NAPAS

BỘ TIÊU CHUẨN KỸ THUẬT KẾT NỐI HỆ THỐNG ACH

Phần III: Hạ tầng, truyền thông và an toàn bảo mật

(Version 1.0)

CÔNG TY CỔ PHẦN THANH TOÁN QUỐC GIA VIỆT NAM

NAPAS

20-Apr-19

MỤC LỤC

LỊCH SỬ PHIÊN BẢN

Phiên bản	Ngày cập nhật	Người biên soạn	Người phê duyệt	Mô tả sự thay đổi
0.9	16/08/2018	Hà Nam Ninh Nguyễn Bảo Khánh	Nguyễn Hưng Nguyên	- Tạo file với các yêu cầu liên quan đến truyền thông, hạ tầng và an toàn bảo mật của dịch vụ trong hệ thống ACH đối với các thành viên - Cập nhật phần yêu cầu Hạ tầng. - Cập nhật phần yêu cầu đối với kết nối truyền thông
0.9.1	26/07/2018	Hà Nam Ninh Nguyễn Bảo Khánh	Nguyễn Hưng Nguyên	- Cập nhật phần yêu cầu về tuân thủ PCIDSS - Cập nhật nội dung liên quan đến tuyên bố tính mật của tài liệu.
0.9.2	11/08/2018	Hà Nam Ninh Nguyễn Bảo Khánh	Nguyễn Hưng Nguyên	- Cập nhật và tinh chỉnh nội dung sau khi việt hóa.
1.0	30/01/2019	Hà Nam Ninh Nguyễn Bảo Khánh	Nguyễn Hưng Nguyên	- Cập nhật thông tin liên quan đến mã hóa - Cập nhật thông tin liên quan đến chữ ký số của thông điệp

Yêu cầu bảo mật tài liệu

Thông tin trong tài liệu này là thông tin mật với Bên tiếp nhận và không được tiết lộ tới bất cứ Bên nào khác. Một phần hoặc toàn bộ hoặc bất cứ thông tin nào trong Tài liệu sẽ không được phép sao chép mà chưa có sự đồng ý trước của NAPAS. Bên tiếp nhận không được thu hút, lôi kéo sự tham gia của bất kỳ tổ chức hoặc cá nhân nào khác theo cách trực tiếp hoặc gián tiếp (cho dù thông qua bên đại diện hoặc bằng các cách khác) mà không có sự chấp thuận trước của cấp có thẩm quyền của NAPAS.

I. Mục đích

Tài liệu *"Bộ Tiêu chuẩn kỹ thuật kết nối Hệ thống ACH"* dành cho các Tổ chức thành viên của NAPAS, bao gồm tất cả các thành viên là Ngân hàng, Trung gian thanh toán được kết nối trực tiếp hoặc gián tiếp vào Hệ thống ACH.

II. Phạm vi

Tài liệu được ban hành với mục tiêu đưa ra các yêu cầu, qui định về hạ tầng, truyền thông và an toàn bảo mật cho các Tổ chức thành viên cần tuân thủ và đảm bảo khi triển khai các dịch vụ thuộc hệ thống ACH của NAPAS.

III. Hạ tầng

Liên quan đến các qui định về hạ tầng, các thành viên cần tuân thủ như sau:

- Đối với thành viên sử dụng mô hình chia sẻ (Shared Member Gateway) với số lượng giao dịch vừa phải, theo mô hình này thì NAPAS sẽ triển khai một hệ thống ứng dụng tại NAPAS để nhiều TCTV kết nối tới, chính vì vạy TCTV không triển khai bất cứ ứng dụng nào tại phía thành viên, vì vậy sẽ không đòi hỏi bất cứ yêu cầu nào liên quan đến hạ tầng mà thành viên phải chuẩn bị.

