệ thống ATM.

Chương 4. Đề xuất giải pháp đảm bảo tính an toàn, bảo mật thông tin cho hệ thống ATM

MỤC LỤC

CHƯƠNG 1 TỔNG QUAN VỀ MÁY ATM VÀ HỆ THỐNG THANH TOÁN TỰ ĐỘNG ATM

1. Sự phát triển của máy ATM.

Máy rút tiền đầu tiên trên thế giới được thiết kế và hoàn thành bởi Luther George Simjian (người Thổ Nhĩ Kỳ), vào năm 1939, máy được thiết kế tại thành phố NewYork cho Ngân hàng City Bank of NewYork, nhưng 6 tháng sau thì bị bỏ đi vì ít người dùng.

Sau 25 năm, vào ngày 27/6/1967, máy rút tiền điện tử đầu tiên được hãng In De la Rue thiết kế tại Enfield Town (gần London Anh) cho Ngân hàng Barclays Bank. Người phát minh là John Shepherd-Barron mặc dù Luther George Simjian và một vài người khác cũng đã đăng ký văn bằng phát minh cho loại máy này. Tuy nhiên, nhiều người cho rằng loại máy ATM đầu tiên theo đúng nghĩa ATM mà thế giới ngày nay đang sử dụng chính là loại máy được ra mắt vào năm 1969 tại Ngân hàng Chemical Bank ở NewYork (Mỹ). Tác giả là Don Wetzel, phó giám đốc một công ty chuyên về máy tự động xử lý hành lý.

ATM ngày nay là thiết bị để Ngân hàng giao dịch tự động với chủ thẻ, thực hiện thông qua các loại thẻ ATM như thẻ ghi nợ, thẻ ghi có (thẻ tín dụng), và các loại thẻ khác, giúp chủ thẻ kiểm tra tài khoản, rút tiền mặt, chuyển khoản thanh toán hàng hóa, dịch vụ. (*theo báo Tin học và Tài chính - Bộ tài chính số 58, tháng 4/2008*).

2. Tình hình sử dụng máy ATM.

Thanh toán tiền qua hệ thống ATM đã phổ biến trên toàn thế giới và ở Việt Nam hệ thống ATM dần trở nên quen thuộc với mọi người dân.

Năm 1993, thị trường thẻ Việt Nam mới xuất hiện những sản phẩm thẻ đầu tiên do Vietcombank phát hành, đến năm 1996 thì thị trưởng thẻ thực sự xuất hiện.

Năm 1996, ngân hàng ngoại thương Vietcombank kết hợp cùng ngân hàng nhà nước triển khai lắp đặt 2 chiếc máy rút tiền tự động tại Hà Nội.

Đến nay, chúng ta đã chứng kiến sự phát triển vượt bậc của thị trưởng thẻ và máy ATM tại Việt Nam: với hơn 20 ngân hàng thương mại phát hành Thẻ nội địa, trong đó có 8 Ngân hàng phát hành thẻ Quốc tế.

Năm	Số lượng thẻ phát hành Gồm thẻ nội địa và quốc tế Đơn vị: chiếc	Số máy ATM
1996	360	
1997	460	
1998	4.500	
1999	2.500	
2000	5.000	
2001	15.000	
2002	40.000	
2003	230.000	
2004	560.000	
2005	1.250.000	
T6/2006	3.500.000	
2007	8.400.000	4.020
T3/2008	10.000.000	4500

Bảng 1.1: Số liệu thống kê thị trường thẻ Việt Nam qua các năm

(Theo hiệp hội ngân hang Việt Nam và hội thảo Banking Việt Nam 2008)

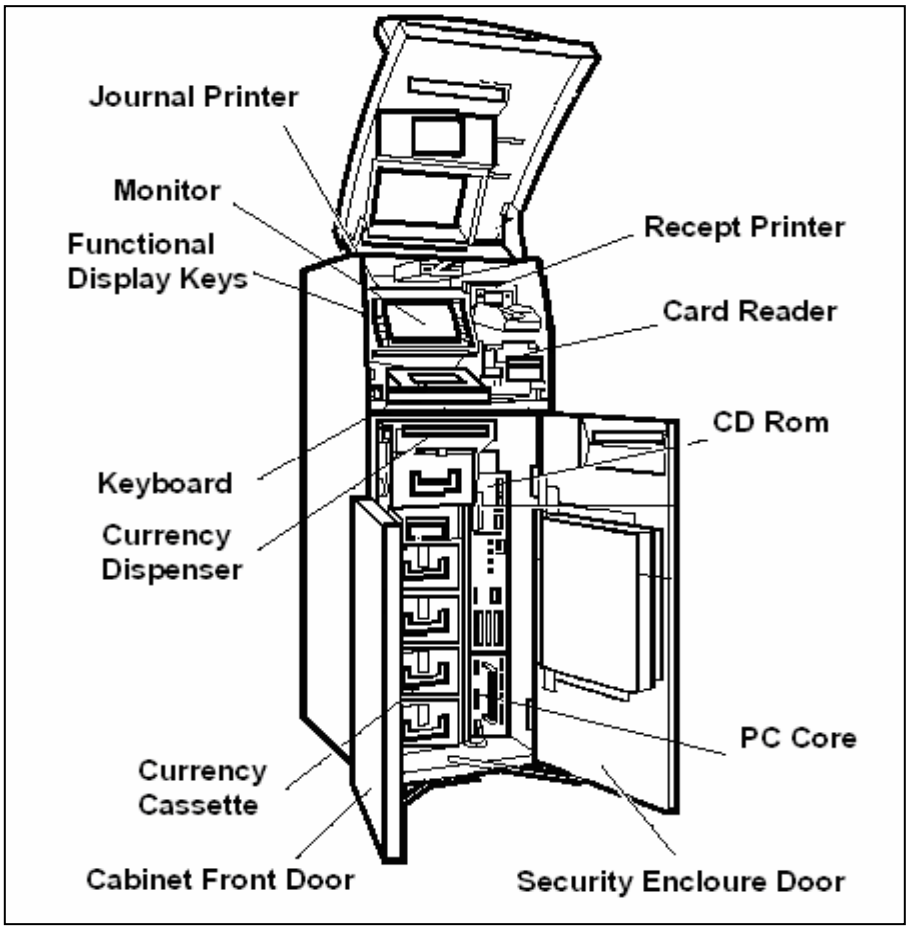
3. Định nghĩa máy ATM.

ATM là máy giao dịch tự động được gọi là hệ thống ngân hang tự động, không chỉ đơn thuần là máy rút tiền tự động mà còn có nhiều dịch vụ khác trên đó như chuyển khoản, thanh toán hóa đơn, các dịch vụ thương mại điện tử…được gọi là hệ thống giao dịch ngân hàng tự động.

Hình 1.1 Máy ATM nhìn từ phía trước

4. Cấu tạo của máy ATM.

ATM được coi như một thiết bị chuyên biệt được sử dụng trong lĩnh vực ngân hàng, nó là một kênh phục vụ tự động của ngân hàng, do đó nó cần có một cấu tạo đặc biệt để có thể thực hiện các chức năng được yêu cầu. Cấu tạo của máy ATM gồm 2 phần là phần cứng và phần mềm.

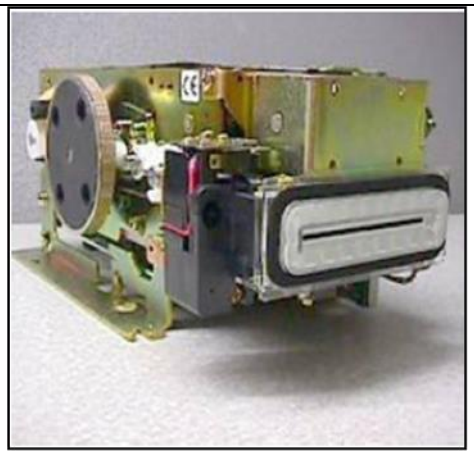


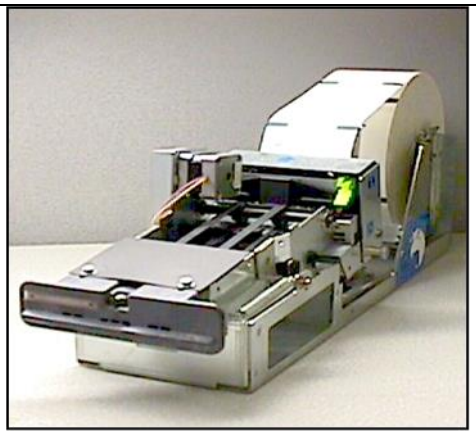
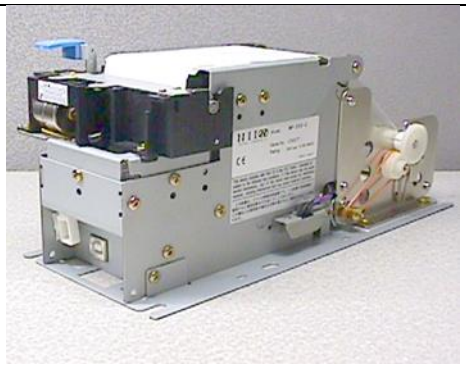
Hình 1.2 Cấu tạo cơ bản của một máy ATM.

4.1. Phần cứng.

Các thiết bị phần cứng có thể được chia như sau:

Thiết bị đầu vào	
Thiết bị đầu ra	

Máy tính điều khiển	
Thiết bị đọc thẻ	
Bàn phím	
Khe nhận tiền	
Màn hình hiển thị	

Thiết bị trả tiền và các khay chứa tiền	
Thiết bị in biên lai giao dịch	
Máy ghi nhật kí giao dịch	
Loa	

Bảng 1.2: Các thiết bị phần cứng cơ bản

Trong máy ATM các thiết bị phần cứng sử dụng các chuẩn giao tiếp sau để kết nối đến máy PC: SDC (Seria Direct Connect), RS 232, Parallel, PCI, ISA, USB

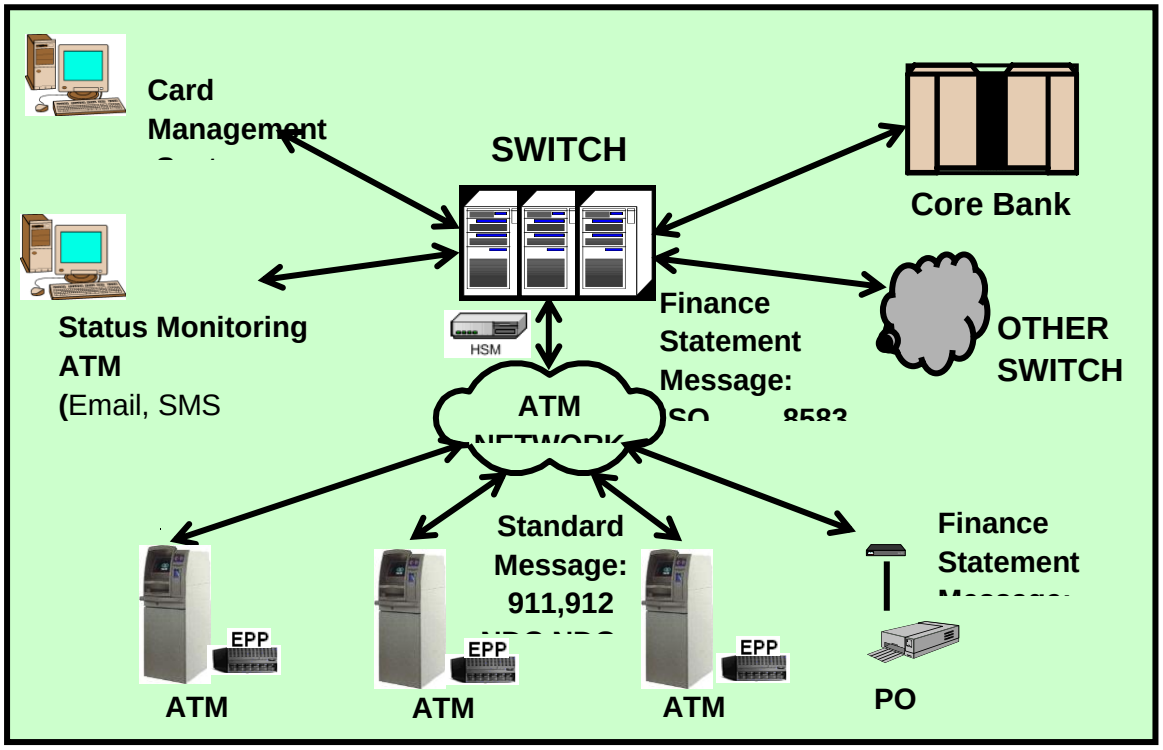
4.2. Phần mềm.

Hầu hết các loại máy ATM đều phải có hệ điều hành (OS-operate system), phần mềm điều khiển thiết bị của máy ATM và phần mềm tiện ích kèm theo. Hiện nay, hệ điều hành là Window NT, Window XP.

5. Cấu trúc hệ thống thanh toán ATM.

5.1. Tổng quan hệ thống thanh toán ATM.

Hệ thống ATM là hệ thống mạng gồm có các thành phần trung tâm như Switch, CoreBank và các hệ thống mạng viễn thông dùng để kết nối các thiết bị thanh toán nhằm giúp cho khách hàng truy cập thuận tiện các dịch vụ một cách nhanh chóng, dịch vụ 24/7 ở bất cứ nơi đâu và vào thời gian nào. Ngoài ra có thể kết nối đến hệ thống mạng của ngân hàng khác.



Hình 2.14 Sơ đồ mạng lưới ATM.

Core Bank: Hệ thống Ngân hàng cốt lõi, là nơi tập trung CSDL thông tin về ngân hàng và thông tin về tài khoản, kiểu tài khoản, số dư tài khoản, số hạn mức tài khoản của chủ thẻ tham gia vào hệ thống ngân hàng.

Switch: Là một hệ thống phần mềm và phần cứng (thường gọi là hệ thống chuyển mạch) được kết nối trực tiếp với Core bank và các thiết bị đầu cuối ATM, POS.

Switch rất quan trọng trong hệ thống ATM, cũng như các giao dịch tài chính khác. Switch là trung tâm của toàn bộ hệ thống, là một thành phần trung gian giữa ATM và cơ sở dữ liệu của ngân hàng. Mọi giao dịch từ ATM đều phải thông qua Switch.

Hệ thống này gồm một số chức năng sau:

- Chức năng quản lý thẻ (Card Management): Chức năng này cho phép kết nối đến hệ thống quản lý các thiết bị sản xuất thẻ, cho phép giám sát và quản lý các thẻ được phát hành.
- Chức năng kết nối các thiết bị đầu cuối như ATM, POS,…
- Chức năng giám sát và điều khiển toàn hệ thống.
- Ghi nhật kí và lưu vết giao dịch
- Hệ thống cung cấp các giao tiếp với các thiết bị mã hóa cứng HSM, đảm bảo mã hóa, giải mã số PIN và xác thực các thông điệp
- Kết nối đến các ngân hàng hay các tổ chức phát hành khác như VISA, MasterCard,…

ATM (Automatic Teller Machine): được biết như là một kênh tự phục vụ thông qua thẻ của ngân hàng, như cho phép rút tiền tự động, chuyển khoản, thanh toán hóa đơn, mua vé, các dịch vụ thương mại điện tử…

POS (Point of Service): được biết như là điểm thanh toán mua hàng bằng thẻ thanh toán.

Status Monitoring ATM: Cho phép quản lý và giám sát toàn bộ tình trạng hiện thời của các ATM theo các nhóm, theo vị trí địa lý…

5.2. Giao thức kết nối hệ thống ATM.

Mỗi ATM được coi như là một máy PC, do đó mỗi ATM có một địa chỉ IP xác định để có thể tham gia vào mạng. Có thể đặt địa chỉ IP tĩnh (static IP) hoặc IP động (dynamic IP).

Hiện nay máy ATM hỗ trợ các giao thức kết nối như: TCP/IP, X.25,...

Ở Việt nam máy ATM chủ yếu sử dụng giao thức TCP/IP để kết nối. Các giao thức này được hỗ trợ bởi các đường truyền thông như đường Lease-line, Dial-up, Mega Wan.

6. Lợi ích của việc sử dụng máy ATM.

Đối với ngân hàng:

ATM được biết đến như là một kênh tự phục vụ của ngân hàng, là một bộ phận chiến lược trong kênh phân phối của ngân hang giúp chủ thẻ truy cập một cách thuận tiện các dịch vụ một cách nhanh chóng, dịch vụ 24/7 ở bất cứ nơi đâu và vào thời gian nào.

ATM là một trong các kênh phân phối vụ bán lẻ của ngân hàng như: ATM, POS (point of service), Telephone banking, SMS .....

Bên cạnh đó, máy ATM còn có một số ưu điểm sau:

- Các địa điểm đặt máy thuận lợi, thời gian phục vụ 24/7 giúp dễ tiếp cận với các dịch vụ ngân hàng nên thu hút nhiều chủ thẻ hơn.
- Mỗi ATM có thể coi là một chi nhánh của Ngân hàng, do đó sẽ giảm thiểu chi phí vận hành chi nhánh Ngân hàng
- Hệ thống ATM là sự khác biệt về chất lượng phục vụ và nhãn hiệu để cạnh tranh với các ngân hàng khác.
- Giảm lượng tiền mặt lưu thông trên thị thường.

