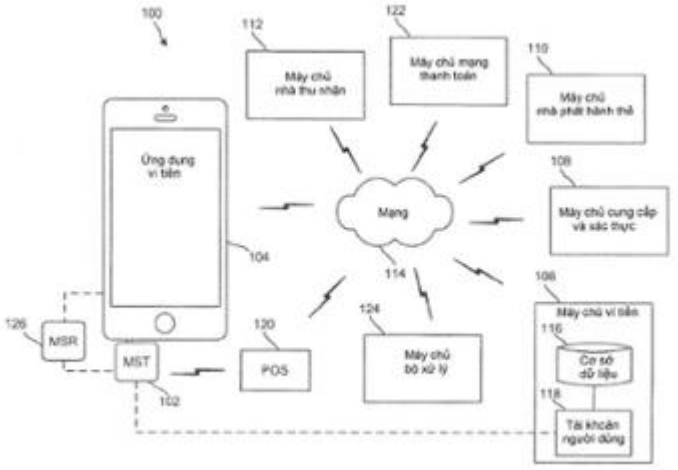
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0027823**
(51)[7] **G06Q 20/36**; G06Q 30/06; G06Q 20/40 (13) **B**

(21) 1-2016-01530 (22) 13/02/2015
(62) 1-2016-01504
(86) PCT/US2015/015855 13/02/2015 (87) WO2015/126753 27/08/2015
(30) 61/942,681 21/02/2014 US; 61/974,696 03/04/2014 US; 14/511,994 10/10/2014 US
(45) 25/04/2021 397 (43) 25/11/2016 344A
(73) SAMSUNG ELECTRONICS CO., LTD. (KR)
129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677, Republic of Korea.
(72) HUANG, Enyang (CN); GRAYLIN, William, Wang (US); WALLNER, George (US).
(74) Công ty Luật TNHH WINCO (WINCO LAW FIRM)

(54) THIẾT BỊ VÀ PHƯƠNG PHÁP TRUYỀN DỮ LIỆU DẢI TỪ CỦA THẺ THANH TOÁN

(57) Sáng chế đề xuất thiết bị, hệ thống, và phương pháp để chuyển đổi một cách an toàn dữ liệu thẻ thanh toán tĩnh hiện có của người dùng thành dữ liệu thẻ động mà có thể được xác thực bởi các nhà phát hành thẻ hoặc bởi nhà cung cấp dịch vụ thay thế, như mạng thanh toán hoặc bộ xử lý mà không cần các nhà phát hành thẻ thực hiện các thay đổi về cơ sở hạ tầng. Dữ liệu động có thể được cung cấp trên MST (magnetic secure transmission device - thiết bị truyền từ tính an toàn) hoặc một cách trực tiếp từ nhà phát hành thẻ hoặc bằng cách sử dụng thiết bị kiểu bộ quẹt. Sáng chế còn đề xuất thiết bị, hệ thống, và phương pháp để cung cấp một cách an toàn thẻ động trên MST bởi nhà phát hành thẻ. Các thẻ động này có thể được sử dụng để truyền dữ liệu rãnh thẻ dùng một lần được biến đổi từ MST đến điểm bán bằng cách sử dụng hệ phương pháp CVV động để tạo ra các mức an toàn cao hơn trong giao dịch.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến việc lưu trữ dữ liệu dải từ và việc truyền an toàn dữ liệu dải từ.

Tình trạng kỹ thuật của sáng chế

Việc truyền dữ liệu dải từ đã được thực hiện chủ yếu bằng cách quẹt thẻ có dải từ qua MSR (magnetic stripe reader - bộ đọc dải từ) để cho phép thực hiện các chức năng thanh toán, ID (identification - nhận dạng) và điều khiển truy nhập. Các ứng dụng ví tiền di động trên các điện thoại thông minh và các máy tính bảng đã và đang gặp khó khăn trong việc tương tác với các thiết bị POS (point of sale - điểm bán) thương nhân hiện có hoặc các thiết bị khác với các MSR. Các thiết bị đầu cuối POS cho phép bộ đọc không tiếp xúc (thường sử dụng, ví dụ, chuẩn ISO-14443) không thường chấp nhận các thức thanh toán NFC (near field communication - truyền thông trường gần) hoặc không tiếp xúc. Sẽ tốn kém và tốn thời gian khi thay thế hàng triệu thiết bị POS thương nhân (hoặc khóa cửa) mà chỉ chấp nhận các thẻ có dải từ, chỉ để tương tác với các điện thoại NFC hoặc các phương tiện truyền khác như các mã vạch.

Ngoài ra, các thẻ thanh toán tài chính chứa số thẻ, được gọi là Số tài khoản chính (Primary Account Number) hoặc PAN, mục đích của chúng là để nhận dạng tài khoản mà thanh toán được thực hiện cho. Các thẻ còn mang Ngày hết hạn, ngày này chỉ thị khi nào thẻ hết hạn. Hầu hết các thẻ còn mang, trong dữ liệu dải từ, Trị số xác định tính hợp lệ của thẻ (còn được biết là CVV1) được tạo ra bằng mật mã, nó ngăn thẻ hợp lệ được tạo ra từ thông tin về PAN và Ngày hết hạn của nó. Thông thường, các thẻ được thay thế sau khoảng 2 đến 3 năm, khi dải từ bị mòn và các nhà phát hành không muốn thẻ hoạt động đến vô hạn.

Ngày nay PAN được sử dụng không chỉ để nhận dạng tài khoản, mà còn để cấp phép cho các khoản phí trong các giao dịch CNP (Card-Not-Present - Không có mặt thẻ) (ngược lại với các giao dịch CP (Card-Present - Có mặt thẻ) trong đó thẻ được quẹt theo cách vật lý ở thiết bị đầu cuối POS), phần rất lớn trong số chúng là các giao

dịch Internet, nhưng cũng bao gồm các đặt hàng qua điện thoại và các đặt hàng qua thư. Nhận biết đơn giản về PAN, Ngày hết hạn, và tên trên thẻ là đủ để tính phí các khoản mua CNP đối với tài khoản. CVV-2, như được biết đến trong lĩnh vực, là trị số gồm 3 hoặc 4 chữ số được in lên trên thẻ hoặc dải chữ ký, nhưng không được mã hóa trên dải từ, để xác nhận là khách hàng có quyền sở hữu thẻ. Trong khi tỷ lệ phần trăm lớn các trang thương mại điện tử cũng yêu cầu CVV-2 cho các giao dịch, thì nhiều trang lại không yêu cầu.

Khó giữ bí mật đối với PAN và Ngày hết hạn: chúng được in ở phía trước thẻ và nằm trong dữ liệu dải từ hoặc dữ liệu vi mạch của thẻ. Trong giao dịch POS, dải từ hoặc vi mạch được đọc bởi thiết bị đầu cuối và dữ liệu của nó (bao gồm PAN, ngày hết hạn, và CVV2) được truyền qua hệ thống của nhà bán lẻ đến nhà thu nhận và sau đó đến nhà phát hành thẻ. PAN, và với phạm vi nhỏ hơn là Ngày hết hạn, được sử dụng cho một số chức năng bởi các hệ thống nhà bán lẻ và không thể được che.

Dữ liệu thẻ vi mạch hoặc dải từ là mục tiêu ăn trộm dữ liệu, khi chuyển tiếp hoặc khi nằm trong bộ nhớ. Khi là dữ liệu tĩnh, dữ liệu dải từ bị chặn lại và sao chép, và bị một số sự tấn công. Dữ liệu bị lấy cắp, mà từ đó PAN và Ngày hết hạn có thể được lấy ra một cách dễ dàng, có thể được sử dụng trong các giao dịch CNP gian lận. Thẻ vật lý có thể bị đánh cắp dữ liệu (skim) nhờ đọc dữ liệu dải từ trên thẻ, hoặc đưa thiết bị đọc đến gần các thiết bị đầu cuối POS của nhà bán lẻ để thu thập dữ liệu rãnh dải từ bao gồm PAN và Ngày hết hạn và tên trên thẻ. Thiết bị nghe lén (sniffing) cũng có thể được sử dụng để lấy dữ liệu rãnh từ các thẻ không tiếp xúc trong túi tiền và ví tiền của những người đi mua hàng không nghi ngờ ở các hãng bán lẻ. Phần mềm độc hại (malware) trong hệ thống POS của các nhà bán lẻ cũng có thể được sử dụng để thu thập dữ liệu thẻ khi định tuyến tới bộ xử lý thanh toán. Dữ liệu bị lấy cắp này có thể chứa PAN và Ngày hết hạn, trong cả giao dịch dải từ và thẻ thông minh (ví dụ, thẻ EMV (Europay, MasterCard and Visa)) và có thể được sử dụng để gian lận CNP. Ngoài ra, dữ liệu dải từ được thu thập còn bao gồm CVV1, trong khi dữ liệu thẻ trực tuyến được thu thập có thể bao gồm CVV2. Điểm yếu chính của cả CVV1 và CVV2 đó là chúng tĩnh: một khi được biết chúng có thể được sử dụng trong các giao dịch gian lận.

Bản chất kỹ thuật của sáng chế

Sáng chế đề cập đến các thiết bị, hệ thống và phương pháp liên quan đến thiết bị truyền và lưu trữ dải từ (còn được gọi là thiết bị MST (magnetic secure transmission - truyền từ tính an toàn)) để sử dụng cùng với nền và ứng dụng ví tiền di động để thu thập, lưu trữ và truyền dữ liệu thẻ dải từ đến các thiết bị đầu cuối POS (point of sale - điểm bán) thông thường của các thương nhân và các thiết bị khác với các MSR (magnetic stripe reader - bộ dọc dải từ) hoặc các hệ thống thanh toán hóa đơn trực tuyến, trong các môi trường vật lý và ảo.

Sáng chế còn đề cập đến các thiết bị, hệ thống và phương pháp để chuyển đổi dữ liệu thẻ tĩnh (ví dụ, CVV1 hoặc CVV2) thành các bản mật mã động mà chỉ có thể được sử dụng một lần, và không thể được phát lại bởi những người gian lận, và các thiết bị di động đòn bẩy để phân phối thông tin thanh toán bao gồm các bản mật mã lại cho nhà phát hành thẻ để xác thực, mà không phải thay đổi cơ sở hạ tầng được chấp nhận hiện có của thương nhân dù nó dành cho thanh toán vật lý qua POS hoặc thanh toán từ xa qua thanh toán hóa đơn trực tuyến. Các thiết bị, hệ thống, và phương pháp cho phép các người dùng tự động chuyển đổi dữ liệu thẻ tĩnh thành dữ liệu thẻ sử dụng một lần động mà có thể được xác thực bởi mạng thanh toán hoặc bộ xử lý thay mặt cho hàng nghìn nhà phát hành thẻ như một dịch vụ, mà không cần tích hợp và thay đổi cơ sở hạ tầng bởi mỗi nhà phát hành.

Theo một khía cạnh, bản mật mã động mà có thể được gọi là dCVV (dynamic-CVV - CVV động) được sử dụng để giữ an toàn cho các thanh toán thẻ. dCVV được tạo ra mới với số tài khoản chính (PAN) cộng khóa, sự hết hạn hoặc ngày hết hạn (EXP), dấu thời gian và bộ đếm, khi thẻ được sử dụng cho thanh toán trong cả giao dịch CNP (Card-Not-Present - Không có mặt thẻ) và CP (Card-Present - Có mặt thẻ). dCVV, mà được tạo ra bằng mật mã, không thể được tạo ra mà không nhận biết về dữ liệu thẻ và khóa bí mật. Ngoài ra, mỗi dCVV chỉ hợp lệ trong khoảng thời gian ngắn. Điều này ngăn cản sự tấn công phát lại được mô tả trên đây, do việc tái sử dụng dCVV từ giao dịch được giám sát trước đó sẽ dẫn đến lỗi cấp phép.

Theo một khía cạnh khác, nhà phát hành thẻ hoặc nhà cung cấp dịch vụ thay thế có thể phân biệt các giao dịch CP mà sử dụng công nghệ dCVV, bởi vì thuật toán xác

nhận tính hợp lệ được sử dụng là khác đối với giao dịch dCVV như ngược lại với các giao dịch CP dải từ thông thường. Các giao dịch dCVV có thể được nhận dạng nhờ thay thế EXP của dữ liệu thẻ với số tương đương với ngày cách xa trong tương lai mà có thể nhận biết được bởi nhà phát hành hoặc nhà cung cấp dịch vụ. Việc này che EXP trong giao dịch thanh toán trong khi cung cấp thẻ cờ thuận tiện cho nhà phát hành để nhận ra thẻ là đang ở trong chế độ dCVV. Các cờ khác có thể được sử dụng để chỉ thị thẻ ở trong chế độ dCVV, như cờ trong trường tùy ý của dữ liệu rãnh được sử dụng để chỉ thị chế độ dCVV. PAN còn có thể được đăng ký trong cơ sở dữ liệu của nhà phát hành hoặc nhà cung cấp dịch vụ làm thẻ dCVV.

Khái niệm của dCVV trong miền của MST vốn cũng áp dụng cho các giao dịch CNP. Trong các giao dịch CNP, mã 3 chữ số được tạo ra theo cách động (hoặc mã 4 chữ số trong trường hợp các thẻ American Express) được lấy từ ứng dụng ví tiền di động, được tính toán theo cách động tại thời điểm yêu cầu, được nhập vào trong ứng dụng hoặc trang web thanh toán hóa đơn. EXP được chắn cũng được lấy từ ứng dụng ví tiền di động, để được nhập vào cũng sử dụng ngày cách xa trong tương lai chỉ thị rằng đây là giao dịch CNP dCVV. Theo cách này cả CVV-2 và EXP ban đầu đều được giấu khỏi người tấn công đang giám sát giao dịch. Hơn nữa, việc chặn giao dịch CNP cụ thể không dẫn đến việc người tấn công sử dụng thông tin trong một giao dịch khác, bởi vì mã CVV được tính toán trong thời gian thực và thay đổi giữa các giao dịch CNP, và được đóng dấu thời gian sao cho nó sẽ hết hạn sau thời gian ngắn.

Để chuyển đổi dữ liệu thẻ tĩnh hiện có thành dữ liệu thẻ động cho các người dùng di động mà không yêu cầu mỗi nhà phát hành thẻ thay đổi cơ sở hạ tầng cung cấp của họ, các thiết bị, hệ thống, và phương pháp cho phép các chủ thẻ chuyển đổi một cách hiệu quả dữ liệu thẻ dải từ hiện có thành dữ liệu thẻ động được tạo thẻ bài động bằng cách sử dụng các thiết bị di động mà không yêu cầu các nhà phát hành thẻ thiết lập hệ thống cung cấp di động từ xa riêng rẽ. Nhà phát hành thẻ, bộ xử lý của nhà phát hành, hoặc mạng thanh toán của nhà phát hành có thể làm chủ máy chủ xác thực cung cấp (PAS) để xác thực dCVV được đóng gói trong khi truyền MST, hoặc dCVV2 cho các giao dịch trực tuyến, và xác nhận tính hợp lệ cho nhà phát hành là dữ liệu thanh toán động là xác thực, hoặc xác nhận tính hợp lệ và trả lại dữ liệu rãnh ban đầu (trong trường hợp mạng thanh toán) hoặc CVV2 ban đầu cho nhà phát hành hoặc bộ xử lý

của nó sao cho mạng thanh toán có thể thực hiện dịch vụ xác thực (hoặc dịch vụ tạo thẻ bài) thay mặt cho nhà phát hành thẻ. Điều này có thể tăng mạnh tốc độ chuyển đổi từ dữ liệu thẻ tĩnh trong trường thành dữ liệu thẻ được tạo thẻ bài động để nâng cao độ an toàn cho các giao dịch CP và CNP.

Mô tả vắn tắt các hình vẽ

Các phương án thực hiện của các thiết bị, hệ thống, và phương pháp được minh họa trên các hình vẽ kèm, các hình vẽ này nhằm làm ví dụ và không giới hạn sáng chế, trong đó các số chỉ dẫn giống nhau nhằm để chỉ các phần tương tự hoặc tương ứng, và trong đó:

Fig.1 là sơ đồ chức năng về tổng quan của hệ thống theo các khía cạnh của sáng chế;

Fig.2 là sơ đồ tiến trình của phương pháp hoạt động để khởi tạo MST theo các khía cạnh của sáng chế;

Fig.3 là sơ đồ tiến trình của phương pháp cung cấp thẻ tĩnh dựa trên việc người dùng quẹt thẻ theo các khía cạnh của sáng chế;

Fig.4 là sơ đồ tiến trình của phương pháp cung cấp thẻ tĩnh từ nhà phát hành thẻ theo các khía cạnh của sáng chế;

Fig.5 là sơ đồ tiến trình của phương pháp cung cấp thẻ theo cách động theo các khía cạnh của sáng chế;

Fig.6 là sơ đồ tiến trình của phương pháp cung cấp thẻ theo các khía cạnh của sáng chế;

Fig.7 là sơ đồ tiến trình của phương pháp cung cấp thẻ động theo các khía cạnh của sáng chế;

Fig.8 là sơ đồ tiến trình của phương pháp thực hiện dCVV (dynamic-CVV - CVV động) theo các khía cạnh của sáng chế;

Fig.9 là sơ đồ tiến trình của một phương pháp khác để thực hiện dCVV theo các khía cạnh của sáng chế;

Fig.10 là sơ đồ thể hiện sự biến đổi ngày hết hạn của dữ liệu thẻ theo các khía

cạnh của sáng chế;

Fig.11 là sơ đồ tiến trình dạng khối của phương pháp thực hiện dCVV cho các giao dịch thương mại điện tử theo các khía cạnh của sáng chế; và

Fig.12 là sơ đồ khối chức năng của MST theo các khía cạnh của sáng chế.

Mô tả chi tiết sáng chế

Các phương án chi tiết của các thiết bị, hệ thống và phương pháp được bộc lộ trong bản mô tả này, tuy nhiên, cần hiểu rằng các phương án được bộc lộ này chỉ nhằm làm ví dụ cho các thiết bị, hệ thống, và phương pháp, mà có thể được biểu hiện dưới nhiều dạng khác nhau. Do đó, các chi tiết về chức năng cụ thể được bộc lộ trong bản mô tả này không được hiểu là nhằm giới hạn, mà chỉ là cơ sở cho các điểm yêu cầu bảo hộ và là cơ sở biểu hiện để hướng dẫn người có hiểu biết trung bình trong lĩnh vực thực hiện sáng chế theo các cách khác nhau.

