BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

ĐỒ ÁN TỐT NGHIỆP

NGÀNH CÔNG NGHỆ THÔNG TIN

HẢI PHÒNG 2013

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

ỨNG DỤNG POS TRONG HỆ THỐNG BÁN LẺ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
Ngành: Công Nghệ Thông Tin

HẢI PHÒNG - 2013

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

ỨNG DỤNG POS TRONG HỆ THỐNG BÁN LẺ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công Nghệ Thông tin

Sinh viên thực hiện : Nguyễn Đăng Thiện
Giáo viên hướng dẫn : Ths. Nguyễn Trịnh Đông
Mã sinh viên : 090055

HẢI PHÒNG 2013

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

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do –Hạnh Phúc
-------o0o-------

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

Sinh viên : Nguyễn Đăng Thiện Mã số: 090055

Lớp : CT1001 Ngành: Công Nghệ Thông Tin

Tên đề tài: **Ứng dụng POS trong hệ thống bán lẻ**

NHIỆM VỤ ĐỀ TÀI

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

a. Nội dung:

b. Các yêu cầu cần giải quyết

2. Các số liệu cần thiết để thiết kế tính toán

3. Địa điểm thực tập

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Người hướng dẫn thứ nhất:

Họ và tên : Nguyễn Trịnh Đông

Học hàm, học vị :Thạc Sỹ Công Nghệ Thông Tin

Cơ quan công tác :Khoa Công Nghệ Thông Tin – Trường Đại Học Dân Lập Hải Phòng

Nội dung hướng dẫn:

- Tìm hiểu về thiết bị ứng dụng trong thanh toán điện tử.
- Tìm hiểu hệ thống POS
- Tìm hiểu giải pháp ứng dụng hệ thống POS.

Người hướng dẫn thứ hai:

Họ và tên:.....

Học hàm, học vị:.....

Cơ quan công tác: .....

Nội dung hướng dẫn: .....

.....

.....

.....

.....

.....

.....

.....

.....

Đề tài tốt nghiệp được giao ngày tháng năm 2013

Yêu cầu phải hoàn thành trước ngày 5 tháng 05 năm 2013

Đã nhận nhiệm vụ: Đ.T.T.N	Đã nhận nhiệm vụ: Đ.T.T.N
Sinh viên	Cán bộ hướng dẫn Đ.T.T.N

Hải Phòng, ngày.....tháng.....năm 2013

HIỆU TRƯỞNG

GS.TS.NGƯT Trần Hữu Nghị

PHẦN NHẬN XÉT TÓM TẮT CỦA CÁN BỘ HƯỚNG DẪN

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp:

.....

.....

.....

.....

.....

.....

2. Đánh giá chất lượng của đề tài tốt nghiệp (so với nội dung yêu cầu đã đề ra trong nhiệm vụ đề tài tốt nghiệp)

.....
.....
.....
.....
.....
.....
.....

Cho điểm của cán bộ hướng dẫn:

(*Điểm ghi bằng số và* chữ)

.....

.....

Hải phòng, ngày.....tháng.....năm 2013

Cán bộ hướng dẫn chính

(Ký, ghi rõ họ tên)

Nguyễn Trịnh Đông

PHẦN NHẬN XÉT ĐÁNH GIÁ CỦA CÁN BỘ CHẤM PHẢN BIỆN ĐỀ TÀI TỐT NGHIỆP

1. **Đánh giá chất lượng đề tài tốt nghiệp(về các mặt như cơ sở lý luận, thuyết minh chườn trình, giá trị thực tế,…)**

2. Cho điểm của cán bộ phản biện

(*Điểm ghi bằng số và chữ*)

.....

.....

Hải Phòng, ngày.....tháng.....năm 2013

Cán bộ chấm phản biện

(Ký, ghi rõ họ tên)

LỜI NÓI ĐẦU

Trong lời đầu tiên của báo cáo đồ án tốt nghiệp "Ứng dụng POS trong hệ thống bán lẻ" này, em muốn gửi những lời cám ơn và biết ơn chân thành nhất của mình tới tất cả những người đã hỗ trợ, giúp đỡ em về kiến thức và tinh thần trong quá trình thực hiện đồ án.

Trước hết, em xin chân thành cảm ơn Thầy Giáo - Ths. Nguyễn Trịnh Đông, Giảng viên Khoa Công Nghệ Thông Tin, Trường ĐHDL Hải Phòng, người đã trực tiếp hướng dẫn, nhận xét, giúp đỡ em trong suốt quá trình thực hiện đồ án.

Xin chân thành cảm ơn các thầy cô trong Khoa Công Nghệ Thông Tin và các phòng ban nhà trường đã tạo điều kiện tốt nhất cho em cũng như các bạn khác trong suốt thời gian học tập và làm tốt nghiệp.

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 khoá luận tốt nghiệp.

Do thời gian thực hiện 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 giáo 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 28 tháng 04 năm 2013

Sinh viên

Nguyễn Đăng Thiện

MỤC LỤC

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY 3
LỜI NÓI ĐẦU 10
MỤC LỤC 11
Chương 1: GIỚI THIỆU POS 13
1.1 Giới thiệu 13
1.2 Tích hợp trong hệ thống mạng của ngân hàng 13
1.3 Giới thiệu kỹ mã hóa trong hệ thống POS 16
1.3.1 Quá trình mã hóa PIN và truyền gửi PIN 16
1.3.2 Thuật toán mã hóa 3DES 17
1.3.3 Nguyên tắc quản lý khóa 20
1.3.4 Vấn đề mã hóa dữ liệu truyền trong hệ thống POS 20
1.3.5 Một số ứng dụng của POS 21
1.4 Nguy cơ mất an toàn trong hệ thống POS 21
1.4.1 Nguy cơ mất an toàn từ phía thiết bị trong hệ thống POS 21
1.4.2 Nguy cơ mất an toàn từ phía thẻ tín dụng 22
1.4.3 Nguy cơ mất an toàn từ phía người dùng 22
1.5 Giải pháp an toàn bảo mật đặt ra 22
1.5.1 Giải pháp an toàn bảo mật đặt ra với các ngân hàng 22
1.5.2. Giải pháp an toàn bảo mật đặt ra với khách hàng 23
Chương 2: CẤU TẠO THẺ VÀ CHUẨN TRUYỀN DỮ LIỆU 26
2.1 Phân loại thẻ 26
2.1.1 Thẻ nổi 26
2.1.2 Thẻ từ 26
2.1.3 Thẻ thông minh 26
2.1.4 Thẻ nhớ quang học 27
2.2 Cấu tạo thẻ 27
2.3 Cấu trúc dữ liệu 27
2.4 Truyền dữ liệu 30

2.4.1 Trả lời để thiết lập lại (Answer to reset – ATR) 31
2.4.2 Giao thức truyền dữ liệu 33
2.4.3 Giao thức truyền dữ liệu với T = 14 50
2.4.4 Giao thức truyền tải USB 51
2.5 Cấu trúc thông điệp: APDUs 52
2.6 An toàn truyền dữ liệu 52
Chương 3: MÔ TẢ HỆ THỐNG POS THỬ NGHIỆM TẠI CÁC ĐIỂM BÁN LẺ 56
3.1 Giới thiệu hệ thống 56
3.2 Các thành phần hệ thống 56
3.2.1 Thiết bị POS 56
3.2.2 Hệ thống chuyển mạch (SWITCH) 57
3.2.3 Hệ thống quản lý thẻ (CMS) 57
3.2.4 Hệ thống lõi (CORE) 58
3.3 MINH HỌA QUY TRÌNH SỬ DỤNG POS 58
3.3.1 GIAO DỊCH THANH TOÁN (SALE ONLINE) 58
3.3.2 GIAO DỊCH XÁC MINH (CARD VERIFY) 59
3.3.3 GIAO DỊCH NGOẠI TUYẾN (OFFLINE). 60
3.3.4 GIAO DỊCH HỦY (VOID). 62
3.3.5 GIAO DỊCH TỔNG KẾT (SETTLE). 63
KẾT LUẬN 65
TÀI LIỆU THAM KHẢO 66

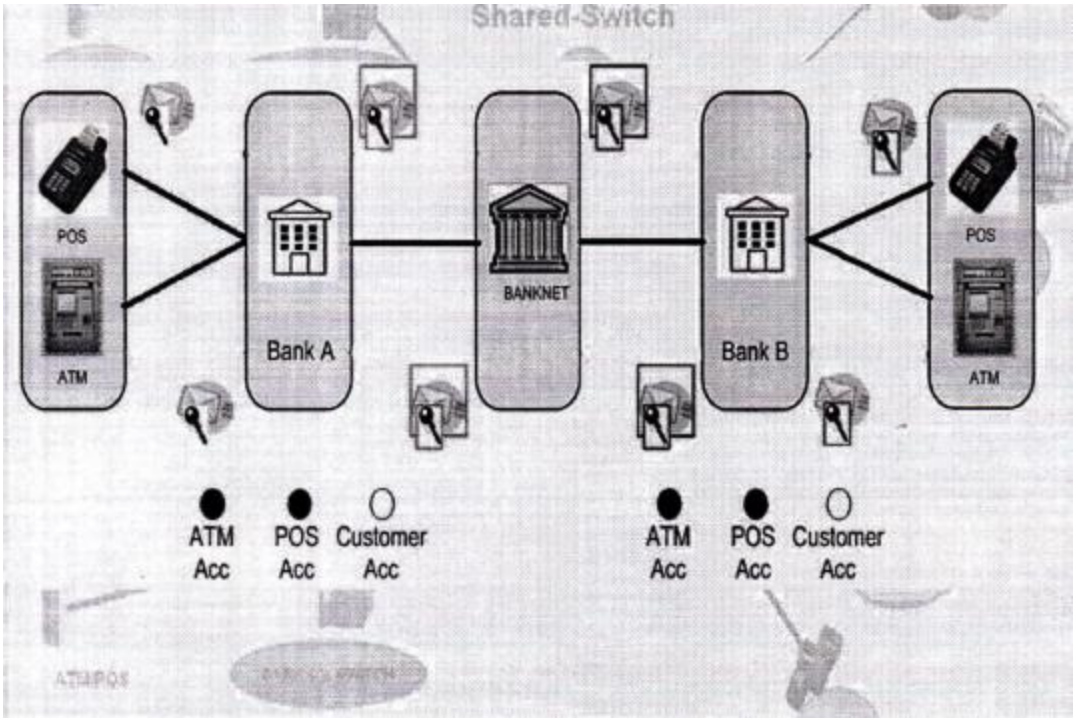
Chương 1: GIỚI THIỆU POS

1.1 Giới thiệu

POS (Point Of Sale) là hệ thống thanh toán điện tử trực tuyến bằng cách sử dụng thẻ điện tử thay bằng việc thanh toán bằng tiền mặt thông thường.

POS giúp khách hàng thanh toán tiền một cách nhanh chóng bằng cách quẹt thẻ, Tiền trả thanh toán của khách hàng bao gồm tiền mua hàng và phí dịch vụ sử dụng hệ thống POS, Tiền mua hàng sẽ được chuyển tới tài khoản của bên bán hàng. Phí dịch vụ sẽ được tính toán theo tỉ lệ thỏa thuận.

1.2 Tích hợp trong hệ thống mạng của ngân hàng



Hình 1.2.1: Mô hình ATM/POS trong hệ thống ngân hàng

Hệ thống POS được ứng dụng thông qua kết nối với mạng lưới mạng lưới ngân hàng, cho đến nay các hệ thống POS là của ngân hàng đặt tại các đại lý, cửa hàng, nhà hàng, khách sạn nếu có nhu cầu. Phí giao dịch sẽ được tính bằng các cộng thêm vào số tiền thanh toán của khách hàng trong các giao dịch.

ATM là hệ thống rút tiền tự động bằng thẻ điện tử, các chức năng chủ yếu trong hệ thống ATM là rút tiền (withdrawal), vấn tin tài khoản (balance inquiry), chuyển tiền(fund tranfer)…

Hình 1.2.1 là mô hình tổng quát về sự tương tác giữa hệ thống POS và ngân hàng, khi khách hàng thực hiện giao dịch tại máy POS (mua hàng, vấn tin số dư tài khoản, hủy bỏ giao dịch). Khách hàng quẹt thẻ tại máy POS, sau đó khách hàng được

yêu cầu nhập mã số PIN. POS sẽ gửi giao dịch về ngân hàng mà máy POS đã kết nối, nếu thẻ thanh toán của khách hàng là của ngân hàng có máy POS thì giao dịch sẽ được thực hiên tại ngân hàng đó, nếu không ngân hàng có máy POS này sẽ chuyển đến ngân hàng khác có trách nhiệm với thẻ thanh toán của khách hàng, lúc đó phí giao dịch của khách hàng sẽ phải trả cho ngân hàng trung gian có đặt máy POS này. trong thực tế các ngân hàng thường liên kết với nhau tạo thành một liên minh ngân hàng, sẽ phân loại thẻ quẹt của khách được xử lý bởi một thiết bị trung chuyển SWITCH. Nhiệm vụ chủ yếu của SWITCH là phân loại thẻ quẹt của khách hàng và gửi đến ngân hàng chấp nhận thẻ đó.

Đặc tả hệ thống

Bước 1:

Khi thực hiện giao dịch, khách hàng quẹt thẻ vào máy POS, đồng thời nhập mã số PIN. Hệ thống POS mã hóa mã số PIN của khách hàng và các thông tin trên thẻ bằng hệ mã đố xứng 3DES. Mã số PIN của khách hàng và số PAN (số định danh tài khoản) được áp dụng phép toán "XOR" với nhau, sau đó được mã hóa bởi thuật toán mã hóa 3DES với khóa master-key 1 đã được thỏa thuận với hệ thống xử lý trung tâm HSM để tạo khối 64 bit đầu ra.

Khối PIN được mã hóa và các thông tin của khách hàng trên thẻ (card number – số thẻ, expiry date- hạn sủ dụng thẻ, cardholder- chủ sở hữu thẻ) sẽ được áp dụng phép toán "XOR" với nhau và được mã hoá bởi thuật toán mã hóa 3DES với khóa master-key2 đã thỏa thuận với hệ thống SWITCH của ngân hàng.

Số tài khoản (PAN) và số thẻ (card number) là khác nhau. Số tài khoản là do hệ thống CORE của ngân hàng sinh ra để quản lý tài khoản, có nhiều loại tài khoản như tài khoản tiết kiệm (saving account), tài khoản thanh toán (current account). Số thẻ do hệ thống CMS (Card Management System) sinh ra để quản lý thẻ. Mỗi thẻ có một số thẻ, số thẻ có thể có nhiều tài khoản.

Bước 2:

Hệ thốn POS gửi thông tin đã mã hóa quá trình điều khiển NCC (trình điều khiển NCC này giống như một ROUTER, có nhiệm vụ chủ yếu là chuyển đổi tính hiệu analog/digital). Máy POS kết nối đến 01 NCC đã định trước, phương thức kết nối là POS dial-up đến NCC (hoặc kết nối không dây wireless bằng công nghệ GPRS trường hợp này sẽ thông qua 01 Gateway của 01 Telco như viettel hay Vinaphone…, để kết nói tới SWITCH hoặc POS có thể kết nối thông qua 01 mang LAN và 01 gateway để kết nối tới SWITCH).

Bước 3:

Trong trường hợp kết nối Dial-up NCC sẽ xác định 01 SWITCH đã định trước của ngân hàng (Không phải là SWITCH gần nhất, mỗi một ngân hàng thường chỉ có

01 SWITCH), hệ thống SWITCH sẽ phân loại và xử lý (dùng khóa master-key2 đã được thỏa thuận với POS để giải mã xác định thẻ thuộc ngân hàng nào, tuy nhiên mã số PIN vẫn được mã hóa). Sau khi xác định được thẻ thuộc ngân hàng nào, thông tin và mã số PIN của khách lại được mã hóa bằng hệ thống 3DES (việc mã hóa và giả mã bằng một master-key3 đã được thỏa thuận với hệ thống HSM) và gửi các thông tin về hệ thống CMS (hệ thống quản lý thẻ của ngân hàng) (hệ thống nà sẽ thuộc về một ngân hàng cụ thể). POS-NCC- SWITCH trong thực tế thường của cùng một ngân hàng hoặc là của một liên minh ngân hàng.

Trong trường hợp kết nối bằng wireless, POS sẽ kết nối tới SWITCH thông qua một gateway, việc mã hóa dữ liệu tương ứng như trong trường hợp kết nối bằng dial-up.

Trong trường hợp kết nối thông qua một mang LAN để kết nối tới SWITCH, việc mã hóa dữ liệu cũng tương tự trong trường hợp kết nối bằng dial-up.

Bước 4:

Hệ thống quản lý thẻ gửi thông tin sang hệ thống HSM (hệ thống check mã số PIN và hạn sử dụng thẻ của khách). Tại đây hệ thống sẽ giải mã dữ liệu nhận được bằng master-key3 đã thỏa thuận với hệ thống SWITCH để kiểm tra mã số PIN và các thông tin tài khoản khách hàng bằng cách: Kiểm tra xem mã số PIN của khách hàng đã tồng tại trong cơ sở dữ liệu của ngân hàng hay chưa (đúng hoặc sai). Nêú đúng, hệ thống HSM sẽ gửi lại hệ thống quản lý thẻ. Nếu sai, hệ thống thiết bị an ninh sẽ gửi lại thông báo cho máy POS: mã số PIN không hợp lệ. Kiểm tra các thông tin tài khoản của khách như số tài khoản, hạn sử dụng thẻ….. nếu hết hạn sử dụng thẻ, sẽ gửi thông báo về hệ thống POS: thẻ hết hạn sử dụng.

Bước 5:

Hệ thống CMS gửi thông tin vào hệ thống CORE của ngân hàng (hệ thống phần mềm lõi của mỗi ngân hàng). Tại đây, việc xử lý giao dịch sẽ được thực hiện (thực hiện các tính toán về số dư tài khoản, chuyển khoản giữa người mua hàng và bán hàng). Các giao dịch qua POS là các giao dịch tính phí, tức là ngoài số tiền trả trong hóa đơn, khách hàng còn phải trả phí giao dịch, phí này sẽ được chia cho các ngân hàng tham gia vào quá trình giao dịch, gồm: ngân hàng phát triển thẻ, ngân hàng đã đầu tư POS,NCC, SWITCH, các ngân hàng trung gian (vì thế SWITCH của ngân hàng này không kết nối trực tiếp được đến với SWITCH của ngân hàng kia mà phải thông qua SWITCH của ngân hàng trung gian). Hệ thống sẽ trừ đi tài khoản của khách hàng nếu số dư tài khoản lớn hơn hoặc bằng số tiền thanh toán cộng với phí giao dịch. Ngược lại, sẽ hiển thị thông báo cho máy POS: Số dư tài khoản của bạn không đủ để thực hiện giao dịch. Giao dịch kết thúc. Trong suốt qúa trình truyền tin, mã số PIN luôn được mã hóa, Thông thường các ngân hàng đầu tư SWITCH, NCC và POS. Tuy nhiên để giảm chi phí nên một ngân hàng thường chỉ đầu tư POS, còn NCC và

SWITCH thì dùng chung với ngân hàng khác trong liên minh. Phí thu được từ khách hàng sẽ chia theo tỷ lệ thỏa thuận giữa các ngân hàng tham gia vào giao dịch.

Về mặt kĩ thuật:

Trong trường hợp kết nối bằng *dial-up* thì 01 POS thì chỉ biết đến 01 NCC quản lý nó, có giao dịch là nó kết nối về NCC đó để truyền thông tin về. NCC cũng chỉ biết đến 01 SWITCH mà nó phải truyền tin đến. Còn nhiệm vụ chủ yếu của SWITCH là phân loại thẻ đó có thuộc ngân hàng cùa mình hay không, nếu không thì sẽ phải chuyển các thông tin sang SWITCH của ngân hàng khác để xử lý. Nếu nó thấy thẻ đó không thuộc ngân hàng mình mà cũng không có SWITCH nào phù hợp để chuyển đến thì nó sẽ báo lỗi.

Trong trường hợp kết nối bằng *wireless* thông qua công nghệ *GPRS* hoặc kết nối qua mạng LAN, thì POS sẽ kết nối tới SWITCH của ngân hàng thông qua *gateway* trong moi trường internet.

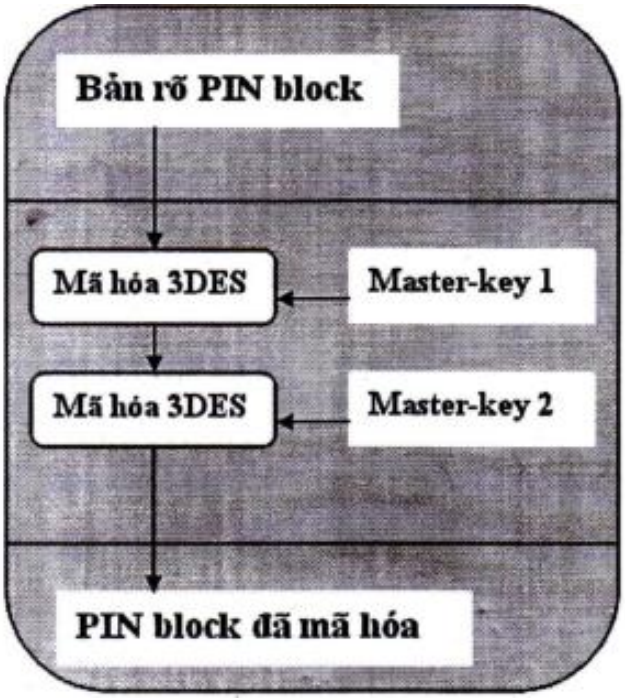
1.3 Giới thiệu kỹ mã hóa trong hệ thống POS

1.3.1 Quá trình mã hóa PIN và truyền gửi PIN

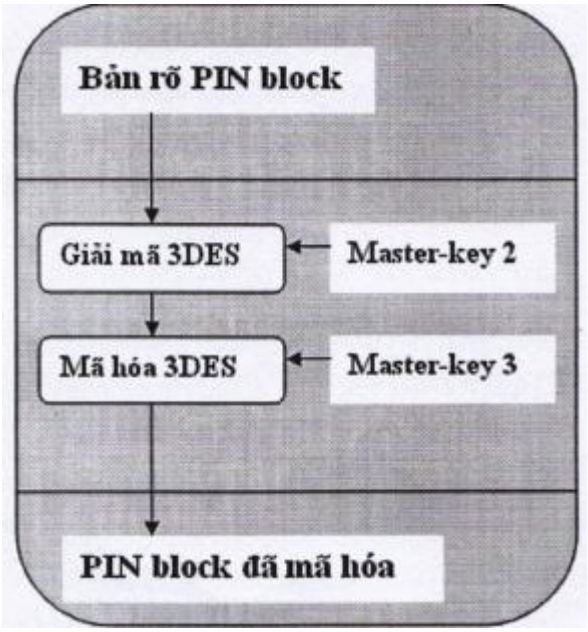
Việc sinh số PIN và mã hóa PIN tùy thuộc vào từng ngân hàng, số PIN không quá 6 ký tự (4-6).

