BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

-------o0o-------

NGHIÊN CỨU, TÌM HIỂU HỆ THỐNG RÚT TIỀN TỰ ĐỘNG ATM VÀ VẤN ĐỀ ATTT CỦA HỆ THỐNG

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
NGÀNH CÔNG NGHỆ THÔNG TIN

Giảng viên hướng dẫn: T.S Hồ Văn Canh
Sinh viên: Phạm Việt Anh
Lớp : CT1102

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 Đồ án.

Trước hết em xin gửi lời cảm ơn đến T.S 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 25 tháng 11 năm 2012

Sinh viên thực hiện

Phạm Việt Anh

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

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 và 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 người dân Việt Nam. Những tiện ích mà các dịch vụ thẻ mang lại đã góp phần từng bước thay đổi thói quen ưa 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, ưu nhược 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 ATM

Chương 2. Cấu trúc máy ATM và hệ thống thanh toán ATM

Chương 3. Thẻ từ, thẻ chip

Chương 4. Vấn đề an toàn thông tin trong hệ thống ATM

Chương 5. Chương trình thực hiện mã hóa và giải mã với hệ mã DES

Chương 1. TỔNG QUAN VỀ MÁY ATM VÀ HỆ THỐNG THANH TOÁN ATM

1.1 Giới thiệu về máy ATM và hệ thống thanh toán ATM

Máy rút tiền đầu tiên được thiết kế và hoàn thành bởi Luther George Simijian vào năm 1939, máy được thiết kế tại thành phố NewYork cho ngân hàng CityBank of NewYork nhưng 6 tháng sau thì bị bỏ đi vì ít người dùng.

Sau 25 năm 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 Sheperd-Barron mặc dù Luther George Simijian và 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 được ra mắt 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.

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 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)

1.2 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	4.500

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

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

1.3 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 hàng, 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.

Nhờ vậy, mà các ngân hàng có thể giữ được khách hàng cũ và nhiều người sử dụng các dịch vụ của ngân hàng.

Đối với khách hàng:

Thuận tiện trong tiếp cận ngân hàng

Nhanh hơn là chờ đợi ở các quầy giao dịch

1.4 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

Hình 2.1 Máy ATM nhìn từ phía trước.

Chương 2. CẤU TRÚC MÁY ATM VÀ HỆ THỐNG THANH TOÁN ATM

2.1 Cấu trúc máy ATM

2.1.1 Định nghĩa

ATM là máy giao dịch tự động được gọi là hệ thống ngân hàng 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, mua vé, các dịch vụ thương mại điện tử … được gọi là hệ thống giao dịch Ngân hàng tự động

2.1.2 Phân loại máy

a. Theo vị trí

- ATM đặt tại sảnh, hành lang
- ATM độc lập
- ATM thường xuyên
- ATM đặt tại nơi thu vé xe

b. Theo chức năng

- Máy chỉ có chức năng trả tiền
- Máy có các chức năng cao cấp

2.1.3 Luồng xử lý giao dịch trong hệ thống ATM

a. Các bước xử lý giao dịch

- Chủ thẻ thực hiện giao dịch
- ATM nhận thông tin giao dịch và gửi lệnh yêu cầu tới Switch
- Switch nhận yêu cầu, xử lý và phản hồi lại lệnh cho ATM
- ATM nhận lệnh phản hồi từ Switch và thực hiện lệnh
- ATM nếu không thực hiện được lệnh phản hồi sẽ gửi hủy bỏ lệnh đã yêu cầu
- Switch sẽ chấp nhận yêu cầu hủy lệnh

b. Luồng giao dịch của hệ thống ATM

- Màn hình đợi (màn hình hiển thị quảng cáo của ngân hàng)

- Cho thẻ vào ATM và nhập số PIN

- Kiểm tra số thẻ: kiểm tra số check digit, số CVV/CVC

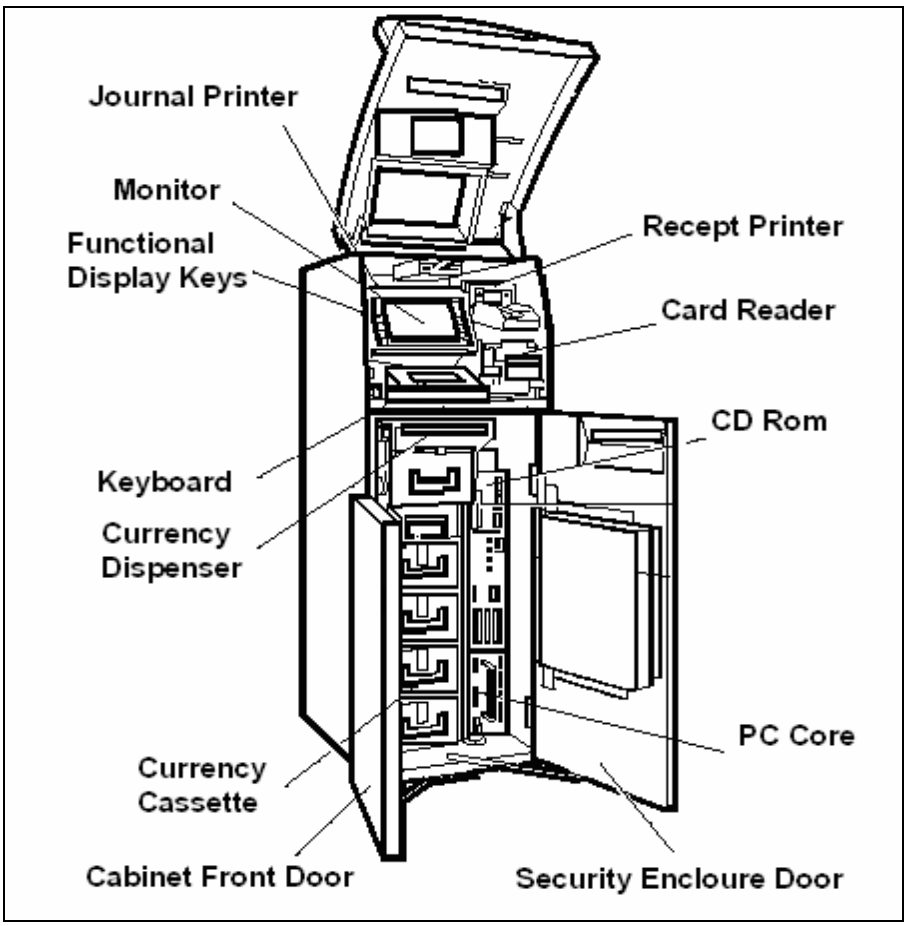
- Kiểm tra PIN: kiểm tra số PIN được nhập vào với PIN được lưu trong CSDL Corebank của ngân hàng, nếu đúng sẽ hiển thị các loại giao dịch để chủ thẻ lựa chọn

- Thực hiện giao dịch: Khi thực hiện thành công, thì tùy theo từng loại giao dịch mà ATM nhả thẻ hoặc không (thường thì rút tiền xong ATM sẽ nhả thẻ)

- Trở về màn hình đợi: Khi không thực hiện các giao dịch nữa (khi nhả thẻ hoặc nuốt thẻ) màn hình ATM trở về trạng thái ban đầu.

2.1.4 Cấu tạo máy

ATM là một thiết bị chuyên dụng được sử dụng trong lĩnh vực ngân hàng, được gọi là 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.



Hình 2.2 Cấu tạo cơ bản của một máy ATM.

Cấu tạo máy ATM gồm 2 phần là phần cứng và phần mềm.

a. Phần cứng

Bao gồm máy vi tính chuyên biệt, thiết bị đếm tiền, thiết bị trả tiền, thiết bị in nhật ký, thiết bị in biên lai, phím nhập mật mã, thiết bị đọc thẻ, hộp đựng tiền và két sắt chứa hộp đựng tiền.

b. Phần mềm

Máy ATM đều có hệ điều hành (OS-operate system), phần mềm điều khiển thiết bị của máy ATM, phần mềm tiện ích kèm theo.

Hiện nay, hệ điều hành là Window NT, Window XP.

2.1.4.1 Màn hình

Có thể là màn hình CRT hoặc màn hình LCD. Hiển thị các hướng dẫn và thông tin của mỗi bước giao dịch. Trong trường hợp màn hình chờ thì hiển thị thông tin quảng cáo của từng ngân hàng.

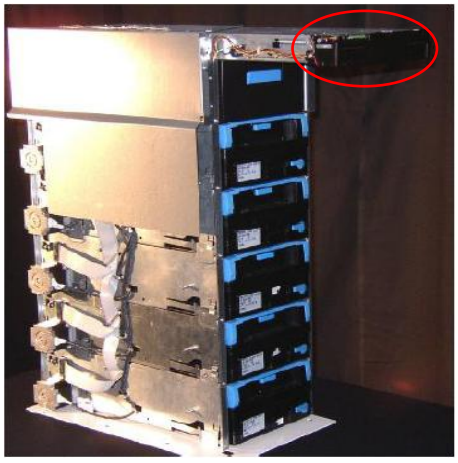
Ví dụ:

- Màn hình của Deibold 10.4'' Color LCD (XGA)

- Màn hình của NCR 9'' LCD text only or 9.5'' VGA flat panel LCD

2.1.4.2 Bộ phận trả tiền

Đây là bộ phận quan trọng của mỗi máy ATM, giúp máy phân loại, đếm và cung cấp tiền cho chủ thẻ. Bao gồm máy đếm tiền, băng truyền tải và khe trả tiền được đặt trên các hộp đựng tiền. Khi thực hiện rút tiền, phần mềm điều khiển ATM sẽ tính toán số tiền được trả theo nhiều mệnh giá khác nhau, được cấu hình theo yêu cầu của ngân hàng.



Hình 2.3 Thiết bi trả tiền và

Máy đếm tiền chủ yếu sử dụng kỹ thuật đếm chân không (kéo tiền lên bằng lực hút), ngoài ra còn dùng kỹ thuật ma sát để lấy tiền trong các hộp đựng tiền.

Có thể trả được 40-50 tờ tiền trong một lần trả. Có thể trả được 1 đến 4 loại tiền.

Hình 2.4 Bàn phím chức năng.

2.1.4.3 Bàn phím

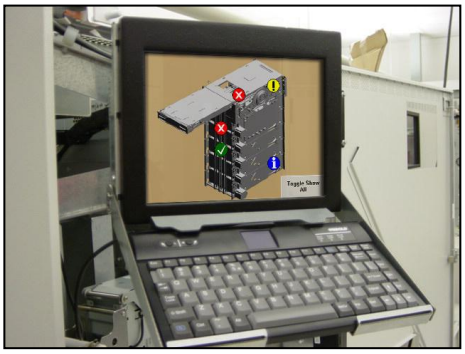
Gồm có hai loại: bàn phím chức năng và bàn phím ký tự.

a. Bàn phím chức năng

Dùng để thực hiện các giao dịch. Chủ thẻ sử dụng bàn phím đẻ nhập mã PIN, số tiền giao dịch, số tài khoản….

Nếu chủ thẻ nhập số PIN sai 3 lần liên tiếp máy ATM sẽ tự động nuốt thẻ (tùy thuộc chính sách ngân hàng), nhằm đảm bảo an toàn trong trường hợp thẻ bị đánh cắp và cố tình dò số PIN.

Bàn phím của máy ATM cũng chính là một thiết bị mã hóa, được mã hóa theo thuật toán DES hay TripleDES bằng thiết bị phần cứng.