Nói chung, sáng chế đề cập đến các thiết bị truyền an toàn và lưu trữ dữ liệu dải từ đòn bẩy để phân phối dữ liệu thanh toán sử dụng một lần bằng mật mã an toàn trên các cơ sở hạ tầng chấp nhận thanh toán hiện có.

Tổng quan về hệ thống 100 liên quan đến việc truyền và cung cấp thẻ an toàn theo một phương án minh họa được mô tả theo Fig.1. Toàn bộ hệ thống 100 bao gồm MST 102, thiết bị truyền thông di động 104, máy chủ ví tiền 106, máy chủ cung cấp và xác thực 108, máy chủ nhà phát hành thẻ 110, máy chủ nhà thu nhận 112, POS (point of sale - điểm bán) 120, máy chủ mạng thanh toán 122, máy chủ bộ xử lý 124 (ví dụ, máy chủ bộ xử lý bên thứ ba của nhà phát hành), và bộ đọc dải từ được mã hóa 126 (MSR) mà có thể là một phần của MST 102 (như được minh họa trên Fig.12) hoặc làm việc riêng với ứng dụng ví tiền trên thiết bị truyền thông di động 104. MST 102 giao tiếp qua giao diện với thiết bị truyền thông di động 104 hoặc có thể được cài vào trong thiết bị truyền thông di động 104, và thiết bị truyền thông di động 104 truyền thông với máy chủ ví tiền 106, máy chủ cung cấp và xác thực 108, máy chủ nhà phát hành thẻ 110, và máy chủ nhà thu nhận 112 qua mạng 114. Mỗi trong số máy chủ ví tiền 106, máy chủ cung cấp và xác thực 108, máy chủ nhà phát hành thẻ 110, máy chủ nhà thu nhận 112, máy chủ mạng thanh toán 122, và máy chủ bộ xử lý 124, cũng có thể

truyền thông với nhau qua mạng 114.

Theo một khía cạnh, máy chủ ví tiền 106 có thể bao gồm một hoặc nhiều cơ sở dữ liệu 116 và tài khoản người dùng 118. Một hoặc nhiều cơ sở dữ liệu 116 có thể lưu trữ dữ liệu kết hợp của MST 102 và các tài khoản người dùng 118, và một hoặc nhiều khóa được sử dụng bởi MST 102 và/hoặc máy chủ ví tiền 106. MST 102 có thể được đăng ký với tài khoản người dùng 118, như được mô tả chi tiết hơn sau đây.

Cần hiểu rõ rằng máy chủ cung cấp và xác thực 108, máy chủ nhà phát hành thẻ 110, và máy chủ nhà thu nhận 112 còn có thể bao gồm một hoặc nhiều cơ sở dữ liệu và thành phần khác, như, phần mềm và/hoặc phần cứng để cho phép thực hiện các phương pháp được bộc lộ trong bản mô tả này.

Như được minh họa, MST 102 có thể là khóa điện tử (dongle) mà có thể được kết nối với và ngắt kết nối khỏi thiết bị truyền thông di động 104. MST 102 có thể truyền thông với thiết bị truyền thông di động 104 qua cổng audio và/hoặc qua các loại giao diện truyền thông khác, ví dụ bao gồm, nhưng không giới hạn vào, cổng USB, giao diện Apple 30 chân cắm hoặc 9 chân cắm, giao diện Bluetooth, NFC (near field communication - truyền thông trường gần), và các giao diện nối tiếp khác. Trong khi MST 102 được minh họa như là khóa điện tử, MST có thể là loại thiết bị ngoại vi khác mà truyền thông với thiết bị truyền thông di động 104 thông qua giao diện không tiếp xúc, như Bluetooth hoặc NFC; hoặc MST 102 có thể được cài vào bên trong thiết bị truyền thông di động 104 như một phần của thiết bị truyền thông di động 104.

Theo một khía cạnh, người dùng có thể thiết lập tài khoản người dùng 118 trên máy chủ ví tiền 106, ví dụ, nhờ tải xuống và/hoặc cài đặt ứng dụng ví tiền lên thiết bị truyền thông di động 104. Ứng dụng ví tiền 104 có thể là giao diện cho người dùng để xem danh sách các thẻ sẵn có cho các giao dịch CNP (Card-Not-Present - Không có mặt thẻ) và CP (Card-Present - Có mặt thẻ). Theo một khía cạnh, người dùng có thể chọn hoặc lựa chọn thẻ và truyền dữ liệu thẻ tương ứng với thẻ (ví dụ, dữ liệu rãnh thẻ) bằng cách sử dụng MST 102, trong chế độ tĩnh hoặc chế độ dCVV (dynamic-CVV - CVV động). Tương tự, khi thực hiện các giao dịch CNP, người dùng có thể xem Ngày hết hạn (EXP) và CVV-2 được tính toán theo cách động và sử dụng chúng để điền các mẫu web thanh toán hóa đơn để thực hiện giao dịch CNP dCVV.

Người dùng còn có thể thiết lập tài khoản người dùng 118 bằng cách sử dụng máy tính được kết nối với mạng 114 nhờ truy nhập cổng web tài khoản người dùng. Để thiết lập tài khoản người dùng 118, người dùng có thể chỉ rõ tên người dùng, mật khẩu và PIN cá nhân. Mật khẩu có thể được sử dụng để đăng nhập ứng dụng ví trên thiết bị truyền thông di động 104. Khi người dùng được đăng nhập, PIN cá nhân có thể được sử dụng để nhập vào phần thẻ thanh toán của ứng dụng ví tiền, cũng như để mở khóa ứng dụng ví tiền.

Người dùng có thể tùy chọn thêm MST 102 vào tài khoản người dùng 118 nhờ chỉ rõ GUID (globally unique identifier - phần tử nhận dạng duy nhất toàn cầu) của MST 102 (trong bản mô tả này còn được gọi là ID_{MST}). PIN (chỉ có người dùng biết được) được sử dụng để xác thực với MST 102 để hoạt động với dữ liệu thẻ bất kỳ được lưu trữ trên MST 102. Bản sao của PIN còn có thể được lưu trữ trên máy chủ ví tiền 106 và được sử dụng như được mô tả sau đây. Hoạt động của MST 102 sử dụng việc xác thực dựa trên PIN có thể được thực hiện cùng với hoặc không cùng với thiết bị truyền thông di động 104 đang được kết nối với máy chủ ví tiền 106 qua mạng 114. Nó cho phép MST 102 được làm hoạt động để sử dụng dữ liệu thẻ được lưu trên MST 102, thậm chí khi không có kết nối mạng nào tồn tại.

MST 102 có thể lưu trữ dữ liệu thẻ dải từ nhờ hoặc là tải ban đầu khi sản xuất, tải qua mạng truyền thông không dây sau khi thiết lập tài khoản người dùng 118, và/hoặc nhờ khách hàng tải dữ liệu (các) thẻ của chính họ một cách trực tiếp vào trong MST 102 sử dụng MSR được mã hóa được gợi ý bởi ứng dụng ví tiền di động. MST 102 có thể truyền dữ liệu thẻ dải từ trong cả chế độ tĩnh (trong đó nó truyền dữ liệu ban đầu mà không biến đổi) và trong chế độ dCVV (trong đó một phần dữ liệu được tính toán theo cách động mỗi lần trong khi truyền). Nói chung, người dùng là người đã thiết lập tài khoản người dùng, ví dụ, trên máy chủ ví tiền 106 thông qua cơ sở hạ tầng điện toán đám mây (như qua mạng 114), và đã khởi tạo ứng dụng ví tiền trên thiết bị truyền thông di động 104 của họ.

Phương pháp 200 để khởi tạo MST 102, có ID thiết bị duy nhất, đối với tài khoản người dùng 118 theo một phương án minh họa được mô tả theo Fig.2. MST được khởi tạo hoặc đăng ký lần đầu đối với tài khoản người dùng bằng cách cắm vào

hoặc kết nối MST với thiết bị truyền thông di động, được minh họa bởi khối 202. Khi kết nối MST với thiết bị truyền thông di động, ứng dụng ví tiền nhận biết MST và đăng ký MST với tài khoản người dùng của người dùng, được minh họa bởi khối 204. Khi MST đã được đăng ký và được kết nối với tài khoản người dùng thích hợp, MST và tài khoản người dùng có thể thực hiện việc bắt tay, được minh họa bởi 206, và gửi và nhận các lệnh, được minh họa bởi khối 208.

Khi MST đã được đăng ký với tài khoản người dùng, người dùng có thể sử dụng ứng dụng ví tiền để tải các thẻ của họ nhờ quẹt các thẻ lên MSR lắp sẵn của MST hoặc MSR riêng rẽ mà có thể được kết nối với MST hoặc thiết bị truyền thông di động. Dữ liệu thẻ có thể được số hóa và được mã hóa, và được lưu trữ trong MST để sử dụng sau. Ví dụ, như được minh họa trên Fig.1, các thẻ có thể được sử dụng bởi MST 102 và được gửi đến POS (point of sale - điểm bán) 120 để thực hiện giao dịch. Theo khía cạnh này, POS 120 còn có thể truyền thông với một hoặc nhiều trong số máy chủ ví tiền 106, máy chủ cung cấp và xác thực 108, máy chủ nhà phát hành thẻ 110, và/hoặc máy chủ nhà thu nhận 112, qua mạng 114.

Phương pháp 300 để cung cấp một cách an toàn thẻ tĩnh dựa trên việc người dùng quẹt thẻ theo một phương án minh họa được mô tả theo Fig.3. Như được sử dụng trong bản mô tả này, "tĩnh" có nghĩa là dữ liệu thẻ giống nhau được truyền đến POS mỗi lần khi được sử dụng. Theo phương án này, người dùng có thể sử dụng thiết bị có bộ quẹt được tích hợp vào trong hoặc được ghép với MST để tải các thẻ vào trong MST của người dùng.

Người dùng quẹt thẻ (ví dụ, thẻ thanh toán hoặc loại thẻ khác bao gồm dữ liệu thẻ từ) vào bộ quẹt trong MST hoặc thiết bị phụ có bộ quẹt riêng rẽ được ghép với MST (302). Việc này cung cấp dữ liệu thẻ bao gồm dữ liệu rãnh thẻ (nghĩa là dữ liệu tương ứng với thẻ) ("TRACK") cho MST. Sau đó, MST mã hóa TRACK bằng cách sử dụng khóa ($K_{working}$) (304) và gửi TRACK được mã hóa và KSN (key serial number - số khóa nối tiếp) (ví dụ, KSN 10-byte) đến thiết bị truyền thông di động (306). Theo một khía cạnh, KSN chứa bộ đếm tăng đơn điệu; theo đó việc quẹt cùng một thẻ hai lần sẽ tạo ra hai đoạn văn bản mã hóa riêng biệt. MST còn có thể gửi một số thông tin phụ (A*) mà có thể được sử dụng bởi máy chủ ví tiền khi máy chủ ví tiền sau đó thực

hiện việc xác nhận chữ ký, như được mô tả sau đây. Theo một ví dụ, MST gửi phần sau đây đến thiết bị truyền thông di động: $\{TRACK\}_{K_{working}}$, KSN, A*, trong đó các dấu ngoặc chỉ thị chức năng mã hóa.

Thiết bị truyền thông di động hỏi MST về phần tử nhận dạng (ID_{MST}) của nó và phiên lúc này R_{MST} (308). Để đáp lại câu hỏi, MST gửi ID_{MST} và R_{MST} đến thiết bị truyền thông di động (310). Thiết bị truyền thông di động chuyển tiếp thông tin này (ví dụ, ID_{MST}, R_{MST}, $\{TRACK\}_{K_{working}}$, KSN, A*) đến máy chủ ví tiền, cộng (các) ủy nhiệm đầu vào của người dùng (ví dụ, tên người dùng và mật khẩu) cho máy chủ ví tiền để xác thực (312).

Máy chủ ví tiền xác thực người dùng bằng cách sử dụng tên người dùng và mật khẩu, và còn kiểm tra để xem liệu ID_{MST} hiện thời có được kết nối với tài khoản ví tiền (314) của người dùng. Máy chủ ví tiền còn có thể xác nhận tính hợp lệ và tính đơn điệu của KSN và độc lập tính toán $K_{working}$ (316). Nếu mọi thứ được xác nhận, máy chủ ví tiền giải mã dữ liệu rãnh được mã hóa và thu được TRACK (318). Máy chủ ví tiền còn có thể thực hiện kiểm tra để đảm bảo dữ liệu nhận được là hợp lệ (320). Ví dụ, máy chủ ví tiền có thể kiểm tra là TRACK chứa các chuỗi ISO-7812 hợp lệ. Đối với các thẻ tài chính, cả dữ liệu rãnh 1 và dữ liệu rãnh 2 sẽ có mặt. Đối với các thẻ phi tài chính (ví dụ, các thẻ quà tặng), ít nhất một trong các rãnh sẽ có mặt. Máy chủ ví tiền còn có thể thực hiện LRC (longitudinal redundancy check - kiểm tra tính dư dọc) để kiểm tra sự chính xác của dữ liệu. Đối với các thẻ tài chính, tên chủ thẻ từ dữ liệu rãnh 1 phải phù hợp với tên người dùng tài khoản ví tiền của người dùng trên hồ sơ, và ngày hết hạn của thẻ phải hợp lệ (nghĩa là thẻ chưa hết hạn).

Nếu máy chủ ví tiền được thỏa mãn, thì máy chủ ví tiền mã hóa lại TRACK bằng cách sử dụng khóa đã được biết với MST (K_{MST}) (322) và gửi lại thẻ bài AC (AddCard - Thêm thẻ) đến thiết bị truyền thông di động (324) qua phiên SSL/TLS. Thẻ bài AC có thể bao gồm R_{MST}, dấu thời gian được tạo ra bởi máy chủ (R_S), TRACK, và A* được mã hóa bằng cách sử dụng K_{MST} (ví dụ, $\{R_{MST}, R_S, TRACK, A^*\}_{K_{MST}}$).

Thiết bị truyền thông di động chuyển tiếp thẻ bài AC đến MST (326) mà không dịch. MST giải mã thẻ bài AC bằng cách sử dụng K_{MST} và xác nhận R_{MST} về tính thích

hợp (328). Nếu mọi thứ xác nhận, MST ký thác TRACK và hoạt động thêm thẻ hoàn thành (330). Việc sử dụng mã hóa điểm tới điểm và ngẫu nhiên lúc này bảo vệ một cách thích hợp cho các yêu cầu về tính bảo mật, tính xác thực và tính mới.

Phương pháp 400 để cung cấp một cách an toàn thẻ tĩnh từ nhà phát hành thẻ theo một phương án minh họa được mô tả theo Fig.4. Theo phương án này, nhà phát hành thẻ có thể đẩy dữ liệu thẻ qua vô tuyến hoặc qua mạng vào trong MST. Phương pháp này tương tự với phương pháp cung cấp tĩnh được mô tả trên đây, ngoại trừ là dữ liệu thẻ (bao gồm TRACK) bắt nguồn từ máy chủ nhà phát hành thẻ và được gửi từ máy chủ nhà phát hành thẻ đến máy chủ ví tiền, và sau đó được đẩy một cách an toàn vào trong MST. Người dùng khởi đầu quy trình nhờ chỉ định máy chủ nhà phát hành nào để gửi yêu cầu thẻ đến. Sau khi thiết lập ban đầu, máy chủ nhà phát hành có thể thông báo cho người dùng khi nào các thẻ mới sẵn có để tải xuống. Sau đó, người dùng có thể xác thực với máy chủ nhà phát hành và tải xuống dữ liệu thẻ thực.

Khi có yêu cầu của người dùng, thiết bị truyền thông di động hỏi MST về ID_{MST} và phiên lúc này R_{MST} (402), và MST gửi ID_{MST} và R_{MST} đến thiết bị truyền thông di động (404). Với đầu vào từ người dùng, thiết bị truyền thông di động chuyển tiếp thông tin này đến máy chủ ví tiền, cộng ủy nhiệm của người dùng (ví dụ, ID_{MST}, R_{MST}, tên người dùng, mật khẩu) (406). Người dùng còn có thể nhập vào thông tin (B*) để xác thực người dùng với máy chủ nhà phát hành thẻ (ví dụ, nhận dạng của nhà phát hành thẻ và (các) ủy nhiệm ngân hàng trực tuyến của người dùng). Máy chủ ví tiền gửi B* đến máy chủ nhà phát hành thẻ (408) để thu được dữ liệu thẻ (bao gồm TRACK). Sau đó, máy chủ ví tiền nhận TRACK từ máy chủ nhà phát hành thẻ (410). Máy chủ ví tiền có thể tương tác với máy chủ nhà phát hành thẻ một cách trực tiếp hoặc thông qua máy chủ cung cấp và xác thực.

Máy chủ ví tiền mã hóa TRACK bằng cách sử dụng K_{MST}, tạo ra thẻ bài AC (ví dụ, $\{R_{MST}, R_S, TRACK, A^*\}_{KMST}$}), như được mô tả trên đây, và gửi thẻ bài AC đến thiết bị truyền thông di động (412). Thiết bị truyền thông di động chuyển tiếp thẻ bài AC đến MST (414). Như được mô tả trên đây, MST giải mã thẻ bài AC bằng cách sử dụng K_{MST} và xác nhận R_{MST} về tính thích hợp, và nếu mọi thứ xác nhận, thì MST ký thác TRACK và hoạt động thêm thẻ hoàn thành (416).

Theo một khía cạnh khác, thẻ động (hỗ trợ dCVV) có thể được cung cấp vào trong MST và sau đó được truyền đến POS. Theo khía cạnh này, khóa dCVV (K_{dCVV}) có thể được tạo ra và được gửi đến MST bởi máy chủ nhà phát hành thẻ hoặc được gửi đến máy chủ nhà phát hành thẻ từ MST để tạo thuận lợi cho việc cung cấp động. Phương pháp 500 để cung cấp động thẻ theo một phương án minh họa được mô tả theo Fig.5. Tương tự các phương pháp được mô tả trên đây, người dùng có thể quẹt thẻ để nhập vào dữ liệu thẻ (bao gồm TRACK) hoặc TRACK có thể được đẩy vào MST bởi máy chủ nhà phát hành thẻ.