Việc truyền gửi số PIN trong hệ thống POS thực hiện theo từng khối (block).

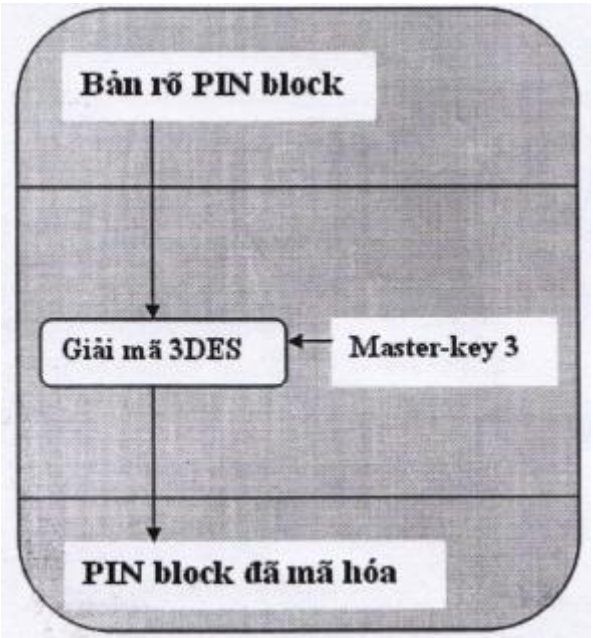
Để đảm bảo an toàn cho khối PIN trong quá trình truyền gửi trên mạng, các ngân hàng phải mã hóa khối PIN trước khi khối PIN được chuyển từ các thiết bị chấp nhận thẻ (thiết bị đọc thẻ tại POS) tới SWITCH của ngân hàng chấp nhận thẻ. Khối PIN của ngân hàng chấp nhận thẻ được bảo mật bằng khóa bí mật đã được thỏa thuận trước.



Hình 1.3.1.1: Mã hóa khối PIN tại POS



Hình 1.3.1.2: Giải mã và mã hóa khối PIN tại SWITCH



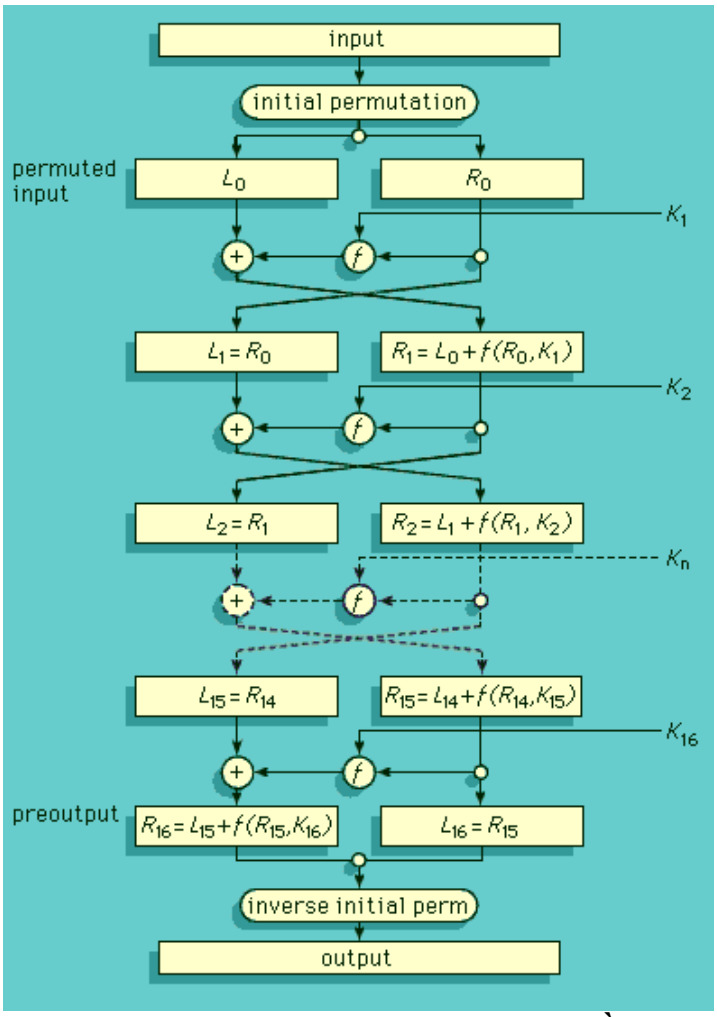
Hình 1.3.1.3: Giải mã khối PIN tại HSM

1.3.2 Thuật toán mã hóa 3DES

DES là một thuật toán khối với kích thước khối 64 bit và kích thước chìa 56 bit. Tiền thân của nó là Lucifer, một thuật toán do IBM phát triển. Cuối năm 1976, DES

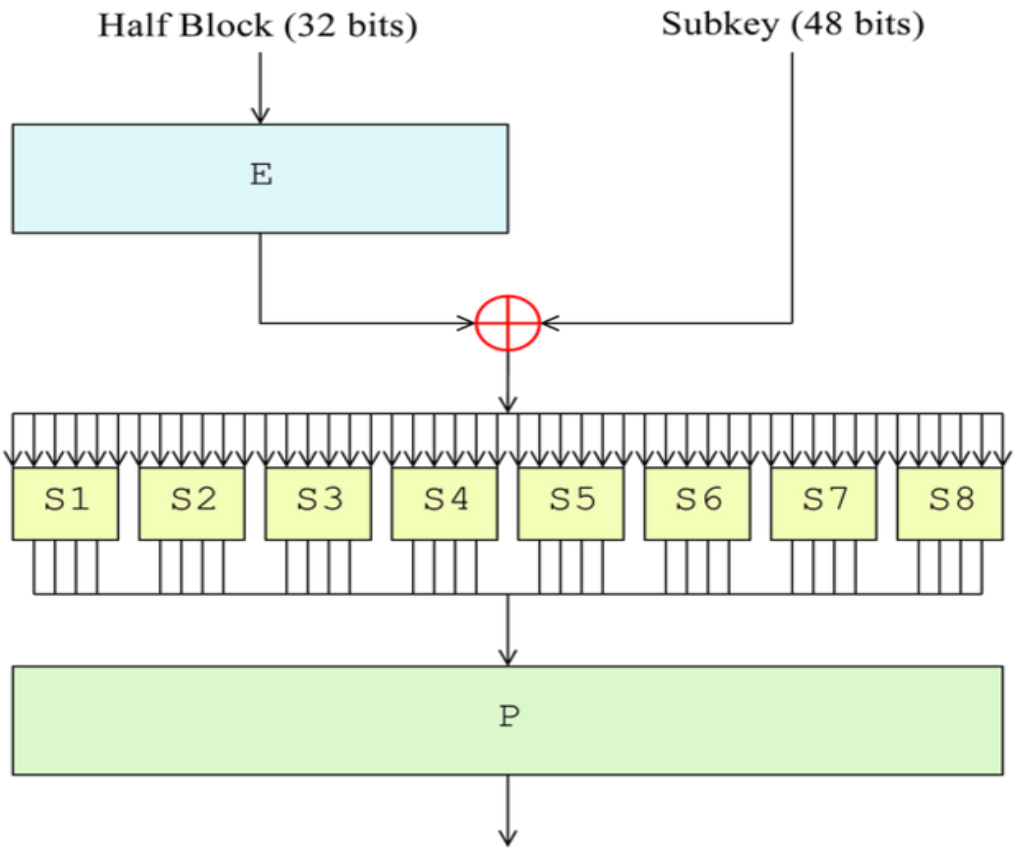
được chọn làm chuẩn mã hóa dữ liệu của nước Mỹ, sau đó được sử dụng rộng rãi trên toàn thế giới. DES cùng với mã hóa bất đối xứng đã mở ra một thời kì mới cho ngành mã hóa thông tin. Trước DES, việc nghiên cứu và sử dụng mã hóa dữ liệu chỉ giới hạn trong chính phủ và quân đội. Từ khi có DES, các sản phẩm sử dụng nó tràn ngập thị trường. Đồng thời, việc nghiên cứu mã hóa thông tin cũng không còn là bí mật nữa mà đã trở thành một ngành khoa học máy tính bình thường.

Trong khoảng 20 năm sau đó, DES đã trải qua nhiều khảo sát, phân tích kỹ lưỡng và được công nhận là an toàn đối với các dạng tấn công (tất nhiên, ngoại trừ brute-force). Dưới đây là hình minh họa 16 bước thực hiện mã hóa DES.



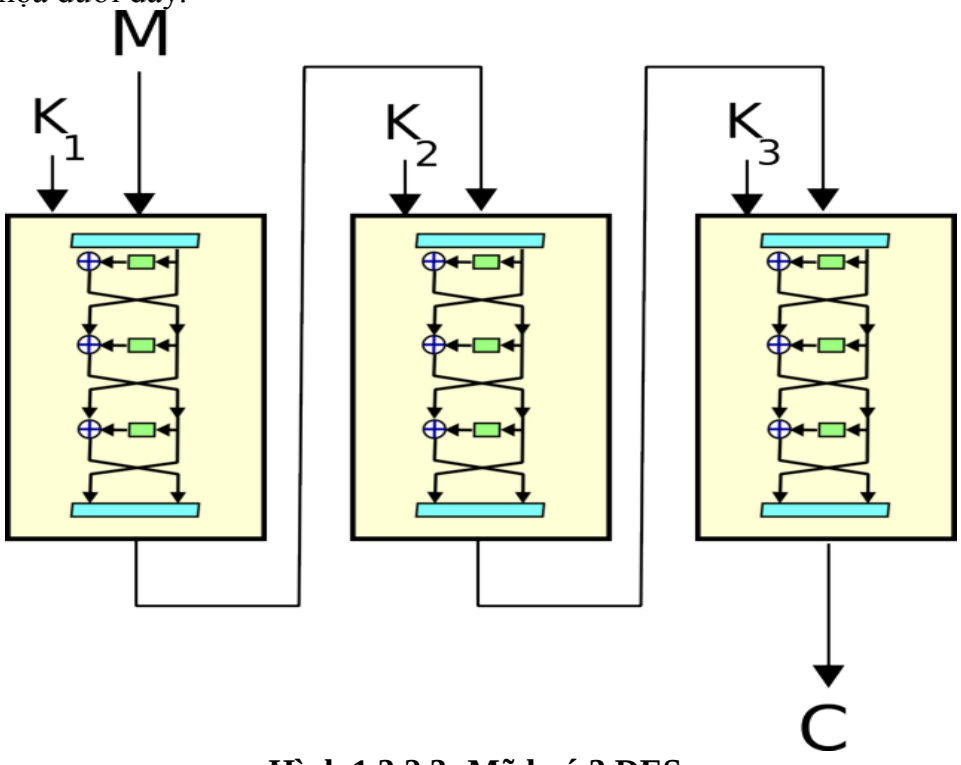
Hình 1.3.2.1: 16 bước trong quá trình mã hóa bằng DES.

Trên hình trên ta thấy mã hóa DES được thực hiện qua 16 vòng. Thông tin đầu vào là 64 bit, sẽ được chia thành 2 block trái (L) và phải (R). Sau đó từ chìa khóa key (56 bit) người ta tạo ra các khóa con (subkey) 48 bit gọi là K_i. Hàm f ở trên thực chất là 1 hàm hoán vị. Minh họa hoạt động của hàm f như sau:



Hình 1.3.2.2: Hoạt động của hàm f.

Còn 3DES thực ra là mã hóa cùng 1 thông tin qua 3 lần mã hóa DES với 3 khóa khác nhau. Do đó, chiều dài mã khóa sẽ lớn hơn và an toàn sẽ cao hơn so với DES. Hình minh họa dưới đây.



Hình 1.3.2.3: Mã hoá 3 DES.

1.3.3 Nguyên tắc quản lý khóa

Các khóa tồn tại theo chuẩn ISO 11568. Không truy cập hoặc xác định bản rõ của bất kỳ khóa bí mật nào.

Hệ thống phải ngăn chặn và phát triển việc thám mã bất kỳ khóa nào, ngăn chặn các thay đổi khi không được cấp phép đối với các vấn đề về thay thế, xóa hay chèn them bất kỳ khóa nào.

Các khóa bí mật được tạo ra theo một tiến trình không thể đoán ra bất kỳ một hay một tập hợp giá trị bất kỳ nào.

Một khóa sẽ bị thay thế bằng khóa mới trong trường khóa cũ có nguy cơ bị làm hại hoặc bị tấn công hoặc bị nghi ngờ bị làm tổn hại.

Việc làm hại một khóa trên một tuyến không ảnh hưởng đến các khóa trên tuyến khác.

Một khóa bị làm tổn hại sẽ không cung cấp bất kỳ thông tin nào cho phép xác định sự thay thế.

Một khóa sẽ chỉ được đọc vào một thiết bị khi thiết bị này an toàn và không dẫn đến quá trình điều chỉnh hay thay thế khi chưa được phép.

Khóa sẽ được mã hóa bí mật bởi thuật toán mã hóa đối xứng 3DES, và lưu trong cơ sở dữ liệu SWITCH (cho phép quản lý khóa sinh hoạt, sao lưu, phục hồi lâu dài, và đáp ứng được yêu cầu khi tăng số khóa).

1.3.4 Vấn đề mã hóa dữ liệu truyền trong hệ thống POS

Vấn đề mã hóa dữ liệu trên đường truyền từ thiết bị đầu cuối POS (POS terminal) đến trung tâm xử lý HSM của ngân hàng.

Dữ liệu được truyền trên đường truyền từ thiết bị đầu cuối POS đến trung tâm xử lý HSM được mã hóa bằng thuật toán mã hóa 3-DES. Việc bị lộ thông tin trên đường truyền xảy ra khi kẻ tấn công có được khóa mã hóa –giải mã.

Dữ liệu bị mất trên đường trền có thể xảy ra trong trường hợp kẻ tấn công là các đại lý đăng ký đặt máy POS.

Trong trường hợp kết nối bằng Dial-up, thì kẻ tấn công này, có thể quay số đến một số điện thoại nào đó để lấy cắp thông tin.

Trong trường hợp kết nối wireless hoặc thông qua một mạng LAN thì kẻ tấn công này có thể cố định đến một địa chỉ IP nào đó để lấy trộm thông tin. Sau khi lấy được thông tin trên đường truyền, kẻ tấn công này có thể dùng thông tin lấy được để thực hiện lại giao dịch đó nhiều lần để lấy tài khoản của khách hàng.

Để giải quyết vấn đề này, thường khi khách hàng sẽ là người liên hệ trực tiếp với ngân hàng để phát hiện ra đại lý gian lận. Ngân hàng sẽ kiểm tra số định danh đại lý (merchant ID) để truy tìm kẻ gian lận.

1.3.5 Một số ứng dụng của POS

Hiện nay, hệ thống POS chỉ áp dụng trong hệ thống ngân hàng, để thực hiện thành công quy trình giao dịch qua hệ thống POS thì cần có sự liên kết với hệ thống viễn thông để truyền dữ liệu ngân hàng, ngoài hệ thống POS có thể được xây dựng để kết nối với hệ thống bán hàng để lấy các dữ liệu dùng để thanh toán (như các mục dùng trong hóa đơn, số km của taxi…) sau đó tổng hợp rồi mới chuyển đến ngân hàng, điều này phụ thuộc vào công nghệ của từng ngân hàng. Về bản chất POS là một thiết bị đầu cuối chủ yếu dùng gửi yêu cầu chuyển khoản một số lượng tiền từ tài khoản này sang tài khoản khác. Đa số ứng dụng của nó là dùng để thanh toán hóa đơn của khách hàng mà không cần dùng tiền mặt, thiết bị này có thể gắn ở bất kỳ điểm bán hàng nào, kể cả trên các phương tiện như taxi. Về mặt lý thuyết thì bất kỳ công ty nào cũng có thể đầu tư một hệ thống POS để phục vụ khách hàng nội bộ nhưng vì lý do kinh tế nên trên thực tế chưa có tổ chức nào xây dựng hệ thống POS (ngoại trừ ngân hàng).

1.4 Nguy cơ mất an toàn trong hệ thống POS

1.4.1 Nguy cơ mất an toàn từ phía thiết bị trong hệ thống POS

1.4.1.1 Các thiết bị ổ đĩa cứng

Khách hàng khi sử dụng thiết bị POS này là phụ thuộc chủ yếu vào việc xóa các thông tin trên ổ đĩa cứng của các đại lý bán hàng đăng ký đặt POS.

1.4.1.2 Nguy cơ từ phía server

Thực tế, tại thiết bị POS có thể chứa đựng thông tin của hàng trăm thẻ tín dụng vì thế mà có thể sẽ xảy ra xung đột khi thực hiện giao dịch và gửi về server xử lý. Và server cũng chỉ cho phép thực hiện được một giao dịch của khách hàng. Đối với các thiết bị POS có cài đặt hệ điều hành, khi đó các thiết bị POS có chức năng tương tự như một máy tính cá nhân, và thường không có cơ chế xác thực tại các thiết bị POS về phía server. Đây là kẽ hở cho kẻ tấn công khi chúng muốn giả danh khách hàng để thực hiện giao dịch. Sự bảo vệ ở đây chỉ là ngăn chặn sự truy cập vật lý tại các thiết bị POS.

1.4.1.3 Vấn đề xác thực POS

Hiện nay hệ thống POS sử dụng thuật toán mã hóa đối xứng 3-DES trong vấn đề bảo mật, độ bảo mật của thuật toán này hiện nay có thể chấp nhận được, trừ khi bị lộ khóa mã hóa- giải mã.

Vậy để giải quyết vấn đề xác thực tại các điểm giao dịch có đặt máy POS, các đại lý cần đặt thiết bị đầu cuối POS tại cửa hàng mình với ngân hàng,thì ngân hàng sẽ cấp cho đại lý một mã số định danh đại lý đăng ký đặt thiết bị POS- merchant ID. Khi

có giao dịch thực hiện thì hệ thống trung tâm xử lý HSM của ngân hàng sẽ kiểm tra merchant ID, card number, expiry date…để xác thực thiết bị đầu cuối POS này có đủ điều kiện để thực hiện giao dich không. Nếu điều kiện là hợp lệ thì giao dịch được tiếp tục, trong trường hợp không hợp lệ giao dịch sẽ bị hủy bỏ.

1.4.1.4 Cơ chế backdoor

Là một chương trình gắn liền với thiết bị POS lưu lại các thông tin giao dịch của khách hàng, các thông tin quan trọng để có thể khôi phục lại dữ liệu mỗi khi cần thiết, việc thực hiện chức năng này thông qua một chuỗi khóa quy định của nhà cung cấp POS. Nếu người quản trị hệ thống có được khóa giải mã thì có thể thực hiện chức năng backdoor này. Đây chính là lỗ hổng cho kẻ tấn công, chúng có thể thực hiện được chức năng này nếu có được khóa giải mã.

1.4.2 Nguy cơ mất an toàn từ phía thẻ tín dụng

Thẻ tín dụng quốc tế có 2 loại, bao gồm thẻ từ và thẻ chip. Do tính bảo mật của thẻ từ không cao, gắn liền với công nghệ thấp của ngân hàng phát hành thẻ nên đối tượng làm thẻ giả thường ăn cắp thông tin của chủ thẻ bằng cách mua thông tin của các hacker khai thác được từ dữ liệu mà điểm chấp nhận thẻ truyền về ngân hàng phát hành thẻ.

1.4.3 Nguy cơ mất an toàn từ phía người dùng

Thực tế khi thanh toán tiền mua hàng hóa, hiện nay đơn vị chấp nhận thẻ chỉ yêu cầu bên mua hàng đưa thẻ tín dụng rồi nhập số tiền, quẹt thẻ qua máy POS mà không cần quan tâm người thanh toán có phải là chủ thẻ hay không.

Việc người dùng sơ ý tiết lộ thông tin của thẻ tín dụng của mình cho kẻ sấu biết là hoàn toàn có thể vì tính nhanh chóng và tiện lợi trong quá chình giao dịch mà hệ thông POS mang lại thì liệc mất tiền trong tài khoản là điều hoàn toàn có thể.

Khi mua hàng qua mạng, chủ thẻ lựa chọn giao dịch tại các website bán hàng không có uy tín, chủ thẻ có thể sẽ để lộ thông tin của thẻ tín dụng trong quá trình khai báo để mua hàng trực tuyến.

1.5 Giải pháp an toàn bảo mật đặt ra

1.5.1 Giải pháp an toàn bảo mật đặt ra với các ngân hàng

1.5.1.1. Về quản lý và tổ chức

Xây dựng hành lang pháp lý đối với các hoạt động ngân hàng bao gồm các quy chế, chính sách, các tiêu chuẩn về an toàn bảo mật thông tin.

Xây dựng một cơ chế quản lý tài nguyên hệ thống và các nguy cơ tương ứng đối với các tài nguyên đó.

Xây dựng cơ chế quản lý và kiểm soát an toàn thông tin với quy trình quản trị hệ thống và ứng dụng các phần mềm quản lý chính sách.

1.5.1.2. Về công nghệ

Kiểm soát truy cập: Thiết lập cơ chế kiểm soát chứng thực người dùng nhiều vòng trước khi cho phép truy cập vào hệ thống. Không chỉ giới hạn trong việc xác thực người dùng.

