BỘ TIÊU CHUẨN KỸ THUẬT KẾT NỐI HỆ THỐNG NAPAS
<Áp dụng cho các Tổ chức thành viên>

PHẦN IV: QUY ĐỊNH VỀ AN TOÀN BẢO MẬT THÔNG ĐIỆP VÀ TRUYỀN THÔNG

CÔNG TY CỔ PHẦN THANH TOÁN QUỐC GIA VIỆT NAM

Hà Nội, tháng 12 năm 2016

MỤC LỤC

QUẢN LÝ THAY ĐỔI VĂN BẢN

Phiên bản	Ngày ban hành	Người lập	Người duyệt	Nội dung thay đổi
0.9	Từ 01/2016 - 11/2016	Hà Nam Ninh Nguyễn Hùng Cường Bùi Thị Kim Dung Đào Thanh Sơn Huỳnh Công Linh Phạm Minh Ngọc Lê Anh Tuấn Nguyễn Thanh Quỳnh	Nguyễn Hưng Nguyên	- Xây dựng Bộ Tiêu chuẩn kỹ thuật phác thảo - Phân tách Bộ Tiêu chuẩn kỹ thuật thành 05 phần gồm: • Quyển 1 – Quy định về luồng xử lý thông điệp • Quyển 2 – Quy định về định dạng thông điệp • Quyển 3 – Quy định về file đối soát • Quyển 4 – Quy định về an toàn bảo mật thông điệp và truyền thông • Quyển 5 – Phụ lục - Bổ sung các quy định về xử lý thông điệp giao dịch thẻ quốc tế trong tài liệu • Quyển 6 – Quy định về luồng xử lý thông điệp quốc tế
1.0	12/2016	Hà Nam Ninh Nguyễn Hùng Cường Nguyễn Thanh Quỳnh Đào Thanh Sơn Huỳnh Công Linh	Nguyễn Hưng Nguyên	Bổ sung một số trường thông tin cho các giao dịch CHIP trong định dạng thông điệp và bảng mã trả lời (Response code) tại: - Quyển 02 - Quy định về định dạng thông

				điệp: mục 6 – Các thành phần dữ liệu; mục 7 – Cấu trúc dữ liệu - Quyển 05 - Phụ lục: mục 4 – Mã trả lời Cập nhật một số thông tin phần luồng xử lý giao dịch thanh toán Ecom, Tokenization đồng bộ với Quy định Tổ chức thành viên tại: - Quyển 01 - Quy định về luồng xử lý thông điệp : mục 4.2, 4.3, 4.5 - Quyển 02 - Quy định về định dạng thông điệp : mục 6.2

1 Đối tượng áp dụng

Đối tượng áp dụng bộ Tiêu chuẩn kỹ thuật kết nối dịch vụ chuyển mạch là Tổ chức thành viên (TCTV) của NAPAS bao gồm nhưng không giới hạn bởi Ngân hàng thành viên (NHTV) của NAPAS và Trung gian thanh toán (TGTT) tham gia kết nối triển khai các dịch vụ chuyển mạch.

2 Phạm vi

Tài liệu này đưa ra các quy định về an toàn bảo mật thông điệp và kết nối truyền thông dành cho các NHTV khi triển khai các dịch vụ chuyển mạch với NAPAS.

3 Thuật ngữ và định nghĩa

Bảng dưới đây mô tả các thuật ngữ và từ viết tắt được sử dụng trong tài liệu

STT	Thuật ngữ/ từ viết tắt	Ý nghĩa
1	PIN	Personal Identification Number
2	PAN	Primary Acccount Number
3	LMK	Local Master Key
4	ZMK	Zone Master Key
5	MK	Master Key
6	ZPK	Zone PIN Key
7	MAK	Message Authentication Key
8	HSM	Hardware Security Module
9	PGP	Pretty Good Privacy

4 Quy định về an toàn bảo mật thông điệp

4.1 Kiểm soát và quản lý khóa

4.1.1 Nguyên tắc quản lý khóa

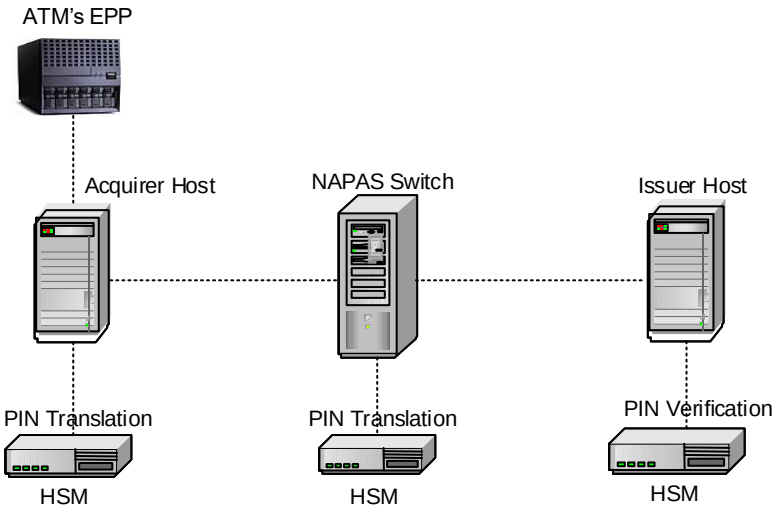
- Các khoá tồn tại theo chuẩn ISO 11568.
- Không truy cập hoặc xác định được bản rõ của bất kỳ khoá bí mật nào.

- Hệ thống phải ngăn chặn và phát hiện việc khám phá bất kỳ khoá nào; ngăn chặn các thay đổi khi không được cấp phép đối với các vấn đề về thay thế, xoá hay chèn thêm bất kỳ khoá nào.
- Các khoá bí mật được tạo ra theo một tiến trình không thể đoán ra bất kỳ một hoặc một tập hợp giá trị bí mật nào.
- Một khoá sẽ bị thay thế bằng một khoá mới trong trường hợp khoá cũ có nguy cơ bị làm hại hoặc bị tấn công hoặc nghi ngờ bị làm tổn hại.
- Việc làm hại một khoá trên một "tuyến" sẽ không làm ảnh hưởng đến khoá khác trong các "tuyến" khác.
- Một khoá khi bị làm tổn hại sẽ không cung cấp bất kỳ thông tin nào cho phép xác định ra sự thay thế.
- Một khoá 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 cấp phép.
- NAPAS và thành viên đều phải có nhật ký quản lý khoá. Mỗi lần truy cập vào dữ liệu khóa đều phải ghi vào nhật ký bao gồm thời gian, ngày, mục đích, các văn bản yêu cầu có chữ kí của người có thẩm quyền.

