

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
BỘ MÔN KHOA HỌC MÁY TÍNH

-----o0o-----



ĐỒ ÁN MÔN HỌC

SECURE ELECTRONIC TRANSACTION

GVHD: PGS.Nguyễn Linh Giang

SVTH:

Nguyễn Hoàng Thuận MSSV: 20173933

Nguyễn Minh Hiếu MSSV: 20173115

Nguyễn Thế Đức MSSV: 20170057

Nguyễn Đức Anh MSSV: 20172937

TP. HÀ NỘI, THÁNG NĂM 20....

Mục lục

Mở đầu	3
CHƯƠNG 1: NHỮNG KHÁI NIỆM CẦN BIẾT	4
Chương 2. Mật mã sử dụng trong SET	5
2.1 Các phương pháp mã hoá.....	5
2.2 Chữ ký số	6
2.3 Chứng chỉ.....	7
2.4 Tóm tắt quá trình mã hoá.....	7
2.4.1 Mã hoá.....	8
2.4.2 Giải mã	9
2.5 Chữ ký kép	9
2.6 Chứng chỉ của các bên tham gia	10
2.6.1 Chứng chỉ chủ thẻ.....	10
2.6.2 Chứng chỉ người bán.....	10
2.6.3 Chứng chỉ công thanh toán	11
2.6.4 Chứng chỉ Acquirer	11
2.6.5 Chứng chỉ Issuer	11
2.7 Phân cấp tin cậy	11
Chương 3. Quy trình thanh toán	13
3.1 Tổng quan	13
3.2 Đăng ký chủ thẻ	17
Quá trình cơ quan cấp chứng chỉ nhận yêu cầu và gửi mẫu đăng ký.....	21
Chủ thẻ nhận chứng chỉ	25
3.3 Đăng kí người bán	25
CA xử lý yêu cầu và gửi mẫu đăng ký	26
3.5 Ủy quyền giao dịch	34
3.6 Ghi nhận thanh toán	37
Tài liệu tham khảo.....	41

Mở đầu

Trong thời đại công nghệ số được phổ cập rộng rãi hiện nay, sức mạnh của Internet được thể hiện rõ rệt. Thật vậy, nó hiện hữu và được ứng dụng trong rất nhiều lĩnh vực như: giáo dục, truyền thông và trong đó không thể không nói đến thương mại. So với cách giao dịch truyền thống trước đây, mọi thứ được thực hiện qua hình thức mặt đối mặt, một hình thức thủ công và tốn thời gian; để đáp ứng một số lượng lớn giao dịch, giao dịch điện tử đã xuất hiện và tác động mạnh mẽ đến nền công nghiệp dịch vụ tài chính. Cụ thể đó là, rất nhiều ngân hàng ứng dụng công nghệ số, yêu cầu xác thực thẻ trên mạng. Như vậy, Internet đã thay đổi cách chúng ta giao dịch, mua bán. Điều này kéo theo những dịch vụ tài chính như thành toán, bảo hành, công nợ cũng phải thay đổi, đó là khả năng mọi người phải sử dụng được những dịch vụ đó trên Internet.

Song song với những đổi mới và lợi ích do sức mạnh của Internet mang lại, những vấn đề mới xuất hiện và đầy thách thức. Đó là sự xuất hiện những hình thức lừa đảo, mạo danh và tấn công đánh cắp tài sản của người sử dụng - sự tin cậy trên một mạng lưới công khai. Do đó tính an toàn và bảo mật là một trong những mảng quan trọng của thương mại điện tử. Bên cạnh đó, xuất hiện những nhu cầu về phương thức giao dịch trên mạng phải tương đương với những phương thức thanh toán mặt đối mặt. Tuy việc sử dụng tiền mặt trong buôn bán điện tử là có thể, nhưng phần lớn người mua bán đều sử dụng phương thức thanh toán điện tử qua thẻ thanh toán. Do đó hệ thống thanh toán đảm nhiệm một vai trò quan trọng. Nó phải cung cấp tính bảo mật cho vận chuyển, xác thực các bên liên quan như chủ thẻ, thương nhân v.v, bảo đảm tính toàn vẹn của thông tin.

SET là viết tắt của Secure Electronic Transaction (Bảo đảm giao dịch điện tử) là một phương thức sử dụng mã hóa giải mã, nhằm đáp ứng những nhu cầu cũng như giải quyết những vấn đề đã đề cập. Nó cung cấp tính bảo mật cho thông tin, đảm bảo tính toàn vẹn trong thanh toán và xác thực cả thương nhân - bên bán - lẫn chủ thẻ.

SET xuất hiện mang lại những lợi ích được coi là động lực cho thương hiệu thẻ thanh toán phát triển: khuyến khích cộng đồng thẻ thanh toán lấy vị trí đứng đầu trong việc thiết lập những đặc tả về bảo đảm thanh toán, giữ sự tin tưởng, duy trì mối quan hệ giữa bên bán và ngân hàng thương nhân, hay bên chủ thẻ và bên cung cấp thẻ thanh toán, hồi đáp nhanh chóng những nhu cầu về dịch vụ tài chính trên mạng và bảo vệ tính toàn vẹn của những thương hiệu thẻ thanh toán.

SET cũng có những yêu cầu nghiệp vụ chính như: cung cấp tính bảo mật cho thông tin thanh toán và cho phép bảo mật thông tin đặt hàng trong lúc vận chuyển cùng với thông tin thanh toán; bảo đảm tính toàn vẹn cho tất cả dữ liệu được vận chuyển; cung cấp sự xác thực để biết chủ thẻ là một người dùng hợp lệ của thẻ dưới một thương hiệu thẻ thanh toán nào đó; tương tự là cung cấp tính xác thực cho thương nhân đối với ngân hàng thương nhân; sử dụng những quy ước an ninh tốt nhất và kỹ thuật thiết kế hệ thống để bảo vệ tất cả các bên hợp lệ trong một giao dịch thương mại điện tử; tạo những phương thức mà không cần phụ thuộc vào cả các cơ chế an ninh vận chuyển cũng như xung khắc với chúng; tạo điều kiện thúc đẩy khả năng tương của phần mềm và nhà mạng.

CHƯƠNG 1: NHỮNG KHÁI NIỆM CẦN BIẾT

Các bên tham gia có trong một hệ thống thanh toán:

Giao dịch trong thương mại điện tử bao gồm nhiều sự tương tác trực tiếp lẫn gián tiếp, trong đó có: người sở hữu thẻ - chủ thẻ, Ngân hàng phát hành, người bán, ngân hàng thu thập, cổng thanh toán, thương hiệu của tổ chức chính và bên thứ ba. Trong SET, người khởi đầu một quy trình trong giao dịch là chủ thẻ. Để thêm minh bạch, dưới đây là một số giải thích khái niệm về các thành phần trong một hệ thống thanh toán.

Chủ thẻ (Card Holder): Trong giao dịch thương mại điện tử, người chủ thẻ là người sử dụng những dịch vụ do bên bán hàng cung cấp, hay là người mua những hàng hóa từ máy tính cá nhân. Người chủ thẻ sử dụng thẻ thanh toán được ủy nhiệm từ Ngân hàng phát hành. Đối với chủ thẻ, SET có nhiệm vụ giữ sự bảo mật cho những mối liên hệ, tương tác với người bán và cả thông tin thanh toán từ tài khoản người dùng.

Ngân hàng phát hành thẻ (Issuer): Là một tổ chức tài chính, có nhiệm vụ phát hành thẻ và xây dựng một tài khoản cho chủ thẻ. Ngân hàng phát hành thẻ bảo đảm rằng, những giao dịch đã được xác thực sử dụng những thẻ thanh toán được cung cấp, phải tuân theo những quy tắc của tổ chức nói riêng và của pháp luật nói chung.

Người bán (Merchant): Là bên cung cấp dịch vụ, rao bán sản phẩm. Ứng dụng SET, bên bán có thể cung cấp cho khách hàng của họ những giao dịch điện tử an toàn. Bên bán chỉ có thể tiếp nhận thẻ thanh toán của khách hàng khi đã có một bên thu nhận nào đó.

Bên thu nhận (Acquirer): bên thu nhận được coi như là ngân hàng thương nhân (merchant bank), có nhiệm vụ chấp nhận những giao dịch tài chính, hay xử lý những vấn đề liên quan đến tài chính. Khi đã tồn tại mối quan hệ (hợp đồng) với bên bán, bên bán có thể tiếp nhận những giao dịch có sử dụng thẻ thanh toán như tín dụng và ghi nợ.

Cổng thanh toán (Payment gateway): là một phương tiện hay chương trình phần mềm được vận hành bởi bên thu nhận, nó có nhiệm vụ xử lý những thông tin giao dịch như cho phép vận chuyển dữ liệu giao dịch từ trình duyệt của người bán sang trung tâm thẻ tín dụng.

Thương hiệu ngân hàng (Brand): Mỗi ngân hàng được thành lập phải có một danh tính riêng, những thương hiệu riêng tương ứng với những tính chất, quy tắc riêng lên thẻ thanh toán của từng ngân hàng, tên thương hiệu của mỗi ngân hàng còn giúp cung cấp mạng lưới liên kết giữa các tổ chức tài chính.

Bên thứ ba: Bên ngân hàng phát hành thẻ và ngân hàng thương gia có thể giao việc xử lý những giao dịch qua thẻ thanh toán cho một bên thứ ba nào đó.

Chương 2. Mật mã sử dụng trong SET

2.1 Các phương pháp mã hoá

Trong giao dịch thương mại điện tử, SET có nhiệm vụ bảo mật thông tin giao dịch được vận chuyển giữa các bên liên quan và bảo mật thông tin tài khoản. Để thực hiện những nhiệm vụ như vậy, SET phải áp dụng những phương pháp mật mã để bảo vệ những thông tin nhạy cảm. Cụ thể là một thông điệp cần bảo mật sẽ được mã hóa bằng cách sử dụng một khóa nào đó, văn bản được mã hóa sẽ được chuyển đến bên nhận; bên nhận sử dụng một khóa để giải mã lấy ra thông tin ban đầu. SET sử dụng cả 2 phương pháp mã hóa nổi bật, đó là: phương pháp mã hóa sử dụng khóa đối xứng và phương pháp sử dụng khóa công khai.

Phương pháp sử dụng khóa đối xứng: phương pháp này, cả bên gửi và bên nhận đều sử dụng chung một khóa nhằm thực hiện cả hai công việc - mã hóa và giải mã. Khóa này sẽ được giữ bí mật để bảo đảm tính bảo mật của thông tin. Trong SET, các bên tổ chức tài chính sử dụng thuật toán mã hóa giải mã khóa đối xứng DES (Data Encryption Standard) để giấu thông tin PIN (Personal Identification Numbers)

Phương pháp sử dụng khóa công khai: trái ngược với phương pháp trên, trong quá trình gửi thông điệp, việc mã hóa – giải mã sử dụng 2 khóa: khóa để mã hóa và khóa để giải mã, tương ứng với khóa công khai và khóa riêng khi muốn bảo mật thông điệp và ngược lại khi muốn xác thực thông tin. Để đảm bảo tính bảo mật, người sử dụng giữ bí mật khóa giải mã, trong khi đó khóa còn lại để mã hóa vẫn được công khai. Điều kiện trên chỉ thỏa mãn khi người sử dụng tự tạo ra cả 2 khóa. SET sử dụng thuật toán mã hóa – giải mã khóa công khai RSA trong phương pháp này.

Dựa sơ đồ quan hệ giữa các bên tham gia của SET, việc sử dụng đồng thời cả hai phương pháp mã hóa giải mã trên là hợp lý. Thật vậy, giữa quan hệ giữa bên bán và bên mua (những chủ thể) là những quan hệ từ một đến nhiều người. Để đảm bảo tính bảo mật thông tin trong một ngữ cảnh như vậy, việc sử dụng khóa đối xứng sẽ là bất hợp lý do phải tạo rất nhiều khóa cho từng khách hàng. Thay vào đó việc sử dụng duy nhất một khóa công khai trong phương pháp khóa bất đối xứng thì rất hợp lý mà vẫn có thể đảm bảo tính bảo mật thông tin giao dịch.

Một số đặc điểm tính chất của các khóa:

- Mỗi quan hệ giữa 2 cặp khóa mật và công khai: Khi 2 bên muốn trao đổi thông điệp một cách bảo mật, mỗi người sử dụng một phần trong 2 cặp khóa mật và công khai. Người gửi muốn bảo mật thông điệp, sẽ sử dụng khóa công khai để mã hóa do bên nhận cung cấp. Bên nhận là người giữ khóa mật để giải mã lấy ra thông tin ban đầu. Do chỉ có khóa mật mới có thể giải mã được văn bản mã hóa bởi khóa còn lại, chừng nào bên nhận giữ bí mật khóa giải mã, thông tin sẽ được bảo mật kể cả khi được trao đổi trên một mạng lưới không an toàn.

- Tác dụng, cách sử dụng khóa đối xứng: SET dựa vào cơ chế mã hóa giải mã để bảo mật thông tin trao đổi. Trong SET, dữ liệu sẽ được mã hóa nhờ một khóa đối xứng được tạo ngẫu nhiên. Sau đó khóa này sẽ được mã hóa bởi một khóa công khai của bên nhận (RSA) để không cho bên thứ 3 biết. Hình thức này giống như việc trao đổi một “phong bao điện tử” che giấu thông tin cần bảo mật. Sau khi bên nhận nhận được “phong bao điện tử”, họ sử dụng khóa mật để mở thư và lấy ra khóa đối xứng, sử dụng nó để mã hóa thông tin ban đầu. Điều này có ích khi muốn gửi từ một bên cho nhiều người nhận, mà không muốn không ai khác biết nội dung thông tin trao đổi của từng cặp người nhận và gửi.

2.2 Chữ ký số

Tính toàn vẹn và xác thực được đảm bảo bằng việc sử dụng chữ ký số.

Mối quan hệ của các khóa: Do mối quan hệ toán học giữa khóa công khai và khóa riêng, dữ liệu được mã hóa với một trong hai khóa chỉ có thể được giải mã với khóa kia. Điều này cho phép người gửi thông điệp mã hóa nó bằng khóa riêng của người gửi. Bất kỳ người nhận nào cũng có thể xác định rằng thông điệp đến từ người gửi bằng cách giải mã tin nhắn bằng khóa công khai của người gửi. Ví dụ: Alice có thể mã hóa một phần dữ liệu đã biết, chẳng hạn như số điện thoại của cô ấy, với khóa riêng của cô ấy và gửi nó cho Bob. Khi Bob giải mã thông điệp bằng cách sử dụng khóa công khai của Alice và so sánh kết quả với dữ liệu đã biết, anh ta có thể chắc chắn rằng thông điệp chỉ có thể được mã hóa bằng khóa riêng của Alice.

Sử dụng message digests (MD): Khi được kết hợp với *message digests*, mã hóa sử dụng khóa riêng cho phép người dùng ký điện tử thông điệp. Message digests là một giá trị được tạo cho một thông điệp (hoặc tài liệu), nó là duy nhất cho thông điệp đó. Message digests được tạo bằng cách đưa thông điệp qua một hàm mã hóa một chiều; đó là một thứ không thể đảo ngược. Khi mà message digests của thông điệp được mã hóa bằng khóa riêng của người gửi và được thêm vào tin nhắn gốc, kết quả được gọi là chữ ký số của tin nhắn. Người nhận chữ ký số có thể chắc chắn rằng tin nhắn thực sự đến từ người gửi. Và bởi vì thay đổi ngay cả một ký tự trong thông điệp cũng thay đổi message digests theo một cách không thể đoán trước, người nhận có thể chắc chắn rằng thông điệp không bị thay đổi sau khi message digests đã được tạo.

Thuật toán được sử dụng bởi SET tạo ra các message digests 160 bit. Nếu mà thay đổi một bit trong thông điệp, trung bình sẽ thay đổi một nửa số bit trong phần message digests. Ước tính, tỷ lệ của hai tin nhắn có cùng message digests là một phần 1.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000. Việc tính toán hai thông điệp khác nhau có cùng message digest là không khả thi.

Ví dụ về việc sử dụng chữ ký số: Alice tính toán message digest của một thông điệp và mã hóa nó với khóa riêng của cô ấy tạo ra một chữ ký số cho thông điệp. Cô ấy truyền cả thông điệp và chữ ký số cho Bob. Khi Bob nhận được tin nhắn, anh ta tính toán message digest của thông điệp và giải mã chữ ký số với khóa công khai của Alice. Nếu hai giá trị khớp nhau, Bob

biết rằng thông điệp đã được ký bằng khóa riêng của Alice và nó đã không thay đổi kể từ khi được ký.

Hai cặp khóa: SET sử dụng cặp khóa công khai / riêng để tạo chữ ký số. Như vậy, mỗi người tham gia SET sẽ sở hữu hai cặp khóa bất đối xứng: một cặp “khóa trao đổi”, được sử dụng trong quá trình mã hóa và giải mã, và một cặp “chữ ký” để tạo và xác minh chữ ký số. Lưu ý rằng vai trò của khóa chung và khóa riêng bị đảo ngược trong quy trình ký số trong đó khóa riêng được sử dụng để mã hóa (ký) và khóa chung được sử dụng để giải mã (xác minh chữ ký).

2.3 Chứng chỉ

Tính xác thực được tăng cường hơn nữa bằng cách sử dụng các chứng chỉ.