Firewall: Vùng ngân hàng điện tử và tại các chi nhánh tạo ra các vùng biên giữa các hệ thống để hạn chế và giám sát luồng thông tin giữa các hệ thống, ngăn chặn các kết nối bất hợp pháp. Các firewall được sử dụng và triển khai hiệu quả với các chính sách kết nối khắt khe nhằm đảm bảo an toàn hệ thống.

Lọc nội dung: Sử dụng các công cụ phần mềm lọc bỏ và cấm các truy xuất vào các nguồn thông tin hoặc tài liệu không thích hợp cho công việc.

Xây dựng các hệ thống phòng chống và phát hiện xâm nhập. Các hệ thống quét Virus, antispyware, antispam...

Thực hiện các cơ chế mã hoá thông tin, xây dựng hạ tầng. Thường xuyên dò tìm, phát hiện lỗ hổng hệ thống.

Thiết lập hệ thống cung cấp bản vá lỗ hổng bảo mật. Xây dựng cơ chế dự phòng và phục hồi hệ thống đảm bảo tính liên tục của hệ thống.

1.5.2. Giải pháp an toàn bảo mật đặt ra với khách hàng

1.5.2.1 Kiểm tra thông tin ngay khi nhận thẻ

Kiểm tra các thông tin trên thẻ đảm bảo đúng với các thông tin Quý khách đã đăng ký.

Ký ngay vào dải chữ ký ở mặt sau thẻ.

Thông báo ngay cho ngân hàng những thay đổi của Quý khách về địa chỉ cư trú, địa chỉ gửi sao kê, thay đổi số điện thoại liên hệ, chữ ký…

1.5.2.2 Kích hoạt thẻ để sử dụng

Thực hiện kích hoạt thẻ tại Chi nhánh/ Phòng giao dịch của ngân hàng hoặc qua tin nhắn SMS (*) để sử dụng thẻ.

1.5.2.3 Bảo mật PIN

Đổi mã PIN tại máy POS ngay sau nhận được thẻ.

Thường xuyên thay đổi mã PIN để bảo mật thông tin.

Không chọn mã PIN gắn liền với các thông tin cá nhân như số di động, ngày sinh…

Tuyệt đối không tiết lộ mã PIN cho bất kỳ ai.

Luôn lấy tay che bàn phím khi nhập mã PIN đề phòng có người nhìn trộm hoặc quay lén.

Không lưu trữ thẻ và PIN cùng nơi.

Không viết mã PIN trên thẻ.

1.5.2.4 Lưu ý khi thực hiện giao dịch trên Internet

- Không cung cấp thông tin thẻ người khác.
- Không lưu thông tin thẻ để người khác có thể lợi dụng.
- Chỉ thực hiện giao dịch tại các website uy tín, các địa chỉ mua hàng tin cậy.
- Cẩn trọng trước bất kỳ thông báo yêu cầu cung cấp thông tin thẻ (để nâng hạng, đổi thẻ, tăng hạn mức,…) từ các website/email tương tự với website/email của Ngân hàng phát hành thẻ, liên hệ với đại lý phát hành thẻ của ngân hàng để xác minh thông tin, chỉ cung cấp thông tin bằng văn bản tại đại lý phát hành.

Để thực hiện được giao dịch trên Internet, chủ thẻ cần lưu ý:

- Đối với thẻ ghi nợ nội địa: Khách hàng phải đăng ký sử dụng dịch vụ eMB Plus.
- Đối với thẻ Visa: Khách hàng phải đăng ký sử dụng tính năng e.commerce.
- Đối với thẻ MasterCard: Khách hàng nên đăng ký sử dụng dịch vụ SMS Banking để có thể kiểm soát giao dịch và chủ động thực hiện khóa và mở thẻ khi cần thiết.

1.5.2.5 Lưu ý khi giao dịch tại máy POS

Nên thực hiện giao dịch tại các máy POS vào ban ngày, nơi có đông người qua lại hoặc có bảo vệ.

Quan sát kỹ trước khi thực hiện giao dịch tại POS. Không giao dịch nếu máy POS có thiết bị lạ gắn vào khe đọc thẻ/bàn phím hoặc nhiều camera gắn tại cùng 1 POS. Nếu phát hiện các trường hợp bất thường thì ngừng giao dịch và thông báo ngay cho người quản lý.

Luôn kiểm tra tiền và lấy lại thẻ sau khi thực hiện giao dịch.

Trường hợp máy báo nhập sai số PIN, kiểm tra kỹ số PIN, sau đó thực hiện lại giao dịch. Nếu nhập sai PIN **03 lần** liên tiếp, thẻ sẽ bị khóa do nghi ngờ gian lận. Trường hợp thẻ bị khóa, Quý khách vui lòng đến Chi nhánh/ Phòng Giao dịch của MB để mở khóa thẻ và phát hành lại PIN.

1.5.2.6 Lưu ý khi thực hiện giao dịch tại thiết bị chấp nhận thẻ (POS)

Luôn yêu cầu thực hiện thanh toán thẻ qua đầu đọc Chip, và chỉ đồng ý thực hiện giao dịch qua dải từ trong trường hợp máy cà thẻ không có đầu đọc Chip.

Đảm bảo giao dịch phải được thực hiện trong tầm mắt của Quý khách để quan sát việc cà thẻ của thu ngân.

Nếu phát hiện thu ngân thực hiện giao dịch nhiều lần, yêu cầu thu ngân dừng lại và liên hệ với Trung tâm Dịch vụ khách hàng để kiểm tra số dư tài khoản thẻ. Sau đó yêu cầu thu ngân xác nhận số tiền giao dịch, hủy các hóa đơn thẻ không chính xác.

Kiểm tra thông tin trên hóa đơn đảm bảo khớp đúng thông tin thẻ và số tiền giao dịch trước khi ký chấp nhận thanh toán.

Nhận lại thẻ ngay sau khi thực hiện xong giao dịch tại các đơn vị chấp nhận thẻ.

Giữ lại các hóa đơn thanh toán thẻ và các chứng từ có liên quan để đối chiếu với các giao dịch trên sao kê tài khoản thẻ.

Quý khách nên xé nhỏ hóa đơn thẻ/ sao kê tài khoản thẻ khi cần hủy để đảm bảo không lộ thông tin thẻ.

1.5.2.7 Kiểm soát thông tin giao dịch thẻ

Đăng ký sử dụng dịch vụ hỗ trợ của ngân hàng để kịp thời cập nhật số dư tài khoản, các giao dịch phát sinh trên thẻ, thông báo ngân hàng ngăn chặn kịp thời các giao dịch lợi dụng thẻ/không do chủ thẻ thực hiện.

Thường xuyên kiểm tra thông tin giao dịch thẻ qua dịch vụ hoặc nhắn tin kiểm tra giao dịch (*).

Đối chiếu các hóa đơn đã lưu giữ với bảng sao kê giao dịch thường xuyên. Nếu có khiếu nại về giao dịch, vui lòng liên hệ với đại lý Phòng Giao dịch của ngân hàng để thực hiện yêu cầu tra soát.

1.5.2.8 Lưu giữ thẻ an toàn

Cất giữ thẻ ở nơi an toàn và bảo mật.

Không cung cấp thông tin thẻ (số thẻ, ngày hiệu lực, mã số PIN, địa chỉ, họ tên chủ thẻ...) khi nhận được email/điện thoại yêu cầu cung cấp/xác nhận thông tin hoặc các cuộc gọi nghi ngờ khác.

Không cho bất kỳ ai mượn, sử dụng, sở hữu và quản lý thẻ của Quý khách.

Không để thẻ ở gần những vật từ tính (điện thoại di động, nam châm…), các nơi có độ ẩm cao.

Tránh để thẻ cùng các vật nhọn dễ gây trầy, xước, tránh để thẻ bị cong vênh, tránh để rơi thẻ xuống nước.

Trường hợp thẻ hết hạn, Quý khách thực hiện đục lỗ Chip và cắt dải băng từ trước khi hủy để đảm bảo thẻ không bị làm giả thông tin và gửi lại cho ngân hàng.

Vì lý do bảo mật, Quý khách không lưu giữ bản sao mặt trước và mặt sau thẻ.

Chương 2: CẤU TẠO THẺ VÀ CHUẨN TRUYỀN DỮ LIỆU

Sự gia tăng của thẻ nhựa dài bắt đầu tại Hoa Kỳ trong những năm 1950. Mức giá thấp của các vật liệu tổng hợp PVC đã làm cho nó có thể sản xuất, thẻ nhựa bền mạnh mẽ hơn nhiều thích hợp cho sử dụng hàng ngày hơn so với giấy và các tông thẻ sử dụng trước đó, có thể không đầy đủ chịu được tác động cơ học và các hiệu ứng khí hậu.

Tính linh hoạt của thẻ thong minh rất cao, thậm chí cho phép các ứng dụng được thêm mới vào một thẻ đã được sử dụng, mở ra ứng dụng hoàn toàn mới vượt ra ngoài ranh giới kiểm soát của việc sử dụng thẻ truyền thống.

Thẻ thông minh cũng đang được sử dụng như "vé điện tử" cho giao thông công cộng địa phương trong nhiều các thành phố trên toàn thế giới. Thẻ thông minh không tiếp xúc thường được sử dụng cho các ứng dụng như vậy, vì chúng là đặc biệt thuận tiện và thân thiện.

2.1 Phân loại thẻ

2.1.1 Thẻ nổi

Làm nổi là kĩ thuật sớm nhất để thêm các tính năng cho máy có thể nhận diện các thẻ định danh. Các kí tự nổi trên thẻ có thể chuyển sang biên lai, thiết bị không quá đắt, và mọi người có thể đọc một cách trực quan. Tính chất và vị trí của các hình nổi được quy định trong tiêu chuẩn ISO 7811. Tiêu chuẩn này được chia thành 5 phần, giao dịch với các mã vạch cũng như dập nổi.

2.1.2 Thẻ từ

Những bất lợi cơ bản của thẻ dập nổi là việc sử dụng của họ tạo ra một loạt những giấy biên lai, tốn kém để xử lý chúng. Một biện pháp khắc phục cho vấn đề này là kĩ thuật mã hoá dữ liệu trên thẻ có mã vạch ở mặt sau của thẻ. Các mã vạch được đọc bằng cách kéo nó qua một đầu đọc, bằng tay hoặc tự động, với các dữ liệu được đọc và lưu trữ điện tử.

2.1.3 Thẻ thông minh

Thẻ thông minh là thành viên trẻ nhất và thông minh nhất của thẻ định danh trong định dạng ID-1. Tính năng đặ trưng của nó là một mạch tích hợp nhúng trong thẻ, trong đó có các thành phần để truyền, lưu trữ và xử lý dữ liệu. Dữ liệu có thể

được truyền bằng cách sử dụng địa chỉ liên hệ trên bề mặt của thẻ hoặc các trường điện từ, không có bất kì liên hệ nào.

2.1.4 Thẻ nhớ quang học

Cho các ứng dụng dung lượng lưu trữ của thẻ thông minh là không đủ, thẻ quang học có thể lưu trữ một số megabyte dữ liệu có sẵn. Tuy nhiên, với công nghệ hiện nay các thẻ này có thể được viết một lần duy nhất và không thể bị xóa.

2.2 Cấu tạo thẻ

Thân thẻ của một thẻ thông minh được thừa hưởng tính chất cơ bản của nó từ người tiền nhiệm của nó là thẻ dập nổi quen thuộc, vẫn thống trị thị trường trong lĩnh vực thẻ tín dụng. Về mặt kỹ thuật mà nói, thẻ này là những cấu trúc bằng nhựa đơn giản được cá nhân hoá bằng cách chạm nổi với một loạt các tính năng sử dụng, chẳng hạn như tên và số của chủ thẻ. Các phiên bản sau của các thẻ này được cung cấp với một mã vạch để máy có thể dễ dàng nhận biết. Khi ý tưởng cấy ghép một con chip trong thẻ đầu tiên xuất hiện, loại hình hiện có của thẻ đã được sử dụng làm cơ sở và một vi điều khiển được nhúng vào trong thân của thẻ. Nhiều tiêu chuẩn liên quan đến tính chất vật lý của thẻ là như vậy, không cụ thể cho thẻ thông minh, nhưng áp dụng tốt cho mã vạch và thẻ dập nổi.

2.3 Cấu trúc dữ liệu

Lưu trữ hoặc truyền dữ liệu không thể tránh khỏi đòi hỏi một định nghĩa chính xác của dữ liệu trong câu hỏi và cấu trúc của chúng. Chỉ sau đó nó có thể nhận ra và giải thích các yếu tố dữ liệu. Chiều dài cố định cấu trúc dữ liệu với trình tự không thể thay đổi thường xuyên gây ra các hệ thống 'sụp đổ'. Ví dụ tốt nhất của điều này là việc chuyển đổi khác nhau nhiều loại tiền Châu Âu với đồng euro. Tất cả các hệ thống và cấu trúc dữ liệu đã nâng cấp sửa lại định nghĩa tiền tệ với chi phí đáng kể. Những khó khăn tương tự trong nhiều ứng dụng thẻ thông minh. Sửa các cấu trúc dữ liệu cần thời gian dài hoặc ngắn, sớm hay muộn làm tăng lên đáng kể nỗ lực và chi phí. Tuy nhiên, vấn đề của cấu trúc dữ liệu đã được xử lý trong khoảng thời gian dài, và có một sự lựa chọn phương pháp thích hợp để có thể giải quyết vấn đề. Một phương pháp mà là rất phổ biến trong thế giới của thẻ thông minh, và được đi vào sử dụng tổng quát hơn trong tin học, đến từ các lĩnh vực truyền tải dữ liệu. Nó được gọi là Abstract Syntax Notaion(Tóm tắt kí hiệu cú pháp) 1 hoặc ASN.1. Đây là một mô tả mã hóa độc lập của các đối tượng dữ liệu, ban đầu được phát triển cho truyền dữ liệu giữa các hệ thống máy tính khác nhau. Một thay thế cho ASN.1 sẽ được sử dụng ngôn ngữ đánh dấu mở

rộng (XML) để cấu trúc dữ liệu, nhưng đến nay phương pháp này đã không đạt được một chỗ đứng trong ứng dụng thực tế trong thế giới thẻ thông minh. Về nguyên tắc, ASN.1 là một loại ngôn ngữ nhân tạo là phù hợp để mô tả dữ liệu và cấu trúc dữ liệu, chứ không phải là chương trình. Cú pháp được chuẩn hóa theo tiêu chuẩn ISO / IEC 8824, và quy tắc mã hóa được xác định theo tiêu chuẩn ISO / IEC 8825. Cả hai tiêu chuẩn được phát triển từ kế hoạch X.409 của CCITT.

Data type	Sort	Meaning
BOOLEAN	Primitive	Boolean value: yes/no
INTEGER	Primitive	Negative and positive integers
OCTET STRING	Primitive	Byte sequence (one byte = one 8-bit octet)
BIT STRING	Primitive	Bit sequence
SEQUENCE	Constructed	Several components combined to form a new data type

Hình 2.3.1 : Một vài loại dữ liệu sử dụng trong ASN-1.

Ý tưởng cơ bản của mã hóa dữ liệu sử dụng ASN.1 là tiền tố từng đối tượng dữ liệu với một nhãn đặc biệt và thông tin về chiều dài của nó. Cú pháp mô tả của ngôn ngữ khá phức tạp cũng cho phép người sử dụng xác định kiểu dữ liệu riêng của họ và tổ đối tượng dữ liệu. Ý tưởng ban đầu là tạo ra một cú pháp cơ bản hợp lệ mà có thể hình thành cơ sở cho việc trao đổi dữ liệu giữa hệ thống máy tính khác nhau, hầu như không được sử dụng trong thẻ thông minh. Hiện nay, chỉ một phần rất nhỏ của các cú pháp có sẵn được sử dụng trong lĩnh vực này, chủ yếu là do sự hạn chế dung lượng bộ nhớ của thẻ thông minh.

```
SC_Controller ::= SEQUENCE {      Definition of a new data type for SC_Controller.
  Name IA5String,                 The name of the microcontroller is an ASCII string.
  CPUType CPUPower,               CPUType refers to the definition of CPUPower.
  NPU BOOLEAN,                    Boolean value as a yes/no assertion regarding
                                  whether a coprocessor (NPU) is present.
  EEPROMSize INTEGER,             The size of the EEPROM is an integer value.
  RAMSize INTEGER,                The size of the RAM is an integer value.
  ROMSize INTEGER}                The size of the ROM is an integer value.

CPUPower ::= ENUMERATED {         Definition of a new data type for CPUPower as an
                                  enumerated type.
  8Bit (8),                       Possible selection value for the 8-bit CPU type.
  16Bit (16),                     Possible selection value for the 16-bit CPU type.
  32Bit (32)}                     Possible selection value for the 32-bit CPU type.
```

Hình 2.3.2: Ví dụ về loại dữ liệu không đầy đủ sử dụng ASN-1.

`SuperXS SC_Controller ::= {`	Specific instance of the SC-Controller data type with the data for SuperXS.
`Name "XS 8 Bit",`	The name of the microcontroller is 'XS 8 Bit'.
`CPUType 8,`	This is an 8-bit CPU.
`NPU true,`	No coprocessor (NPU) is present.
`EEPROMSize 1024,`	The size of the EEPROM is 1024 bytes.
`RAMSize 256,`	The size of the RAM is 256 bytes.
`ROMSize 8192}`	The size of the ROM is 8192 bytes.

Hình 2.3.3: Trường dữ liệu cho một vi điều khiển đặc biệt.

`'30 1C'`	Tag '30' for a string with a length of 28 bytes ('1C').
`'16 08 58 53 20 38 20 42 69 74'`	Tag '16' for an IA5 string with a length of 8 bytes ('08') and a content of '58 53 20 38 20 42 69 74' (= "XS 8 Bit").
`'0A 01 08'`	Tag '0A' for an enumerated data type with a length of 1 byte ('01') and a content of '08'.
`'01 01 FF'`	Tag '01' for a Boolean data type with a length of 1 byte ('01') and a content of 'FF', which corresponds to the value 'true'.
`'02 02 04 00'`	Tag '02' for an integer data type with a length of 2 bytes ('02') and a content of '04 00' (1024).
`'02 02 01 00'`	Tag '02' for an integer data type with a length of 2 bytes ('02') and a content of '01 00' (256).
`'02 02 20 00'`	Tag '02' for an integer data type with a length of 2 bytes ('02') and a content of '02 00' (8192).

Hình 2.3.4: Mã sử dụng ASN-1 BER.

Quy tắc mã hóa cơ bản (BER) cho ASN.1 được định nghĩa trong tiêu chuẩn ISO / IEC 8825. Đối tượng dữ liệu được tạo theo các quy tắc này được gọi là đối tượng dữ liệu BER-TLV-coded. Một đối tượng dữ liệu BER-coded có một nhãn (được gọi là 'từ khóa'), một lĩnh vực chiều dài và phần dữ liệu thực tế, với một tùy chọn kết thúc đánh dấu. Một số bit trong thẻ được xác định trước theo các quy tắc mã hóa. Cấu trúc thực tế là thể hiện trong hình 4.1. Quy tắc mã hóa sắc (DER) tạo thành một tập hợp con của BER Các quy tắc mã hóa chỉ định, trong số những thứ khác, mã hóa các thông tin chiều dài, có thể là một, hai hoặc ba byte dài. Một bản tóm tắt cơ bản của BER và DER có thể được tìm thấy trong Burton Kaliski [Kaliski 93]. ASN.1 đối tượng được mã hóa bằng cách sử dụng cấu trúc TLV cổ điển, trong đó "T" (tag) biểu thị nhãn của đối tượng, "L" (chiều dài) đề cập đến chiều dài của nó và "V" (giá trị) là dữ liệu thực tế. Trường đầu tiên của một cấu trúc TLV là thẻ cho các đối tượng dữ liệu trong lĩnh vực V sau. Tránh sự cần thiết cho mỗi người dùng để định nghĩa các thẻ riêng của mình, trong đó sẽ mở cửa không tương thích, đó là tiêu chuẩn để xác định thẻ cho khác nhau, cấu trúc dữ liệu thường xuyên được sử dụng. ISO / IEC 7816-6, ví dụ, định nghĩa các thẻ cho các đối tượng sử dụng trong các ứng dụng công nghiệp nói chung, ISO / IEC 7816-4 định nghĩa các thẻ để nhắn tin an toàn, và EMV cũng định nghĩa

một số thẻ khác. Nó là do không có phương tiện trường hợp một thẻ đã cho là phổ biến sử dụng cho cùng một loại phần tử dữ liệu, nhưng một quá trình tiêu chuẩn hóa về cơ bản đang diễn ra.

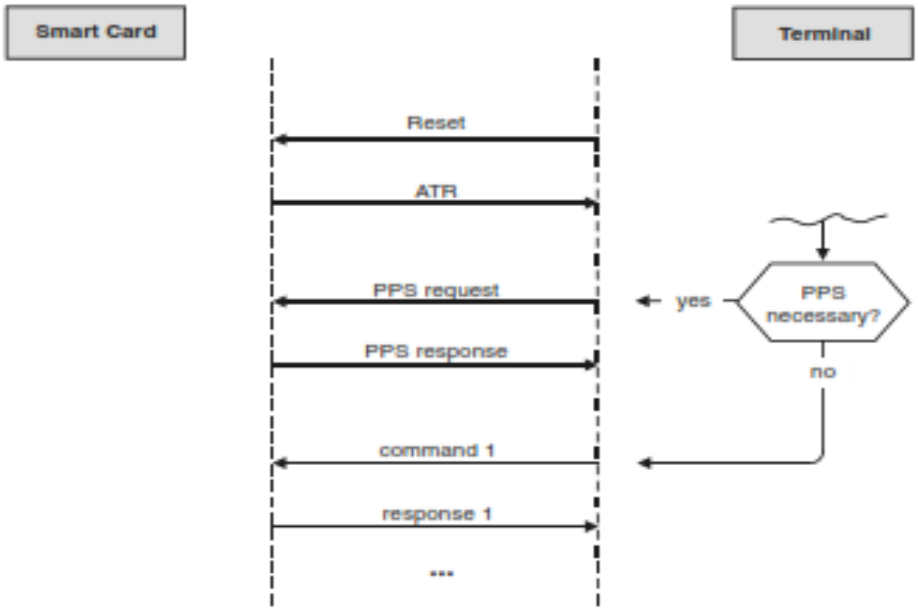
2.4 Truyền dữ liệu

Khả năng thông tin liên lạc hai chiều là một điều kiện tiên quyết cho tất cả các tương tác giữa thẻ thông minh và thiết bị đầu cuối. Tuy nhiên, chỉ có một dòng duy nhất có sẵn. Dữ liệu kỹ thuật số được trao đổi giữa thẻ và thiết bị đầu cuối thông qua kết nối điện tử. Vì chỉ có một dòng tồn tại, thẻ và thiết bị đầu cuối phải thay phiên truyền dữ liệu, với bên kia hành động như người nhận. Việc thay thế truyền và nhận dữ liệu được gọi là một thủ tục một chiều.

