(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) **1-0028977**

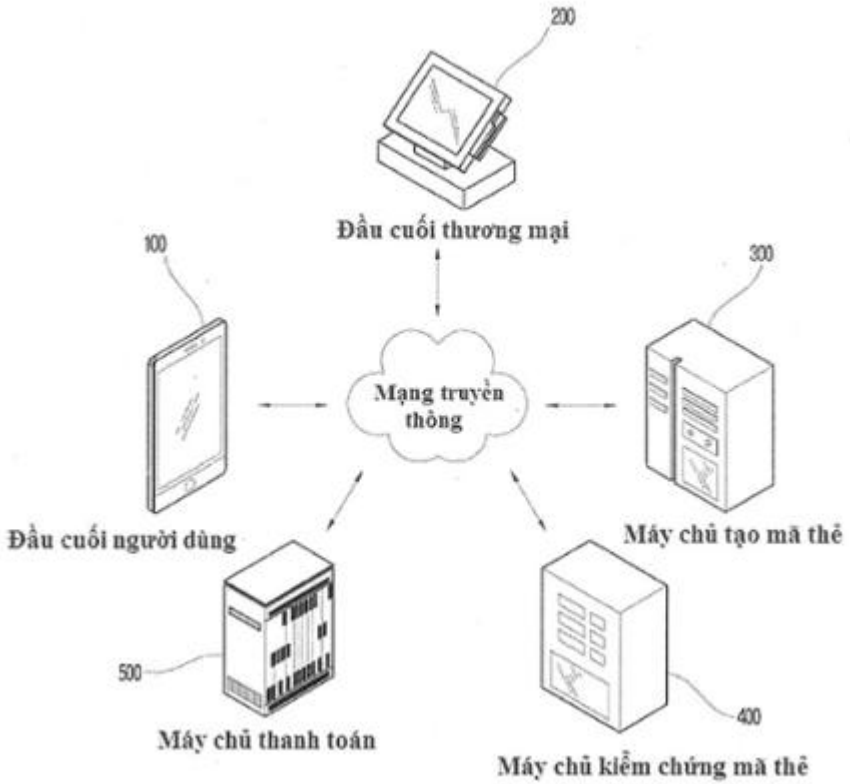
(51)[8] **H04L 9/32**; G06Q 20/14

(13) **B**

(21) 1-2017-03873
(22) 17/09/2015
(86) PCT/KR2015/009769 17/09/2015
(87) WO2016/159462 06/10/2016
(30) 10-2015-0047577 03/04/2015 KR; 10-2015-0056211 21/04/2015 KR
(45) 25/07/2021 400
(43) 25/12/2017 357A
(73) BC CARD CO., LTD. (KR)
Hyoryeong-ro 275, Seocho-gu, Seoul 06654, Korea
(72) YI, Ji Ho (KR).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG XÁC THỰC MÃ THẺ SỬ DỤNG GIÁ TRỊ KIỂM TRA TẠO RA DỰA TRÊN THỜI GIAN HIỆN TẠI

(57) Sáng chế đề cập đến phương pháp dùng để xác thực mã thẻ bằng hệ thống xác thực mã thẻ, sử dụng giá trị kiểm tra tạo ra dựa trên thời gian hiện tại; và hệ thống xác thực mã thẻ. Phương pháp này bao gồm các bước: tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ, và cấp số thẻ ảo này tới đầu cuối người dùng, bằng máy chủ tạo mã thẻ; tiếp nhận yêu cầu xác thực bao gồm thông tin nhận dạng tương ứng với số thẻ ảo qua đầu cuối thương mại mà nhận ra thông tin nhận dạng từ đầu cuối người dùng, bằng máy chủ kiểm chứng mã thẻ; tạo lại giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin nhận dạng, bằng máy chủ kiểm chứng mã thẻ; và khi việc xác thực mã thẻ được hoàn thành, truyền yêu cầu thanh toán bao gồm mã thẻ tới máy chủ thanh toán khiến cho việc thanh toán được thực hiện bởi phương tiện thanh toán phù hợp với mã thẻ này, bằng máy chủ kiểm chứng mã thẻ.