4.1.2 Thiết bị bảo mật Hardware Security Module (HSM)

4.1.2.1 Mô hình hoạt động

Mô hình hoạt động của thiết bị bảo mật Hardware Security Module (HSM):



Hình 1. Mô hình hoạt động của thiết bị HSM

Để đảm bảo dữ liệu được bảo mật khi truyền đi giữa các bên, tại Acquirer Host, Issuer Host và NAPAS Switch phải sử dụng thiết bị HSM để thực hiện việc:

- Mã hóa/ giải mã PIN
- Sinh/ xác thực MAC
- Mã hóa/ giải mã khóa

4.1.2.2 Các mức bảo mật phần cứng

Một số mức bảo mật phần cứng của FIPS cho thiết bị HSM:

a. **Security Level 1**:

Security Level 1 cung cấp mức bảo mật thấp nhất và đưa ra các yêu cầu bảo mật cơ bản cho module mã hoá. Các kỹ thuật bảo mật vật lý không được yêu cầu trong module.

b. **Security Level 2**:

Security Level 2 nâng cao tính bảo mật vật lý của một module bảo mật Level 1 bằng cách thêm vào yêu cầu cho tamper evident coatings hoặc seals các khoá có độ bảo vệ cao. Tamper evident coatings hoặc seals có thể được đặt trong một module mã hoá để coating hoặc seal phải được phá vỡ mới có thể truy cập vật lý tới các khoá mã hoá và các tham số bảo mật quan trọng khác trong module. Các khóa có độ bảo vệ cao có thể đặt bên ngoài hoặc tại cửa để bảo vệ các truy nhập vật lý không được phép.

Level 2 cung cấp chứng nhận thực dựa vào vai trò (role) trong đó một module phải kiểm tra người vận hành (operator) để chấp nhận một vai trò riêng và thực hiện một tập các dịch vụ tương ứng.

c. **Security Level 3**:

Security Level 3 yêu cầu bảo mật vật lý nâng cao có sẵn trong nhiều sản phẩm thương mại.

Level 3 cung cấp chứng nhận thực theo định danh (identity-based authentication), là hình thức chứng nhận thực mạnh hơn chứng nhận thực dựa theo vai trò (role based-authentication) được dùng ở Level 2. Một module phải chứng nhận thực định danh của người vận hành (operator) để có được một vai trò và thực hiện tập các dịch vụ tương ứng.

Level 3 cung cấp yêu cầu cao hơn với việc nhập và xuất các thông tin bảo mật. Các cổng dữ liệu dùng cho các thông tin bảo mật phải được tách biệt về mặt vật lý với các cổng dữ liệu khác. Hơn nữa, các thông tin này phải được đưa vào hoặc lấy ra module ở dạng mã hoá sử dụng các thủ tục hiểu biết riêng rẽ (split knowledge procedure).

d. **Security Level 4**:

Security Level 4 cung cấp mức bảo mật cao nhất.

Bảo mật vật lý Level 4 cung cấp một vỏ bọc bảo vệ xung quanh module mã hoá. Ngược lại các chuyển mạch phát hiện giả mạo của các module mức thấp có thể bỏ qua, mục đích của bảo vệ Level 4 là phát hiện xự xâm nhập vào thiết bị từ bất kỳ hướng nào. Nếu một ai đó phá lớp vỏ của module mã hoá, nỗ lực này sẽ bị phát hiện và tất cả các thông tin bảo mật quan trọng sẽ bị xoá.

Level 4 cũng bảo vệ module không bị làm hại đến tính bảo mật trong các điều kiện môi trường hoặc sự thay đổi bất thường bên ngoài khoảng hoạt động điện áp và nhiệt độ bình thường của module.

4.1.2.3 Cấu hình thiết bị HSM

Với HSM cần cấu hình một vài thông số theo chuẩn. Những thông số được đánh dấu sau là cần thiết. Đặc biệt, hai thông số Enable X9.17 for import, Enable X9.17 for export cần được đặt là Yes để đảm bảo cho quá trình trao đổi ZPK không lỗi.

Ví dụ: cấu hình HSM Thales 8000:

```
Online>qs

PIN length: 06
Encrypted PIN length: 07
Echo: OFF
Atalla ZMK variant support: OFF
Transaction key support: Racal
User storage key length: Double
Single-DES: Enabled
Select clear PINs: Y
Enable ZMK translate command: YES
Enable X9.17 for import: YES
Enable X9.17 for export: YES
Solicitation batch size: 1024
ZMK length: D
Prevent Single-DES keys masquerading as double or triple-length keys: NO
PIN encryption algorithm: A
Card/password authorisation: C
Decimalization tables: PLAINTEXT
Decimalization table checks: Disabled
Authorised State required when Importing DES key under RSA key: YES
```

```
Minimum HMAC key length in bytes: 08
Enable PKCS#11 import and export for HMAC keys: YES
Enable ANSI X9.17 import and export for HMAC keys: YES
Enable ZEK encryption of all printable ASCII chars : NO
Enable ZEK encryption of "Base94" ASCII chars : NO
Enable ZEK encryption of "Base64" ASCII chars : NO
Enable ZEK encryption of "Hex-only" ASCII chars : NO
Restrict Key Check Values to 6 hex chars : YES
Enable multiple authorised activities: YES
LMK check: XXXX XXXX XXXX XXXX
```

4.1.3 Quản lý khóa

4.1.3.1 Các loại khóa

- LMK (Local Master Key hay Master File Key): Khoá dùng để mã hóa các loại khóa khác trong lưu trữ.
- ZMK (Zone Master Key) hay MK (Master Key): Khóa dùng để mã hóa/giải mã khóa ZPK và MAK trong quá trình trao đổi khóa giữa NAPAS và các Tổ chức, Ngân hàng thành viên. Khóa ZMK có chiều dài 128 bit.
- ZPK (Zone PIN Key hay PIN Encryption Key hoặc Working Key - WK): đây là khoá Data Key dùng để mã hoá PIN Block, hay khoá phiên. Khoá này có chiều dài 128 bit.
- MAK (Message Authentication Key): đây là khóa Data Key dùng trong quá trình tính MACing. MAK là double length (32H), có thể hỗ trợ single length (16H) đối với mỗi ngân hàng.

Các khoá trên (trừ khóa LMK được lưu trữ trên HSM) sẽ được mã hoá bởi thuật toán 3DES và được lưu trữ trong cơ sở dữ liệu (cho phép quản lý khoá linh hoạt, backup/thu hồi/lưu trữ lâu dài, và đáp ứng được yêu cầu khi tăng số khoá).

4.1.3.2 Sinh khóa, phân phối và lưu trữ khóa

4.1.3.2.1 Khóa LMK

- Khóa LMK được sinh ra với 03 thành phần khóa được sinh ngẫu nhiên.
- Khóa LMK được lưu trữ trong thiết bị HSM của mỗi thành viên.