- Đối với thành viên sử dụng mô hình độc lập (Standalone member gateway), theo mô hình này thì mỗi TCTV, NAPAS sẽ triển khai tương ứng một ứng dụng Member Gateway dành riêng. Với định hướng triển khai tập trung về mặt ứng dụng tại NAPAS nên tùy thuộc vào sizing của từng thành viên (số người sử dụng, số lượng giao dịch/ngày,…), NAPAS sẽ chuẩn bị sẵn và phân bổ hạ tầng phần cứng (được dự tính) để cài đặt ứng dụng tương ứng cho TCTV nhằm đảm bảo hiệu năng như sau:

	5 concurrent users, 15.000 ppd (payment per day/transaction per day).	**50 concurrent users, 120.000 ppd.**	**200 concurrent users, 200.000 ppd.**
Application server			
Processor	Application is installed on DB server.	one six-core CPU	Two six-core CPUs
RAM		32 GB or higher	32 GB or higher
Hard Disk		2 x 300 GB SAS disks with 15K RPM (RAID 1	2 x 300 GB SAS disks with 15K RPM (RAID

		with 1GB BBWC / FBWC)	1 with 1GB BBWC / FBWC)
Operating System		Windows 2008 R2 Server or 2012 R2 SE x64 (64-bit) Standard Edition, Oracle Solaris, Red Hat Linux, IBM AIX	Windows 2008 R2 Server or 2012 R2 SE x64 (64-bit) Standard Edition, Oracle Solaris, Red Hat Linux, IBM AIX
DB server			
Processor	One Quad-Core CPU	One quad-core CPU	One quad-core CPU
RAM	32 GB or higher	24 GB or higher	24 GB or higher
Local Hard Disk	2 x 300 GB SAS disks with 15K RPM (RAID 1 with 1GB BBWC / FBWC)	4 x 300 GB SAS disks with 15K RPM (RAID 10 with 1GB BBWC / FBWC)	6 x 450 GB SAS disks with 15K RPM (RAID 10 with 1GB BBWC / FBWC)
DB growth per year	70GB	500GB	900GB
Operating System	Windows 2008 R2 or 2012 R2 SE x64 (64-bit), Oracle Solaris, Red Hat Linux, IBM AIX		
RDBMS software	Oracle XE (v. 11R2) Oracle Standard Edition Two (v. 12c) Oracle Enterprise Edition (v. 12c) Microsoft SQL server 2012 or higher Postgres SQL v. 9.2 or higher	Oracle Standard Edition Two (v. 12c) Oracle Enterprise Edition (v. 12c) Microsoft SQL server 2012 or higher Postgres SQL v. 9.2 or higher	Oracle Standard Edition Two (v. 12c) Oracle Enterprise Edition (v. 12c) Microsoft SQL server 2012 or higher Postgres SQL v. 9.2 or higher

IV. Kết nối truyền thông

Để khởi tạo kết nối truyền thông với NAPAS đối với dịch vụ thuộc hệ thống ACH, các tổ chức thành viên cần triển khai các kết nối với các lưu ý như sau:

- Thành viên kết nối gián tiếp sẽ kết nối tới thành viên kết nối trực tiếp và sử dụng đường kết nối truyền thông của thành viên kết nối trực tiếp trong kết nối với hệ thống ACH.
- Đối với thành viên kết nối trực tiếp (với cả thành viên sử dụng Mô hình sử dụng Member Gateway chia sẻ (Shared) hoặc độc lập (Standalone):
    - Nếu thành viên đã kết nối với NAPAS với dịch vụ chuyển mạch hoặc chuyển tiền đang có, NAPAS và thành viên sẽ sử dụng đường kết nối truyền thông đang có sẵn để truyền và xử lý các giao dịch qua hệ thống ACH.
    - Nếu thành viên không có kết nối với dịch vụ chuyển mạch và chuyển tiền của NAPAS đang có, NAPAS đề nghị quý thành viên để triển khai kết nối truyền thông theo các yêu càu được đòi hỏi trong mục "Yêu cầu truyền thông" và "Thông tin kết nối mạng" bên dưới để có thể xử lý và chuyển tiếp các giao dịch ACH.