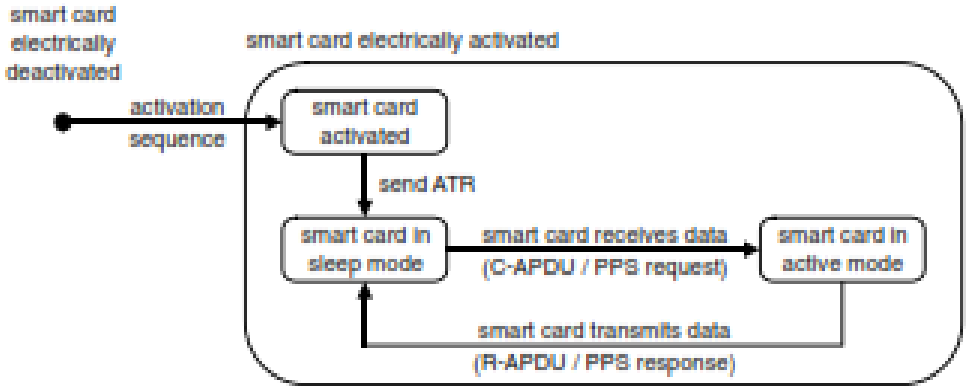
Một thủ tục hai chiều, trong đó cả hai bên có thể truyền và nhận đồng thời, là hiện nay không được thực hiện cho thẻ thông minh. Tuy nhiên, kể từ khi bộ xử lý thẻ thông minh nhất có hai cổng I/O, và hai trong số tám địa chỉ liên lạc được dành riêng cho các ứng dụng trong tương lai (ví dụ như cổng I/O thứ hai kết nối hoặc giao diện USB), hoạt động hai chiều sẽ chắc chắn được về mặt kỹ thuật có thể. Điều này không nghi ngờ sẽ được thực hiện trong phần cứng và hệ điều hành trong thời gian trung kỳ.

Thông tin liên lạc với các thẻ luôn luôn khởi xướng bởi các thiết bị đầu cuối. Thẻ luôn luôn đáp ứng các lệnh từ thiết bị đầu cuối, có nghĩa là các thẻ không bao giờ gửi dữ liệu mà không có một kích thích kinh tế ben ngoài. Điều này mang lại một mối quan hệ chủ - khách, với các thiết bị đầu cuối như là chủ và thẻ như khách. Các thủ tục lệnh chủ động được sử dụng bởi các thẻ thông minh viễn thong và cho phép các thẻ thông minh để gửi lệnh đến thiết bị đầu cuối, cũng dựa trên các tiêu chuẩnsắp xếp chủ - khách.

Sau khi thẻ đã được đưa vào trong một thiết bị đầu cuối, tiếp xúc của lần đầu tiên được kết nối với máy móc như của các thiết bị đầu cuối. Năm tiếp xúc tích cực sau đó được kích hoạt bằng điện trong đúng trình tự. Sau này, các thẻ tự động thực thi một quyền lực trên thiết lập lại và sau đó gửi một trả lời để thiết lập lại (ATR) cho các thiết bị đầu cuối. Thiết bị đầu cuối đánh giá ATR, trong đó có nhiều các thông số liên quan đến thẻ và dữ liệu được truyền đi, và sau đó gửi lệnh đầu tiên. Các thẻ xử lý lệnh và tạo ra một phản ứng, mà nó sẽ gửi trở lại thiết bị đàu cuối. Việc trở lại và tương tác của các lệnh và phản ứng tiếp tục cho đến khi thẻ được kích hoạt. Giữa ATR và lệnh đầu tiên được gửi vào thẻ, thiết bị đầu cuối cũng có thể gửi thông số lựa chọn giao thức (PPS). Thiết bị đầu cuối có thể sử dụng lệnh này, giống như ATR là độc lập với các giao thức truyền dẫn, thiết lập các thông số truyền khác nhau cho giao thức truyền dẫn của thẻ.



Hình 2.4.1: Chuyển dữ liệu ban đầu giữa một thiết bị đầu cuối và một thẻ thông minh.



Hình 2.4.2: Một thẻ thông minh kích hoạt và giao tiếp với các thiết bị đầu cuối.

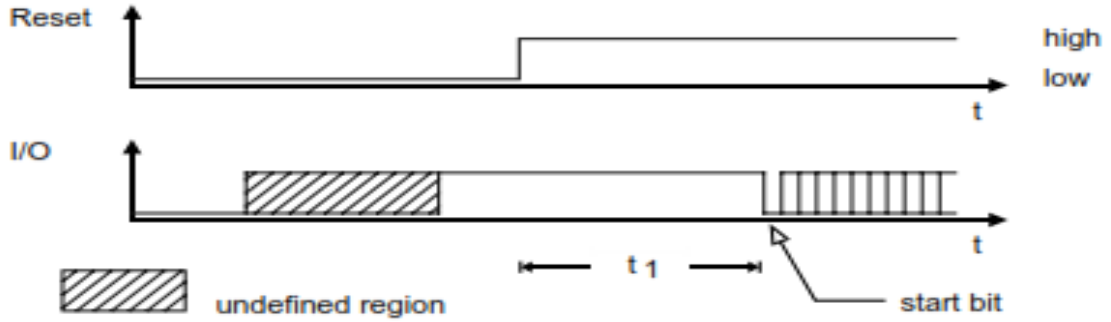
2.4.1 Trả lời để thiết lập lại (Answer to reset – ATR)

Sau khi cung cấp điện áp, tín hiệu đồng hồ và tín hiệu thiết lập lại đã được áp dụng, thẻ thông minh sẽ gửi một câu trả lời để thiết lập lại (ATR) thông qua I/O. Chuỗi dữ liệu, trong đó có nhiều nhất là 33 byte, luôn luôn gửi với giá trị chia (đồng hồ tốc độ chuyển đổi) của 372 phù hợp với tiêu chuẩn ISO / IEC 7816-3. Nó chứa các thông số khác nhau liên quan đến các giao thức truyền dẫn và thẻ. Giá trị chia này nên được sử dụng ngay cả khi các giao thức truyền dẫn sử dụng sau ATR sử dụng một giá trị chia khác nhau (ví dụ 64). Điều này đảm bảo rằng một ATR từ bất kỳ thẻ luôn luôn có thể được nhận, bất kể các thông số của giao thức truyền dẫn cuối cùng sử dụng.

Nó là rất hiếm cho một ATR phải có chiều dài tối đa cho phép. Nó thường bao gồm một vài byte. Đặc biệt là trong các ứng dụng thẻ nên được sử dụng một cách

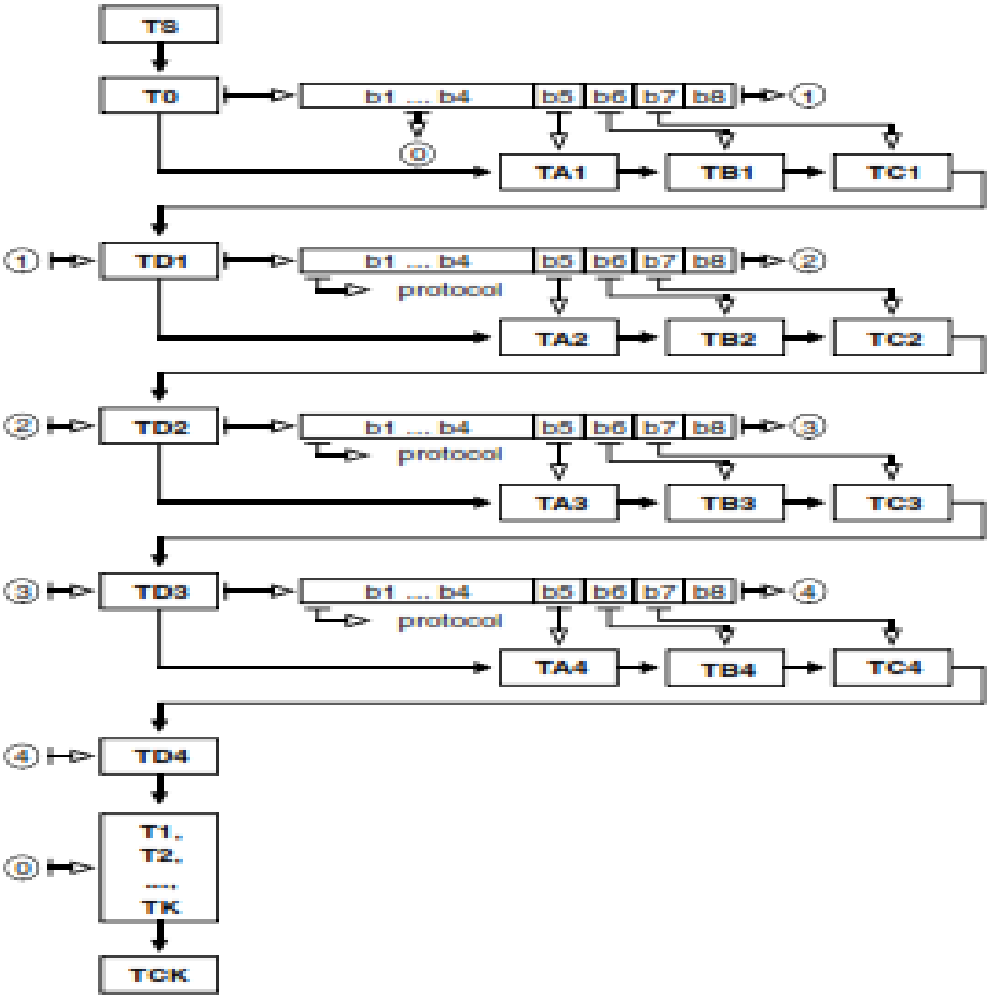
nhanh chóng sau trình tự kích hoạt. Một ví dụ điển hình được trả một số điện thoại đường sử dụng một thẻ ví điện tử thông minh. Ngay cả khi chiếc xe đi qua cổng số điện thoại một cách nhanh chóng, nó phải có khả năng đáng tin cậy ghi nợ thẻ trong thời gian ngắn có sẵn.

Sự bắt đầu của truyền ATR phải xảy ra từ 400 đến 40.000 chu kỳ đồng hồ sau khi thiết bị đầu cuối phát hành các tín hiệu đặt lại. Với tốc độ đồng hồ của 3,5712 MHz, điều này tương ứng với một khoảng thời gian 112 µs để 11,20 ms, trong khi tại 4,9152 MHz khoảng thời gian là 81,38 µs đến 8,14 ms. Nếu thiết bị đầu cuối không nhận được sự bắt đầu của ATR trong khoảng thời gian này, nó lặp đi lặp lại kích hoạt trình tự nhiều lần (thường lên đến ba lần) để cố gắng phát hiện một ATR. Nếu tất cả những nỗ lực thất bại, các thiết bị đầu cuối giả định rằng các thẻ bị lỗi và phản ứng phù hợp.



Hình 2.4.3: Biểu đồ thời gian thiết lập lại và bắt đầu của ATR, phù hợp tiêu chuẩn ISO/IEC 7816-3.

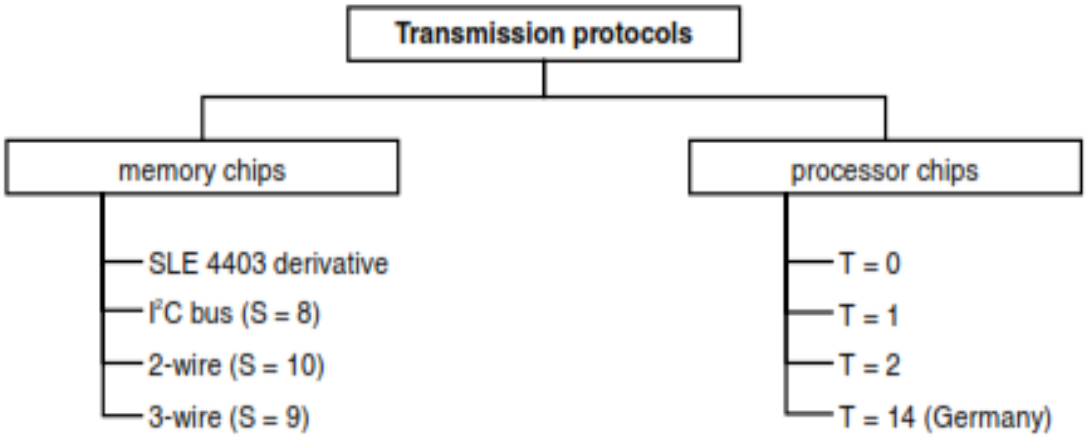
Trong ATR, thời gian giữa hai byte liên tiếp có thể lên 9600 etu theo tiêu chuẩn ISO / IEC 7816-3. Giai đoạn này được chỉ định của các thời gian chờ đợi ban đầu, và đó chính xác là thứ hai với tốc độ đồng hồ của 3,5712 MHz. Điều này có nghĩa rằng các tiêu chuẩn cho phép một sự chậm trễ một giây giữa các byte cá nhân của ATR khi nó được gửi đến thiết bị đầu cuối. Trong một số hệ điều hành thẻ thông minh, thời gian này được sử dụng để tính toán nội bộ và EEPROM viết truy cập.



Hình 2.4.4: Cấu trúc cơ bản và yếu tố dữ liệu của ATR.

2.4.2 Giao thức truyền dữ liệu

Sau khi các thẻ thông minh đã gửi một ATR, có thể theo sau bởi một PPS, nó chờ lệnh đầu tiên từ các thiết bị đầu cuối. Quá trình tiếp theo luôn luôn tương ứng với các nguyên tắc chủ - khách với các thiết bị đầu cuối. Trong điều kiện cụ thể, các thiết bị đầu cuối sẽ gửi một lệnh vào thẻ, và sau này thực hiện nó và sau đó trả về một phản ứng. Việc trở lại và ra tương tác của các lệnh và trả lời không bao giờ thay đổi. Có nhiều cách khác nhau, trong đó thông tin liên lạc với một thẻ thông minh có thể được thành lập. Cũng có một số phương pháp khác nhau cho truyền thông resynchronizing nếu một sự xáo trộn xảy ra. Việc thực hiện chính xác của các lệnh, các câu trả lời tương ứng và các thủ tục được sử dụng trong trường hợp lỗi truyền dẫn được xác định trong các hình thức của giao thức truyền tải.



Hình 2.4.2.1: Phân loại các giao thức truyền tải được sử dụng với các loại thẻ tiếp xúc thông minh.

Protocol	Meaning
T = 0	Asynchronous, half-duplex, byte oriented, specified in ISO/IEC 7816-3
T = 1	Asynchronous, half-duplex, block oriented, specified in ISO/IEC 7816-3 Amd. 1
T = 2	Asynchronous, full duplex, block oriented, specified in ISO/IEC 10536-4
T = 3	Full duplex; not yet specified.
T = 4	Asynchronous, half-duplex, byte oriented, extension of T = 0, not yet specified
T = 5 … T = 13	Reserved for future use, not yet specified
T = 14	For national use, not standardized by ISO
T = 15	Reserved for future use and not yet specified

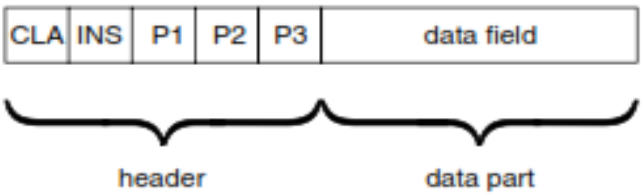
Hình 2.4.2.2: Tóm tắt các phương thức truyền theo ISO/IEC 7816-3.

Hai trong số các giao thức này chiếm ưu thế trong việc sử dụng quốc tế. Đầu tiên là giao thức T = 0, đã trở thành một tiêu chuẩn quốc tế vào năm 1989 (theo tiêu chuẩn ISO/IEC 7816-3). Khác là T = 1, đã được giới thiệu vào năm 1992 trong một sửa đổi một tiêu chuẩn quốc tế (tại thời điểm các tiêu chuẩn ISO/IEC 7816-3 AMD. 1, bây giờ tiêu chuẩn ISO/IEC 7816-3). Giao thức truyền hai chiều với T = 2 dựa trên T = 1, hiện đang trong giai đoạn định nghĩa và sẽ có sẵn như một tiêu chuẩn quốc tế trong một vài năm.

Ở Đức, hệ thống thẻ điện thoại được phân phối sử dụng rộng rãi nhưng một giao thức thứ ba. Nó được định nghĩa trong một đặc điểm kỹ thuật nội bộ của Deutsche Telekom. Các yếu tố dữ liệu được vận chuyển bằng các giao thức truyền tải được gọi là giao thức truyền dẫn đơn vị dữ liệu (TPDUs). Chúng có thể được coi là thùng chứa giao thức phụ thuộc vào dữ liệu giao thong đến và đi từ thẻ. Các dữ liệu ứng dụng thực tế được nhúng vào trong các thùng chứa. Ngoài các giao thức truyền thẻ thông minh kỹ thuật phức tạp, có thêm thiết lập các giao thức đồng bộ rất đơn giản cho thẻ nhớ. Họ thường được sử dụng với thẻ điện thoại, thẻ bảo hiểm y tế và các loại tương tự. Tuy nhiên, họ không có sửa lỗi cơ chế, và chúng được dựa trên ổ cứng máy tính logic trong chip.

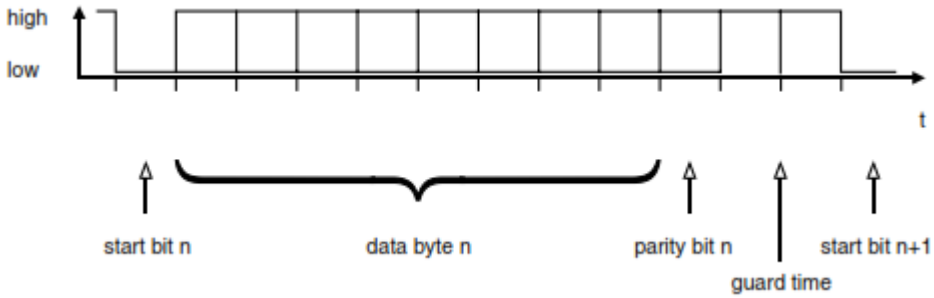
2.4.2.1 Giao thức truyền dữ liệu với T = 0

Giao thức truyền dữ liệu với T = 0 lần đầu tiên được sử dụng tại Pháp trong sự phát triển ban đầu của thẻ thông minh, và nó cũng là tiêu chuẩn quốc tế giao thức thẻ thông minh đầu tiên. Nó được tạo ra trong những năm đầu của công nghệ thẻ thông minh, và do đó nó được thiết kế để sử dụng bộ nhớ tối thiểu và đơn giản tối đa. Giao thức này được sử dụng trên toàn thế giới trong thẻ GSM, nó sử dụng rộng rãi cho tất cả các giao thức thẻ thông minh hiện nay. Giao thức T = 0 là chuẩn hóa ISO/IEC 7816-3. Thông số kỹ thuật tương thích bổ sung được chứa trong GSM 11.11, TS 102,221 và chi tiết kỹ thuật EMV. Giao thức T = 0 là byte định hướng, có nghĩa là đơn vị nhỏ nhất xử lý bởi các giao thức là một byte duy nhất. Các đơn vị truyền dữ liệu bao gồm một tiêu đề có chứa một lớp byte, một byte lệnh và ba byte thông số, tùy chọn theo sau là một phần dữ liệu. Ngược lại với các giao thức ứng dụng dữ liệu đơn vị (APDU) theo quy định của tiêu chuẩn ISO/IEC 7816-4, chiều dài thông tin chỉ được cung cấp bởi tham số P3. Điều này cho thấy chiều dài của dữ liệu lệnh hoặc phản ứng dữ liệu. Nó cũng được quy định theo tiêu chuẩn ISO / IEC 7816-3.



Hình 2.4.2.1.1: Cấu trúc của một lệnh với giao thức T = 0.

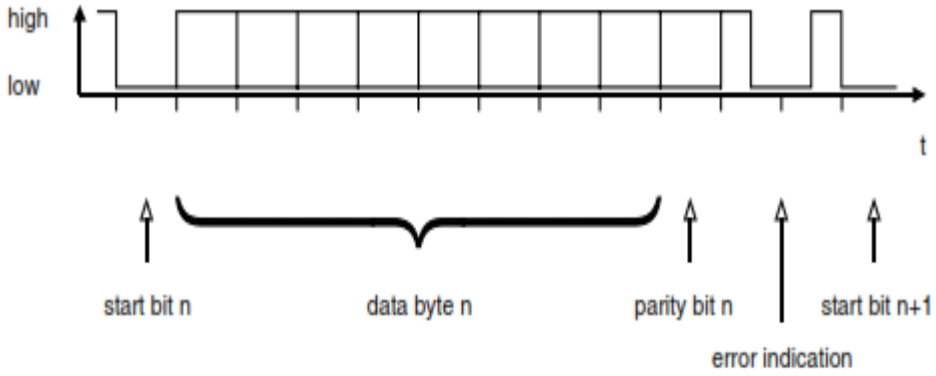
Do định hướng byte của giao thức T = 0, nếu một lỗi truyền dẫn được phát hiện, các byte truyền lại không chính xác phải được yêu cầu ngay lập tức. Với các giao thức khối, ngược lại, toàn bộ khối (một chuỗi các byte) phải được truyền lại nếu lỗi xảy ra. Lỗi phát hiện với T = 0 dựa hoàn toàn vào một bit chẵn lẻ nối vào mỗi byte gửi đi.