4.1.3.2.2 Khóa ZMK

Quy trình tạo khóa ZMK giữa NAPAS và các NHTV như sau:

Khi một NHTV muốn kết nối vào hệ thống của NAPAS thì các bước tiến hành khởi tạo khóa Zone Master Key (ZMK) hay khóa Master Key (MK) giữa NAPAS và NHTV được tiến hành như sau:

- **Bước 1:** Tổ chức thành viên gửi yêu cầu khởi tạo thành phần khóa MK bằng văn bản đến NAPAS.
- **Bước 2:** Đơn vị quản trị HSM của NAPAS tiếp nhận, xem xét yêu cầu và khởi tạo một thành phần khóa MK tương ứng với NHTV đó. NHTV cũng đồng thời khởi tạo một thành phần khóa MK dành riêng cho kết nối với NAPAS. Thông thường, khóa MK sẽ được tạo từ 02 thành phần, trong trường hợp yêu cầu khóa MK phải được tạo từ nhiều hơn 02 thành phần, NAPAS và NHTV sẽ thỏa thuận cụ thể số lượng thành phần khóa mà mỗi bên sẽ khởi tạo.
- **Bước 3:** NAPAS và NHTV tiến hành khởi tạo khóa MK bằng phương thức như sau: NAPAS và NHTV thống nhất địa điểm, thời gian và cử cán bộ trực tiếp đến nạp thành phần khóa MK của mình vào HSM của bên kia trong quá trình khởi tạo MK (có biên bản xác nhận hoàn thành quá trình khởi tạo MK có chữ ký của cán bộ tham gia thực hiện). So sánh đối chiếu giá trị KCV (Key Check Value) thu được của quá trình tạo MK trên HSM ở NAPAS và NHTV qua các phương thức liên lạc thông thường (ví dụ như qua đường điện thoại, email…). Nếu hai giá trị thu được là giống nhau, quá trình tạo khóa MK thành công. Nếu hai giá trị thu được là không giống nhau, quá trình tạo khóa MK thất bại và hai bên phải xem kỹ lại các bước 1 và 2 để tìm nguyên nhân sai khác.
- **Bước 4:** Khóa MK sau khi khởi tạo thành công sẽ được nạp vào hệ thống của NAPAS và NHTV. Khóa này được sử dụng để tiến hành trao đổi khóa mã hóa phiên kết nối giữa hai bên.

Khóa ZMK và các khóa Data Key (ZPK, MAK) phải được lưu trữ trong thiết bị HSM hoặc lưu trữ dưới dạng mã hóa bởi khóa LMK tại hệ thống của mỗi thành viên.

Lưu ý: *TCTV cần lưu ý đến công đoạn khởi tạo khóa/thành phần khóa để đảm bảo an toàn cho khóa ZMK được sinh ra*.

4.1.3.2.3 Khóa Data Key

Các khóa Data Key bao gồm ZPK và MAK được hệ thống của NAPAS sinh ra ngẫu nhiên sử dụng thiết bị HSM.

Trong trường hợp trao đổi khóa động, quy trình phân phối các khóa Data Key tới các NHTV như sau:

- NAPAS mã hóa các khóa Data Key bằng khóa ZMK với thành viên và gắn kèm khóa Data Key được mã hóa này vào thông điệp trao đổi khóa để gửi tới NHTV;
- NHTV giải mã khóa Data Key, và lưu trữ khóa Data Key vào thiết bị HSM hoặc mã hóa khóa Data Key bằng LMK rồi lưu trữ tại hệ thống;
- NHTV gửi thông điệp trả lời xác nhận việc trao đổi khóa thành công cho NAPAS để áp dụng khóa Data Key mới giữa 2 bên.

4.1.4 Bảo mật Zone Master Key (Master Key)

Khóa Master key là khoá được dùng để trao đổi các khóa Working key (các khóa Working key được mã hoá bằng Master key và được gửi đi trong các thông điệp 0800/0810). Vì vậy cần phải bảo vệ an toàn Khóa Master key. Khóa Master key giữa NAPAS và từng thành viên sẽ là khác nhau. Các khóa Master key được sinh ra từ HSM của NAPAS và các TCTV bằng việc kết hợp bản rõ các thành phần khóa của hai bên. Khi tạo Master key cho một thành viên, cần phải có sự tham gia của hai bên gồm tối thiểu một người được NAPAS chỉ định và tối thiểu một người được thành viên chỉ định. NAPAS quy định các công việc và trách nhiệm của người giữ khóa Master key như sau:

1) Bổ nhiệm người quản lí khóa:
   - Người chịu trách nhiệm quản lí khóa Master Key của thành viên sẽ do Tổ chức Thành viên chỉ định và một người của NAPAS do NAPAS chỉ định.

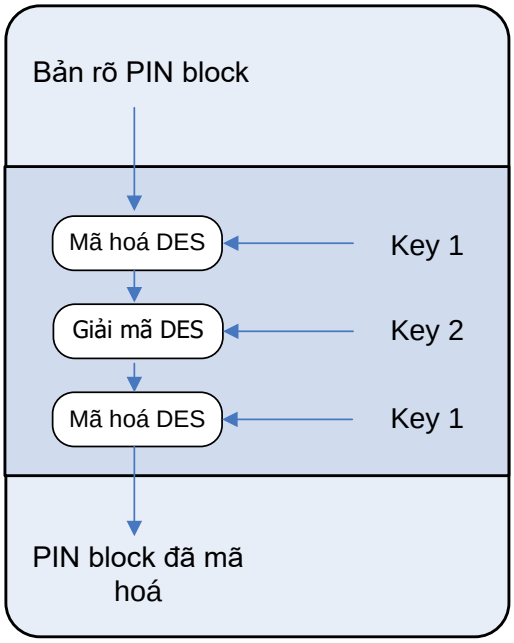
2) Trách nhiệm của người quản lí khóa:
   - Nhận và lưu trữ an toàn các thành phần khóa.
   - Kiểm soát các dữ liệu khóa, kiểm tra các dữ liệu đó và việc lưu trữ chúng an toàn.
   - Không tiết lộ khoá cho các cá nhân không có trách nhiệm.
   - Duy trì các bản ghi và nhật kí theo dõi truy cập đến và việc sử dụng dữ liệu khóa bao gồm thời gian truy cập, ngày, mục đích,....
   - Chứng kiến, thực hiện phá hủy các thành phần khóa đã hết hạn sử dụng hoặc việc huỷ khoá cũ khi có sự đồng ý của cả NAPAS và thành viên.
   - Nhập dữ liệu khóa vào các module mã hóa bảo mật (HSM) khi được yêu cầu.