Theo một khía cạnh, người dùng quẹt thẻ (ví dụ, thẻ thanh toán hoặc loại thẻ khác bao gồm dữ liệu thẻ từ) vào bộ quẹt trong MST hoặc thiết bị phụ có bộ quẹt riêng rẽ được ghép với MST (502). Việc này cung cấp dữ liệu thẻ (bao gồm TRACK) cho MST. MST hoặc MSR riêng rẽ mã hóa dữ liệu TRACK bằng cách sử dụng khóa ($K_{working}$) và gửi TRACK được mã hóa đến thiết bị truyền thông di động (504), nó gửi TRACK được mã hóa đến máy chủ ví tiền (506). MST còn có thể gửi thông tin bổ sung với TRACK, ví dụ, MST có thể gửi ID_{MST}, R_{MST}, tên người dùng, mật khẩu, KSN, và A* (nghĩa là thông tin phụ mà máy chủ ví tiền sử dụng để thực hiện việc xác nhận chữ ký cũng như cho máy chủ nhà phát hành thẻ để thực hiện việc xác thực người dùng/chủ thẻ) cùng với TRACK được mã hóa.

Theo cách thức tương tự như được mô tả trên đây, máy chủ ví tiền xác thực người dùng bằng cách sử dụng tên người dùng và mật khẩu, và còn kiểm tra để xem liệu ID_{MST} hiện thời có được kết hợp với tài khoản ví tiền của người dùng. Máy chủ ví tiền có thể xác nhận tính hợp lệ và tính đơn điệu của KSN. Máy chủ ví tiền còn có thể thực hiện kiểm tra để đảm bảo dữ liệu nhận được là hợp lệ. Ví dụ, máy chủ ví tiền có thể kiểm tra là TRACK chứa các chuỗi ISO-7812 hợp lệ. Đối với các thẻ tài chính, cả dữ liệu rãnh 1 và dữ liệu rãnh 2 sẽ có mặt. Đối với các thẻ phi tài chính (ví dụ, các thẻ quà tặng), ít nhất một trong các rãnh sẽ có mặt. Máy chủ ví tiền còn có thể thực hiện LRC (longitudinal redundancy check - kiểm tra tính dư dọc) để kiểm tra sự chính xác của dữ liệu được truyền. Đối với các thẻ tài chính, tên chủ thẻ từ dữ liệu rãnh 1 phải phù hợp với tên người dùng tài khoản ví tiền của người dùng trên hồ sơ, và ngày hết hạn của thẻ phải hợp lệ (nghĩa là thẻ chưa hết hạn).

Trong một số tình huống, máy chủ ví tiền có thể xác định liệu thẻ có đủ tiêu chuẩn cho dCVV nhờ kiểm tra để xem liệu PAN (Permanent Account Number - Số tài khoản thường xuyên) của thẻ là từ nhà phát hành tham dự dựa trên BIN (Bank Identification Number - Số nhận dạng ngân hàng, 6 chữ số đầu tiên của PAN). Nếu không, việc cung cấp tĩnh được mô tả trên đây có thể thực hiện. Giả thiết là thẻ có đủ tiêu chuẩn cho dCVV, máy chủ ví tiền gửi yêu cầu cung cấp đến máy chủ cung cấp và xác thực (508). Yêu cầu có thể bao gồm PAN và thông tin phụ cho nhà phát hành thẻ/máy chủ nhà phát hành thẻ để xác thực người dùng, như CVV-2, tên, ngày sinh, câu trả lời cho câu hỏi thử thách, và/hoặc thông tin khác.

Cần hiểu rõ rằng các bước được mô tả trên đây chỉ là một cách để nhận dạng người dùng và chủ thể thẻ về dCVV đối với nhà phát hành thẻ và (các) máy chủ cung cấp và xác thực. Các cách khác có thể được tiến hành. Ví dụ, người dùng mà không có thiết bị quẹt có thể kết nối với máy chủ nhà phát hành thẻ nhờ cung cấp các ủy nhiệm ngân hàng trực tuyến, và yêu cầu việc tải xuống của thẻ dCVV từ máy chủ nhà phát hành thẻ. Máy chủ nhà phát hành thẻ còn có thể báo với máy chủ ví tiền là nó sẵn sàng.

Máy chủ cung cấp và xác thực có thể nhận dạng là yêu cầu, từ bước 508, là từ máy chủ ví tiền, và máy chủ ví tiền đáng tin cậy. Theo một khía cạnh, máy chủ cung cấp và xác thực tin rằng máy chủ ví tiền đã xác thực MST thay mặt nó. Theo một khía cạnh khác, máy chủ cung cấp và xác thực có thể thực hiện việc xác nhận bổ sung với máy chủ nhà phát hành thẻ, bằng cách sử dụng A^* (510). Máy chủ nhà phát hành thẻ có thể tùy chọn trả về, ngoài kết quả xác nhận, một số thông tin phụ B^*, như bí danh PAN, đồ họa in nổi, v.v. (512).

Máy chủ cung cấp và xác thực tạo ra khóa ngẫu nhiên (K_{dCVV}) cho thẻ (514), và chèn vào trong cơ sở dữ liệu của nó bộ-3 gồm: {PAN, K_{dCVV}, T_{stamp}}, trong đó T_{stamp} là dấu thời gian của thời gian hiện thời trong UTC (universal time coordinated - giờ quốc tế phối hợp), hoặc so với chuẩn thời gian cố định. Dấu thời gian còn có thể chứa bộ đếm CC mà tăng lên với mỗi giao dịch MST. Sự kết hợp của dấu thời gian và bộ đếm được sử dụng để tạo ra thành phần mới cho các giao dịch động.

Máy chủ cung cấp và xác thực gửi K_{dCVV} đến máy chủ ví tiền, tùy chọn cùng

với thông tin phụ B^* (516). Máy chủ ví tiền gửi K_{dCVV} và SYNC (trong đó SYNC chứa thông tin dấu thời gian, và được sử dụng để đồng bộ hóa thời gian giữa MST và máy chủ ví tiền) đến thiết bị truyền thông di động (518), sau đó nó chuyển tiếp K_{dCVV} và SYNC đến MST (520). K_{dCVV} và SYNC có thể được ký hoặc được mã hóa để tạo ra tính an toàn. Máy chủ ví tiền còn có thể gửi một số thông tin bổ sung đến MST, qua thiết bị truyền thông di động, cùng với K_{dCVV}; ví dụ, máy chủ ví tiền còn có thể gửi TRACK.

SYNC có thể là gói được sử dụng bởi MST để điều chỉnh chuẩn thời gian trong của nó. Việc này cho phép MST cung cấp dấu thời gian chính xác. Khi được sử dụng, MST truyền dấu thời gian cộng bản mật mã mà được tạo ra bằng cách sử dụng K_{dCVV}, PAN, EXP, và dấu thời gian. Do dấu thời gian được đồng bộ hóa, nên máy chủ mà thực hiện việc cấp phép có thể kiểm tra tính mới của gói và xác nhận bản mật mã. Việc sử dụng dấu thời gian có tác dụng ngăn chặn các tấn công kiểu phát lại bởi vì việc tạo ra bản mật mã được đóng dấu thời gian, và độ trễ bất kỳ khi dùng bản mật mã có nguy cơ khiến nó bị từ chối bởi lôgic cấp phép trên máy chủ.

Trong trường hợp trong đó dữ liệu thẻ (bao gồm TRACK) được đẩy qua vô truyến vào MST thay vì được quẹt vào trong MST bởi người dùng, máy chủ cung cấp và xác thực nhận TRACK từ máy chủ nhà phát hành thẻ và gửi TRACK đến máy chủ ví tiền cùng với K_{dCVV}, và tùy chọn là B*. Phần còn lại của quy trình tương tự với quy trình được mô tả trên đây. Ví dụ, máy chủ ví tiền mã hóa TRACK và K_{dCVV} bằng cách sử dụng K_{MST}, tạo ra thẻ bài AC (ví dụ, $\{R_{MST}, R_S, TRACK, K_{dCVV}, B^*\}K_{MST}\}$), và gửi thẻ bài AC đến MST qua thiết bị truyền thông di động.

Ngoài ra, dữ liệu thẻ tĩnh, được mô tả trên đây, có thể được chuyển đổi thành dữ liệu thẻ động (dCVV) theo bước trên Fig.5. Ví dụ, thay vì quẹt thẻ vào trong MST ở bước 502, thẻ tĩnh có thể được kéo ra từ bộ nhớ hoặc bộ lưu trữ và được chuyển đổi thành thẻ động theo cùng cách thức như các bước 504-520. Cần hiểu rõ rằng các bước 510 và 512 có thể là tùy chọn, và máy chủ cung cấp và xác thực có thể chuyển đổi một cách đơn giản thẻ tĩnh thành thẻ động mà không cần xác thực người dùng với máy chủ nhà phát hành thẻ.

Theo một khía cạnh khác, dữ liệu thẻ, ví dụ, bao gồm TRACK, có thể được

cung cấp một cách an toàn từ máy chủ nhà phát hành thẻ (hoặc bộ xử lý thay mặt cho nhà phát hành thẻ) đến MST của chủ tài khoản, mà không để lộ nội dung dữ liệu của chủ tài khoản ra bên ngoài, ví dụ khi nhà phát hành thẻ hoặc bộ xử lý của nó muốn cung cấp cho ứng dụng ví tiền hoặc chính ứng dụng ngân hàng di động của chúng mà không cần đi qua máy chủ ví tiền. Phương pháp 600 để cung cấp thẻ dCVV theo một phương án minh họa được mô tả theo Fig.6.

Như được minh họa trên Fig.6, người dùng (nghĩa là, người dùng có tài khoản với nhà phát hành thẻ) xác thực với máy chủ nhà phát hành thẻ (602), ví dụ, nhờ nhận và gửi dữ liệu tài khoản người dùng (ví dụ, đăng nhập và mật khẩu ngân hàng trực tuyến của người dùng) từ thiết bị truyền thông di động đến máy chủ nhà phát hành thẻ. Máy chủ nhà phát hành thẻ xác nhận tính hợp lệ người dùng bằng cách sử dụng dữ liệu tài khoản người dùng (604). Sau đó, máy chủ nhà phát hành thẻ thông báo cho máy chủ cung cấp và xác thực về thông tin tài khoản của người dùng (606), ví dụ, bao gồm, nhưng không giới hạn vào PAN, tên chủ thẻ, cũng như "chuỗi cấp phép" để xác thực và nhận dạng người dùng và tài khoản, và phần tử nhận dạng được chỉ định cho nhà phát hành thẻ ("ID_I"). Máy chủ cung cấp và xác thực lưu trữ chuỗi cấp phép, ID_I, và thông tin tài khoản của người dùng (608). Thông tin tài khoản của người dùng có thể bao gồm khóa làm việc được tạo ra bởi máy chủ cung cấp và xác thực, và/hoặc tệp in nổi trong trường hợp cung cấp thẻ tĩnh.

Sau đó, máy chủ cung cấp và xác thực báo với máy chủ nhà phát hành thẻ là việc chuẩn bị cung cấp hoàn thành (610). Để đáp lại, máy chủ nhà phát hành thẻ báo với thiết bị truyền thông di động là việc chuẩn bị hoàn thành, ví dụ, nhờ gửi chuỗi cấp phép và ID_I đến thiết bị truyền thông di động (612). Thiết bị truyền thông di động sử dụng chuỗi cấp phép và ID_I để yêu cầu dữ liệu thẻ từ máy chủ cung cấp và xác thực nhờ gửi yêu cầu về dữ liệu (614). Dữ liệu sẽ chỉ để lộ đối với chủ tài khoản của nhà phát hành thẻ (nghĩa là, người dùng có tài khoản với nhà phát hành thẻ). Để đáp lại yêu cầu, máy chủ cung cấp và xác thực trả về dữ liệu thẻ và tùy chọn là phân loại dữ liệu được gọi là "DD" (616). DD có thể bao gồm phần băm của dữ liệu thẻ, tên của chủ tài khoản nếu đây là tệp in nổi của thẻ, và dấu thời gian của việc tạo ra DD này. Theo một khía cạnh, chữ ký của DD cũng có thể được trả về với dữ liệu. Chữ ký có thể được ký bởi nhà phát hành thẻ hoặc khóa làm việc riêng của bộ xử lý thẻ, và phải có

thể xác nhận được một cách công khai bằng cách sử dụng chứng nhận công cộng tương ứng.

Sau đó, thiết bị truyền thông di động thực hiện việc bắt tay với MST (618) và MST gửi ID_{MST} và R_{MST} đến thiết bị truyền thông di động (620). Thiết bị truyền thông di động gửi thông tin này cùng với thông tin bổ sung (ví dụ, ID_{MST}, R_{MST}, DD, và chữ ký của DD) đến máy chủ ví tiền và yêu cầu sự cho phép (622). Chú ý là, dữ liệu thực không được gửi đến máy chủ ví tiền trong trường hợp này. Máy chủ ví tiền thực hiện một hoặc nhiều sự xác nhận tính hợp lệ (624), ví dụ, để xác nhận chữ ký nhằm đảm bảo chữ ký tương ứng với DD và đến từ nhà phát hành thẻ mà máy chủ ví tiền nhận biết và được cấp phép, cũng như các kiểm tra phụ khác, như để đảm bảo tên trong DD khớp với tên tài khoản ví tiền; và dấu thời gian cho việc tạo ra DD là hiện thời. Nếu mọi thứ được xác nhận tính hợp lệ hoặc thanh toán hóa đơn, máy chủ ví tiền lấy K_{MST} tương ứng với ID_{MST}, và tạo ra bản mật mã cho phép, bao gồm $\{DD, R_{MST}\}K_{MST}$. Máy chủ ví tiền trả về sự cho phép này cho thiết bị truyền thông di động (626). Thiết bị truyền thông di động đưa dữ liệu thẻ, ID_I và sự cho phép vào trong MST (628). MST giải mã sự cho phép bằng cách sử dụng K_{MST} và thu được DD và R_{MST}, và xác nhận tính hợp lệ dữ liệu thẻ với DD (630). MST biết R_{MST} là mới nên không có sự tấn công phát lại. Việc giải mã thành công còn đề xuất rằng sự cho phép đã đến từ máy chủ ví tiền. Sau đó, MST độc lập tính toán phần băm của dữ liệu và so sánh nó với phần tương ứng của DD. Nếu hai phần này khớp, MST tiếp diễn và cài đặt dữ liệu. Như được mô tả trên đây, dữ liệu có thể bao gồm, ví dụ, TRACK. Ngoài ra, theo quy trình này, máy chủ ví tiền không có truy nhập đến dữ liệu thẻ trong toàn bộ quy trình cung cấp. Máy chủ ví tiền chỉ cung cấp sự cho phép đối với phân loại của dữ liệu.

Trong khi Fig.6 được mô tả liên quan đến việc thực hiện cung cấp thẻ mà không đi qua máy chủ ví tiền, máy chủ nhà phát hành thẻ có thể truyền thông với máy chủ ví tiền để thực hiện cung cấp thẻ và máy chủ cung cấp và xác thực có thể xử lý việc xác thực. Cần hiểu rõ rằng có nhiều cách trong đó các máy chủ khác nhau có thể truyền thông với nhau để thực hiện việc cung cấp và xác thực thẻ.

Theo một phương án khác, các người dùng có thể xác thực với nhà phát hành thẻ và khởi đầu việc tải xuống của các thẻ một cách trực tiếp từ các nhà phát hành thẻ.

Nếu thẻ là từ nhà phát hành tham dự mà có các khả năng xác thực các thẻ động, nhờ chính chúng hoặc nhờ mạng thanh toán của chúng, thì máy chủ ví tiền có thể tự động khởi đầu việc chuyển đổi của dữ liệu rãnh tĩnh thành thẻ động thông qua máy chủ cung cấp và xác thực. Phương pháp 700 để cung cấp thẻ dCVV theo một phương án minh họa được mô tả theo Fig.7. Người dùng (nghĩa là, người dùng có tài khoản với nhà phát hành thẻ) xác thực với máy chủ nhà phát hành thẻ.

Theo phương án này, thiết bị truyền thông di động gửi thông tin xác thực (ví dụ, ID_{MST}, R_{MST}, tên người dùng, mật khẩu, và A* (trong đó A* bao gồm thông tin, như, ủy nhiệm tài khoản nhà phát hành dựa trên các yêu cầu xác thực của nhà phát hành)) đến máy chủ ví tiền (702). Máy chủ ví tiền chuyển tiếp thông tin xác thực (ví dụ A*) đến máy chủ nhà phát hành thẻ để xác nhận (704). Máy chủ nhà phát hành thẻ thực hiện việc xác nhận tính hợp lệ và gửi lại cho máy chủ ví tiền TRACK cho thẻ và thông tin bất kỳ khác được yêu cầu trình diện (ví dụ, TRACK và C* (trong đó C* có thể bao gồm biểu tượng (logo), hình ảnh và/hoặc đồ họa khác) (706).

Máy chủ ví tiền kiểm tra và xác định liệu nhà phát hành thẻ có được đăng ký và/hoặc tham gia vào việc xác thực thẻ động (708). Nếu nhà phát hành thẻ không, thì quy trình tiếp diễn theo quá trình cung cấp thẻ tĩnh, như được mô tả trên đây. Nếu nhà phát hành thẻ có tham gia vào việc xác thực thẻ động, thì máy chủ ví tiền gửi yêu cầu cung cấp đến máy chủ cung cấp và xác thực (710). Yêu cầu có thể bao gồm PAN và thông tin phụ, như CVV-2, tên, ngày sinh, câu trả lời cho câu hỏi thử thách, và/hoặc thông tin khác.

Máy chủ cung cấp và xác thực tạo ra khóa ngẫu nhiên (K_{dCVV}) cho thẻ (712), và chèn vào trong cơ sở dữ liệu của nó bộ-3 gồm: {PAN, K_{dCVV}, T_{stamp}} (như được mô tả trên đây theo Fig.5). Máy chủ cung cấp và xác thực gửi K_{dCVV} đến máy chủ ví tiền, tùy chọn cùng với thông tin phụ B^* (714). Máy chủ ví tiền lấy K_{MST} của MST từ ID_{MST}, và gửi K_{dCVV} và SYNC (trong đó SYNC chứa thông tin dấu thời gian, và được sử dụng để đồng bộ hóa thời gian giữa MST và máy chủ ví tiền) đến thiết bị truyền thông di động (716), nó chuyển tiếp K_{dCVV} và SYNC đến MST (718). K_{dCVV} và SYNC có thể được mã hóa hoặc được ký bằng cách sử dụng K_{MST} để tạo ra tính an toàn. Máy chủ ví tiền còn có thể gửi một số thông tin bổ sung đến MST, qua thiết bị truyền thông di động,

cùng với K_{dCVV}; ví dụ, máy chủ ví tiền còn có thể gửi TRACK, R_{MST}, R_S, B^*, trong đó B^* là một số thông tin phụ từ nhà phát hành thẻ.