Hình 2.4.2.1.2: Một byte truyền qua giao diện I / O không có lỗi bằng cách sử dụng giao thức T = 0.

Nếu người nhận phát hiện một lỗi truyền dẫn, nó phải thiết lập các đường I/O đến một mức độ thấp cho thời hạn một etu bắt đầu nửa chừng khoảng bit đầu tiên của thời gian bảo vệ của bị lỗi byte. Điều này chỉ ra cho bên kia là byte gần đây nhất phải được truyền lại. Cơ chế lặp lại byte là rất đơn giản, và nó có lợi thế mà nó là lựa chọn, kể từ byte không chính xác phải được lặp đi lặp lại. Thật không may, cơ chế này bị một bất lợi nghiêm trọng. Hầu hết các IC giao diện điều trị khoảng etu là đơn vị nhỏ

nhất được phát hiện, vì vậy họ không thể nhận ra một mức thấp trên các đường I/O được đặt nằm qua một bit dừng. Tiêu chuẩn giao diện IC như vậy không phù hợp với giao thức T = 0. Tuy nhiên, nếu mỗi bit được nhận riêng bằng phần mềm, đây không phải là một vấn đề.



Hình 2.4.2.1.3: Một lỗi truyền dữ liệu được chỉ định trong giao thức T = 0 bởi một mức độ thấp tại giao diện I/O trong suốt thời gian bảo vệ.

Giao thức T = 0 cũng cho phép một lập trình điện áp bên ngoài cho các EEPROM hoặc EPROM được bật hoặc tắt. Điều này được thực hiện bằng cách thêm 1 để các byte nhận lệnh được và gửi lại cho các thiết bị đầu cuối như một byte xác nhận. Đây là lý do tại sao chỉ còn có giá trị lệnh byte được phép, vì nếu không thì cơ chế này sẽ không làm việc. Tuy nhiên, chuyển đổi một điện áp lập trình bên ngoài là lạc hậu kỹ thuật, vì tất cả các vi điều khiển thẻ thông minh bây giờ tạo ra điện áp lập trình trong các chip riêng của mình.

Để minh họa cho T = 0 chuỗi lệnh-phản ứng, chúng ta hãy giả định rằng thiết bị đầu cuối gửi thẻ lệnh với một phần dữ liệu, và các thẻ đáp ứng với dữ liệu và mã trở lại. Thiết bị đầu cuối đầu tiên gửi các thẻ 5-byte tiêu đề lệnh, bao gồm một lớp byte, một byte lệnh và P1, P2 và P3 byte. Nếu điều này là nhận được một cách chính xác, thẻ trả sự thừa nhận (ACK) trong hình thức của một byte thủ tục (PB). Sự thừa nhận này là mã hóa giống như các byte lệnh nhận được. Khi nhận được các byte thủ tục, các thiết bị đầu cuối gửi chính xác số lượng các byte dữ liệu được chỉ định bởi các byte P3. Bây giờ các thẻ đã nhận được lệnh đầy đủ, và nó có thể xử lý chúng và tạo ra một phản ứng.

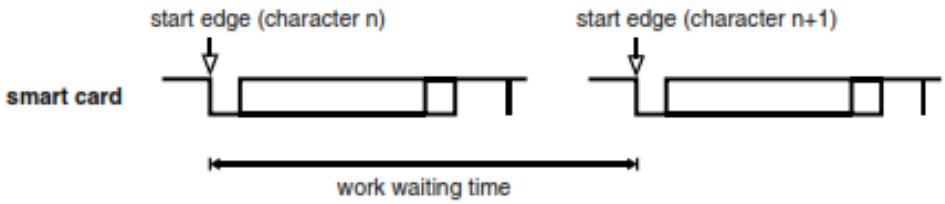
Nếu trả lời có chứa dữ liệu thêm vào 2-byte mã trở lại, thẻ thông báo thiết bị đầu cuối của điều này thông qua một mã trở lại đặc biệt, với số lượng dữ liệu được chỉ định bởi SW2. Sau khi nhận được phản ứng này, các thiết bị đầu cuối sẽ gửi thẻ lệnh GET RESPONSE, bao gồm một tiêu đề chỉ huy và một dấu hiệu cho thấy số lượng dữ liệu được gửi đi. Các thẻ tại thiết bị đầu cuối sẽ gửi số lượng yêu cầu của dữ liệu được tạo ra để đáp ứng lệnh đầu tiên, với mã lợi nhuận hợp lý. Điều này hoàn thành một chuỗi lệnh.

Nếu một lệnh được gửi vào thẻ và thẻ chỉ tạo ra một mã trả lại không có mục dữ liệu, GET RESPONSE của hình dưới đây không xảy ra. Kể từ khi thêm lệnh từ lớp ứng dụng là cần thiết để thực hiện hành động này (lấy dữ liệu liên quan để một lệnh trước đó), tự nhiên không còn nghiêm ngặt tách biệt giữa các lớp giao thức. Một lớp lệnh ứng dụng (GET RESPONSE) phải được sử dụng ở đây để hỗ trợ liên kết dữ liệu, trong đó có tác dụng nhất định trên các ứng dụng trong câu hỏi.

Smart card		Terminal
	←	5-byte command header [CLA, INS, P1, P2, P3]
Header received without error, request transmission of data section: [ACK] (acknowledge ACK)	→	
	←	[data section] with number of data bytes = P3
command processing Command executed and data available; data length in SW2: [SW1 || SW2]	→	
	←	GET RESPONSE P3 =quantity of data to be sent [CLA, INS, P1, P2, P3]
[data || SW1 || SW2]	→	Command–response sequence completed.

Hình 2.4.2.1.4: Thông tin liên lạc không điển hình T = 0 liên tục với dữ liệu trong cả hai lệnh và đáp ứng.

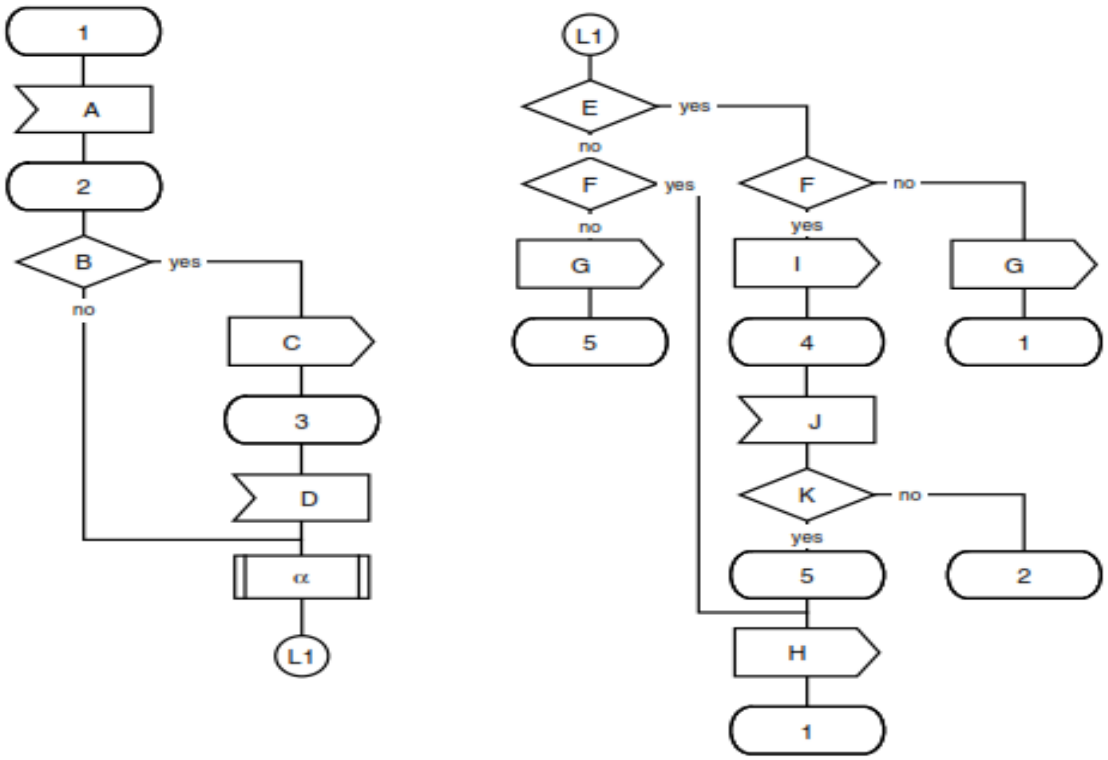
Tất cả điều này có thể xuất hiện phức tạp ngay từ cái nhìn đầu tiên, vì vậy nó được hiển thị lại đồ họa trong hình dưới đây. Khoảng cách tối đa giữa các cạnh hàng đầu của hai byte liên tiếp được chỉ định làm việc thời gian chờ đợi. Điều này được mã hóa trong dữ liệu yếu tố TC2 của ATR.



Hình 2.4.2.1.5: Định nghĩa của công việc thời gian chờ.

Các chức năng chính của thời gian bảo vệ là để tách riêng byte trong quá trình truyền. Điều này cho phép người gửi và người nhận thêm thời gian để thực hiện các chức năng của giao thức truyền dẫn. Nếu thẻ thông minh trả về một byte thủ tục có chứa các giá trị null ('60 ') tới các thiết bị đầu cuối, điều này không có bất kỳ ảnh hưởng đến trình tự thực tế của giao thức, nhưng nó thông báo cho thiết bị đầu cuối là thẻ thông minh vẫn đang xử lý lệnh cuối cùng mà nó nhận được. Gửi một giá trị null

có thể được sử dụng như một loại chờ đợi thời gian gia hạn (WTX), mặc dù nó không phải là tiêu chuẩn hóa theo hình thức này.



Hình 2.4.2.1.6: Bộ máy thẻ thông minh của nhà nước cho quá trình thông tin liên lạc, sử dụng giao thức truyền thông T = 0, mà không có xử lý lỗi.

α Xử lý lệnh

1 Quiescent state

2 Tiêu đề nhận được với CLA, INS, P1, P2 và P3

3 Đợi đoạn dữ liệu
(P3 = số byte)

4 Chờ một lệnh
(tiêu đề với CLA, INS, P1, P2 và P3)
(P3 = số lượng dữ liệu phản ứng)

5 SW1, SW2 gửi và
nhận được GET RESPONSE

A Nhận tiêu đề (5 byte)

B Dữ liệu có sẵn (P3 = 0)?

C Mục dữ liệu có sẵn,
thủ tục gửi byte đến thiết bị đầu cuối

D Nhận phần dữ liệu
(P3 = number of bytes)

E Đã lệnh chứa một đoạn dữ
liệu (ví dụ, C và D thực hiện)?

F Là phản ứng dữ liệu có sẵn
(không xảy ra lỗi)?

G Gửi SW1 và SW2

H Gửi phản ứng dữ liệu có sẵn
SW1 và SW2

I Gửi SW1 và SW2
(SW2 = số lượng dữ liệu phản hồi)

J Nhận lệnh
(header = 5 byte)

K là lệnh nhận GET RESPONSE?

Giao thức T = 0 cho phép các thẻ nhận được các byte trong phần dữ liệu cá nhân sau khi nó đã nhận được các tiêu đề. Để làm như vậy, nó chỉ có thể gửi các byte ngược với thiết bị đầu cuối như là một byte thủ tục, sau đó thiết bị đầu cuối sẽ gửi một byte

dữ liệu duy nhất. Các byte dữ liệu theo sau các byte thủ tục tiếp từ thẻ. Cách truyền byte khôn ngoan này có thể tiếp tục cho đến khi thẻ đã nhận được tất cả các byte trong phần dữ liệu, hoặc cho đến khi nó sẽ gửi các byte không ngược với thiết bị đầu cuối như là một byte thủ tục. Khi nhận được byte không đảo ngược, các thiết bị đầu cuối sẽ gửi tất cả các byte dữ liệu còn lại vào thẻ, sẽ có sau đó nhận được lệnh hoàn tất.

Có hai điều không tương thíchgiữa GSM 11.11 và ISO/IEC 7816-3. Đầu tiên là theo tiêu chuẩn GSM, một GET RESPONSE được yêu cầu sử dụng SW1 = '9F ', trong khi theo tiêu chuẩn ISO/IEC tiêu chuẩn giá trị thông thường là '61'. Trong mỗi trường hợp, SW2 có chứa số lượng dữ liệu được lấy. Sự không tương thích thứ hai giữa hai tiêu chuẩn liên quan đến cách thức mà dữ liệu được lấy sử dụng GET RESPONSE. Cách mô tả ở trên tương ứng với tiêu GSM và là đại diện cho phần lớn các ứng dụng thẻ thông minh trên toàn thế giới. Theo tiêu chuẩn ISO/IEC, một số lượng nhất định của dữ liệu có thể được lấy sử dụng GET RESPONSE, nhưng không có dấu hiệu cho phép các gói dữ liệu sau đó được yêu cầu sau khi khác. Với tiêu chuẩn ISO/IEC, GET RESPONSE luôn luôn bắt đầu với các byte đầu tiên.

Hai điều không tương thích có thể dễ dàng xử lý các thiết bị đầu cuối của phần mềm phù hợp. Điều quan trọng là phải biết rằng chúng tồn tại.

Smart card		**Terminal**
	←	5-byte command header [CLA, INS, P1, P2, P3]
'Send one data byte'	→	
	←	[Data byte 1]
'Send one data byte'	→	
	←	[Data byte 2]
further reception of individual bytes		*further transmission of individual bytes*
'Send all remaining data bytes'	→	
	←	[Data bytes *n*–P3] (P3 = number of data bytes)
command processing [SW1 || SW2]	→	Command–response sequence completed

Hình 2.4.2.1.7: Tiếp nhận byte đơn với T = 0.

Với một giao thức truyền dẫn, các mối quan tâm chính của người sử dụng chỉ có tốc độ dữ liệu truyền tải và phát hiện lỗi và cơ chế điều chỉnh cuối cùng. Truyền một byte 8-bit đòi hỏi phải gửi 12 bit, trong đó có một bit bắt đầu, một bit chẵn lẻ và hai etu cho thời gian bảo vệ. Truyền một byte do đó mất 12 etu, tương đương với 1,25 ms với một tần số đồng hồ 3,5712 MHz và một giá trị chia 372.

Command	User data	Protocol data	Data transmission time
READ BINARY	C: 5 bytes R: 2 + 8 bytes	—	18.75 ms
UPDATE BINARY	C: 5 + 8 bytes R: 2 bytes	—	18.75 ms
ENCRYPT	C: 5 + 8 bytes R: 2 + 8 bytes	C: 5 bytes R: 2 bytes	37.50 ms

Hình 2.4.2.1.8: Danh sách dữ liệu thời gian truyền một số lệnh điển hình.

Tốc độ truyền dữ liệu tự nhiên giảm nếu lỗi truyền xảy ra. Tuy nhiên, cơ chế lặp lại byte đơn là rất thuận lợi ở đây, vì chỉ nhận được byte không chính xác phải được truyền lại.

Cơ chế phát hiện lỗi của giao thức T = 0 chỉ bao gồm một kiểm tra chẵn lẻ vào cuối mỗi byte. Điều này cho phép công nhận đáng tin cậy của các lỗi bit đơn, nhưng lỗi hai-bit không thể được phát hiện. Hơn nữa, nếu một byte bị mất trong quá trình truyền từ thiết bị đầu cuối vào thẻ, kết quả này trong một vòng lặp vô tận (bế tắc) trong thẻ, kể từ khi nó được mong đợi một số cụ thể của byte và không có khả năng thời gian ra ngoài. Chỉ cách thiết thực cho các thiết bị đầu cuối để thoát khỏi tình trạng này là để thiết lập lại thẻ và thiết lập liên lạc lại từ đầu.

Có một tình huống tương tự như khi các thiết bị đầu cuối được mong đợi nhiều dữ liệu hơn so với thẻ thông minh sẽ gửi. Điều này cũng không thể tránh khỏi dẫn đến bế tắc. Vì lý do này, một số hiện thực của giao thức T = 0 trong thiết bị đầu cuối có một bộ đếm thời gian mà gây nên chấm dứt thông tin liên lạc sau một khoảng thời gian tối đa cấu hình. Cơ chế sử dụng cho điều này là tương tự như đối với các khối thời gian chờ đợi (BWT) với T = 1 giao thức. Tuy nhiên, nó không phải là tiêu chuẩn hóa và do đó thực hiện phụ thuộc.

Trong thông tin liên lạc bình thường, sự tách biệt đủ của liên kết và lớp vận chuyển không gây ra bất kỳ vấn đề lớn. Hoạt động thông suốt của các ứng dụng GSM là bằng chứng tốt nhất về điều này. Tuy nhiên, các vấn đề phát sinh một cách nhanh chóng nếu tin nhắn an toàn được sử dụng. Với một tiêu đề phần được mã hóa và một phần dữ liệu mã hóa hoàn toàn, nó không còn có thể hỗ trợ giao thức T = 0 sử dụng các thủ tục được mô tả trước đây mà không chịu các chi phí lớn. Điều này là do byte không được mã hóa phải được sử dụng cho các byte thủ tục trong giao thức T = 0. Tuy nhiên, thực tế này đã được công nhận bởi các tổ chức tiêu chuẩn và được đưa vào tài khoản trong các tiêu chuẩn liên quan đến bảo mật tin nhắn, vì vậy tất cả các loại tin nhắn an toàn là có thể sử dụng giao thức T = 0.

Do sự vắng mặt của tách lớp và các vấn đề rõ ràng trong trường hợp một kết nối xấu, giao thức T = 0 thường được coi là lỗi thời. Tuy nhiên, lỗi truyền dẫn gần như không bao giờ xảy ra trong thông tin liên lạc giữa các thiết bị đầu cuối và các thẻ. Các ưu điểm chính của giao thức T = 0 là tốt tỷ lệ trung bình của nó truyền tải, chi phí thực hiện tối thiểu và sử dụng rộng rãi.

2.4.2.2 Giao thức truyền dữ liệu với T = 1

Giao thức T = 1 truyền dẫn là không đồng bộ giao thức một chiều cho thẻ thông minh. Nó được dựa trên tiêu chuẩn quốc tế ISO/IEC 7816-3. TS 102.221 và chi tiết kỹ thuật EMV cũng có liên quan cho giao thức này. Giao thức T = 1 là một giao thức khối theo định hướng, có nghĩa là một khối là đơn vị dữ liệu nhỏ nhất có thể được truyền giữa thẻ và thiết bị đầu cuối.

Giao thức này có tách lớp nghiêm ngặt, và nó có thể được giao cho các liên kết dữ liệu (lớp vận chuyển) trong mô hình tham chiếu OSI. Trong bối cảnh này, tách lớp có nghĩa là dữ liệu dành cho các lớp cao hơn, chẳng hạn như các lớp ứng dụng, có thể được xử lý hoàn toàn minh bạch bởi các liên kết dữ liệu. Nó không phải là cần thiết cho các lớp khác so với những người trực tiếp tham gia để giải thích hoặc sửa đổi các nội dung của dữ liệu truyền đi.

Tin nhắn an toàn (SM), đặc biệt đòi hỏi phải tuân thủ tách lớp. Chỉ sau đó dữ liệu người dùng được mã hóa có thể được truyền qua giao diện mà không cần đến các thủ tục phức tạp hoặc thủ đoạn. Giao thức T = 1 hiện nay là chỉ giao thức thẻ thông minh quốc tế cho phép tất cả các loại truyền dữ liệu an toàn mà không có bất kỳ thỏa hiệp.

Trình tự giao thức truyền dẫn bắt đầu sau khi thẻ đã gửi ATR hoặc sau một PPS thành công đã được thực hiện. Khối đầu tiên được gửi đi bởi các thiết bị đầu cuối, và khối tiếp theo là thẻ gửi đến. Thông tin liên lạc sau đó tiếp tục theo cách này, với truyền đặc quyền xen kẽ giữa các thiết bị đầu cuối và các thẻ.

Ngẫu nhiên, giao thức T = 1 không giới hạn được sử dụng để giao tiếp giữa thẻ thông minh và thiết bị đầu cuối. Nó cũng được sử dụng bởi nhiều thiết bị đầu cuối để trao đổi ứng dụng và kiểm soát dữ liệu với các máy tính mà họ được kết nối.

Command	User data	Protocol data	Data transmission time
READ BINARY	C: 5 bytes R: 2 + 8 bytes	C: 4 bytes R: 4 bytes	28.75 ms
UPDATE BINARY	C: 5 + 8 bytes R: 2 bytes	C: 4 bytes R: 4 bytes	23.00 ms
ENCRYPT	C: 5 + 8 bytes R: 2 + 8 bytes	C: 4 bytes R: 4 bytes	38.75 ms

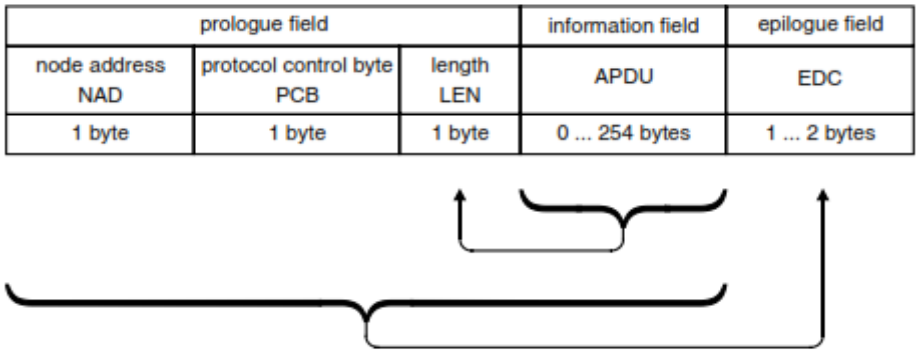
Hình 2.4.2.2.1: Liệt kê các lần truyền cho một số lệnh điển hình bằng cách sử dụng giao thức T = 1.

a) Cấu trúc khối

Các khối truyền về cơ bản được sử dụng cho hai mục đích khác nhau. Một trong số đó là việc truyền tải minh bạch các dữ liệu ứng dụng cụ thể, trong khi người kia đang gửi dữ liệu giao thức điều khiển, xử lý lỗi truyền dẫn.