4.2 Mã hóa và giải mã PIN

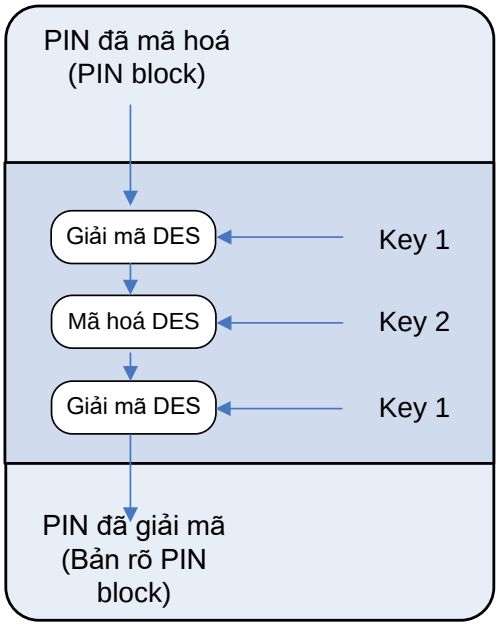
4.2.1 Quá trình mã hóa và vận chuyển PIN

Quá trình mã hóa và vận chuyển PIN được thực hiện như sau:

- Việc sinh số PIN và phương thức lưu PIN, khóa mã hóa PIN tùy thuộc vào từng ngân hàng thành viên, số PIN không quá 6 (sáu) ký tự.
- Việc vận chuyển số PIN trong hoạt động chuyển mạch của NAPAS thông qua khối PIN (PIN Block). Định dạng khối PIN tuân theo quy định trong phân mục "Khuôn dạng khối PIN".
- Để đảm bảo tính an toàn của khối PIN trong quá trình truyền trên mạng, các ngân hàng phải mã hóa khối PIN trước khi khối PIN được chuyển từ các thiết bị chấp nhận thẻ tới Switch của ngân hàng chấp nhận thẻ. Khối PIN của ngân hàng chấp nhận thẻ được bảo mật bằng các khoá thoả thuận với NAPAS trước khi được chuyển tới NAPAS:
  - + NAPAS nhận các khối PIN đã mã hoá từ ngân hàng chấp nhận thẻ, giải mã rồi mã hoá theo khoá thoả thuận với bên phát hành thẻ rồi gửi đến ngân hàng phát hành mà không lưu bản rõ khối PIN.
  - + Số PIN có số ký tự tối đa là 6 (thường là 4 hoặc 6 ký tự).
- Trong các giao dịch tài chính qua NAPAS, định dạng của khối PIN tuân theo ISO 9564-1 format 0. Trong đó bản rõ khối PIN và số PAN (Primary Account Number) được áp dụng phép toán "XOR" với nhau, sau đó được mã hoá bởi thuật toán "3DES" để tạo thành một khối mã hoá 64 bit đầu ra.
- ATM của ngân hàng thành viên phải có module EPP (Encrypting PIN Pad) hỗ trợ 3DES đáp ứng các yêu cầu theo ISO 9564-1, ISO 13491-1 và ISO 13491-2. Module EPP sẽ mã hoá khối PIN ngay khi nhận PIN gõ vào của khách hàng trước khi gửi đến host (trung tâm xử lý) của ngân hàng để nâng cao tính bảo mật PIN cho khách hàng.
- Bản rõ của khối PIN không bao giờ được xuất hiện bên ngoài một EPP hay HSM.



Mã hoá PIN tại ATM (EPP)



Hình 2. Giải mã PIN tại Trung tâm xử lý

4.2.2 Khuôn dạng khối PIN - PIN Block

Do thuật toán DES (3DES) chỉ làm việc với khối dữ liệu đầu vào có độ dài là 64 bit (nên độ dài tối đa của mỗi số PIN là 16 số).

Theo chuẩn ISO 9564-1 cấu trúc khối dữ liệu PIN 64 bit. Trong đó 4 bit quan trọng nhất trong khối này ở trường điều khiển (C) có giá trị là:

0000	Format 0 (***Định dạng được đề nghị***)
0001	Format 1
0010	Format 2 định nghĩa trong ISO 9564-3
0011	Format 3

Khối PIN Format 0 được xây dựng bằng cách module-2 (XOR) hai trường 64 bit: trường bản rõ PIN (với các số điền đầy là F - hệ Hexa) và trường số PAN với các thông tin gồm:

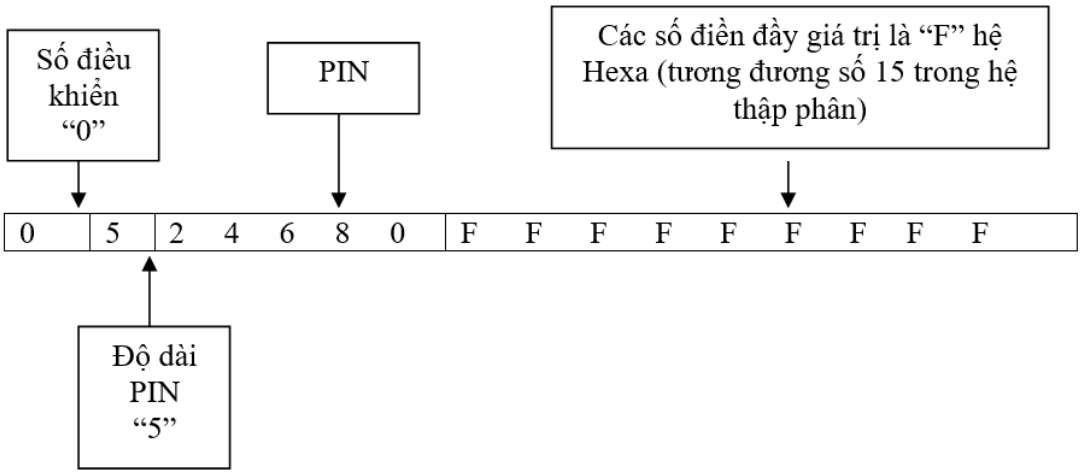
- Trường bản rõ PIN có khuôn dạng như sau:

Vị trí Bit	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61..64
Giá trị	C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

Trong đó:

C = Trường điều khiển	0000
N = Chiều dài PIN	4 bit với giá trị từ 0100 (4) đến 1100 (12)
P = Số PIN	4 bit với giá trị từ 0000 (0) đến 1001 (9)
P/F = Số PIN/Số lấp đầy	Trường này được xác định bởi giá trị N
F = Số lấp đầy (Hexadecimal)	Trường 4 bit giá trị 1111 (15)

Ví dụ: Bản rõ của khối PIN format 0:



- Trường số PAN có khuôn dạng như sau:

Vị trí Bit	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61..64
Giá trị	0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12

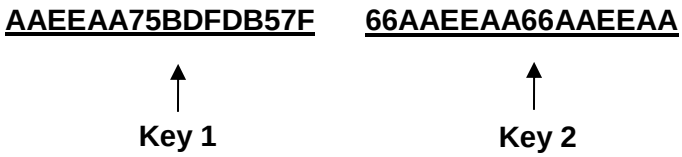
Trong đó:

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

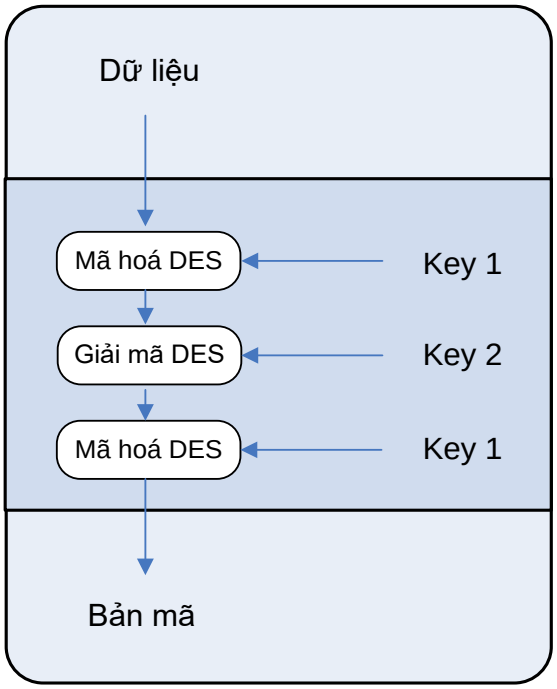
4.2.3 Phương thức mã hóa PIN

Mã hóa PIN bằng thuật toán mã hóa 3DES, sử dụng khóa bộ hai (128 bit). 3DES dùng 64 bit bên trái của khóa để mã hóa dữ liệu, 64 bit bên phải của khóa để giải mã kết quả của mã hóa đó và dùng lại 64 bit bên trái của khóa để mã hóa kết quả của việc giải mã trước đó (Phần bên trái phải khác phần bên phải của khóa. Nếu 2 phần giống nhau thì việc mã hóa, giải mã và mã hóa lần nữa với cùng một khóa sẽ đồng nhất với việc sử dụng khóa đơn 56 bit).

Ví dụ: một khoá bộ hai 3DES (128 bit) với 64 bit bên trái (key 1) và 64 bit bên phải (key 2) như sau:



Sơ đồ dưới đây mô tả việc dùng khoá 3DES bộ hai để mã hoá dữ liệu:



Việc sử dụng 3DES bộ hai trong mạng chuyển mạch đòi hỏi tính đồng bộ và thống nhất trong tất cả các ngân hàng thành viên, điều này đòi hỏi các ngân hàng thực hiện các công việc sau:

- Nâng cấp hoặc thay thế các thiết bị ATM và HSM.
- Nâng cấp hoặc viết lại phần mềm quản trị mạng ATM và quản lý các giao dịch ATM.
- Thay thế hoặc chỉnh sửa CSDL lưu trữ khóa đã được mã hóa để thích hợp với kích thước khóa lớn hơn.
- Tạo (create), trao đổi (exchange), thay thế (replace), nạp (load) và lưu trữ nhiều khóa 3DES mới.
- Mở rộng việc kiểm tra và chứng nhận.

- Hủy khóa độ dài đơn đang dùng.

4.3 Tính toán giá trị MAC cho thông điệp

4.3.1 Mục đích sử dụng MAC

Mã xác thực thông điệp (Message Authentication Code - MAC) đảm bảo tính toàn vẹn trong quá trình trao đổi dữ liệu giữa NAPAS và cácTổ chức, Ngân hàng thành viên.

MAC thực hiện hai mục đích chính:

- Cho phép bên nhận xác thực rằng nội dung của thông điệp không bị giả mạo và nó không bị sửa đổi hay can thiệp vào nội dung trong quá trình vận chuyển.
- Cho phép bên nhận xác thực rằng thông điệp xuất phát từ người gửi xác định.

Để đảm bảo tính toàn vẹn dữ liệu, quá trình xác thực gồm 2 bước:

- Sử dụng thuật toán tính MAC và khóa mã hóa dữ liệu (MAC Key hay khóa MAK) đối với khối dữ liệu được lựa chọn để tính toán sinh ra số MAC, sau đó gắn kèm số MAC vào cuối thông điệp trước khi gửi đi.
- Nơi nhận thông điệp sử dụng cùng một thuật toán tính MAC và khóa mã hóa MAK đã thỏa thuận với bên gửi thông điệp để sinh lại số MAC đối với thông điệp nhận được và xác thực thông điệp đó bằng cách so khớp số MAC mới tạo lại với số MAC nhận được.

4.3.2 Các trường dùng để tính toán giá trị MAC

MACing sẽ được cấu hình để áp dụng cho tất cả các loại mã xử lý – Pcode, cho cả giao dịch tài chính (Cash withdrawal, IBFT…) và phi tài chính (Balance inquiry, Mini statement) và tất cả các loại thông điệp 0200/0210/0420/0430.

MACing không áp dụng cho các giao dịch mạng 0800/0810.

MACing là bắt buộc đối với tất cả các giao dịch qua hệ thống NAPAS (trừ giao dịch mạng).

Các trường sau đây là cố định và được dùng trong việc tính MACing và chỉ tính trên các trường nào tồn tại trong thông điệp được gửi.

- Nếu bit ON → trường được tính MAC.
- Nếu bit OFF → trường không được tính MAC.

Message	Data Element Required for MAC Generation/Validation
0200/0210/0420/0430	MSG TYPE, DE2, DE3, DE4, DE5, DE6, DE7, DE11, DE32, DE37, DE38, DE39, DE41, DE42, DE48, DE63, DE90, DE102, DE103

4.3.3 Tính toán giá trị MAC

Hệ thống NAPAS tạo MAC cho các giao dịch đi từ NAPAS và kiểm tra MAC cho các giao dịch đến NAPAS. Sử dụng key MAK và các trường tính MAC đã định nghĩa trên.

Trường DE128 (length 16H) được dùng lưu giá trị MAC cho các giao dịch yêu cầu và phản hồi.

- Đối với MAK double length (32H) sẽ sử dụng chuẩn ANSI X9.19
- Đối với MAK double length (16H) sẽ sử dụng chuẩn ANSI X9.9

Cách xây dựng dữ liệu khi sinh số MAC và xác thực từ các thành phần dữ liệu như sau:

- Trường có độ dài thay đổi: dữ liệu tính MAC bao gồm cả phần định nghĩa độ dài và phần nội dung của trường dữ liệu.
- Trường có độ dài cố định: dữ liệu tính MAC chỉ có phần nội dung của trường dữ liệu
- Các thành phần dữ liệu này được gộp thành một chuỗi của dữ liệu đầu vào để tính MAC (nếu thành phần dữ liệu nào không được định nghĩa trong thông điệp thì nó sẽ bị bỏ qua).
- Nếu dữ liệu đầu vào để tính MAC không là bội số của 8 Bytes, thì thêm vào số 0 nhị phân - binary 0 (hexadecimal value of 0x00) vào cuối của chuỗi dữ liệu để tạo thành bội số của 8byte. Sau đó khối dữ liệu này được tính MAC theo chuẩn ANSI X9.19 hoặc ANSI X9.9.
- Giá trị MAC trong thông điệp, có độ dài 16 ký tự (Hex) và được lưu trong trường DE128.