Đối với khách hàng:

- Thuận tiện trong tiếp cận ngân hàng
- Nhanh hơn là chờ đợi ở các quầy giao dịch

7. Các dịch vụ trên máy ATM.

- Rút tiền mặt (Card Withdrawal)
- Chuyển khoản (Fund Transfer)
- Tiện ích/ Thanh toán hóa đơn (Điện thoại, điện, nước..)
- Gửi tiền
- Các giao dịch internet thương mại điện tử, điện thoại, điện, nước..

CHƯƠNG 2: HỆ THỐNG THANH TOÁN ATM CHO THẺ TỪ VÀ THẺ CHIP

1. Hệ thống thanh toán cho thẻ từ.

1.1. Thẻ từ.

Là loại thẻ nhựa cứng, các thông tin về thẻ được lưu trên băng từ. Thẻ có thể thực hiện các giao dịch tự động như kiểm tra số dư, rút tiền, chuyển khoản,…từ máy rút tiền ATM.

1.1.1. Tính chất vật lí của thẻ

Các tính chất vật lý của thẻ từ (kích cỡ, khối lượng, cấu trúc vật liệu, tính chất cứng, tính mềm dẻo, tính bền …) tuân theo chuẩn ISO 7810

Chuẩn ISO 7810 là một tập các chuẩn mô tả các đặc tính vật lý và kích cỡ của thẻ.

- Thẻ có 4 loại kích thước khác nhau:

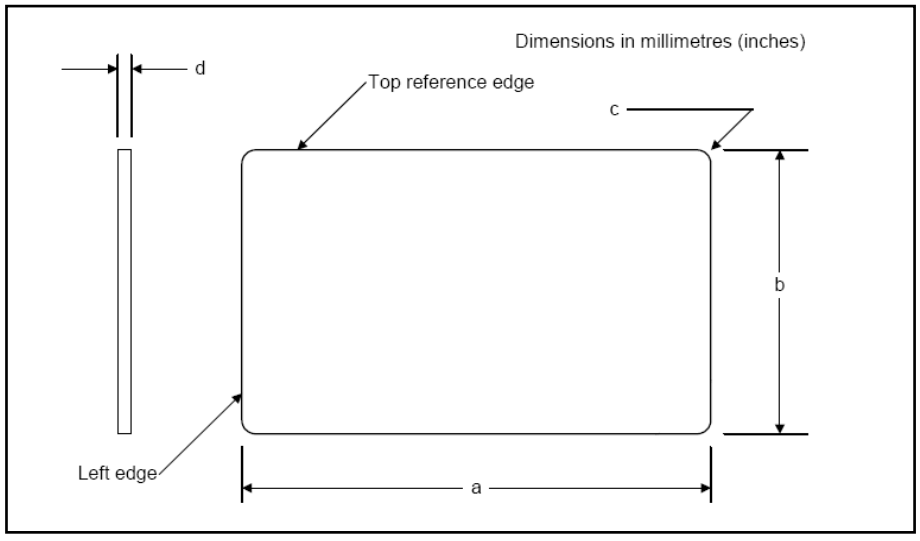
• ID-000: Dài 25 mm Rộng 15 mm Dày 0.76 mm,

• ID-1: Dài 85.60 mm Rộng 53,98 mm Dày 0.76 mm

• ID-2: Dài 105 mm Rộng 74 mm Dày 0.76 mm

• ID-3: Dài 125 mm Rộng 88 mm Dày 0.76 mm

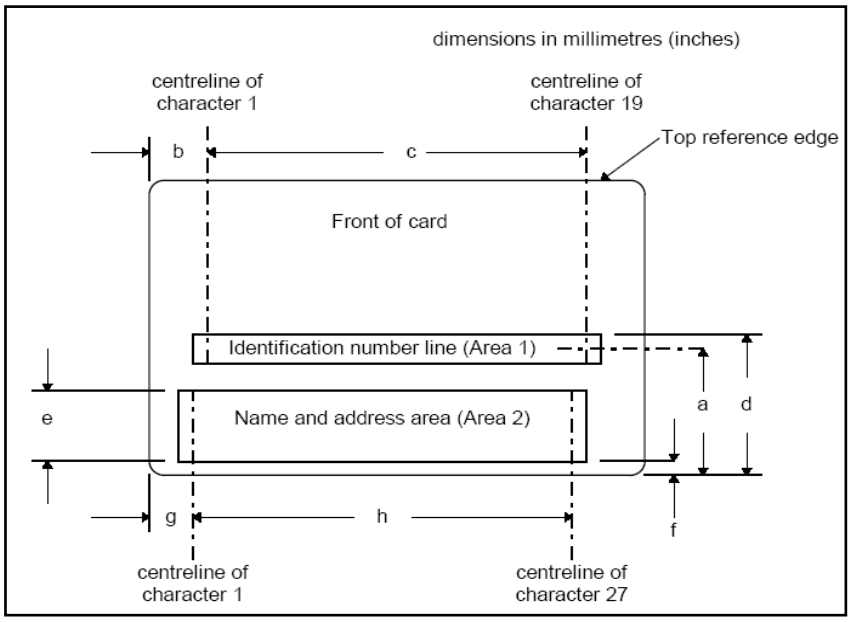
- Thẻ ATM là loại thẻ ID-1



Hình 2.1 Kích thước thẻ

1.1.2. Thông tin dập nổi trên thẻ

Các thông tin dập nổi trên thẻ tuân theo chuẩn ISO 7811-1



Hình 2.2 Các vị trí dập nổi trên thẻ (mặt trước)

Identification number line (Area 1)		**Name and address area (Area 2)**	
A	21,42 ± 0,12 (0.843 ± 0.005)	E	14,53 (0.572) maximum
B	10,18 ± 0,25 (0.401 ± 0.010)	F	2,54 (0.100) minimum 3,30 (0.130) maximum
C	65,31 ± 0,76 (2.571 ± 0.030)	G	7,65 ± 0,25 (0.301 ± 0.010)
D	24,03 (0.946) maximum	H	66,04 ± 0,76 (2.600 ± 0.030)

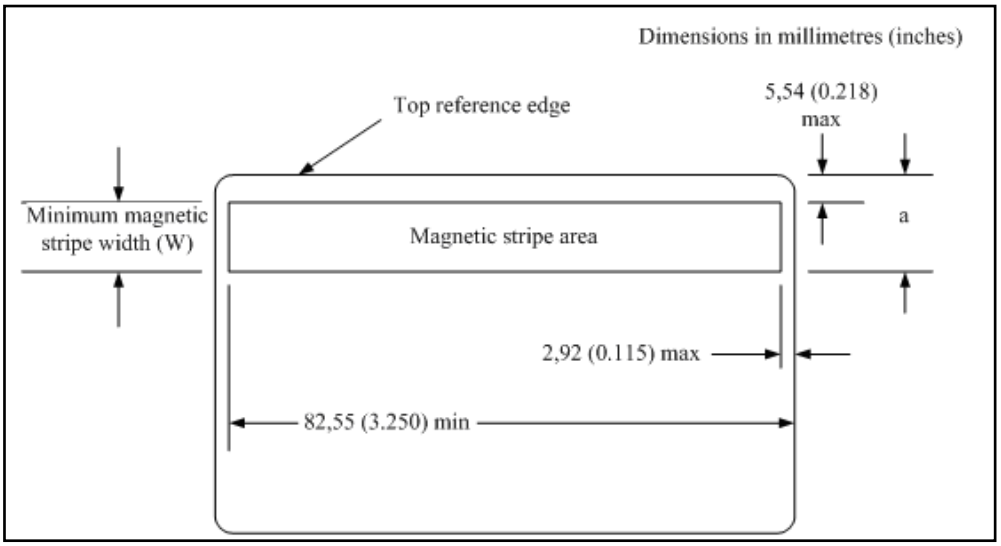
Bảng 2.1: Bảng định nghĩa kích thước vị trí dập nổi, đơn vị milimet (Inches)

Trên thẻ có 2 khu vực dập nổi:

- Khu vực 1 (Area 1) – được sử dụng để dập nổi số định dạng thẻ (Identification number).
- Khu vực 2 (Area 2) – được sử dụng để dập nổi tên, địa chỉ và các thông tin liên quan đến chủ thẻ.

1.1.3 Thông tin lưu trên vạch của thẻ

Các thông tin lưu trên vạch từ và cấu trúc các trường thông tin của thẻ tuân theo chuẩn ISO 7811-2, ISO 7811-6 và ISO 7813.

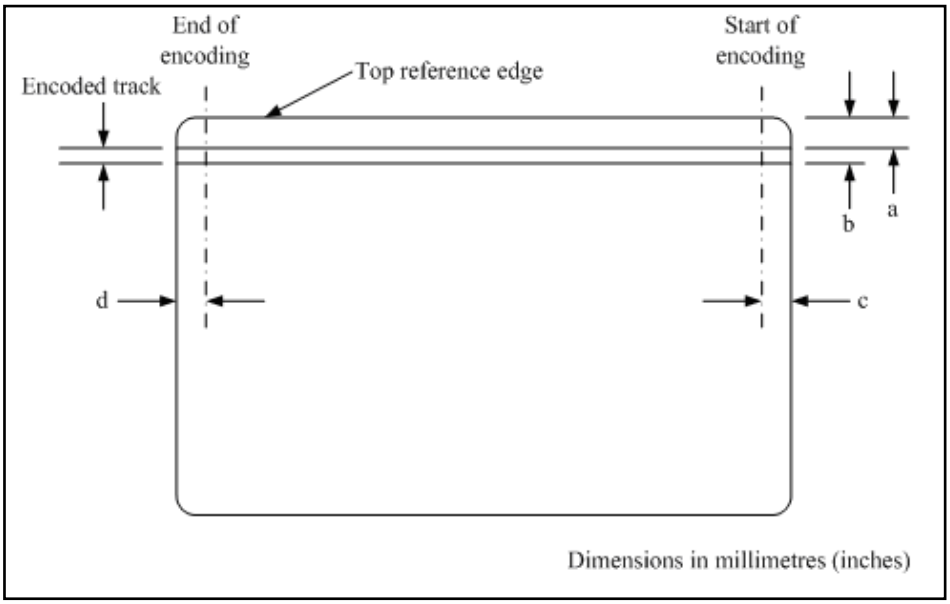


Hình 2.3 Vị trí dải từ (Mặt sau thẻ)

a = 11,89 (0.468): Khi sử dụng cho các tracks 1 và 2

a = 15,95 (0.628): Khi sử dụng cho các tracks 1, 2, và 3

Đơn vị milimet (inches)



Hình 2.4 Vị trí của các rãnh từ trong dải từ.

Term	Track 1	Track 2	Track 3
A	5,79 (0.228) maximum	8,33 (0.328) minimum 9,09 (0.358) maximum	11,63 (0.458) minimum 12,65 (0.498) maximum
B	8,33 (0.328) minimum 9,09 (0.358) maximum	11,63 (0.458) minimum 12,65(0.498) maximum	15,19 (0.598) minimum 15,82 (0.623) maximum
C	744 ± 1,00 (0.293 ± 0.039)	7,44 ± 0,50 (0.293 ± 0.020)	7,44 ± 1,00 (0.293 ± 0.039)
D	6,93 (0.252) minimum	6,93 (0.252) minimum	6,93 (0.252) minimum

Bảng 2.2: Bảng định nghĩa kích thước vị trí rãnh từ, đơn vị milimet (Inches)

Các chuẩn này quy định trên thẻ gồm 3 track nhưng thường chỉ được sử dụng track 1 và 2

- *Track 1* là track tuân theo chuẩn IATA (International Air Bansport Associantion). Đây là Track chỉ đọc, được ghi với mật độ cao và có thể chứa cả số lẫn ký tự chữ cái.
- *Track 2* là track tuân theo chuẩn ABA (America Banker Association). Đây là Track chỉ đọc với mật độ ghi thấp và chỉ chứa ký tự số.
- *Track 3* là track tuân theo chuẩn TTS (Thift Third) với mật độ ghi cao, chỉ chứa ký tự số nhưng có khả năng ghi đè (rewrite) lên thành phần dữ liệu đã có. Thông thường chỉ sử dụng thông tin trên track 1 và 2.
- Thông tin về các tính chất, mật độ ghi,… trên từng Track của thẻ có thể được tóm lược lại như sau:

Track	**Tính chất**	**Mật độ ghi**	**Thể hiện**	**Độ dài**	**Định dạng mã**	**Số lượng ký tự**
Track 1	Chỉ đọc	210 bits/inch	Chữ và số	Tối đa 79 ký tự	Mỗi ký tự được tạo bởi 7 bit (6 bit dữ liệu + 1 bit kiểm tra chẵn lẻ)	2^6=64

Track 2	Chỉ đọc	75 bits/inch	Số (0→9)	Tối đa 40 ký tự	Mỗi ký tự được tạo bởi 5 bit (4 dữ liệu + 1 kiểm tra chẵn lẻ)	2^4=16
Track 3	Đọc, ghi đè	210 bits/inch	Số (0→9)	Tối đa 107 ký tự	Mỗi ký tự được tạo bởi 5 bit (4 dữ liệu + 1 kiểm tra chẵn lẻ)	2^4=16

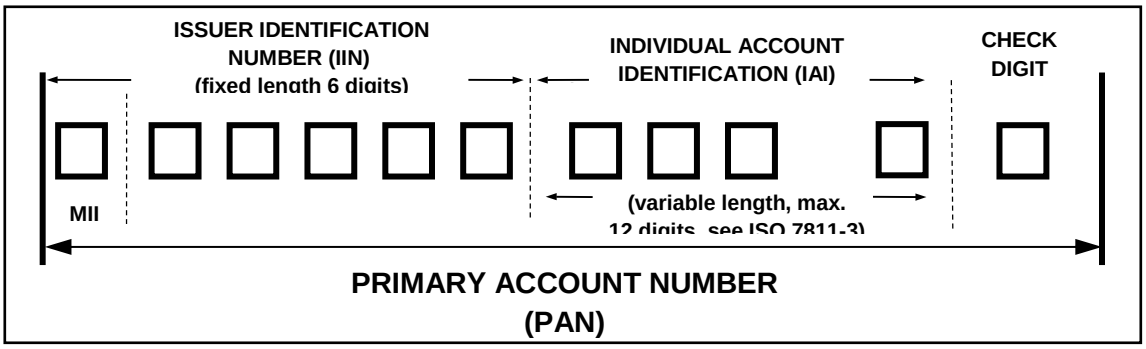
Bảng 2.3 Bảng m tả định nghĩa các Track

1.2. Cấu trúc của số thẻ

Đối với mỗi thẻ khi được lưu hành đều có một dãy số xác định đó là số PAN – Primarry Account Number. Số PAN còn có thể được gọi với các tên khác như số thẻ hoặc số tài khoản chính.

1.2.1. Số PAN

Số PAN là số định danh duy nhất đối với từng thẻ. Tuân theo chuẩn ISO 7812.



Hình 2.5 Cấu trúc số PAN

Số PAN có thể lên tới 19 số, hiện tại hầu hết thẻ từ của các Ngân hàng Việt Nam đều có 16 chữ số. Số PAN gồm 3 thành phần như sau:

IIN - Issuer Identification Number: số định danh đối với nhà phát hành thẻ, IIN cũng được gọi là số BIN –Bank Identification Number

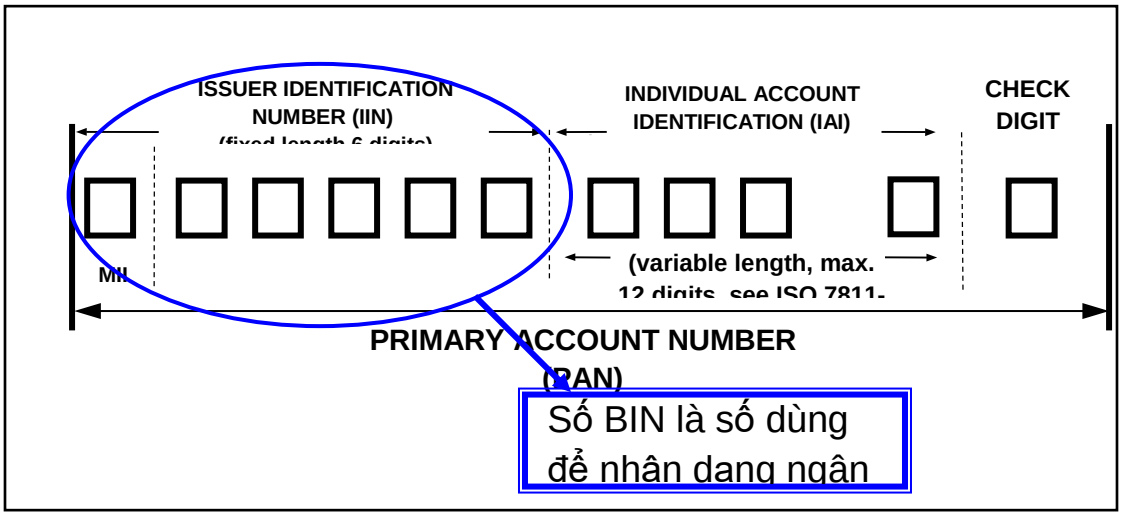
IAI - Individual Account Identification: Số nhận dạng tài khoản chủ thẻ. Các ngân hàng có thể qui định cấu trúc trong trường thông tin này.