200
Đầu cuối thương mại
100
Đầu cuối người dùng
Mạng truyền thông
300
Máy chủ tạo mã thẻ
500
Máy chủ thanh toán
400
Máy chủ kiểm chứng mã thẻ

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp xác thực mã thẻ sử dụng giá trị kiểm tra tạo ra dựa trên thời gian hiện tại và hệ thống xác thực mã thẻ sử dụng phương pháp xác thực mã thẻ này, và cụ thể hơn, tới phương pháp xác thực mã thẻ trong đó giá trị kiểm tra được tạo ra dựa trên thời gian hiện tại, mã thẻ được xác thực nhờ sử dụng giá trị kiểm tra đã tạo ra, và, khi việc xác thực mã thẻ được hoàn thành, việc thanh toán được thực hiện, và hệ thống xác thực mã thẻ sử dụng phương pháp này.

Tình trạng kỹ thuật của sáng chế

Việc giao dịch qua thiết bị di động dễ bị tấn công an ninh với sự sao chép giao dịch ngoại trừ thẻ di động cấp trên miền an toàn. Do đó, việc sử dụng mã thẻ, mà là số thẻ ảo sử dụng một lần, đang tăng lên với các kiểu phương pháp thanh toán thương mại khác nhau, như ký tự, mã vạch, mã đáp ứng nhanh (QR), thẻ truyền thông trường gần (NFC), và tương tự.

Để sử dụng mã thẻ, máy chủ tạo mã thẻ có thể liên tục tạo ra các mã thẻ mới và cấp mã thẻ tới đầu cuối người dùng, và có thể chứa mã thẻ đã cấp trong thời gian xác định trong cơ sở dữ liệu để xác minh hiệu lực của mã thẻ này, và máy chủ kiểm chứng mã thẻ có thể so sánh mã thẻ tiếp nhận từ đầu cuối thương mại tại thời gian chấp nhận giao dịch bằng thẻ chứa tạm thời trong cơ sở dữ liệu để kiểm tra hiệu lực giao dịch khiến cho có thể đạt được độ an toàn thích hợp theo cách đơn giản.

Tuy nhiên, phương pháp sử dụng mã thẻ mô tả nêu trên yêu cầu máy chủ tạo mã thẻ và máy chủ kiểm chứng mã thẻ tồn tại trong cùng máy chủ, nghĩa là, yêu cầu kết cấu hệ thống hợp nhất, mà khó tạo ra dịch vụ nhất quán trong trường hợp không mong muốn, như lỗi hệ thống.

Ngoài ra, để sử dụng mã thẻ, các yêu cầu với việc cấp và kiểm chứng mã thẻ luôn cần phải được thực hiện trực tuyến, và sau đó quá trình thích hợp được thực hiện.

Do đó, làm tăng nhu cầu với các hệ thống có khả năng tách biệt về mặt vật lý hoặc lôgic hệ thống cấp mã thẻ với hệ thống xác thực mã thẻ, và giải pháp để giải quyết sự hạn chế nêu trên là một yêu câu cấp bách.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề cập đến phương pháp xác thực mã thẻ trong đó giá trị kiểm tra được tạo ra dựa trên thời gian hiện tại, mã thẻ được xác thực nhờ sử dụng giá trị kiểm tra đã tạo ra, và, khi việc xác thực mã thẻ được hoàn thành, việc thanh toán được thực hiện, và hệ thống xác thực mã thẻ sử dụng phương pháp này.

Ngoài ra, sáng chế cũng đề cập đến phương pháp xác thực mã thẻ trong đó thiết bị để cấp số thẻ ảo bao gồm mã thẻ được tách biệt về mặt vật lý hoặc lôgic với thiết bị để xác thực mã thẻ, và hệ thống xác thực mã thẻ sử dụng phương pháp xác thực mã thẻ này.

Ngoài ra, sáng chế cũng đề cập đến phương pháp xác thực mã thẻ trong đó nguy cơ sao chép giao dịch trong quá trình giao dịch qua thiết bị di động được giải quyết, hệ thống để xử lý giao dịch được đơn giản hóa, và mã thẻ được sử dụng một cách ổn định trong các môi trường và phương tiện khác nhau, và hệ thống xác thực mã thẻ sử dụng phương pháp xác thực mã thẻ này.

Các mục đích của sáng chế không bị giới hạn ở các phương án bộc lộ nêu trên, và các mục đích khác có thể trở nên rõ ràng với người có hiểu biết trung bình trong lĩnh vực kỹ thuật này từ phần mô tả dưới đây.