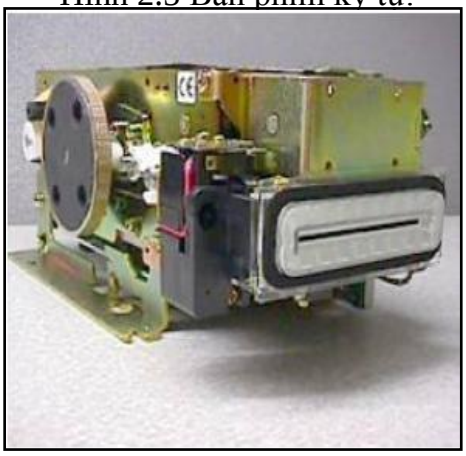
Hình 2.5 Bàn phím ký tự.

b. Bàn phím ký tự

Dùng để thực hiện nhập tham số cho hệ thống phần mềm ATM (như bàn phím thông thường của máy PC). Được dùng cho nhà quản trị.

2.1.4.4 Đầu đọc thẻ

Đọc các thông tin trên rãnh từ ở mặt sau của thẻ. Các thông tin này sẽ được gắn vào thông điệp và chuyển đến ngân hàng nơi chủ thẻ mở tài khoản. Đầu đọc thẻ được thiết kế để có thể đọc được hai loại thẻ là thẻ từ và thẻ chip.

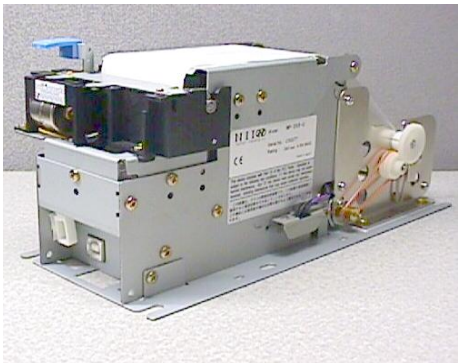


Hình 2.6 Đầu đọc thẻ

2.1.4.5 Máy ghi nhật ký giao dịch

Ghi lại thông tin toàn bộ các giao dịch được thực hiện tại máy ATM

Các thông tin này sẽ được sử dụng để kiểm soát và đối chiếu khi kiểm quỹ và yêu cầu tra soát của chủ thẻ

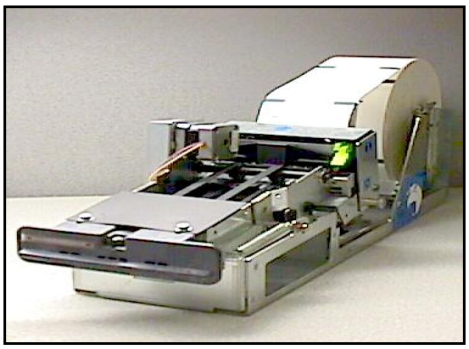


Hình 2.7 Máy ghi nhật ký giao dịch.

2.1.4.6 Máy in biên lai giao dịch

Thông thường sau mỗi giao dịch máy sẽ tự động in biên lai, giúp người sử dụng ATM dễ dàng nắm bắt được thông tin của lần giao dịch đó

Thông tin trên biên lai giao dịch tùy thuộc ngân hàng và tùy theo từng loại giao dịch. Thông thường bao gồm: tên ngân hàng, ngày tháng giao dịch, mã máy ATM, khối lượng giao dịch.



Hình 2.8 Máy in biên lai giao dịch.

2.1.4.7 Máy PC (core) điều khiển

Là một máy tính PC chuyên dụng được dùng cho máy ATM.

Máy PC này thông thường chạy hệ điều hành Window XP hoặc Window NT (hiện nay Microsoft ngừng hỗ trợ hệ điều hành Window NT nên các dòng máy mới dùng hệ điều hành Window XP).

Hình 2.9 Máy tính (Core) điều khiển.

Trên mỗi PC sẽ cài đặt một phần mềm dùng để kiểm soát các hoạt động của ATM

- Với máy Diebold là Agilis ™

- Với máy NCR là APTRA

2.1.4.8 Khay chứa tiền

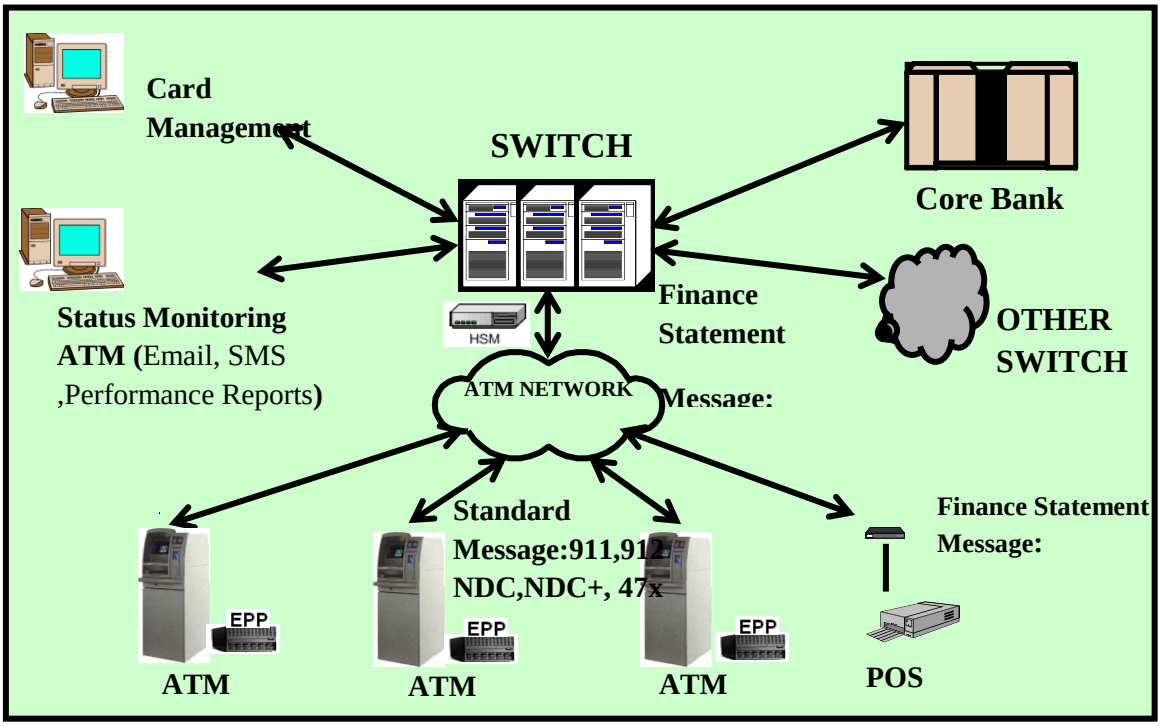
Mỗi máy ATM thường có 4 -5 khay đựng tiền, tùy theo nhà sản xuất mỗi khay đựng tiền sẽ được cấu hình theo từng mệnh giá tiền khác nhau. Ngoài ra máy còn có các hộp để đựng tiền xu. Mỗi khay đựng tiền thường chứa khoảng 3000 đến 4000 tờ tiền.

Hình 2.10 Khay chứa tiền.

2.2 Cấu trúc hệ thống thanh toán ATM

2.2.1 Tổng quan hệ thống thanh toán ATM

Hệ thống thanh toán 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 24x7 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 2.11 Mô tả một hệ thống ATM của một ngân hàng, trong đó:

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 được gọi là hệ thống chuyển mạch) được kết nối trực tiếp với Core bank và các thiết bị đầu cuối ATM, POS.

Swich 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:

- Quản lý thẻ (Card management): cho phép kết nối đến hệ thống quản lý các thiết bị sản xuất thẻ, giám sát và quản lý các thẻ được phát hành.

- Kết nối các thiết bị đầu cuối như ATM, POS….

- Giám sát và điều khiển toàn bộ hệ thống.

- Ghi nhật ký và lưu vết giao dịch.

- Hệ thống cung cấp các giao tiếp với thiết bị mã hóa cứng HSM, đảm bảo mã hóa và 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, Master Card, Euro pay…..

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 mai 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……

2.2.2 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 hoặc IP động.

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

Ở Việt Nam, máy ATM 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, mega-wan, Dial-up…..

Chương 3. THẺ TỪ, THẺ CHIP

3.1 Hệ thống thanh toán cho thẻ từ

3.1.1 Thẻ từ

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

3.1.1.1 Tính chất vật lý 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 tiêu chuẩn ISO 7810.

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

- Thẻ có 4 loại kích thước khác nhau:

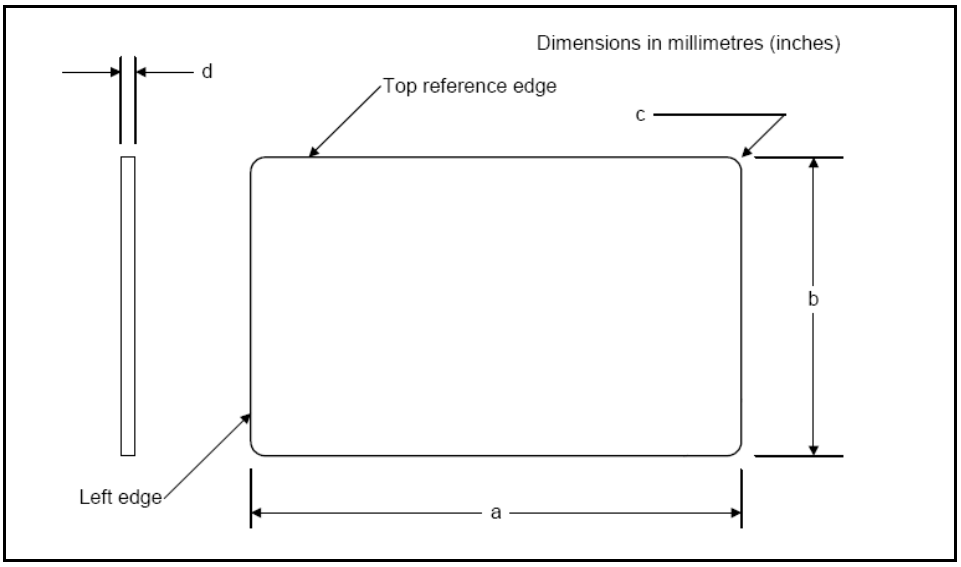
+ ID-000: Dài 25mm Rộng 15mm Dầy 0.76mm

+ ID-1 : Dài 85.60mm Rộng 53.98mm Dầy 0.76mm

+ ID-2 : Dài 105mm Rộng 74mm Dầy 0.76mm

+ ID-3: Dài 125mm Rộng 88mm Dầy 0.76mm

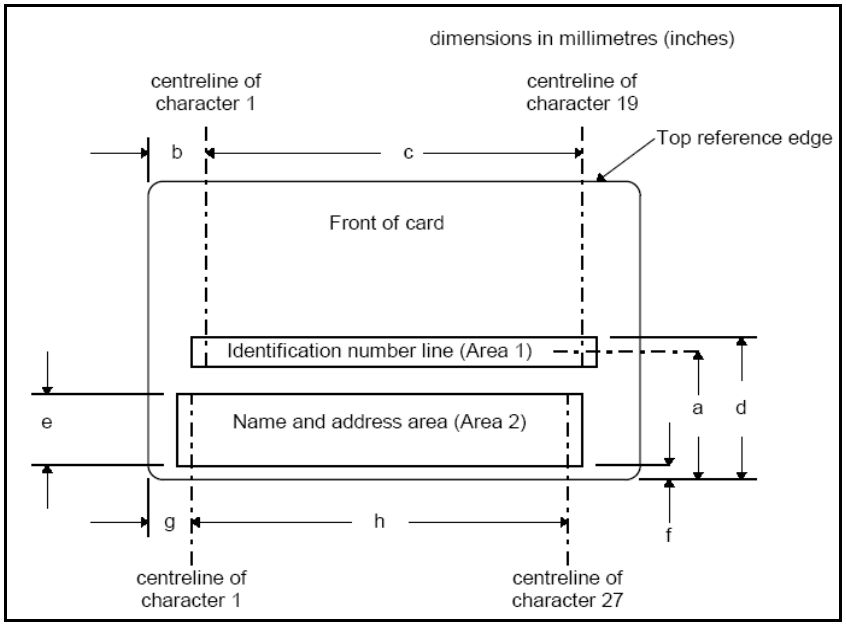
Thẻ ATM là loại thẻ ID-1.