CD - Check Digit: Số với ý nghĩa mang tính chất kiểm tra số thẻ này có hợp lệ hay không. Số này được tạo ra từ việc sử dụng giải thuật Luhn.

1.2.2 Số IIN (số BIN)

Mỗi một ngân hàng đều có một số BIN đại diện. Hệ thống đánh số BIN của thẻ tuân theo chuẩn ISO 7812 và ISO 3166.

BIN –Bank Identification Number là số dùng để nhận dạng ngân hàng, hay còn được gọi là IIN (Issuer Identification Number) số nhận dạng đối với nhà phát hành thẻ, Số BIN có độ dài là 6 chữ số, là một thành phần trong số PAN.



Hình 2.6 Vị trí số BIN

Trong đó chữ số đầu tiên là MII (Major Industry Identifier) – là số xác định dịch vụ trong lĩnh vực công nghiệp. Số này có các giá trị tuân theo chuẩn như sau:

0: Để dành dự trữ cho tương lai được sử dụng bởi ISO/TC 68.

1: Dùng cho các tổ chức hàng không.

2: Được phân ra để dùng cho các tổ chức hàng không trong hiện tại cũng như tương lai.

3: Dành cho các tổ chức du lịch và giải trí.

4: Dành cho các tổ chức tài chính, ngân hàng.

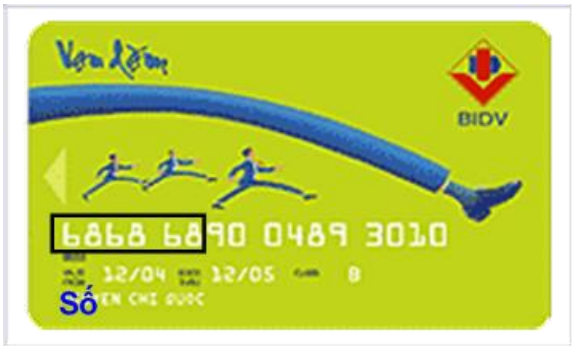
5: Dành cho các tổ chức tài chính, ngân hàng.

6: Dành cho lĩnh vực ngân hàng cũng như trong lĩnh vực công thương buôn bán.

7: Dành cho các tổ chức liên quan đến dầu mỏ.

8: Dành cho những tổ chức liên quan đến lĩnh vực truyền thông.

9: Được dữ trữ dành cho lưu hành nội bộ trong phạm vi quốc gia.



Hình 2.7 Thẻ vạn dặm của ngân hàng BIDV.

1.3. Định dạng thông điệp (message) của máy ATM

Định dạng thông điệp là cấu trúc thông điệp để ATM có thể trao đổi thông tin với Switch.

Thông điệp được chia làm 2 loại, loại thông điệp từ ATM đến Switch và thông điệp từ Switch đến ATM.

Định dạng thông điệp trong giao dịch tài chính được sử dụng trong máy ATM thường gồm các loại sau: 91x, NDx và ISOx. Do hiện nay có hai hãng chính về sản xuất máy ATM lớn trên thế giới là Diebold và NCR nên chuẩn 91x, NDx là hai loại định dạng chính được sử dụng.

Thông điệp chuẩn của hãng Diebold:

- 911
- 912+

Thông điệp chuẩn của hãng NCR:

- NDC
- NDC+
- Cấu trúc chung của thông điệp như sau

STX	Header	Body	ETX

Trong đó:

- STX- Start of text: Trường khởi đầu của thông điệp.
- Header: Phần đầu của thông điệp.
- Body: Phần thân của thông điệp.
- ETX-End of text: Trường kết thúc của thông điệp.

1.3.1. Thông điệp từ ATM đến Switch

Giới thiệu một số định dạng thông điệp từ ATM đến Switch.

1. Xác thực PIN - PIN Verification (PNV)
2. Rút tiền - Cash Withdrawal (CWD)
3. Đổi PIN - PIN Change (PIN)
4. Vấn tin và in sao kê - Balance Inquiry and Mini Statement (INQ)
5. Chuyển khoản - Funds Transfer (TFR)
6. Yêu cầu đổi khóa - Request Transmission Key (RQK)

1) Đầu mục thông điệp (Message header)

Đầu mục này sẽ xuất hiện trong tất cả các thông điệp được gửi từ ATM đến Switch.

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX- Start Of Text		1	02	Hex
2	Transaction Code	Mã giao dịch	3	xxx	xxx là mã giao dịch
3	Type 1 Note Status	Trạng thái 1	1	0 – 2	Note 1
4	Type 2 Note Status	Trạng thái 2	1	0 – 2	Note 1
5	Type 3 Note Status	Trạng thái 3	1	0 – 2	Note 1
6	Type 4 Note Status	Trạng thái 4	1	0 – 2	Note 1
7	Journal Status	Trạng thái nhật ký	1	0 – 2	Note 1
8	Receipt Status	Trạng thái in hóa đơn	1	0 – 2	Note 1
9	Dispenser Status	Trạng thái thiết bị trả	1	0 – 2	Note 2

		tiền			
10	Encryptor status	Trạng thái thiết bị mã hóa	1	0 – 2	Note 2
11	Card reader status	Trạng thái đầu đọc thẻ	1	0 – 2	Note 2
12	Transaction Sequence No	Số tuần tự giao dịch	6	[999999]	Kiểu số
13	ATM Status	Trạng thái ATM	1	O-Open C-Close	
14	ATM Identification	Số nhận dạng ATM	8	[99999999]	Kiểu số
	Tổng độ dài		24		Byte

Chú ý:

- Các trạng thái được định nghĩa:

0 - good

1 - low

2 - out

- Các trạng thái được định nghĩa:

0 - Normal

1 - Missing

2 - Inoperative

2) Thông điệp xác thực pin (PNV)

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã sử lý: 'PNV'
15	Track 2	Track 2 của thẻ từ	104		
16	Encrypted PIN Block	Khối PIN block đã được mã hóa	16		
17	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		145		Byte

3) Thông điệp Rút tiền CWD

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã sử lý: 'CWD'
15	Track 2	Track 2 của thẻ từ	104		
16	Transaction A/C No.	Số tài khoản giao dịch	16		
17	Transaction Amount	Khối lượng giao dịch	8	[99999999]	Kiểu số
18	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		153		Byte

4) Thông điệp Đổi PIN

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã sử lý: 'PIN'
15	Track 2	Track 2 của thẻ từ	104		
16	Old PIN Block (Encrypted)	PIN cũ (đã được mã hóa).	16		
17	New PIN Block (Encrypted)	PIN mới (đã được mã hóa)	16		
18	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		161		Byte

5) Thông điệp Vấn tin - INQ

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã sử lý: 'INQ'
15	Track 2	Track 2 của thẻ từ	104		
16	Transaction A/C No.	Số tài khoản giao dịch	16		Giá trị bằng rỗng
17	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		145		Byte

6) Thông điệp Chuyển khoản - TFR

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã xử lý: 'INQ'
15	Track 2	Track 2 của thẻ từ	104		
16	Source Transaction A/C No.	Số tài khoản nguồn	16		Giá trị bằng rỗng
17	Destination Transaction A/C No.	Số tài khoản đích	16		
18	Transaction Amount.	Khối lượng giao dịch	8	[99999999]	Kiểu số
17	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		169		Byte

7) Tthông điệp Yêu cầu truyền khóa (RQK)

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã xử lý: 'RQK'
15	ATM state	Trạng thái ATM	1	C-Cold Strt S-Supervisor	
16	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		26		Byte

1.3.2. Thông điệp từ Switch đến ATM

Giới thiệu một số định dạng thông điệp từ Switch đến ATM

1. Phản hồi chấp nhận xác thực PIN - Accepted Response to PIN Verification (PNV)
2. Phản hồi từ chối xác thực PIN - Rejected Response to PIN Verification (PNV)

3. Phản hồi chấp nhận rút tiền -Accepted Response to Cash Withdrawal (CWD)
4. Phản hồi từ chối rút tiền - Rejected Response to Cash Withdrawal (CWD)
5. Phản hồi xác nhận thay đổi PIN - Accepted Response to PIN Change (PIN)
6. Phản hồi được chấp nhận yêu cầu số dư & báo cáo nhỏ - Accepted Response to Balance Inquiry & Mini Statement (INQ)
7. Phản hồi xác nhận chuyển tiền - Accepted Response to Funds Transfer (TFR)

1) Phản hồi chấp nhận xác thực PIN.

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Ký hiệu bắt đầu	1	02	Số Hex
2	TPC		1	66	Số Hex
3	Operating Mode		1		P - Production T – Testing
4	Transaction Date		12		YYYYMMDDHHMM
5	Status		2		00 – Good 01 – Bad 02 – Retained 03 – Force change PIN
6	A/C Ditails		100		Note 1
7	Transaction sequence No		6	[999999]	Kiểu số
8	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		124		Byte

Thông tin chi tiết của số thẻ “account detail” sẽ được gửi theo định dạng sau: Type:A/C number:Type:A/C number: Type:A/C number:Type:A/C number:

Có các kiểu tài khoản là: CUR=Current; SAV=Saving

Ví dụ ‘:SAV:123456789:SAV:98765432109:CUR:987789654456:’

Nếu độ dài nhỏ hơn 100 thì sẽ được điền thêm số 0

2) Phản hồi không chấp nhận xác thực PIN.

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Ký hiệu bắt đầu	1	02	Số Hex
2	TPC		1	47 hoặc 54	Số Hex
3	Operating Mode		1		P - Production T – Testing
4	Transaction Date		12		YYYYMMDD HHMM
5	Reject Code		4		
6	Transaction sequence No		6	[000000-999999]	
7	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		26		Byte

Nếu TCP là 47H thì tương ứng mã nhận được từ Switch 3001 (Từ chối bởi không đồng bộ được khóa giao dịch). Nếu TPC là 54H từ chối thông thường.

3) Phản hồi chấp nhận giao dịch rút tiền

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Ký hiệu bắt đầu	1	02	Số Hex
2	TPC		1	66	Số Hex
3	Operating Mode	Chế độ hoạt động	1		P - Production T – Testing
4	Transaction Date	Ngày giao dịch	12		YYYYMMDD HHMM
5	Transaction A/C No.	Số tài khoản	16		
6	Accepted		1		1-Online
7	Fund Available	Giá trị hiện có	15		
8	Transaction Amount	Khối lượng giao	8		

		dịch			
9	Transaction Sequence No	Số thứ tự giao dịch	6	[000000-999999]	
10	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		62		Byte

4) Trả lời từ chối giao dịch rút tiền

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Ký hiệu bắt đầu	1	02	Số Hex
2	TPC		1	54	Số Hex
3	Operating Mode	Chế độ hoạt động	1		P - Production T – Testing
4	Transaction Date	Ngày giao dịch	12		YYYYMMDDHHMM
5	Reject Code		4		
6	Transaction Sequence No	Số thứ tự giao dịch	6	[999999]	
7	ETX	Ký hiệu kết thúc	1	3	Số Hex
	Tổng độ dài		24		Byte

Note: TPC = 54H, đây là thông điệp từ chối thông thường

5) Trả lời từ chối giao dịch rút tiền do không đủ tiền

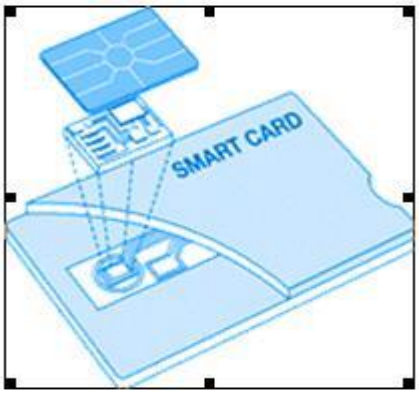
Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Ký hiệu bắt đầu	1	02	Số Hex
2	TPC		1	55	Số Hex
3	Operating Mode	Chế độ hoạt động	1		P - Production T – Testing
4	Transaction Date	Ngày giao dịch	12		YYYYMMDD

					HHMM
5	Reject Code		4		
6	Fund Available		15		
7	Transaction Sequence No	Số thứ tự giao dịch	6	[999999]	
8	ETX	Ký hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		24		Byte

2. Hệ thống thanh toán ATM cho thẻ chip.

2.1. Thẻ chip.

Thẻ Chip – Chip Card hay còn được gọi là thẻ thông minh – Smart Card. Là loại thẻ nhựa cứng, thông tin về thẻ được lưu trên chip nhớ. Thẻ có thể thực hiện được các giao dịch tự động như kiểm tra số dư, rút tiền, chuyển khoản,… từ máy rút tiền tự động ATM.



Hình 2.8 Mô hình thẻ chip

2.2. Tổng quan về thẻ chip.

Thẻ chip ra đời dựa trên hai nhân tố chính, các thuật toán mã hóa mạnh: mã hóa khóa công khai RSA, mã hóa khóa đối xứng 3DES, hàm băm SHA-1.

Chip trên thẻ có thể thực hiện các tính toán mã hóa trên dữ liệu. Thuật toán mã hóa PIN và thuật toán dành cho chữ kí số là RSA, hàm băm là SHA-1, MACing và việc mã hóa các thông điệp theo từng phiên thì sử dụng 3DES.

Thẻ chip có thể được cập nhật hay lập trình lại một cách an toàn khi đang sử dụng. Ngân hàng phát hành thẻ có thể cập nhật các tham số quản lí rủi ro chứa trong một ứng dụng ngân hàng từ xa trong một giao dịch trực tuyến tại terminal.

Một số loại thẻ đa ứng dụng hỗ trợ việc tải xuống các ứng dụng mới và xóa đi các ứng dụng cũ từ xa tại terminals chuyên dụng hay qua Internet.

Các thông tin lưu trong thẻ chip gồm:

- Dữ liệu công khai: thông tin về CA, chứng chỉ khóa công khai của nhà phát hành thẻ, chứng chỉ khóa công khai của thẻ, chứng chỉ khóa công khai để mã hóa PIN...
- Dữ liệu bí mật: khóa riêng của thẻ, khóa riêng mã hóa PIN, khóa chủ (Master Key), PIN.

2.3. Phân loại thẻ chip.

• Có hai cách để phân loại thẻ chíp theo công nghệ chíp hay phương thức đọc dữ liệu:

- Chíp nhớ - memory chip.
- Chíp vi xử lý - microprocessor chip.

• Phân loại theo phương thức đọc dữ liệu trên thẻ. Nó được chia ra làm 3 loại:

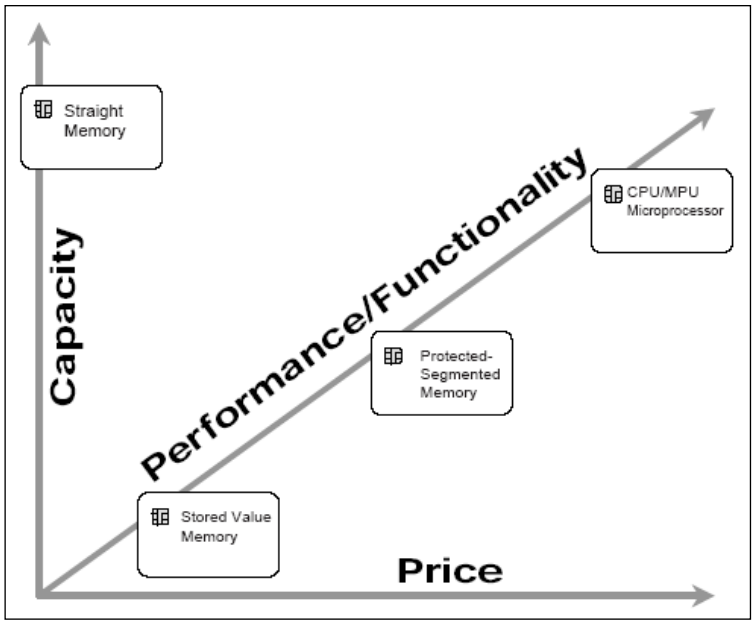
- Contact (tiếp xúc).
- Contacless (không tiếp xúc).
- Dual interface (có cả 2 chức năng trên).

Thẻ tiếp xúc: Để đọc và ghi dữ liệu lên thẻ thì thẻ phải được đặt vào thiết bị đầu cuối hay máy đọc thẻ. Loại thẻ này được các tổ chức tài chính và các cơ quan truyền thông chọn lựa và đang sử dụng phổ biến vì các ưu điểm về giá cả, về các chuẩn và độ bảo mật.

Thẻ không tiếp xúc: Việc đọc/ghi dữ liệu thẻ không cần phải có một kết nối vật lý. Thẻ có thể được đặt cách máy đọc thẻ vài chục centimet. Tốc độ xử lý thẻ không tiếp xúc là cao hơn so với các thẻ tiếp xúc. Thẻ không tiếp xúc được ứng

dụng tại những nơi cần phải xử lý nhanh như các hệ thống quá cảnh, trên các phương tiện giao thông công cộng. Thẻ không tiếp xúc đắt hơn nhưng lại không an toàn bằng thẻ tiếp xúc.