Một khía cạnh của sáng chế đề cập đến phương pháp xác thực mã thẻ sử dụng giá trị kiểm tra tạo ra dựa trên thời gian hiện tại trong hệ thống xác thực mã thẻ, phương pháp xác thực mã thẻ này bao gồm các bước, tạo ra, bằng máy chủ tạo mã thẻ, giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ, và cấp số thẻ ảo đã tạo tới đầu cuối người dùng; tiếp nhận, bằng máy chủ kiểm chứng mã thẻ, yêu cầu xác thực bao gồm thông tin nhận dạng tương ứng với số thẻ ảo qua đầu cuối thương mại mà nhận ra thông tin nhận dạng từ đầu cuối người dùng; tạo lại, bằng máy chủ kiểm chứng mã thẻ, giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và, khi việc xác thực mã thẻ được hoàn thành, truyền, bằng máy chủ kiểm chứng mã thẻ, yêu cầu thanh toán bao gồm mã thẻ tới máy chủ thanh toán khiến cho việc thanh toán được thực hiện bằng phương tiện thanh toán phù hợp với mã thẻ này.

Việc cấp số thẻ ảo có thể bao gồm, tạo ra, bằng máy chủ tạo mã thẻ, khóa duy nhất bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

Khía cạnh khác của sáng chế đề cập đến phương pháp xác thực mã thẻ sử dụng giá trị kiểm tra tạo ra dựa trên thời gian hiện tại trong hệ thống xác thực mã thẻ, phương pháp xác thực mã thẻ này bao gồm các bước: tiếp nhận, bằng đầu cuối người dùng, thông tin tạo khóa từ máy chủ tạo mã thẻ, tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại từ thông tin tạo khóa, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ, và cấp số thẻ ảo đã tạo tới bộ nhớ mã thẻ nối với đầu cuối người dùng; tiếp nhận, bằng máy chủ kiểm chứng mã thẻ, yêu cầu xác thực bao gồm thông tin nhận dạng tương ứng với số thẻ ảo qua đầu cuối thương mại mà nhận ra thông tin nhận dạng từ đầu cuối người dùng; tạo lại, bằng máy chủ kiểm chứng mã thẻ, giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và, khi việc xác thực mã thẻ được hoàn thành, truyền, bằng máy chủ kiểm chứng mã thẻ, yêu cầu thanh toán bao gồm mã thẻ tới máy chủ thanh toán khiến cho việc thanh toán được thực hiện bằng phương tiện thanh toán phù hợp với mã thẻ này.

Việc cấp số thẻ ảo có thể bao gồm, tạo ra, bằng đầu cuối người dùng, khóa duy nhất bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

Khía cạnh khác nữa của sáng chế đề cập đến hệ thống xác thực mã thẻ bao gồm: máy chủ tạo mã thẻ được tạo kết cấu để tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ, và cấp số thẻ ảo đã tạo tới đầu cuối người dùng; đầu cuối thương mại được tạo kết cấu để nhận ra thông tin nhận dạng tương ứng với số thẻ ảo từ đầu cuối người dùng; máy chủ kiểm chứng mã thẻ được tạo kết cấu để tiếp nhận yêu cầu xác thực bao gồm thông tin nhận dạng đã nhận ra qua đầu cuối thương mại, tạo lại giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra, và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và máy chủ thanh toán được tạo kết cấu để, khi việc xác thực mã thẻ được hoàn thành, tiếp nhận yêu cầu thanh toán bao gồm mã thẻ từ máy chủ xác thực mã thẻ và thực hiện việc thanh toán bằng phương tiện thanh toán phù hợp với mã thẻ này.

Khóa duy nhất có thể được tạo ra bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

Khía cạnh khác nữa của sáng chế đề cập đến hệ thống xác thực mã thẻ bao gồm: đầu cuối người dùng được tạo kết cấu để tiếp nhận thông tin tạo khóa từ máy chủ tạo mã thẻ, tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại từ thông tin tạo khóa, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ, và cấp số thẻ ảo đã tạo tới bộ nhớ mã thẻ; đầu cuối thương mại được tạo kết cấu để nhận ra thông tin nhận dạng tương ứng với số thẻ ảo từ đầu cuối người dùng; máy chủ kiểm chứng mã thẻ được tạo kết cấu để tiếp nhận yêu cầu xác thực bao gồm thông tin nhận dạng đã nhận ra qua đầu cuối thương mại, tạo lại giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra, và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và máy chủ thanh toán được tạo kết cấu để, khi việc xác thực mã thẻ được hoàn thành, tiếp nhận yêu cầu thanh toán bao gồm mã thẻ từ máy chủ xác thực mã thẻ và thực hiện việc thanh toán bằng phương tiện thanh toán phù hợp với mã thẻ này.