Hình 3.1 Kích thước thẻ

3.1.1.2 Thông tin dập nổi trên thẻ

Các thông tin dập nổi trên thẻ tuân theo chuẩn ISO7811-1



Hình 3.2 Các vị trị dập nổi trên thẻ

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

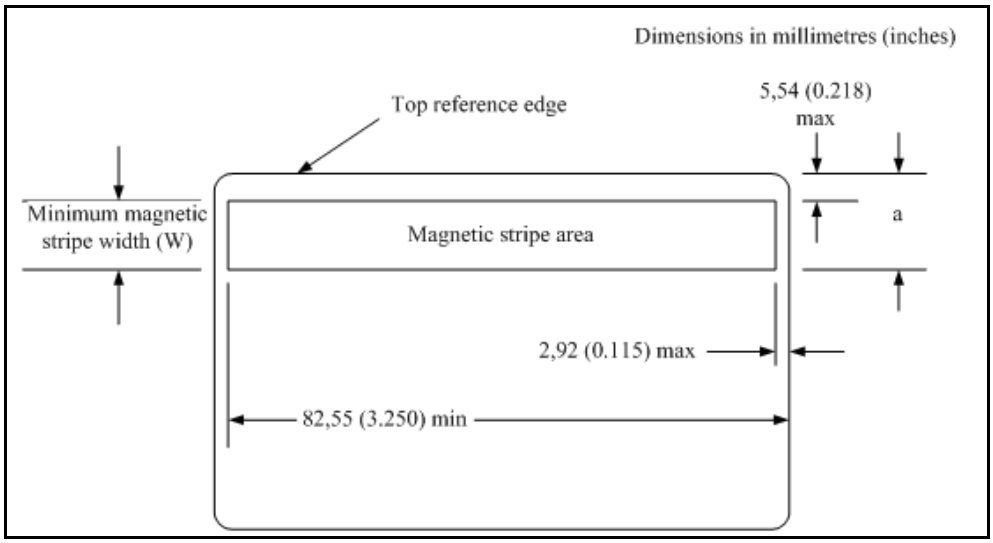
Trên thẻ có hai khu vực dập nổi:

- Khu vực 1 (Area 1) – được sử dụng để dập nổi định dạng thẻ (Indentification number), được tiến hành dập nổi trên một dòng đơn, tối đa là 19 ký tự.

- Khu vực 2 (Area 2) – được sử dụng để dập nổi tên, địa chỉ và các thông tin liên quan đến chủ thẻ, được dập nổi trên 4 dòng với tối đa là 27 ký tự.

3.1.1.3 Thông tin lưu trên vạch từ của thẻ

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

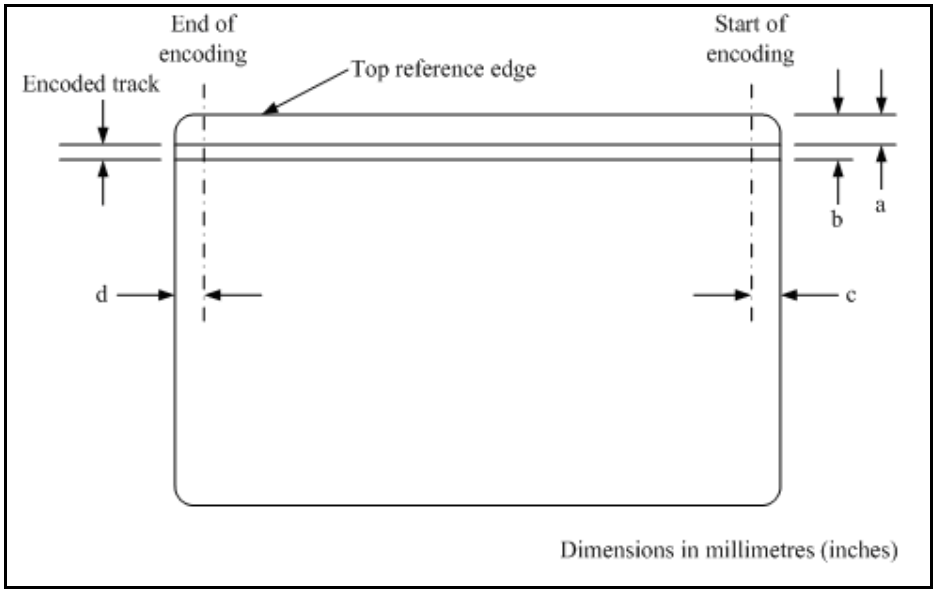


Hình 3.3 Vị trí dải từ (mặt sau thẻ)

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 3.4 Vị trí 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 3.2 Bảng định nghĩa kích thước vị trí rãnh từ, đơn vị milimet (Inches)

Các chuẩn này qui định trên thẻ gồm 3 tracks nhưng thường chỉ sử dụng track 1 và 2.

- Track 1 là track tuân theo chuẩn IATA (International Air Bansport Association). 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 Thrid) với mật độ ghi cao, chỉ chứa ký tự số nhưng có khả năng ghi đè lên thành phần dữ liệu đã có.

Thông tin về các tính chất, mật độ ghi,… trên từng Track của thể 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)*	$2^4=16$

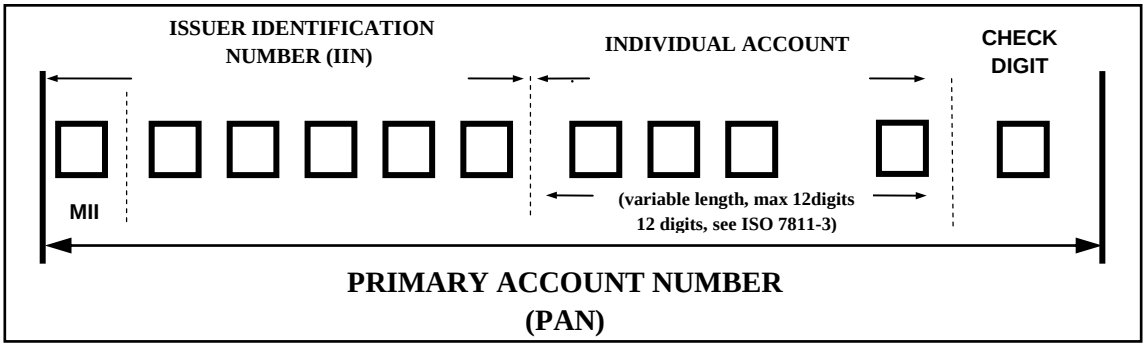
Bảng 3.3 Bảng mô tả định nghĩa các Track

3.1.2 Cấu trúc của số thẻ

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

3.1.2.1 Số PAN

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



Hình 3.5 Cấu trúc số PAN

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

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

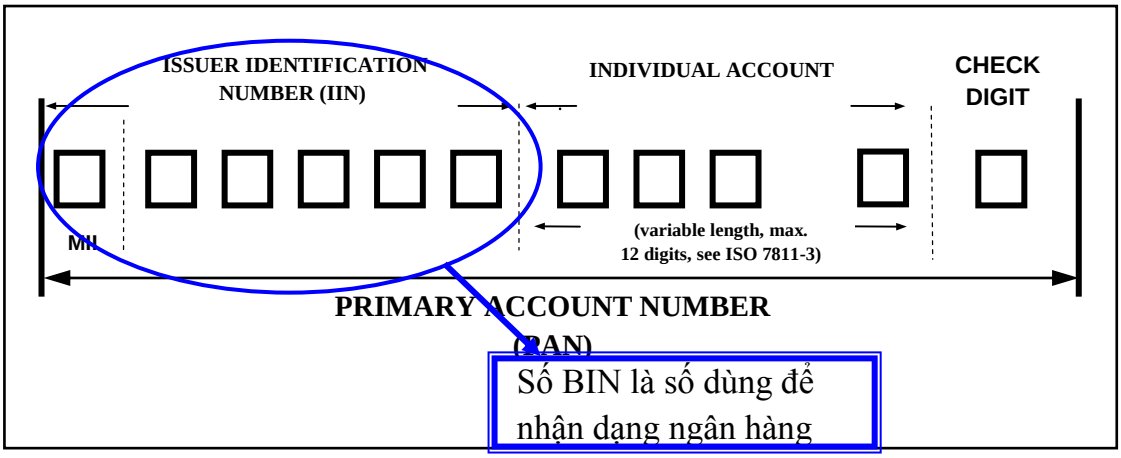
2. IAI – Individual Account Identification: số nhận dạng tài khoản chủ thẻ. Các ngân hàng có thể qui định cấu trúc trong trường thông tin này.

3. 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.

3.1.2.2 Số IIN (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 đội dài là 6 chữ số, là một thành phần trong số PAN.



Hình 3.6 Vị trí số BIN

Minh họa cách đánh số BIN của một số ngân hàng của Việt Nam

Tên các ngân hàng	**Số BIN**	**Số thẻ - PAN**
Ngân hàng Nông nghiệp và Phát triển Nông thôn (VBARD)	**272728**	**272728**000000000-**272728**999999999
Ngân hàng Đầu tư và Phát triển (BIDV)	**668899**	**668899**000000000-**668899**999999999
Ngân hàng Công thương (ICB)	**621060**	**621060**000000000-**621060**999999999
Ngân hàng Á Châu (ACB)	**999907**	**999907**000000000-**999907**999999999
Ngân hàng Sài Gòn Thường Tín (Sacombank)	**627128**	**627128**000000000-**627128**999999999
Ngân hàng Đông Á (EAB)	**179200**	**179200**000000000-**179200**999999999
Ngân hàng Sài Gòn Công Thương (SCICB)	**161087**	**161087**000000000-**161087**999999999

Bảng 3.4 Bảng số Bin của một số ngân hàng.

3.1.3 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 đang được sử dụng.

- Thông điệp chuẩn của hàng 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

3.1.3.1 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 Withdrawl (CWD).

3. Đổi PIN – PIN Change (PIN).