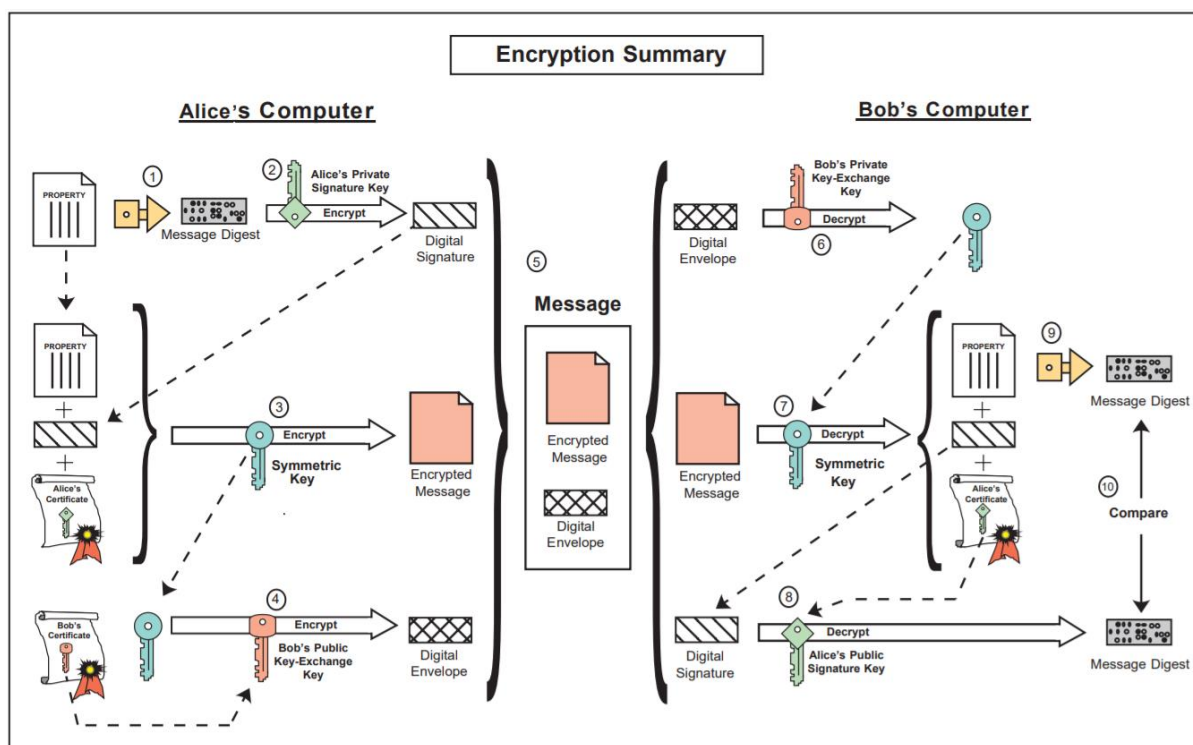
Nhu cầu xác thực: Trước khi hai bên sử dụng mật mã khóa công khai để tiến hành trao đổi thông tin, mỗi bên muốn chắc chắn rằng bên kia được xác thực. Trước khi Bob chấp nhận một tin nhắn với chữ ký số của Alice, anh ta muốn chắc chắn rằng khóa công khai thuộc về Alice chứ không phải của ai đó giả dạng Alice trên một mạng mở. Một cách để chắc chắn rằng khóa công khai thuộc về Alice là nhận nó qua một kênh an toàn trực tiếp từ Alice. Tuy nhiên, trong hầu hết trường hợp giải pháp này là không thực tế.

Cần có một bên thứ ba tin cậy: Một cách khác để truyền khóa an toàn là sử dụng bên thứ ba đáng tin cậy để xác thực khóa công khai thuộc về Alice. Một bên như vậy được gọi là Cơ quan cấp chứng chỉ (CA). Cơ quan cấp chứng chỉ xác thực các yêu cầu của Alice theo các chính sách được công bố. Ví dụ, Tổ chức phát hành chứng chỉ có thể cung cấp các chứng chỉ mang lại sự đảm bảo cao về danh tính cá nhân, có thể được yêu cầu để thực hiện các giao dịch kinh doanh; Cơ quan cấp chứng chỉ có thể yêu cầu Alice xuất trình giấy phép lái xe hoặc hộ chiếu cho công chứng viên công khai trước khi nó sẽ cấp giấy chứng nhận. Khi Alice đã cung cấp bằng chứng về danh tính của mình, Cơ quan cấp chứng chỉ tạo một thông điệp chứa tên của Alice và khóa công khai của cô ấy. Thông điệp này được gọi là chứng chỉ, được ký số bởi của Cơ quan cấp chứng chỉ. Nó chứa thông tin nhận dạng chủ sở hữu, cũng như bản sao của một trong các khóa công khai của chủ sở hữu (khóa trao đổi hay chữ ký). Để có được lợi ích cao nhất, khóa công khai của Cơ quan cấp chứng chỉ nên được biết đến với càng nhiều người càng tốt. Do đó, bằng cách tin tưởng vào một khóa duy nhất, toàn bộ hệ thống phân cấp có thể được thiết lập trong đó người ta có thể có mức độ tin cậy cao. Bởi vì những người tham gia SET có hai cặp khóa, họ cũng có hai chứng chỉ. Cả hai chứng chỉ được tạo và ký cùng lúc bởi Cơ quan cấp chứng chỉ.

Xác thực trong SET: Có nghĩa là phương thức mà các tổ chức tài chính sử dụng để xác thực chủ thẻ hoặc người bán không được đặc tả ở đây. Mỗi thương hiệu thẻ thanh toán và tổ chức tài chính sẽ chọn một phương pháp phù hợp.

2.4 Tóm tắt quá trình mã hoá

Sơ đồ sau cung cấp tổng quan về toàn bộ quá trình mã hóa khi Alice muốn ký, ví dụ, một mô tả tài sản và gửi nó trong một tin nhắn được mã hóa cho Bob. Các bước được đánh số trong sơ đồ được giải thích ở các trang sau.



Hình 1. Tổng quan quản trị mã hoá và giải mã

2.4.1 Mã hoá

Quá trình mã hóa trong Hình 1 bao gồm các bước sau:

Bước	Mô tả
1	Alice đưa mô tả tài sản thông qua thuật toán một chiều để tạo ra một giá trị duy nhất được gọi là message digest. Đây là một loại dấu vân tay kỹ thuật số của mô tả thuộc tính và sẽ được sử dụng sau này để kiểm tra tính toàn vẹn của tin nhắn.
2	Sau đó, cô mã hóa message digest bằng khóa chữ ký riêng của mình để tạo ra chữ ký số.
3	Tiếp theo, cô tạo một khóa đối xứng ngẫu nhiên và sử dụng nó để mã hóa mô tả thuộc tính, chữ ký của cô ấy và một bản sao giấy chứng nhận của cô ấy, trong đó chứa khóa công khai chữ ký của cô ấy. Để giải mã mô tả thuộc tính, Bob sẽ yêu cầu một bản sao an toàn của khóa đối xứng ngẫu nhiên này.
4	Alice phải có được chứng chỉ của Bob trước khi bắt đầu liên lạc bảo mật với anh ta, chứa một bản sao của khóa trao đổi công khai của anh ta. Để đảm bảo truyền khóa đối xứng an toàn, Alice mã hóa nó bằng cách sử dụng khóa trao đổi công khai của Bob. Khóa được mã hóa, được gọi là phong bì kỹ thuật số, sẽ được gửi đến Bob cùng với chính thông điệp được mã hóa.
5	Alice gửi tin nhắn cho Bob bao gồm những điều sau đây: mô tả thuộc tính, chữ ký và chứng chỉ được mã hóa đối xứng, cũng như Khóa đối xứng được mã hóa bất đối xứng (phong bì kỹ thuật số).

2.4.2 Giải mã

Tương tự, quá trình giải mã bao gồm các bước sau:

Bước	Mô tả
6	Bob nhận được tin nhắn từ Alice và giải mã phong bì kỹ thuật số bằng khóa trao đổi riêng của anh ta để lấy khóa đối xứng.
7	Anh ta sử dụng khóa đối xứng để giải mã mô tả thuộc tính, chữ ký Alice, và chứng chỉ của cô ấy.
8	Anh ta giải mã chữ ký số của Alice bằng khóa chữ ký công khai của cô ấy, mà anh ta có được từ chứng chỉ của cô. Điều này phục hồi message digest của mô tả thuộc tính.
9	Anh ta chạy mô tả thuộc tính thông qua thuật toán một chiều như được Alice sử dụng và tạo ra một message digest mới về mô tả thuộc tính được giải mã.
10	<p>Cuối cùng, anh so sánh message digest của mình với message digest thu được từ chữ ký số của Alice. Nếu chúng giống hệt nhau, anh xác nhận rằng nội dung tin nhắn đã không bị thay đổi trong quá trình truyền và nó đã được ký bằng cách sử dụng chữ ký khóa riêng của Alice.</p> <p>Nếu chúng không giống nhau, thì tin nhắn hoặc có nguồn gốc ở một nơi khác hoặc đã bị thay đổi sau khi nó được ký. Trong trường hợp đó, Bob thực hiện một số hành động thích hợp như thông báo cho Alice hoặc loại bỏ tin nhắn.</p>

2.5 Chữ ký kép

SET giới thiệu một ứng dụng mới về chữ ký số, cụ thể là khái niệm chữ ký kép. Để hiểu sự cần thiết của khái niệm mới này, hãy xem xét kịch bản sau đây:

Bob muốn gửi cho Alice lời đề nghị mua một phần tài sản và ủy quyền cho ngân hàng của anh ta để chuyển tiền nếu Alice chấp nhận lời đề nghị, nhưng Bob không muốn ngân hàng xem các điều khoản của đề nghị cũng không muốn Alice xem thông tin tài khoản của mình. Hơn nữa, Bob muốn liên kết đề nghị với việc chuyển khoản để tiền chỉ được chuyển nếu Alice chấp nhận phục vụ. Anh ta hoàn thành tất cả những điều này bằng cách ký điện tử cả hai tin nhắn bằng một thao tác chữ ký duy nhất tạo ra một chữ ký kép.

Tạo một chữ ký kép: Một chữ ký kép được tạo bằng cách tạo ra message digest của cả hai tin nhắn, nối hai message digest với nhau, tính toán message digest của kết quả và mã hóa phần tóm tắt này với chữ ký riêng của người ký. Người ký phải thêm vào message digest của tin nhắn khác để người nhận xác minh chữ ký kép. Người nhận của một trong hai tin nhắn có thể kiểm tra tính xác thực của nó bằng cách tạo message digest trên bản sao của tin nhắn, nối nó với message

digest của tin nhắn khác (do người gửi cung cấp) và tính toán message digest kết quả. Nếu message digest mới được tạo ra phù hợp với chữ ký kép được giải mã, người nhận có thể tin tưởng vào tính xác thực của tin nhắn.

Ví dụ: Nếu Alice chấp nhận lời đề nghị của Bob, cô ấy có thể gửi tin nhắn đến ngân hàng cho biết sự chấp nhận của cô ấy và bao gồm cả message digest về lời đề nghị. Ngân hàng có thể xác minh tính xác thực của ủy quyền chuyển nhượng Bob, và đảm bảo rằng sự chấp nhận dành cho cùng một lời đề nghị bằng cách sử dụng bản tóm tắt ủy quyền và bản tóm tắt thông báo do Alice cung cấp để xác thực chữ ký kép. Do đó, ngân hàng có thể kiểm tra tính xác thực của lời đề nghị đối với chữ ký kép, nhưng ngân hàng không thể thấy các điều khoản của đề nghị.

Sử dụng chữ ký kép: Trong SET, chữ ký kép được sử dụng để liên kết một thông điệp đặt hàng được gửi đến người bán với các hướng dẫn thanh toán có chứa thông tin tài khoản được gửi đến Acquirer. Khi người bán gửi yêu cầu ủy quyền cho Acquirer, nó bao gồm các hướng dẫn thanh toán được gửi bởi chủ thẻ và message digest về thông tin đặt hàng. Bên mua sử dụng message digest từ người bán và tính toán message digest hướng dẫn thanh toán để kiểm tra chữ ký kép.

2.6 Chứng chỉ của các bên tham gia

2.6.1 Chứng chỉ chủ thẻ

Chứng chỉ chủ thẻ có chức năng như một đại diện điện tử của thẻ thanh toán. Bởi vì chúng được ký số bởi một tổ chức tài chính, chúng không thể bị thay đổi bởi bên thứ ba và chỉ có thẻ được tạo bởi một tổ chức tài chính. Chứng chỉ chủ thẻ không chứa số tài khoản và ngày hết hạn. Thay vào đó, thông tin tài khoản và giá trị bí mật chỉ được biết đến bởi phần mềm của chủ thẻ được mã hóa bằng thuật toán băm một chiều. Nếu số tài khoản, ngày hết hạn và giá trị bí mật được biết, liên kết đến chứng chỉ có thể được chứng minh, nhưng thông tin không thể được lấy bằng cách xem chứng chỉ. Trong giao thức SET, chủ thẻ cung cấp thông tin tài khoản và giá trị bí mật cho cổng thanh toán nơi liên kết được xác minh.

Chứng chỉ chỉ được cấp cho chủ thẻ khi tổ chức tài chính phát hành của chủ thẻ phê duyệt nó. Bằng cách yêu cầu chứng chỉ, chủ thẻ đã chỉ ra ý định thực hiện thương mại thông qua các phương tiện điện tử. Giấy chứng nhận này được truyền tới các thương nhân với yêu cầu mua hàng và hướng dẫn thanh toán được mã hóa. Khi nhận được chứng nhận của chủ thẻ, tối thiểu, một thương gia có thể được đảm bảo rằng số tài khoản đã được xác nhận bởi tổ chức tài chính phát hành thẻ hoặc đại lý của nó.

Trong phần đặc tả này, chứng chỉ chủ thẻ là tùy chọn theo quyết định của thương hiệu thẻ thanh toán.

2.6.2 Chứng chỉ người bán

Chứng chỉ người bán có chức năng thay thế điện tử cho nhãn hiệu thanh toán xuất hiện trong cửa sổ cửa hàng. Bản thân nhãn hiệu là một đại diện cho thương gia có mối quan hệ với một tổ chức

tài chính cho phép nó chấp nhận thương hiệu thẻ thanh toán. Bởi vì chúng được ký số bởi tổ chức tài chính của người bán, nên chứng chỉ người bán không thể được thay đổi bởi bên thứ ba và chỉ có thể được tạo bởi một tổ chức tài chính.

Các chứng chỉ này được chấp thuận bởi tổ chức tài chính của người bán và đảm bảo rằng người bán giữ một thỏa thuận hợp lệ với một Acquirer. Một người bán phải có ít nhất một cặp chứng chỉ để tham gia vào môi trường SET, nhưng có thể có nhiều cặp chứng chỉ cho mỗi người bán. Một người bán sẽ có một cặp chứng chỉ cho mỗi thương hiệu thẻ thanh toán mà nó chấp nhận.

2.6.3 Chứng chỉ cổng thanh toán

Chứng chỉ cổng thanh toán được lấy bởi Acquirers hoặc bộ phận xử lý của họ cho hệ thống xử lý việc xác thực và ghi nhận thông điệp. Khoá mã hoá công, thứ mà người dùng nhận được từ chứng chỉ này, được dùng để bảo vệ thông tin tài khoản của người dùng. Chứng chỉ cổng thanh toán được cấp cho Acquirers bởi nhãn hiệu thanh toán.

2.6.4 Chứng chỉ Acquirer

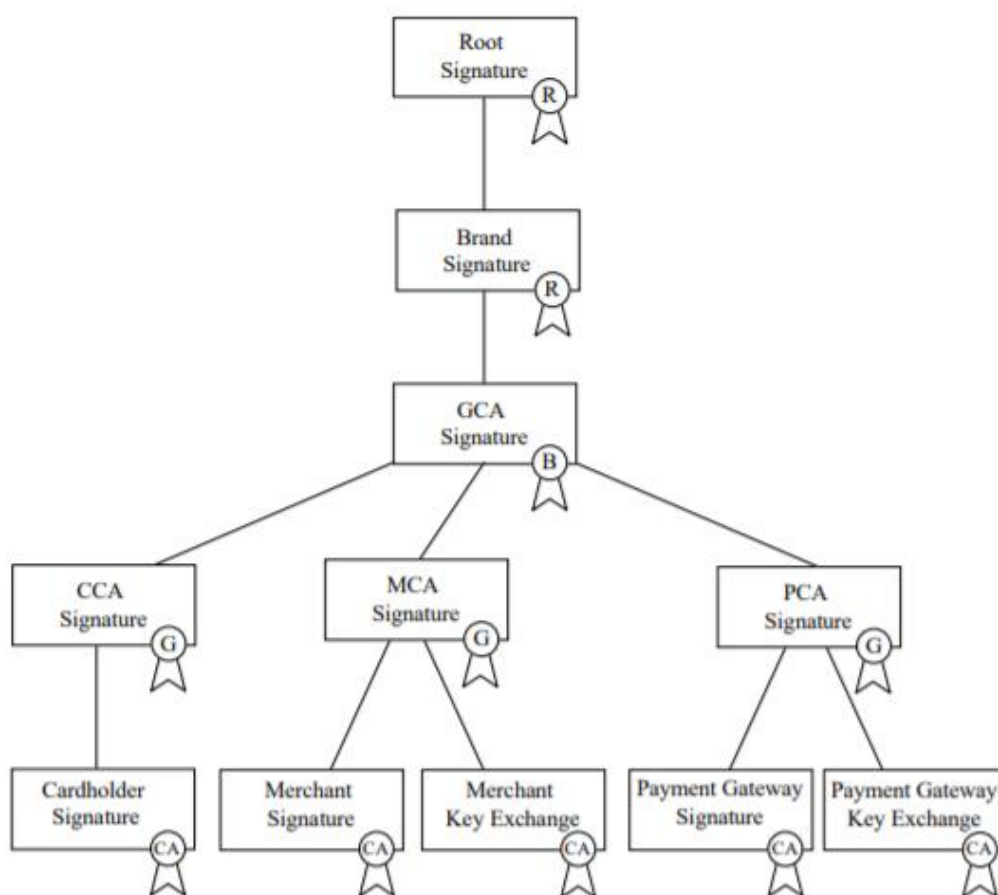
Một Acquirer bắt buộc phải có những chứng chỉ để vận hành Certificate Authority mà có thể chấp nhận và xử lý các yêu cầu cấp chứng chỉ trực tiếp từ người bán trên cả mạng public và private. Những Acquirers có nhãn hiệu thẻ thanh toán xử lý những yêu cầu cấp chứng chỉ thay cho họ, sẽ không cần những chứng chỉ này bởi vì họ không trực tiếp xử lý thông điệp SET. Acquirers nhận chứng chỉ của họ từ nhãn hiệu thẻ thanh toán

2.6.5 Chứng chỉ Issuer

Một Issuer bắt buộc phải có những chứng chỉ để vận hành Certificate Authority mà có thể chấp nhận và xử lý các yêu cầu cấp chứng chỉ trực tiếp từ người dùng trên cả mạng public và private. Những Issuers có nhãn hiệu thẻ thanh toán xử lý những yêu cầu cấp chứng chỉ thay cho họ sẽ không cần những chứng chỉ này bởi vì họ không xử lý thông điệp SET. Issuer nhận chứng chỉ của họ từ nhãn hiệu thẻ thanh toán.

2.7 Phân cấp tin cậy

Một chứng chỉ SET được xác thực thông qua một cây phân cấp tin cậy. Mỗi chứng chỉ được gắn với chữ ký chứng chỉ của thực thể đã ký số nó. Bằng việc đi theo cây tin cậy đến một thành phần tin cậy đã biết, cái mà có thể được đảm bảo rằng chứng chỉ còn hiệu lực. Ví dụ, một chứng chỉ của chủ thẻ được liên kết với chứng chỉ của Issuer (hoặc một thương hiệu đại diện cho Issuer). Chứng chỉ của Issuer được liên kết ngược trở lại với gốc của khóa thông qua chứng chỉ của nhãn hiệu. Chữ kí khóa công khai của gốc được công khai cho tất cả phần mềm SET và có thể được dùng để xác thực mỗi chứng chỉ một cách lần lượt. Biểu đồ sau đây mô tả cây phân cấp tin cậy.



Hình 2. Cây phân cấp tin cậy

Số lượng cấp được trình bày trong biểu đồ trên chỉ mang tính minh họa. Một nhãn hiệu thẻ thanh toán có thể không cần luôn luôn vận hành Cơ quan cấp chứng chỉ giữa chính nó và các tổ chức tài chính.