Một khi (các) thẻ hoặc (các) TRACK được tải vào trong MST, MST có thể được sử dụng để truyền dữ liệu thẻ ở POS để thực hiện giao dịch. Theo một khía cạnh, dữ liệu có thể được tạo ra theo cách động để tạo ra tính an toàn cho dữ liệu đang được truyền.

Theo khía cạnh này, ở mỗi lần truyền, MST cấu tạo, ví dụ, dữ liệu rãnh 2 được biến đổi (MT) chứa dCVV, nó được suy ra từ dữ liệu thẻ, T_{stamp} từ MST (dấu thời gian hiện thời từ MST) và K_{dCVV}. dCVV có thể bao gồm mã 3 chữ số mà được tính toán như hàm của K_{dCVV}, bao gồm PAN, ngày hết hạn của thẻ (EXP), mã dịch vụ (SVC), và T_{stamp}. Ví dụ, dCVV = fK_{dCVV} (PAN, EXP, SVC, T_{stamp}). Sau khi dCVV được tạo ra, trị số bộ đếm được lưu trữ trong MST trong khoảng đơn vị thời gian hiện thời (nghĩa là 10 phút, 1 giờ, v.v.), được tăng lên một.

Phương pháp 800 để thực hiện dCVV theo một phương án minh họa được mô tả theo Fig.8. Trình tự của các bước truyền và xác nhận bởi máy chủ nhà phát hành thẻ bao gồm MST gửi dữ liệu thẻ được biến đổi với dCVV đến thiết bị đầu cuối POS (802), nó chuyển tiếp dữ liệu thẻ được biến đổi đến máy chủ nhà thu nhận (804), sau đó nó chuyển tiếp dữ liệu thẻ được biến đổi đến máy chủ nhà phát hành thẻ (806). Tải truyền có thể bao gồm: SS (start sentinel - cờ hiệu bắt đầu), PAN, FS (field separator - phần tử tách trường), EXP, SVC, T_{stamp}, dCVV, MI, ES (end sentinel - cờ hiệu kết thúc), và LRC (error checksum character - ký tự kiểm tra tổng lỗi). MI có thể là cờ cho máy chủ nhà phát hành thẻ nhận ra và thực hiện việc cấp phép trong chế độ dCVV. Tuy nhiên, MI có thể không được sử dụng nếu EXP trong tương lai được sử dụng như phần tử chỉ thị, như được mô tả chi tiết hơn sau đây.

Khi nhận dữ liệu, máy chủ nhà phát hành thẻ có thể hiểu việc truyền là giao dịch dCVV dựa trên MI hoặc EXP trong tương lai. Cần hiểu rõ rằng PAN còn có thể được đăng ký bởi máy chủ cung cấp và xác thực để thực hiện việc khớp trong khi giao dịch sao cho PAN đã đăng ký có thể được kiểm tra đối với máy chủ cung cấp và xác thực để xác thực dCVV. Máy chủ nhà phát hành thẻ có thể yêu cầu máy chủ cung cấp và xác thực để xác nhận dCVV (808). Sau đó, máy chủ cung cấp và xác thực trả về sự

xác thực hoặc thất bại cấp phép (810). Nếu không tìm thấy PAN, máy chủ cung cấp và xác thực trả về lỗi không đăng ký PAN. Máy chủ cung cấp và xác thực so sánh T_{stamp} nhận được với thời gian hiện thời trên máy chủ. Thuật toán so sánh có thể được thực hiện như sau: nếu T_{stamp} nhận được là chậm hơn về thời gian so với T_{stamp} được lưu trữ, thì dấu thời gian là đúng; nếu T_{stamp} nhận được là sớm hơn về thời gian so với T_{stamp} được lưu trữ, thì dấu thời gian không đúng và trả về thất bại cấp phép; nếu T_{stamp} nhận được khớp với T_{stamp} được lưu trữ thì thất bại cấp phép được trả về khi trị số bộ đếm nhận được nhỏ hơn trị số bộ đếm được lưu trữ, nếu không thì dấu thời gian là đúng.

Trong khi xác nhận, máy chủ cung cấp và xác thực độc lập tính toán dCVV với K_{dCVV} được lưu trữ trên máy chủ cung cấp và xác thực và kiểm tra để xem liệu trị số được tính toán có giống hệt với dCVV nhận được. Nếu dCVV được tính toán khớp với dCVV nhận được và T_{stamp} là đúng, thì máy chủ cung cấp và xác thực cập nhật T_{stamp} được lưu trữ hiện thời bằng T_{stamp} mà nó nhận được. Sau đó, máy chủ cung cấp và xác thực trả về sự xác thực hoặc thất bại cấp phép (810). Nếu trị số được tính toán không giống hệt với dCVV nhận được, thì máy chủ cung cấp và xác thực trả về thất bại cấp phép. Máy chủ nhà phát hành thẻ còn có thể thực hiện một hoặc nhiều kiểm tra chu kỳ mà máy chủ nhà phát hành thẻ thường tiến hành khi cấp phép thẻ định kỳ (812) và trả về kết quả cấp phép cuối cùng cho máy chủ nhà thu nhận (814), nó chuyển tiếp tin nhắn đến POS (816). Nếu thất bại được trả về cho POS, thì giao dịch có thể bị hủy bỏ. Nếu sự cấp phép cuối cùng được trả về cho POS, thì giao dịch có thể tiếp diễn.

Theo một phương án khác, mạng thanh toán (ví dụ, VISA) hoặc máy chủ bộ xử lý bên thứ ba có thể xử lý dCVV và cấp phép cho giao dịch. Fig.9 minh họa phương pháp 900 này để thực hiện dCVV theo một phương án minh họa. Theo phương án này, dữ liệu rãnh được biến đổi chứa dCVV được gửi từ MST đến thiết bị đầu cuối POS (902), nó chuyển tiếp dữ liệu thẻ được biến đổi đến máy chủ nhà thu nhận (904), sau đó nó chuyển tiếp dữ liệu thẻ được biến đổi đến mạng thanh toán, như máy chủ được vận hành bởi VISA (906), nếu có thể áp dụng được. Trong một số trường hợp máy chủ nhà thu nhận gửi giao dịch trực tiếp đến nhà phát hành thẻ hoặc máy chủ bộ xử lý vòng qua mạng thanh toán (được biết đến như giao dịch “on us” (chủ thẻ sở hữu)), đối với các trường hợp này máy chủ xác thực cung cấp thay vào đó sẽ được làm chủ ở máy chủ bộ xử lý hoặc nhà phát hành thẻ. Như được mô tả trên đây, dCVV có thể bao

gồm mã 3 chữ số mà được tính toán như hàm của K_{dCVV}, bao gồm PAN, ngày hết hạn của thẻ (EXP), mã dịch vụ (SVC), và T_{stamp}. Ví dụ, dCVV = fK_{dCVV} (PAN, EXP, SVC, T_{stamp}). Sau khi dCVV được tạo ra, trị số bộ đếm được lưu trữ trong MST trong khoảng đơn vị thời gian hiện thời (nghĩa là 10 phút, 1 giờ, v.v.), được tăng lên một.

Sau đó, mạng thanh toán kiểm tra liệu dữ liệu có tương ứng với thẻ động (908), ví dụ, nhờ kiểm tra đối với MI hoặc trị số EXP được biến đổi. Như được mô tả trong bản mô tả này, việc thay thế EXP hiện thời bằng ngày cố định trong tương lai (ví dụ, tháng 12 năm 2048) có thể có chức năng như MI. Khi thấy EXP cụ thể này, mạng thanh toán có thể tiếp diễn với việc xác nhận tính hợp lệ dCVV. Khi EXP được sử dụng làm MI, không cần cấp phát chữ số bổ sung cho MI và EXP đúng, ban đầu trên thẻ vật lý được phát hành có thể được bảo vệ bởi vì nó không được truyền.

Khi mạng thanh toán nhận biết dữ liệu là động, mạng thanh toán yêu cầu máy chủ cung cấp và xác thực xác nhận dCVV (910), ví dụ, bằng cách sử dụng PAN. Nếu không tìm thấy PAN trong máy chủ cung cấp và xác thực, thì trả về thất bại cấp phép cho POS. Khi PAN nằm trong máy chủ cung cấp và xác thực, máy chủ cung cấp và xác thực xác nhận thẻ (912). Để thực hiện việc xác nhận này, máy chủ cung cấp và xác thực có thể kiểm tra để xem liệu T_{stamp} nhận được từ giao dịch có gần đây dựa trên thời gian máy chủ của chính nó, nghĩa là, nó không phải là sự phát lại của giao dịch cũ. Ví dụ, máy chủ cung cấp và xác thực so sánh T_{stamp} mà nó nhận được từ giao dịch với T_{stamp} mà nó thấy lần cuối với cùng thẻ. Nếu T_{stamp} nhận được lớn hơn (chậm hơn về thời gian) so với T_{stamp} được lưu trữ, thì dấu thời gian là đúng; nếu T_{stamp} nhận được nhỏ hơn (sớm hơn về thời gian) so với T_{stamp} được lưu trữ, dấu thời gian là không đúng, thất bại cấp phép được trả về; và nếu T_{stamp} nhận được bằng với T_{stamp} được lưu trữ, thì thất bại cấp phép được trả về khi $CC_{Received}$ nhỏ hơn CC_{Stored}, nếu không thì dấu thời gian là đúng. Khi dấu thời gian là đúng, máy chủ cung cấp và xác thực cập nhật T_{stamp} được lưu trữ hiện thời bằng T_{stamp} mà nó nhận được, và trong trường hợp cuối cùng, CC_{Stored} được tăng lên một.

Máy chủ cung cấp và xác thực độc lập tính toán dCVV bằng cách sử dụng K_{dCVV} được lưu trữ, và kiểm tra để xem liệu trị số được tính toán có khớp với với trị số nhận được. Nếu không, thất bại cấp phép được trả về. Nếu bản mật mã dCVV vừa hợp

lệ và mới được tạo ra, thì máy chủ cung cấp và xác thực thực hiện quy trình khôi phục. Quy trình này loại bỏ các thành phần động của dữ liệu rãnh, như, SVC, T_{Stamp} và dCVV, và chèn nội dung rãnh ban đầu ở các vị trí tương ứng bên trong rãnh. Quy trình này khôi phục hoàn toàn dữ liệu rãnh ban đầu (TRACK) như được phát hành bởi nhà phát hành thẻ. Sau đó, máy chủ cung cấp và xác thực gửi TRACK được khôi phục đến mạng thanh toán (914).

Mạng thanh toán còn có thể chuyển tiếp TRACK đến máy chủ nhà phát hành thẻ để xác nhận (916), nó xác nhận TRACK và gửi sự xác nhận hoặc thất bại cấp phép trở lại mạng thanh toán (918). Sau đó, mạng thanh toán gửi sự cấp phép của thanh toán hoặc thất bại cấp phép đến máy chủ nhà thu nhận (920), nó chuyển tiếp sự cấp phép của thanh toán hoặc thất bại cấp phép đến POS (922).

Khi nhà phát hành thẻ dùng bộ xử lý bên thứ ba, mạng thanh toán có thể truyền thông với bộ xử lý bên thứ ba để xác nhận TRACK. Ngoài ra, theo một số phương án, máy chủ nhà phát hành thẻ hoặc bộ xử lý bên thứ ba có thể truyền thông trực tiếp với máy chủ cung cấp và xác thực để xác nhận dCVV và xử lý giao dịch.

Theo một khía cạnh khác, người dùng có thể dùng dCVV và/hoặc ngày EXP được biến đổi trong giao dịch CNP, ví dụ, khi điền mẫu thanh toán trực tuyến. Theo khía cạnh này, ứng dụng ví tiền trên thiết bị truyền thông di động, có thể tính toán hoặc làm cho MST tính toán dCVV và/hoặc EXP được biến đổi và hiển thị một hoặc nhiều trong số đó cho người dùng. Sau đó, người dùng có thể nhập dCVV và/hoặc EXP được biến đổi vào trong mẫu giao dịch trực tuyến và gửi dữ liệu rãnh được biến đổi, bao gồm dCVV và/hoặc EXP được biến đổi, đến máy chủ thương mại điện tử (924), sau đó máy chủ thương mại điện tử có thể chuyển tiếp dữ liệu rãnh được biến đổi đến máy chủ nhà thu nhận (926). Sau đó, việc cấp phép có thể tiếp diễn như được mô tả trên đây theo các bước 906-920.

Một cách khác để chỉ thị dữ liệu thẻ là truyền rãnh dCVV là sử dụng trị số EXP được biến đổi. Theo một ví dụ, thay thế EXP hiện thời của thẻ bằng trị số cố định, ví dụ, ‘4812’ (tháng 12 năm 2048). Khi xem EXP cụ thể này, máy chủ nhà phát hành thẻ có thể tiếp diễn theo chế độ dCVV. Theo khía cạnh này, không cần cấp phát chữ số bổ sung cho MI và EXP đúng, ban đầu trên thẻ vật lý được phát hành có thể được bảo vệ

bởi vì nó không được truyền, theo đó bảo vệ PAN để được sử dụng với EXP và tên cho các giao dịch CNP hoặc trực tuyến nhất định. Nếu MI không được sử dụng, thì dCVV chiếm 6 chữ số.

Theo một khía cạnh, sáng chế còn đề cập đến các thiết bị, hệ thống, và phương pháp mà che và tái sử dụng EXP trong các giao dịch hoặc các hệ thống thẻ. Việc thay thế EXP bởi số tương đương với ngày cách xa trong tương lai sẽ che EXP trong giao dịch trong khi cung cấp cho nhà phát hành thẻ cờ thuận tiện để nhận ra thẻ là động. Ví dụ, nếu người không được cấp phép cố sử dụng EXP này để mua trực tuyến, thì nó sẽ bị từ chối bởi máy chủ nhà phát hành thẻ, trừ khi nó được kèm theo bởi CVV-2 mà cũng được được tạo ra theo cách động bởi MST, hoặc bởi phương tiện từ xa từ TSP (Token Service Provider - Nhà cung cấp dịch vụ thẻ bài) (ví dụ, máy chủ cung cấp và xác thực) hoặc máy chủ nhà phát hành thẻ, được hiển thị cho chủ thẻ trên thiết bị di động của họ tại thời điểm yêu cầu giao dịch và sẽ thay đổi ở mỗi yêu cầu mới bởi người dùng, và hết hạn sau thời gian ngắn. Sau đó, CVV-2 động này có thể được xác thực trong máy chủ xác thực cung cấp được chạy bởi máy chủ nhà phát hành thẻ hoặc TSP. Nhờ đó, theo cách hiệu quả, làm cho dữ liệu thẻ bị lấy cắp đối với thẻ động hoặc thẻ dCVV không sử dụng được không chỉ cho các giao dịch có mặt thẻ, mà còn cho các giao dịch CNP, bởi vì số thay thế cho EXP có thể được sử dụng làm phần tử chỉ thị đặc biệt cho độ an toàn động hoặc các thẻ dCVV.

Điều này quan trọng vì nó có thể giúp các nhà phát hành thẻ/các máy chủ nhà phát hành thẻ tạo ra phương pháp giao dịch an toàn hơn cho các chủ thẻ của họ không chỉ cho các thanh toán thẻ vật lý sử dụng cơ sở hạ tầng POS hiện có, mà còn cho các thanh toán thẻ trực tuyến hoặc CNP cũng sử dụng cơ sở hạ tầng thanh toán CNP hiện có mà không cần thay đổi các hệ thống thanh toán hóa đơn trực tuyến của các thương nhân. Đây là giải pháp nhanh chóng để cải thiện độ an toàn thay toán trực tuyến mà không cần chờ đợi sự thay đổi lớn của thương nhân.

Đã cho rằng dữ liệu thẻ có thể được tạo ra cho mỗi giao dịch mới và được phân phối thông qua thiết bị truyền thông di động thay vì các thẻ làm bằng chất dẻo, EXP cho các loại giao dịch này có thể không còn cần thiết, các nhà phát hành thẻ/các máy chủ nhà phát hành thẻ không phải thay thế các thẻ dùng một lần di động này tại hiện

trường. EXP được in ở phía trước của thẻ vật lý làm bằng chất dẻo mà các nhà phát hành gửi trong thư, hoặc các thẻ tĩnh được thể hiện trong ví điện tử có thể duy trì cách truyền thống với EXP ban đầu nhằm mục đích mua hàng trực tuyến với các thẻ làm bằng chất dẻo của người tiêu dùng. Nhà phát hành thẻ/máy chủ nhà phát hành thẻ và mạng có khả năng phân biệt đây là thẻ tĩnh chuẩn và xử lý nó theo đó.

Trong các giao dịch POS, các hệ thống bán lẻ đọc EXP và sẽ từ chối thẻ nếu dữ liệu EXP (MMYY - tháng năm) trên dải từ hoặc trong tin nhắn EMV là sớm hơn so với ngày hiện tại. Tuy nhiên, các EXP cách xa trong tương lai được chấp nhận bởi các hệ thống nhà thu nhận và POS là hợp lệ.

EXP trên dải từ, trong tin nhắn thẻ thông minh (như thẻ EMV) hoặc truyền dải từ (MST) có thể được thay thế bởi số cụ thể mà biểu diễn ngày cách xa trong tương lai. Số, theo định dạng YYMM (năm tháng), được dịch nhờ POS đọc nó là ngày trong tương lai, nhưng đối với nhà phát hành thẻ/máy chủ nhà phát hành thẻ, trên thực tế nó là phần tử chỉ thị rằng dữ liệu thẻ chứa phần tử xác thực có thể thay đổi, như dCVV. Ví dụ, EXP có thể được thay thế bởi số 4912. Hệ thống bán lẻ sẽ dịch số này là ngày trong tương lai (tháng 12 năm 2049) trong khi nhà phát hành thẻ/máy chủ nhà phát hành thẻ sẽ nhận biết 4912 là phần tử chỉ thị cho thẻ dCVV và chuyển đổi hoặc xử lý nó theo đó.

Fig.10 minh họa cách thức dữ liệu rãnh 2 được biến đổi theo một khía cạnh của sáng chế. Nó chỉ minh họa khái niệm của định dạng rãnh dCVV. Định dạng dCVV rãnh 1 là tương tự, nhưng có trường thêm vào, như, tên chủ thẻ và các phần tử tách trường của nó.