4. Vấn tin và in sao kê – Balance Inquiry anh Mini Statement (INQ).

5. Chuyển khoản – Funds Transfer (TFR).

6. Yêu cầu truyền khóa – Request Tranmission Key (RQK).

a. 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 tiền	1	0 – 2	Note 2
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:

1. Các trạng thái được định nghĩa

0 - good

1 - low

2 – out

2. Các trạng thái được định nghĩa

0 - Normal

1 - Missing

2 - Inoperative

b. Thông điệp xác thực pin (PNV)

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã xử 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

c. Thông điệp rút tiền (CWD)

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã xử 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

d. Thông điệp đổi PIN

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1-14	Message Header		24		Mã xử 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

e. Thông điệp vấn tin (INQ)

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	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

f. 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

g. Thông 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

3.1.3.2 Thông điệp từ Switch đến ATM

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

a. Phản hồi chấp nhận xác thực PIN – Accepted Response to PIN Verification (PNV)

b. Phản hồi từ chối xác nhận PIN – Rejected Response to PIN Verification (PNV)

c. Phản hồi chấp nhận rút tiền – Accepted Response to Cash Withdrawal (CWD)

d. Phản hồi từ chối rút tiền – Rejected Response to Cash Withdrawal (CWD)

e. Phản hồi chấp nhận đổi PIN – Accepted Response to PIN Change (PIN)

f. Phản hồi chấp nhận vấn tin tài khoản và in sao kê – Accepted Response to Balance Inquiry & Mini Statement (INQ)

g. Phản hồi chấp nhận chuyển khoản – Accepted Response to Funds Transfer (TFR)

a. Phản hồi chấp nhận xác thực PIN – Accepted Response to PIN Verification (PNV)

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

Chú ý:

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:987654312:CUR:456123798:

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

b. Phản hồi từ chối xác nhận PIN – Rejected Response to PIN Verification (PNV)

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		YYYYMMDDHHMM
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

c. Phản hồi chấp nhận rút tiền – Accepted Response to Cash Withdrawal (CWD)

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 dịch	8		
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

d. Phản hồi từ chối rút tiền – Rejected Response to Cash Withdrawal (CWD)

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

e. Phản hồi 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		YYYYMMDDHHMM
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

3.2. Hệ thống thanh toán cho thẻ chip

3.2.1 Thẻ chip

Thẻ chip – chipcard 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.

3.2.2 Sự phát triển của thẻ chip

Giữa những năm 80, Châu Âu đã triển khai những chiếc thẻ thông minh đầu tiên, giờ đây phạm vi sử dụng của thẻ thông minh đã được mở rộng ra trên toàn thế giới.

Thẻ thông minh cung cấp rất nhiều tính năng vượt trội so với thẻ từ truyền thống như khả năng lưu trữ lớn, khả năng bảo mật an toàn thông minh, hỗ trợ nhiều ứng dụng.

Hiện nay các tổ chức thẻ quốc tế như Europay, MasterCard, Visa – EMV đang thúc đẩy việc chuyển đổi từ thẻ từ sang thẻ SmartCard trên phạm vi toàn cầu. Theo EMV từ ngày 1/1/2006, khi tham gia vào hệ thống của các tổ chức này các ngân hàng sẽ phải chuyển đổi sang sử dụng thẻ thông minh đạt chuẩn EMV. Nếu không các ngân hàng sẽ phải chịu toàn bộ rủi ro do gian lận thẻ gây ra.

Việc thay đổi từ thẻ từ sang thẻ thông minh đối với Việt Nam không thể diễn ra trong chốc lát. Các thẻ từ có thể tiếp tục được sử dụng trong nhiều năm nữa. Trong quá trình chuyển đổi, các thiết bị đầu cuối, các mạng thanh toán và các hệ thống máy chủ phải hỗ trợ cả 2 loại thẻ.

Quá trình chuyển dịch đòi hỏi các ngân hàng phải thực hiện những thay đổi mang tính hệ thống trên hệ thống phát hành thẻ, hệ thống chuyển mạch tài chính, hệ thống giao dịch đầu cuối ATM/POS vì công nghệ phát hành và thanh toán thẻ thông minh có sự khác biệt lớn so với công nghệ thẻ từ truyền thống, có những thành phần phải được đầu tư nâng cấp nhưng cũng có những thành phần mới phải đầu tư riêng. Sự tốn kém đầu tư là không nhỏ, vì vậy lý giải tại sao các nước, các ngân hàng chưa thể đồng loạt chuyển từ sử dụng thẻ từ sang thẻ thông minh một cách nhanh chóng được.

Tuy nhiên, vai trò của thẻ từ chỉ đến 1 ngưỡng nhất định. Khi hệ thống an toàn không còn đảm bảo nữa việc chuyển sang sử dụng thẻ thông minh là việc làm tất yếu, hợp xu thế.

3.2.3 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 3 DES, 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 ký số là RSA, hàm băm là SHA-1, MACing và việc mã hóa các thông điệp theo từng phiên thì chỉ sử dụng 3DES.

Chip trên thẻ được cập nhật hay lập trình lại một cách an toàn khi đang sử dụng. Ngân hàng 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.

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.

Chương 4. VẤN ĐỀ AN TOÀN THÔNG TIN TRONG 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.

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)

4.1 Mã hóa trong hệ thống ATM

4.1.1 Thuật toán mã hóa

Trong hệ thống ATM hiện nay thường dùng thuật toán DES và 3DES để mã hóa và giải mã dữ liệu.

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

4.1.1.1 Thuật toán mã hóa 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, K. Khóa K được xây dựng từ bộ ba khóa 64 bit (K1, K2, K3) có độ dài 3*64 = 192 bit.

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

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

4.1.1.2 Xây dựng khóa K1, K2, K3

a. Key single length (Bộ một khóa 64 bit)

K1= K2= K3

Độ dài khóa 64 bit

b. Key double length (Bộ hai khóa 64 bit)

K1# K2 và K3=K1

Độ dài khóa 128 bit

c. Key triple length (Bộ ba khóa 64 bit)

K1# K2# K3# K1

Độ dài khóa 192 bit

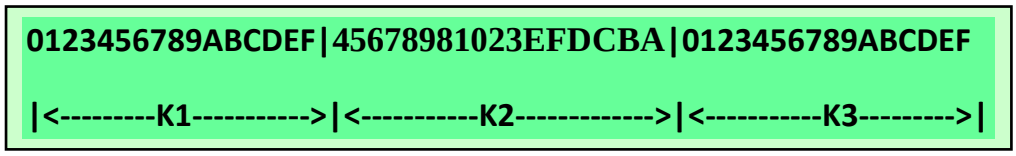
Trường hợp này không gian khóa 3*56 = 168 bit

4.1.1.3 Ví dụ

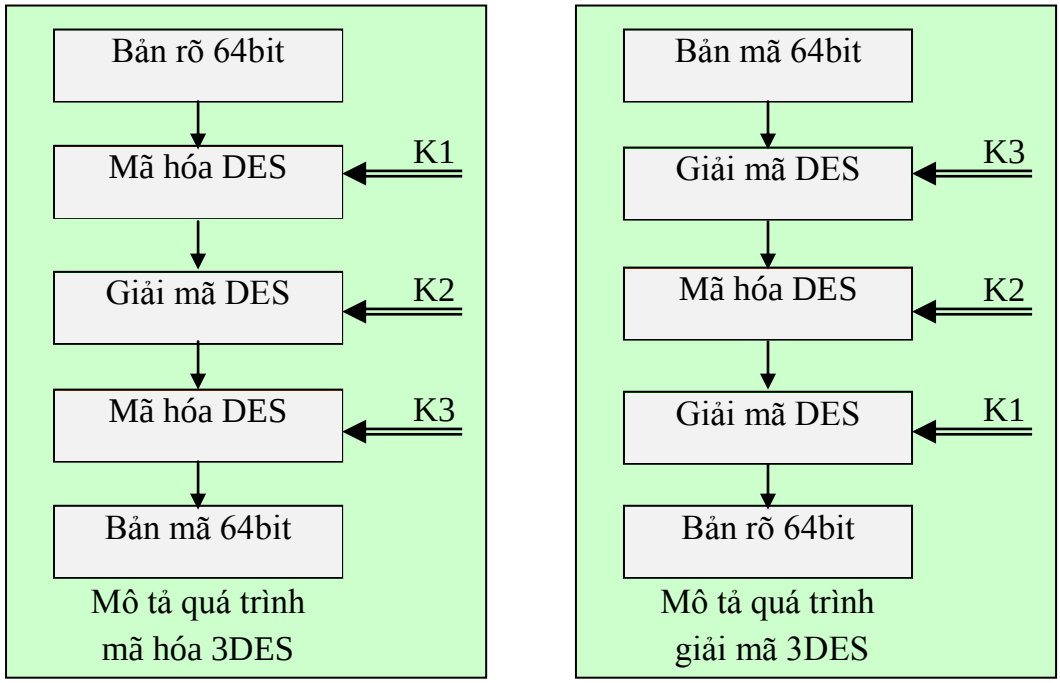
Key double length

K=
0123456789ABCDEF45678981023EFDCBA0123456789ABCDEF

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



4.1.1.4 Quá trình mã hóa và giải mã



Hình 4.1 Các bước thực hiện trong quá trình mã hóa và giải mã 3DES

4.1.2 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 64 bit, 128 bit hoặc 192 bit tùy theo cách sử dụng khóa hoặc chọn mã hóa DES hay 3 DES.

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 ra 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.

4.1.2.1 Định nghĩa các khóa trong hệ thống ATM

a. Khóa LMK- Local Master Keys

LMK được tạo thành 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 64 bit, 128 bit hoặc 192 bit.

b. 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 64 bit, 128 bit hoặc 192 bit.

c. 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 64 bit, 128 bit hoặc 192 bit.

d. Khóa WK – Working Keys (hay PIN Encryption Pad)

Khóa WK được sinh ra 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 hóa bởi khóa LMK và lưu trong CSDL của Switch.

- Bản mã thứ hai được mã hóa 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 ngân hàng, 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 64 bit, 128 bit hoặc 192 bit.

e. 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.

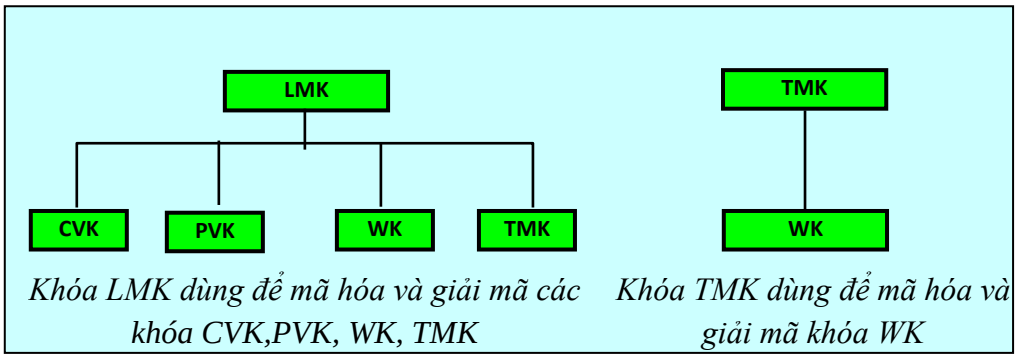
- Tại Switch khóa được lưu trong CSDL dưới dạng bản mã, mã hóa bởi LMK.

Khóa này chỉ được thay đổi khi có yêu cầu, khi thay đổi thì nhân viên kỹ thuật thực hiện.