Phân phối khóa gốc: khóa gốc sẽ được phân phối ở một chứng chỉ tự ký. Chứng chỉ khóa gốc này sẽ sẵn sàng với phần mềm của các nhà bán lẻ và bao gồm trong các phần mềm của họ.

Đánh giá khóa gốc: phần mềm có thể xác nhận rằng nó có một khóa gốc còn hiệu lực bằng cách gửi một yêu cầu khởi tạo đến CA mà chứa giá trị băm của chứng chỉ gốc. Trong trường hợp phần mềm không có chứng chỉ khóa gốc còn hiệu lực, CA sẽ gửi một trong thông điệp trả về. Chú ý: Trong trường hợp hiếm khi xảy ra này khi mà khóa gốc của phần mềm không còn hiệu lực, người dùng(chủ thẻ hoặc người bán) phải nhập vào một chuỗi tương ứng với giá trị băm của chứng chỉ. Sự xác nhận giá trị băm này phải thu được từ một nguồn tin cậy, như tổ chức tài chính của chủ thẻ.

Thay thế khóa gốc: khi một khóa gốc được sinh ra, một khóa thay thế cũng đồng thời được tạo ra. khóa thay thế được lưu trữ một cách bí mật cho đến khi thật cần thiết. Chứng chỉ khóa tự ký và giá trị băm của khóa thay thế được phân phối cùng nhau. Phần mềm sẽ được thông báo về sự thay thế thông qua một tin nhắn chưa đựng chứng chỉ tự ký của gốc thay thế và giá trị

băm của khóa gốc thay thế tiếp theo. Phần mềm đánh giá khóa thay thế bằng cách tính toán giá trị băm của nó và so sánh nó với giá băm của khóa thay thế chứa đựng trong chứng chỉ gốc.

Chương 3. Quy trình thanh toán

3.1 Tổng quan

Mục đích: Phần này mô tả luồng giao dịch được xử lý bởi nhiều hệ thống khác nhau.

Mô tả về giao dịch: SET định nghĩa một vài phương thức giao dịch có sử dụng những khái niệm về mã hóa giải mã đã được đề cập đến ở chương 2. Chương này sẽ mô tả một số giao dịch sau:

Giao dịch:

- Đăng ký bên chủ thẻ
- Đăng ký bên buôn bán
- Yêu cầu mua hàng
- Xác thực thanh toán
- Ghi nhận thanh toán

Một số giao dịch khác: những giao dịch khác được liệt kê dưới đây là một phần trong mô tả về SET, nhưng sẽ không được đề cập ở trong bài viết này.

Tra hỏi chứng chỉ (Certificate Inquiry) và trạng thái: Nếu trung tâm cấp chứng chỉ không đáp ứng việc xử lý những yêu cầu cấp chứng chỉ một cách nhanh chóng, nó sẽ gửi một lời nhắn về cho chủ thẻ hoặc bên bán để cho biết rằng, người gửi yêu cầu nên đợi và quay lại lúc khác. Người chủ thẻ hoặc người bán gửi những thông điệp tra hỏi chứng chỉ (Certificate Inquiry message) của họ để xác định trạng thái của yêu cầu chứng chỉ (đã được duyệt hay phải đợi thêm) hoặc để nhận chứng chỉ khi yêu cầu đó đã được duyệt.

Tra hỏi việc mua sản phẩm: Cho phép chủ thẻ kiểm tra trạng thái của việc xử lý đơn hàng sau khi họ đã nhận được hồi đáp cho việc mua sản phẩm từ hệ thống. Lưu ý rằng thông điệp này không bao gồm trạng thái của hàng hóa nằm trong những đơn hàng dự trữ - loại đơn hàng chưa được xử lý và sẽ được xử lý trong tương lai -. Những thông điệp này lại cho biết trạng thái của việc xác thực (Việc mua hàng hóa đã được xác thực hay chưa), trạng thái của việc lưu trữ thông tin và trạng thái của việc xử lý thanh toán.

Đảo ngược xác thực: Cho phép người bán chỉnh sửa những yêu cầu xác thực trước đó sao cho đúng. Nếu đơn đặt hàng không được hoàn thành, người bán đảo ngược toàn bộ quá trình xác thực. Nếu một phần của đơn hàng không được hoàn thành (ví dụ là những mặt hàng trong đơn hàng dự trữ), người bán sẽ đảo ngược một phần xác thực.

Đảo ngược việc thu nhận: cho phép người bán chỉnh sửa chính xác lại những lỗi xảy ra trong quá trình thu nhận những yêu cầu ví dụ như số tiền giao dịch bị điền sai bởi một nhân viên nào đó được gửi về hệ thống.

Vay nợ: cho phép người bán ghi nợ vào tài khoản người chủ thẻ trong những trường hợp như hàng bị vỡ trong lúc vận chuyển hay bị trả về bởi khách hàng. Lưu ý rằng thông điệp ghi nợ luôn được tạo bởi người bán không phải người chủ thẻ.

Đảo ngược ghi nợ: cho phép người bán điều chỉnh lại những yêu cầu ghi nợ trước đó.

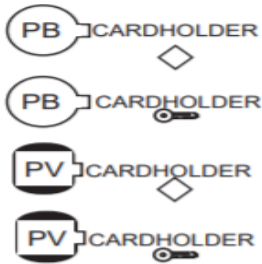

Yêu cầu chứng chỉ cho công thanh toán: cho phép người bán truy vấn đến công thanh toán và thu về một bản sao của khóa trao đổi hiện tại và chữ ký ủy quyền của công đó.


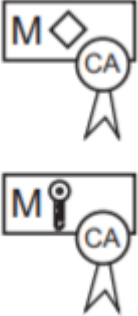



Quản trị theo lô: cho phép người bán truyền thông đến công thanh toán liên quan đến các lô bên buôn bán.

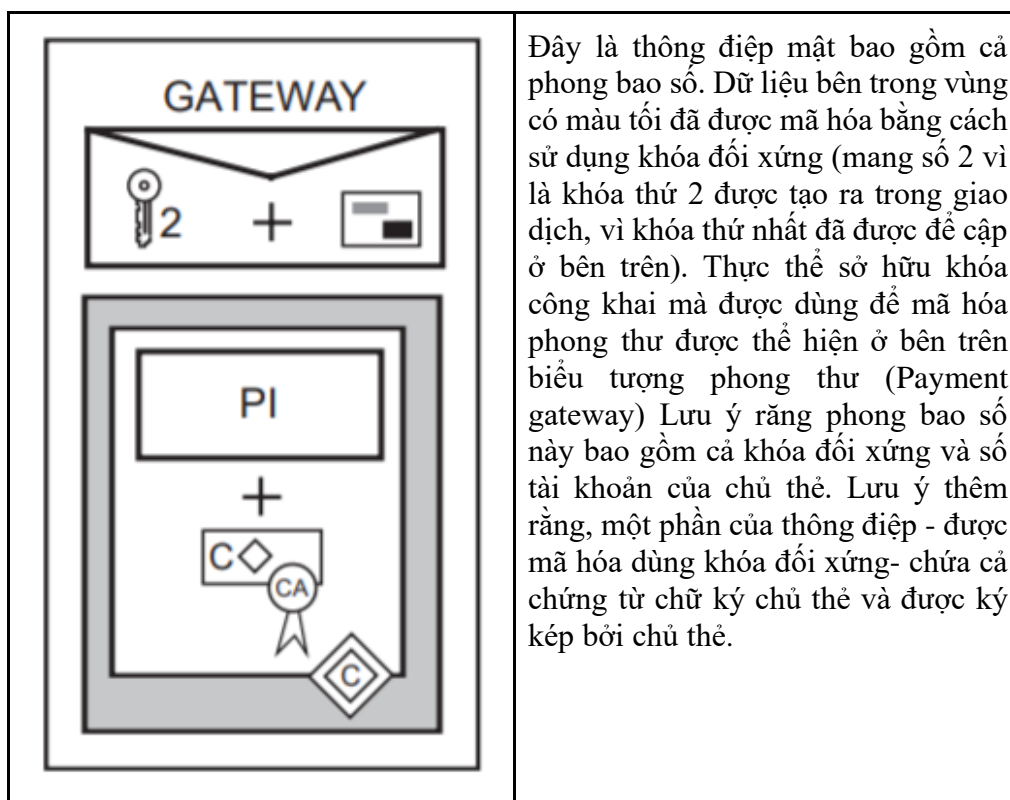
Thông điệp lỗi: thể hiện rằng người trả lời từ chối thông điệp vì sai định dạng hay không vượt qua vòng xác thực nội dung.

Giải thích ký tự:

- C: Chủ thẻ
- M: Bên buôn bán
- P: Công thanh toán
- CA: Tổ chức cấp phát chứng thực

Ký hiệu	Mô tả
	<p>Đây là những khóa mã hóa giải mã.</p> <ul style="list-style-type: none"> - Đầu khóa cho biết người sở hữu khóa. - Khóa với PB ở cuối là khóa công khai, những cái với PV là khóa mật. Khóa mật luôn có chủ. - Khóa đi với ký tự hình thoi (<>) là khóa chữ ký và những cái đi cùng biểu tượng chiếc khóa con là những khóa trao đổi.
	<p>Đây là chữ ký số</p> <ul style="list-style-type: none"> - Chữ cái bên trong cho biết chữ ký được mã hóa bởi khóa mật của ai - ví dụ M: là của bên bán

	<p>Đây là chữ ký kép.</p> <ul style="list-style-type: none"> - Chữ cái bên trong có cùng ý nghĩa với biểu tượng chữ ký số bên trên - cho biết chữ ký được mã hóa bởi khóa mật của bên nào.
	<p>Đây là các chứng thư(Chứng chỉ).</p> <ul style="list-style-type: none"> - Chữ cái viết tắt trong dấu niêm phong cho biết, khóa riêng của ai được sử dụng để ký chứng thư. - Chữ cái bên trong chứng thư cho biết khóa công khai đang được chứng nhận là của ai. - Biểu tượng kim cương và chìa khóa phân biệt 2 chứng thư khoá chữ ký và chứng thư khóa trao đổi. <p>Ví dụ: CA trong 2 biểu tượng trên cũng cho biết ai là người tạo ra chứng thư- CA. Và chữ M cho biết chứng từ thuộc về ai - bên bán.</p>
	<p>Đây là khóa đối xứng được sử dụng để mã hóa dữ liệu. Nó luôn được gửi cùng với dữ liệu được mã hóa bên trong phong bao điện tử. Chữ số đi kèm phân biệt với những khóa khác trong giao dịch.</p>
	<p>Đây là thẻ thanh toán được dùng để cho biết khi nào số tài khoản của chủ thẻ được gửi đi bên trong phong bao điện tử cùng với khóa đối xứng.</p>
	<p>Đây là dữ liệu đã được bảo mật. Nó được dùng để biểu diễn thông tin tài khoản khi được gửi bên trong phong bao điện tử có nội dung yêu cầu đăng ký của bên bán và cổng thanh toán</p>



Các chức năng của chứng từ xác thực:

Phần 3.2 và 3.3 bao gồm lược đồ mô tả luồng xử lý của chứng chỉ xác thực. 3 chức năng chính của chứng chỉ này là để:

- Tiếp nhận một yêu cầu đăng ký vai trò
- Xử lý và phê duyệt / từ chối những yêu cầu
- Ủy quyền cho bên yêu cầu một chứng chỉ xác thực

Những luồng xử lý mô tả các chức năng trên như thể chúng được thực hiện bởi một thực thể đơn lẻ, nhưng chúng được vận hành bởi từ 1 đến 3 thực thể. Thương hiệu thẻ tín dụng và một tổ chức tài chính nào đó sẽ xem xét lại nhu cầu nghiệp vụ của họ cho những chức năng trên, nhằm chọn ra một phương án để thực thi(hoạt động). Phương án được chọn có thể được thực thi bởi một thiết bị máy chủ đơn lẻ - có nhiệm vụ cung cấp những chức năng chứng thực số - hoặc nhiều thiết bị rồi phân phối việc xử lý chứng thực đó.

Để mô tả kỹ hơn, dưới đây gợi ý một thứ tự có thể xảy ra cho các cách phân phối của 3 chức năng trên:

- Một công ty có thể ủy quyền một thể độc quyền có thể thực hiện cả 3 chức năng đã đề cập.
- Hoặc một tổ chức tài chính có thể thực hiện 2 chức năng đầu - tiếp nhận, xử lý phê duyệt / từ chối xác thực chứng từ- sau đó chuyển tiếp thông tin cho một thương hiệu thẻ hợp lý để cấp chứng từ xác thực.
- Hoặc cũng có thể mỗi thực thể sẽ thực hiện 1 trong 3 chức năng trên, một cơ quan đăng ký - có nhiệm vụ xử lý những yêu cầu chứng thực thẻ thanh toán từ nhiều nhãn hiệu thẻ khác

nhau - có thể tiếp nhận những yêu cầu chứng từ và chuyển tiếp chúng cho một tổ chức tài chính hợp lệ để xử lý và phê duyệt. Sau cùng, bên này chuyển cho một thương hiệu thẻ hợp lý để cấp một chứng từ xác thực cho bên yêu cầu.

Những kịch bản trên đã gợi ý cách bố trí các chức năng có thể xảy ra. Rõ ràng, một nhãn hiệu thẻ hoặc một tổ chức tài chính nào đó có thể lựa chọn những chiến lược trên dựa vào nhu cầu nghiệp vụ của họ.

Chứng từ tùy chọn cho chủ thẻ: Những lược đồ và luồng xử lý đi kèm, mô tả việc xử lý những giao dịch khi chủ thẻ thuộc quyền sở hữu của một chứng từ số ủy quyền dưới một cây tín nhiệm của nhãn hiệu thẻ thanh toán nào đó. Vậy nên, những thương hiệu thẻ có thể lựa chọn việc cho phép chủ thẻ xử lý giao dịch không cần chứng từ xác thực.

Xác thực chủ thẻ: Phương thức SET sử dụng chứng từ chữ ký cho chủ thẻ để xác nhận rằng, giao dịch là từ người sử dụng thẻ thanh toán - đã được đăng ký

Sức mạnh của chứng từ chủ thẻ: Một chứng từ chủ thẻ tuy không đảm bảo danh tính của chủ thẻ. Sức mạnh thực sự của chứng từ chủ thẻ là toàn bộ sự lệ thuộc vào những phương thức được sử dụng bởi nhãn hiệu thẻ thanh toán và bên cung cấp thẻ thanh toán để xác thực được chủ thẻ - ưu tiên cho chứng từ đã được ủy quyền.

Trường hợp không dùng chữ ký số: Khi chủ thẻ không sở hữu một chữ ký chứng từ, sẽ không có chữ ký số nào được tạo ra. Thay vào đó, chủ thẻ tạo ra một message digest của dữ liệu (văn bản) và thêm nó vào trong bao thư điện tử.

Đảm bảo tính toàn vẹn: Người nhận sau khi nhận bao thư, lấy ra message digest để kiểm tra tính toàn vẹn.

3.2 Đăng ký chủ thẻ

Phần này mô tả việc thực hiện đăng ký của chủ thẻ, bên tham gia:

- Chủ thẻ sử dụng máy tính
- Bên có thẩm quyền xử lý

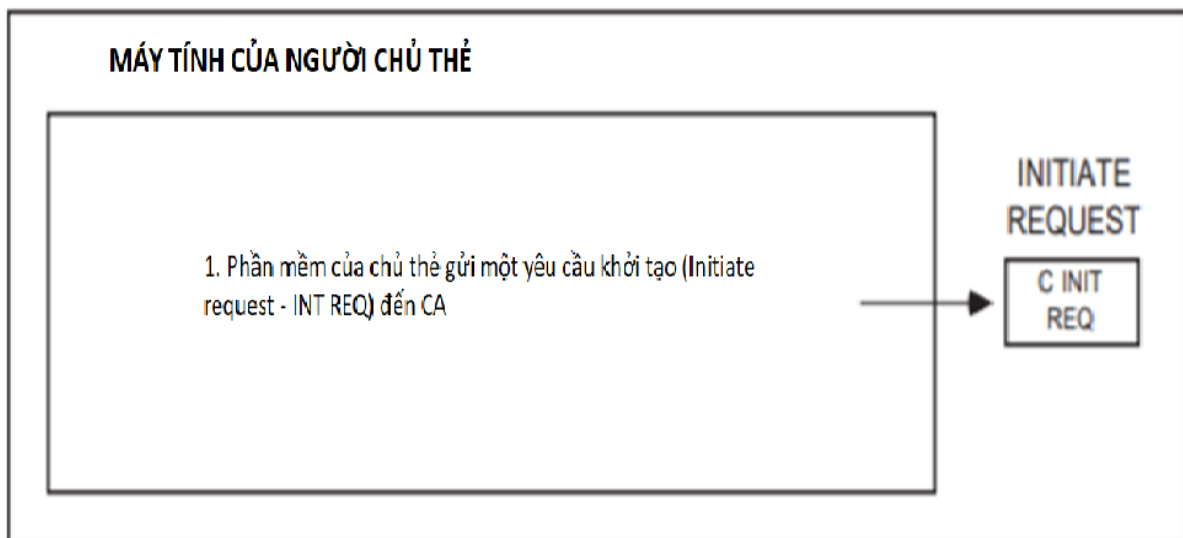
Luồng thực hiện một cách tổng quan:

- Ban đầu từ máy tính của chủ thẻ, người chủ thẻ mở đầu việc đăng ký bằng cách gửi yêu cầu khởi đầu (Initiate request) cho bên CA, bên CA tiếp nhận và trả lại một hồi đáp tương ứng (Initiate response).
- Bên chủ thẻ nhận hồi đáp và gửi yêu cầu về một biểu mẫu để đăng ký bằng cách gửi thông điệp yêu cầu biểu mẫu từ máy tính (registration form request) đến CA, CA tiếp nhận phê duyệt và gửi trả về biểu mẫu cho chủ thẻ.