Như được minh họa trên Fig.10, Phần tử chỉ thị chế độ động (Dynamic Mode Indicator - DMI hoặc chỉ là MI) 1000 có thể được sử dụng để thay thế EXP thẻ 1002. DMI 1000 là số dài 4 chữ số mà thay thế EXP thẻ 1002 và được thiết lập cách xa trong tương lai. Các nhà thu thập và hệ thống POS đọc DMI 1000 là dữ liệu hết hạn, nhưng các nhà phát hành thẻ/các máy chủ nhà phát hành thẻ nhận biết số là phần tử chỉ thị của chế độ động hoặc thẻ bài. Ngoài ra, PVKI (Pin Verification Key Indicator - Phần tử chỉ thị khóa xác nhận Pin)/dữ liệu tùy ý 1004 có thể được biến đổi hoặc được thay thế bởi dữ liệu động hoặc thẻ bài 1006.

Dữ liệu động 1006 thường chứa hai phần: dấu thời gian (hoặc biến thể dựa trên bộ đếm, số tăng đơn điệu 7 chữ số), và dCVV là chuỗi số có 3 chữ số đến 6 chữ số được tính toán bằng cách sử dụng hàm băm được khóa một chiều qua SS, PAN, DMI và SVC. MST có thể được cấu hình để điều chỉnh chuẩn thời gian trong của nó, ví dụ, thành 15:00 ngày 1 tháng 1 năm 2014. Việc này cho phép MST cung cấp dấu thời gian chính xác. MST truyền dấu thời gian cộng bản mật mã mà được tạo ra bằng cách sử dụng K_{dCVV}, PAN, EXP, và dấu thời gian (dấu thời gian + bản mật mã là 1006). Do dấu thời gian được đồng bộ hóa, như được mô tả trên đây, nên máy chủ mà thực hiện việc cấp phép có thể kiểm tra tính mới của gói và xác nhận bản mật mã. Việc sử dụng dấu thời gian có tác dụng ngăn chặn các tấn công kiểu phát lại bởi vì việc tạo ra bản mật mã được đóng dấu thời gian, và độ trễ bất kỳ khi dùng bản mật mã có nguy cơ khiến nó bị từ chối bởi lôgic cấp phép trên máy chủ.

Theo đó, dải từ hoặc dữ liệu thẻ thông minh bị lấy cắp chứa PAN và EXP được biến đổi (DMI) sẽ không hữu dụng đối với gian lận không có mặt thẻ bởi vì EXP thu được từ dữ liệu thẻ bị lấy cắp sẽ không khớp với EXP trên hồ sơ cho tài khoản và theo đó sẽ bị từ chối bởi nhà phát hành thẻ/máy chủ nhà phát hành thẻ.

Fig.11 minh họa sơ đồ tiến trình dạng khối của phương pháp 1100 của dCVV cho các giao dịch thương mại điện tử trực tuyến. Như được minh họa trên Fig.11, người dùng xác thực với máy chủ nhà phát hành thẻ và thẻ được cung cấp vào trong MST mà hỗ trợ CVV động, được minh họa bởi khối 1102, như được mô tả trên đây. Máy chủ nhà phát hành thẻ và/hoặc mạng thanh toán ghi lại, trong máy chủ cung cấp và xác thực, là thẻ được cung cấp hỗ trợ chế độ dCVV chỉ cho các giao dịch thương mại điện tử trực tuyến hoặc cho cả giao dịch thương mại điện tử và quẹt vật lý ở POS, được minh họa bởi khối 1104. Như được mô tả trên đây, PAN (hoặc phần băm của PAN) có thể được sử dụng làm phần tử nhận dạng trong máy chủ cung cấp và xác thực, K_{dCVV} còn có thể được phát hành và được phân phối một cách an toàn cho MST.

Sau đó, người dùng có thể sử dụng thẻ lúc thanh toán hóa đơn ở trang web thương mại điện tử trực truyến. Ví dụ, người dùng có thể làm cho thiết bị truyền thông di động hiển thị PAN và EXP 16 chữ số cho thẻ được cung cấp thông qua ứng dụng ví tiền, được minh họa bởi khối 1106. Sau đó, người dùng có thể nhập PAN và EXP vào

trong trang web thương mại điện tử trực tuyến lúc thanh toán hóa đơn, được minh họa bởi khối 1108. Ứng dụng ví tiền làm việc với MST tính toán và hiển thị CVV-2 được tạo ra theo cách động cho người dùng để nhập vào trong trang web thương mại điện tử trực tuyến, được minh họa bởi khối 1110.

EXP có thể là EXP thực của thẻ hoặc EXP trong tương lai được biến đổi để sử dụng làm phần tử chỉ thị chế độ. Khi EXP không được biến đổi, máy chủ cung cấp và xác thực cấp phép giao dịch dựa trên dCVV bởi vì nó biết, dựa trên PAN, là thẻ được đăng ký dưới dCVV cho các giao dịch thương mại điện tử. Khi EXP được biến đổi, điều này tạo ra hiệu ứng làm nhòe để giấu EXP đúng; và sự bảo hiểm bổ sung là thẻ sẽ được cấp phép dưới dCVV.

CVV-2 có thể được tính toán bởi ứng dụng ví tiền và MST dựa trên PAN, EXP thực, SVC và dấu thời gian hiện thời. Do dấu thời gian được đồng bộ hóa ngầm và toàn cầu, như được mô tả trên đây, nên máy chủ cấp phép (ví dụ, máy chủ nhà phát hành thẻ hoặc máy chủ cung cấp và xác thực) không cần được báo về dấu thời gian mà CVV-2 đã dựa vào. CVV-2 ở đây có thể là hàm tất định của bản mật mã được mô tả trên đây và được tạo ra theo cách về cơ bản là tương tự. Bản mật mã còn có thể được số hóa bằng cách sử dụng hàm số hóa. Ví dụ, nhờ lấy ba ký tự đầu tiên từ bản mật mã và thực hiện phép toán mođun trên mỗi ký tự, ví dụ, với 10, để thu được CVV-2 3 chữ số.

Người dùng nhập CVV-2 được tạo ra theo cách động vào trong trang web thương mại điện tử trực tuyến, được minh họa bởi khối 1112. Máy chủ cấp phép (ví dụ, máy chủ nhà phát hành thẻ, mạng thanh toán, hoặc máy chủ cung cấp và xác thực) nhận PAN, EXP, Tên, và CVV-2 và kiểm tra dấu thời gian hiện thời của nó, và độc lập tính toán CVV-2 bằng cách sử dụng cùng thuật toán, được minh họa bởi khối 1114. CVV-2 đã tính toán được so sánh với CVV-2 được nhập vào bởi người dùng, được minh họa bởi khối 1116, để cấp phép giao dịch nếu chúng khớp, được minh họa bởi khối 1118, hoặc từ chối giao dịch nếu chúng không khớp, được minh họa bởi khối 1120. Máy chủ cấp phép (ví dụ, máy chủ nhà phát hành thẻ, mạng thanh toán, hoặc máy chủ cung cấp và xác thực) còn có thể cho phép dung sai dấu thời gian +/- X trong đó X có thể cấu hình được.

Trong tình huống, trang web thương mại điện tử trực tuyến hoặc thương nhân lưu trữ EXP và không lưu trữ CVV2 cho các giao dịch lặp lại, nhà phát hành thẻ có thể cho phép giao dịch đi qua mà không có CVV2. Ví dụ, có thể không yêu cầu CVV2 cho thanh toán liên tục và khi có chỉ thị là thương nhân đang sử dụng dữ liệu thẻ cho các mục đích thanh toán liên tục thì nhà phát hành thẻ có thể cho phép giao dịch tiếp diễn. Trong trường hợp trong đó EXP là động, khi EXP được tái sử dụng trong giao dịch thông thường thì giao dịch có thể thất bại. Trong tình huống bất kỳ, khi sử dụng các thanh toán liên tục, nhà phát hành thẻ có thể chọn để cho phép giao dịch tiếp tục bởi vì giao dịch hợp lệ trước đó đã hoàn thành một cách thành công, nếu không thì nhà phát hành thẻ có thể từ chối giao dịch. Tương tự đối với các sự hoàn trả, các nhà phát hành thẻ có thể tin vào PAN để phát hành sự hoàn trả liên quan đến giao dịch cụ thể trong hệ thống của chính họ.

Nói chung, MST 102 có thể được sử dụng để tương tác với POS (point of sale - điểm bán) thương nhân nhờ truyền dữ liệu thẻ từ bộ truyền từ trường đến MSR (magnetic stripe reader - bộ đọc dải từ) của POS thương nhân và được sử dụng trong các giao dịch thương mại điện tử như được mô tả trên đây. Như được minh họa trên Fig.12, MST 102 có thể bao gồm bộ vi xử lý 1202, bộ chỉ thị LED (light-emitting diode - điốt phát sáng) 1204, nguồn năng lượng 1206, tùy chọn là MSR (magnetic stripe reader - bộ đọc dải từ) 1208, thành phần lưu trữ bộ nhớ hoặc phần tử an toàn 1210, giao diện đầu vào/đầu ra 1212 (ví dụ, cổng auđio 3.5mm hoặc cổng auđio chuẩn khác, giao diện cổng/đầu cắm USB hoặc giao diện truyền thông khác, bao gồm nhưng không giới hạn vào giao diện Apple 30 chân cắm hoặc 9 chân cắm, giao diện Bluetooth, và các giao diện nối tiếp khác), và bộ truyền từ trường 1214 bao gồm bộ dẫn động và cuộn cảm để truyền các xung từ cần được nhận bởi thiết bị POS bất kỳ với MSR, như POS 120.

Bộ vi xử lý 1202 quản lý tính an toàn và truyền thông với thiết bị truyền thông di động 104. Bộ vi xử lý 1202 còn có thể truyền và nhận dữ liệu thẻ được mã hóa đến và từ phần tử an toàn 1210. Bộ truyền từ trường 1214 truyền dữ liệu dải từ của chủ thẻ đến thiết bị POS 120 nhờ truyền các xung từ đến MSR của thiết bị POS 120. MST 102 còn có thể được sử dụng để đọc các thẻ dải từ khác bằng cách sử dụng MSR 1208 tùy chọn. MSR 1208 có thể được sử dụng để tải dữ liệu thẻ thanh toán lên trên phần tử an

toàn 1210 và để thu thập dữ liệu rãnh thẻ.

Thiết bị truyền thông di động 104 bao gồm ứng dụng ví tiền, và còn có thể bao gồm màn hình với vùng phím hoặc màn hình bảng chạm và CPU (central processing unit - bộ phận xử lý trung tâm). Ứng dụng ví khởi tạo và mở khóa MST 102, tương tác với MST 102 và chấp nhận dữ liệu thanh toán thẻ từ MST 102. Thiết bị truyền thông di động 104 còn có thể tương tác với MST 102 để hiển thị CVV-2 cho người dùng để nhập vào trong giao dịch thương mại điện tử trực tuyến sử dụng dCVV.

Dữ liệu thẻ có thể được mã hóa, và dữ liệu được mã hóa có thể được truyền đến thiết bị truyền thông di động 104. Ứng dụng ví có thể truyền dữ liệu đến máy chủ. Dữ liệu này có thể được giải mã ở máy chủ và dữ liệu PAN (Primary account number - dữ liệu số tài khoản chính), số thẻ, sự hết hạn và tên chủ thẻ được lấy ra khỏi dữ liệu rãnh. Ứng dụng ví tiền hoặc máy chủ còn có thể thực hiện xác định xem liệu thẻ từ là thẻ thanh toán hay thẻ không thanh toán. Nếu thẻ từ là thẻ không thanh toán thì MST 102 có thể tự động lưu trữ dữ liệu thẻ trong bộ nhớ để truyền không thanh toán. Nếu thẻ từ là thẻ thanh toán, ví dụ, có định dạng cụ thể mà có thể nhận biết được đối với hệ thống, thì thẻ này có thể được phát hiện là thẻ thanh toán và hệ thống xác định nếu tên trên thẻ thanh toán khớp với tên của tài khoản người dùng. Nếu tên không khớp, tin nhắn lỗi có thể xuất hiện. Nếu tên trên thẻ thanh toán khớp với với tên của tài khoản người dùng, thì hệ thống có thể xác định nếu số PAN khớp với thẻ hiện có mà đã được lưu trữ trên máy chủ, để tạo ra tài khoản mới hoặc để lại tài khoản hiện có. Nếu thẻ mới được tạo ra, thì hệ thống có thể lưu trữ dữ liệu thẻ trong phần thanh toán của bộ nhớ an toàn được mã hóa của MST.

Như được mô tả trên đây, MST 102 có khả năng tải loại thẻ dải từ bất kỳ vào trong phương tiện nhớ, không chỉ các thẻ thanh toán. Các thẻ không thanh toán có thể được lưu trữ riêng rẽ với độ an toàn nhỏ hơn để cho thuận tiện. Ví dụ, một số ứng dụng không thanh toán có thể bao gồm các thẻ để mở cửa, thẻ khách hàng trung thành, v.v.. Việc nạp dữ liệu thanh toán so với dữ liệu không thanh toán có thể được tách riêng thành hai trường hoặc vùng lưu trữ riêng rẽ. Theo một ví dụ, các thẻ thanh toán có thể không được tải vào trong phần lưu trữ không thanh toán. Ví dụ, dữ liệu thanh toán có thể có định dạng cụ thể mà có thể được phát hiện và có thể không được cho

phép được tải vào trong vùng lưu trữ không thanh toán. Các thẻ thanh toán còn có thể yêu cầu xác thực với ứng dụng trước khi được truyền. Mặt khác, dữ liệu không thanh toán mặc định có thể được truyền mà không cần xác thực.

Các thiết bị, hệ thống, và phương pháp được bộc lộ trong bản mô tả này cung cấp dữ liệu thẻ để được thu thập và lưu trữ trực tiếp trong phương tiện nhớ an toàn của MST bởi người dùng mà không cần biến đổi, và để được sử dụng sau đó bởi thiết bị POS hoặc thiết bị MSR khác. Kết nối hoặc đăng ký duy nhất của MST đối với tài khoản người dùng sao cho MST có thể chỉ được sử dụng với tài khoản đó để sử dụng trong truyền và lưu trữ dữ liệu thẻ tạo ra tính an toàn.

MST có khả năng kết nối với các thiết bị truyền thông di động qua các giao diện khác nhau ngoài các kết nối đầu cắm audio và USB (như Bluetooth, và các giao diện truyền thông không dây khác). Các thiết bị, hệ thống, và phương pháp cho phép tải dữ liệu thẻ được mã hóa vào trong phương tiện nhớ của MST mà sau đó có thể được giải mã và được truyền đến POS, hoặc có thể được truyền được mã hóa đến thiết bị truyền thông di động và sau đó được định tuyến đến máy chủ thanh toán để giải mã và xử lý để tải tài khoản người sử dụng lên máy chủ hoặc xử lý giao dịch POS. Các thiết bị, hệ thống, và phương pháp tạo ra khả năng sử dụng dữ liệu thẻ được lưu trữ hoặc dữ liệu thẻ được quẹt cho các môi trường thanh toán hóa đơn ảo cho giao dịch an toàn hơn và chi phí thấp hơn cho các thương nhân. Các thiết bị, hệ thống, và phương pháp tạo ra việc truyền và tải từ xa của dữ liệu thẻ từ nhà phát hành thẻ đến nhà cung cấp máy chủ ví tiền, đến ứng dụng ví tiền trên thiết bị truyền thông di động, và đến SE hoặc phương tiện nhớ của MST để sử dụng sau. Các thiết bị, hệ thống, và phương pháp còn tạo ra khả năng tải thông tin tài khoản khách hàng trung thành cùng với dữ liệu thẻ thanh toán vào trong một hoặc nhiều trường tùy ý của dữ liệu thẻ để được đọc bởi nhà phát hành trong hoặc sau khi giao dịch, khả năng này có thể dẫn tới các đề nghị và các chương trình khách hàng trung thành được kết hợp với giao dịch thanh toán.

Nói chung, các thiết bị, hệ thống, và phương pháp được bộc lộ trong bản mô tả này có thể bao gồm, và có thể được thực hiện trong, một số thiết bị và hệ thống máy tính khác nhau, bao gồm, ví dụ, các hệ thống tính toán đa năng, hệ thống POS, hệ

thống tính toán máy chủ-máy khách, hệ thống tính toán máy tính lớn, cơ sở hạ tầng điện toán đám mây, hệ thống tính toán điện thoại, máy tính xách tay, máy tính để bàn, điện thoại thông minh, điện thoại ô, PDA (personal digital assistants - thiết bị trợ giúp cá nhân dạng số), máy tính bảng, và các thiết bị di động khác. Các thiết bị và hệ thống tính toán có thể có một hoặc nhiều cơ sở dữ liệu và các thiết bị lưu trữ, máy chủ, và các thành phần bổ sung khác, ví dụ, các bộ xử lý, môđem, thiết bị đầu cuối và màn hình, thiết bị đầu vào/đầu ra, phương tiện đọc được bởi máy tính, thuật toán, môđun, và các thành phần liên quan đến máy tính khác. Các thiết bị và các hệ thống máy tính và/hoặc các cơ sở hạ tầng tính toán được tạo cấu hình, được lập trình, và được làm thích ứng để thực hiện các chức năng và các quy trình của các hệ thống và các phương pháp như được bộc lộ trong bản mô tả này.

Truyền thông giữa các thành phần trong các thiết bị, hệ thống, và phương pháp được bộc lộ trong bản mô tả này có thể là truyền thông điện tử một chiều hoặc hai chiều thông qua cấu hình hoặc mạng có dây hoặc không dây. Ví dụ, một thành phần có thể được nối dây hoặc được nối mạng không dây một cách trực tiếp hoặc gián tiếp, thông qua bên thứ ba trung gian, qua Internet, hoặc theo cách khác là với một thành phần khác để cho phép truyền thông giữa các thành phần. Các ví dụ về truyền thông không dây bao gồm, nhưng không giới hạn vào, RF (radio frequency - tần số rađio), hồng ngoại, Bluetooth, WLAN (wireless local area network - mạng cục bộ không dây) (như WiFi), hoặc rađio mạng không dây, như rađio có khả năng truyền thông với mạng truyền thông không dây như mạng LTE (Long Term Evolution - phát triển dài hạn), mạng WiMAX, mạng 3G, mạng 4G, và các mạng truyền thông khác thuộc loại này.

Các phương pháp được bộc lộ trong bản mô tả này có thể được thực hiện dưới các dạng khác nhau của phần mềm, phần sụn, và/hoặc phần cứng. Các phương pháp được bộc lộ trong bản mô tả này có thể được thực hiện trên một thiết bị hoặc có thể được thực hiện trên nhiều thiết bị. Ví dụ, các môđun chương trình bao gồm một hoặc nhiều thành phần có thể được đặt trong các thiết bị khác nhau và mỗi trong số chúng có thể thực hiện một hoặc nhiều khía cạnh của sáng chế.