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

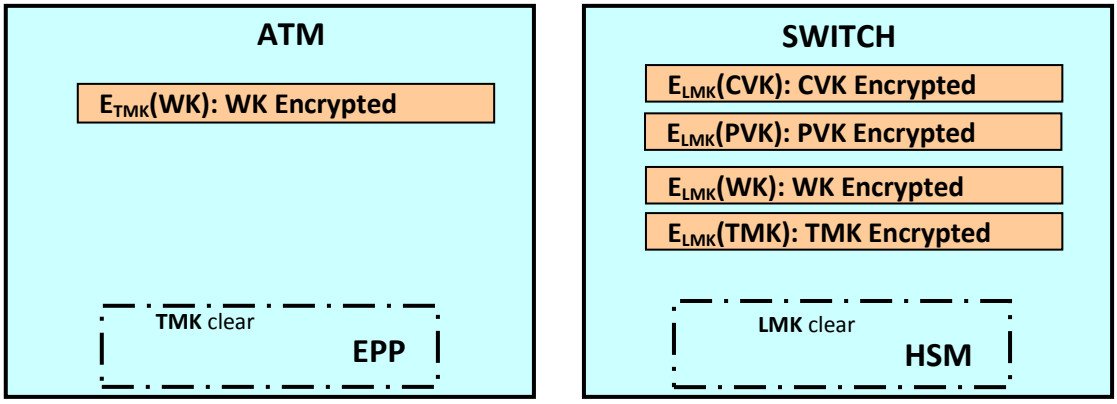
4.1.2.2 Sơ đồ phân cấp khóa trong hệ thống ATM

Các khóa trên được phân cấp như sau:



Hình 4.3 Phân lớp các khóa sử dụng trong hệ thống ATM

Mô tả vị trí các khóa trong hệ thống ATM



Hình 4.3 Mô tả vị trí các khóa trong ATM và Switch

- Tại ATM

+ TMK được lưu dưới dạng bản rõ trong thiết bị EPP

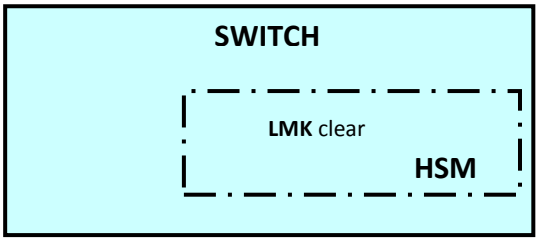
+ WK được mã hóa bởi TMK và lưu trong CSDL của máy ATM.

- Tại Switch

+ CVK, PVK, WK, TMK được mã hóa bởi LMK và lưu trong CSDL của Switch.

4.1.2.3 Trao đổi khóa giữa ATM và Switch

a. Thiết lập khóa LMK cho HSM

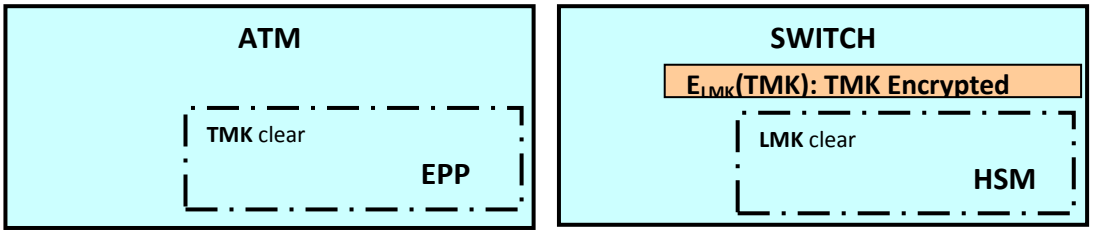


Hình 4.4 Thiết lập khóa LMK cho HSM

1. Tạo khóa LMK ngay trong HSM

2. Lưu LMK dưới dạng bản "rõ" trong HSM và một bản dự phòng được lưu trong một smartcard (smartcard cũng được bảo mật).

b. Thiết lập khóa TMK cho EPP



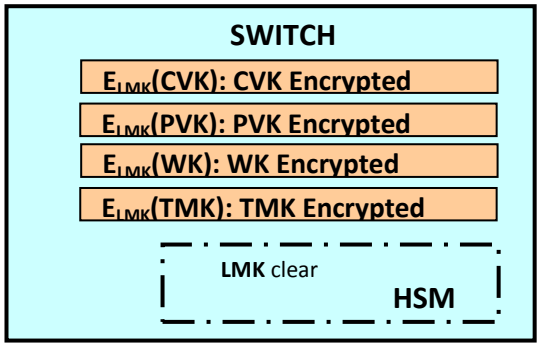
Hình 4.5 Thiết lập khóa TMK cho EPP

1. Khóa TMK được tạo trong HSM

2. Một bản rõ lưu tại EPP

3. Một bản mã lưu tại Switch (được mã hóa bởi khóa LMK)

c. Thiết lập các khóa khác tại Switch

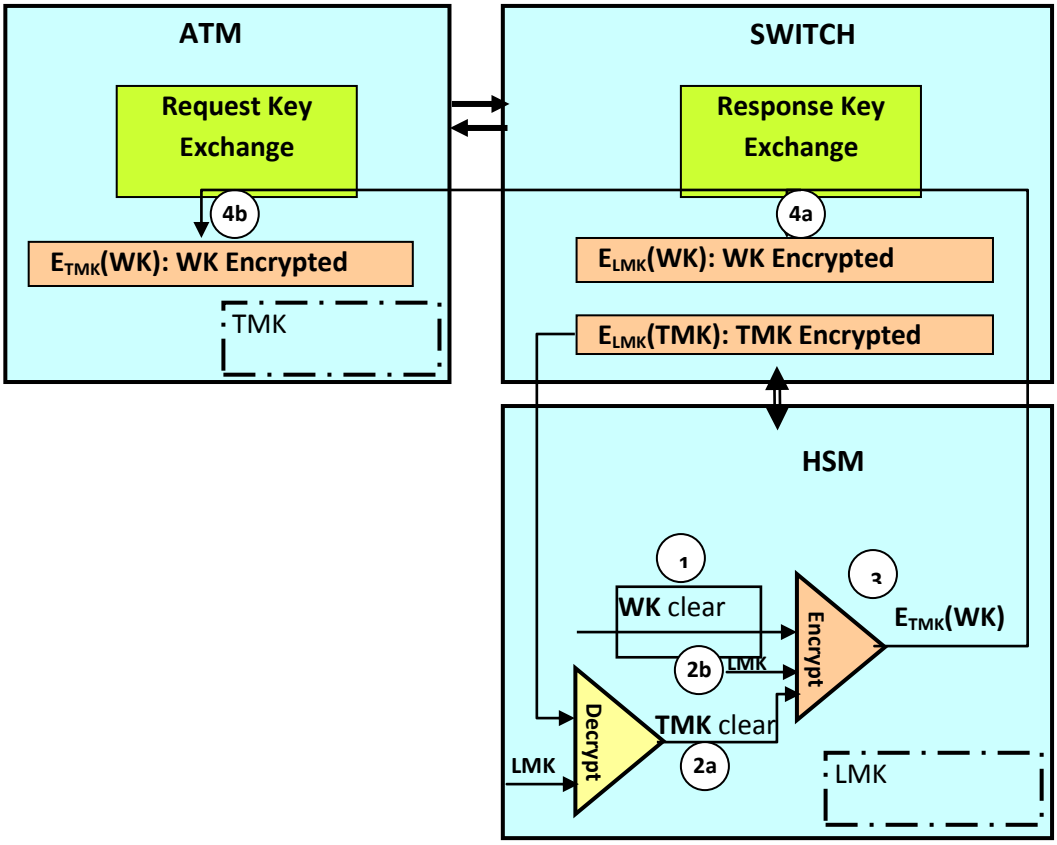


Hình 4.6 Thiết lập các khóa khác tại Switch

1. Tất cả các khóa trên đều được sinh trong HSM và được mã hóa bởi khóa LMK.

2. Các bản mã các khóa trên được lưu trong CSDL của Switch, không lưu bản rõ

d. Trao đổi khóa WK giữa ATM và Switch



Hình 4.7 Các bước trao đổi khóa giữa ATM và Switch

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

1. HSM tạo bản rõ khóa WK

2. Bản mã TMK được giải mã bởi khóa LMK trong HSM

3. Bản rõ WK sẽ được mã hóa bởi khóa LMK và TMK

4. 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

4.1.3 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.

Thiết bị này như là một "hộp đen", toàn bộ quá trình được thực hiện bên trong ta chỉ cần quan tâm đến giá trị đầu vào và kết quả đầu ra.

4.1.3.1 Thiết bị EPP (Encrypt PIN Pad)

Hình 4.8 Thiết bị mã hóa EPP.

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 ký bản rõ nào của số PIN chỉ lưu bản mã.

Hình 4.9 Thiết bị mã hóa HSM.

4.1.3.2 Thiết bị HSM (Hardware Security Module)

HSM là thiết bị mã hóa cứng dùng để mã hóa và giải mã, đây là một phần của hệ thống Switch. Toàn bộ quá trình mã hóa, giải mã và so sánh số PIN đều thực hiện bên trong thiết bị HSM.

Các thiết bị này đều lưu trữ các khóa bí mật và đảm bảo các tính chất sau:

+ Không truy cập hoặc xác định được bản rõ của bất kỳ khóa 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.

Với các thiết bị mã hóa cứng này và cách mã hóa và giải mã hạn được những sơ hở ở phía hai đầu (tiền mã hóa và hậu mã dịch), đây là những sơ hở mà hacker chuyên nghiệp có tổ chức có thể moi thông tin ngay từ đó mà không cần "thám mã" nữa.

4.2 Mã hóa và giải mã số PIN

Hệ thống sử dụng thiết bị phần cứng để mã hóa và giải mã số PIN. Các thiết bị 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 EPP hay HSM.

4.2.1 Khái niệm 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.

4.2.2 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 khóa được cấu hình (thỏa 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 64 bit.

Quá trình xác thực PIN sẽ được làm ở HSM, giá trị trả về của HSM sẽ cho biết số PIN nhập là đúng hay là sai.

4.2.2.1 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 Bít	1-4	5-8	9-12	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:

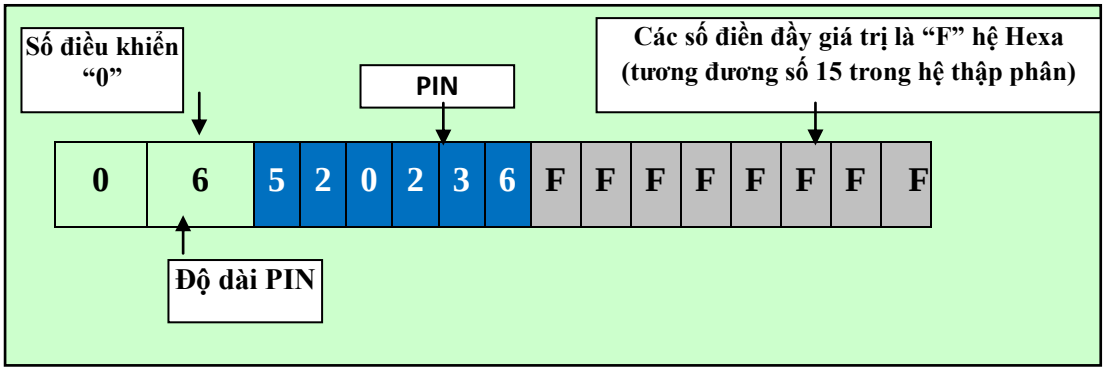
0 = Pad digit	Trường 4 bit có giá trị là 0 (thể hiện dạng nhị phân 0000)
A1 … A12 = account number A1 đến A12 thuộc [0,..,9]	12 số bên phải của số PAN ngoại trừ check digit (bỏ số cuối cùng bên phải). A12 là số đứng trước check digit của số PAN. Nếu số PAN không tính check digit mà nhỏ hơn 12 số thì 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= 520236 có độ dài là 6 chữ số.