- Bên chủ thẻ tiếp nhận biểu mẫu, thực hiện đăng ký và yêu cầu chứng từ xác thực bằng cách gửi thông điệp yêu cầu chứng từ chủ thẻ (Card holder certificate) cho CA. Bên CA tiếp nhận, nếu phê duyệt thì gửi trả về chứng từ cho chủ thẻ.
- Bên chủ thẻ nhận chứng từ đã cấp

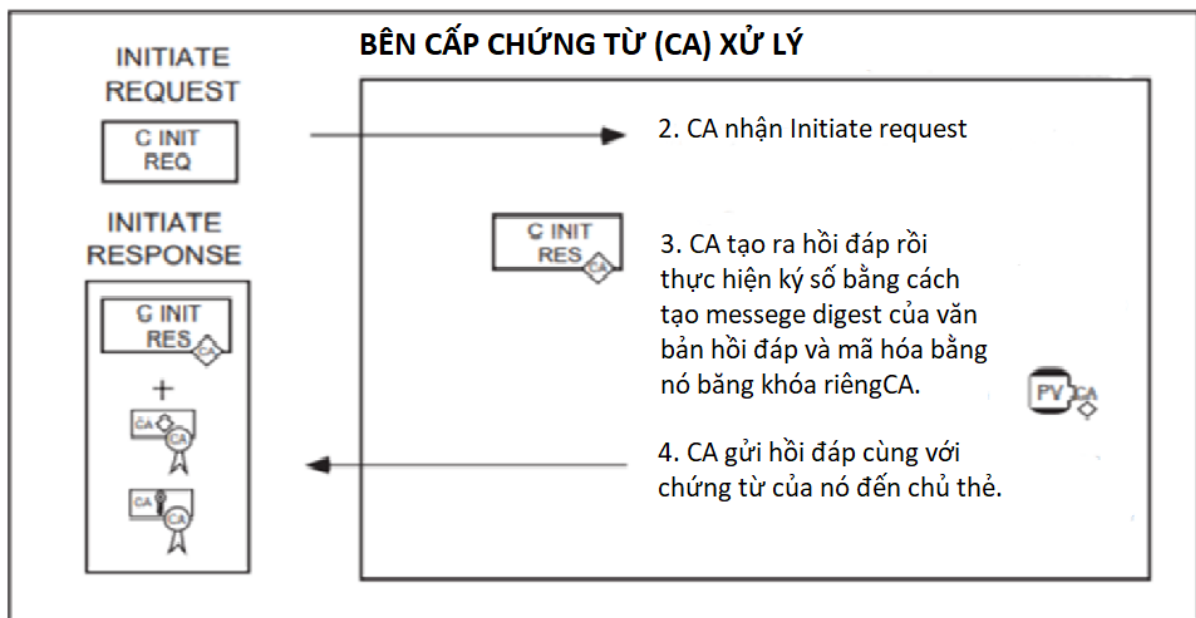
Chủ thẻ gửi yêu cầu khởi tạo đến CA:

- Chủ thẻ phải đăng ký với bên CA trước khi họ có thể gửi những thông điệp SET đến bên bán. Để gửi thông điệp SET đến CA, chủ thẻ phải có một bản copy của khóa công khai từ CA - được cung cấp trong chứng từ trao đổi khóa công khai. Chủ thẻ cũng cần một bản sao của biểu mẫu đăng ký từ nhà cung cấp thẻ tín dụng (Issuer). Để CA cung cấp một biểu mẫu đăng ký, phần mềm bên chủ thẻ phải định danh tổ chức tài chính cung cấp thẻ tín dụng cho CA. Kết hợp những yêu cầu trên thì bên chủ thẻ mới được cấp phát biểu mẫu. Việc xử lý đăng ký bắt đầu khi phần mềm chủ thẻ yêu cầu một bản sao chứng từ khóa công khai.



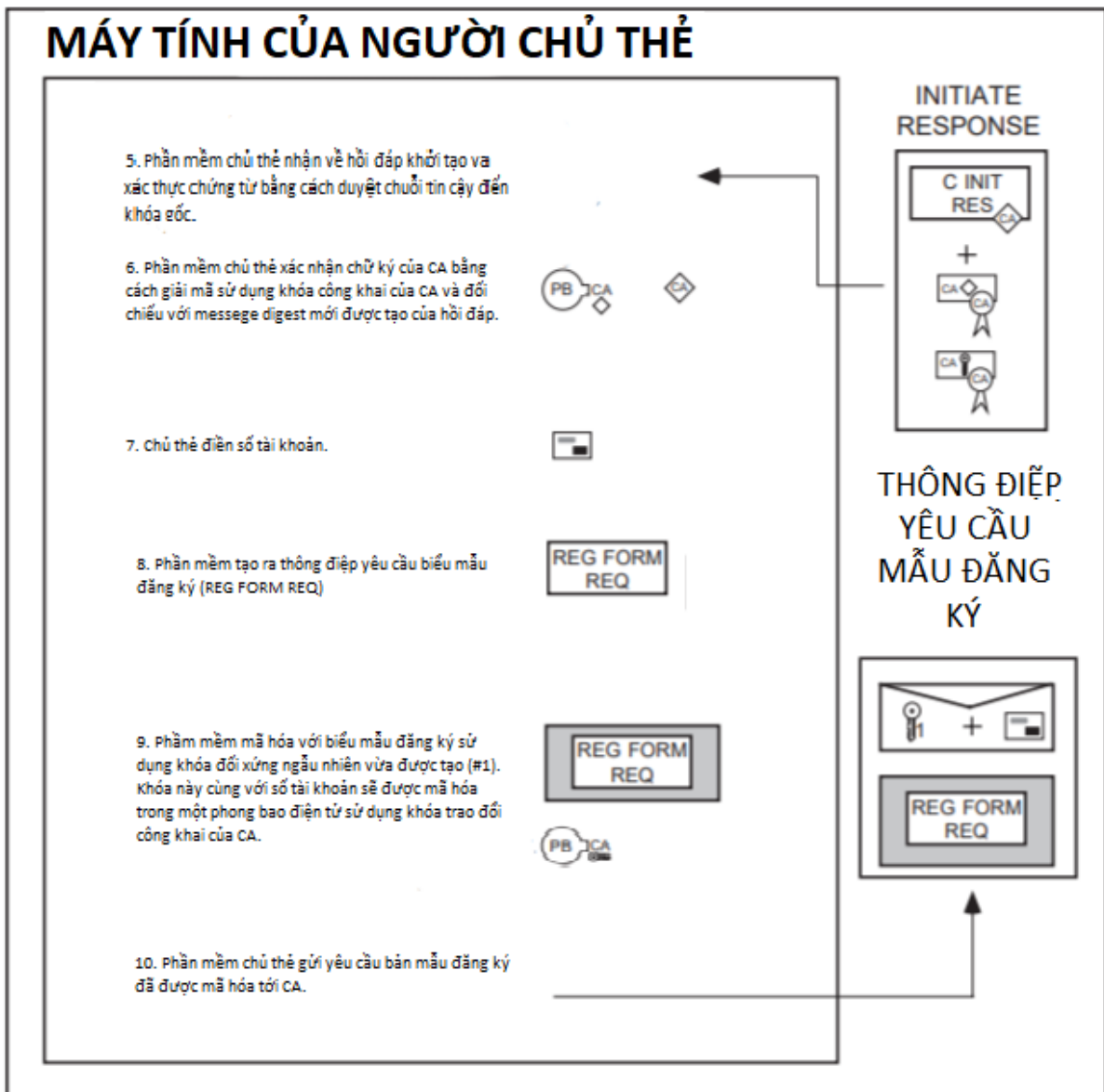
CA nhận được yêu cầu, và gửi hồi đáp đến chủ thẻ:

- Khi CA nhận được yêu cầu, CA vận chuyển chứng từ của nó đến chủ thẻ. Thành phần chứng từ mã hóa khóa cung cấp cho phần mềm chủ thẻ một thông tin cần thiết để bảo vệ số tài khoản giao dịch trong thông điệp yêu cầu bản mẫu đăng ký..



Chủ thẻ nhận được hồi đáp và yêu cầu CA cung cấp mẫu điền đăng ký:

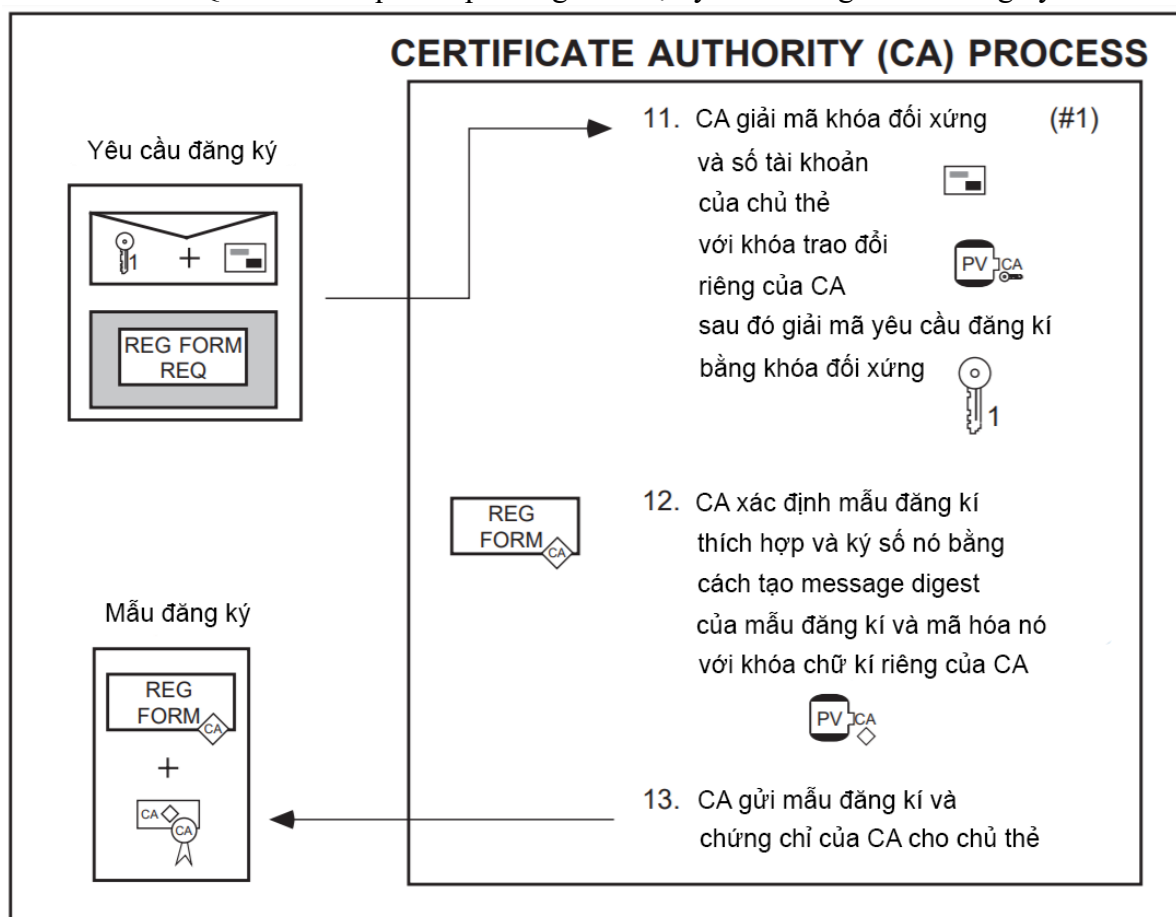
- Phần mềm chủ thẻ xác nhận chứng từ của CA bằng cách duyệt chuỗi tin cậy đến khóa gốc như mô tả ở 3.3. Phần mềm phải giữ chứng từ CA để sử dụng lúc sau trong quá trình đăng ký. Một khi phần mềm đã có bản copy của chứng từ khóa trao đổi của CA, chủ thẻ có thể gửi yêu cầu mẫu đăng ký. Phần mềm của chủ thẻ tạo ra một thông điệp yêu cầu bản mẫu, sau đó nó tạo một khóa đối xứng ngẫu nhiên. Sử dụng khóa này để mã hóa thông điệp yêu cầu bản mẫu, sau đó nó cũng được mã hóa với số tài khoản và bao bọc bởi thư điện tử sử dụng khóa công khai của CA. Cuối cùng, phần mềm vận chuyển tất cả thành phần trên đến CA.
- Tóm lại, ở giai đoạn này, phía chủ thẻ phải thực hiện những công việc sau:
 - + Xác nhận chứng từ xác thực CA bằng cách duyệt chuỗi tin cậy đến khóa gốc
 - + Tạo ra thông điệp yêu cầu biểu mẫu đăng ký
 - + Tạo ra khóa đối xứng để mã hóa thông điệp kia
 - + Mã khóa khóa đối xứng trên và số tài khoản sử dụng khóa công khai CA
 - + Vận chuyển đến bên CA



CA xác định tổ chức tài chính của chủ thẻ (sử dụng sáu đến mười một chữ số đầu tiên của số tài khoản) và chọn mẫu đăng ký thích hợp. Nó ký điện tử và sau đó trả lại mẫu đăng ký này cho chủ thẻ.

Trong một số trường hợp, CA có thể không có bản sao của mẫu đăng ký nhưng có thể thông báo cho phần mềm chủ thẻ nơi mẫu đăng ký có thể được lấy. Ví dụ: tổ chức tài chính phát hành thẻ có thể vận hành CA của riêng mình. Trong trường hợp này, CA trả về phản hồi giới thiệu thay vì mẫu đăng ký. (Phản hồi giới thiệu này không được hiển thị trong sơ đồ bên dưới.)

Quá trình cơ quan cấp chứng chỉ nhận yêu cầu và gửi mẫu đăng ký



Phần mềm chủ thẻ xác minh chứng chỉ CA bằng cách duyệt qua chuỗi tin cậy đến chìa khóa gốc.

Chủ thẻ cần một cặp khóa công khai / riêng để sử dụng với SET. Phần mềm của chủ thẻ tạo cặp khóa này nếu nó chưa tồn tại.

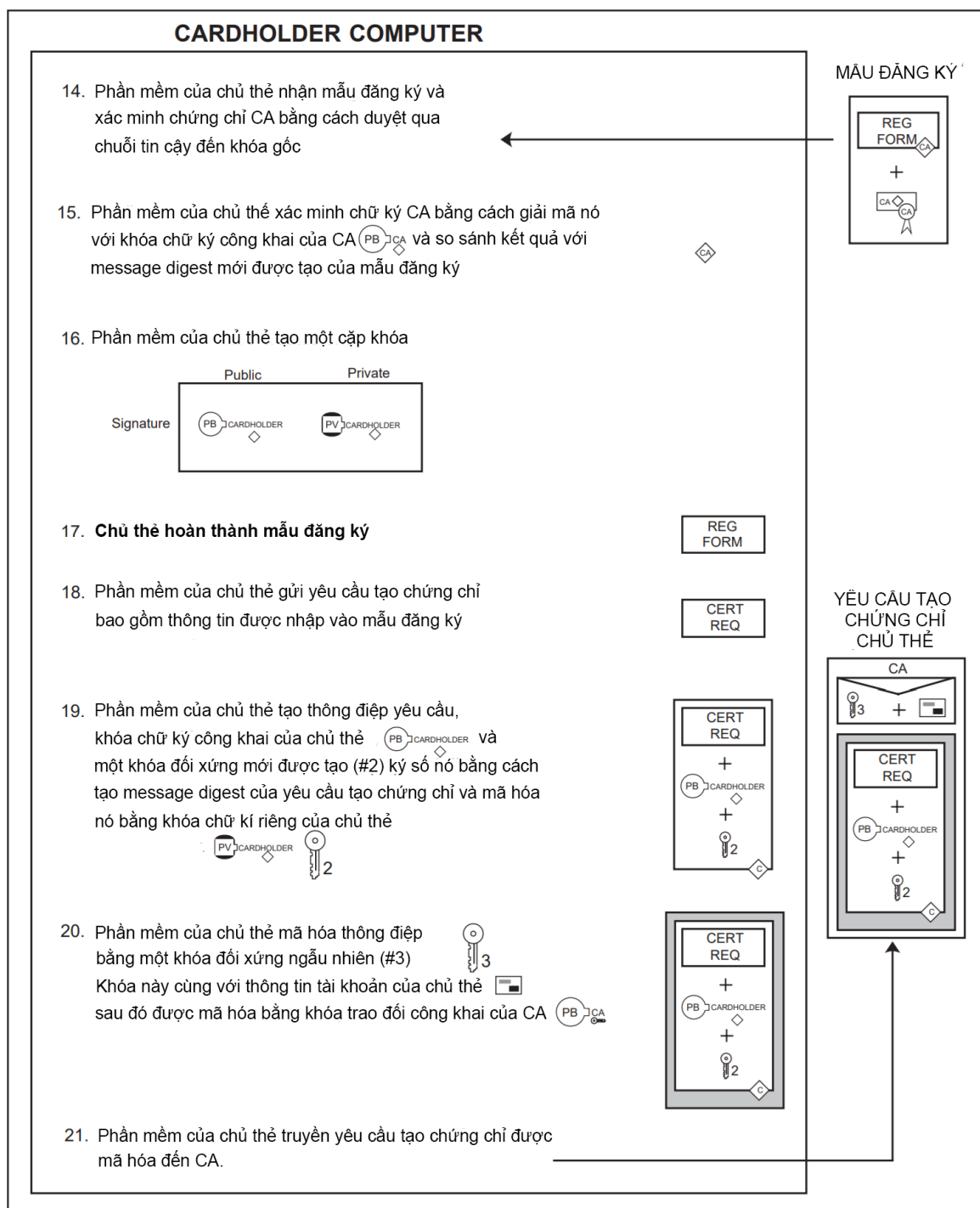
Để đăng ký tài khoản, chủ thẻ điền vào mẫu đăng ký đã được trả lại bởi CA với thông tin như tên chủ thẻ, ngày hết hạn, địa chỉ thanh toán tài khoản, và bất kỳ thông tin bổ sung nào mà tổ chức tài chính phát hành thấy cần thiết để xác định người yêu cầu chứng nhận là chủ thẻ hợp lệ.

Phần mềm của chủ thẻ tạo ra một số ngẫu nhiên sẽ được CA sử dụng trong tạo chứng chỉ. Việc sử dụng số ngẫu nhiên này được mô tả trong quá trình xử lý được thực hiện bởi CA.

Phần mềm chủ thẻ lấy thông tin đăng ký này và kết hợp nó với khóa công khai trong một tin nhắn đăng ký. Phần mềm ký số thông điệp đăng ký. Tiếp theo phần mềm tạo ra hai khóa mã hóa đối xứng ngẫu nhiên. Phần mềm đặt một khóa đối xứng ngẫu nhiên bên trong tin nhắn; CA sẽ sử dụng khóa này để mã hóa phản hồi. Nó sử dụng khóa ngẫu nhiên còn lại để mã hóa tin nhắn đăng ký. Khóa ngẫu nhiên này sau đó được mã hóa cùng với số tài khoản, ngày hết hạn và số ngẫu nhiên vào phong bì kỹ thuật số sử dụng khóa trao đổi công khai CA. Cuối cùng, phần mềm truyền tất cả các thành phần này cho CA.

Lưu ý: Nếu CA trả về phản hồi giới thiệu như được mô tả trước đó trong quá trình xử lý CA, thì phần mềm chủ thẻ sẽ bắt đầu lại quá trình đăng ký với CA được giới thiệu để nhận chứng chỉ của CA đó và mẫu đăng ký thích hợp.

Chủ thẻ nhận được mẫu đăng kí và yêu cầu chứng nhận



Khi CA nhận được yêu cầu của chủ thẻ, nó sẽ giải mã phong bì kỹ thuật số để có được Khóa mã hóa đối xứng, thông tin tài khoản và số ngẫu nhiên được tạo bởi phần mềm chủ thẻ. Nó sử dụng khóa đối xứng để giải mã yêu cầu đăng ký. Sau đó nó sử dụng Khóa chữ ký trong tin nhắn để đảm bảo yêu cầu được ký bằng cách sử dụng khóa chữ ký riêng tương ứng. Nếu chữ ký được xác

minh, tin nhắn tiếp tục được xử lý; mặt khác, tin nhắn bị từ chối và một tin nhắn phản hồi thích hợp được trả về chủ thẻ.