Khóa duy nhất có thể được tạo ra bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

Theo một phương án, hệ thống xác thực mã thẻ, trong đó thiết bị để cấp số thẻ ảo bao gồm mã thẻ được tách biệt về mặt vật lý hoặc lôgic với thiết bị để xác thực mã thẻ, có thể được tạo khiến cho dịch vụ nhất quán có thể được tạo ngay cả trong trường hợp không mong muốn, như lỗi hệ thống.

Theo một phương án, đầu cuối người dùng có thể tự tạo ra giá trị kiểm tra và cấp số thẻ ảo bao gồm giá trị kiểm tra và mã thẻ ngay cả khi ngoại tuyến khiến cho quá trình cấp số thẻ ảo bao gồm mã thẻ có thể đạt được ngay cả khi đầu cuối người dùng không ở trạng thái trực tuyến.

Theo một phương án, nguy cơ sao chép giao dịch trong quá trình giao dịch qua thiết bị di động có thể được giải quyết, hệ thống để xử lý giao dịch có thể được đơn giản hóa, và có thể đảm bảo sự an toàn trong khi sử dụng mã thẻ trong các phương tiện và môi trường khác nhau.

Cần hiểu rằng các hiệu quả của sáng chế không bị giới hạn ở các hiệu quả nêu trên và bao gồm tất cả các hiệu quả mà có thể suy ra từ phần mô tả chi tiết của sáng chế hoặc kết cấu của sáng chế mô tả trong các điểm yêu cầu bảo hộ.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ thể hiện hệ thống xác thực mã thẻ theo một phương án;

Fig.2 là hình vẽ thể hiện quá trình tiến hành thanh toán qua việc xác thực mã thẻ theo một phương án; và

Fig.3 là hình vẽ thể hiện quá trình thực hiện việc thanh toán nhờ xác thực mã thẻ theo một phương án khác.

Mô tả chi tiết sáng chế

Sáng chế sẽ được mô tả chi tiết trong phần mô tả dưới đây cùng các hình vẽ kèm theo. Sáng chế có thể được thể hiện theo các cách khác nhau và không được xem như bị giới hạn ở các phương án đưa ra trong bản mô tả này. Trên các hình vẽ, các phần không liên quan tới việc mô tả đã được bỏ qua để cho rõ ràng, và các số chỉ dẫn tương tự biểu thị các chi tiết tương tự trên toàn bộ cách hình vẽ này.

Cần hiểu rằng khi chi tiết được xem như "được nối" hoặc "được ghép" với chi tiết khác, chi tiết này có thể được nối hoặc được ghép trực tiếp với chi tiết khác, hoặc có thể có các chi tiết trung gian. Các thuật ngữ "bao gồm", "bao gồm", "bao gồm", và/hoặc "bao gồm" nghĩa là các chi tiết cấu thành, các bước, hoạt động và/hoặc các chi tiết đã mô tả được bao gồm và không loại trừ việc bổ sung một hoặc nhiều chi tiết cấu thành, bước, hoạt động và/hoặc sự tồn tại hoặc bổ sung các chi tiết khác trừ khi được chỉ ra theo cách khác.

Dưới đây, các phương án của sáng chế sẽ được mô tả chi tiết có dựa vào các hình vẽ kèm theo.

Fig.1 là hình vẽ thể hiện hệ thống xác thực mã thẻ theo một phương án;

Như được thể hiện trên Fig.1, hệ thống xác thực mã thẻ theo một phương án có thể bao gồm đầu cuối người dùng 100, đầu cuối thương mại 200, máy chủ tạo mã thẻ 300, máy chủ kiểm chứng mã thẻ 400, và máy chủ thanh toán 500, mà có thể truyền thông với nhau qua mạng truyền thông.