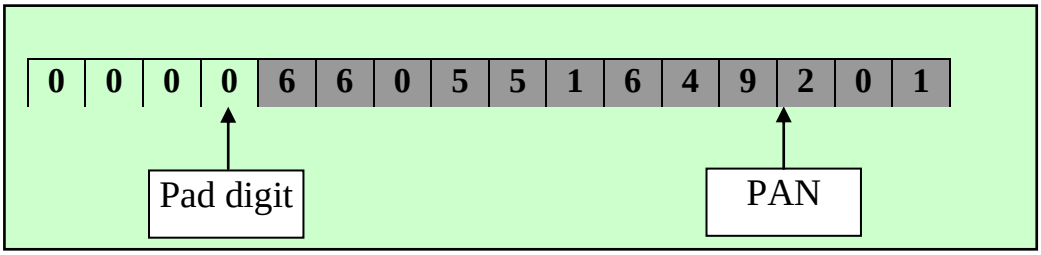
Số PAN = 9704366605516492016 có độ dài là 19 chữ số

Khuôn dạng trường số PIN:



Hình 4.10 Minh họa khuôn dạng trường số PIN

Khuôn dạng trường số PAN:



Hình 4.11 Minh họa khuôn dạng trường số PAN

Khối PIN Block được tính như sau:

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

Hình 4.12 Minh họa cách tính khối PIN Block

Khối PIN Block là: 06526433AE9B6FR9

4.2.2.2 Mã hóa khối PIN Block

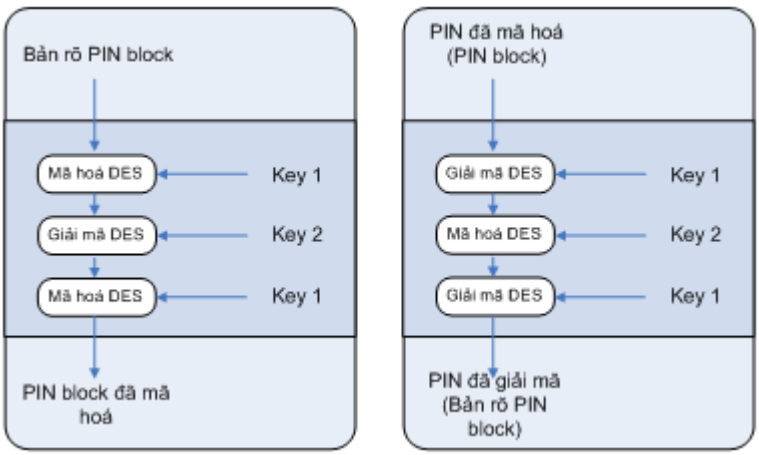
Khối PIN này được mã hóa bởi 3DES trước khi truyền đi, ví dụ với một khoá bộ hai (128 bit) sẽ được dùng để mã hóa như sau :

A12EAA75BDF2B57F 66A3EEAA67AAE8AA

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

A12EAA75BDF2B57F **66A3EEAA67AAE8AA**

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



Hình 4.13 Minh họa các bước mã hóa và giải mã PIN Block

4.2.3 Xác thực PIN tại HSM

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

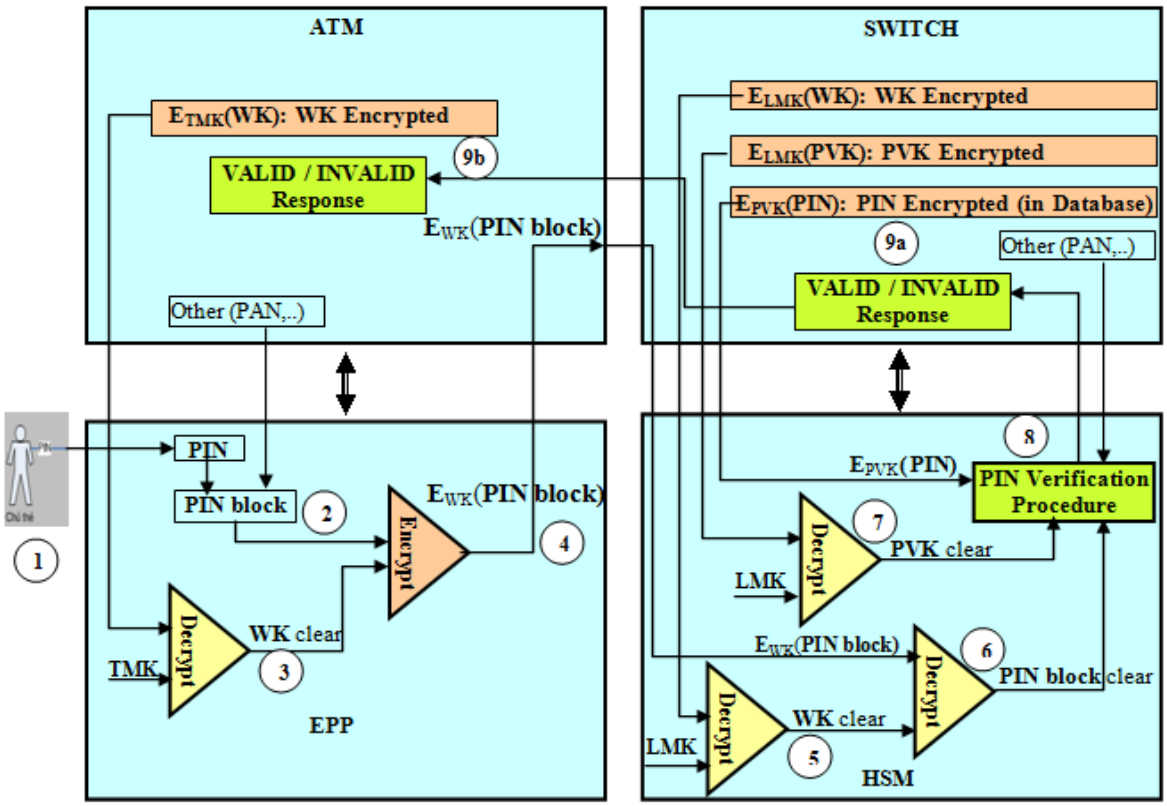
- Giải mã PIN được nhập vào từ máy ATM đã được mã hóa
- Giải mã PIN lưu trong CSDL của CoreBank đã được mã hóa

- So sánh số PIN được nhập vào và số PIN được lưu trong CSDL

- Quá trình xác thực đều được 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 4.14 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 gửi lại cho ATM

4.3 Giải pháp bảo mật và đảm bảo an toàn thông tin trong ATM

Đảm bảo 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 đảm bảo an toàn thông 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

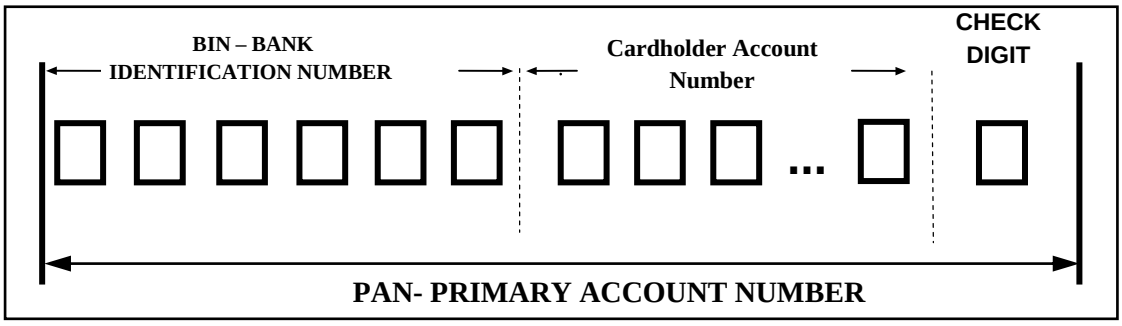
12. Bảo đảm an toàn từ phía người dùng.

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

4.3.1.1 Định nghĩa số CD – Check Digit

Trong quá trình phát hành thẻ, module quản lý thẻ CMS (Card Management System) 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 4.15 Cấu trúc của số PAN và vị trí số CD

Chữ số này 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 0-9.

4.3.1.2 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 thẻ thì hệ thống Swtich 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.

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

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: 118822987654321Y, ta cần sinh số Y sao cho số thẻ là hợp lệ

	BIN						Cardholder Account Number									CD
PAN	1	1	8	8	2	2	9	8	7	6	5	4	3	2	1	Y
Nhân 2 (cột	x2		x2		x2		x2		x2		x2		x2		x2	Y
Kết quả	2	1	16	8	4	2	18	8	14	6	10	4	6	2	2	Y
Trừ 9 nếu > 9			-9				-9		-9		-9					Y
Kết quả	2	1	7	8	4	2	9	8	5	6	1	4	6	2	2	Y
Cộng các chữ số lại	2+1+7+8+2+4+9+8+5+6+1+4+6+2+2+Y = 67 + Y ***Giải bài toán:*** lấy số hàng đơn vị của 66 cộng với Y có tổng bằng 10. 7+Y=10 => Y=3															
Kết quả	1	1	8	8	2	2	9	8	7	6	5	4	3	2	1	3

Bảng 4.16 Cách sinh số CD

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	1	1	8	8	2	2	9	8	7	6	5	4	3	2	1	3
Nhân 2 (cột	x2		x2		x2		x2		x2		x2		x2		x2	
Kết quả	2	1	16	8	4	2	18	8	14	6	10	4	6	2	2	3
Trừ 9 nếu >			-9				-9		-9		-9					3
Kết quả	2	1	7	8	4	2	9	8	5	6	1	4	6	2	2	3
Cộng các chữ số lại	2 + 1 + 7 + 8 + 2 + 4 + 9 + 8 + 5 + 6 +1 + 4 + 6 + 2 + 2 + 3 = 70 ***Giải bài toán:*** 70 mod 10 = 0															
Kết quả	Số thẻ hợp lệ															

Bảng 4.17 Cách kiểm tra số CD

4.3.2 Xác thực tính hợp lệ của thẻ - Card Authentiocation values

4.3.2.1 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/ 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 do 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 64 bit

Input: chuỗi 64 bit hay 16 bit ký tự hexa được gọi 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

TSP 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: 2244661234567890

Exp date: 1012

Service code: 101

TSP = 1234567891012101

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.