Mặc dù, các thiết bị, hệ thống, và phương pháp đã được mô tả và được minh

họa liên quan đến các phương án nhất định, nhưng nhiều thay đổi và biến đổi là hiển nhiên đối với những người có hiểu biết trung bình trong lĩnh vực và có thể được thực hiện mà không lệch khỏi phạm vi bảo hộ của sáng chế. Theo đó, sáng chế không bị giới hạn vào các chi tiết chính xác của hệ phương pháp hoặc kết cấu được bộc lộ trên đây, do các thay đổi và biến đổi như vậy được bao hàm trong phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Thiết bị truyền dữ liệu dải từ của thẻ thanh toán bao gồm:

bộ truyền từ tính bao gồm bộ dẫn động và cuộn cảm để truyền các xung từ cần được nhận ra theo cách không tiếp xúc bởi thiết bị đầu cuối ở điểm bán; và

bộ xử lý chạy ứng dụng ví tiền được cấu hình để:

nhận thẻ bài và khóa được kết hợp với thẻ thanh toán từ một hoặc nhiều máy chủ,

tạo ra dữ liệu bản mật mã dựa trên khóa và thông tin đếm được kết hợp với việc truyền dải từ,

tạo ra tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, bằng cách sử dụng dữ liệu bản mật mã và thẻ bài, và

truyền, qua bộ truyền từ tính, các xung từ tương ứng với tin nhắn được tạo ra đến thiết bị đầu cuối ở điểm bán.

2. Thiết bị theo điểm 1, trong đó tin nhắn thanh toán được tạo ra nhờ bao gồm dữ liệu bản mật mã trong một trong các trường của dữ liệu rãnh 2.

3. Thiết bị theo điểm 1, trong đó tin nhắn thanh toán bao gồm dữ liệu rãnh 2 có nhiều trường được sắp xếp theo định dạng dữ liệu rãnh 2, và dữ liệu rãnh 2 được biến đổi nhờ chèn dữ liệu bản mật mã vào trong một trong các trường của dữ liệu rãnh 2.

4. Thiết bị theo điểm 1, trong đó bộ xử lý chạy ứng dụng ví tiền được cấu hình để cung cấp giao diện người dùng để hiển thị danh sách các thẻ sẵn có cho các giao dịch.

5. Thiết bị theo điểm 1, trong đó bộ xử lý chạy ứng dụng ví tiền được cấu hình để cung cấp giao diện người dùng để hiển thị danh sách các thẻ sẵn có cho các giao dịch CNP (card-not-present - không có mặt thẻ) và CP (card-present - có mặt thẻ).

6. Thiết bị theo điểm 1, trong đó định dạng dữ liệu rãnh thẻ từ bao gồm các trường dữ liệu cho PAN (primary account number - số tài khoản chính) và ngày hết hạn (EXP).

7. Thiết bị theo điểm 6, trong đó tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, bao gồm FS (field separator - phần tử tách trường) được bố trí giữa trường dữ liệu cho PAN và trường dữ liệu cho EXP.

8. Thiết bị theo điểm 7, trong đó tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, còn bao gồm LRC (error checksum character - ký tự kiểm tra tổng lỗi).

9. Thiết bị theo điểm 8, trong đó tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, còn bao gồm ES (end sentinel - cờ hiệu kết thúc).

10. Thiết bị theo điểm 6, trong đó định dạng dữ liệu rãnh thẻ từ còn bao gồm trường dữ liệu cho cờ cho máy chủ nhà phát hành thẻ để nhận ra và thực hiện cấp quyền trong chế độ CVV (card validation value - trị số xác nhận tính hợp lệ của thẻ).

11. Phương pháp truyền dữ liệu dải từ của thẻ thanh toán bao gồm các bước:

cung cấp bộ truyền từ tính bao gồm bộ dẫn động và cuộn cảm để truyền các xung từ cần được nhận ra theo cách không tiếp xúc bởi thiết bị đầu cuối ở điểm bán; và

cung cấp bộ xử lý chạy ứng dụng ví tiền bao gồm các bước,

nhận thẻ bài và khóa được kết hợp với thẻ thanh toán từ một hoặc nhiều máy chủ,

tạo ra dữ liệu bản mật mã dựa trên khóa và thông tin đếm được kết hợp với việc truyền dải từ,

tạo ra tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, bằng cách sử dụng dữ liệu bản mật mã và thẻ bài, và

truyền, qua bộ truyền từ tính, các xung từ tương ứng với tin nhắn được tạo ra đến thiết bị đầu cuối ở điểm bán.

12. Phương pháp theo điểm 11, trong đó bước tạo ra tin nhắn thanh toán bao gồm bước bao gồm dữ liệu bản mật mã trong một trong các trường của dữ liệu rãnh 2.

13. Phương pháp theo điểm 11, trong đó bước tạo ra tin nhắn thanh toán bao gồm bước sử dụng dữ liệu rãnh 2 có nhiều trường được sắp xếp theo định dạng dữ liệu rãnh 2, và biến đổi dữ liệu rãnh 2 nhờ chèn dữ liệu bản mật mã vào trong một trong các trường của dữ liệu rãnh 2.

14. Phương pháp theo điểm 11, trong đó phương pháp này còn bao gồm bước cấu hình bộ xử lý chạy ứng dụng ví tiền để cung cấp giao diện người dùng để hiển thị danh sách các thẻ sẵn có cho các giao dịch.

15. Phương pháp theo điểm 11, trong đó phương pháp này còn bao gồm bước cấu hình bộ xử lý chạy ứng dụng ví tiền để cung cấp giao diện người dùng để hiển thị danh sách các thẻ sẵn có cho các giao dịch CNP (card-not-present - không có mặt thẻ) và CP (card-present - có mặt thẻ).

16. Phương pháp theo điểm 11, trong đó định dạng dữ liệu rãnh thẻ từ bao gồm các trường dữ liệu for PAN (primary account number - số tài khoản chính) và ngày hết hạn (EXP).

17. Phương pháp theo điểm 16, trong đó tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, bao gồm FS (field separator - phần tử tách trường) được bố trí giữa trường dữ liệu cho PAN và trường dữ liệu cho EXP.

18. Phương pháp theo điểm 17, trong đó tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, còn bao gồm LRC (error checksum character - ký tự kiểm tra tổng lỗi).

19. Phương pháp theo điểm 18, trong đó tin nhắn thanh toán, tuân theo định dạng dữ liệu rãnh thẻ từ, còn bao gồm ES (end sentinel - cờ hiệu kết thúc).

20. Phương pháp theo điểm 16, trong đó định dạng dữ liệu rãnh thẻ từ còn bao gồm trường dữ liệu cho cờ cho máy chủ nhà phát hành thẻ để nhận ra và thực hiện cấp quyền trong chế độ CVV (card validation value - trị số xác nhận tính hợp lệ của thẻ).

FIG. 1

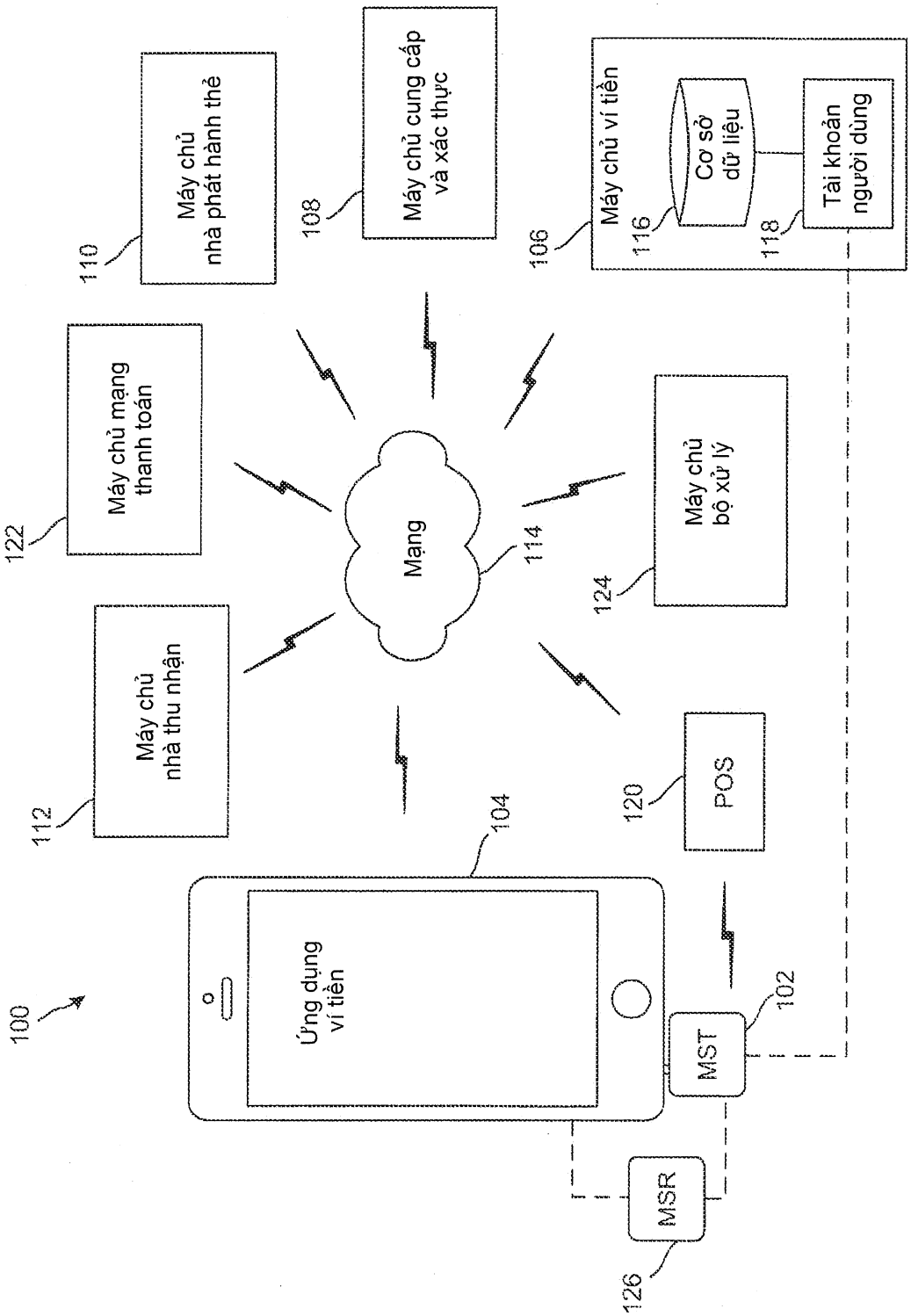

100
Ứng dụng ví tiền
104
MST
102
MSR
126
POS
120
Máy chủ nhà thu nhận
112
Máy chủ mạng thanh toán
122
Máy chủ nhà phát hành thẻ
110
Máy chủ cung cấp và xác thực
108
Mạng
114
Máy chủ bộ xử lý
124
Máy chủ ví tiền
106
Cơ sở dữ liệu
116
Tài khoản người dùng
118

FIG. 2

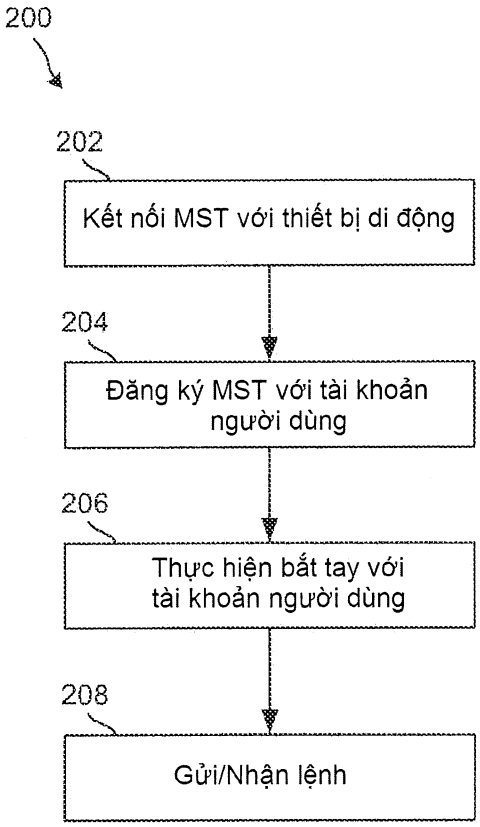

200
202
Kết nối MST với thiết bị di động
204
Đăng ký MST với tài khoản người dùng
206
Thực hiện bắt tay với tài khoản người dùng
208
Gửi/Nhận lệnh

FIG. 3

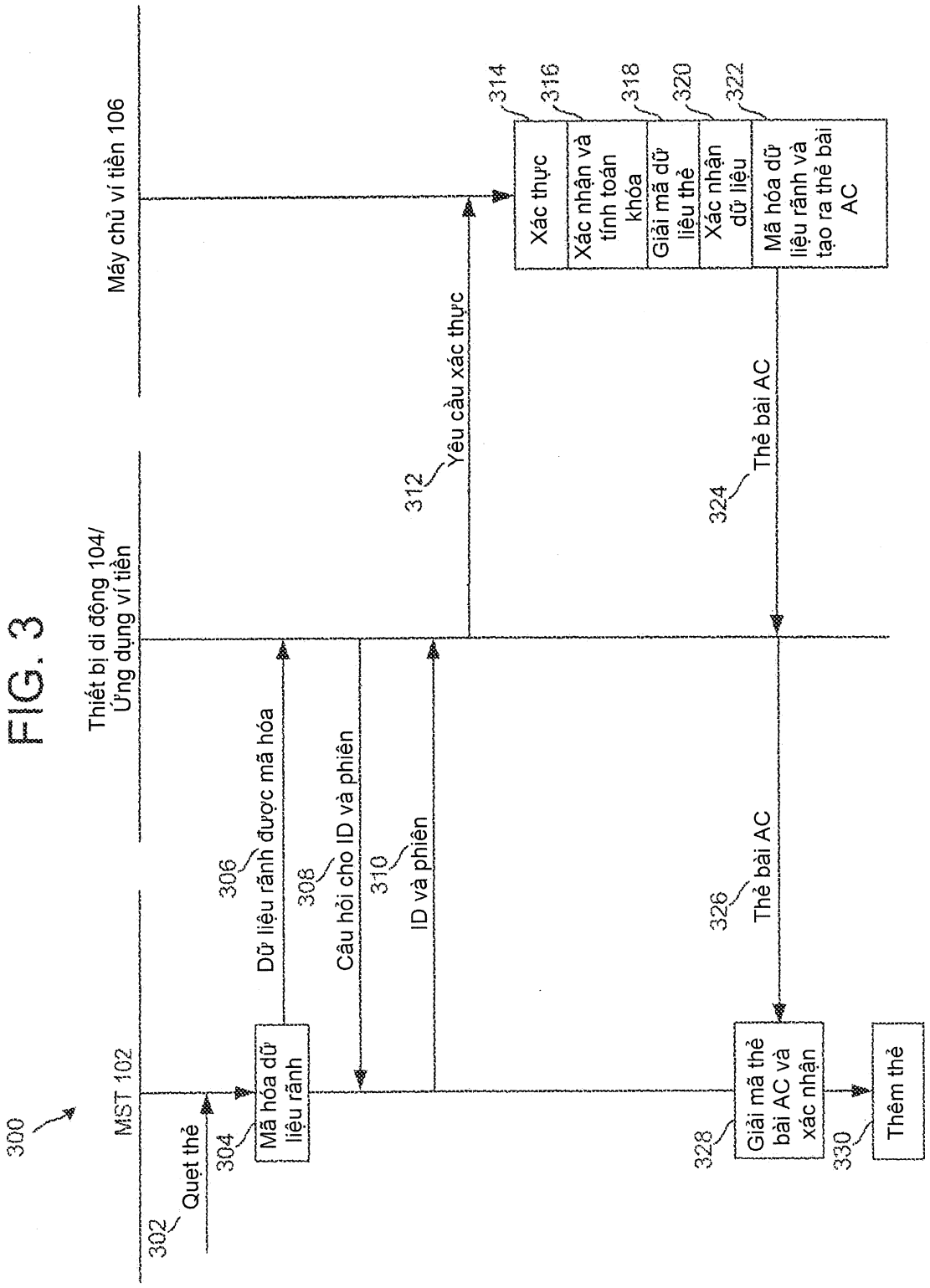

300
MST 102
Thiết bị di động 104/
Ứng dụng ví tiền
Máy chủ ví tiền 106
302
Quẹt thẻ
304
Mã hóa dữ liệu rãnh
306
Dữ liệu rãnh được mã hóa
308
Câu hỏi cho ID và phiên
310
ID và phiên
312
Yêu cầu xác thực
314
Xác thực
316
Xác nhận và tính toán khóa
318
Giải mã dữ liệu thẻ
320
Xác nhận dữ liệu
322
Mã hóa dữ liệu rãnh và tạo ra thẻ bài AC
324
Thẻ bài AC
326
Thẻ bài AC
328
Giải mã thẻ bài AC và xác nhận
330
Thêm thẻ