Thẻ lưỡng tính: kết hợp các đặc điểm của thẻ tiếp xúc và thẻ không tiếp xúc. Dữ liệu được truyền hoặc bằng cách tiếp xúc, hoặc không tiếp xúc. Thẻ lưỡng tính đắt hơn rất nhiều so với 2 loại trên.



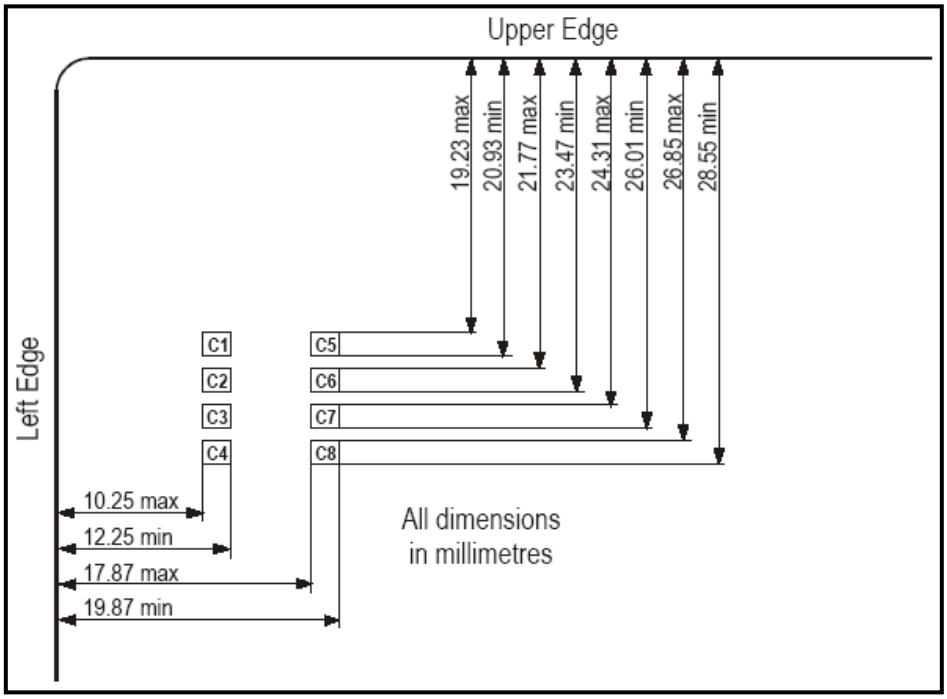
Hình 2.9 Mối tương quan giữa giá, dung lượng và hiệu năng (tính năng)

2.4. Các thành phần trong kiến trúc của thẻ chip.

Smart Cards là thẻ mỏng có gắn một con chip, và điều này tự nhiên đặt ra các thách thức cho riêng nó về thiết kế kiến trúc. Nhưng thực ra là các giải pháp hướng tới việc thu nhỏ các chip thông thường chứ không phải là phát minh một chip mới hoàn toàn.

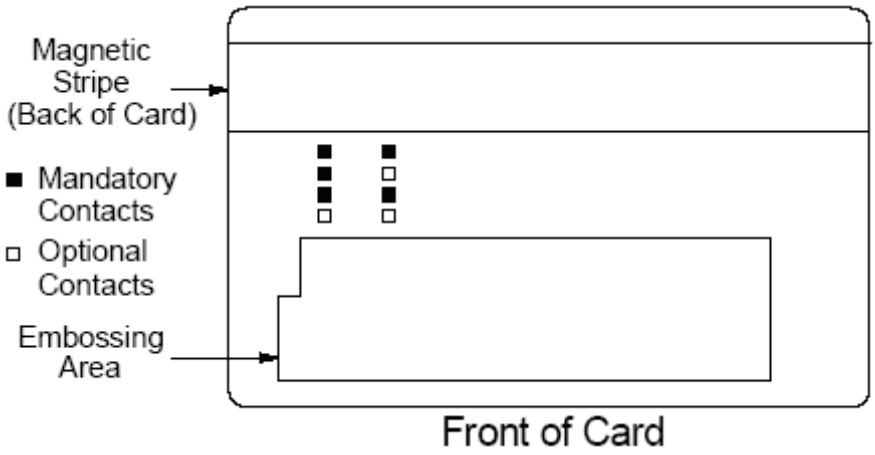
2.4.1. Vị trí và các chiều của các điểm tiếp xúc

Con chíp được gắn trên thẻ phải đảm bảo vị trí và các chiều của các tiếp xúc như được chỉ ra trong hình:



Hình 2.10 Vị trí và các chiều của các điểm tiếp xúc.

Các vùng C1, C2, C3, C5, và C7 phải được bao phủ toàn bộ bằng các mặt dẫn tạo nên các tiếp xúc ICC tối thiểu. các vùng C4, C6, C8 có thể có các mặt dẫn một cách tùy chọn.



Hình 2.11 Tương quan giữa vị trí của con chíp và dải từ trên thẻ.

Chỉ định cho các tiếp xúc

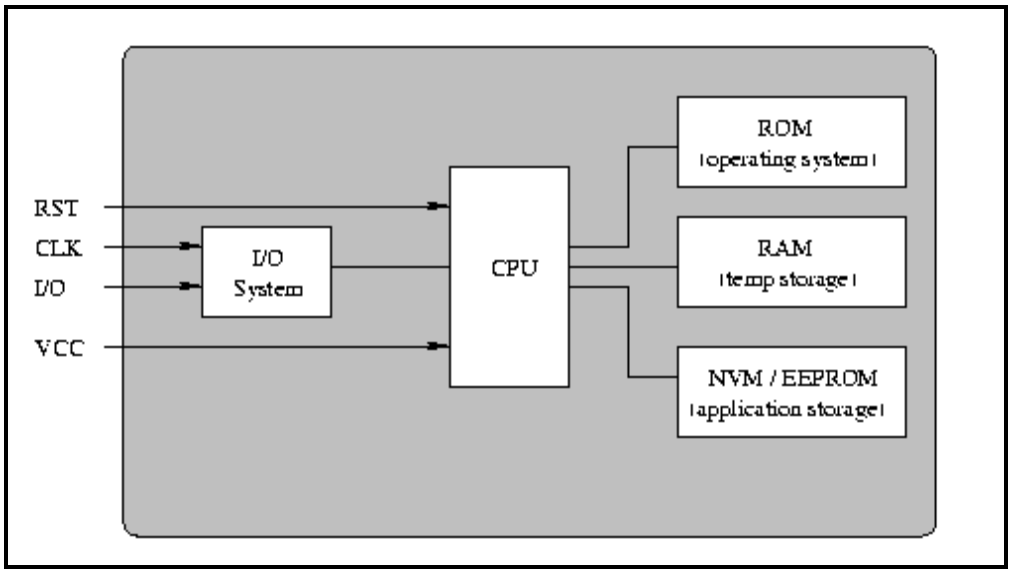
Việc gán các tiếp xúc ICC phải được định nghĩa như trong ISO/IEC 7816-2 và được thể hiện trong bảng.

C1	Supply voltage (VCC)	C5	Ground (GND)
C2	Reset (RST)	C6	RFU [2]
C3	Clock (CLK)	C7	Input/output (I/O)
C4	Not used; need not be physically present	C8	Not used; need not be physically present

Bảng 2.12 Mô tả vị trí các điểm tiếp xúc.

2.4.2. Bộ xử lý trung tâm.

Thông thường nó là một microcontroller 8-bit nhưng để tăng cường sức mạnh hơn nữa thì các chip 16 và 32-bit cũng đang được sử dụng. Nhưng không một chip nào có khả năng đa luồng (multi-threading) và các tính năng mạnh mẽ khác đang rất phổ biến trong các máy tính chuẩn. Smart Card CPUs thi hành các chỉ thị máy với tốc độ xấp xỉ 1 MIPS. Một bộ đồng xử lý (coprocessor) cũng thường được thêm vào để cải thiện tốc độ của các tính toán mã hóa.



Hình 2.13 Cấu trúc của bộ xử lý

2.4.3 Hệ thống bộ nhớ.

Có ba loại bộ nhớ chính trên thẻ:

- RAM. 1K. Nó cần thiết cho việc tính toán và phản hồi nhanh chóng. Chỉ có sẵn dung lượng rất nhỏ.
- EEPROM (Electrically Erasable PROM). Khoảng từ 1 đến 24K. Không giống như RAM, nội dung của nó không bị mất khi rút nguồn điện. Các ứng dụng có thể chạy lại và ghi vào nó, nhưng nó rất chậm và người ta chỉ có thể đọc/ghi vào nó khoảng 100 000 lần.
- ROM. Khoảng từ 8 đến 24K. Hệ điều hành và các phần mềm cơ bản khác giống như các thuật toán mã hóa được lưu ở đây.

2.4.4. Input / Output.

Nó chỉ thông qua một cổng I/O được điều khiển bởi bộ xử lý để đảm bảo rằng các truyền thông được chuẩn hóa theo khuôn mẫu của APDUs (Application Protocol Data Unit).

2.4.5. Các thiết bị giao tiếp – Interface Devices.

Thẻ thông minh cần năng lượng và một tín hiệu đồng hồ để chạy các chương trình, nhưng chúng không thể tự trang bị được. Thay vào đó, chúng được cung cấp bởi Interface Device – thiết bị giao tiếp (thông thường là một thiết bị đọc thẻ thông minh) khi giao tiếp với thẻ. Điều đó rõ ràng là thẻ thông minh không có gì khác hơn là một thiết bị lưu trữ.

Smart Card	Word size	ROM	EEPROM	RAM	Voltage	Clock	Write/erase cycles	Transmission rate
Infineon SLE 44C10S	8-bit	9K	1K	256b	2.7 - 5.5V	5 MHz	500 000	9600 baud
Orga ICC4	8-bit	6K	3K	128b	4.7 - 5.3V		10 000	

GemCombi	8-bit		5K		4.5 - 5.5V	13.6 MHz	100 000	106 kbaud
DNP Risona	8-bit		1K		5V	3.5 MHz		9600 baud
AmaTech Contactless	8-bit		1K		5V	13.6 MHz	100 000 cycles	
Schlumberger Cyberflex	8/16-bit	8K	16K	256b	5V	1-5 MHz	100 000 cycles	9600 baud

Bảng 2.4 Một số loại thẻ chip

2.4.6 Hệ điều hành.

Hệ điều hành thông dụng trên phần lớn các thẻ thông minh cài đặt một tập hợp các câu lệnh chuẩn (thường là từ 20-30) theo đó thẻ thông minh có thể trả lời lại. Các chuẩn thẻ thông minh như ISO 7816 và CEN 726 mô tả một dải lệnh mà thẻ thông minh có thể cài đặt. Thiết bị đọc thẻ gửi một lệnh đến thẻ thông minh, thẻ thông minh chạy lệnh và trả về kết quả (nếu có) cho thiết bị đọc thẻ và chờ cho câu lệnh khác.

Microsoft phát hành một phiên bản Windows mini cho thẻ thông minh vào năm 1998 và các phiên bản trước của Gnu O/S đã được phát hành.

Đối với thẻ thông minh sử dụng chíp vi xử lý, cũng giống như máy tính cá nhân (PC), cần có hệ điều hành để quản lý, thực thi các ứng dụng và trao đổi dữ liệu với thiết bị đọc thẻ. Hiện tại trên thị trường có 3 loại hệ điều hành chính hỗ trợ đa ứng dụng là:

- Javacard
- MULTOS
- Windows for SmartCards.

Những hệ điều hành này và các ứng dụng được đưa vào thẻ trong quá trình cá thể hóa thẻ.

Sau đó, khi một ứng dụng như Visa's VSDC (Visa Smart Debit Credit), MasterCard'sM/Chip hay JCB's J/Smart được tải vào smart card, cùng với dữ liệu duy nhất để cá thể hóa ứng dụng cho một chủ thẻ được cấp phép, thẻ có thể tương tác với terminals thanh toán để thực hiện các giao dịch được bảo mật.

- JCB (J/Smart)
- MasterCard (M/Chip)
- Visa (VSDC)

2.4.7 Hệ thống File.

Mỗi file có một danh sách của các bên được cấp quyền thực hiện các thao tác trên nó. Có nhiều loại file khác nhau: linear, cyclic, transparent, SIM, v.v. Các thao tác thông thường như tạo, xóa, đọc, ghi và cập nhật có thể được thực hiện trên tất cả các loại file trên. Một số tha01234 o tác khác chỉ được hỗ trợ trên các loại file cụ thể.

Type	**Special Operations**	**Example**
Linear	Seek	credit card account table
Cyclic	read next, read previous	transaction log
Transparent	read and write binary	Picture
SIM file	encrypt, decrypt	cellular telephone

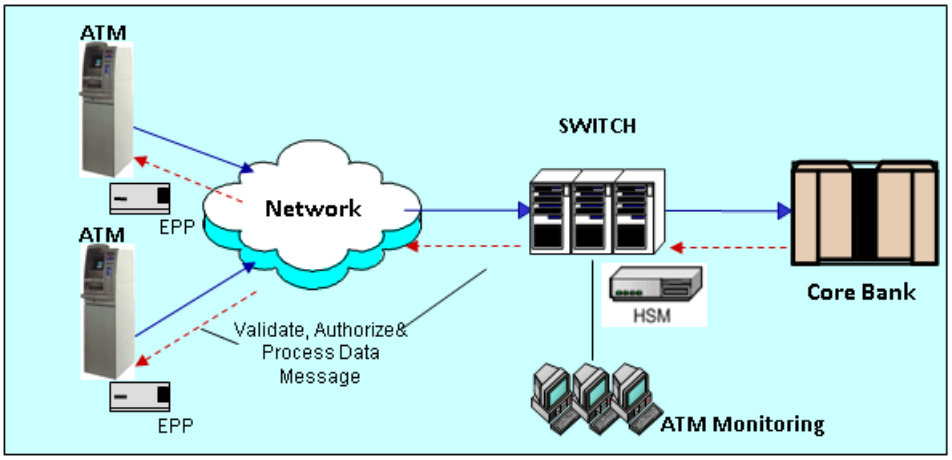
Bảng 2.5 Các hệ thống file.

CHƯƠNG 3: CƠ CHẾ BẢO MẬT VÀ AN TOÀN THÔNG TIN TRÊN HỆ THỐNG ATM

ATM là một phần trong hệ thống mạng không tập trung mà nằm phân bố ở các địa điểm khác nhau, do đó việc bảo mật và an toàn thông tin được đặt lên rất cao. Không những bảo mật an toàn trên từng máy ATM mà còn bảo mật an toàn trong toàn bộ hệ thống mạng.

Trong chương này ta tìm hiểu về bảo mật và an toàn thông tin trên hệ thống thanh toán ATM cho thẻ từ.

Hình vẽ bên dưới mô thể hiện sơ đồ tổng thể một hệ thống mạng ATM của một ngân hàng.



Hình 3.1 Sơ đồ tổng thể mạng lưới ATM.

3.1 Thuật toán, khóa bí mật và thiết bị mã hóa trong hệ thống ATM

ATM được coi như là một máy PC trong hệ thống mạng. Do đó, cần có những giải pháp nhằm đảm bảo an toàn khi các giao dịch được thực hiện.

Để đảm bảo an toàn thông tin giao dịch trong quá trình truyền thông giữa ATM và Switch, hệ thống sử dụng thiết bị mã hóa cứng để mã hóa và giải mã thông tin. Máy ATM có thiết bị EPP (Encrypting PIN Pad), hệ thống Switch có thiết bị HSM (Hardware Security Module).

3.1.1 Thuật toán mã hóa.

3.1.1.1. Thuật toán mã hoá 3DES - Triple DES.

Thuật toán 3DES chính là DES, gọi là 3DES bởi vì người ta dùng liên tiếp ba lần DES với ba khóa K1, K2, K3. Khóa K được xây dựng từ bộ ba khóa 64bit (K1, K2, K3) có độ dài 3*64 = 192 bit.

- Khi mã hóa sử dụng K1 mã hóa, K2 giải mã, K3 mã hóa.
- Khi giải mã sử dụng K3 giải mã, K2 mã hóa, K3 giải mã.