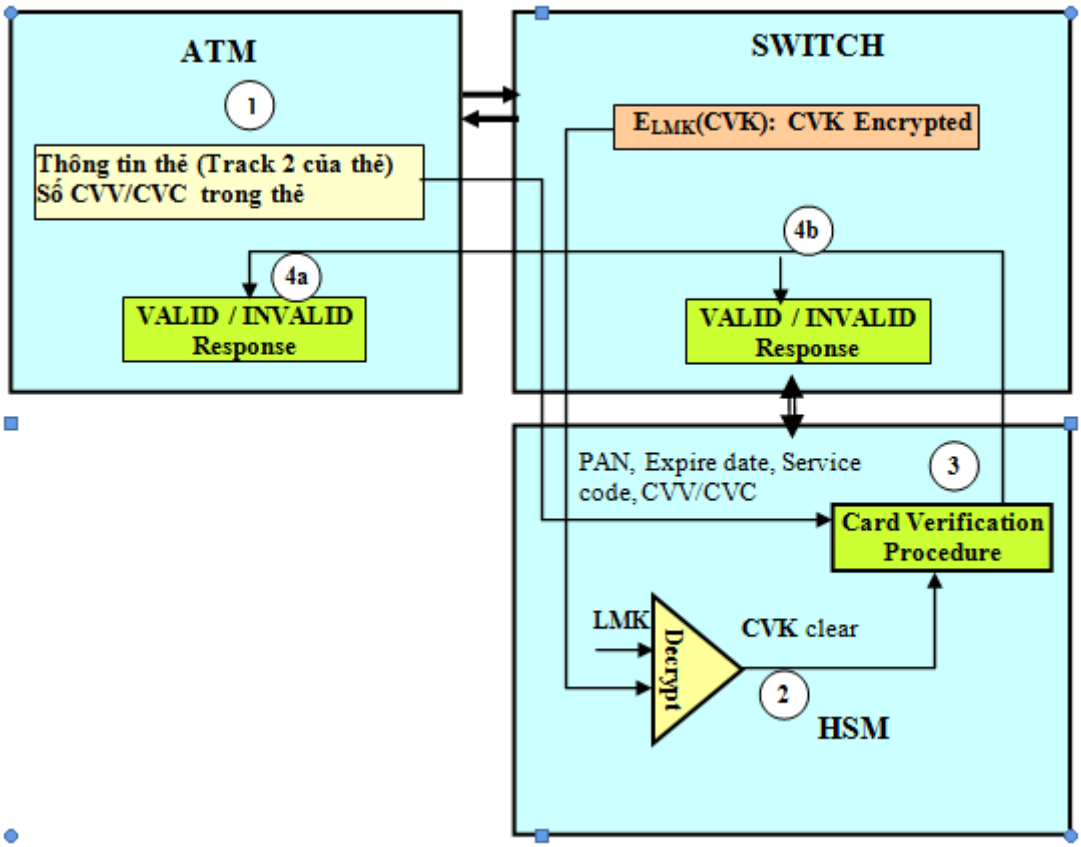
- Nếu không tìm được đủ 3 số thập phân trong đó thì số còn thiếu sẽ sử dụng là các số không phải số thập phân tính từ trái qua và chuyển sang số thập phân theo công thức A-> 0; B-> 1; C-> 2; D-> 3; E-> 4; F-> 5.

Ví dụ: output from DES: 0FAB9CDEFFEFDCBA

=>> CVV/CVC là 095

4.3.2.2 Xác thực số CVV/CVC

Quá trình xác thực này diễn ra cùng với quá trình xác thực PIN của chủ thẻ và được mô tả bên dưới



Hình 4.18 Quá trình xác thực số CVV/CVC giữa ATM và Switch

a. 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.

b. Bản mã của khóa CVK tại Switch được giải mã bởi khóa LMK trong HSM

c. Sử dụng khóa CVK trong thuật toán DES để sinh số CVV/CVC. Kiểm tra số CVV/CVC được sinh ra với số CVV/CVC được gửi đến

d. Kết quả kiểm tra được gửi trả lại cho ATM

4.3.3 Bảo đảm an toàn thông tin giao dịch

+ Bảo mật số PIN

+ Bảo đảm an toàn các khóa bí mật trong hệ thống ATM

Để đảm bảo an toàn thông tin khi giao dịch trên ATM số PIN sẽ được mã hóa trước khi thực hiện giao dịch

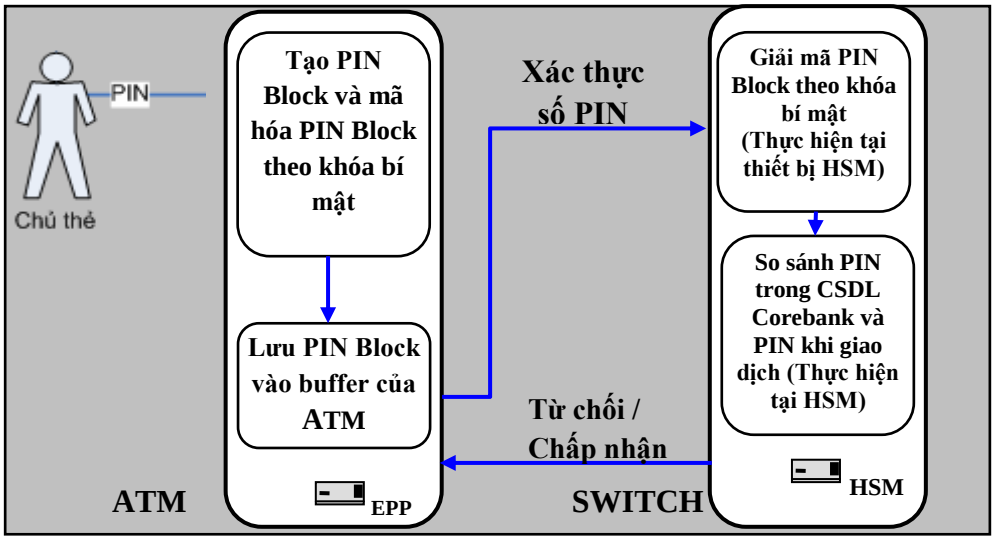
Số PIN của chủ thẻ được lưu trong CSDL Corebank

Không truy cập hoặc xác định được bản rõ của bất ký khóa 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 hủy

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

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



Hình 4.19 Quy trình mã hóa và xác thực PIN

Bước 1: Chủ thẻ đưa thẻ và nhập PIN tại máy ATM

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

4.3.4 Bảo đảm an toàn phần mềm ATM

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

Đảm bảo an toàn mật khẩu truy nhập vào phần mềm

4.3.5 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. Vì hệ điều hành trong máy ATM được sử dụng ở đây về nguyên lý là một hệ điều hành thông thường nên ta cần bảo đảm sự an toàn theo như khuyến cáo của nhà sản xuất.

- Tắt các service không dùng

- Đóng các cổng không dùng

- Thiết lập Firewall cho máy ATM

4.3.6 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 thông phun mực vào các tờ tiền khi các hộp đựng tiền bị xâm nhập trái phép.

ATM có hệ thống camera giám sát

4.3.7 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.

4.3.8 Bảo đảm an toàn từ phía người dùng

Một trong những cái khó ở đây chính là bản thân chủ thẻ cũng không biết mình bị mất cắp tài khoản, chỉ đến khi kiểm tra số dư mới thấy ngh ngờ. Còn bản thân ngân hàng thì cũng không thể nắm rõ đâu là giao dịch của chủ thẻ, đâu là của tội phạm. Vì thế, sự cảnh giác của các chủ thẻ là vô cùng quan trọng và chính khách hàng là người đảm bảo an toàn cho những thông tin giao dịch của mình.

Khi thông tin về thẻ bị lộ, ngay lập tức thông báo cho phía ngân hàng để ngân hàng khóa thẻ và kiểm tra giao dịch nghi vấn liên quan đến thẻ.

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

4.3.8.1 Lấy cắp thẻ và số PIN

Bước đầu tiên, bọn tội phạm sẽ lắp vào khe đọc thẻ của một máy một miến nhựa có khả năng giữ thẻ và ngăn máy thả ra. Khi đó chủ thẻ sẽ nghĩ mình thao tác nhầm và bị máy nuốt thẻ, chứ không chú ý xem khe đọc thẻ có gì bất thường không.

Khi đó kẻ gian lại gần chúng sẽ "tư vấn" chủ thẻ nên nhập lại số PIN để lấy lại thẻ và theo dõi. Tất nhiên việc nhập lại số PIN chả giúp gì cho chủ thẻ cả nhưng lại là cơ hội để kẻ gian biết được mật mã truy cập vào tài khoản thẻ của nạn nhân.

Khi chủ thẻ thất vọng bỏ đi, kẻ gian sẽ ở lại lấy thẻ ra, rồi dùng PIN vừa nhìn trộm được để truy cập vào tài khoản và rút tiền.

4.3.8.3 Trộm dữ liệu

Đây là cách ăn cắp thông tin tài khoản và PIN mà không cần tiếp cận trực tiếp với chủ thẻ. Thông thường, bọn tội phạm cài thêm một thiết bị đọc dữ liệu vào khe đọc của ATM

Khi chủ thẻ thực hiện giao dịch, toàn bộ thông tin trên thẻ đã được lưu giữ lại trong thiết bị đọc thẻ mà bọn tội phạm cài vào.

Khi nạn nhân ra đi, bọn tội phạm sẽ lấy thiết bị ra, sử dụng các thông tin vừa chôm được để làm thẻ giả hoặc mua hàng qua mạng, qua điện thoại.

4.3.8.4 Trộm dữ liệu bằng camera

Bọn tội phạm vẫn lắp đặt thiết bị đọc thẻ vào máy như trước, nhưng chúng có thể lấy dữ liệu về tài khoản và số PIN từ xa nhờ một chiếc camera mà chúng lắp kín tại máy ATM. Camera thường đặt kín đáo, một vị trí có thể ghi hình toàn bộ các thao tác của chủ thẻ cũng như lưu giữ dữ liệu.

4.3.8.5 Nhìn trộm qua vai

Bọn tội phạm có thể đứng gần ATM, theo dõi quá trình bạn thao tác trên máy. Để tránh loại tội phạm này, phần lớn người tiêu dùng đều cảnh giác che bàn phím khi nhập mã số. Việc ăn cắp dữ liệu rất thô sơ, song rất dễ thực hiện vì không phải chủ thẻ nào cũng thận trọng mỗi khi giao dịch trên

máy. Bọn tội phạm sẽ đứng nấp gần ATM và theo dõi chủ thẻ khi họ nhập PIN. Sau đó, chúng sẽ tìm cách làm chủ thẻ mất tập trung, chẳng hạn hét lên hoặc đánh rơi tiền và hỏi đó là tiền của ai. Trong lúc chủ thẻ sao nhãng, kẻ gian liền cuỗm thẻ của chủ thẻ.

4.4 Nhận xét

Qua nghiên cứu các hoạt động và bảo mật thông tin của hệ thống thanh toán tự động ATM đã được trình bày ở các chương trên, thì việc bảo mật CSDL, bảo mật thông tin trên đường truyền và bảo mật mã PIN là quan trọng nhất, ngoài ra bảo mật hệ thống cũng đóng vai trò quan trọng.

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

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 bảo an toàn khi giao dịch

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, sao chép) do đó xu thế trong tương lai thẻ chip sẽ thay thế thẻ từ.