FIG. 4

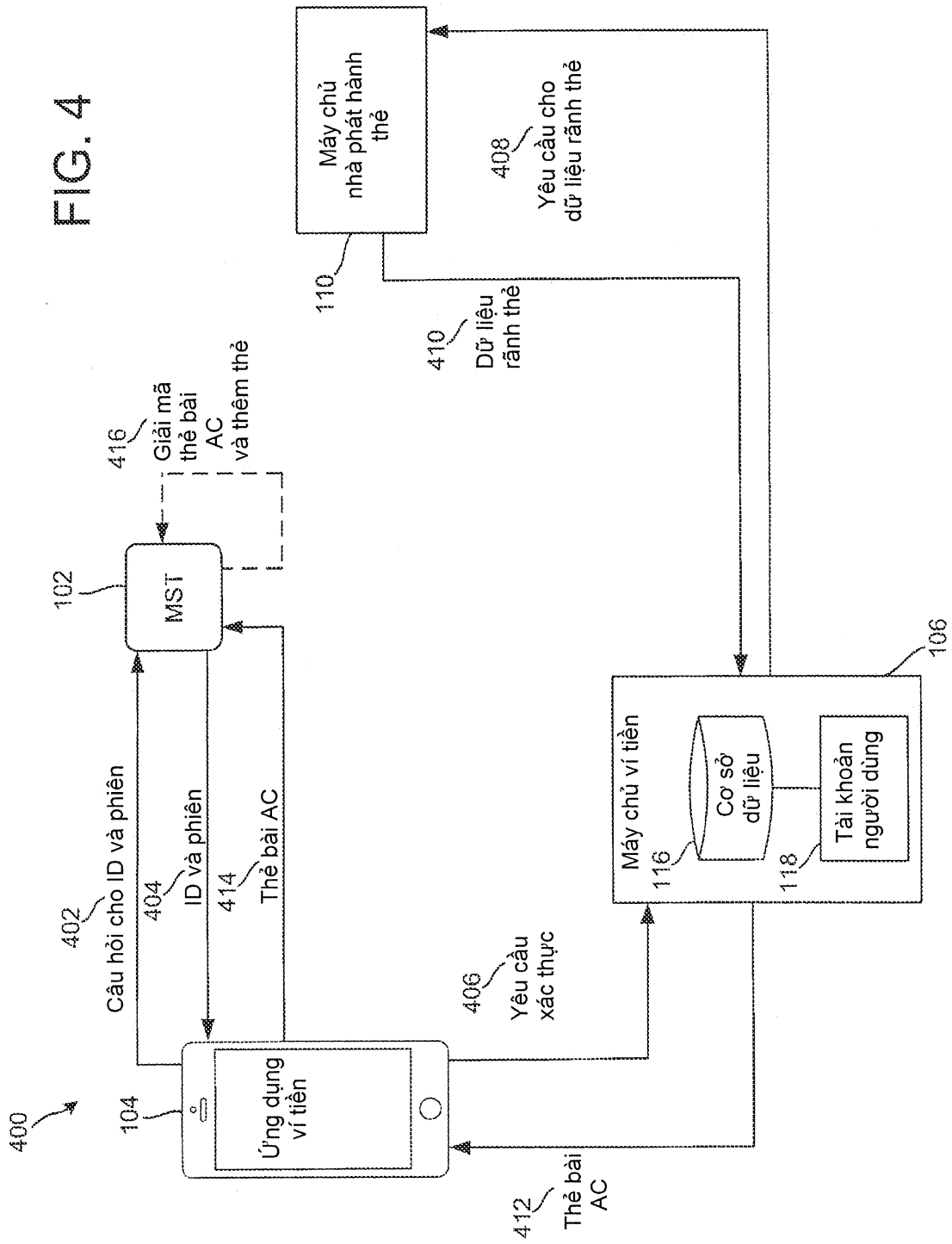

400
104
Ứng dụng ví tiền
102
MST
106
Máy chủ ví tiền
116
Cơ sở dữ liệu
118
Tài khoản người dùng
110
Máy chủ nhà phát hành thẻ
402
Câu hỏi cho ID và phiên
404
ID và phiên
414
Thẻ bài AC
406
Yêu cầu xác thực
408
Yêu cầu cho dữ liệu rãnh thẻ
410
Dữ liệu rãnh thẻ
412
Thẻ bài AC
416
Giải mã thẻ bài AC và thêm thẻ

FIG. 5

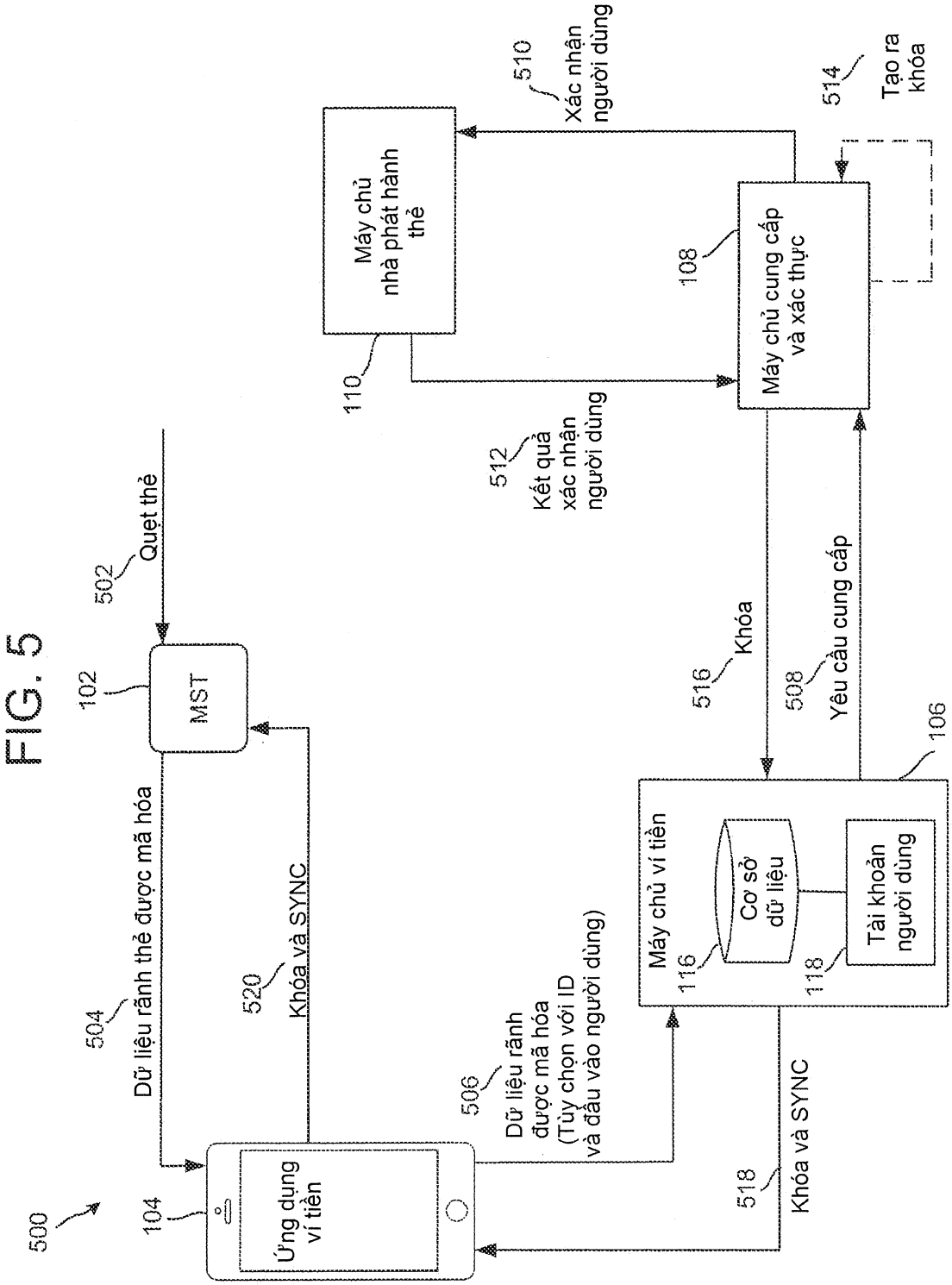

500
104
Ứng dụng ví tiền
MST
102
Quẹt thẻ
502
Dữ liệu rãnh thẻ được mã hóa
504
Khóa và SYNC
520
Dữ liệu rãnh được mã hóa (Tùy chọn với ID và đầu vào người dùng)
506
Khóa và SYNC
518
Máy chủ ví tiền
116
Cơ sở dữ liệu
118
Tài khoản người dùng
106
Khóa
516
Yêu cầu cung cấp
508
Máy chủ cung cấp và xác thực
108
Tạo ra khóa
514
Máy chủ nhà phát hành thẻ
110
Xác nhận người dùng
510
Kết quả xác nhận người dùng
512

FIG. 6

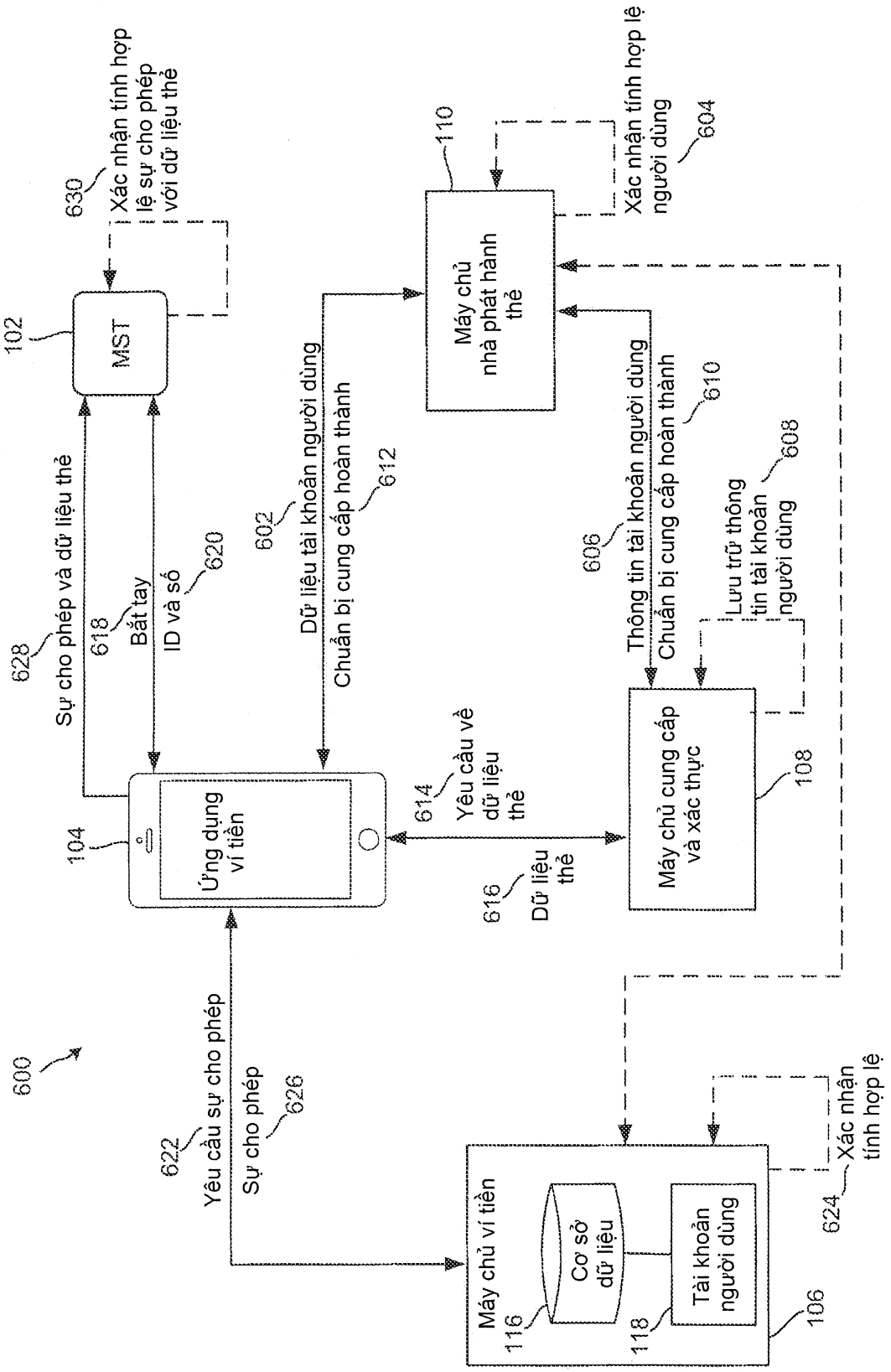

600
102
MST
104
Ứng dụng ví tiền
110
Máy chủ nhà phát hành thẻ
108
Máy chủ cung cấp và xác thực
106
Máy chủ ví tiền
116
Cơ sở dữ liệu
118
Tài khoản người dùng
630
Xác nhận tính hợp lệ sự cho phép với dữ liệu thẻ
628
Sự cho phép và dữ liệu thẻ
618
Bắt tay
620
ID và số
602
Dữ liệu tài khoản người dùng
612
Chuẩn bị cung cấp hoàn thành
614
Yêu cầu về dữ liệu thẻ
616
Dữ liệu thẻ
606
Thông tin tài khoản người dùng
610
Chuẩn bị cung cấp hoàn thành
608
Lưu trữ thông tin tài khoản người dùng
604
Xác nhận tính hợp lệ người dùng
622
Yêu cầu sự cho phép
626
Sự cho phép
624
Xác nhận tính hợp lệ

FIG. 7

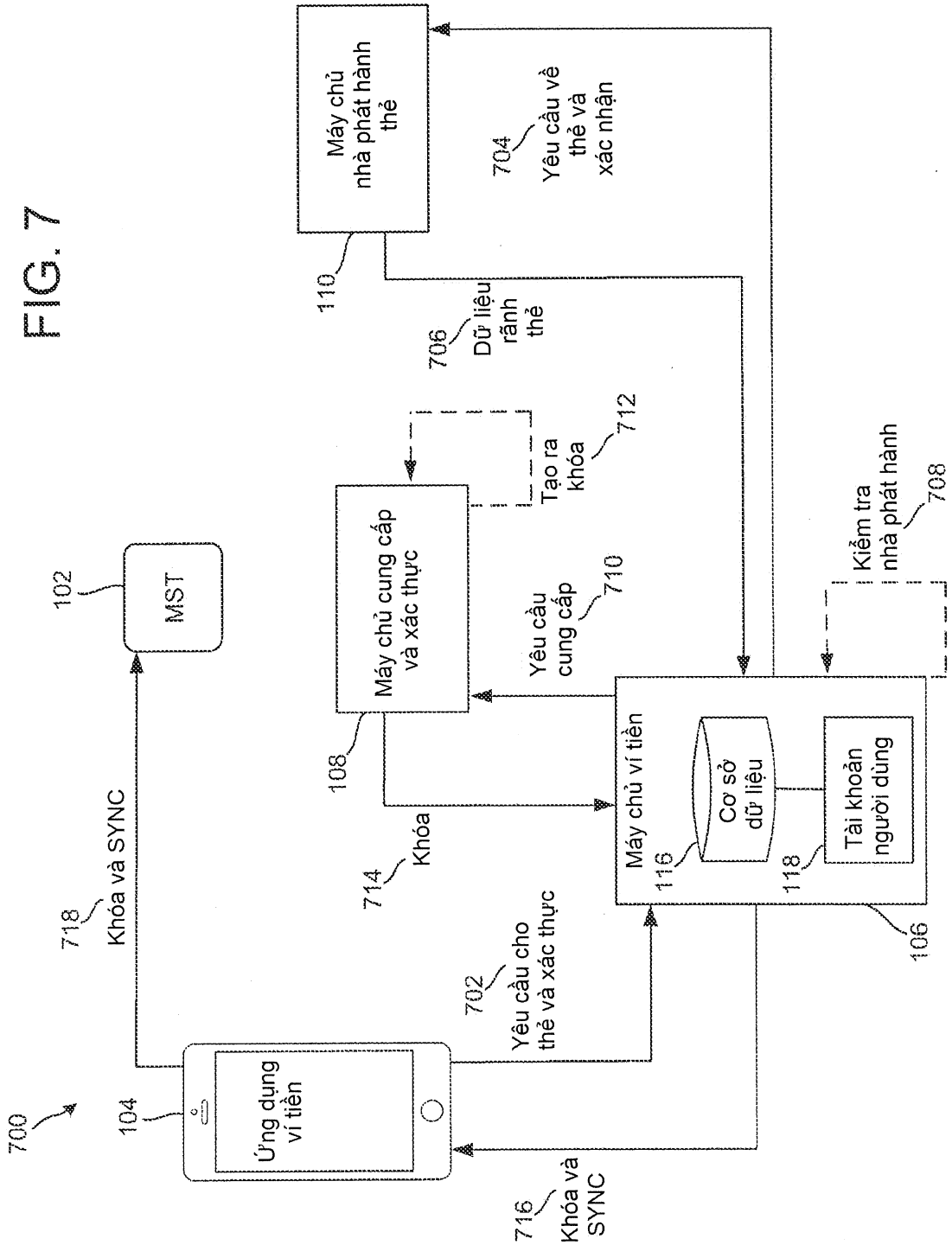

700
104
Ứng dụng ví tiền
102
MST
718
Khóa và SYNC
716
Khóa và SYNC
702
Yêu cầu cho thẻ và xác thực
714
Khóa
108
Máy chủ cung cấp và xác thực
Yêu cầu cung cấp
710
Tạo ra khóa
712
110
Máy chủ nhà phát hành thẻ
706
Dữ liệu rãnh thẻ
704
Yêu cầu về thẻ và xác nhận
Kiểm tra nhà phát hành
708
Máy chủ ví tiền
116
Cơ sở dữ liệu
118
Tài khoản người dùng
106

FIG. 8

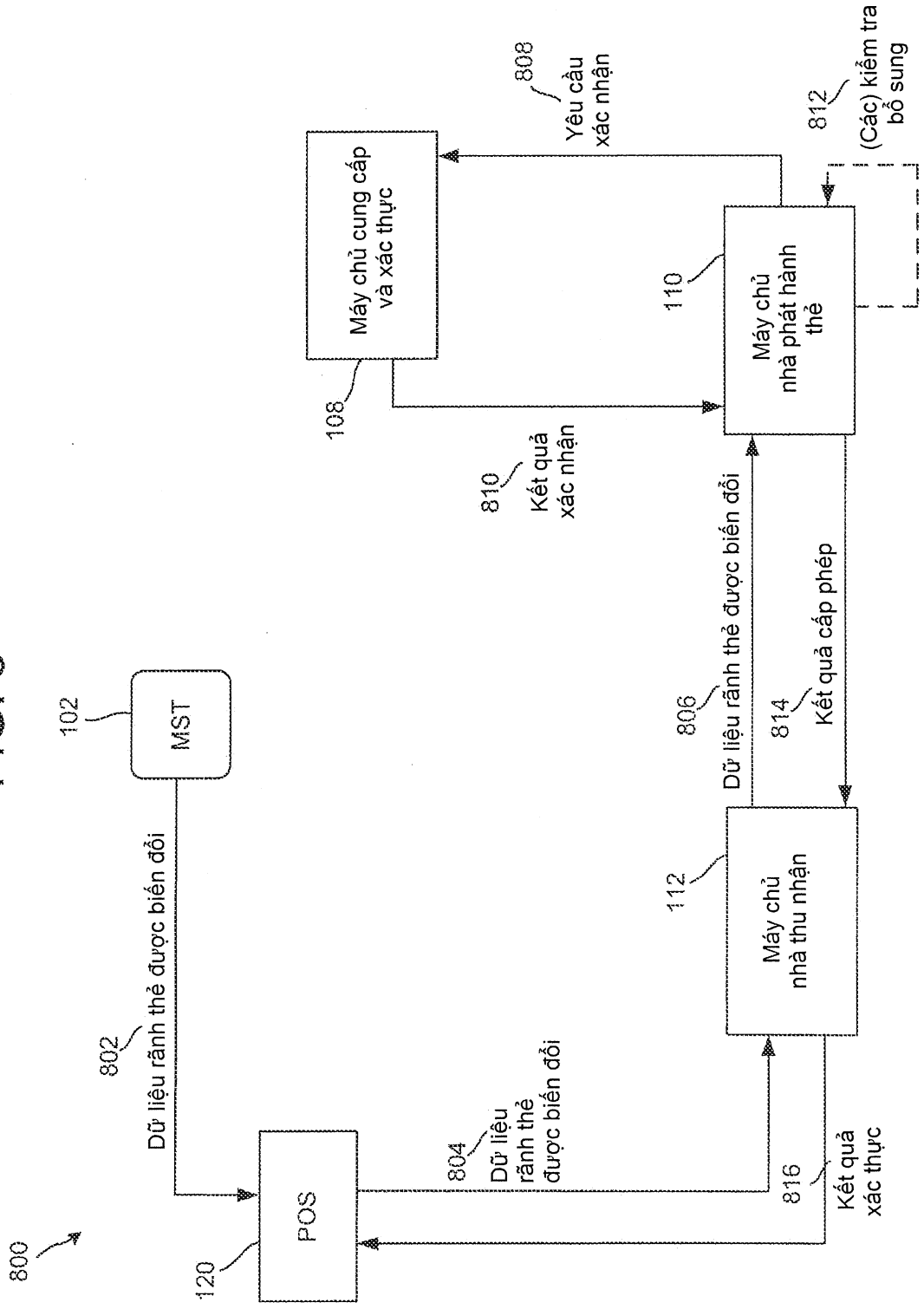

800
102
MST
802
Dữ liệu rãnh thẻ được biến đổi
120
POS
804
Dữ liệu rãnh thẻ được biến đổi
806
Dữ liệu rãnh thẻ được biến đổi
112
Máy chủ nhà thu nhận
814
Kết quả cấp phép
816
Kết quả xác thực
108
Máy chủ cung cấp và xác thực
808
Yêu cầu xác nhận
810
Kết quả xác nhận
110
Máy chủ nhà phát hành thẻ
812
(Các) kiểm tra bổ sung