4.3.4 Xử lý lỗi giá trị MAC

Trong trường hợp sai MAC, NAPAS trả lại thông điệp từ chối với mã lỗi tuân theo quy định về bảng mã lỗi.

4.4 Đặc tả DLL tạo và kiểm tra giá trị Checksum trong file trao đổi

NAPAS cung cấp cho các ngân hàng thành viên DLL để thực hiện tạo và kiểm tra các trường checksum trong file trao đổi.

DLL kiểm tra bao gồm 2 hàm:

4.4.1.1 Hàm tạo giá trị checksum 32 bytes từ một chuỗi ký tự gốc

string getMd5Hash (string input)

string getCS(string MaBM,string input)

MaBM: mã bí mật của ngân hàng

input: Nội dung cần tính checksum

4.4.1.2 Hàm kiểm tra giá trị checksum với 1 chuỗi ký tự gốc

bool verifyMd5Hash(string input, string hash)

bool verifyCS(string MaBM,string input, string hash)

MaBM : mã bí mật của ngân hàng

input : Nội dung cần tính checkSum

hash : xâu đã được checkSum

Để có thêm thông tin về giải thuật mã hoá MD5, xin xem thêm tại trang web: http://en.wikipedia.org/wiki/MD5

Giải thuật biến đổi Md5:

```
public string GetCS(string input,string MaBM)
{  string str="";
string strMa = getMd5Hash(input);
string strKQ = strMa;
```

```
            MaBM = "5" + MaBM + "5";
        if(IsNumeric(MaBM))
        {//Ma bi mat la so
            char[] chars = MaBM.ToCharArray();
            for(int i=0; i<chars.Length - 1; i++)
            {
                str = str + strMa.Substring(Convert.ToInt16(chars[i].ToString()), 20 - Convert.ToInt16(chars[i + 1].ToString()));
            }
            strKQ = getMd5Hash(str);
        }
        return strKQ;
    }
```

5 Áp dụng PGP trong việc truyền nhận file dữ liệu an toàn

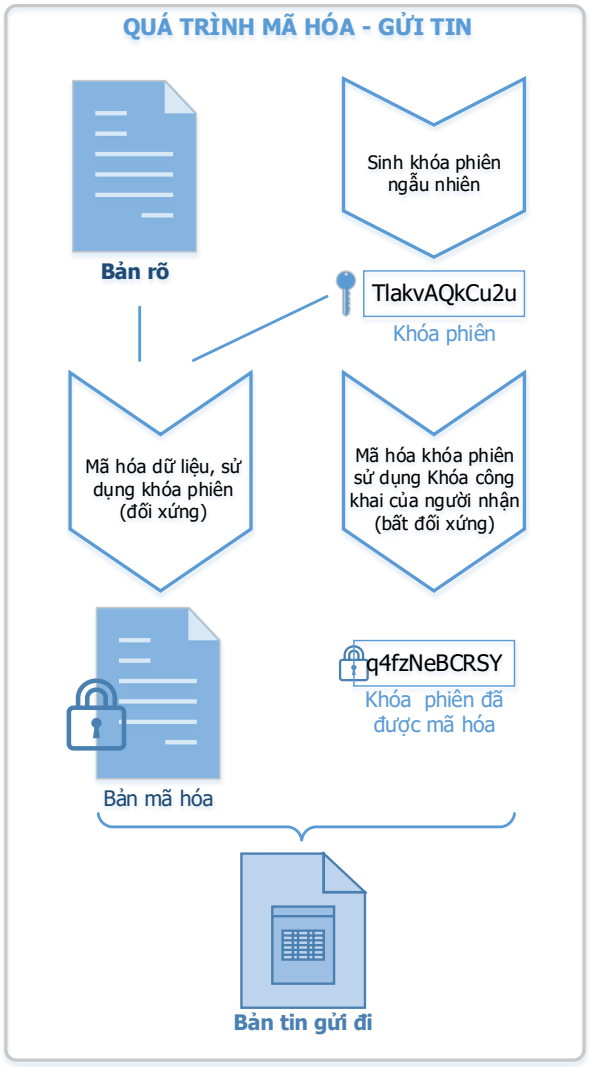
5.1 Giới thiệu về PGP (Pretty Good Privacy)

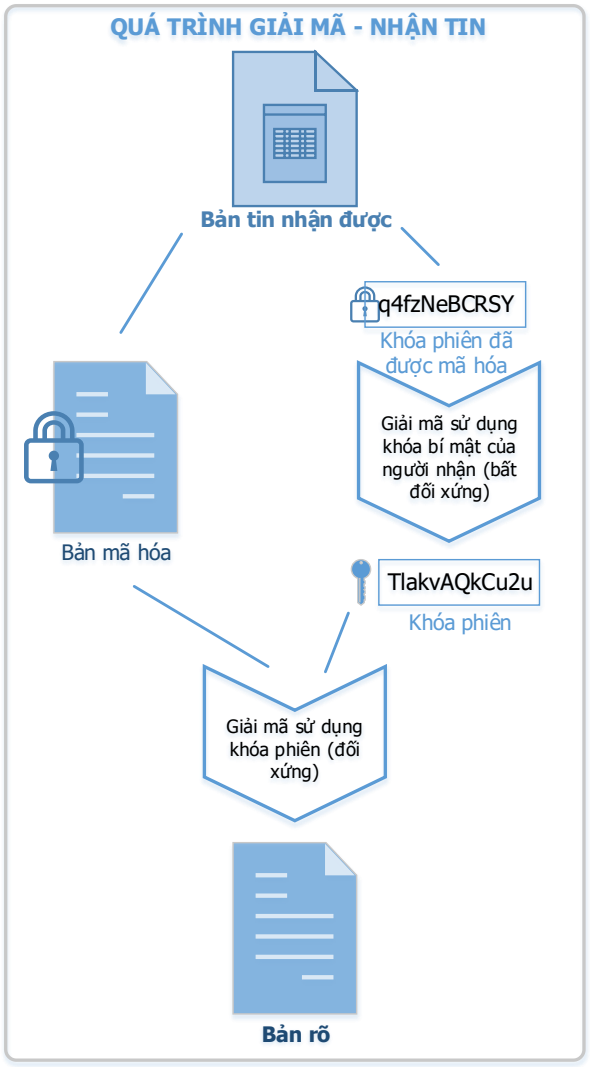
PGP (Pretty Good Privacy): là một phương pháp (phần mềm) phổ biến và mạnh mẽ để mã hóa dữ liệu, phiên bản đầu tiên do Phil Zimmerman công bố vào năm 1991. Các phần mềm dựa trên PGP được dùng để mã hóa và bảo vệ thông tin lưu trữ trên máy tính cá nhân, máy chủ và trong quá trình trao đổi thông tin qua email, IM, hoặc chuyển file.