1. Yêu cầu truyền thông

Để đảm bảo duy trì hoạt động 24/7 của dịch vụ ACH và các dịch vụ khác giữa NAPAS với Thành viên, hiện NAPAS đang áp dụng sử dụng 02 đường truyền để kết nối với mỗi Thành viên. 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 Thành viên: 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 Thành viên: Yêu cầu địa điểm đặt thiết bị phía Thành viên 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 Thành viên, sau khi đã phối hợp cấu hình để đưa đường truyền vào sử dụng phía Thành viên sẽ có trách nhiệm kiểm tra đường truyền định kỳ và chịu trách nhiệm về đường truyền từ phía Thành viên tới đầu Router đặt tại phía NAPAS. Khi có sự cố xảy ra NAPAS sẽ cùng phối hợp với các cán bộ phía Thành viên để xử lý.

2. Thông tin kết nối mạng

Thành viên 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

V. An toàn bảo mật

1. Quy định về đảm bảo tuân thủ PCIDSS

Để đảm bảo về bảo mật thông tin dữ liệu chủ thẻ, hệ thống của NAPAS và Thành viên 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

2. Mã hóa, xác thực thành viên và chữ ký số của thông điệp

2.1 Mã hóa

Ngoài việc các thông điệp được mã hóa ở mức hạ tầng truyền thông, NAPAS cũng triển khai thêm phần mã hóa ở mức ứng dụng thông qua giao thức https (SSL) ở tầng transport. Việc triển khai mã hóa SSL cũng giúp NAPAS đáp ứng tuân thủ các yêu cầu của PCIDSS trong bảo mật các dữ liệu được trao đổi giữa các bên.

2.2 Xác thực thành viên

Trước khi TCTV có thể gửi và nhận các thông điệp liên quan đến tài chính tới hệ thống ACH của NAPAS, TCTV cần gửi một thông điệp đến ACH để xác thực thành viên, sau đó hệ thống ACH sẽ tạo mã truy cập (Token) và gửi lại cho TCTV. Bất cứ các giao dịch nào gửi đi từ phía TCTV phải gắn thêm mã truy cập (Token) này trong phần "Authorization header" (sử dụng lược đồ Bearer - JWT token based on RFC7159).

Các giao tiếp giữa hệ thống ACH của NAPAS và TCTV dựa trên chuẩn MX (ISO 20022) theo kiểu định dạng dữ liệu là JSON, vì vậy NAPAS và TCTV sẽ triển khai xác thực bằng JSON Web Token (viết tắt là JWT). Chi tiết quy định về việc xác thực thành viên tham khảo tài liệu "Phần 2: Định dạng thông điệp" trong Bộ tiêu chuẩn kỹ thuật của hệ thống ACH, tại mục "4.1 Thông điệp xác thực thành viên (REST API Authentication)).

2.3 Chữ ký số của thông điệp

Để đảm bảo tính toàn vẹn và chống trối cãi đối với các giao dịch được gửi giữa NAPAS và các TCTV, các bên sẽ triển khai áp dụng việc ký số và gắn kèm chữ ký vào trong thông điệp trước khi gửi đi.

Dựa trên kiểu định dạng dữ liệu JSON được trao đổi giữa các bên, NAPAS và các TCTV triển khai chữ ký web JSON (JWS).

Chi tiết qui định về chữ ký JWS được qui định trong tài liệu "Phần 2: Định dạng thông điệp" trong Bộ tiêu chuẩn kỹ thuật của hệ thống ACH, tại mục "Phụ lục A: Bảo mật dữ liệu"

3. Hạ tầng PKI (PKI Infrastructure)

3.1 Khái niệm hạ tầng PKI

Cơ sở của hạ tầng khoá công khai là sử dụng các thuật toán khóa không đối xứng: khoá được sử dụng để mã hóa một thông điệp không giống với khóa được sử dụng để giải mã. Mỗi người dùng có một cặp khóa mã hóa - một khóa công cộng (public key) và một khóa riêng (private key). Khóa riêng được giữ bí mật, trong khi khóa công khai có thể được phân phối rộng rãi.