FIG. 9

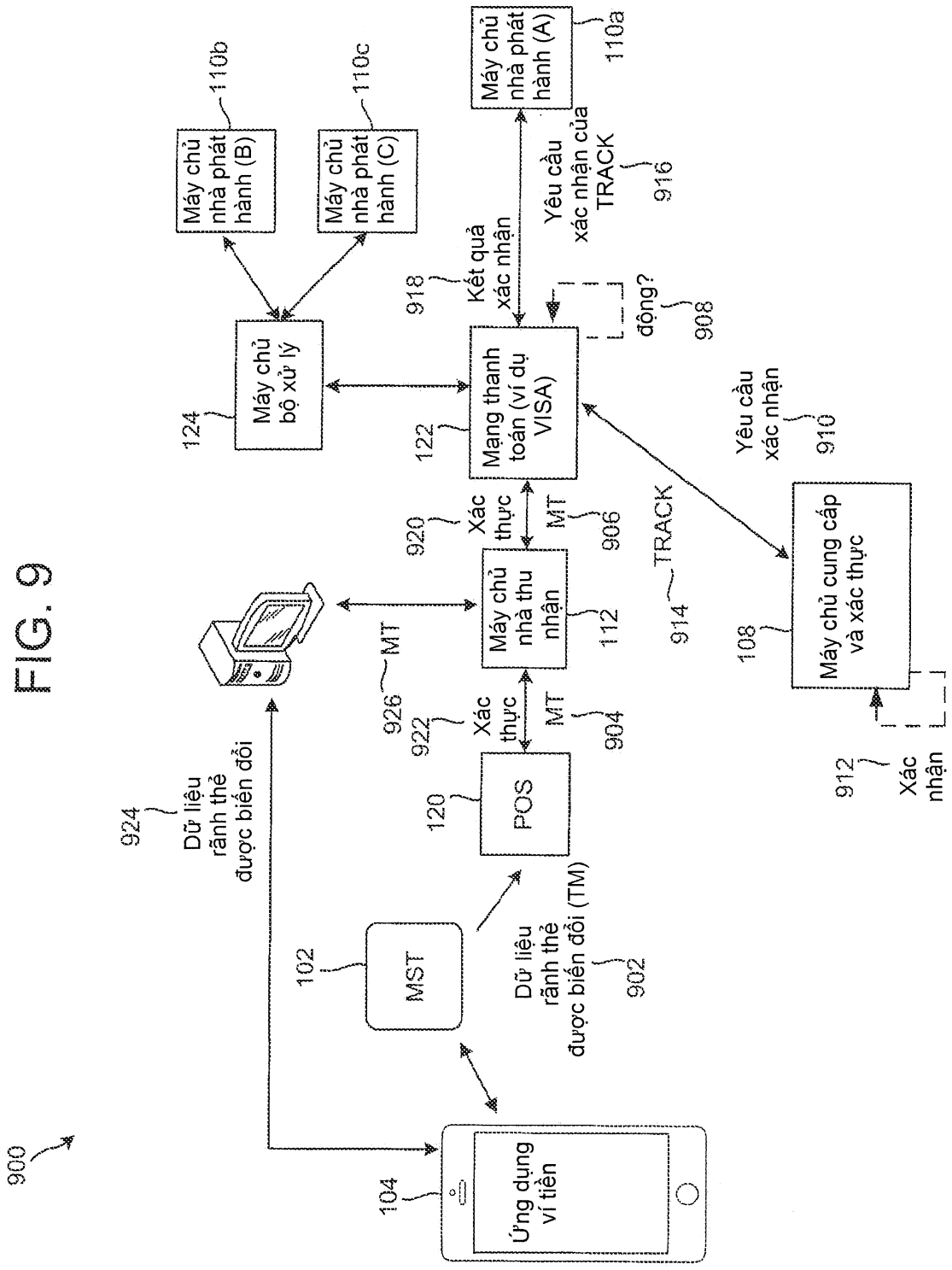

900
Ứng dụng ví tiền
104
MST
102
Dữ liệu rãnh thẻ được biến đổi (TM)
902
Dữ liệu rãnh thẻ được biến đổi
924
POS
120
Xác thực MT
922
904
MT
926
Máy chủ nhà thu nhận
112
Xác thực MT
920
906
Mạng thanh toán (ví dụ VISA)
122
Máy chủ bộ xử lý
124
Máy chủ nhà phát hành (B)
110b
Máy chủ nhà phát hành (C)
110c
Máy chủ nhà phát hành (A)
110a
Kết quả xác nhận
918
Yêu cầu xác nhận của TRACK
916
động?
908
TRACK
914
Yêu cầu xác nhận
910
Máy chủ cung cấp và xác thực
108
Xác nhận
912

FIG. 10

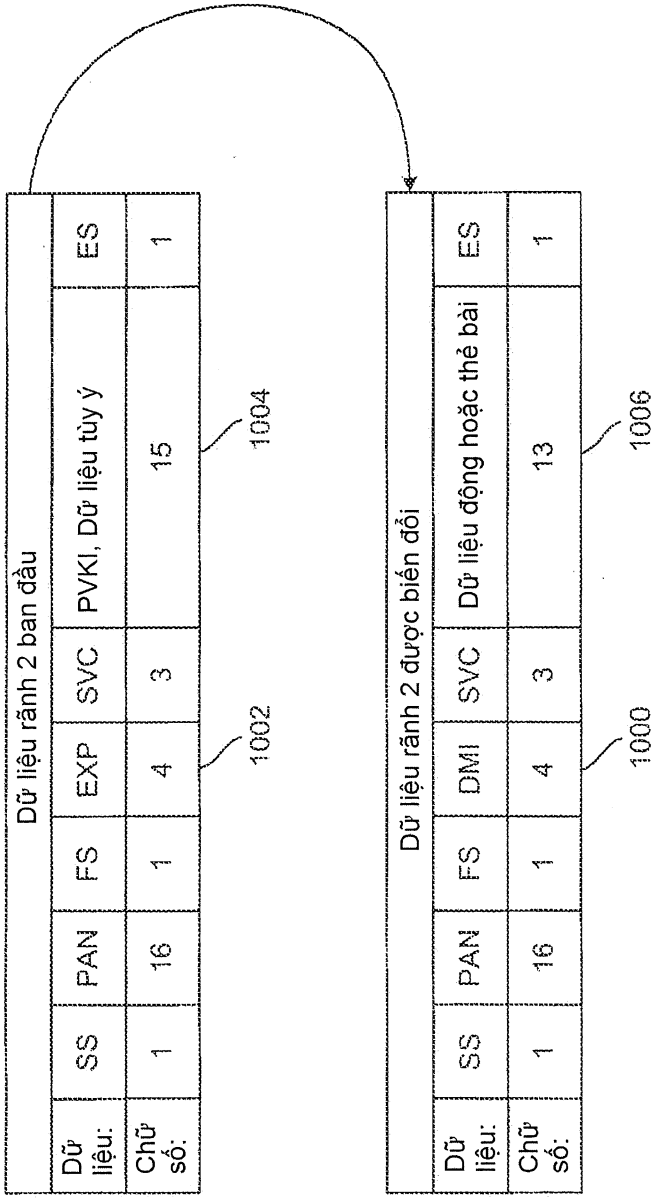

Dữ liệu rãnh 2 ban đầu
Dữ liệu:
Chữ số:
SS
1
PAN
16
FS
1
EXP
4
SVC
3
PVKI, Dữ liệu tùy ý
15
ES
1
1002
1004
Dữ liệu rãnh 2 được biến đổi
Dữ liệu:
Chữ số:
SS
1
PAN
16
FS
1
DMI
4
SVC
3
Dữ liệu động hoặc thẻ bài
13
ES
1
1000
1006

FIG. 11

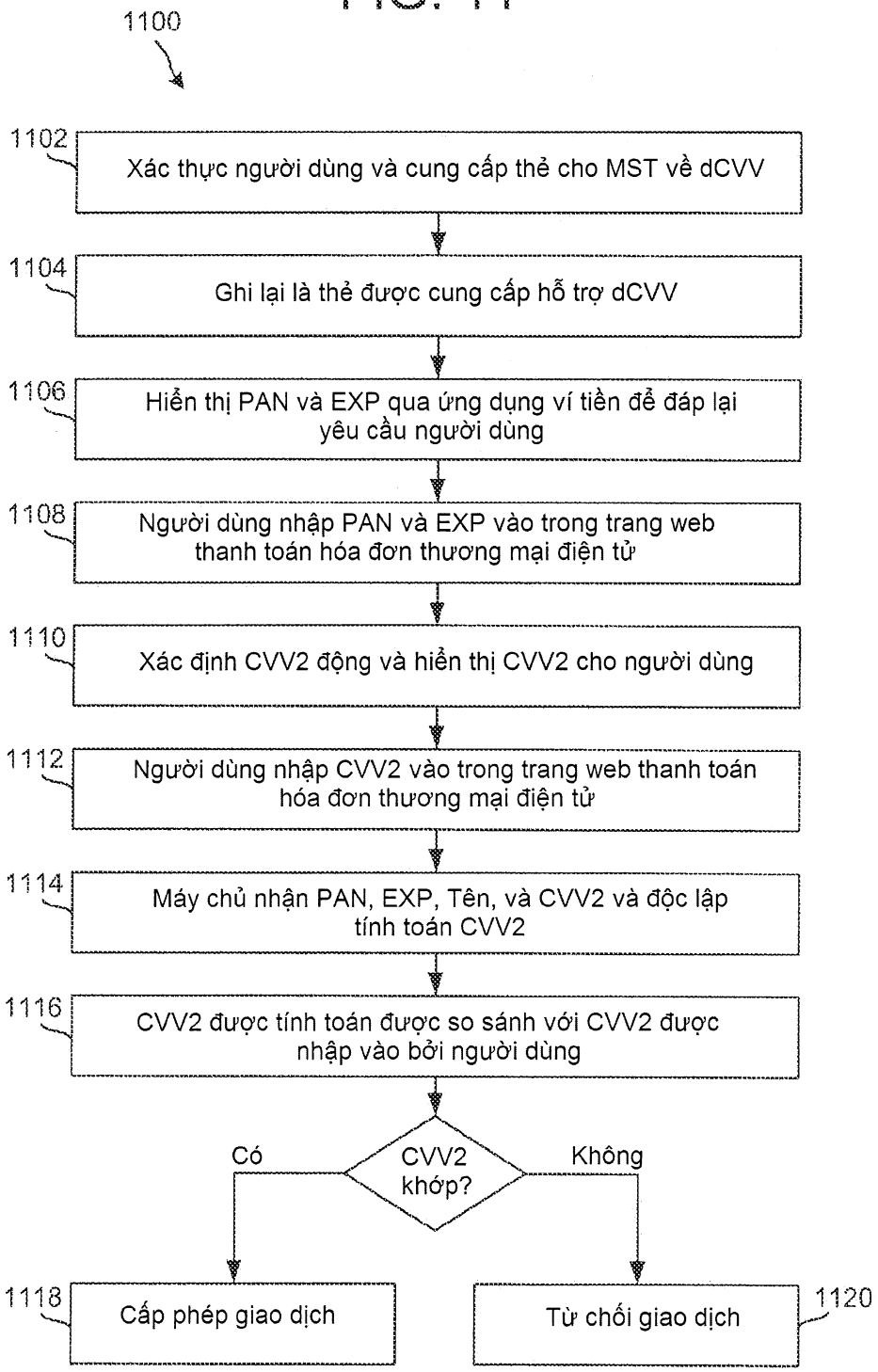
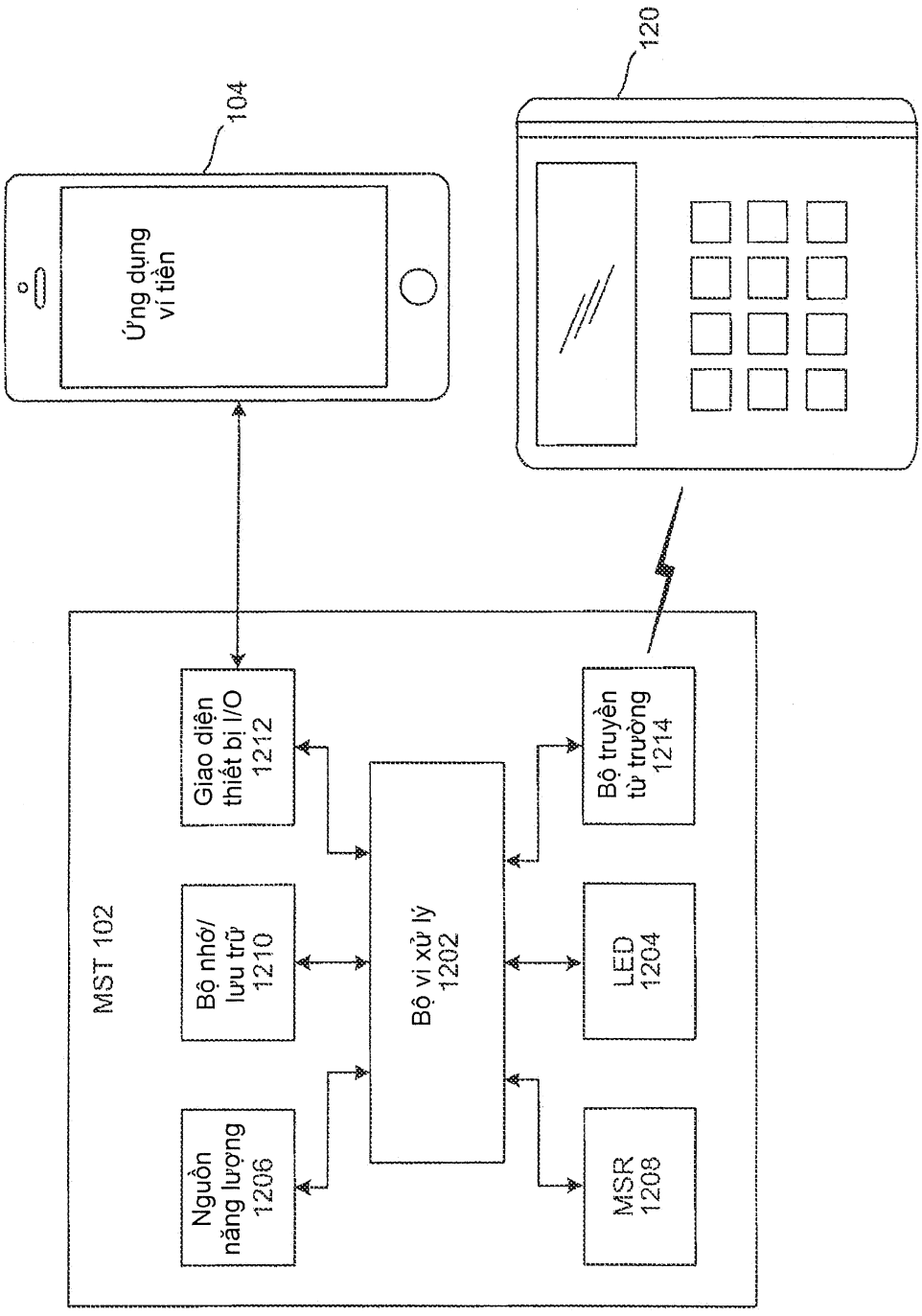

1100
1102
Xác thực người dùng và cung cấp thẻ cho MST về dCVV
1104
Ghi lại là thẻ được cung cấp hỗ trợ dCVV
1106
Hiển thị PAN và EXP qua ứng dụng ví tiền để đáp lại yêu cầu người dùng
1108
Người dùng nhập PAN và EXP vào trong trang web thanh toán hóa đơn thương mại điện tử
1110
Xác định CVV2 động và hiển thị CVV2 cho người dùng
1112
Người dùng nhập CVV2 vào trong trang web thanh toán hóa đơn thương mại điện tử
1114
Máy chủ nhận PAN, EXP, Tên, và CVV2 và độc lập tính toán CVV2
1116
CVV2 được tính toán được so sánh với CVV2 được nhập vào bởi người dùng
CVV2 khớp?
Có
Không
1118
Cấp phép giao dịch
1120
Từ chối giao dịch

FIG. 12


104
Ứng dụng ví tiền
120
MST 102
Giao diện thiết bị I/O 1212
Bộ truyền từ trường 1214
Bộ nhớ/ lưu trữ 1210
Bộ vi xử lý 1202
LED 1204
Nguồn năng lượng 1206
MSR 1208