Một khối truyền tải bao gồm một lĩnh vực mở đầu ban đầu, một lĩnh vực thông tin và lĩnh vực phần kết thúc. Các lĩnh vực phần kết mở đầu và là bắt buộc và phải

luôn luôn được gửi đi. Lĩnh vực thông tin là tùy chọn và chứa dữ liệu cho lớp ứng dụng, đó có thể là một APDU gửi vào thẻ hoặc một APDU phản hồi từ thẻ.



Hình 2.4.2.2.2: Cấu trúc của môt khối truyền T = 1.

Có ba loại cơ bản khác nhau của các khối trong T = 1: khối thông tin, khối xác nhận tiếp nhận và khối hệ thống. Khối thông tin (khối I) được sử dụng để minh bạch trao đổi dữ liệu tầng ứng dụng. Khối thừa nhận biên lai (khối R), không chứa bất kỳ trường dữ liệu, được sử dụng để xác nhận tiếp nhận tích cực hay tiêu cực. Khối hệ thống (khối S) được sử dụng để kiểm soát thông tin liên quan đến giao thức riêng của mình. Tùy thuộc vào dữ liệu kiểm soát cụ thể, họ có thể có một trường thông tin.

Lĩnh vực mở đầu

Lĩnh vực mở đầu bao gồm ba trường con: địa chỉ nút (NAD), giao thức điều khiển byte (PCB) và chiều dài (LEN). Nó dài ba byte và có điều khiển cơ bản và con trỏ dữ liệu cho các khối truyền tải thực tế.

Địa chỉ nút (NAD)

Byte đầu tiên trong lĩnh vực mở đầu được gọi là địa chỉ nút (NAD) byte. Nó chứa các desti quốc gia và địa chỉ nguồn cho khối. Mỗi trong số này được mã hóa sử dụng ba bit. Nếu một địa chỉ không được sử dụng, các bit của nó được thiết lập là 0. Hơn nữa, để tương thích với vi điều khiển lớn hơn, kiểm soát được cung cấp cho các EEPROM hoặc điện áp lập trình PROM. Tuy nhiên, không có sử dụng thực tế cho điều này, vì tất cả các vi điều khiển thẻ thông minh đã có máy phụ trách trên tàu.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	...	...	...	X	...	...	...	Vpp control
...	X	X	X	...	...	...	...	DAD (destination address)
...	...	...	...	...	X	X	X	SAD (source address)

Hình 2.4.2.2.3: Địa chỉ nút (NAD).

Protocol control byte (PCB)

Trường con theo địa chỉ nút là byte điều khiển giao thức (PCB). Như tên gọi, nó phục vụ để kiểm soát và giám sát các giao thức truyền dẫn. Điều này làm tăng số lượng mã hóa cần thiết. Lĩnh vực PCB chủ yếu mã hóa các loại hình khối, cũng như các thông tin bổ sung liên quan.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	…	…	…	…	…	…	…	I block identifier
…	N(S)	…	…	…	…	…	…	Send sequence number
…	…	X	…	…	…	…	…	Sequence data bit M
…	…	…	X	X	X	X	X	Reserved

Hình 2.4.2.2.4: Lĩnh vực PCB cho một khối I

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	0	…	…	…	…	…	…	R block identifier
…	…	0	N(R)	0	0	0	0	No error
…	…	0	N(R)	0	0	0	1	EDC or parity error
…	…	0	N(R)	0	0	1	0	Other error

Hình 2.4.2.2.5:Lĩnh vực PCB cho một khối R.

Lĩnh vực chiều dài (LEN)

Lĩnh vực chiều dài một byte (LEN) cho biết chiều dài của lĩnh vực thông tin ở dạng thập lục phân. Giá trị của nó có thể là '00 'to'FE. Mã 'FF' được dành riêng cho các phần mở rộng trong tương lai và hiện tại không nên được sử dụng.

Lĩnh vực thông tin

Trong một khối I, lĩnh vực thông tin phục vụ như một container cho dữ liệu lớp ứng dụng (OSI lớp 7). Nội dung của trường này được truyền hoàn toàn minh bạch. Điều này có nghĩa là các nội dung trực tiếp thông qua trực tiếp bởi giao thức truyền tải mà không cần bất kỳ phân tích hay đánh giá.

Trong một khối S, lĩnh vực thông tin truyền dữ liệu cho các giao thức truyền tải. Đây là trường hợp duy nhất mà nội dung này của lĩnh vực này được sử dụng bởi tầng giao thông.

Theo tiêu chuẩn ISO, kích thước của lĩnh vực thông tin có thể từ '00 'to'FE (254) byte. Giá trị 'FF' (255) được dành riêng theo tiêu chuẩn ISO để sử dụng trong tương lai. Thiết bị đầu cuối và thẻ có thể có các lĩnh vực I với kích cỡ khác nhau. Kích thước mặc định của lĩnh vực thiết bị đầu cuối I là 32 byte (IFSD = thông tin kích thước trường cho các thiết bị giao diện), điều này có thể được sửa đổi thông qua một lĩnh vực S đặc biệt. Giá trị mặc định của 32 byte cũng áp dụng cho các thẻ (IFSC = thông tin kích thước trường cho các thẻ), nhưng điều này có thể được sửa đổi bởi một tham số trong ATR. Trong thực tế, kích thước của các lĩnh vực I cho cả hai thiết bị đầu cuối và các thẻ là từ 50 đến 254 byte.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	…	…	…	…	…	…	S block identifier
…	…	0	0	0	0	0	0	Resync request (only from terminal)
…	…	1	0	0	0	0	0	Resync response (only from smart card)
…	…	0	0	0	0	0	1	Request change to information field size
…	…	1	0	0	0	0	1	Response to request change to information field size
…	…	0	0	0	0	1	0	Request abort
…	…	1	0	0	0	1	0	Response to abort request
…	…	0	0	0	0	1	1	Request waiting time extension (only from smart card)
…	…	1	0	0	0	1	1	Response to waiting time extension (only from terminal)
…	…	1	0	0	1	0	0	Vpp error response (only from smart card)

Hình 2.4.2.2.6: Lĩnh vực PCB cho một khối S.

Lĩnh vực phần kết

Lĩnh vực phần kết, được truyền vào cuối khối, có chứa một mã phát hiện lỗi tính từ tất cả các byte trước trong khối. Việc tính toán sử dụng hoặc một LCR (longitudinal redundancy check – kiểm tra tính dư lọc) hoặc một CRC (cyclic redundancy check – kiểm tra dư vòng). Phương pháp sử dụng phải được xác định trong các kí tự giao diện của ATR. Nếu nó không được xác định theo quy ước phương pháp LRC là mặc nhiên sử dụng. Nếu không, việc tính toán CRC được thực hiện theo tiêu chuẩn ISO 3309. Đa thức chia sử dụng, $G(x)=x^{16}+x^{12}+x^5+1$, cũng giống như cho CCITT kế hoạch V.41. Cả hai mã phát hiện lỗi chỉ có thể được sử dụng để phát hiện lỗi, họ không thể sửa chữa một lỗi khối.

Kiểm tra tính dư lọc byte đơn dọc dự phòng kiểm tra được tính toán sử dụng XOR nối của tất cả các byte trước trong khối. Tính toán này có thể được thực hiện rất nhanh chóng, và việc thực hiện không phải là mã chuyên sâu. Nó thường được thực hiện trong quá trình truyền dữ liệu hoặc tiếp nhận. Nó là một phần tiêu chuẩn của hầu như tất cả T = 1 hiện thực.

Sử dụng các thủ tục CRC để tạo ra một mã phát hiện lỗi mang lại một khả năng lớn hơn nhiều của việc phát hiện lỗi so với kiểm tra XOR khá nguyên thủy. Tuy nhiên, thủ tục này hiện nay không được sử dụng trong thực tế, kể từ khi kiểm tra XOR đã trở thành tiêu chuẩn được thiết lập trên toàn thế giới. Với các thủ tục CRC, lĩnh vực phần kết phải được mở rộng tới hai byte, mà tiếp tục làm giảm tốc độ truyền dữ liệu.

b) Trình tự truy cập gửi và nhận

Mỗi khối thông tin trong các giao thức T = 1 có một số thứ tự gửi bao gồm chỉ có một chút nằm ở byte PCB. Con số này được tăng lên theo modulo 2, có nghĩa là nó luân phiên giữa 0 và 1. Trình tự truy cập gửi cũng được chỉ định N (S). Giá trị của nó

bắt đầu tại giao thức bắt đầu là 0. Các bộ đếm trong các thiết bị đầu cuối và các thẻ thông minh đang tăng lên độc lập với nhau.

Mục đích chính của trình tự truy cập gửi là để hỗ trợ các yêu cầu gửi lại các khối nhận được có lỗi, kể từ khi khối dữ liệu cá nhân có thể được giải quyết một cách rõ ràng thông qua N (S).

c) Thời gian chờ

Nhiều thời gian chờ đợi được xác định để cung cấp thiết bị phát và thu với mức tối thiểu quy định một cách chính xác và khoảng thời gian tối đa cho các hoạt động khác nhau trong quá trình truyền dữ liệu. Họ cũng cung cấp cách xác định chấm dứt truyền thông để ngăn chặn sự bế tắc trong trường hợp lỗi. Giá trị mặc định được định nghĩa cho tất cả các thời gian chờ đợi trong tiêu chuẩn, nhưng có thể được sửa đổi để tối đa hóa tốc độ truyền tải. Các giá trị sửa đổi được chỉ định trong các nhân vật giao diện cụ thể của ATR.

Thời gian chờ đợi ký tự (CWT)

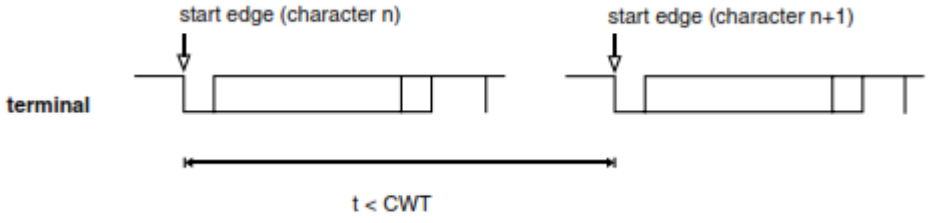
Thời gian chờ đợi ký tự được định nghĩa là khoảng thời gian tối đa giữa các cạnh hàng đầu của hai ký tự liên tiếp trong một khối. Người nhận bắt đầu một đồng hồ đếm ngược trên mỗi cạnh hàng đầu, bằng cách sử dụng thời gian chờ đợi ký tự như giá trị ban đầu. Nếu bộ đếm thời gian hết hạn và không có cạnh hàng đầu cho một bit mới đã được phát hiện, người nhận giả định rằng các khối truyền tải đã được nhận đầy đủ. "CWT tiếp nhận tiêu chuẩn" như vậy có thể được thường được sử dụng để phát hiện điểm cuối cùng của khối. Tuy nhiên, điều này làm giảm đáng kể tốc độ truyền dữ liệu, kể từ thời điểm cho mỗi khối được tăng thời hạn của CWT. Vì thế, tốt hơn để phát hiện điểm cuối của khối bằng cách đếm byte nhận được.

Các CWT được tính toán bằng cách sử dụng phần tử dữ liệu CWI chứa trong ATR, theo công thức sau:

$$CWT = (2^{CW} + 11) \text{ work etu}$$

Giá trị mặc định cho CWI là 13, trong đó sản lượng các giá trị sau cho CWT:

$$CWT = (2^{13} + 11) \text{ work etu} = 8203 \text{ work etu}$$



Hình 2.4.2.2.7: Định nghĩa về thời gian chờ đợi ký tự (CWT).

Với một tần số đồng hồ của 3,5712 MHz và một giá trị chia 372, điều này mang lại một khoảng thời gian 0,85 giây.

Khoảng thời gian này, được quy định trong các tiêu chuẩn như các thiết lập mặc định, quá dài để truyền dữ liệu nhanh. Trong thực tế, giá trị thông thường của CWI là

giữa 3 và 5. Điều này có nghĩa rằng đối với một trình tự phát bình thường, trong đó các kí tự theo nhau mà không cần bất kỳ sự chậm trễ thời gian, người nhận chờ đợi một khoảng thời gian 1-2 byte trước khi phát hiện sự kết thúc của khối hoặc gián đoạn thông tin liên lạc.

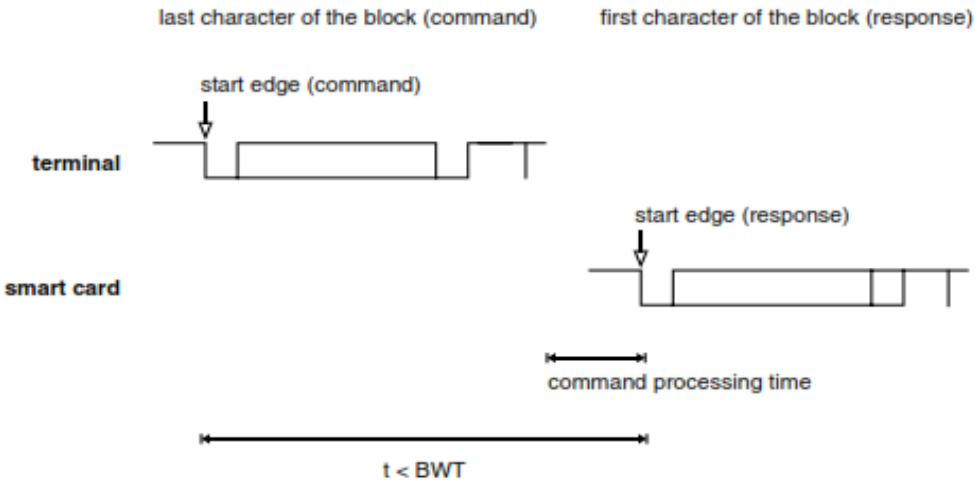
Thông thường, các thói quen tiếp nhận phát hiện phần cuối của một khối từ các thông tin chiều dài khối trong lĩnh vực LEN. Tuy nhiên, nếu nội dung của lĩnh vực này là sai lầm, thời gian chờ đợi nhân vật có thể được sử dụng như một phương tiện bổ sung để chấm dứt tiếp nhận. Vấn đề này chỉ thể hiện khi thông tin dài quá lâu, vì trong trường hợp này người nhận sẽ chờ đợi cho các ký tự bổ sung mà không bao giờ đến. Điều này sẽ ngăn chặn các giao thức truyền dẫn, và tình trạng này chỉ có thể được xóa bởi một thẻ thiết lập lại. Kí tự chờ đợi cơ chế thời gian nhận được xung quanh vấn đề này.

Thời gian chờ đợi khối (BWT)

Mục đích của các khối thời gian chờ đợi là để cho phép truyền thông phải được chấm dứt một cách xác định nếu các thẻ thông minh không trả lời. Khối thời gian chờ đợi là khoảng thời gian tối đa cho phép giữa các cạnh hàng đầu của byte cuối cùng của một khối gửi vào thẻ và cạnh hàng đầu của các byte đầu tiên được trả về bởi thẻ.

Trong điều khoản của một khối thông thường T = 1, đây là khoảng thời gian tối đa cho phép giữa các cạnh hàng đầu của các byte XOR trong lĩnh vực kết của khối lệnh và cạnh hàng đầu của các byte NAD trong phản hồi từ thẻ. Nếu thời gian chờ đợi này hết hạn mà không có một phản ứng được nhận từ thẻ, thiết bị đầu cuối có thể giả định rằng thẻ bị lỗi và bắt đầu một phản ứng thích hợp. Điều này có thể ví dụ như là một thiết lập lại thẻ, theo sau là một nỗ lực mới để thiết lập truyền thông. Các BWT được quy định trong dạng viết tắt trong các nhân vật giao diện của ATR bởi tham số BWI. Giá trị của BWT được cho bởi công thức:

$$BWT = 2^{BWI} \times 960 \times \frac{372}{f} \text{ s} + \text{work etu}$$



Hình 2.4.2.2.8: Định nghĩa của thời gian chờ đợi khối (BWT).

Nếu không có giá trị BWI được đưa ra trong ATR, giá trị mặc định của 4 được sử dụng. Với 3,5712 MHz và một giá trị chia 372, điều này sẽ cho 1,6 s như giá trị cho các khối thời gian chờ đợi:

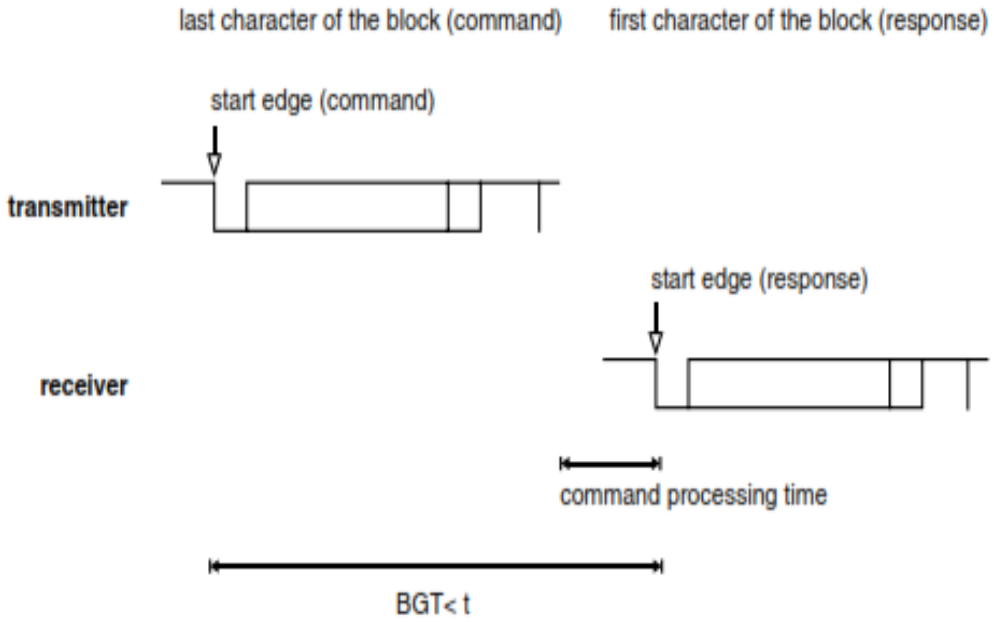
$$BWT = 2^4 \times 960 \times \frac{372}{3{,}571{,}200\ \text{Hz}}\ \text{s} + 11\ \text{work etu} = 2^4 \times 0.1\text{s} + 11\ \text{work etu} \approx 1.6\text{s}$$

Như có thể thấy, giá trị này là khá hào phóng. Trên thực tế, giá trị của 3 thường được sử dụng cho BWI, trong đó sản lượng một khối thời gian 0,8 s chờ đợi. Thời gian xử lý lệnh điển hình trong thẻ thường khoảng 0,2 s. Một BWT thời hạn trên do đó đại diện cho một sự thỏa hiệp giữa thời gian xử lý lệnh bình thường và phát hiện nhanh chóng của một thẻ thông minh được không còn đáp ứng với các lệnh.

Khối bảo vệ thời gian (BGT)

Thời gian bảo vệ khối được định nghĩa là khoảng cách tối thiểu giữa các cạnh hàng đầu của byte cuối cùng và các cạnh hàng đầu của byte đầu tiên theo hướng ngược lại. Nó là đối lập với BWT, được định nghĩa là thời gian tối đa giữa hai mép định. Một khác biệt nữa là thời gian bảo vệ khối là bắt buộc đối với cả hai bên và phải được quan sát, trong khi khối thời gian chờ đợi chỉ có ý nghĩa cho các thẻ thông minh. Mục đích của thời gian bảo vệ khối là cung cấp cho người gửi với một khoảng thời gian tối thiểu, trong đó để chuyển qua từ truyền tới nhận.

Thời gian bảo vệ khối có một giá trị cố định tiêu chuẩn của 22 etu. Trong một thẻ thông minh chạy ở 3,5712 MHz với một giá trị chia 372, điều này mang lại một khoảng thời gian khoảng 2,3 ms.



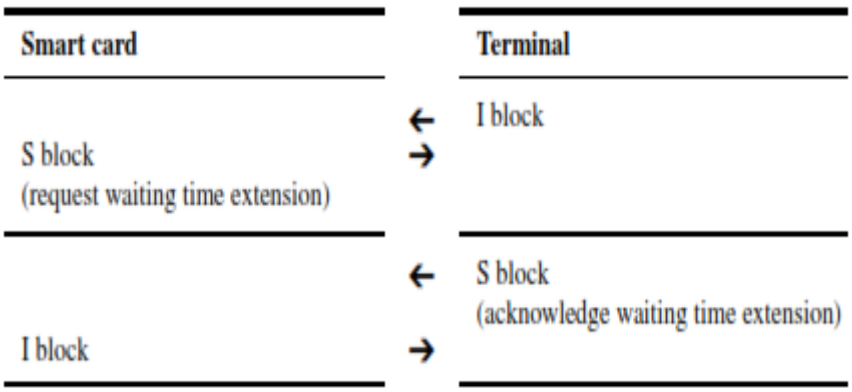
Hình 2.4.2.2.9: Định nghĩa của thời gian bảo vệ khối (BGT).

d) Cơ chế giao thức truyền dẫn

Chờ đợi thời gian mở rộng

Nếu thẻ thông minh cần thêm thời gian để tạo ra một phản ứng hơn so với thời gian tối đa cho phép của khối thời gian (BWT) chờ đợi, nó có thể yêu cầu gia hạn thời gian chờ đợi từ các thiết bị đầu cuối. Nó như vậy bằng cách gửi một khối S đặc biệt yêu cầu một phần mở rộng, và nó nhận được một khối S tương ứng từ thiết bị đầu cuối trong sự thừa nhận. Thiết bị đầu cuối không được phép từ chối yêu cầu này.

Một byte trong lĩnh vực thông tin thông báo cho thiết bị đầu cuối của chiều dài của phần mở rộng. Byte này, nhân với thời gian chờ đợi khối, cung cấp cho một khối mới thời gian chờ đợi.



Hình 2.4.2.2.10: Thủ tục gia hạn thời gian chờ đợi.