Hoạt động:

- PGP hoạt động dựa trên một tập hợp ba loại khóa để mã hóa và giải mã thông điệp: khóa công khai, khóa bí mật, khóa phiên.
- PGP sử dụng cả hai loại mã hóa: mã hóa đối xứng (TripleDES, AES…) và mã hóa bất đối xứng (RSA).

5.2 Sơ đồ hoạt động





Bước	Gửi tin – Mã hóa	Nhận tin – giải mã
B1	Người gửi tạo ngẫu nhiên một khóa phiên – sẽ được sử dụng để mã hóa bản tin gốc.	Nhận bản tin tổng phân tách thành bản mã hóa và khóa phiên được mã hóa
B2	Mã hóa bản tin gốc sử dụng khóa phiên (TripleDES, AES) => nhận được bản tin đã được mã hóa	Giải mã khóa phiên sử dụng khóa bí mật của người nhận (RSA)
B3	Mã hóa khóa phiên sử dụng khóa công khai của người nhận (mã hóa bất đối xứng – RSA)	Giải mã bản mã hóa sử dụng khóa phiên đã giải mã từ bước trước
B4	Kết hợp bản tin mã hóa và khóa đã mã hóa	Nhận được bản tin gốc hoàn chỉnh.

	thành bản tin tổng gửi cho người nhận	

5.3 Truyền nhận file an toàn tại Napas

5.3.1 Hiện trạng – yêu cầu:

Hiện tại bộ phận Thanh toán, tra soát, đối soát tại Napas hàng ngày đều gửi các file tới đối tác trong đó có các thông tin nhạy cảm liên quan đến dữ liệu thẻ của Khách hàng cần được giữ bí mật.

Do vậy, ngoài việc sử dụng đường truyền được mã quá (FTPS), cần thiết phải áp dụng một thuật toán mã hóa dữ liệu đủ mạnh trong việc truyền nhận file dữ liệu có các thông tin thẻ, ở đây là PGP.

5.3.2 Tiêu chuẩn kỹ thuật:

5.3.2.1 Khóa phiên, khóa bí mật, khóa công khai

- Khóa phiên được sinh ra hoàn toàn ngẫu nhiên (có thể sử dụng phần mềm hoặc thiết bị phần cứng) với độ dài 128 bit.
- Khóa phiên được sinh ra tương ứng với từng file dữ liệu (mỗi file dữ liệu sẽ có một khóa phiên khác nhau).
- Cặp khóa bí mật, khóa công khai độ dài 2048 bit, sẽ được đối tác sinh ra và gửi khóa công khai cho Napas qua các kênh bảo mật tốt như: lấy từ chứng thư số đã được một CA chứng thực, trao đổi trực tiếp, v.v…
- Khóa bí mật (Private Key) của mỗi tổ chức sẽ do tổ chức đó lưu trữ và bảo vệ đảm bảo an toàn theo các Quy định về an toàn bảo mật trong ngành ngân hàng của Cục Công nghệ tin học – Ngân hàng Nhà nước (CNTH NHNN).

5.3.2.2 Thuật toán mã hóa

- Mã hóa đối xứng sử dụng khóa phiên: dùng thuật toán mã hóa mạnh AES.
- Mã hóa bất đối xứng sử dụng thuật toán RSA.

5.3.2.3 File mã hóa

- Mã hóa trên toàn bộ nội dung file dữ liệu gốc
- Tên file sau khi được mã hóa gồm: [Tên file gốc]+[.pgp] (VD: abc.dat.pgp)
- Nội dung file mã hóa gồm:

- Dòng 1: Khóa phiên sau khi đã được mã hóa bằng thuật toán bất đối xứng dưới định dạng BASE64 và loại bỏ ký tự xuống dòng.
- Dòng tiếp theo đến hết: nội dung của file sau khi đã được mã hóa sử dụng khóa phiên, dưới định dạng BASE64.

6 Quy định về truyền thông

6.1 Giao thức kết nối

6.1.1 Các dịch vụ cơ bản trên ATM/POS

NAPAS hỗ trợ NHTV kết nối Host-To-Host qua giao thức TCP/IP. Trong đó, NAPAS đóng vai trò là Server và các NHTV đóng vai trò là Client. Với mỗi NHTV, NAPAS sẽ mở một port để NHTV kết nối đến và tại một thời điểm chỉ cho phép duy nhất một phiên kết nối đến cổng trên Server.

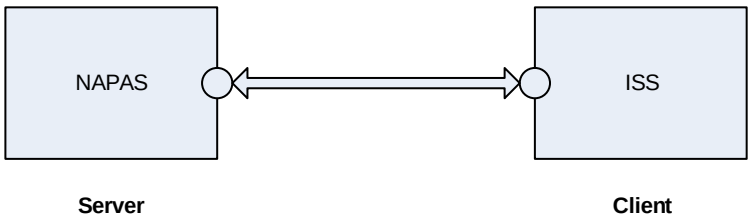
NAPAS hỗ trợ kết nối Multi-port dựa trên nguyên tắc luân chuyển vòng (Round robin method) để gửi thông điệp.

- Thông điệp được gửi đến từ cổng nào NAPAS sẽ phản hồi lại về cổng đó. Trong trường hợp cổng ở trạng thái “down” NAPAS sẽ chuyển sang cổng khác còn đang ở trạng thái sẵn sàng.
- Các thông điệp được luân chuyển vòng, không phân biệt kiểu giao dịch ATM hay POS.
- Mỗi Ngân hàng chỉ có một Key duy nhất được sử dụng chung cho các Port (khóa ZMK, ZPK và MAK được sử dụng chung khi cấu hình Multi-port).
- Khi thực hiện trao đổi khóa, giá trị Key ZPK và MAK được NAPAS trả lời luân chuyển vòng trên các port (yêu cầu trao đổi khóa được thực hiện trên một port nhưng NAPAS trả lời giá trị của khóa ZPK và MAK có thể trên port khác nếu như cấu hình Multi-port).

- Khi sử dụng Multi-port, các giao dịch mạng như Sign-On, Key Exchange, v.v… chỉ cần được thực hiện một lần trên một port nào đó. Không cần thực hiện nhiều lần các giao dịch mạng cho các port kết nối.

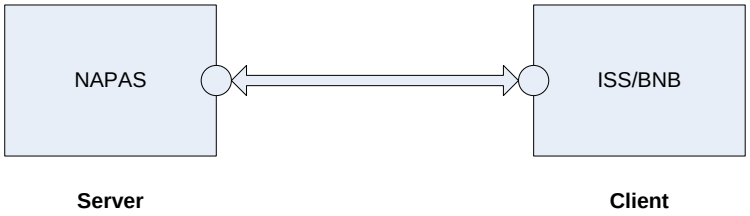
6.1.2 Dịch vụ Ecom

Đối với kết nối qua giao thức Socket (TCP/IP), NAPAS đóng vai trò là Server và các NHTV đóng vai trò là client. Ngân hàng sẽ kết nối đến port đã mở trước đó dành cho các dịch vụ cơ bản trên ATM/POS. Nếu ngân hàng chưa có kết nối các dịch vụ cơ bản trên ATM/POS đến NAPAS thì NAPAS sẽ mở port mới cho Ngân hàng kết nối đến.