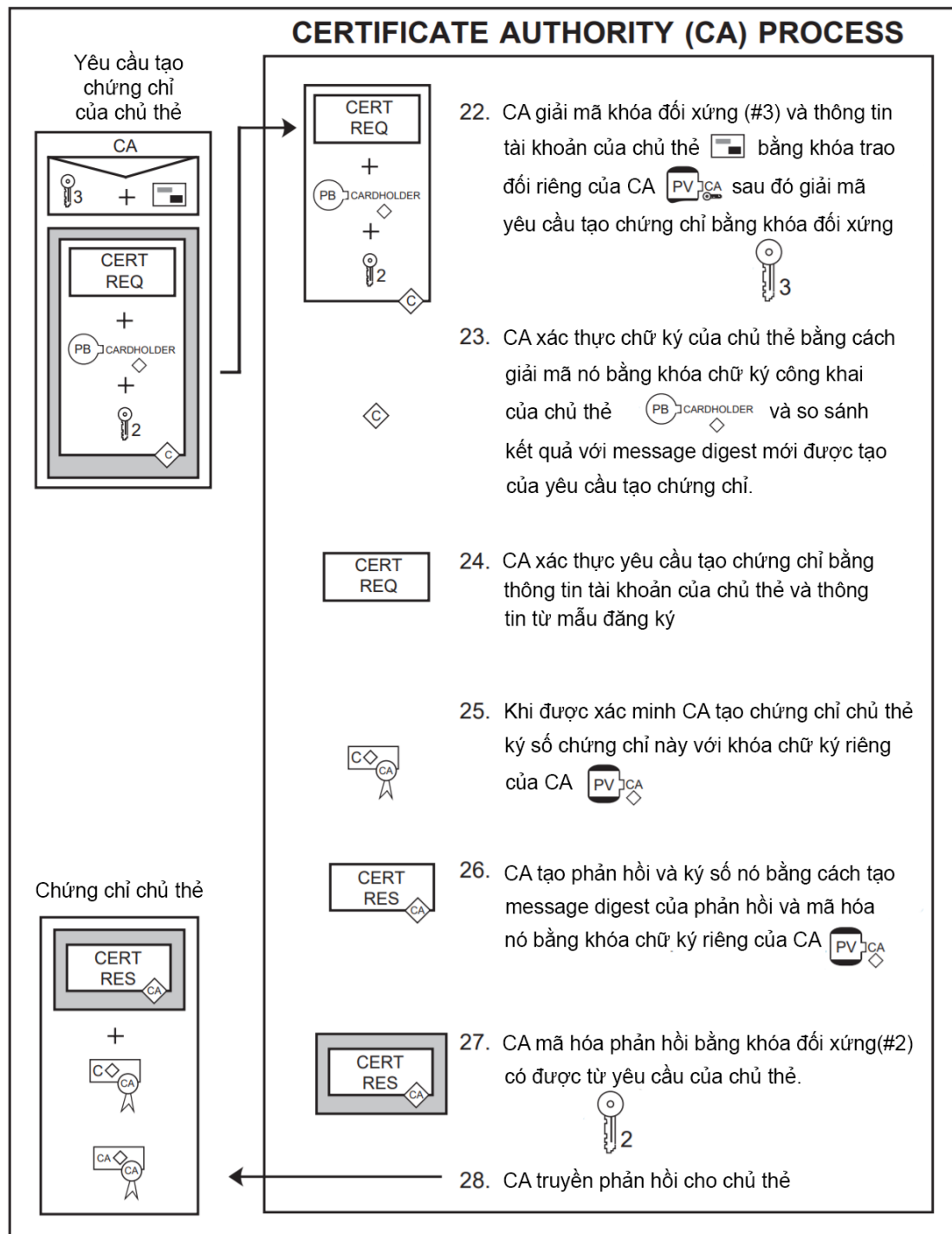
Tiếp theo, CA phải xác minh thông tin từ yêu cầu đăng ký bằng cách sử dụng thông tin tài khoản thẻ của chủ thẻ. Quá trình CA và Người phát hành trao đổi thông tin và các bước thực hiện để xác minh thông tin trong yêu cầu đăng ký nằm ngoài phạm vi đặc tả này. Như được mô tả trong Phần 3.1, có một số cách để cấu hình việc xử lý được thực hiện bởi CA và Nhà phát hành, chẳng hạn như có thương hiệu thẻ thanh toán cung cấp một số hoặc tất cả các chức năng thay mặt cho Nhà phát hành hoặc yêu cầu Nhà phát hành cung cấp tất cả chức năng.

Nếu thông tin trong yêu cầu đăng ký được xác minh, chứng chỉ sẽ được cấp. Đầu tiên CA tạo một số ngẫu nhiên được kết hợp với số ngẫu nhiên được tạo bởi phần mềm chủ thẻ để tạo ra một giá trị bí mật. Giá trị bí mật này được sử dụng để bảo vệ thông tin tài khoản trong giấy chứng nhận chủ thẻ. Số tài khoản, ngày hết hạn và giá trị bí mật được mã hóa bằng thuật toán băm một chiều. Kết quả của thuật toán băm được đặt vào giấy chứng nhận chủ thẻ. Nếu số tài khoản, ngày hết hạn và giá trị bí mật được biết, liên kết đến chứng chỉ có thể được chứng minh, nhưng không thể có được thông tin bằng cách nhìn vào giấy chứng nhận.

Tiếp theo, CA tạo và ký điện tử chứng nhận chủ thẻ. Thời hạn hiệu lực của giấy chứng nhận sẽ được xác định bởi chính sách CA; thường thì nó sẽ tương ứng với ngày hết hạn thẻ thanh toán, nhưng nó có thể hết hạn sớm hơn.

Một thông điệp phản hồi có chứa số ngẫu nhiên được tạo bởi CA và các thông tin khác (như logo thương hiệu) sau đó được tạo và mã hóa bằng cách sử dụng khóa đối xứng được gửi bởi phần mềm chủ thẻ trong thông báo đăng ký. Phản hồi truyền đến chủ thẻ.

Tổ chức phát hành chứng chỉ xử lý yêu cầu và tạo chứng chỉ

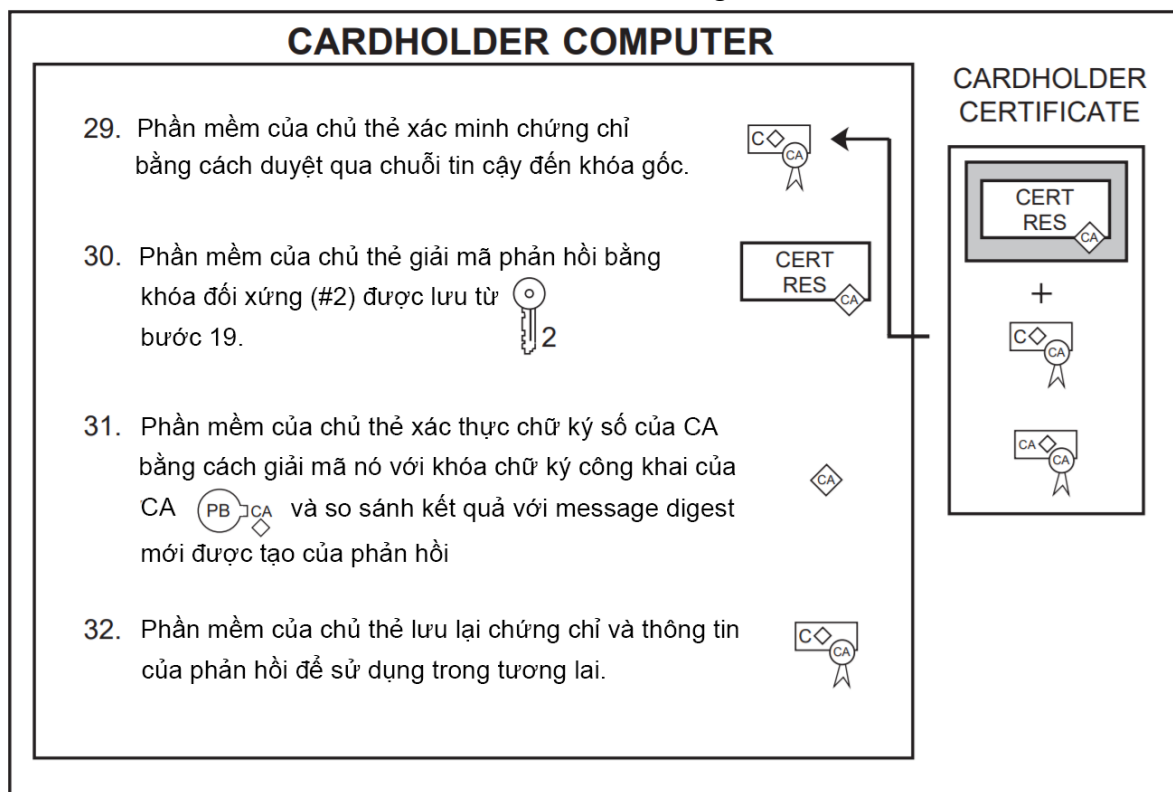


Khi phần mềm chủ thẻ nhận được phản hồi từ CA, nó sẽ xác minh chứng chỉ bằng cách duyệt qua chuỗi tin cậy đến khóa gốc, như được mô tả trong Phần 3.3. Nó lưu chứng chỉ trên máy tính của chủ thẻ để sử dụng trong các giao dịch thương mại điện tử trong tương lai.

Tiếp theo, phần mềm chủ thẻ giải mã phản hồi đăng ký bằng cách sử dụng khóa đối xứng mã hóa mà nó đã gửi cho CA trong thông báo đăng ký. Nó kết hợp số ngẫu nhiên được CA trả về với giá trị mà nó đã gửi trong thông báo đăng ký tới xác định giá trị bí mật. Sau đó, nó lưu trữ giá trị bí mật để sử dụng với chứng chỉ.

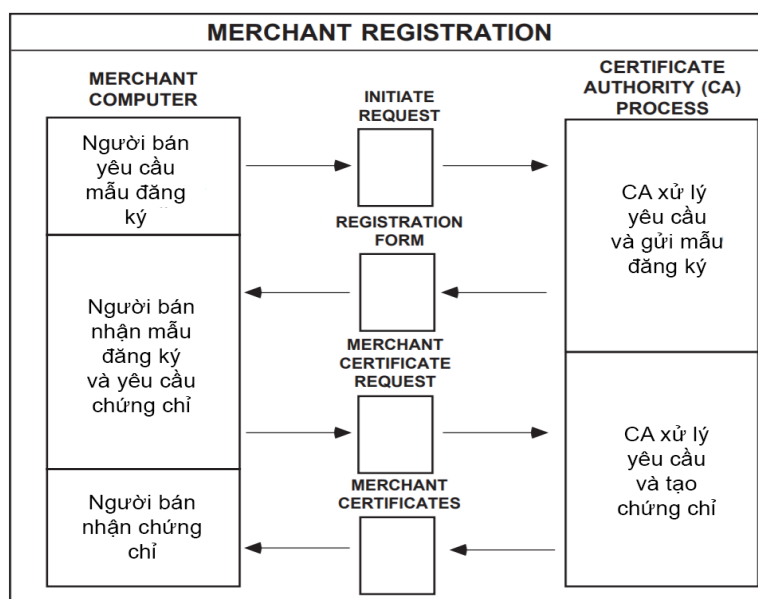
Các nhà cung cấp phần mềm chủ thẻ sẽ đảm bảo rằng chứng chỉ và thông tin liên quan được lưu trữ trong một cách để ngăn chặn truy cập trái phép.

Chủ thẻ nhận chứng chỉ



3.3 Đăng kí người bán

Hình 3 cung cấp một cái nhìn tổng quan cấp cao về quy trình đăng ký người bán, hiển thị năm bước cơ bản. Các phần chi tiết theo mô tả từng bước.

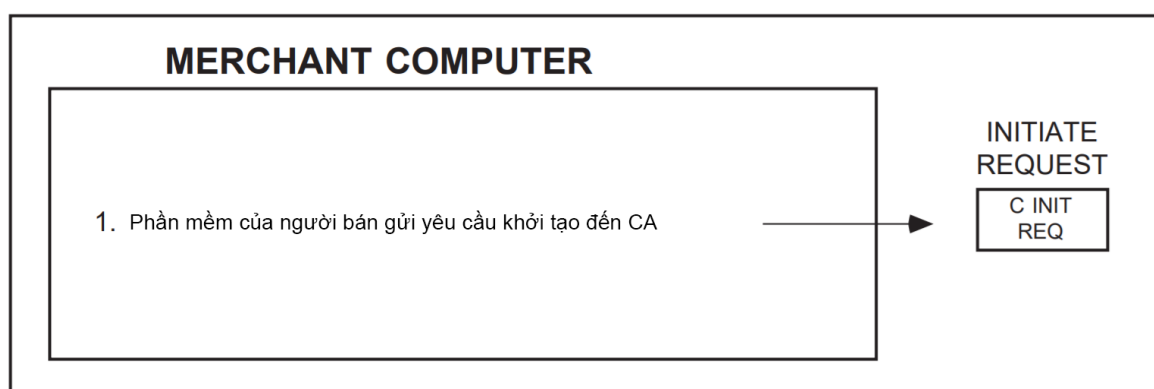


Hình 3. Tóm tắt quá trình đăng ký người bán

Người bán phải đăng ký với Tổ chức phát hành chứng chỉ (CA) trước khi họ có thể nhận được SET hướng dẫn thanh toán từ chủ thẻ hoặc xử lý giao dịch SET thông qua cổng thanh toán. Để gửi tin nhắn SET đến CA, người bán phải có một bản sao khóa trao đổi công khai của CA, được cung cấp trong chứng chỉ khóa trao đổi CA. Người bán cũng cần một bản sao của mẫu đăng ký từ Tổ chức tài chính của người bán. Phần mềm người bán phải xác định Người mua cho CA.

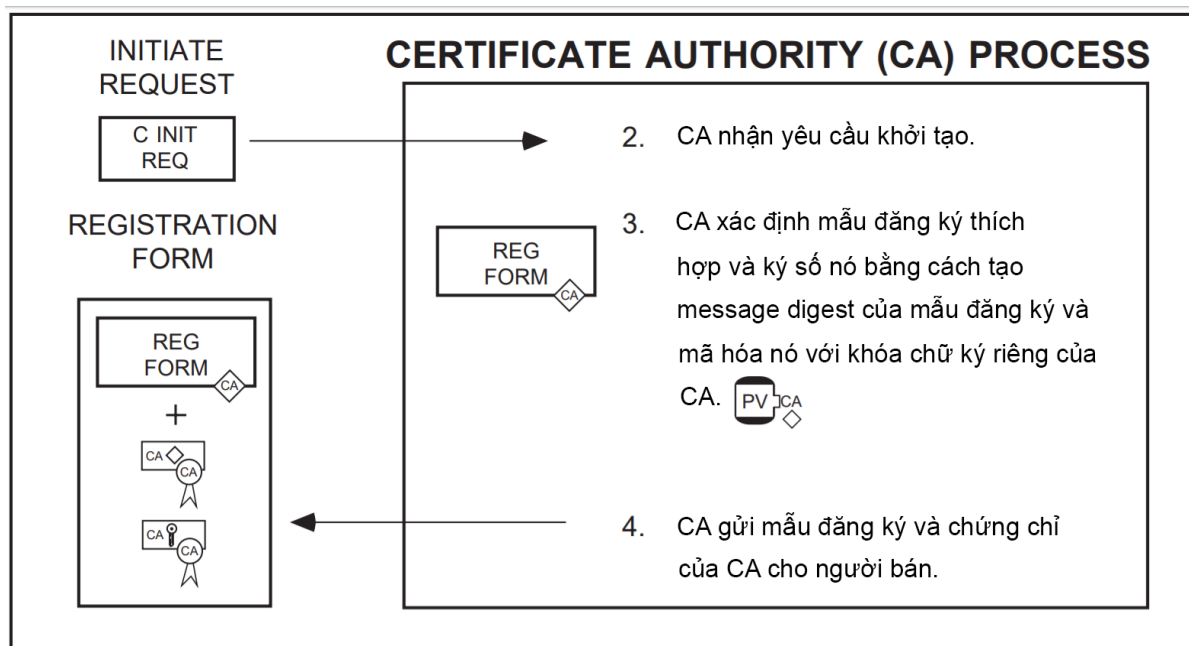
Quá trình đăng ký bắt đầu khi phần mềm người bán yêu cầu một bản sao chứng chỉ của khóa trao đổi công khai của CA và mẫu đăng ký thích hợp.

Người bán yêu cầu mẫu đăng ký



CA xác định tổ chức tài chính của người bán và chọn hình thức đăng ký thích hợp. Nó trả về mẫu đăng ký này cùng với một bản sao chứng chỉ khoá trao đổi của mình đến các người bán.