Các khóa K1, K2, K3 được xây dựng như sau:

1) Key single length (Bộ một khóa 64bit)

K1 = K2 = K3

Độ dài khóa 64bit

2) Key double length (Bộ hai khóa 64bit)

K1 # K2 và K3 = K1

Độ dài khóa 128bit

3) Key triple length (Bộ ba khóa 64bit)

K1 # K2 # K3 # K1

Độ dài khóa 192bit

Trường hợp này không gian khóa 3*56=168bit

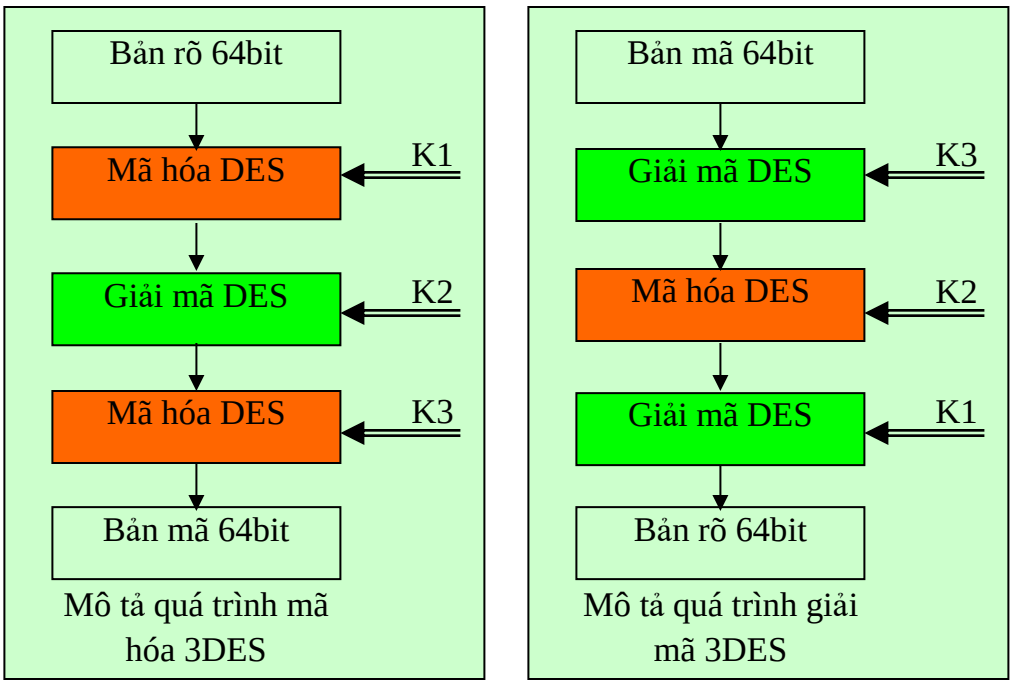
Ví dụ : Key triple length

K = ABCDEF987654210FEDCBA012345678901ABCDEF23456789

Khi đó các khóa con K1, K2, K3 được tách như sau :

```
ABCDEF9876543210|FEDCBA0123456789|01ABCDEF23456789
|<----------K1----------->|<----------K2----------->|<----------K3---------->|
```

Quá trình mã hóa và giải mã được thực hiện như sau :



Hình 3.2 Các bước thực hiện trong quá trình mã hóa và giải mã theo 3DES.

3.1.2. Khóa bí mật trong hệ thống ATM.

Khóa được sử dụng trong hệ thống ATM gồm có CVK, PVK, WK, LMK, TMK và được đảm bảo một số tính chất sau:

- Với các khóa được lưu trong EPP và HSM, khi bị xâm nhập một cách bất hợp pháp, khóa bí mật sẽ tự bị hủy.
- Khóa có độ dài 64bit, 128bit hoặc 192bit tùy theo cách sử dụng khóa hoặc chọn mã hóa DES hay 3DES.

Tất cả các khóa trên đều được tạo ra trong thiết bị HSM và khóa LMK phải được tạo trước tiên còn các khóa CVK, PVK, WK, TMK tạo ra sau.

Khóa được chia làm hai loại khi lưu là lưu dưới dạng bản rõ và lưu dưới dạng bản mã :

- Khóa LMK và TMK được lưu dưới dạng bản rõ trong các thiết bị tương ứng là HSM và EPP.

Khóa CVK, PVK, WK, TMK được lưu dưới dạng bản mã trong CSDL của Switch và của ATM.

3.1.2.1 Định nghĩa các khóa trong hệ thống ATM.

1. Khóa LMK- Local Master Keys.

LMK được tạo trước tiên trong HSM sau đó được lưu trong HSM và một bản sao được lưu trong smartcard. Nếu HSM bị mở ra vì bất cứ lý do gì hay xâm nhập trái phép, thì LMK sẽ bị xóa và phải được nhập lại vào HSM.

Để sinh khóa LMK và tải vào HSM thì phải có ít nhất 3 thành phần khác nhau dưới dạng bản rõ (3 clear component khác nhau, trong HSM ta có thể cấu hình khóa LMK được sinh ra từ 3 đến 9 thành phần LMK component). Để đảm bảo an toàn thì mỗi thành phần khóa bản rõ sẽ do mỗi người giữ.

Để tạo ra LMK thì người ta sử dụng phép XOR (Modulo 2) từ các LMK component.

Khóa LMK có các thông tin sau:

- Khóa được lưu trong HSM dưới dạng bản "rõ".
- Khóa được dùng để mã hóa và giải mã các khóa CVK, PVK, WK và TMK.
- Khóa này chỉ được thay đổi khi có yêu cầu.

Khóa có độ dài 64bit, 128bit hoặc 192bit.

2. Khóa CVK-Card Verification Keys.

Khóa CVK được sinh ngẫu nhiên trong HSM và được mã hóa bởi khóa LMK.

Khóa dùng để sinh số CVV/CVC, để đảm bảo thẻ không bị làm giả, khi phát hành người ta dựa trên các thông tin về thẻ để sinh số CVV/CVC, số này được lưu trên thẻ.

Bản mã của khóa CVK sẽ được lưu vào hệ thống Switch. Không lưu bản rõ

Khóa có độ dài 64bit, 128bit hoặc 192bit.

3. Khóa PVK- PIN Verification Keys.

Khóa PVK được sinh ngẫu nhiên trong HSM và được mã hóa bởi khóa LMK.

Khóa được dùng để mã hóa và giải mã số PIN của chủ thẻ, số PIN này được mã hóa và lưu trong CSDL của CoreBank.

Bản mã của khóa PVK sẽ được lưu vào hệ thống Switch. Không lưu bản rõ

Khóa thường không thay đổi, nếu thay đổi khóa thì phải thay đổi toàn bộ số PIN mới cho chủ thẻ.

Khóa có độ dài 64bit, 128bit hoặc 192bit.

4. Khóa WK- Working Keys (hay PIN Encryption Key).

Khóa WK được sinh ngẫu nhiên trong HSM. Khóa được dùng để mã hóa và giải mã số PIN trong quá trình trao đổi thông điệp giữa ATM và Switch.

Khóa được dùng để mã hóa số PIN tại máy ATM trước khi được gửi đi và dùng để giải mã số PIN khi nhận về tại Switch.

Khóa được lưu dưới hai bản mã tại Switch và ATM:

- Bản mã thứ nhất được mã bởi khóa LMK và lưu trong CSDL của Switch.
- Bản mã thứ hai được mã bởi khóa TMK và lưu trong CSDL của ATM.

Khóa này được đồng bộ giữa ATM và Switch thông qua quá trình trao đổi khóa.

Khóa được thay đổi thường xuyên tùy theo yêu cầu của NH, để đảm bảo an toàn thông tin giao dịch thông thường sau mỗi lần thực hiện giao dịch khóa này sẽ được thay đổi.

Khóa có độ dài 64bit, 128bit hoặc 192bit.

5. Khóa TMK- Terminal Master Keys.

Khóa TMK được sinh ngẫu nhiên trong HSM và được mã hóa bởi khóa LMK. Khóa được sử dụng để giải mã khóa WK.

Khóa được lưu tại hai nơi là tại EPP và Switch:

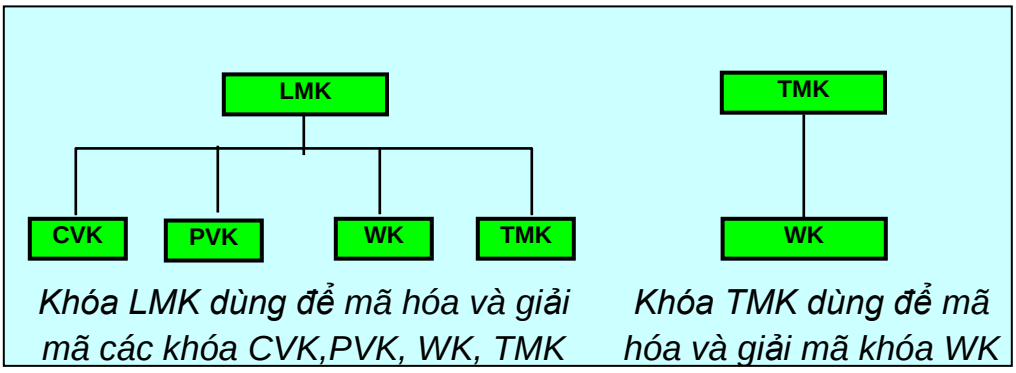
- Tại EPP khóa được lưu dưới dạng bản rõ.
- Tại Switch khóa được lưu trong CSDL dưới dạng bản mã, mã hóa bởi LMK.

Khóa này chỉ được thay đổi khi có yêu cầu

- Khóa có độ dài 64bit, 128bit hoặc 192bit.

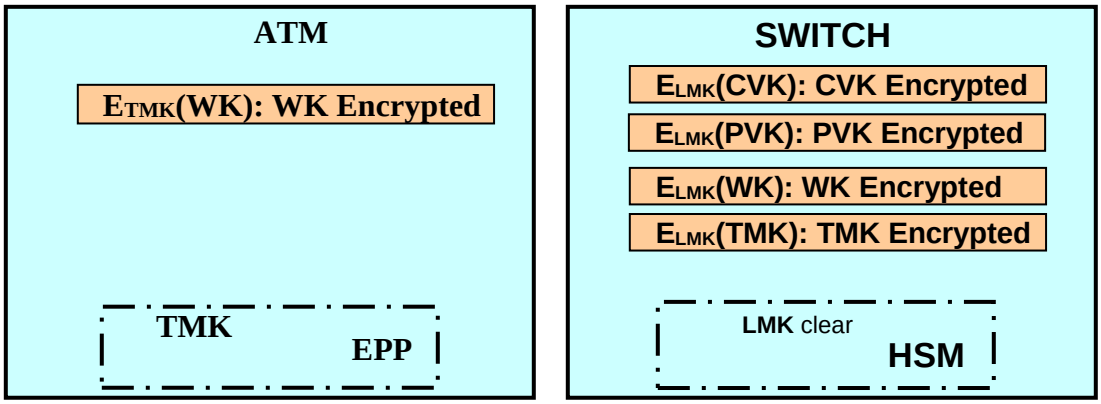
3.1.2.2 Sơ đồ phân cấp khóa trong hệ thống ATM.

Các khóa trên được phân cấp như sau:



Hình 3.3 Phân lớp các khóa sử dụng trong hệ thống ATM.

Mô tả vị trí các khóa trong hệ thống ATM



Hình 3.4 Mô tả các vị trí khóa trong hệ thống ATM.

Tại ATM:

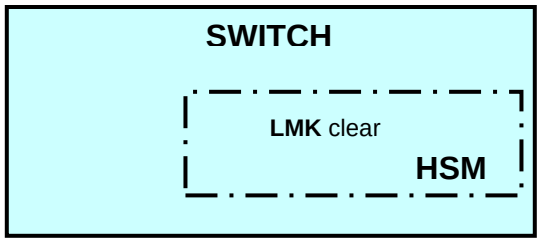
- TMK được lưu dưới dạng bản rõ trong thiết bị EPP.
- WK được mã hóa bởi TMK và lưu trong CSDL của máy ATM.

Tại SWITCH:

- LMK được lưu dưới dạng bản rõ trong thiết bị HSM.
- CVK, PVK, WK, TMK được mã hóa bởi LMK và lưu trong CSDL của Switch.

3.1.3.3. Trao đổi khóa giữa ATM và Switch.

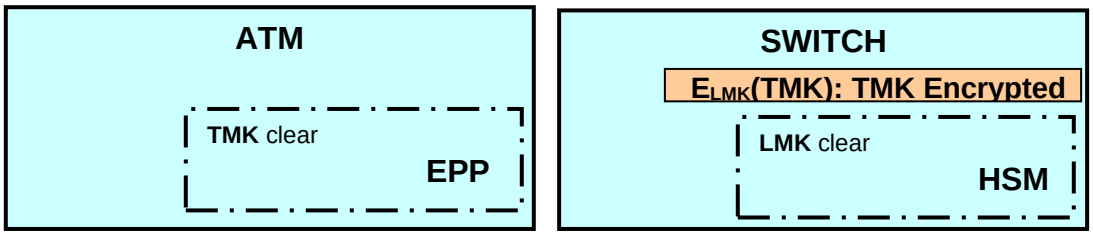
1. Thiết lập khóa LMK cho HSM.



Hình 3.5 Thiết lập khóa LMK cho HSM

- Tạo khóa LMK ngay trong HSM.
- Lưu LMK dưới dạng bản ”rõ” trong HSM và một bản dự phòng được lưu trong một Smartcard (Smrtcard cũng được bảo mật).

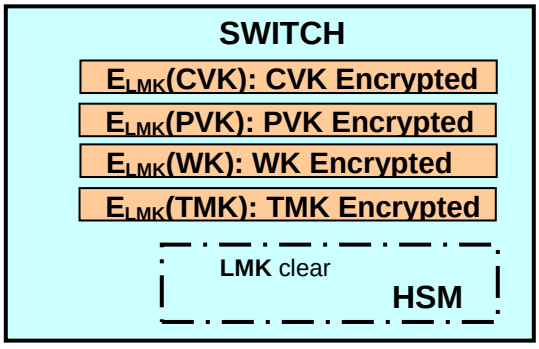
2. Thiết lập khóa TMK cho EPP



Hình 3.6 Thiết lập khóa TMK cho EPP.

- Khóa TMK được tạo trong HSM.
- Một bản rõ lưu tại EPP.
- Một bản mã lưu tại Switch (được mã hóa bởi khóa LMK).

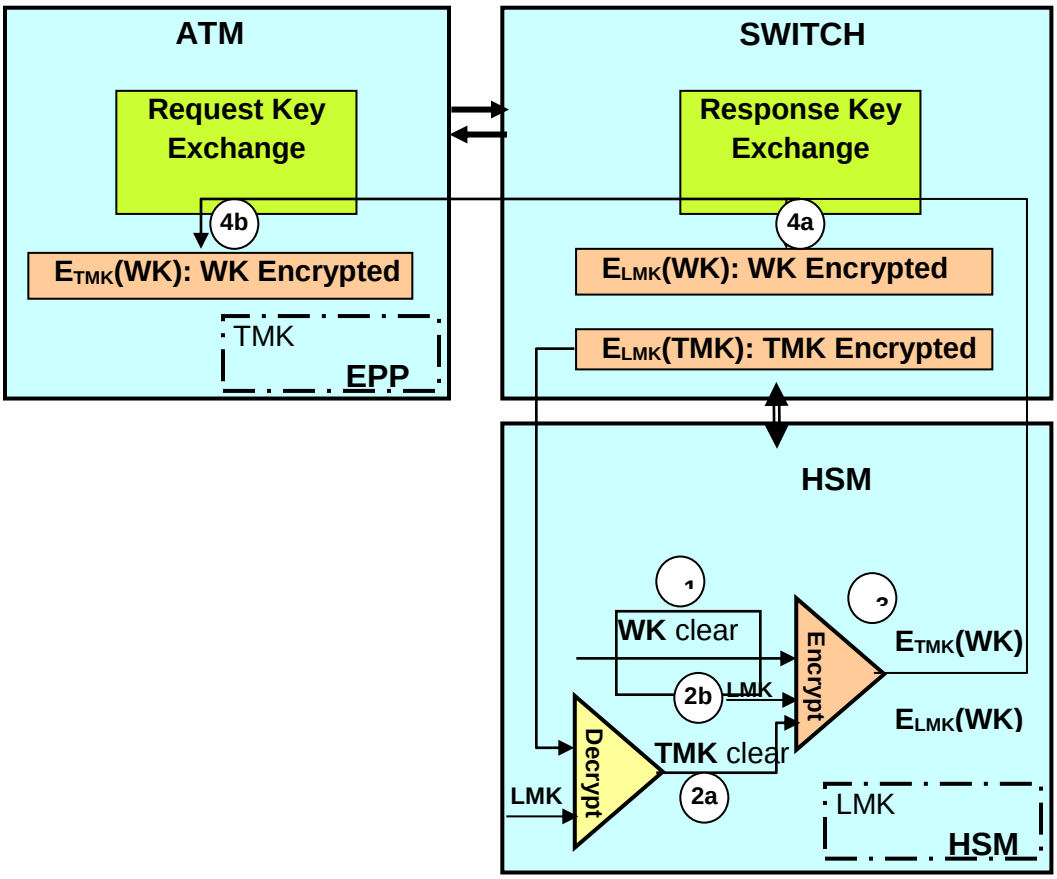
3. Thiết lập các khóa khác tại Switch.



Hình 3.7 Thiết lập khóa khác tại Switch.

- Tất cả các khóa trên đều được sinh trong HSM và được mã hóa bởi khóa LMK.
- Các bản mã của các khóa trên được lưu trong CSDL của Switch, không lưu bản rõ.

4. Trao đổi khóa WK giữa ATM và Switch.



Hình 3.8 Các bước trao đổi khóa WK giữa ATM và Switch.

Khi có yêu cầu trao đổi khóa WK giữa ATM và Swith thì quá trình được thực hiện như sau:

- HSM tạo ra bản rõ khóa WK.
- Bản mã TMK được giải mã bởi khóa LMK trong HSM.
- Bản rõ WK sẽ được mã hóa bởi khóa LMK và TMK .
- Bản mã bởi LMK được lưu tại Switch, bản mã bởi TMK sẽ được gửi cho ATM, bản mã này sẽ được lưu tại ATM.

3.1.3. Thiết bị mã hóa trong hệ thống ATM.

Trong hệ thống ATM sử dụng hai thiết bị mã hóa là EPP và HSM. EPP là thiết bị dùng mã hóa trên máy ATM, còn HSM là thiết bị mã hóa và giải mã của hệ thống Switch, đây là các thiết bị mã hóa cứng.