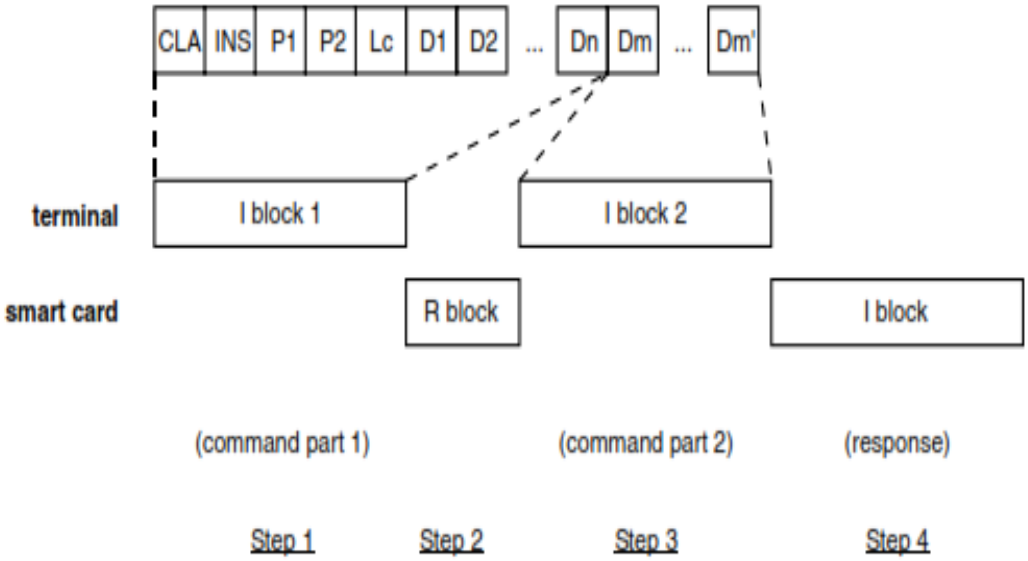
Chuỗi khối

Một trong những tính năng hiệu suất cần thiết của giao thức T = 1 là chức năng chuỗi khối. Điều này cho phép một trong hai bên để gửi khối dữ liệu có dung lượng lớn hơn so với kích thước của truyền hoặc nhận được bộ đệm. Điều này đặc biệt hữu ích trong ánh sáng của dung lượng bộ nhớ hạn chế của thẻ thông minh. Chuỗi chỉ được phép cho các khối thông tin, vì chỉ có khối như vậy có thể chứa một lượng lớn dữ liệu. Trong quá trình xâu chuỗi, dữ liệu ứng dụng được phân chia thành các khối cá nhân được gửi đến một người nhận sau khi khác.

Các dữ liệu lớp ứng dụng phải được phân chia như vậy mà không có kết quả là phân đoạn lớn hơn so với kích thước khối tối đa của người nhận. Các phân đoạn đầu tiên sau đó được đặt trong một lĩnh vực thông tin phù hợp với giao thức T = 1, cung cấp với đoạn mở đầu và phần kết các lĩnh vực và gửi đến người nhận. Các bit M (bit 'hơn dữ liệu ") được thiết lập trong lĩnh vực PCB của khối để chỉ ra cho người nhận rằng các chức năng chuỗi khối đang được sử dụng và dữ liệu xích nằm trong các khối sau.

Ngay sau khi người nhận đã thành công nhận được khối thông tin này với các phân đoạn đầu tiên của dữ liệu người dùng, nó chỉ ra rằng nó đã sẵn sàng để nhận được xích tiếp theo khóa I bằng cách trả lại một khối R có số thứ tự N (R) là giống như gửi chuỗi số N (S) của tôi khối tiếp theo. Khối tiếp theo sau đó được gửi cho người nhận.

Này trao đổi hỗ tương của khối I và R tiếp tục cho đến khi các vấn đề người gửi một khối với một chút M trong lĩnh vực PCB chỉ ra rằng nó là khối cuối cùng trong chuỗi I(M bit = 0). Sau khi khối này đã được nhận, người nhận có tất cả các dữ liệu lớp ứng dụng và có thể xử lý các khối dữ liệu đầy đủ.



Hình 2.4.2.2.11: Ví dụ về khối chuỗi để truyền dữ liệu từ các thiết bị đầu cuối tới các thẻ thông minh.

Xử lý lỗi

Giao thức T = 1 có phát hiện lỗi và xây dựng các cơ chế xử lý. Nếu một khối không hợp lệ được nhận, giao thức cố gắng để khôi phục thông tin liên lạc lỗi bằng cách thủ tục xác định chính xác.

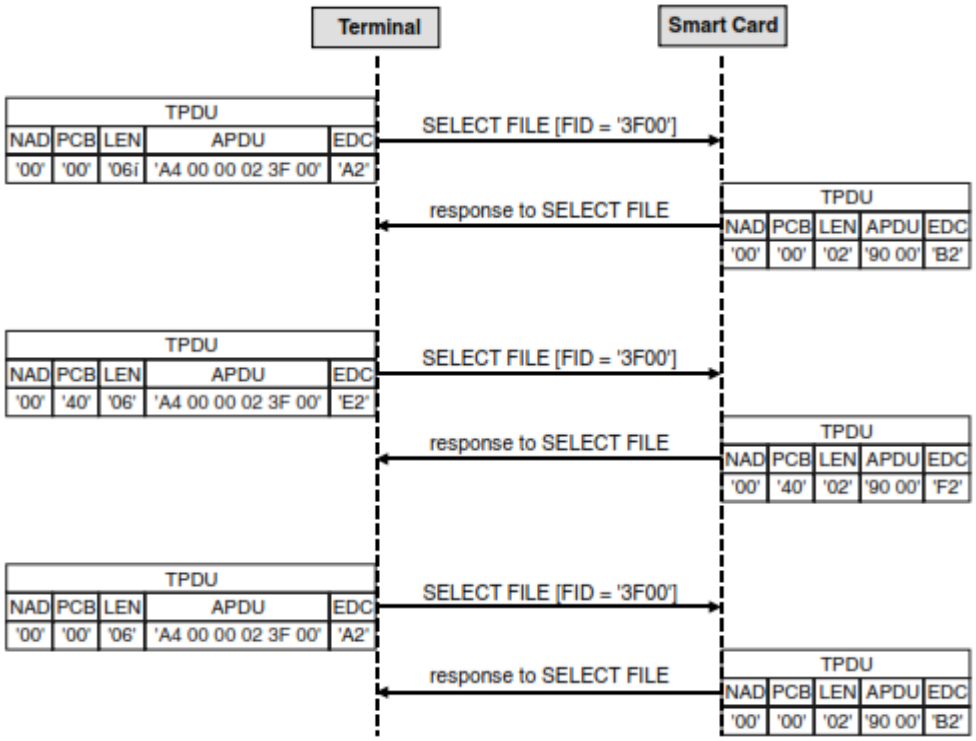
Nhìn từ quan điểm của thiết bị đầu cuối, có ba giai đoạn đồng bộ hóa. Trong giai đoạn đầu tiên, người gửi của một khối bị lỗi nhận được một khối R chỉ ra một EDC/lỗi bit chẵn lẻ hoặc một lỗi chung. Sau đó người nhận của khối R này (người gửi ban đầu) phải truyền lại khối cuối cùng mà nó gửi.

Synchronization stage	Mechanism
Stage 1	Repeat the erroneous block
Stage 2	Resynchronize and then repeat the erroneous block
Stage 3	Reset the smart card and establish the connection anew

Hình 2.4.2.2.12: Giai đoạn xử lý lỗi T = 1.

e) Sự khác nhau giữa ISO / IEC T = 1 và EMV T = 1

Định nghĩa ban đầu của giao thức T = 1 theo tiêu chuẩn ISO/IEC 7816-3 có quy định cho nhiều lựa chọn và cơ chế, một số trong đó là mã chuyên sâu và hiếm khi sử dụng.



Hình 2.4.2.2.13: Giao thức truyền dữ liệu với T = 1.

2.4.3 Giao thức truyền dữ liệu với T = 14

Tiêu chuẩn 7816-3 ISO/IEC bao gồm một thẻ trong ATR cho việc thiết kế một giao thức truyền tải quốc gia. Một giao thức truyền dẫn như vậy được chỉ định T = 14. Với sự ra đời của C-Netz cho điện thoại và thẻ điện thoại di động ở Đức, một giao thức là cần thiết để giao tiếp với các thẻ thông minh được sử dụng trong các hệ thống này. Các ký tự theo định hướng T = 0 giao thức được coi là không mong muốn, và tại thời điểm đó vẫn không có một khối tiêu chuẩn giao thức định hướng. Do đó, vào năm 1987 Telekom quyết định sử dụng một giao thức được phát triển bởi một nhóm làm việc DIN. Giao thức này đã nhận được sự chỉ định T = 14, mà chỉ đơn giản có nghĩa là nó là một thực hiện quốc gia cụ thể. Nó không có ý nghĩa bên ngoài của Đức, nhưng nó đã có ảnh hưởng to lớn đối với sự phát triển của các tiêu chuẩn quốc tế T = 1 giao thức, kể từ khi có giao thức T = 14 hình thành nền tảng chính cho các giao thức này.

Mechanism or option	ISO/IEC 7816-3	EMV
BWT expired	Reset the card (for example)	Deactivate the card
Smart card sends a request to change the IFS	Allowed	A maximum of three successive requests is allowed
Smart card sends an S block with an abort request	Allowed	Deactivate the card
Zero-length I block	Allowed	Prohibited
Terminal sends three successive blocks without receiving a valid response	Behavior according to specified error handling; usually a resync request	Deactivate the card

Hình 2.4.3.1: Tóm tắt các sự khác biệt trong việc thực hiện của giao thức T=1 truyền dẫn giữa các tiêu chuẩn ISO / IEC 7816-3 và đặc tả EMV.

Giao thức T = 14 được sử dụng rất rộng rãi ở Đức, vì nó đã được sử dụng trong các mạng viễn thông C-Netz điện thoại di động và điện thoại thẻ công cộng. Với việc đóng cửa của C-Netz vào cuối năm 2000 và thay đổi đối với giao thức T = 1 cho điện thoại thẻ công cộng, giao thức T = 14 không còn là một giao thức quan trọng ở Đức, đó là lý do tại sao nó được mô tả ở đây chỉ một thời gian ngắn.

Giao thức T = 14 có cấu trúc khối theo định hướng và hoạt động không đồng bộ bằng cách sử dụng tín hiệu đồng hồ được áp dụng. Bộ chia (đồng hồ tốc độ chuyển đổi) có giá trị là 512, trong đó sản lượng dữ liệu tốc độ truyền của 9.600 bit/s ở một tần số đồng hồ của 4,9512 MHz. Truyền dữ liệu ở lớp 2 (lớp liên kết dữ liệu) luôn luôn diễn ra theo quy ước trực tiếp. Kích thước của bộ đệm cho các khối truyền và nhận phải có ít nhất 50 byte, với một giá trị tối đa 255 byte. Không có cơ chế chuỗi khối.

2.4.4 Giao thức truyền tải USB

Một sửa đổi trong tương lai theo tiêu chuẩn ISO/IEC 7816-3 sẽ có một đặc điểm kỹ thuật cho một giao thức truyền tải mới cho thẻ thông minh. Đây là giao thức Universal Serial Bus (USB), mà đã đến để chiếm ưu thế hơn các giao thức cạnh tranh, chẳng hạn như Firewire và các loại tương đương, để sử dụng với các ứng dụng thẻ thông minh.

Các giao thức USB đòi hỏi một thành phần phần cứng đặc biệt trong các vi điều khiển thẻ thông minh, nhưng thành phần này đã có mặt trong nhiều chips, ít nhất là một lựa chọn. Ưu điểm chính của USB đối với các giao thức truyền tải hiện đang được sử dụng với nó là một tiêu chuẩn công nghiệp thành lập đến từ thế giới máy tính. USB cũng cung cấp tốc độ truyền tải cao hơn so với T = 0 hay T = 1.

Hiện nay dường như phiên bản 1.1 của đặc tả USB sẽ được sử dụng cho thẻ thông minh, với cả hai tùy chọn tốc độ thấp (1,5 Mbit/s) và các tùy chọn tốc độ đầy đủ

(12 Mbit/s) được hỗ trợ, tùy thuộc vào loại vi điều khiển. Cần lưu ý rằng tốc độ truyền tải hiệu quả là thấp hơn đáng kể so với giá trị ghi một khi dữ liệu giao thức cần thiết đã được trừ. Phiên bản USB 2.0, trong đó có một tốc độ truyền tải dữ liệu lên đến 480 Mbit/s (ở chế độ tốc độ cao), sẽ không được sử dụng trong tương lai gần.

2.5 Cấu trúc thông điệp: APDUs

Các ứng dụng giao thức đơn vị dữ liệu (APDUs) được sử dụng để trao đổi tất cả các dữ liệu chuyển giữa các thẻ thông minh và các thiết bị đầu cuối. Các APDU là một đơn vị dữ liệu tiêu chuẩn quốc tế cho các lớp ứng dụng, đó là lớp 7 trong mô hình OSI. Trong thẻ thông minh, lớp này nằm ngay phía trên tầng giao thức truyền dẫn. Các đơn vị dữ liệu giao thức phụ thuộc vào các lớp giao thức truyền dẫn được gọi là "giao thức truyền dẫn các đơn vị dữ liệu" (TPDUs).

Một sự phân biệt giữa lệnh APDUs (C-APDUs), đại diện cho các lệnh đến thẻ, và APDUs phản ứng (R-APDUs), đại diện trả lời cho các lệnh này từ thẻ. Trong thuật ngữ đơn giản, một APDU là một loại container chứa một lệnh hoàn thành vào thẻ hoặc đáp ứng hoàn toàn từ thẻ. APDUs được thông qua các giao thức truyền tải minh bạch, có nghĩa là không có sửa đổi hoặc giải thích.

APDUs mà thực hiện theo tiêu chuẩn ISO/IEC 7816-4 được dùng để không phụ thuộc vào giao thức truyền dẫn. Do đó, nội dung và định dạng của một APDU không phải thay đổi khi một giao thức truyền dẫn khác nhau được sử dụng. Áp dụng cho tất cả với hai giao thức tiêu chuẩn, T = 0, T = 1. Nhu cầu này độc lập giao thức ảnh hưởng đến cấu trúc của APDUs, vì nó phải có khả năng truyền tải chúng minh bạch sử dụng cả các byte theo định hướng giao thức T = 0 và khối hướng T = 1 giao thức.

2.6 An toàn truyền dữ liệu

Toàn bộ trao đổi dữ liệu giữa các thiết bị đầu cuối và một thẻ thông minh sử dụng xung điện kỹ thuật số trên các dòng của thẻ thông minh I/O. Có thể hiểu được và không có kỹ thuật khó khăn để hàn một sợi dây tới liên lạc I/O, ghi lại tất cả các thông tin liên lạc cho một phiên và sau đó phân tích chúng. Bằng cách này, nó có thể đạt được kiến thức của tất cả các dữ liệu được truyền theo cả hai hướng.

Một nhiệm vụ có phần khó khăn hơn là để cô lập liên lạc I/O, gắn kết một số liên lạc giả trên đầu trang của nó, và sau đó sử dụng sợi dây mỏng để kết nối cả hai địa chỉ liên lạc với một máy tính. Với sự sắp xếp này, nó rất dễ dàng để cho phép chỉ một số lệnh để đạt được thẻ hoặc chèn lệnh 'nước ngoài' vào chuỗi thông tin liên lạc.

Cả hai loại điển hình của cuộc tấn công có thể thành công chỉ khi dữ liệu bí mật đi không được bảo vệ trên đường I/O. Truyền dữ liệu nên do đó về cơ bản được thiết

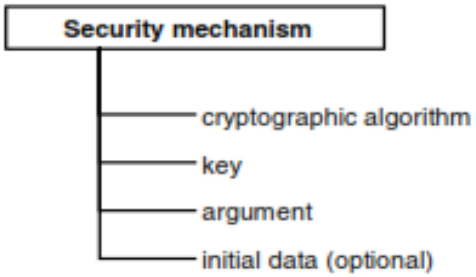
kế như vậy mà ngay cả khi một kẻ tấn công có thể nghe trộm trên truyền dữ liệu và chèn khối thông điệp của mình.

Có những cơ chế khác nhau và phương pháp có thể được sử dụng để bảo vệ chống lại các cuộc tấn công và chống lại các loại tấn công thậm chí phức tạp hơn. Chúng được gọi chung là 'tin nhắn an toàn. Các cơ chế này không cụ thể cho thẻ thông minh, và họ đã được sử dụng trong một thời gian dài trong các hệ thống truyền thông dữ liệu. Là những gì đặc biệt trong lĩnh vực thẻ thông minh là không công suất chế biến của các bên giao tiếp cũng như tốc độ truyền là đặc biệt lớn. Do đó, thường được sử dụng phương pháp tiêu chuẩn đã được thu nhỏ lại để phù hợp với khả năng của thẻ thông minh, không có trong bất kỳ cách nào làm giảm sự an toàn của những phương pháp.

Mục tiêu của tin nhắn là an toàn để đảm bảo tính xác thực, và nếu cần thiết bảo mật, một phần hoặc tất cả các dữ liệu được truyền. Một loạt các cơ chế bảo mật được sử dụng để đáp ứng mục tiêu này. Một cơ chế bảo mật được định nghĩa là một chức năng đòi hỏi phải có các mục sau đây: một thuật toán mã hóa, một chìa khóa, một đối số và dữ liệu ban đầu khi cần thiết. Một điều kiện chung cũng phải được hài lòng, đó là tất cả các cơ chế bảo mật phải cư xử hoàn toàn minh bạch đối với các lớp giao thức hiện tại với, để đảm bảo rằng, các thủ tục tiêu chuẩn hiện hành không bị ảnh hưởng bởi tin nhắn an toàn. Điều này đặc biệt với hai giao thức truyền T = 0, T = 1, cũng như thường được sử dụng các lệnh thông minh tiêu chuẩn.

Trước khi sử dụng một phương pháp tin nhắn an toàn, cả hai bên phải đồng ý trên các thuật toán mật mã được sử dụng và một khóa bí mật chung. Theo nguyên tắc của Kerckhoff, sự an toàn của phương pháp này phụ thuộc hoàn toàn vào quan trọng này. Nếu nó được tiết lộ, tin nhắn an toàn được giảm xuống thường được biết đến là làm giảm tốc độ truyền tải dữ liệu hiệu quả và tốt nhất có thể được sử dụng để sửa lỗi truyền dẫn.

Một số loại phương pháp khác nhau tin nhắn an toàn đã được biết đến trong nhiều năm. Tất cả chúng đều khá khắt khe và phù hợp với các ứng dụng cụ thể. Hầu hết trong số chúng không thể bị coi là lỗi liên quan đến an ninh. Tuy nhiên, không ai trong số chúng chiếm ưu thế được trên quốc tế hoặc đã được chứng minh là đủ linh hoạt để được bao gồm trong các tiêu chuẩn hiện hành.



Hình 2.6.1: Các dữ liệu và các chức năng cần thiết cho một cơ chế bảo mật.

Các yêu cầu về tính minh bạch đối với các lệnh hiện có, sử dụng với hai giao thức truyền dẫn cơ bản khác nhau và khả năng thích ứng tối đa đã dẫn đến sự tiêu chuẩn hóa của một (và tương ứng phức tạp và tỉ mỉ) phương pháp tin nhắn an toàn rất linh hoạt trong tiêu chuẩn ISO/IEC 7816-4, với chức năng liên quan khác theo quy định tại tiêu chuẩn ISO/IEC 7816-8. Phương pháp này dựa trên nhúng tất cả các dữ liệu người dùng trong đối tượng dữ liệu mã TLV. Ba loại đối tượng dữ liệu khác nhau được định nghĩa:

- data objects for plaintext: chứa dữ liệu trong bản rõ (ví dụ, phần dữ liệu của một APDU)
- data objects for security mechanisms: chứa các kết quả của một cơ chế bảo mật (ví dụ, một MAC)
- data objects for auxiliary functions: chứa dữ liệu điều khiển để nhắn tin an toàn (ví dụ, phương pháp sử dụng đệm)

Lớp byte cho biết có tin nhắn an toàn được sử dụng cho các lệnh. Hai byte có sẵn có thể mã hóa cho dù phương pháp quy định trong tiêu chuẩn ISO / IEC 7816-4 được sử dụng và có tiêu đề cũng được bao gồm trong kiểm tra mật mã (CCS). Nếu các tiêu đề được bao gồm trong tính toán, nó là xác thực, vì nó không thể thay đổi trong quá trình truyền không có điều này là hiển nhiên.

Đối tượng dữ liệu bản rõ (data objects for plaintext)

Theo tiêu chuẩn, tất cả các dữ liệu mà không phải là mã hóa BER-TLV phải được đóng gói, có nghĩa là họ phải được nhúng vào trong đối tượng dữ liệu. Nhiều thẻ khác nhau được sử dụng. Bit 1 của mỗi thẻ chỉ ra cho dù các đối tượng dữ liệu được bao gồm trong các tính toán của các kiểm tra mật mã. Nếu bit này không được thiết lập (ví dụ, 'B0), các đối tượng dữ liệu không nằm trong tính toán, trong khi nếu nó được thiết lập (ví dụ,' B1 '), bao gồm các đối tượng dữ liệu.

Tag	Meaning
'B0', 'B1'	BER-TLV coded; contains data objects related to secure messaging
'B2', 'B3'	BER-TLV coded; contains data objects not related to secure messaging
'80', '81'	No BER-TLV coded data
'99'	State information for secure messaging

Hình 2.6.2: Từ khoá cho các dữ liệu bản rõ.

Đối tượng dữ liệu cho cơ chế bảo mật (Data objects for security mechanisms)

Các đối tượng dữ liệu được sử dụng cho cơ chế bảo mật được chia thành những người sử dụng để xác thực và những người sử dụng để bảo mật.

Đây là "xác thực" đề cập đến tất cả các đối tượng dữ liệu liên quan đến kiểm tra mã hóa và chữ ký số. Mã hóa dữ liệu, và đánh dấu dữ liệu như mã hóa trong bối cảnh

của tin nhắn an toàn, thuộc nhóm của 'bí mật'. Các thẻ được liệt kê trong bảng trên phải được sử dụng để nhắn tin an toàn theo kiểu của phương pháp sử dụng.