CA xử lý yêu cầu và gửi mẫu đăng ký



Phần mềm thương gia xác minh chứng chỉ CA bằng cách duyệt qua chuỗi tin cậy đến khóa gốc, sau đó giữ chứng chỉ CA để sử dụng sau trong quá trình đăng ký. Một khi phần mềm có bản sao chứng chỉ trao đổi khóa CA, người bán có thể đăng ký để chấp nhận đặt hướng dẫn

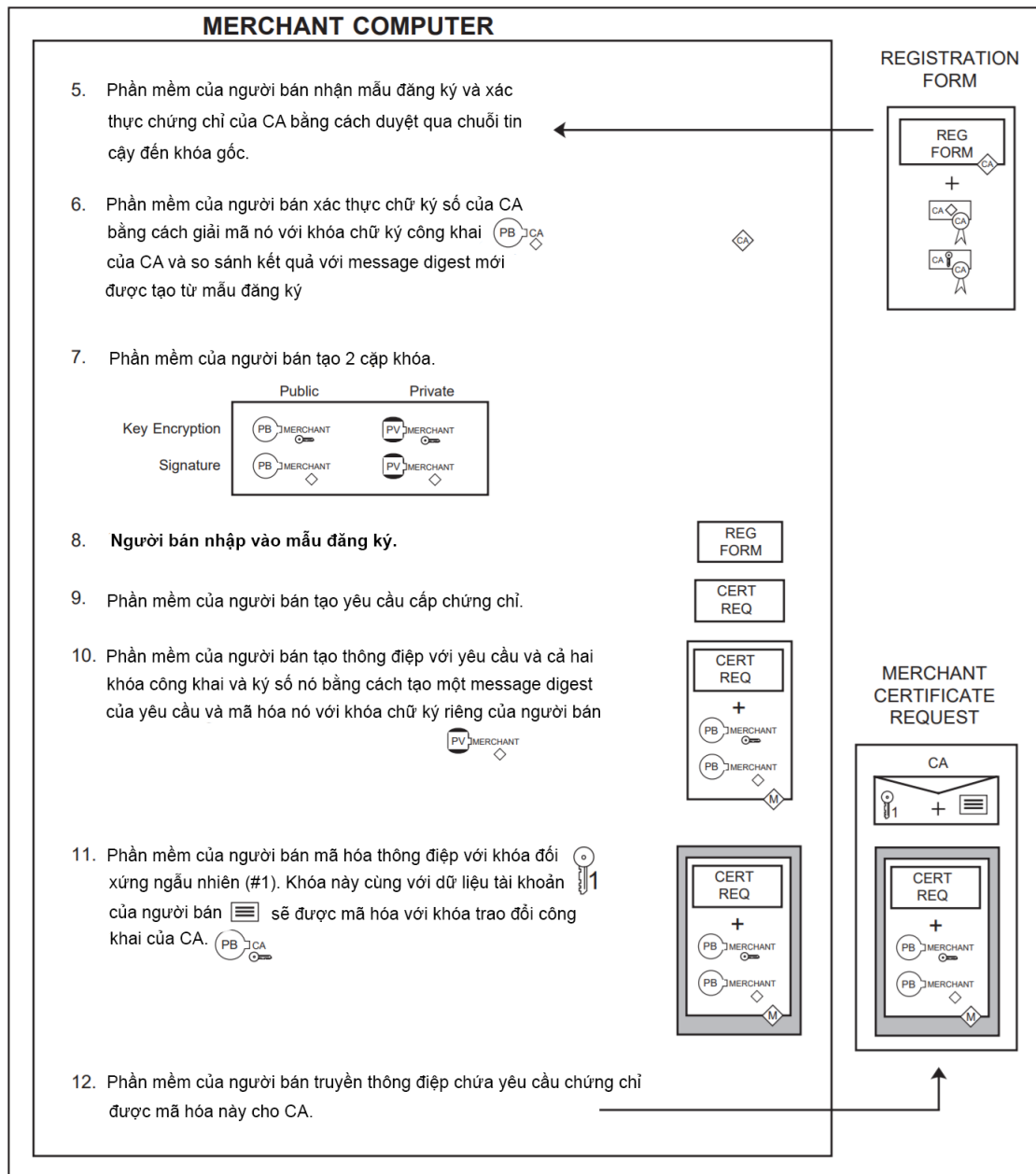
thanh toán và xử lý giao dịch SET. Các người bán phải có một mối quan hệ với Acquirer xử lý các giao dịch SET trước khi yêu cầu chứng chỉ có thể được xử lý.

Người bán cần hai cặp khóa công khai / riêng để sử dụng với SET: khóa trao đổi và khóa chữ ký. Phần mềm người bán tạo các cặp khóa này nếu chúng chưa tồn tại.

Để đăng ký, người bán điền vào mẫu đăng ký trên màn hình với thông tin như tên, địa chỉ và ID thương gia.

Phần của người bán gia lấy thông tin đăng ký này và kết hợp nó với khóa công khai trong một tin nhắn đăng ký. Phần mềm ký số thông báo đăng ký. Tiếp theo phần mềm tạo khóa mã hóa đối xứng ngẫu nhiên. Nó sử dụng khóa ngẫu nhiên này để mã hóa thông điệp. Khóa ngẫu nhiên sau đó được mã hóa vào phong bì kỹ thuật số bằng cách sử dụng khóa trao đổi công khai của CA. Cuối cùng, phần mềm truyền tất cả các thành phần này đến CA.

Người bán nhận mẫu đăng ký và yêu cầu tạo chứng chỉ



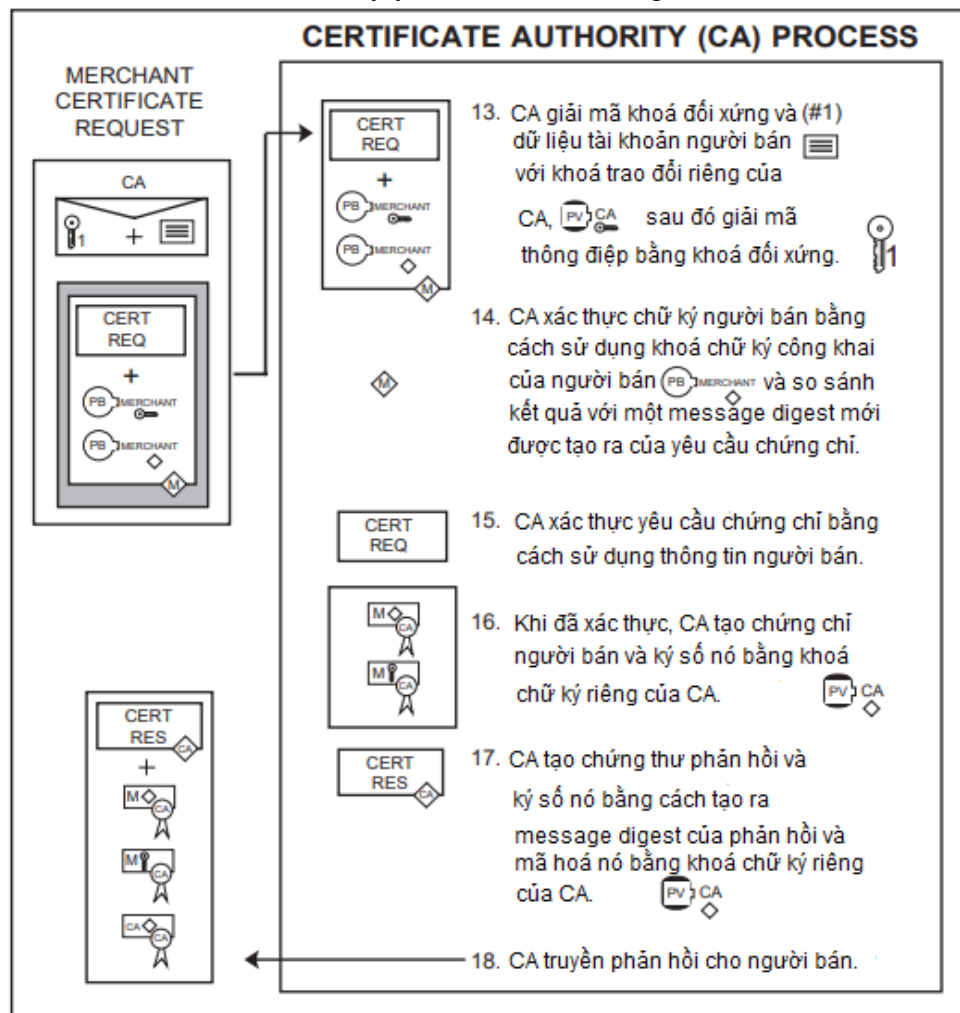
Khi CA nhận được yêu cầu từ người bán, nó sẽ giải mã phong bì số để lấy khóa mã hóa đối xứng, được sử dụng để giải mã yêu cầu đăng ký. Sau đó, nó sử dụng khóa chữ ký trong tin nhắn để đảm bảo rằng yêu cầu đã được ký bằng khóa chữ ký riêng tương ứng. Nếu chữ ký được xác minh, quá trình xử lý tin nhắn tiếp tục; mặt khác, tin nhắn bị từ chối và một tin nhắn phản hồi thích hợp được trả về cho người bán.

Tiếp theo, CA phải xác minh thông tin từ yêu cầu đăng ký bằng thông tin người bán đã biết. Quá trình CA và Acquirer trao đổi thông tin và các bước được thực hiện để xác minh thông tin trong yêu cầu đăng ký nằm ngoài phạm vi đặc tả. Như được mô tả trong Phần 3.1, có một số cách để định cấu hình xử lý được thực hiện bởi CA và Acquirer, chẳng hạn như có thương hiệu

thẻ thanh toán cung cấp một số hoặc tất cả các chức năng thay mặt cho Acquirer hoặc yêu cầu Acquirer cung cấp tất cả các chức năng.

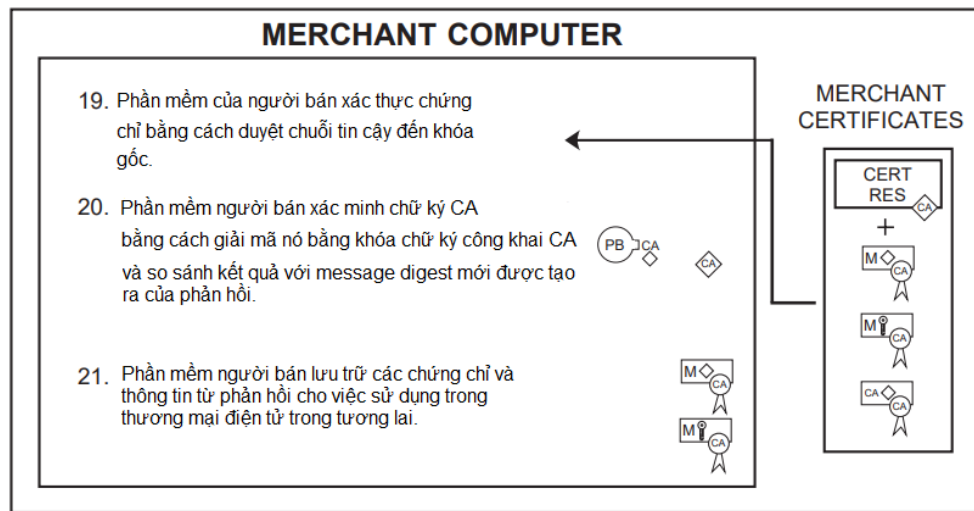
Nếu thông tin trong yêu cầu đăng ký được xác minh, CA sẽ tạo và ký điện tử chứng nhận người bán. Thời hạn hiệu lực của các chứng chỉ này sẽ được xác định bởi chính sách CA; thông thường, nó sẽ tương ứng với ngày hết hạn của hợp đồng người bán với Acquirer, nhưng nó có thể hết hạn sớm hơn. Các chứng chỉ sau đó được mã hóa bằng khóa đối xứng được tạo ngẫu nhiên mới, sau đó được mã hóa bằng trao đổi khóa công khai của người bán. Phản hồi sau đó được truyền đến người bán.

CA xử lý yêu cầu và tạo chứng chỉ

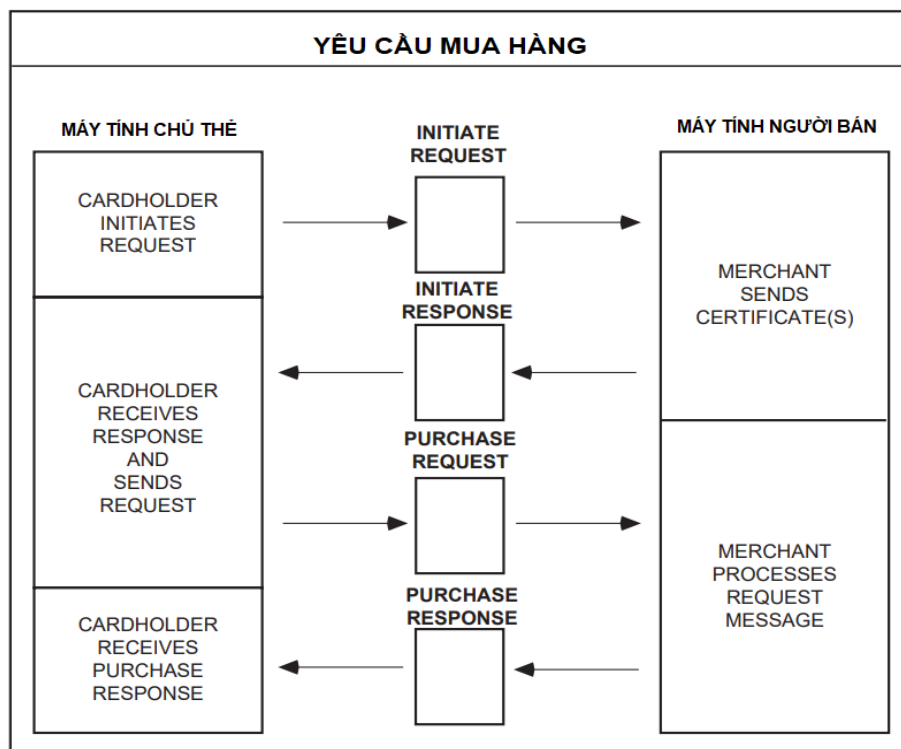


Khi phần mềm của người nhận được phản hồi từ CA, nó sẽ giải mã phong bì kỹ thuật số để lấy khóa mã hóa. Sau khi phần mềm của người bán xác minh chứng chỉ bằng cách duyệt chuỗi tin cậy đến khóa gốc, nó sẽ lưu chứng chỉ trên máy tính của người bán để sử dụng trong giao dịch thương mại điện tử trong tương lai.

Người bán nhận được chứng thư



Hình 4 cung cấp một cái nhìn tổng quan cấp cao về phần yêu cầu mua hàng trong quy trình đặt hàng của chủ thẻ, cho thấy năm bước cơ bản của nó. Các phần chi tiết tiếp theo mô từng bước.

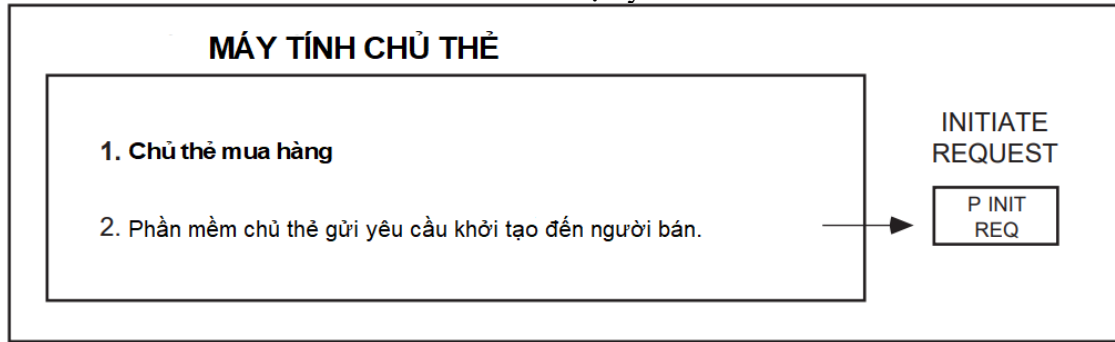


Hình 4. Yêu cầu mua hàng

Giao thức SET được gọi sau khi chủ thẻ hoàn tất việc duyệt, lựa chọn và đặt hàng. Trước khi luồng này bắt đầu, chủ thẻ sẽ được trình bày một mẫu đơn đặt hàng đã hoàn thành và phê duyệt nội dung cũng như các điều khoản của nó, chẳng hạn như số lần thanh toán trả góp nếu người bán đang cho phép thanh toán cho các giao dịch thành nhiều đợt. Ngoài ra, chủ thẻ sẽ chọn một thẻ thanh toán làm phương tiện thanh toán.

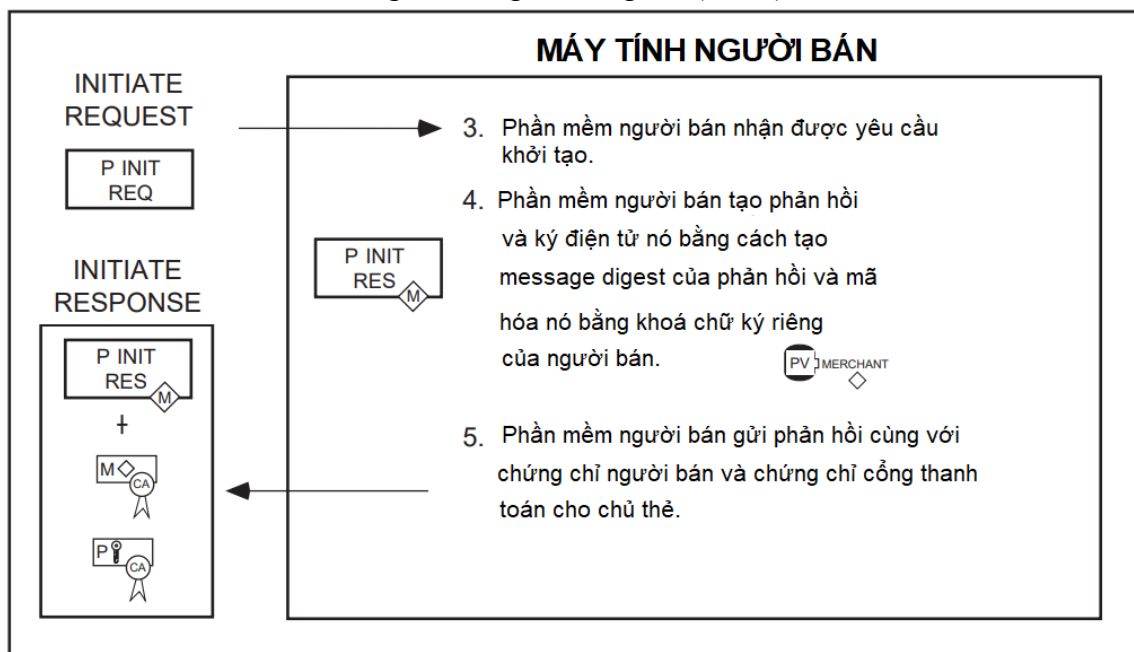
Để gửi tin nhắn SET cho một người bán, chủ thẻ phải có một bản sao của các khóa trao đổi của Cổng thanh toán. Quá trình đặt hàng SET được bắt đầu khi phần mềm chủ thẻ yêu cầu một bản sao chứng chỉ cổng thanh toán. Thông báo từ chủ thẻ cho biết thương hiệu thẻ thanh toán nào sẽ được sử dụng cho giao dịch.

Chủ thẻ khởi tạo yêu cầu



Khi người bán nhận được yêu cầu, nó sẽ gán một định danh giao dịch duy nhất cho tin nhắn. Sau đó, nó truyền các chứng nhận người bán và chứng chỉ công tương ứng với nhãn hiệu thẻ thanh toán được chỉ định bởi chủ thẻ, cùng với số định danh giao dịch cho chủ thẻ

Người bán gửi chứng chỉ (nhiều)



Phần mềm chủ thẻ xác minh chứng chỉ người bán và chứng chỉ công thanh toán bằng cách duyệt chuỗi tin cậy đến khóa gốc, sau đó giữ các chứng chỉ này để sử dụng sau trong quá trình đặt hàng.

Phần mềm chủ thẻ tạo Thông tin đặt hàng (OI) và Hướng dẫn thanh toán (PI). Phần mềm đặt mã định danh giao dịch được chỉ định bởi người bán trong OI và PI; định danh này sẽ được Cổng thanh toán sử dụng để liên kết OI và PI với nhau khi người bán yêu cầu ủy quyền.