3.1.3.1 Thiết bị EPP- Encrypt PIN Pad.

Bàn phím để nhập PIN của máy ATM chính là thiết bị mã hóa, thiết bị này được gọi là EPP.

Đây là thiết bị mã hóa cứng chuyên dụng, dùng mã hóa trực tiếp số PIN khi được nhập vào và kết quả đầu ra là số PIN đã mã hóa.

Số PIN được mã hóa ngay khi chủ thẻ nhập đủ độ dài số PIN hoặc gõ enter để kết thúc nhập PIN. Không lưu bất kỳ bản rõ nào của số PIN chỉ lưu bản mã.

Hình 3.9 Thiết bị mã hóa EPP.

3.1.3.2 Thiết bị HSM - Hardware Security Module.

HSM thiết bị mã hóa cứng dùng để mã hóa và giải mã, đây là một phần của hệ thống phần mềm Switch.

Toàn bộ quá trình mã hóa và giải mã ở hệ thống Switch đều được thực hiện tại HSM.

Hình 3.10 Thiết bị mã hóa HSM.

3.2 Cơ chế mã hóa và giải mã số PIN trong hệ thống ATM.

Các thiết bị được sử dụng bao gồm EPP dùng trong máy ATM và HSM dùng trong hệ thống Switch. Bản rõ của PIN không bao giờ được xuất hiện ngoài FPP hay HSM.

3.2.1 Định nghĩa số PIN - Personal Identification Number

Số PIN – số nhận dạng cá nhân hay còn được gọi là mã số bí mật của chủ thẻ. Số PIN được dùng để xác định định danh tài khoản của chủ thẻ.

Độ dài tối thiểu của số PIN là 4 chữ số và tối đa là 12 chữ số, hiện nay các ngân hàng ở Việt nam số PIN có độ dài không quá 6 chữ số.

3.2.2 Mã hóa PIN tại ATM

Để đảm bảo độ an toàn của số PIN trong quá trình truyền trên mạng, số PIN sẽ được chuyển thành khối PIN (PIN Block) và khối PIN này sẽ được mã hóa trước khi chuyển từ ATM tới hệ thống Switch.

Khối PIN được mã hóa bằng khoá được cấu hình (thoả thuận) trước giữa ATM và hệ thống Switch.

Thuật toán DES (3DES) chỉ làm việc với khối dữ liệu đầu vào có độ dài là 64 bit, nên PIN Block được xây dựng bằng cách module-2 (XOR) hai trường 64 bit theo chuẩn ISO 9564-1 gồm:

- Trường số PIN theo khuôn dạng 64 bit.
- Trường số PAN theo khuôn dạng 64 bit.

Điều kiện đầu vào và kết quả đầu ra của quá trình mã hóa số PIN.

Đầu vào: Số thẻ - PAN.

Số PIN.

Đầu ra: Khối PIN Block được mã hóa bằng thuật toán DES (3DES) có độ dài 64bit.

Quá trình xác thực PIN sẽ được làm ở HSM (không làm trong phần mềm Switch), giá trị trả về của HSM sẽ cho biết số PIN nhập là đúng hay sai.

3.2.2.1 Khuôn dạng PIN Block.

Khuôn dạng trường số PIN được định nghĩa như sau:

Vị trí Bit	1-4	5-8	9-12	13-	17-	21-	25-	29-	33-	37-	41-	45-	49-	53-	57-	61-
Giá trị	**C**	**N**	**P**	**P**	**P**	**P**	**P/F**	**P/F**	**P/F**	**P/F**	**P/F**	**P/F**	**P/F**	**P/F**	**F**	**F**

Trong đó:

Ký hiệu	Miêu tả	Giá trị
C	Trường điều khiển	0000
N	Chiều dài PIN (4-12)	4 bit với giá trị từ 0100 (4) đến 1100 (12)
P	Chữ số trong số PIN	4 bit với giá trị từ 0000 (0) đến 1001 (9)
P/F	Số PIN/Số lấp đầy	Trường này được xác định bởi giá trị N
F	Số mặc định (Hex) 15	Trường 4 bit giá trị 1111 (15)

Khuôn dạng trường số PAN được định nghĩa như sau:

Vị trí Bit	1-4	5-8	9-	13-	17-	21-	25-	29-	33-	37-	41-	45-	49-	53-	57-	61-
Giá trị	**0**	**0**	**0**	**0**	**A1**	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**	**A9**	**A10**	**A11**	**A12**

Trong đó:

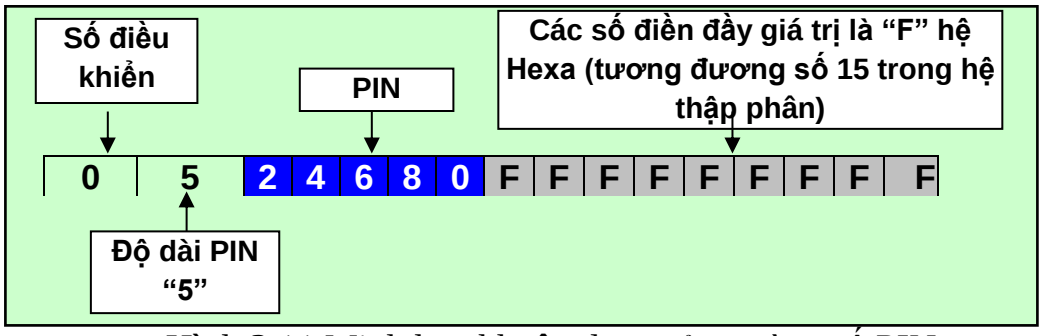
0 = Pad digit	Trường 4 bit có giá trị là 0 (thể hiện dạng nhị phân 0000)
A1 … A12 = account number A1 đến A12 thuộc [0,..,9]	12 số bên phải của số PAN ngoại trừ check digit (bỏ số cuối cùng bên phải). A12 là số đứng trước check digit của số PAN. Nếu số PAN không tính check digit mà nhỏ hơn 12 số thì được sắp dần vào từ bên phải và được điền ở bên trái bằng các số Pad digit

Ví dụ cho số PIN và số PAN của một thẻ ATM như sau:

Số PIN=24680 có độ dài là 5 chữ số.

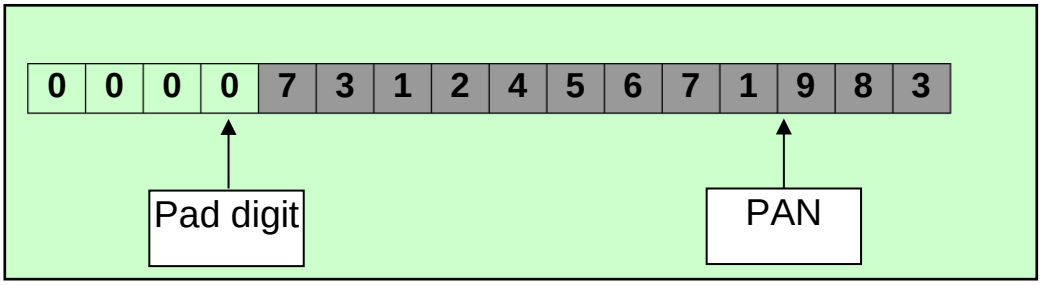
Số PAN=6688997312456719831 có độ dài là 19 chữ số

- Khuôn dạng trường số PIN:



Hình 3.11 Minh họa khuôn dạng của trường số PIN

- Khuôn dạng trường số PAN:



Hình 3.12 Minh họa khuôn dạng của trường số PAN

- Khối PIN Block được tính như sau:

PIN	0	5	2	4	6	8	0	F	F	F	F	F	F	F	F	F	
PAN	0	0	0	0	7	3	1	2	4	5	6	7	1	9	8	3	
	0	**5**	**2**	**4**	**1**	**B**	**1**	**D**	**B**	**A**	**9**	**8**	**E**	**6**	**7**	**C**	**XOR**

Hình 3.13 Minh họa cách tính khối PIN Block.

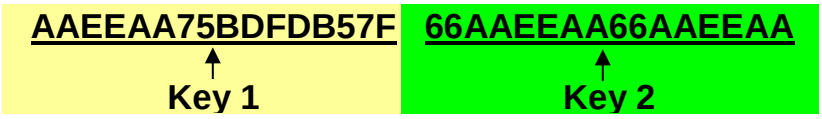
Khối PIN Block là : **05241B1DBA98E67C**

3.2.2.2 Mã hóa khối PIN Block

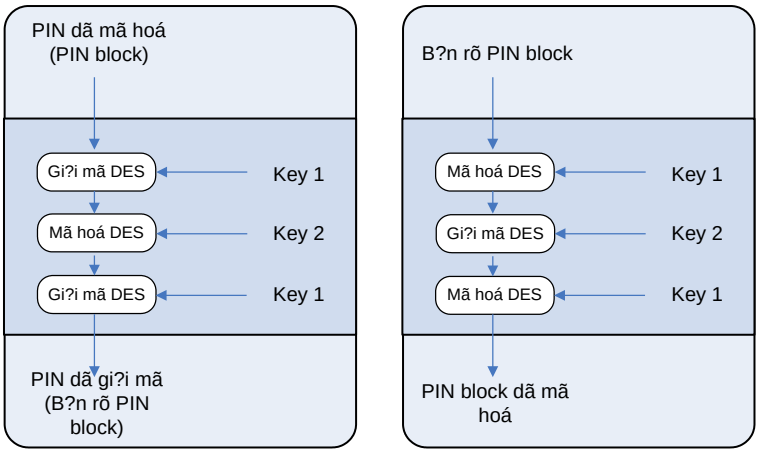
Khối PIN này được mã hóa bởi 3DES trước khi truyền đi, ví dụ với một khoá bộ hai (128 bit) sẽ được dùng để mã hóa như sau :

AAEEAA75BDFDB57F 66AAEEAA66AAEEAA

với 64 bit bên trái (key 1) và 64 bit bên phải (key 2) ta có 2 như sau:



Sơ đồ dưới đây mô tả việc dùng khoá 3DES bộ hai để mã hoá và giải mã PIN block:



Hình 3.14 – Các bước mã hoá và giải mã PIN Block.

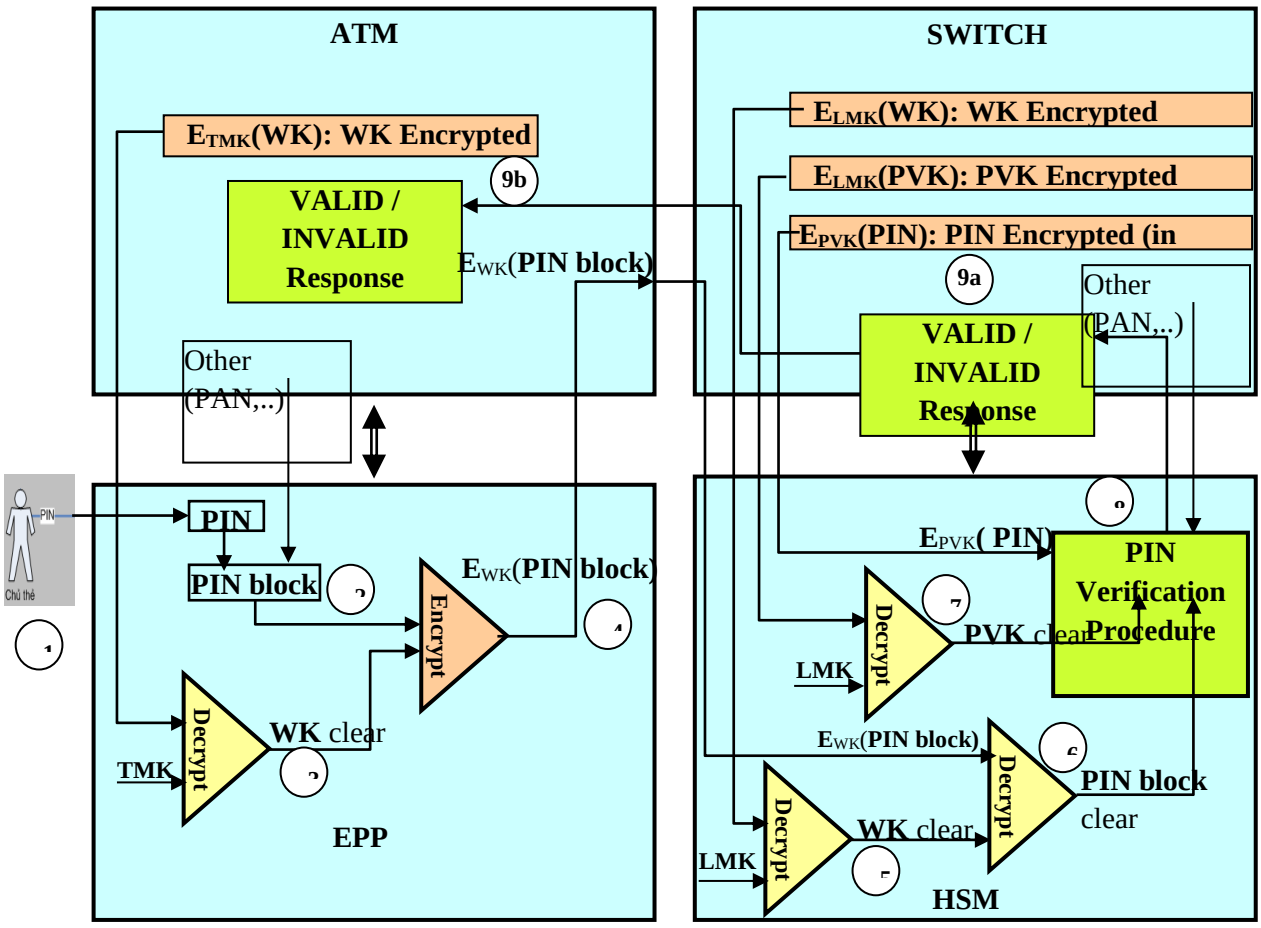
3.2.3 Xác thực PIN tại HSM

Tại HSM để xác thực PIN gồm các quá trình sau:

- Giải mã PIN được nhập vào từ máy ATM đã được mã hóa.
- Giải mã PIN lưu trong CSDL của Corebank đã được mã hóa.
- So sánh số PIN được nhập vào và số PIN được lưu trong CSDL.
- Quá trình xác thực đều thực hiện trong thiết bị HSM.

Kết quả đầu ra sẽ là số PIN nhập vào đúng hay sai.

Các bước thực hiện xác thực PIN:



Hình 3.15 Quá trình xác thực số PIN giữa ATM và Switch.

1. Người dùng cho thẻ vào ATM và nhập số PIN.
2. Thiết bị EPP sẽ tạo PIN block .
3. Giải mã khóa WK bởi khóa LMK.
4. Mã hóa PIN block theo khóa WK, khối PIN này được gắn vào thông điệp và gửi cho Switch.
5. Bản mã WK tại Switch được giải mã bởi khóa LMK trong HSM.
6. Khối PIN block được giải mã bởi khóa WK.
7. Bản mã của PVK tại Switch được giải mã bởi khóa LMK trong HSM.
8. Khối PIN được lưu trong CSDL của khách hàng được giải mã bởi khóa PVK, sau đó được so sánh với khối PIN block trong Module PIN Verification.
9. Kết quả so sánh sẽ được giửi lại cho ATM.

3.3. Một số giải pháp bảo mật và đảm bảo an toàn thông tin trong hệ thống ATM.

Bảo đảm an toàn thông tin trong hệ thống có thể được chia ra làm 3 lĩnh vực sau :

- Đảm bảo an toàn phía Ngân hàng.
- Đảm bảo an toàn phía Người dùng.
- Đảm bảo an toàn cơ sở hạ tầng của hệ thống bao gồm phần cứng, phần mềm và mạng truyền thông.

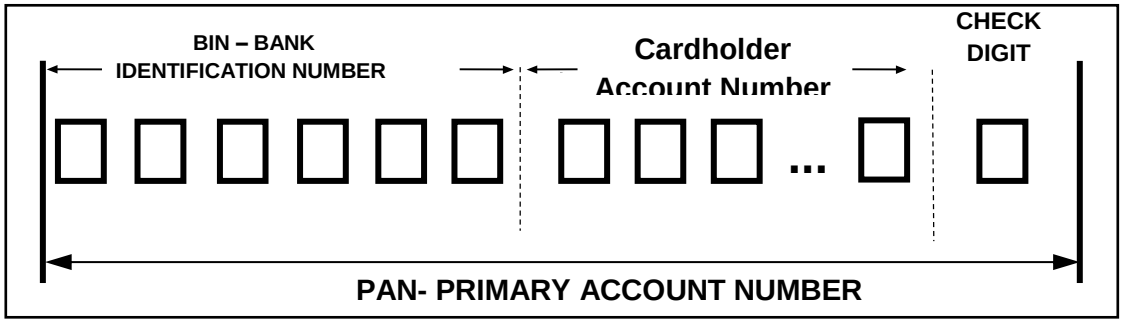
Dưới đây là các liệt kê các giải pháp nhằm bảo đảm an toàn thong tin trong hệ thống:

1. Kiểm tra số thẻ phát hành.
2. Kiểm tra tính hợp lệ của thẻ.
3. Bảo đảm an toàn các khóa bí mật.
4. Mã hóa số PIN của chủ thẻ trong CSDL Corebank
5. Mã hóa số PIN của chủ thẻ khi thực hiện giao dịch.
6. Bảo đảm an toàn CSDL.
7. Bảo đảm an toàn Phần mềm.
8. Bảo đảm an toàn Hệ điều hành.
9. Bảo đảm an toàn trên đường truyền.
10. Bảo đảm chống tấn công vật lý.
11. Bảo đảm an toàn từ phía ngân hàng.
12. Bảo đảm an toàn từ phía người dùng.