Dữ liệu trao đổi được mã hóa bằng khóa công khai của người nhận và chỉ có thể được giải mã bằng khóa riêng tương ứng. Các khóa này có liên quan về mặt toán học, nhưng khóa riêng không thể được suy ra với các thông tin có được từ khóa công khai.

Mã hóa khóa công khai được sử dụng cho hai mục đích chính như sau:

- Chữ ký số (Digital signatures) – một thông điệp được ký với khóa riêng của người gửi thì có thể được xác minh bởi bất cứ ai người có quyền truy cập hoặc có khóa công khai, và phần thông tin của thông điệp đó thì không bị giả mạo sau khi được ký. Chữ ký số được sử dụng với mục đích chính là xác thực người gửi (authentication) và trống chối bỏ (non-repudiation).
- Mã hóa khóa công khai (public key encryption) – thông điệp được mã hóa bằng khóa công khai của người nhận không thể được giải mã bởi bất kỳ ai ngoại trừ người sở hữu khóa riêng, đây sẽ là chủ sở hữu của khóa riêng đó và là người được liên kết cặp khóa với khóa công khai được sử dụng để mã hóa. Mã hóa hóa công khai được sử dụng để đảm bảo tính mật của dữ liệu.

3.2 Yêu cầu về hạ tầng PKI đối với thành viên

Các thành phần được đòi hỏi đối với ứng dụng Member Gateway trong việc cung cấp hạ tầng khóa công khai (PKI) tới người dùng của thành viên như sau:

- Truy cập tới khu vực lưu trữ khóa riêng của người sử dụng trong kết nối giữa ACH và Member gateway (tức người gửi thông điệp)

- Truy cập tới khu vực lưu trữ với chứng thư khóa công khai của các người dùng khác trong hệ thống ACH cũng như khu vực lưu trữ các chứng thư bị thu hồi (CRLs). Các dữ liệu này có thể được đặt cục bộ (offline storage – Java KeyStore) hoặc truy cập trực tiếp tới LDAP server (thông qua kết nối giữa NAPAS và thành viên).

    - Trong trường hợp của việc sử dụng lưu trữ cục bộ (local), điều này đòi hỏi các hoạt động với thao tác người dùng trong việc xuất các danh mục (export items) từ dữ liệu được lưu trữ online và nhập vào trong khu vực offline cục bộ. Các CRL file cũng được xuất thủ công và được phân phối cho các ứng dụng của thành viên (member gateway).

    - Cấp phát các chứng thư CA có sẵn để lưu cục bộ (bao gồm tất cả các chứng thư sub-CA)

Hiệu lực pháp lý

1. *Tài liệu này là một phần không tách rời và đính kèm theo Hợp đồng nguyên tắc Tổ chức thành viên tham gia Hệ thống ACH số ……. ký ngày …./…./…… giữa Công ty Cổ phần Thanh toán Quốc gia Việt Nam và Ngân hàng ……..*
2. *Tài liệu này có giá trị pháp lý áp dụng bắt buộc đối với NAPAS và TCTV.*
3. *Những nội dung chưa được đề cập trong Tài liệu này được thực hiện theo quy định tại Hợp đồng nguyên tắc Tổ chức thành viên tham gia Hệ thống ACH nêu trên.*
4. *Tài liệu này có hiệu lực kể từ ngày ……..và có thời hạn hiệu lực theo Hợp đồng nguyên tắc Tổ chức thành viên tham gia Hệ thống ACH, trừ khi các bên có thỏa thuận khác.*