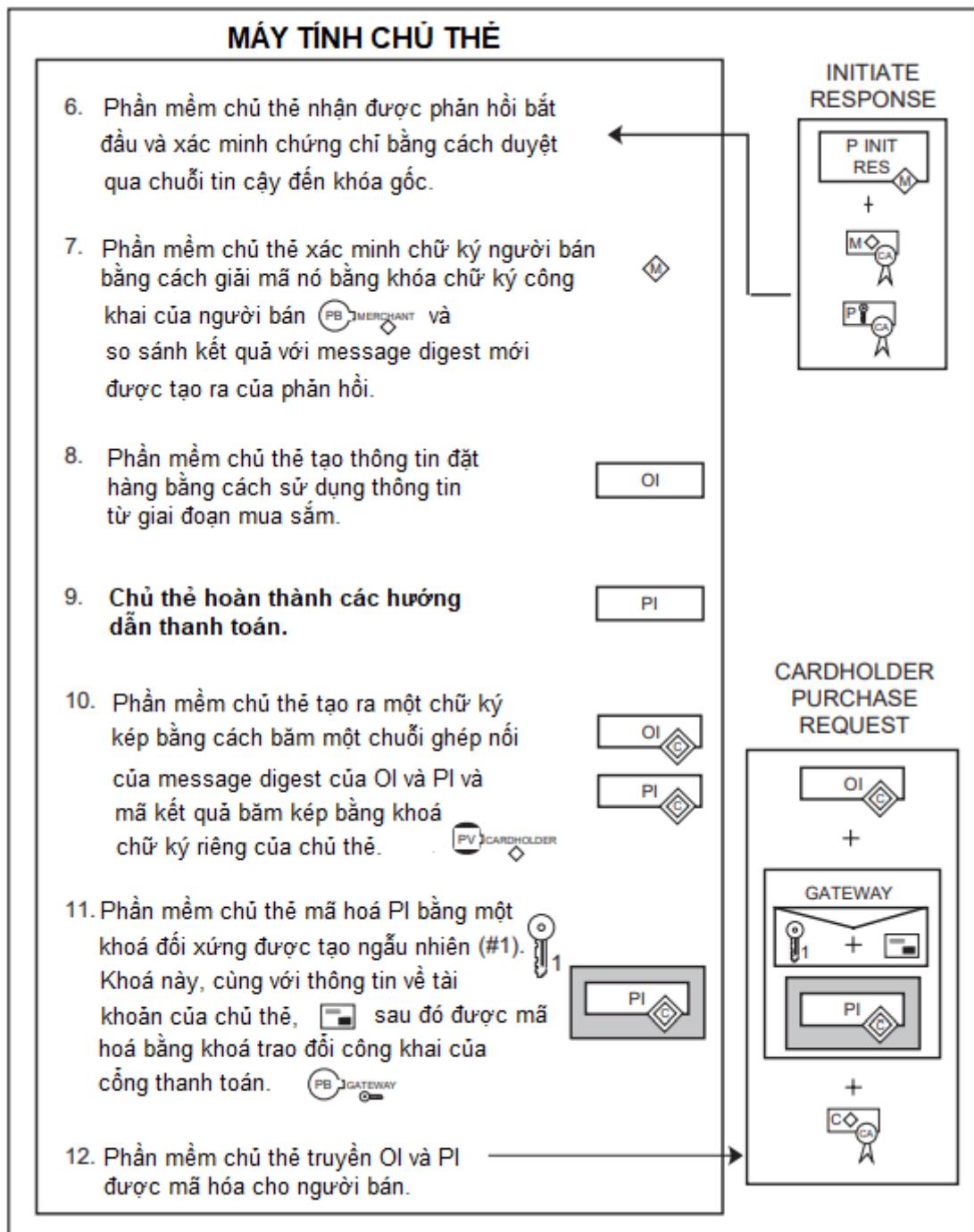
Lưu ý: OI không chứa dữ liệu đơn hàng như mô tả hàng hóa (các mặt hàng và số lượng) hoặc các điều khoản của đơn hàng (chẳng hạn như số lần thanh toán trả góp). Thông tin này được trao đổi giữa chủ thẻ và phần mềm người bán trong giai đoạn mua sắm trước thông điệp SET đầu tiên.

Phần mềm chủ thẻ tạo ra một chữ ký kép cho OI và PI bằng cách tính toán các message digest của cả hai, nối hai bản tóm tắt, tính toán thông báo kết quả và mã hóa bằng cách sử dụng khóa chữ ký riêng của chủ thẻ. Message digest của OI và PI được gửi cùng với chữ ký kép.

Tiếp theo phần mềm tạo khóa mã hóa đối xứng ngẫu nhiên và sử dụng nó để mã hóa PI được ký kép. Sau đó, phần mềm mã hóa số tài khoản chủ thẻ cũng như khóa đối xứng ngẫu nhiên được sử

dùng để mã hóa PI thành một phong bì kỹ thuật số bằng cách sử dụng khóa trao đổi của Cổng thanh toán.

Cuối cùng, phần mềm truyền thông điệp bao gồm OI và PI cho thương gia.



Khi phần mềm người bán nhận được đơn đặt hàng, nó sẽ xác thực chứng nhận chữ ký của chủ thẻ bằng cách duyệt qua chuỗi tin cậy đến khóa gốc. Tiếp theo, nó sử dụng khóa chữ ký công khai của chủ thẻ và message digest của PI (bao gồm OI) để kiểm tra chữ ký số để đảm bảo rằng đơn đặt hàng không bị giả mạo trong quá trình truyền và nó đã được ký bằng khóa chữ ký riêng của chủ thẻ.

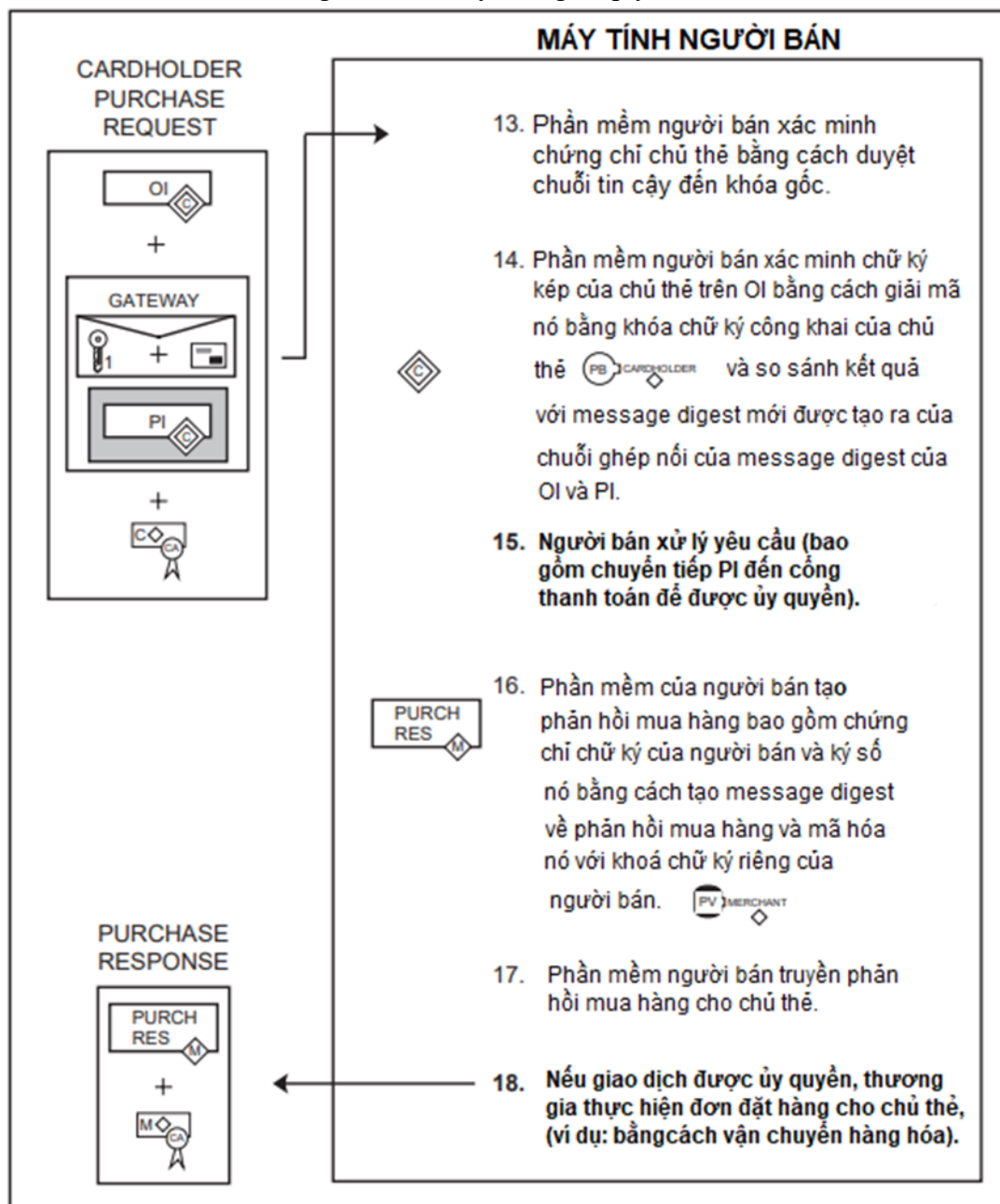
Phần mềm thương gia sau đó xử lý đơn đặt hàng bao gồm ủy quyền thanh toán được mô tả trong Phần 3.5.

Lưu ý: Không cần thiết rằng người bán phải thực hiện giai đoạn ủy quyền trước khi gửi phản hồi cho chủ thẻ. Chủ thẻ có thể xác định sau nếu ủy quyền đã được thực hiện bằng cách gửi thông điệp yêu cầu điều tra đơn hàng.

Sau khi OI được xử lý, phần mềm người bán tạo và ký điện tử một thông báo phản hồi mua hàng, bao gồm chứng nhận chữ ký của người bán và cho biết rằng đơn đặt hàng của chủ thẻ đã được nhận bởi người bán. Phản hồi sau đó được truyền tới chủ thẻ.

Nếu phản hồi ủy quyền (xem Phần 3.5) chỉ ra rằng giao dịch đã được phê duyệt, thương gia sẽ giao hàng hoặc thực hiện các dịch vụ được chỉ định trong đơn đặt hàng.

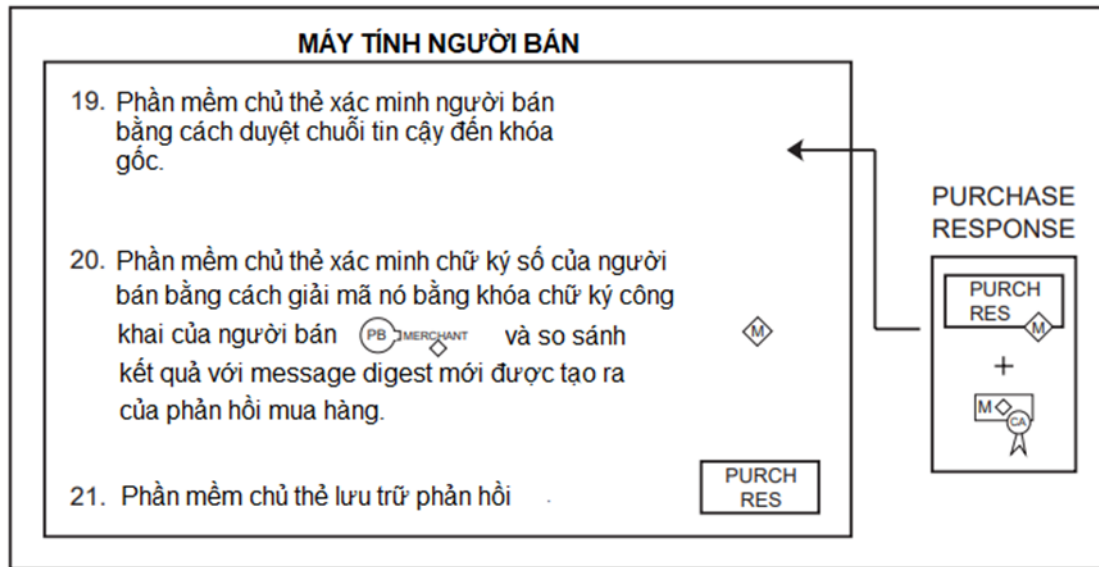
Người bán xử lý thông điệp yêu cầu



Khi phần mềm chủ thẻ nhận được thông báo phản hồi mua hàng từ người bán, nó sẽ xác minh chứng nhận chữ ký của người bán bằng cách duyệt qua chuỗi tin cậy đến khóa gốc. Nó sử dụng khóa chữ ký công khai của người bán để kiểm tra chữ ký số của người bán. Cuối cùng, phải thực hiện một số hành động dựa trên nội dung của thông báo phản hồi, chẳng hạn như hiển thị thông báo cho chủ thẻ hoặc cập nhật cơ sở dữ liệu với trạng thái của đơn đặt hàng.

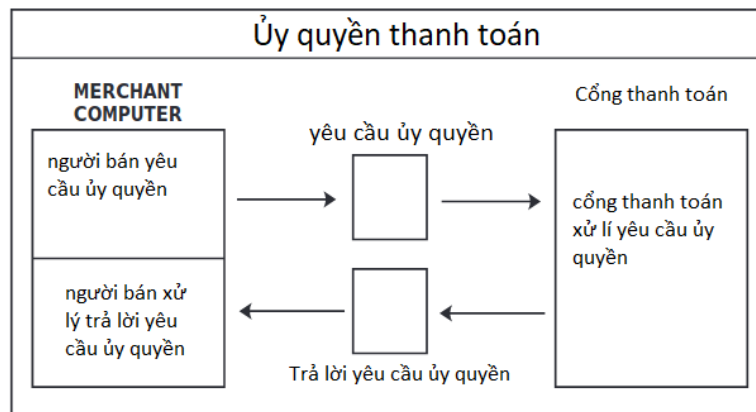
Chủ thẻ có thể xác định trạng thái của đơn đặt hàng (chẳng hạn như liệu nó đã được ủy quyền hay gửi để thanh toán) bằng cách gửi thông điệp điều tra đơn hàng.

Chủ thẻ nhận được phản hồi mua hàng



3.5 Ủy quyền giao dịch

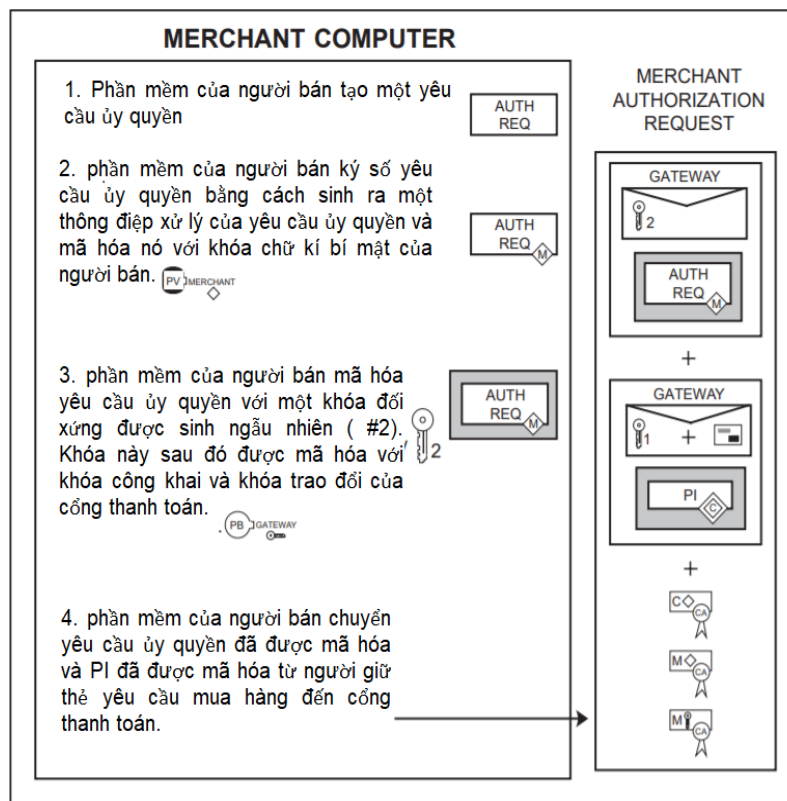
Hình 5 cung cấp cái nhìn tổng quan ở mức độ cao hơn của một quá trình ủy quyền thanh toán của merchant, bao gồm 3 bước cơ bản. Phần chi tiết sau đây sẽ miêu tả từng bước.



Hình 5. Ủy quyền giao dịch

Trong suốt quá trình xử lý 1 đơn đặt hàng từ chủ thẻ, nhà bán lẻ sẽ ủy quyền giao dịch. Phần mềm của nhà bán lẻ sinh và ký một yêu cầu ủy quyền, cái mà bao gồm số lượng cần được ủy quyền, người ủy quyền giao dịch từ OI, và những thông tin khác về giao dịch. Yêu cầu sau đó được mã hóa sử dụng một khóa đối xứng mới được sinh ra, khóa này lần lượt được mã hóa bởi khóa công khai- khóa trao đổi của cổng thanh toán. Khóa này giống với khóa mà chủ thẻ sử dụng để mã hóa gói tin kỹ thuật số của hướng dẫn thanh toán. Yêu cầu ủy quyền và hướng dẫn thanh toán chủ thẻ sau đó được chuyển đến cổng thanh toán.

Chú ý: giao thức SET cũng bao gồm cả giao dịch trao đổi mà cho phép một thương gia ủy quyền một giao dịch và yêu cầu thanh toán trong một thông điệp. Trong khi đó thông điệp bán bao gồm thêm một khối của dữ liệu trong yêu cầu từ thương gia, điều đó mặt khác làm song song hóa quá trình truyền gửi thông điệp được mô tả ở phần này.