3.3.1 Kiểm tra tính đúng đắn số thẻ - Card number Check Digit

3.3.1.1 Định nghĩa số CD - Check Digit

Trong quá trình phát hành thẻ, modul quản lý thẻ CMS của hệ thống Switch sẽ tính toán ra một con số (nằm trong khoảng từ 0 đến 9) và gắn vào cuối thẻ, số này được gọi là Check Digit CD, chữ số này để kiểm tra số thẻ này là đúng hay sai.



Hình 3.16 Cấu trúc của số PAN và vị trí số CD

Tuy nhiên, vì chữ số này nằm trong khoảng [0, 9] nên có thể dễ dàng tìm ra được bằng cách thay đổi chữ số cuối của thẻ với các giá trị lần lượt từ 0 đến 9.

Do số CD chỉ nằm trong khoảng [0, 9], nên số CD chỉ dùng kiểm tra một cách tương đối.

3.3.2.2 Giải thuật tính số CD

Sử dụng giải thuật Luhn để sinh số CD. Giải thuật Luhn là cách thức kết hợp các chữ số của một mã số thẻ tín dụng (các chữ số xen kẽ nhau) và kiểm tra tổng cuối cùng có chia hết cho 10 hay không. Nếu đúng thì thẻ này hợp lệ.

Khi kiểm tra PIN nhập vào của chủ thẻ thì hệ thống Switch sẽ kiểm tra đồng thời số CD. Căn cứ vào thông tin thẻ, hệ thống tính số CD nếu so khớp thì thẻ hợp lệ.

Hình 3.17 Mặt trước của thẻ ATM và vị trí số CD

Giải thuật này thực hiện như sau:

1. Từ các số thẻ cho trước ta làm từ trái qua phải.
2. Các số nằm ở dòng chẵn thì nhân với 1(để bình thường).
3. Các số nằm ở dòng lẻ thì nhân với 2.
4. Kiểm tra kết quả tính được, nếu số nào lớn hơn 9 thì trừ đi 9.
5. Cộng các kết quả tính được lại với nhau ta được một số.
6. Thực hiện phép tính lấy số đơn vị của số đó cộng với số cần tính để thành 10, khi đó giải phép toán ta được số CD.

A) Quy trình tạo số CD.

Ví dụ: ta có số thẻ như sau: 668899123456789Y, ta cần sinh số Y sao cho số thẻ là hợp lệ.

	BIN						Cardholder Account Number									CD
PAN	6	6	8	8	9	9	1	2	3	4	5	6	7	8	9	Y
Nhân 2 (cột lẻ)	x2		x2		x2		x2		x2		x2		x2		x2	Y
Kết quả	12	6	16	8	18	9	2	2	6	4	10	6	14	8	18	Y
Trừ 9 nếu > 9	-9		-9		-9						-9		-9		-9	Y
Kết quả	3	6	7	8	9	9	2	2	6	4	1	6	5	8	8	Y
Cộng các chữ số lại	3 + 6 + 7 + 8 + 9 + 9 + 2 + 2 + 6 + 4 +1 + 6 + 5 + 8 + 8 + Y = 84 + Y ***Giải bài toán:*** lấy số hàng đơn vị của 84 cộng với Y có tổng bằng 10. 4 + Y = 10 => Y =6															
Kết quả	6	6	8	8	9	9	1	2	3	4	5	6	7	8	9	6

Bảng 3.1 Cách sinh số CD

Y=6 => Số thẻ hợp lệ cho dãy số trên: PAN=6688991234567896

B) Quy trình kiểm tra số CD.

Hoàn toàn tương tự như trên, sau khi cộng được các chữ số lại gồm cả số CD ta được tổng, nếu tổng này chia hết cho 10 thì số thẻ đó hợp lệ.

	BIN-Bank Identification Number						Cardholder Account Number									Check Digit
PAN	6	6	8	8	9	9	1	2	3	4	5	6	7	8	9	6
Nhân 2 (cột lẻ)	x2		X		x2		X		x2		x2		x2		x2	
Kết quả	12	6	16	8	18	9	2	2	6	4	10	6	14	8	18	6
Trừ 9 nếu > 9	-9		-9		-9						-9		-9		-9	6
Kết quả	3	6	7	8	9	9	2	2	6	4	1	6	5	8	8	6
Cộng các chữ số lại	3 + 6 + 7 + 8 + 9 + 9 + 2 + 2 + 6 + 4 +1 + 6 + 5 + 8 + 8 + 6 = 90 ***Giải bài toán:*** 90 mod 10 = 0															
Kết quả	Số thẻ hợp lệ															

Bảng 3.2 Cách kiểm tra số CD

3.3.2 Xác thực tính hợp lệ của thẻ - Card Authentication Values.

3.3.2.1 Định nghĩa số CVV/CVC.

Khi phát hành thẻ để đảm bảo thẻ không bị làm giả, người ta sử dụng số CVV/CVC (Card Verification Value/ Card Verification Code) để phân biệt thẻ thật thẻ giả.

Mỗi một loại thẻ khi phát hành sẽ có một số CVV/CVC được lưu trong rãnh từ, để sinh số này người ta sử dụng các điều kiện đầu vào bao gồm Số thẻ PAN, ngày hết hạn thẻ Card expiration date và Mã dịch vụ Service code.

Các giá trị đầu vào là duy nhất dó đó mỗi thẻ chỉ có một số CVV/CVC duy nhất.

Khi kiểm tra PIN nhập vào của chủ thẻ thì hệ thống Switch sẽ kiểm tra đồng thời số CVV/CVC. Căn cứ vào thông tin thẻ, hệ thống tính số CVV/CVC và so khớp với số CVV/CVC được lưu trong thẻ, nếu khớp thì thẻ hợp lệ.

Giải thuật sinh số CVV/CVC :

Sử dụng thuật toán DES với độ dài khóa bí mật 64bit

Input : chuỗi 64 bít hay 16 ký tự hexa được gọi là Transformed Security Parameter (TSP), TSP tính từ Số thẻ PAN, Ngày hết hạn thẻ Card Expiration date (YYMM) và Mã dịch vụ Service code.

Output : 16 ký tự hexa (64 bit).

A) Cách tạo số TSP.

TPS có định dạng gồm 9 chữ số tính từ bên phải của số PAN loại trừ số cuối cùng cộng với 4 số Exp date cộng với 3 số Service code

PAN : 668899123456789 6

Exp date : 0909

Service code: 101

TSP = 123456789 0909 101

B) Cách tính số CVV/CVC.

Ba số CVV/CVC được tính như sau :

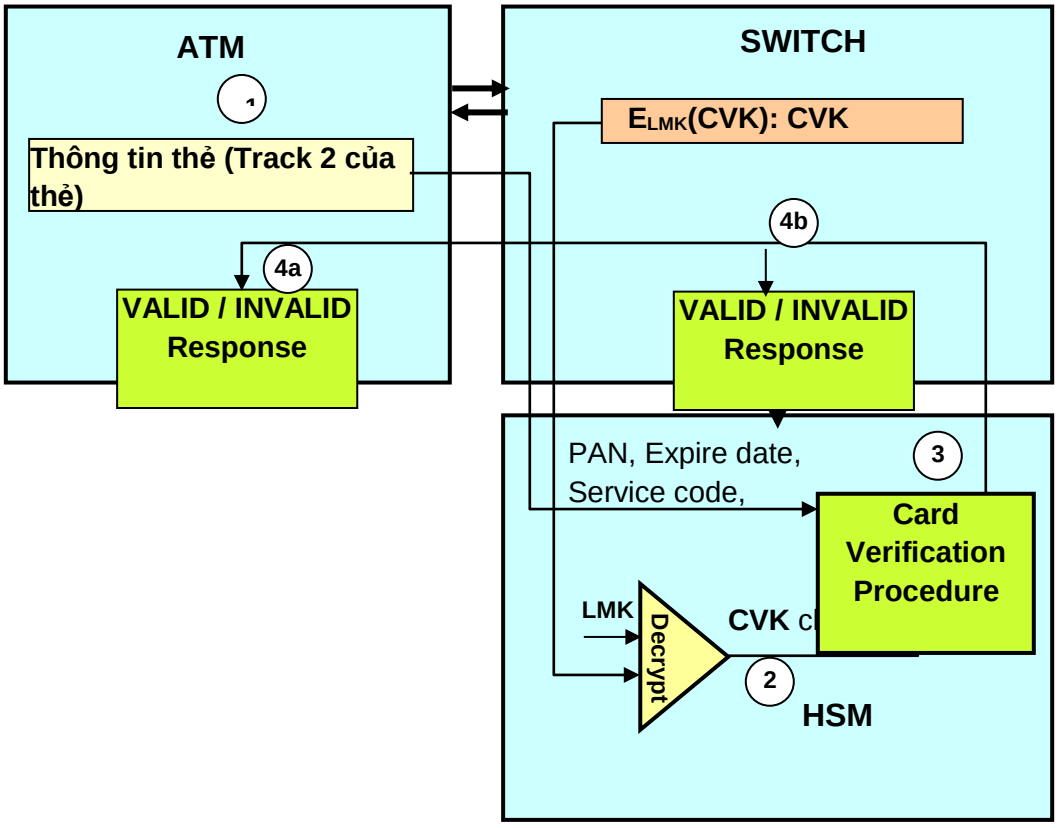
- Từ dãy số 16 ký tự hexa kết quả đầu ra ta đi từ trái qua phải, khi đó CVV/CVC là 3 số thập phân đầu tiên trong dãy số 16 ký tự hexa.
- Nếu không tìm được đủ 3 số thập phân trong đó thì số còn thiếu sẽ sử dụng là các số không phải là thập phân tính từ trái qua và chuyển sang số thập phân theo công thức A→ 0 ; B→1 ; C→2 ; D→3 ; E→4 ; F→5.

Ví dụ : Output from DES: **0F**AB**9**CDEFFEFDCBA

=> CVV/CVC là 095.

3.3.2.2 Xác thực số CVV/CVC.

Quá trình xác thực này diễn ra cùng với quá trình xác thực PIN của chủ thẻ.



Hình 3.18 Quá trình xác thực số CVV/CVC giữa ATM và Switch.

1. Khi thực hiện xác thực PIN, thì đồng thời các thông tin của thẻ là Track 2 sẽ được gửi đến Switch. Thông tin để xác thực bao gồm số PAN, ngày hết hạn thẻ Expire date, mã dịch vụ Service code và số CVV/CVC.

2. Bản mã của khóa CVK tại Switch được giải mã bởi khóa LMK trong HSM,
3. Sử dụng khóa CVK trong thuật toán DES để sinh số CVV/CVC. Kiểm tra số CVK được sinh ra với số CVV/CVC được gửi đến.
4. Kết quả kiểm tra được gửi lại cho ATM.

3.3.3. Bảo đảm an toàn thông tin giao dịch.

- Bảo mật số PIN.
- Bảo đảm an toàn các khóa bí mật trong hệ thống ATM.

Bản rõ của PIN không bao giờ được xuất hiện bên ngoài một thiết bị EPP hay HSM.

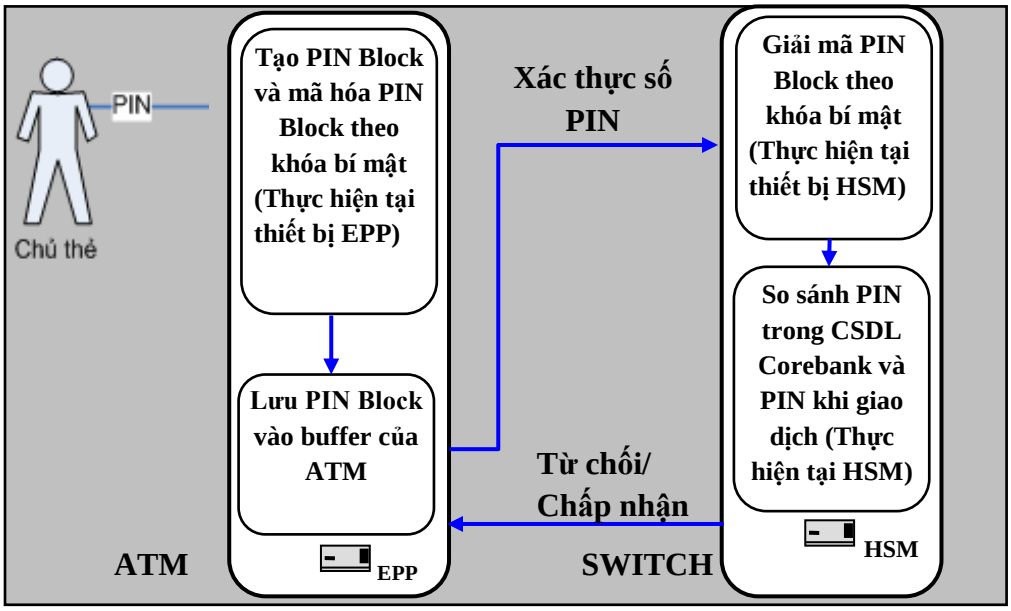
Để đảm bảo an toàn thông tin khi giao dịch trên ATM số PIN sẽ được mã hóa trước khi thực hiện giao dịch. Số PIN của chủ thẻ được lưu trong CSDL Corebank dưới dạng bản đã được mã hóa.

Không truy cập hoặc xác định được bản rõ của bất kỳ khoá bí mật nào được lưu trữ trong thiết bị EPP, HSM một cách bất hợp pháp.

Khi bị xâm nhập một cách bất hợp pháp, khóa bí mật sẽ tự bị hủy.

Khóa có độ dài 64bit, 128bit hoặc 192bit tùy theo cách sử dụng khóa hoặc chọn mã hóa DES hay 3DES.

Quá trình xác thực PIN được thực hiện theo mô hình sau:



Hình 5.19 Quy trình mã hóa và xác thực PIN.

Bước 1: Chủ thẻ đưa thẻ và nhập PIN tại máyATM.

Bước 2: Tạo và mã hóa PIN Block bằng thuật toán DES (3DES) tại EPP.

Bước 3: Lưu PIN Block vào bộ đệm của ATM.

Bước 4: Giải mã PIN Block tại HSM.

Bước 5: So sánh PIN trong CSDL của chủ thẻ và PIN của giao dịch tại HSM.

Bước 6: Kết quả phản hồi cho máy ATM là từ chối hay chấp nhận giao dịch.

3.3.4. Bảo đảm an toàn phần mềm ATM.

Đảm bảo phần mềm cài đặt có bản quyền và không cài đặt các phần mềm không được phép.

Đảm bảo an toàn mật khẩu truy nhập vào phần mềm.

3.3.5. Bảo đảm an toàn hệ điều hành.

Để đảm bảo an toàn cho hệ điều hành ta cần thực hiện một số nội dung sau:

- Tắt các service không dùng
- Đóng các cổng không dùng
- Thiết lập FireWall cho máy ATM

3.3.6. Bảo đảm an toàn chống tấn công vật lý.

ATM được bảo vệ bằng vỏ thép, các hộp đựng tiền được đặt trong một tủ mà được gọi là két sắt. Két sắt gồm có khóa số và khóa chìa để đảm bảo an toàn.

ATM còn sử dụng cơ chế phát hiện rung, khi đó hệ thống chuông sẽ rung để thông báo ATM bị tấn công.

ATM có hệ thống phun mực vào các tờ tiền khi các hộp đựng tiền bị xâm nhập trái phép.

ATM có hệ thống camera giám sát và ghi lại ….

3.3.7. Bảo đảm an toàn từ phía ngân hàng.

Thiết lập các danh sách thẻ nóng, thẻ đen để hạn chế sự gian lận của tội phạm.

Phân quyền và kiểm soát truy cập đến tài nguyên của hệ thống, sao cho thông tin không bị lộ với người không được phép, thông tin sẵn sàng cho người dùng hợp pháp.

3.3.8. Bảo đảm an toàn từ phía người dùng.

Chủ thẻ cần phải chú ý đến những trò gian lận ATM sau:

- Lấy cắp thẻ và số PIN
- Trộm dữ liệu
- Trộm dữ liệu bằng camera
- Nhìn trộm qua vai

CHƯƠNG 4: ĐỀ XUẤT GIẢI PHÁP ĐẢM BẢO TÍNH AN TOÀN, BẢO MẬT THÔNG TIN CHO HỆ THỐNG ATM.

Ta thấy việc bảo mật CSDL, bảo mật thông tin trên đường truyền và bảo mật Password là quan trọng nhất, ngoài ra bảo mật hệ thống cũng đóng vai trò quan trọng.

Có một số điểm cần được lưu ý như sau: lưu ý đối với hệ thống ATM và lưu ý đối với người dùng.

1. Đối với người dùng.