Mạng truyền thông có thể được lắp đặt mà không bị giới hạn ở kiểu truyền thông, như truyền thông có dây hoặc truyền thông không dây. Mạng truyền thông có thể được lắp đặt dưới dạng các mạng truyền thông khác nhau, chẳng hạn, mạng cục bộ (LAN), mạng thành phố lớn (MAN), mạng diện rộng (WAN), và mạng tương tự. Tốt hơn là, mạng truyền thông mô tả theo sáng chế này có thể được lắp đặt dưới dạng mạng truyền thông di động hoặc mạng toàn cầu (WWW) mà đã biết trong kỹ thuật và khác với mạng truyền thông di động.

Đầu cuối người dùng 100 có thể bao gồm tất cả các loại thiết bị truyền thông không dây cầm tay mà có thể được nối với máy chủ bên ngoài qua mạng, ví dụ, điện thoại di động, điện thoại thông minh, hỗ trợ số cá nhân (PDA), máy đọc đa phương tiện xác tay (PMP), máy tính bảng cá nhân (máy tính bảng PC), và tương tự. Ngoài ra, đầu cuối người dùng 100 có thể bao gồm thiết bị truyền thông mà có thể được nối với máy chủ bên ngoài qua mạng Internet, ví dụ, máy tính cá nhân để bàn, máy tính bảng, máy tính xách tay, và máy thu hình giao thức Internet (IPTV) bao gồm hộp đặt trên nóc .

Đầu cuối người dùng 100 có thể thực hiện việc xác thực người dùng sử dụng phương pháp nhận dạng cá nhân đăng ký trước, ví dụ, dịch vụ tin nhắn ngắn (SMS), giấy chứng nhận, mật khẩu thanh toán, và tương tự.

Đầu cuối người dùng 100 có thể sử dụng số thẻ ảo cấp bởi máy chủ tạo mã thẻ 300 để tạo ra thông tin nhận dạng tương ứng với số thẻ ảo này, và có thể cho phép thông tin nhận dạng được nhận ra bởi đầu cuối thương mại 200. Trong bản mô tả này, thông tin nhận dạng có thể được tạo trong các dạng khác nhau, như âm thanh, ký tự, mã vạch, mã đáp ứng nhanh (QR), thông tin thẻ truyền thông trường gần (NFC), và tương tự. Thông tin nhận dạng có thể thông tin về phương pháp thanh toán hoặc thông tin cụ thể tương ứng với phương pháp thanh toán.

Nghĩa là, đầu cuối người dùng 100 có thể cho phép các phương pháp thanh toán khác nhau, như âm thanh, ký tự, mã vạch, mã QR, và mã thẻ NFC sẵn sàng, sử dụng thông tin nhận dạng tương ứng với số thẻ ảo, và cũng có thể cho phép thông tin nhận dạng được nhận ra bởi đầu cuối thương mại 200 sao cho việc thanh toán được yêu cầu qua phương pháp thanh toán đăng ký trước tương ứng với thông tin nhận dạng.

Đầu cuối thương mại 200 có thể là đầu cuối lắp đặt ở chi nhánh của người điều hành (nghĩa là, người điều hành công ty thẻ tín dụng) mà điều hành máy chủ thanh toán

500, ví dụ, đầu cuối điểm bán (POS). Đầu cuối POS có thể được ấn định trước giá trị POS. Giá trị POS có thể là giá trị mã dịch vụ cho hệ thống thẻ để xử lý dịch vụ kết hợp và có thể được cấp trên vùng xác định của thẻ mềm (chẳng hạn, vùng 2 rãnh).

Theo một phương án, vùng của thẻ thực mà giá trị POS được cấp ở đó có thể bao gồm số thẻ, hạn sử dụng, mã dịch vụ (mã kiểm tra thẻ (CVC)), RPU, và tương tự, hoặc có thể bao gồm số thẻ ảo, mã thẻ, hạn sử dụng, mã dịch vụ (a CVC), và giá trị kiểm tra.

Đầu cuối thương mại 200 có thể nhận ra thông tin nhận dạng tương ứng với số thẻ ảo từ đầu cuối người dùng 100.

Ví dụ, đầu cuối thương mại 200 có thể nhận ra thông tin nhận dạng, như mã vạch, mã QR và tương tự, được hiển thị trên đầu cuối người dùng 100, và có thể nhận ra thông tin nhận dạng, như thẻ NFC, qua NFC khi đầu cuối người dùng 100 được đặt trong phạm vi định trước của đầu cuối thương mại 200.