6.1.3 Dịch vụ chuyển tiền nhanh NAPAS

Đối với kết nối qua giao thức Socket (TCP/IP), NAPAS đóng vai trò là Server và các NHTV đóng vai trò là client. NAPAS mở một port mới để các Ngân hàng kết nối đến.



6.2 Đường truyền kết nối

6.2.1 Thông tin về kỹ thuật

Để đảm bảo duy trì hoạt động 24/7 của dịch vụ chuyển mạch và các dịch vụ khác giữa NAPAS với Ngân hàng, hiện NAPAS đang áp dụng sử dụng 02 đường truyền để kết nối với mỗi Ngân hàng. Đường truyền chính là đường truyền số liệu Metronet hoặc MegaWAN của nhà cung cấp VNPT với tốc độ 1Mbps trở lên kết nối đến Trung tâm dữ liệu (DC – Data Center) của NAPAS và đường truyền dự phòng là đường Metronet của một trong các nhà cung cấp CMC, FPT hoặc Viettel tốc độ 1 Mbps trở lên kết nối đến Trung tâm phục hồi thảm họa (DRC – Disaster Recovery Center) của NAPAS.

Yêu cầu về cấu hình đường truyền: Do yêu cầu bảo mật trên đường truyền nên thông tin trên đường truyền sẽ được mã hóa VPN với khóa sử dụng là **pre-shared key** giữa 2 Router đặt tại đầu kết nối NAPAS và đầu kết nối Ngân hàng.

Yêu cầu về thiết bị tại đầu Ngân hàng: bao gồm các yêu cầu tối thiểu như sau

- 01 optical electrical converter (bộ chuyển đổi quang điện dành cho đường truyền Metronet)
- 01 Modem MegaWan (sử dụng cho đường truyền MegaWan)
- 01 Router Cisco Series Security bundle có hệ điều hành Cisco Router IOS Advanced Security (phục vụ cho việc mã hóa đường truyền VPN).

***Yêu cầu về địa điểm kết nối tại phía Ngân hàng*:** Yêu cầu địa điểm đặt thiết bị phía Ngân hàng phải có hệ thống phòng chống cháy nổ, hệ thống điều hòa nhiệt độ và hệ thống UPS để đảm bảo thiết bị hoạt động ổn định.

***Yêu cầu về đội ngũ triển khai*:** Phối hợp với các cán bộ truyền thông phía NAPAS để sớm thực hiện trong việc thuê đường truyền, và cấu hình đường truyền.

***Yêu cầu về quản trị đường truyền*:** Để đảm bảo duy trì hoạt động ổn định giữa NAPAS và các Ngân hàng, sau khi đã phối hợp cấu hình để đưa đường truyền vào sử dụng phía Ngân hàng sẽ có trách nhiệm kiểm tra đường truyền định kỳ và chịu trách nhiệm về đường truyền từ phía Ngân hàng tới đầu Router đặt tại phía NAPAS. Khi có sự cố xảy ra NAPAS sẽ cùng phối hợp với các cán bộ phía Ngân hàng để sử lý.

6.2.2 Thông tin về đường truyền

Ngân hàng làm chủ hợp đồng với các nhà mạng triển khai các đường truyền đến NAPAS với các thông tin như sau:

	Đường truyền chính	**Đường truyền dự phòng**
Địa điểm kết nối	**Global Data Service., JSC** Thang Long Data Center, Plot P-5, Khu công nghiệp Thăng Long, Đông Anh, HN	**Trụ sở NAPAS** Tòa nhà Pacific Place 83B Lý Thường Kiệt, phường Trần Hưng Đạo, quận Hoàn Kiếm, Hà Nội.
Nhà cung cấp	VNPT	CMC, FPT, Viettel
Loại đường truyền	Metronet hoặc MegaWAN	Metronet

Tốc độ tối thiểu	1 Mbps	1 Mbps
Mã hóa đường truyền	GRE over Ipsec	GRE over Ipsec

7 Quy định về đảm bảo tuân thủ đáp ứng chuẩn bảo mật PCI DSS

Để đảm bảo về bảo mật thông tin dữ liệu chủ thẻ, hệ thống của NAPAS và Ngân hàng cần thực hiện việc lưu trữ (trong log ứng dụng và cơ sở dữ liệu) đáp ứng yêu cầu của chuẩn bảo mật PCI DSS như sau:

		Thành phần dữ liệu	**Được phép lưu trữ**	**Thông tin lưu trữ dưới dạng bản rõ**
Dữ liệu khách hàng	**Dữ liệu chủ thẻ**	Primary Account Number (PAN)	Có	Không
		Cardholder Name	Có	Có
		Service Code	Có	Có
		Expiration Date	Có	Có
	Dữ liệu xác thực nhạy cảm	Full Track Data	Không	Không được lưu
		CAV2/CVC2/CVV2/CID	Không	Không được lưu
		PIN/PIN Block	Không	Không được lưu

Đối với các File trao đổi giữa NAPAS và Ngân hàng thành viên (File đối chiếu, File tra soát khiếu nại,..) cần đảm bảo các yêu cầu sau:

- File trao đổi dữ liệu cần được mã hóa theo phương pháp PGP **(chi tiết mục 5. Áp dụng trong việc truyền nhận file dữ liệu an toàn)**
- File trao đổi giữa NAPAS và NHTV không được chứa các trường dữ liệu xác thực nhạy cảm

8 Hiệu lực văn bản

Bộ Tiêu chuẩn kỹ thuật này có hiệu lực từ ngày **01/01/2017.**

9 Quản lý văn bản

Văn bản tham chiếu nội bộ:

STT	Tên văn bản
1	Tiêu chuẩn kỹ thuật kết nối BANKNETVN (Phiên bản 1.6.1)
2	Bộ Quy định Tiêu chuẩn kỹ thuật SMARTLINK (Phiên bản 2.0)
3	Bộ Quy định hoạt động Tổ chức thành viên SMARTLINK
4	Bộ Quy chế thành viên tham gia hệ thống chuyển mạch BANKNETVN
5	Quy định nghiệp vụ thanh toán, quyết toán giao dịch thẻ qua hệ thống chuyển mạch BANKNETVN (ban hành ngày 28/02/2013)

Văn bản tham chiếu bên ngoài:

STT	Tên văn bản
1	Bộ Tiêu chuẩn kỹ thuật ISO 8583 -1987
2	Bộ Tiêu chuẩn kỹ thuật của Tổ chức VISA
3	Bộ Tiêu chuẩn kỹ thuật của Tổ chức MASTERCARD
4	Bộ Tiêu chuẩn kỹ thuật của Tổ chức UPI