- Nếu bọn tội phạm ăn cắp (hoặc làm giả thẻ) và có số PIN thì coi như người dùng bị mất tiền trong tài khoản.
- Số PIN là một số có từ 4 đến 6 chữ số thập phân, thì đây là con số không lớn, nên có thể dễ mò được.
- Người dùng chưa coi trọng thẻ ATM như là một phần cuộc sống của mình nên dễ bị mất các thông tin liên quan đến thẻ hoặc bị mất thẻ dẫn đến mất tiền trong tài khoản.
- Nhiều người dùng sợ quên số PIN của mình nên đã ghi chép ra giấy, mỗi khi giao dịch thì lấy ra để nhập. Đây là một sơ hở rất nguy hiểm.

2. Đối với hệ thống

- Việc đảm bảo an toàn khi xác định định danh tài khoản của chủ thẻ thông qua số PIN nhập từ máy ATM cần được cải tiến, vì bản thân mật khẩu của người dùng đã được lưu trong CSDL của corebank nên nó đẻ ra hai lỗ hổng:

+ Khi mật khẩu (số PIN) nhập tại máy ATM có thể có những phần mềm của bọn hacker đã được cài sẵn vào trong đó sẽ thu được mật khẩu đó trước lúc nó được mã hóa được truyền đến Switch hoặc từ Switch đến corebank.

+ Rất có thể có nhân viên trong bộ phận quản trị hệ thống liên kết với hacker, lúc đó cả khóa bí mật có thể bị lộ và số PIN của khách hàng có thể lấy ra được dưới dạng bản rõ, như vậy rất nguy hiểm.

- Thông tin đi trên đường truyền của hệ thống đều được mã hóa. Thế nhưng ở phía hai đầu (tiền mã hóa và hậu mã dịch) là những sơ hở mà hacker chuyên nghiệp có tổ chức có thể moi được thông tin ngay từ đó mà không cần thám mã nữa.
- Thông tin trên đường truyền có thể bị thay đổi mà không bị phát hiện.
- Bọn tội phạm có thể tìm mọi cách truy cập trực tiếp CSDL để lấy trộm thông tin.

Qua các phân tích trên chúng tôi đề xuất một số các giải pháp sau

1) Gợi ý cách quản lý số PIN.
2) Sử dụng kỹ thuật hàm Hash để mã hóa số PIN.
3) Nhập số PIN không dùng bàn phím.
4) Bảo đảm toàn vẹn và xác thực nguồn gốc thông tin.
5) Mã hóa thông điệp.

Thiết lập kênh kết nối an toàn trong hệ thống ATM.

4.1 Gợi ý cách quản lý số PIN.

Đối với chủ thẻ cần phải hết sức cảnh giác, coi thẻ ATM và số PIN là một phần cuộc sống của mình, cần lưu ý một số vấn đề sau:

- Không truy cập tài khoản khi có người ở cạnh.
- Hãy nhớ số PIN để khi nhập số PIN không cần phải lấy ra xem.
- Tuyệt đối không lưu số PIN vào tờ giấy riêng.
- Không được lấy ngày tháng năm sinh của mình làm số PIN.
- Trước khi cho thẻ vào máy ATM, cần quan sát xem máy có gì bất thường không, nếu có thì báo ngay cho phía Ngân hàng.

Trường hợp sử dụng ngày tháng năm sinh (hoặc số chứng minh thư) làm số PIN thì có thể dùng theo cách sau. Dùng ngày tháng năm sinh cộng với một hằng số nào đó (theo modulo 10) có độ dài bằng số PIN và dùng kết quả đó làm số PIN (nếu độ dài lớn hơn độ dài số PIN thì lấy kết quả có độ dài bằng độ dài số PIN tính từ phải sang trái).

Ví dụ nếu lấy ngày sinh 08/08/2008 làm số PIN là 080808 thì có thể cộng thêm với số 686868 khí đó số PIN có được là 767676.

Ví dụ

080808

\+ 686868

= 767676

Với cách làm đơn giản trên, có thể giúp tạo và nhớ số PIN một cách đơn giản mà hiệu quả. Khi đó, nếu có mất chứng minh thư cùng thẻ ATM thì cũng không dễ để dò ra số PIN.

4.2. Sử dụng kỹ thuật hàm Hash để mã hóa số PIN.

4.2.1. Giới thiệu hàm Hash – hàm băm.

Hàm băm là hàm một chiều, nghĩa là một hàm mà biết giá trị đầu vào việc xác định giá trị đầu ra là dễ thực hiện, còn nếu biết giá trị đầu ra thì việc xác định giá trị đầu vào là bài toán 'khó'.

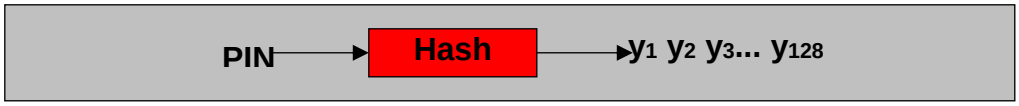
Việc dùng hàm Hash không cần sử dụng đến khóa để mã hóa mà chỉ cần quản lý giá trị Hash thôi, do đó việc bảo mật vừa đơn giản mà lại giảm bộ nhớ rất nhiều và thời gian tính toán cực nhanh. Các phép toán này hoàn toàn được cứng hóa.

Để bảo mật số PIN cho chủ thẻ, ta có thể dùng hàm hash mạnh, trong trường hợp này ta có thể sử dụng SHA-1 hoặc MD5 hoặc có thể tạo ra thuật toán hash riêng, việc này không đơn giản nhưng có thể kết hợp với các chuyên gia trên lĩnh vực an toàn thông tin thì có thể tạo ra hàm hash riêng cho mình.

Với kỹ thuật này, giá trị của số PIN lưu trong CSDL là giá trị đã được Hash. Khi đó để so sánh số PIN được nhập và từ máy ATM và số PIN lưu trong CSDL thì ta chỉ cần Hash số PIN được nhập vào và so sánh trực tiếp với số PIN đã được Hash trong CSDL.

4.2.2 Ứng dụng hàm Hash vào mã hóa số PIN.

Số PIN sau khi Hash sẽ có độ dài cố định.



Hình 4.1 Minh họa số PIN sau khi Hash

Để đảm bảo an toàn hơn ta thêm vào một thuật toán mã hóa rất đơn giản là phép chuyển vị. Đối với phép chuyển vị, độ dài khóa được lấy lớn hơn hoặc bằng 25 (không lấy các độ dài 4,8,16,32,64,….)

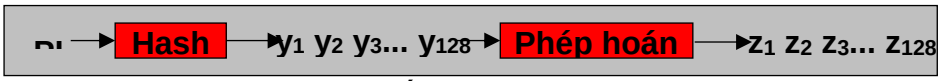
Quy trình mã hóa số PIN trong cơ sở dữ liệu như sau với h là hàm Hash còn π là phép chuyển vị:

PIN

→h(PIN) $= y_1\ y_2\ y_3 \ldots\ y_{128}\ , y_i \in \{0,1\}$

→π(h(PIN))$= z_1\ z_2\ z_3 \ldots\ z_{128,}\ z_i \in \{0,1\}$

Giá trị $z_1, z_2, \ldots, z_{128}$ sẽ được lưu vào CSDL, $z_i \in \{0,1\}$. Việc lưu các giá trị $z_1, z_2, \ldots, z_{128}$ chỉ cần đảm bảo tuyệt đối an toàn nhưng không cần thiết phải bảo mật, nghĩa là $z_1, z_2, \ldots, z_{128}$ phải không được sửa chữa, thay đổi, thêm bớt …vv chứ không cần bảo mật, thậm chí công khai cũng được.



Hình 4.2 Minh họa số PIN sau khi Hash sẽ được hoán vị

Khóa chuyển vị π được lấy tùy ý có độ dài

Ví dụ khóa $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \ldots 30 \\ 5 & 4 & 8 & 6 & 3 & 2 & 1 & 10 & 30 \ldots 7 \end{pmatrix}$

Giả sử $h(PIN) = y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7\ y_8\ y_9 \ldots\ y_{30} y_{31} y_{32} \ldots y_{128} = Y$

$\pi(Y) = y_5\ y_4\ y_8\ y_6\ y_3\ y_2\ y_1\ y_{10}\ y_{30} \ldots y_7 y_{31} y_{32} \ldots y_{128}$

- Ưu điểm của kỹ thuật này:

- Tốc độ mã hóa nhanh

- Giá trị PIN đã được Hash khi lưu trong CSDL sẽ chống lại được kẻ gian chính là trong nội bộ hệ thống.

- Giá trị PIN sau khi được Hash thì có thể không nhất thiết phải bảo mật.

4.3 Nhập số PIN không dùng bàn phím.

Số PIN có thể bị đánh cắp thông qua kỹ thuật "chặn bắt" bàn phím. Do đó sử dụng giải pháp không bàn phím sẽ hạn chế được số PIN bị đánh cắp thông qua kỹ thuật "chặn bắt" bàn phím.

Trên máy ATM được thiết kế một thiết bị giao tiếp có thể đọc được đĩa CD, đĩa mềm, ổ USB … (đề xuất dùng USB vì tính tiện lợi của nó), khi đó người dùng chỉ việc cắm USB đã lưu sẵn số PIN vào máy ATM và tiến hành tải số PIN vào máy mà không phải gõ PIN trực tiếp trên bàn phím.

Đối với giải pháp này thì người dùng phải đảm bảo an toàn cho USB của mình, USB chỉ được dùng khi nhập số PIN và không được dùng để trao đổi số liệu.

4.4 Bảo đảm toàn vẹn nguồn gốc thông tin (MAC- Message Authentication Code).

4.4.1 Định nghĩa MAC.

Trong quá trình truyền nhận thông tin, thì một vấn đề đặt ra là thông tin nhận được có bị thay đổi hay không. Do đó, ta sử dụng một trong các chế độ hoạt động của DES là CBC-Cipher Block Chaining Mode để tạo ra mã xác thực MAC.

MAC đảm bảo tính trung thực (xác thực), tính toàn vẹn dữ liệu và nguồn gốc của thông điệp giữa bên gửi và bên nhận (nhưng tất nhiên nó không cung cấp độ bảo mật).

MAC được bổ sung vào cuối của thông điệp.

Hình 4.3 Mô phỏng mã xác thực MAC được gắn vào cuối thông điệp.

4.4.2 Chế độ hoạt động CBC.

CBC-Cipher Block Chaining Mode có thể tạm dịch là chế độ liên kết khối mở.

Gọi $x = x_1,x_2,.., x_n$ là thông điệp cần gửi, $y = y_1,y_2,.., y_n$ là các khối mã hóa nhận được khi mã hóa các giá trị x_i tương ứng, trong đó x_i, y_i là các khối 8 byte.

Gọi $y_0 = 00000000$ là vecter khởi điểm dài 8 byte.

Tính y_i theo công thức sau:

$y_i = e_k(y_{i-1} \oplus x_i)$, i = 1, 2, …n

giá trị y_n chính là MAC.

Quá trình giải mã như sau: $x_i = y_{i-1} \oplus d_k(y_i)$, i=n, n-1,…,1

Trong đó: e_k là mã hóa DES theo khóa k.

d_k là giải mã DES theo khóa k.

là phép toán XOR modulo 2

4.4.3 Xác thực thông điệp MAC giữa ATM và hệ thống Switch.

Chọn $y_0 = 00000000$, sử dụng khóa WK làm khóa để mã hóa và giải mã khi đó k= WK. Dùng khóa k để thiết lập các khối mã hóa $y_1y_2…y_n$ theo CBC. Cuối cùng, xác định MAC là y_n.

Gửi thông điệp gốc ban đầu cùng với MAC.

Khi nhận được thông điệp, để kiểm tra xem thông điệp có bị thay đổi hay không ta có thể dùng theo hai cách sau:

1. Từ thông điệp gốc nhận được và khóa bí mật k, ta tính y_n theo CBC và kiểm tra y_n có trùng với MAC không.

2. Từ giá trị MAC nhận được và khóa bí mật k, ta tính $x=x_1x_2…x_n$ theo CBC và kiểm tra x có trùng với thông điệp gốc hay không.

4.5 Mã hóa thông điệp (KME Message Encryption Keys)

Sử dụng khóa WK để mã hóa thông điệp nhằm bản đảm an toàn thông điệp trên đường truyền.

Để đảm bảo về thời gian ta có thể mã hóa và giải mã các vị trí xác định của thông điệp (encrypt and decrypt a certain portion of the message).

Thông thường các giá trị được mã hóa sẽ là số tài khoản, số thẻ, số tiền giao dịch.

Thuật toán sử dụng

Sử dụng Thuật toán DES và khóa WK để mã hóa và giải mã các trường trong thông điệp đã chọn.

Input: Các trường được đề nghị số tài khoản, số thẻ, số tiền giao dịch (độ dài max của các trường là 64bit)

Output: Giá trị mã hóa của các trường, độ dài 64bit.

4.6 Bảo đảm an toàn trên đường truyền

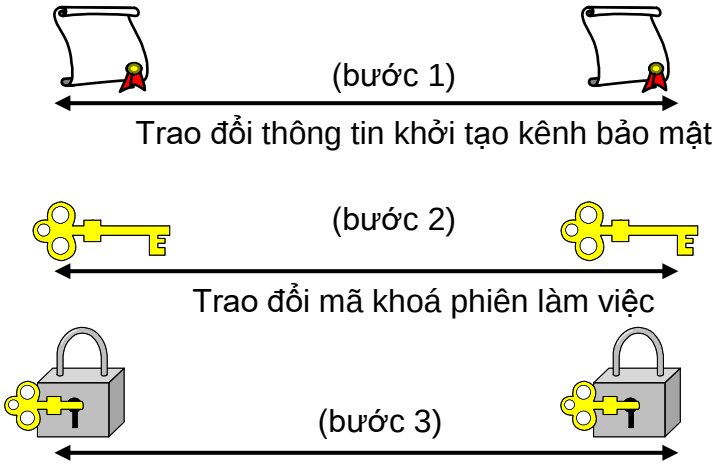
Để đảm bảo an toàn thông tin trên đường truyền, giữa ATM và Switch cần tạo ra một kênh kết nối riêng.

Phương thức mã hóa gồm có các bước sau:

Bước 1: Trao đổi thông tin khởi tạo kênh bảo mật.

Bước 2: Trao đổi khóa phiên làm việc.

Bước 3: Mã hóa toàn bộ thông tin trên kênh truyền giữa hai thiết bị.



Hình 4.4 Mã hoá thông tin trên kênh truyền giữa hai thiết bị

ATM và Switch sẽ tạo kênh kết nối trước khi chúng trao đổi dữ liệu với nhau. Khi tạo kết nối thành công thì kênh này được duy trì liên tục, còn khóa phiên làm việc được thay đổi theo chu kỳ. Có thể dùng thuật toán PGP10 - Pretty Good Privacy để bảo mật thông tin trên đường truyền.

KẾT LUẬN

Sau khi nghiên cứu đề tài "Tìm hiểu cơ chế an toàn và bảo mật của hệ thống ATM" có thể rút ra được một số kết luận sau đây.

1. Với các giải pháp về an toàn và bảo mật cho hệ thống ATM đã được nêu, thì hệ thống ATM an toàn cho người sử dụng.
2. Về phía người sử dụng, cần có ý thức hơn trong việc đảm bảo an toàn đối với các thẻ ATM của mình đó là giữ tuyệt đối an toàn cho số PIN, thẻ ATM và đảm bao an toàn khi giao dịch
3. Đối với Việt nam hiện nay thẻ từ đang phổ biến, nhưng do mức độ an toàn của thẻ từ là không cao (dễ bị làm giả, bị sao chép) do đó xu thế trong tương lai thẻ chip sẽ thay thế thẻ từ.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. AES (mã hóa) - Bách khoa toàn thư mở Wikipedia. Được lấy về tại: http://vi.wikipedia.org/wiki/AES_(m%C3%A3_h%C3%B3a).
2. Báo Tin học và Tài chính - Bộ tài chính số 58, (4/2008).
3. Banknetvn (2006), Tài liệu tiêu chuẩn kỹ thuật.
4. DES (mã hóa) - Bách khoa toàn thư mở Wikipedia. Được lấy về tại: http://vi.wikipedia.org/wiki/DES_(m%C3%A3_h%C3%B3a).
5. DIEBOLD (2007), Tài liệu giới thiệu hệ thống máy ATM.
6. Hiệp hội ngân hàng Việt nam, 10 năm phát triển của thị trường thẻ. Được lấy về tại: http://www.vnba.org.vn/index.php?option=com_content&task=view&id=374&Itemid=92.
7. Hồ Văn Canh (2003), Tài liệu giảng dạy.
8. NCR – MICROTEC (2007), Tài liệu giới thiệu hệ thống máy ATM.
9. Trịnh Nhật Tiến (2007), Tài liệu giảng dạy.

Tiếng Anh

10. ISO 8583-1987 MessFormat.
11. ISO_IEC_7810_2003(E)-Identification cards-Physical characteristics.
12. ISO_IEC_7811-1_2002(E)-Identification cards-Recording technique-Part 1-Embossing.
13. ISO_IEC_7812-1_2000(E)-Identification cards-Identification of issuers-Part 1-Numbering system.
14. ISO_IEC_7813_2001(E)-Identification cards-Financial transaction cards.