Đối tượng dữ liệu cho các chức năng phụ trợ (Data objects for auxiliary functions)

Các đối tượng dữ liệu cho các chức năng phụ trợ được sử dụng trong tin nhắn an toàn phối hợp những khó khăn chung. Hai bên sử dụng các đối tượng dữ liệu để trao đổi thông tin về các thuật toán mã hóa và các phím được sử dụng, dữ liệu ban đầu và thông tin cơ bản tương tự. Về nguyên tắc, các mặt hàng này có thể khác nhau đối với từng truyền APDU, hoặc thậm chí giữa các lệnh và phản hồi của nó. Tuy nhiên, trong thực tế chức năng phụ trợ đối tượng dữ liệu ít được sử dụng, vì tất cả các hạn chế chung cho các tin nhắn an toàn được định nghĩa ngầm, vì vậy họ không cần phải được xác định cụ thể trong thông tin liên lạc.

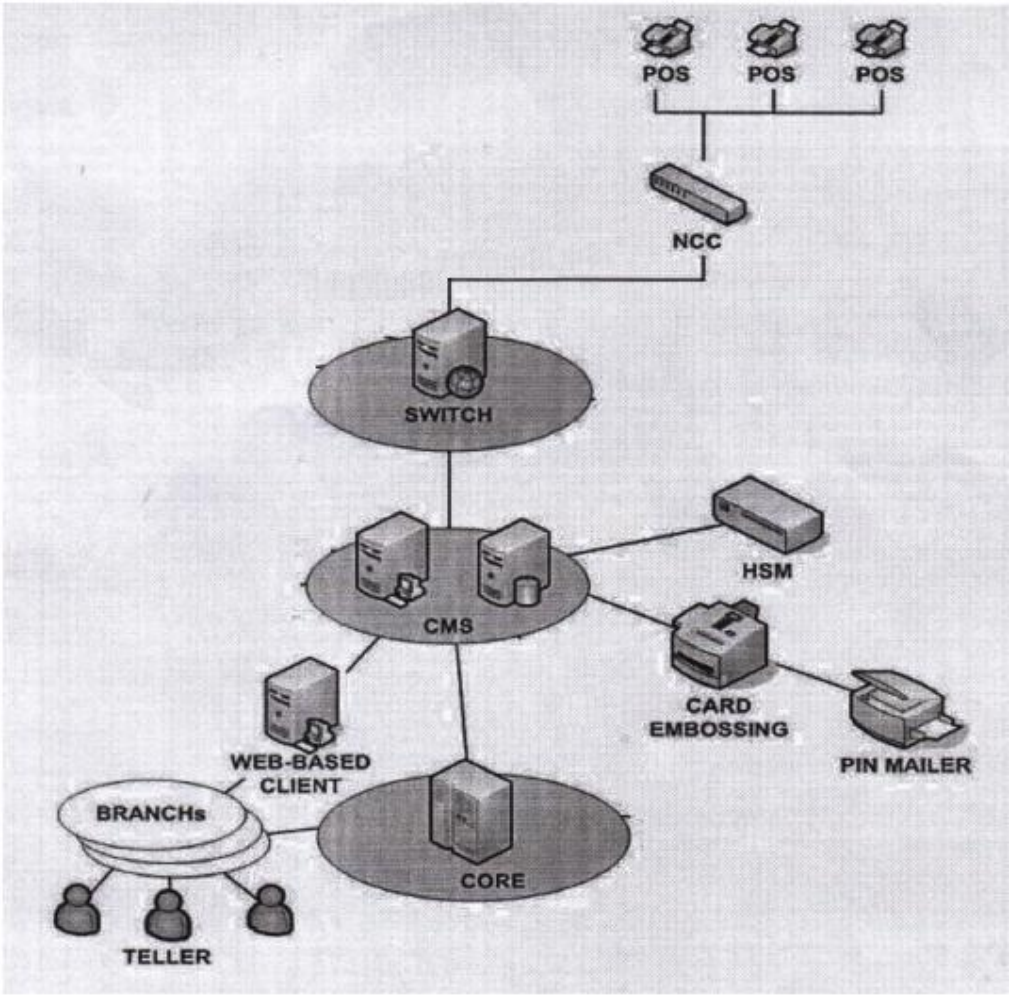
Dựa trên các tùy chọn để nhắn tin an toàn quy định trong tiêu chuẩn ISO/IEC 7816-4, đã được đưa ra chỉ một thời gian ngắn ở trên, chúng ta có thể mô tả hai thủ tục cơ bản. Chúng tôi đã giữ những mô tả đơn giản nhất có thể để làm cho nó hiểu được dễ dàng hơn cơ chế phức tạp có liên quan. Do mức độ cao của tính linh hoạt được cung cấp bởi các tiêu chuẩn, có rất nhiều sự kết hợp khác có thể có cơ chế bảo mật, một số trong đó thậm chí còn phức tạp hơn. Hai thủ tục mô tả ở đây đại diện cho một sự thỏa hiệp giữa sự đơn giản và bảo mật.

Thủ tục của “chế độ xác thực” sử dụng một tổng kiểm tra mật mã (CCS hoặc MAC) để bảo vệ các dữ liệu ứng dụng (APDU) chống lại các thao tác trong quá trình truyền. Thủ tục của các “chế độ kết hợp”, ngược lại, được sử dụng để hoàn toàn mã hóa dữ liệu ứng dụng, do đó, một kẻ tấn công không thể rút ra bất kỳ kết luận về nội dung dữ liệu của các lệnh và đáp ứng được trao đổi. Một trình tự truy cập gửi chỉ được sử dụng với một trong hai thủ tục này. Truy cập này, có giá trị ban đầu là một số ngẫu nhiên, được tăng lên cho mỗi lệnh và mỗi câu trả lời. Điều này cho phép cả hai bên để xác định xem một lệnh hoặc phản ứng đã được bỏ qua hoặc chèn vào. Khi một chuỗi truy cập gửi được sử dụng kết hợp với các thủ tục của các kết hợp chế độ ', APDUs giống hệt nhau xuất hiện là khác nhau. Điều này được gọi là "đa dạng".

Chương 3: MÔ TẢ HỆ THỐNG POS THỬ NGHIỆM TẠI CÁC ĐIỂM BÁN LẺ

3.1 Giới thiệu hệ thống

Đây là một số kết quả và tư liệu về hệ thống POS được triển khai thực tế tại ngân hàng Vietcombank.



3.2 Các thành phần hệ thống

3.2.1 Thiết bị POS

Thiết bị có một đầu đọc thẻ từ cho phép đọc các thông tin từ track 1 và track 2 của thẻ để lấy các thông tin về khách hang.

Các thể chia làm 3 loại:

- Kết nối qua Dial-up: POS kết nối và gửi dữ liệu tới NCC thông qua đường điện thoại.
- Kết nối qua LAN: POS được gán một địa chỉ IP, kết nối và gửi dữ liệu trực tiếp tới NCC thông qua đường mạng LAN.

- Kết nối không dây- wireless: POS kết nối và gửi dữ liệu tới một gateway thông qua tín hiệu không dây (GSM, GPRS,….), sau đó dữ liệu sẽ được gửi từ gateway tới NCC thông qua kết nối *Dial-up*.

Sau khi khách hàng quẹt thẻ và lựa chọn giao dịch, thông tin về khách hàng và giao dịch sẽ được mã hóa bằng một master-key trước khi gửi lên SWITCH.

Thuật toán được dùng để mã hóa là triple-DES.

Master-key lưu trên POS phải giống với master khai báo trên SWITCH.

3.2.2 Hệ thống chuyển mạch (SWITCH)

Các nhiệm vụ chính của SWITCH.

Xác định đường đi của Message trong hệ thống.

Quản lý các thông tin về POS (terminal ID, terminal IP, merchant ID…).

Giám sát các giao dịch.

Cung cấp các báo cáo của tất cả các giao dịch.

Khi SWITCH nhận được thông điệp từ POS, SWITCH sẽ xác định đây là thẻ On-us (thẻ ngân hàng hay của liên minh ngân có POS) hay Off-us (thẻ của ngân hàng khác không có trong lien minh ngân hàng có POS) dựa trên số BIN (bank identify number) của ngân hàng. Nếu là thẻ On-us, SWITCH sẽ đẩy vào CMS để xử lý. Nếu là thẻ Off-us, hệ thống sẽ đẩy sang SWITCH của ngân hàng hay liên minh thẻ tương ứng.

Tất cả các giao dịch đi qua SWITCH sẽ được lưu lại thông tin của cơ sở dữ liệu và sau đó xuất ra báo cáo.

Thông tin trước khi gửi đến CMS cũng được mã hóa bằng một Master-key khác đã thỏa thuận với *master-key* của CMS.

Đi kèm với SWITCH có hệ thống Monitor cho phép người quản trị theo dõi các giao dịch đi qua SWITCH.

3.2.3 Hệ thống quản lý thẻ (CMS)

Các nhiệm vụ chính của hệ thống quản lý thẻ:

Quản lý tất cả các thông tin có liên quan đến thẻ (thông tin khách hàng, số tài khoản gắn với thẻ, tình trạng thẻ,….).

Quản lý quá trình phát hành thẻ, hủy thẻ, thiết lập hạn mức cho thẻ, tạo PIN mới.

Giám sát các giao dịch.

Cung cấp các báo cáo liên quan đến thẻ.

Để có thể phát hành thẻ, CMS được kết nối với một thiết bị khác như: thiết bị tạo và kiểm tra PIN: HSM (Hardware Sercuriry Machine), máy dập thẻ (card embossing), máy in PIN (PIN mailer).

Khi nhận được thông điệp từ hệ thống chuyển mạch, hệ thống quản lý thẻ kiểm tra ngày hết hạn của thẻ và gửi *PIN_Bloack* vào thiết bị an ninh để kiểm tra. Nếu PIN

đúng, hệ thống quản lý thẻ sẽ xác định số tài khoản tương ứng với thẻ và tạo thông điệp gửi vào CORE để xử lý.

Ngoài ra. CMS còn một module Online Monitor cho phép giám sát các giao dịch trên từng thẻ.

3.2.4 Hệ thống lõi (CORE)

Hệ thống lõi của ngân hàng, xử lý tất cả các giao dịch liên quan tới nghiệp vụ của ngân hàng. Sau khi nhận thông điệp từ hệ thống quản lý thẻ, hệ thống CORE sẽ xác định loại giao dịch, tài khoản của khách hàng, tài khoản của đại lý đặt POS, số tiền giao dịch, số tiền phí…., kiểm tra số dư tài khoản của khách hàng và tạo bút toán thực hiện giao dịch. Bút toán giống như bản ghi trong cơ sở dữ liệu ghi lại quá trình thực hiện một giao dịch nào đó.

3.3 MINH HỌA QUY TRÌNH SỬ DỤNG POS

3.3.1 GIAO DỊCH THANH TOÁN (SALE ONLINE)

Giao dịch này là loại giao dịch mua hàng hóa, thanh toán dịch vụ,… sử dụng cho cả 2 loại thẻ Credit (tín dụng) và Debit (ghi nợ). Giao dịch này là giao dịch online, máy kết nối đến hệ thống xử lý ngay lúc thực hiện giao dịch. Trong quá trình thực hiện giao dịch này cũng như các giao dịch khác, có thể máy sẽ yêu cầu chọn, nhập thêm thông tin, như chọn loại tiền tệ, nhập số PIN, khi đó, người sử dụng cần thực hiện theo yêu cầu. Một số trường hợp máy không yêu cầu thực hiện việc chọn lựa, đó là do tiến trình cài đặt đã qui định từ trước, chẳng hạn, thẻ Credit không yêu cầu phải nhập PIN.

MM DD , YYYY HH:MM  SWIPE OR INSERT CARD	Màn hình hiển thị ban đầu.
SALE VISA NGUYEN QUOC TUAN 4129654851234578 EXP DATE: 09/08	Kéo thẻ qua khe đọc, màn hình hiển thị loại thẻ, tên chủ thẻ, số thẻ và thời hạn hiệu lực theo thứ tự tháng trước năm sau, so sánh với thông tin trên thẻ. Nếu đúng bấm phím Enter.

SELECT CURRENCY VND USD	Bấm số 1 hoặc 2 để chọn loại tiền tệ giao dịch. Giả sử chọn số 2.USD
SALE ENTER AMOUNT? $23.00	Nhập số tiền giao dịch và nhấn phím Enter. (Nếu nhập sai số tiền, bấm phím CLEAR để xóa và nhập lại số tiền đúng).
SALE DIALING… PROCESSING…	Chờ máy xử lý thông tin…
SALE PRINTING APPV CODE 180772	… và in ra hóa đơn. Giao dịch kết thúc.

3.3.2 GIAO DỊCH XÁC MINH (CARD VERIFY)

Là loại giao dịch chỉ sử dụng cho thẻ Credit, dùng để kiểm tra thẻ và khóa (block) lại một số tiền nào đó của thẻ. Thường được sử dụng trong trường hợp cơ sở chấp nhận thẻ là các khách sạn hoặc hệ thống siêu thị, bộ phận tiếp tân hoặc thu ngân, tính toán trước số tiền chủ thẻ sẽ phải trả và thực hiện giao dịch ngay khi chủ thẻ đến lưu trú.

MM DD , YYYY HH:MM  SWIPE OR INSERT CARD	Màn hình hiển thị ban đầu, bấm phím Menu
1 LOGON 2 OFFLINE 3 CARD VERIFY SELECT:	Bấm số 3 để chọn Card Verify

CARD VERIFY VCB PLS SWIPE CARD	Kéo thẻ qua khe đọc
CARD VERIFY VISA NGUYEN QUOC TUAN 4129654851234578 EXP DATE: 09/03	Màn hình hiển thị loại thẻ, tên chủ thẻ, số thẻ và thời hạn hiệu lực theo thứ tự tháng trước năm sau, so sánh với trên thẻ. Nếu đúng bấm phím Enter.
SELECT CURRENCY 1. VND 2. USD	Bấm số 1 hoặc 2 để chọn loại tiền tệ giao dịch. Giả sử chọn số 2.USD
CARD VERIFY ENTER AMOUNT? $1.00	Nhập vào số tiền cần làm verify & bấm Enter.
CARD VERIFY PROCESSING... APPV CODE 180772	Chờ máy xử lý và in ra hóa đơn, giao dịch kết thúc.

Thực hiện với số tiền nhỏ, giao dịch này chỉ mang ý nghĩa kiểm tra thẻ. Với số tiền lớn hơn, ngoài ý nghĩa kiểm tra, thẻ còn bị khóa lại với số tiền đã làm Verify, và liên quan tới việc thực hiện loại giao dịch kế tiếp – OFFLINE - với số tiền thực thụ, khi chủ thẻ rời khỏi khách sạn.

3.3.3 GIAO DỊCH NGOẠI TUYẾN (OFFLINE).

Loại giao dịch sử dụng trong 2 trường hợp:

Trường hợp máy đọc thẻ không thể kết nối trực tuyến đến hệ thống. Nhân viên giao dịch gọi điện thoại đến trung tâm cấp phép của ngân hàng để xin số cấp phép. Số cấp phép được cung cấp sẽ được sử dụng trong tiến trình thực hiện giao dịch.

Trường hợp thanh toán chính thức sau khi đã thực hiện giao dịch Card Verify, đã khóa số tiền nào đó của thẻ từ trước.

MM DD , YYYY HH:MM  SWIPE OR INSERT CARD	Màn hình hiển thị ban đầu, bấm phím Menu
1 LOGON 2 OFFLINE 3 CARD VERIFY SELECT:	Bấm số 2 để chọn Offline.
OFFLINE VCB PLS SWIPE CARD	Kéo thẻ qua khe đọc
OFFLINE VISA NGUYEN QUOC TUAN 4129654851234578 EXP DATE: 09/03	Màn hình hiển thị loại thẻ, tên chủ thẻ, số thẻ và thời hạn hiệu lực theo thứ tự tháng trước năm sau, so sánh với trên thẻ. Nếu đúng bấm phím Enter.
SELECT CURRENCY 1. VND 2. USD	Bấm số 1 hoặc 2 để chọn loại tiền tệ giao dịch. Giả sử chọn số 2.USD
OFFLINE ENTER AMOUNT? $23.00	Tương tự như khi làm giao dịch On-line. Nhập vào số tiền giao dịch & bấm Enter. Sau đó máy sẽ hiển thị một lần nữa số tiền đã nhập. Nếu đúng bấm Enter.
OFFLINE APPV CODE?	Chương trình yêu cầu nhập vào mã số chuẩn chi (Approval Code) đã được cung cấp & bấm Enter.

OFFLINE PROCESSING... TXN. ACCEPTED	Chờ máy in ra hóa đơn, giao dịch kết thúc.

Đối với trường hợp (a), số cấp phép sẽ là số phòng cấp phép ngân hàng đã cấp.

Đối với trường hợp (b), số cấp phép sẽ là số có được của lần thực hiện giao dịch Card Verify. Vấn đề số tiền thực hiện Verify và số tiền thanh toán thực tế khi Offline nếu có chênh lệnh, nhiều hay ít hơn, thuộc về qui định của ngân hàng, các tổ chức phát hành thẻ.

Ghi chú: Nếu mã số chuẩn chi có ký tự là chữ, bấm phím số có chữ tương ứng, sau đó bấm phím Alpha cho đến khi xuất hiện chữ mong muốn.

3.3.4 GIAO DỊCH HỦY (VOID).

Giao dịch này dùng để hủy các giao dịch đã được thanh toán trước đó. Khi thực hiện giao dịch, người sử dụng không cần phải quẹt thẻ, nhưng phải chọn số hóa đơn (trace) của giao dịch thanh toán cần hủy (mỗi giao dịch thanh toán có số hóa đơn riêng).

MM DD , YYYY HH:MM  SWIPE OR INSERT CARD	Màn hình hiển thị ban đầu. Bấm phím VOID.
VOID VOID PASSWORD?	Nhập mật mã (0000) và bấm phím Enter.
VOID TRACE NO?	Nhập vào số của hóa đơn (Trace No.) cần hủy (bao gồm 06 số) và bấm phím Enter.Nếu nhập sai bấm phím CLEAR và nhập lại số đúng.
VOID TOTAL $27.00 CORRECT? Y/N	Máy sẽ hiển thị số tiền giao dịch của hóa đơn đó để xác định lại. Bấm phím Enter.

VOID DIALING… PROCESSING…	Chờ máy xử lý giao dịch...
VOID PRINTING TXN ACCEPTED	...và in ra hóa đơn hủy giao dịch.

3.3.5 GIAO DỊCH TỔNG KẾT (SETTLE).

Giao dịch tổng kết là giao dịch thực hiện cuối ngày, cuối phiên làm việc,.. dùng để tổng kết tất cả các giao dịch đã thực hiện với hệ thống xử lý. Sau khi thực hiện giao dịch này, tất cả các giao dịch đã lưu trong máy trước đó sẽ bị xóa, máy trở lại tình trạng ban đầu, sẵn sàng sử dụng cho phiên làm việc mới.

MM DD , YYYY HH:MM  SWIPE OR INSERT CARD	Màn hình hiển thị ban đầu, bấm phím SETTLE
SETTLEMENT SETTLEMENT PWD	Nhập vào mật mã (0000).
SALE 2 US$27.00 REFUND 0 US$0.00	Màn hình hiển thị tổng số tiền USD đã giao dịch. Nếu số tiền tổng kết đúng, bấm phím Enter (nếu số tiền sai bấm phím CLEAR & kiểm tra lại).
SALE 3 VND450,000 REFUND 0 VND0.00	Tương tự, màn hình hiển thị tổng số tiền VND đã giao dịch, kiểm tra lại rồi bấm Enter
SETTLEMENT DIALING… PROCESSING...	Chờ máy xử lý các thông tin và in ra hóa đơn, kết thúc tiến trình làm tổng kết.

CLOSED

KẾT LUẬN

Kết quả đạt được

Khoá luận này đã thu được một số kết quả sau:

- Trình bày một cách khá đầy đủ về hệ thống POS: khái niệm POS là gì, tích hợp trong hệ thống mạng của ngân hàng, đặc tả hệ thống, kỹ thuật đảm bảo an toàn trong hệ thống POS (mã hoá PIN, thuật toán mã hoá 3DES, nguyên tắc quản lý khoá), tương tác với các hệ thống khác.
- Tập trung giới thiệu một cách khái quát về các chuẩn truyền thông tin POS với các hệ thống khác: chuẩn ISO 11568, chuẩn ISO 9561, chuẩn 13491; các vấn đề liên quan đến bảo mật trong một hệ thống POS: vấn đề xác thực máy POS, vấn đề mã hoá dữ liệu trong hệ thống POS, vấn đề đảm bảo tính trong suốt trong hệ thống POS.
- Mô tả dữ liệu vào trong hệ thống POS, hỗ trợ cả hai loại thẻ: thẻ từ (magnetic stripe card) và thẻ chip (smart card): định dạng dữ liệu và các ví dụ cụ thể về các loại thẻ.
- Trình bày một cách chi tiết về một hệ thống POS: mô tả các thành phần trong hệ thống POS (POS, NCC, SWITCH, CMS, HSM, CORE) và cũng đã chỉ ra một ví dụ chi tiết về quy trình thực hiện một giao dịch trong hệ thống POS.
- Đề cập đến độ an toàn của hệ thống POS: con người và thiết bị, các nguy cơ về an toàn cũng đã được trình bày khi triển khai một hệ thống POS.

Các ứng dụng POS trong thực tế

Hiện nay, POS chủ yếu được triển khai và tích hợp trong hệ thống ngân hàng trong lĩnh vực thanh toán điện tử trực tuyến bằng cách sử dụng thẻ. Tuy nhiên, hệ thống POS đã được xây dựng để kết nối với hệ thống bán hàng để lấy các dữ liệu dùng để thanh toán (như các mục dùng trong hoá đơn, số km của taxi…) sau đó tổng hợp rồi mới chuyển đến ngân hàng, điều này phụ thuộc vào công nghệ của từng hãng.

TÀI LIỆU THAM KHẢO