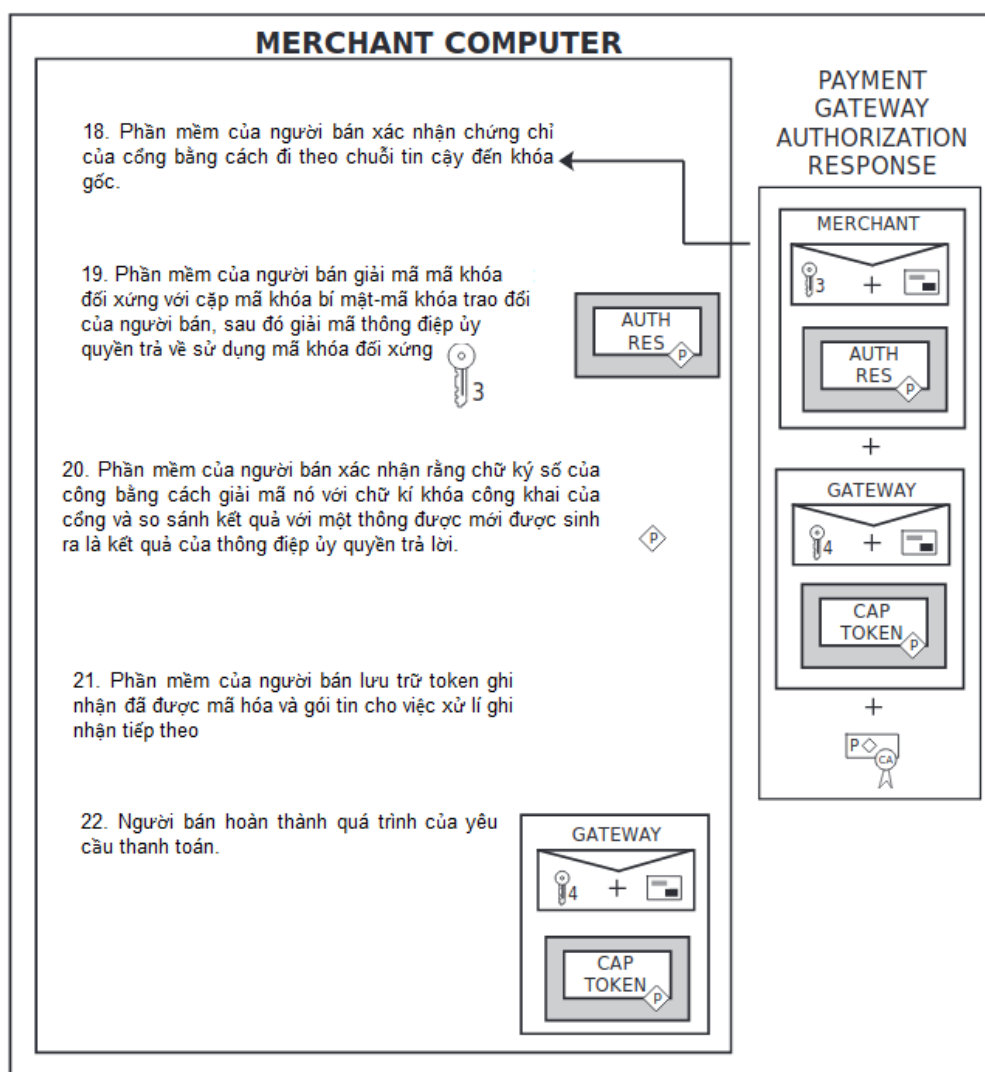
Khi cổng thanh toán nhận được yêu cầu ủy quyền, nó giải mã gói tin kỹ thuật số của yêu cầu ủy quyền để lấy được cặp mã hóa đối xứng. Nó dùng cặp mã hóa đối xứng để giải mã yêu cầu. Sau đó xác nhận chữ ký chứng chỉ của người bán bằng cách đi qua chuỗi tin cậy đến khóa gốc; nó cũng xác nhận rằng chứng chủ vẫn chưa hết hạn. Nó dùng chữ ký khóa công khai của người bán để chắc chắn rằng yêu cầu được ký sử dụng chữ ký khóa bí mật của người bán.

Tiếp theo cổng thanh toán giải mã gói tin kỹ thuật số của hướng dẫn thanh toán để lấy ra cặp mã hóa đối xứng và thông tin tài khoản, Nó sử dụng cặp mã khóa đối xứng để giải mã hướng dẫn thanh toán. Sau đó nó xác nhận chữ ký chứng chỉ của chủ thẻ bằng việc đi theo chuỗi tin cậy đến gốc, nó cũng xác nhận rằng chứng chỉ chưa hết hạn. Tiếp theo nó sử dụng chữ ký khóa công khai của chủ thẻ và thông điệp xử lý của OI (bao gồm trong PI) để kiểm tra chữ ký kỹ thuật số để đảm bảo rằng PI đã không được giả mạo trong giao dịch và nó được ký sử dụng chữ ký khóa bí mật của chủ thẻ.

Tiếp theo, cổng thanh toán xác nhận rằng định danh của giao dịch nhận từ người bán phải khớp với cái ở trong PI của chủ thẻ. Cổng thanh toán sau đó xóa và gửi một yêu cầu ủy quyền cho Issuer trên một hệ thống thanh toán.

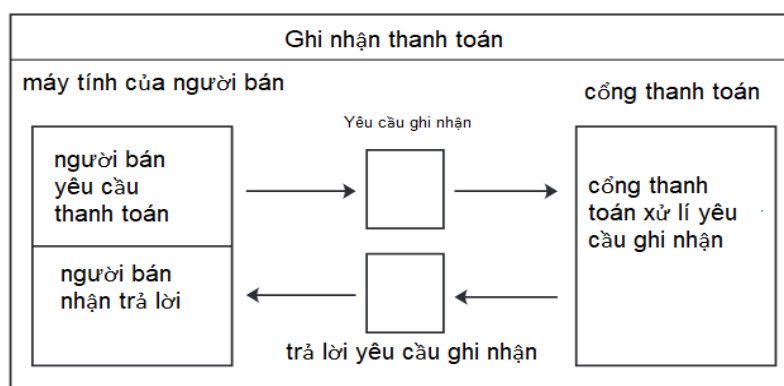
Khi nhận được một thông điệp ủy quyền trả về từ Issuer, Cổng thanh toán sinh ra và ký số một thông điệp ủy quyền trả lời, cái mà chứa cả thông điệp trả lời của Issuer và một bản sao của chữ ký chứng chỉ cổng thanh toán. Thông điệp trả lời cũng bao gồm một token tùy chọn với thông tin của cổng thanh toán sẽ cần để xử lý một yêu cầu ghi nhận. token ghi nhận chỉ được bao gồm nếu được yêu cầu bởi Acquirer.

Thông điệp trả lời sau đó được mã hóa sử dụng một khóa đối xứng mới được sinh ngẫu nhiên, cái mà lần lượt được mã hóa sử dụng khóa công khai - khóa trao đổi của người bán. Thông điệp trả về sau đó được chuyển cho người bán



3.6 Ghi nhận thanh toán

Hình 6 cung cấp cái nhìn tổng quan ở mức cao của một quá trình ghi nhận thanh toán của người bán, nó có 3 bước cơ bản. Chi tiết sẽ được giải thích sau đây cho từng bước.



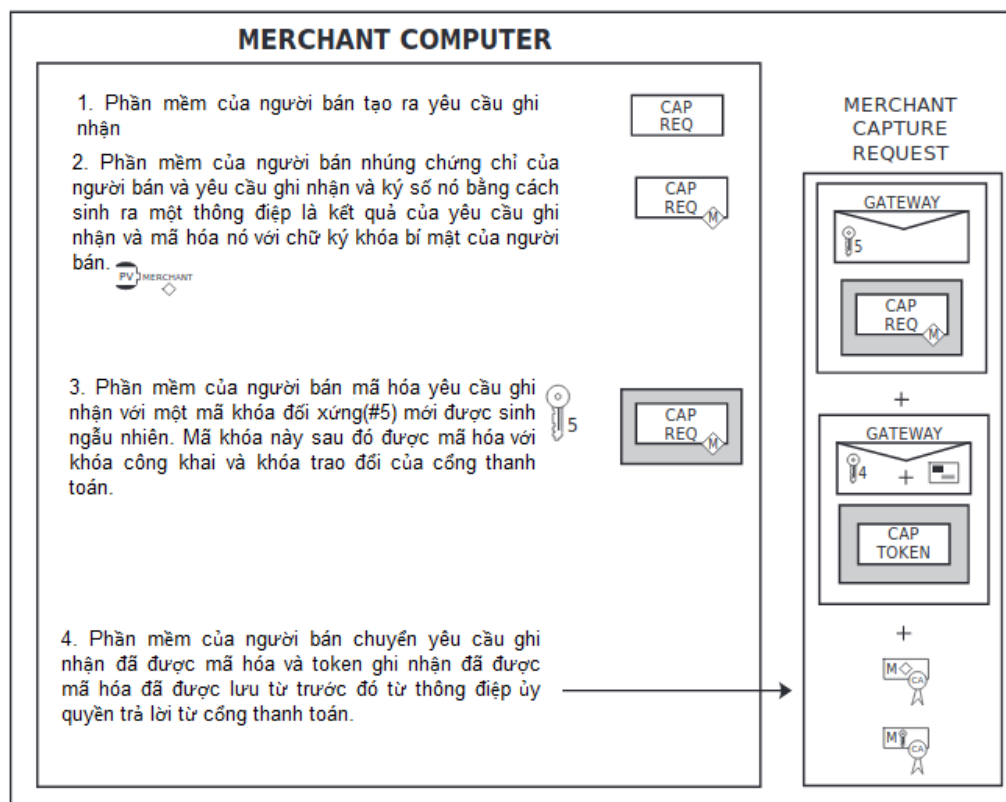
Hình 6. Ghi nhận thanh toán

Sau khi hoàn tất quá trình xử lý một đơn đặt hàng của chủ thẻ, người bán sẽ yêu cầu thanh toán. Sẽ thường có một khoảng thời gian chờ đủ lâu giữa thông điệp yêu cầu ủy quyền mà thông điệp yêu cầu thanh toán.

Phần mềm của người bán sinh ra và ký số một yêu cầu ghi nhận, cái mà chứa trong giao dịch cuối cùng, cái mà định danh giao dịch từ OI, và những thông tin khác của giao dịch. Yêu cầu sau đó được mã hóa sử dụng một mã khóa đối xứng mới được sinh ngẫu nhiên. cái mà lần lượt

được mã hóa sử dụng cặp mã khóa công khai mã khóa trao đổi của cổng thanh toán. Yêu cầu ghi nhận và tùy chọn token ghi nhận nếu nó được chứa trong thông điệp ủy quyền trả về sau được được chuyển đến cổng thanh toán.

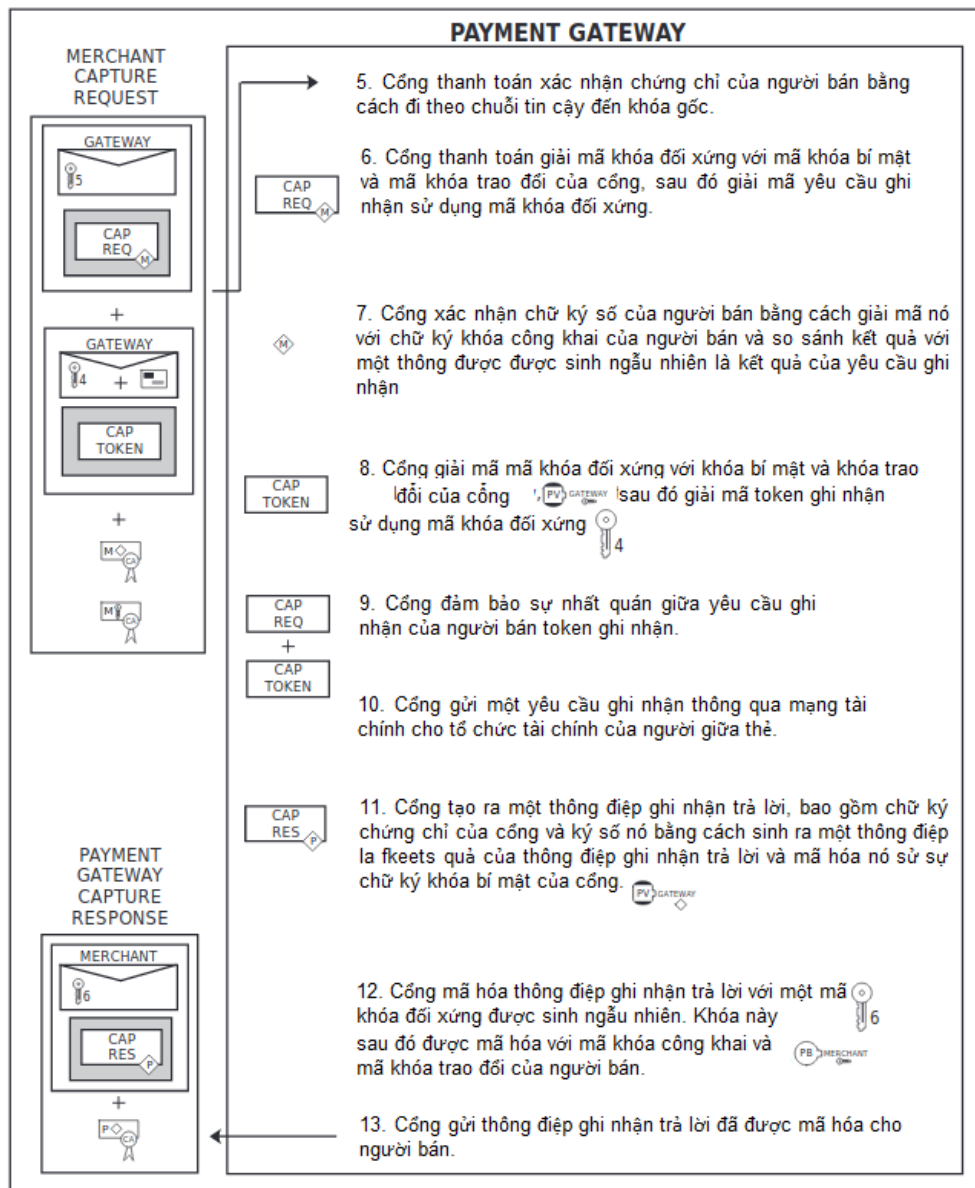
Chú ý: Trong khi quá trình được miêu tả dưới đây chỉ chứa 1 yêu cầu ghi nhận, phần mềm của người bán được cho phép nhóm nhiều yêu cầu lại thành 1 thông điệp.



Khi cổng thanh toán nhận yêu cầu ghi nhận, nó giải mã yêu cầu ghi nhận, nó giải mã gói tin kỹ thuật số của yêu cầu ghi nhận để lấy mã khóa đối xứng. Nó sử dụng mã khóa đối xứng để giải mã yêu cầu, Sau đó nó dùng chữ ký khóa công khai của người bán để đảm bảo yêu cầu đã được ký sử dụng chữ ký khóa bí mật của người bán.

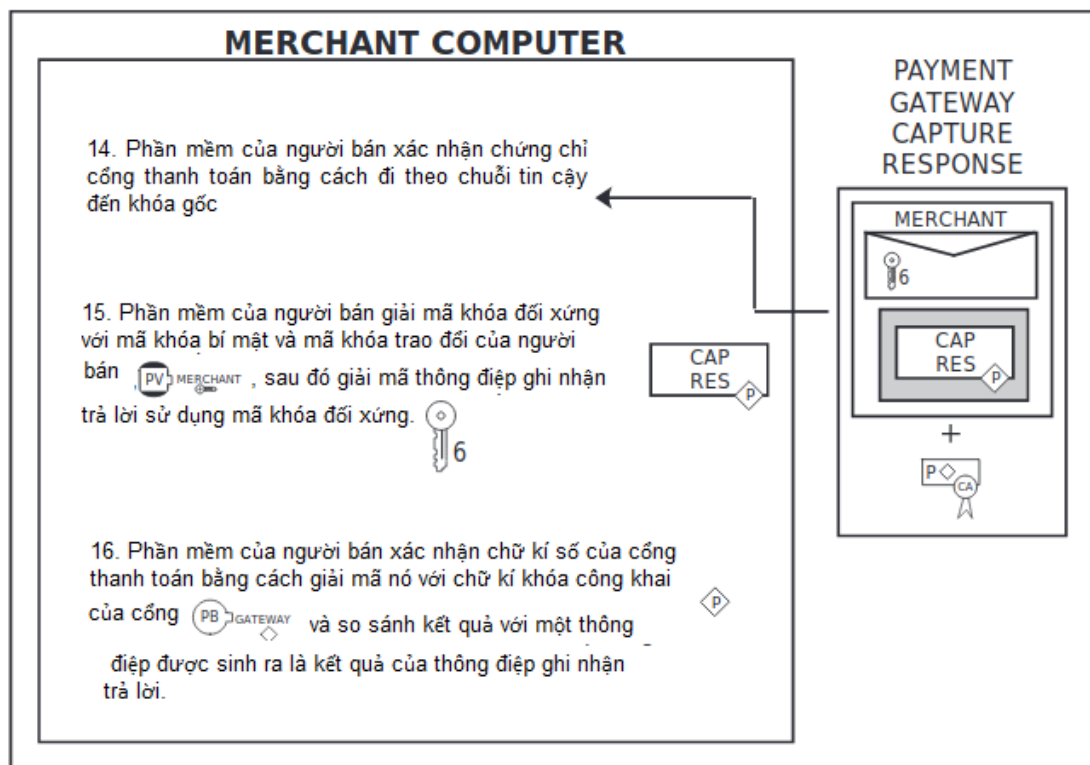
Cổng thanh toán giải mã token ghi nhận và sau đó sử dụng thông tin từ yêu cầu ghi nhận và token ghi nhận để tạo ra một yêu cầu làm sạch, cái mà được gửi tới Issuer thông qua một hệ thống thanh toán thẻ.

Cổng thanh toán sau đó sinh ra và ký số một thông điệp ghi nhận trả lời, cái mà chưa trong đó bản sao của chữ ký chứng chỉ cổng thanh toán. Yêu cầu trả về sau đó được mã hóa sử dụng một cặp mã hóa đối xứng mới được sinh ngẫu nhiên, cái mà lần lượt được mã hóa sử dụng khóa công khai- khóa trao đổi của người bán, Thông điệp trả về sau đó được chuyển cho người bán.



Khi phần mềm của người bán nhận được thông điệp ghi nhận trả về từ cổng thanh toán, nó giải mã gói tin kỹ thuật số để lấy được mã khóa đối xứng. Nó sử dụng mã khóa đối xứng để giải mã thông điệp trả về. Sau đó nó xác nhận chữ ký chứng chỉ cổng thanh toán bằng cách đi theo chuỗi tin cậy đến khoá gốc. Nó sử dụng chữ ký khóa công khai của cổng thanh toán để kiểm tra chữ kí số của cổng thanh toán.

Phần mềm của người bán lưu trữ thông điệp ghi nhận trả lời để sử dụng cho việc đối chiếu với thanh toán nhận được từ Acquirer.



Tài liệu tham khảo

SET Secure Electronic Transaction Specification Book 1: Business Description, Version 1.0, Mastercard and Visa, 1997

Answers to Frequently Asked Questions about Today's Cryptography, Paul Fahn, RSA Laboratories, 1993. (<http://www.rsa.com/rsalabs/faq/>)

Data Encryption Standard, Federal Information Processing Standards Publication 46, 1977.

Applied Cryptography, Second Edition, Bruce Schneier, John Wiley & Sons, Inc., 1996.

"Asymmetric Encryption: Evolution and Enhancements," Don B. Johnson and Stephen M. Matyas, CryptoBytes, volume 2, number 1, Spring 1996

BSAFE 2.1™, RSA Data Security, Inc., 1994.
(http://www.rsa.com/rsa/prodspec/bsafe/rsa_bsaf.htm)

BSAFE 2.1™, RSA Data Security, Inc., 1994.
(http://www.rsa.com/rsa/prodspec/bsafe/rsa_bsaf.htm)

Public-Key Cryptography Standards (PKCS), RSA Data Security, Inc., Version 1.5, revised Nov. 1, 1993.