Chương 5. CHƯƠNG TRÌNH THỰC HIỆN MÃ HÓA VÀ GIẢI MÃ VỚI HỆ MÃ DES

5.1. Giới thiệu về chương trình

Chương trình thực hiện mã hóa và giải mã với hệ mã DES được viết bằng ngôn ngữ lập trình VB.net

Cấu hình:

Phần cứng (tối thiểu):

Ổ cứng: 10gb

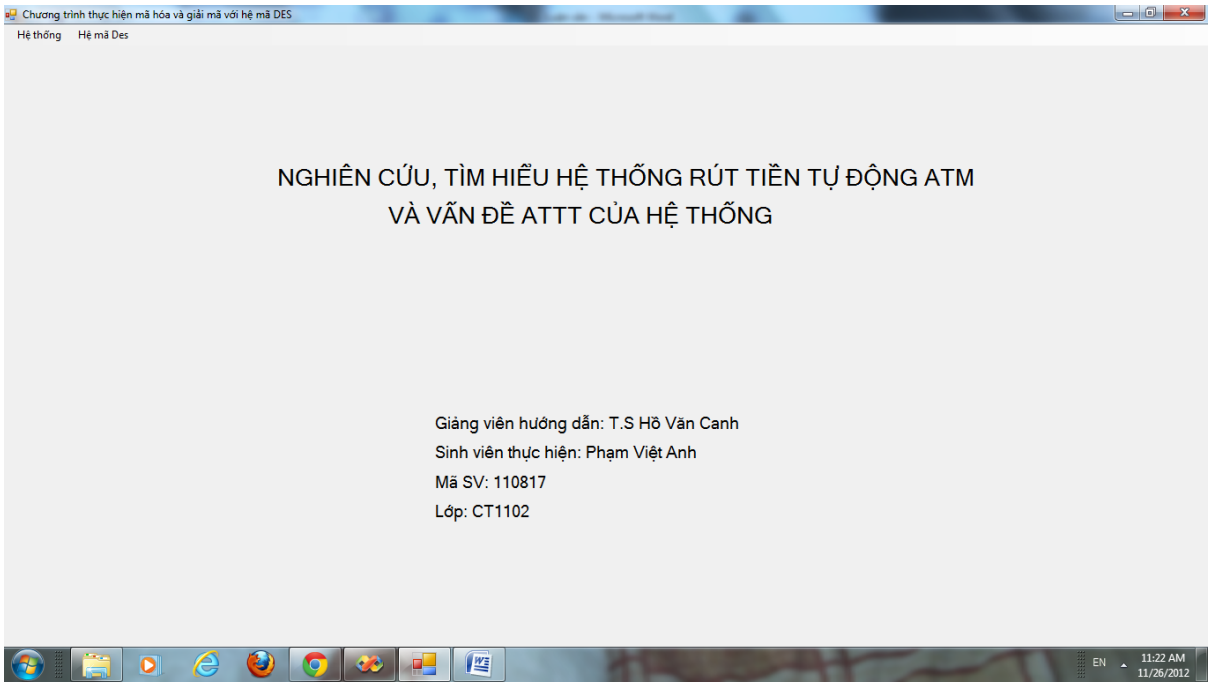
Ram: 256mb

CPU: 2.0GHz

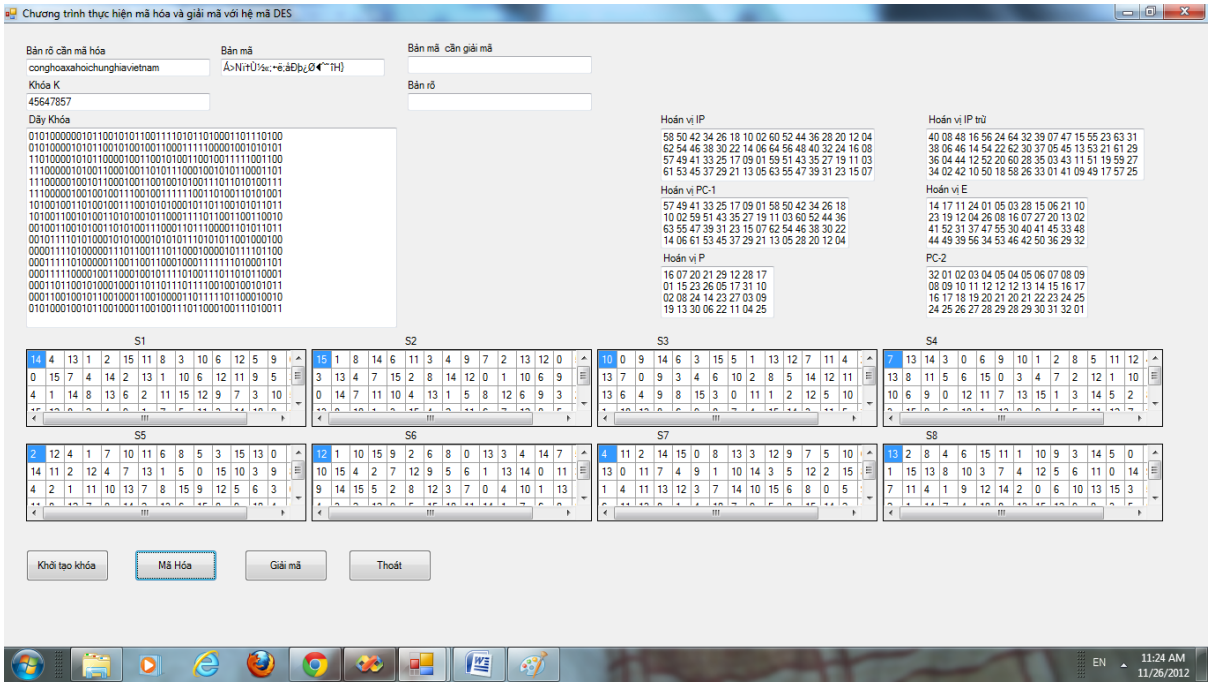
Hệ điều hành: Window XP, Window 7……

5.2 Các chức năng chính

5.2.1 Giao diện chính của chương trình



5.2.2 Quá trình lập mã



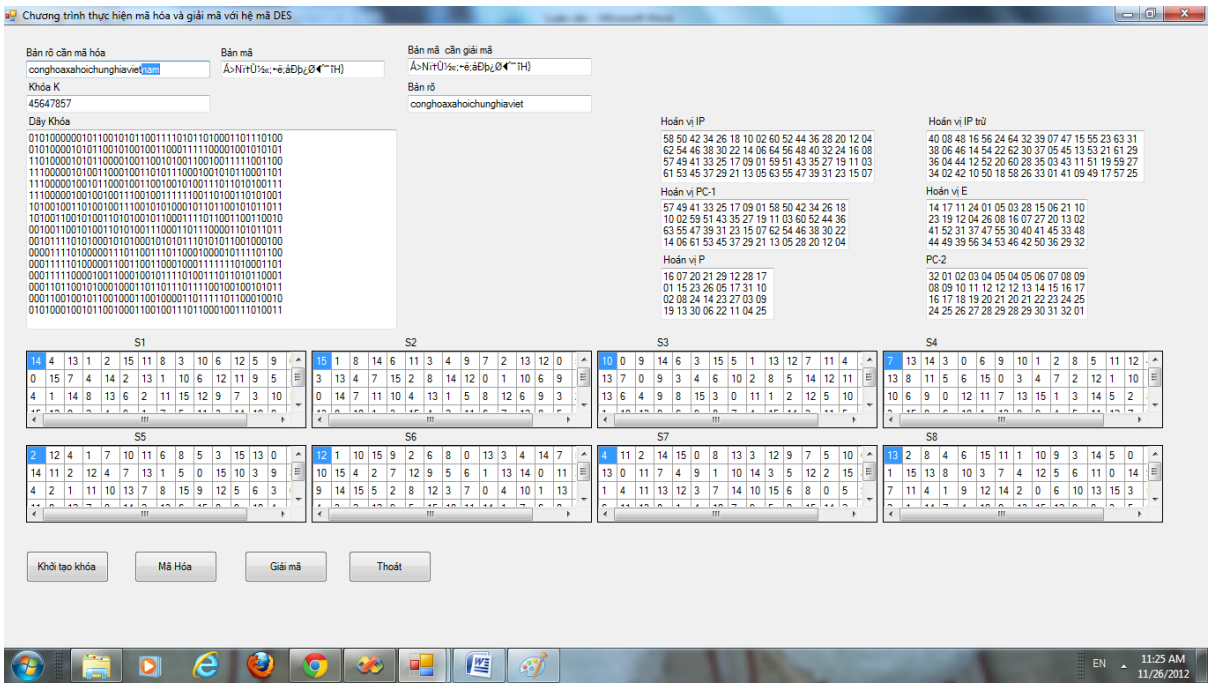
Bước 1: Nhập chuỗi cần mã hóa

Bước 2: Nhập khóa K gồm 8 ký tự

Bước 3: Click nút khởi tạo khóa để tạo dãy khóa

Bước 4: Click nút mã hóa để bắt đầu lập mã

5.2.3 Quá trình giải mã



Bước 1: Nhập chuỗi cần giải mã

Bước 2: Nhập khóa K gồm 8 ký tự

Bước 3: Click nút khởi tạo khóa để tạo dãy khóa

Bước 4: Click nút giải mã để bắt đầu giải mã

KẾT LUẬN

Trong đồ án em đã tìm hiểu tổng quan về máy ATM, cấu trúc của máy ATM, hệ thống thanh toán máy ATM. Trong đó, em tập trung tìm hiểu về thẻ từ, vấn đề an toàn thông tin cho hệ thống ATM: mã hóa, giải mã số PIN, thuật toán dùng để mã hóa thông tin, mã hóa, giải mã thông tin truyền và lưu trong hệ thống ATM…..

Mặc dù ở nước ta, chủ yếu các Ngân hàng đang sử dụng thẻ từ, nhưng tương lai không xa thẻ từ sẽ bị thay thế bởi thẻ chip. Do đó đáng ra ngay từ bây giờ chúng ta phải nghiên cứu sâu hơn về thẻ chip nhưng do tài liệu về thẻ chip bằng tiếng Việt quá ít nếu có chủ yếu là tài liệu tiếng Anh, nên trong báo cáo luận văn của em, em chưa tìm hiểu được nhiều về thẻ chip. Có lẽ đây cũng là một nhược điểm trong đề tài luận văn của em.

Ngoài ra, do trình độ hạn chế và thời gian có hạn, tài liệu không có nhiều nên trong đồ án của em còn nhiều thiếu sót, em mong sự chỉ bảo của các thầy, cô để đồ án của em được hoàn thiện hơn.

Em xin chân thành cảm ơn các thầy, cô đặc biệt là thầy Hồ Văn Canh và các bạn cùng lớp đã tạo điều kiện giúp em hoàn thành đồ án.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Báo tin học và Tài chính – Bộ tài chính, Sự hình thành và phát triển của máy ATM số 58 (4/2008)

2. Banknetvn (2006), tài liệu tiêu chuẩn kỹ thuật về hệ thống Switch

3. Bách khoa toàn thư mở Wikipedia, Hệ mã hóa DES

4. DIEBOLD (2007), Tài liệu giới thiệu hệ thống ATM

5. 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.

6. Hồ Văn Canh (2003), Tài liệu giảng dạy về an toàn bảo mật thông tin.

7. Trịnh Nhật Tiến (2007), Tài liệu giảng dạy về mật mã và an toàn thông tin

8. Hồ Văn Canh, Nguyễn Viết Thế (2010), Nhập môn phân tích thông tin có bảo mật, NXB thông tin và truyền thông

Tiếng Anh

9. ISO 8583-1987 MessFormat.

10. ISO_IEC_7810_2003(E)-Identification cards-Physical characteristics.

11. ISO_IEC_7811-1_2002(E)-Identification cards-Recording technique-Part 1-Embossing.

12. ISO_IEC_7812-1_2000(E)-Identification cards-Identification of issuers-Part 1-Numbering system.

13. ISO_IEC_7813_2001(E)-Identification cards-Financial transaction cards.