Đầu cuối thương mại 200 có thể gửi tới máy chủ kiểm chứng mã thẻ 400, yêu cầu xác thực bao gồm thông tin nhận dạng nhận ra từ đầu cuối người dùng 100. Trong trường hợp này, đầu cuối thương mại 200 có thể gửi yêu cầu xác thực tới máy chủ kiểm chứng mã thẻ 400 sao cho việc thanh toán được thực hiện bằng phương pháp thanh toán đăng ký trước tương ứng với thông tin nhận dạng.

Máy chủ tạo mã thẻ 300 có thể tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại như điểm bắt đầu. Trong trường hợp này, máy chủ tạo mã thẻ 300 có thể tạo ra giá trị kiểm tra khi việc xác thực người dùng được hoàn thành ở đầu cuối người dùng 100.

Theo một phương án, giá trị kiểm tra là giá trị hàm băm tạo ra bằng cách mã hóa và băm mỗi lần số thẻ được tạo ra hoặc việc xác thực được yêu cầu để xác minh hiệu lực thanh toán, và được sử dụng cho máy chủ kiểm chứng mã thẻ 400 kiểm tra xem mã thẻ có được cấp bình thường hay không.

Ngoài ra, chiều dài của giá trị kiểm tra có thể được chọn nhỏ hơn lượng số định trước. Trong trường hợp này, số lượng ở vị trí mà không ở vị trí định trước có thể không được sử dụng. Ví dụ, khi chỉ năm số đầu tiên của giá trị kiểm tra được chọn để được sử dụng và giá trị kiểm tra bao gồm tám số, năm số đầu tiên này được sử dụng và ba số sau không được sử dụng.

Trong bản mô tả này, quá trình tạo ra giá trị kiểm tra sẽ được mô tả dưới giả định rằng máy chủ tạo mã thẻ 300 được nối với máy chủ thanh toán 500. Tuy nhiên, sáng chế không bị giới hạn ở đó. Ví dụ, máy chủ tạo mã thẻ 300 có thể được chứa trong máy chủ thanh toán khiến cho máy chủ thanh toán 500 có thể dùng như máy chủ tạo mã thẻ 300.

Trước hết, máy chủ tạo mã thẻ 300 có thể thu được khóa chính từ máy chủ thanh toán 500, mà quản lý thông tin về phương tiện thanh toán (ví dụ, thẻ) được cấp trước cho người dùng. Trong trường hợp này, máy chủ thanh toán 500 có thể tạo ra và quản lý các khóa chính theo các người dùng được đăng ký trước là thành viên để sử dụng phương tiện thanh toán này. Ví dụ, máy chủ thanh toán 500 là máy chủ công ty thẻ, và máy chủ công ty thẻ có thể tạo ra và quản lý các khóa chính theo các người sử dụng được đăng ký là thành viên sử dụng mã thẻ.

Theo một phương án, khóa chính có thể là khóa duy nhất phù hợp với số nhận dạng (nghĩa là, số thẻ) của phương tiện thanh toán cấp cho người dùng, và có thể được sử dụng trong quá trình mã hóa khi tạo ra giá trị kiểm tra.

Máy chủ tạo mã thẻ 300 có thể tạo ra khóa thẻ sử dụng khóa chính. Khóa thẻ có thể được sử dụng để xác minh các thẻ riêng biệt hoặc để xác thực các người dùng.

Máy chủ tạo mã thẻ 300 có thể tạo ra khóa thời gian giao dịch sử dụng khóa thẻ. Trong trường hợp này, máy chủ tạo mã thẻ 300 có thể tạo ra khóa thời gian giao dịch bằng cách sử dụng phút và dữ liệu bổ sung và bằng cách sử dụng số phút theo lịch Giu-liêng.

Theo một phương án, số phút theo lịch Giu-liêng là phần mở rộng của ngày theo lịch Giu-liêng tính theo phút. Ngày theo lịch Giu-liêng biểu thị số ngày trôi qua từ khi bắt đầu năm định trước. Ví dụ, ngày theo lịch Giu-liêng cho ngày 15 tháng 1 năm 2015 có thể là "15."

Nghĩa là, số phút theo lịch Giu-liêng được xem như số phút trôi qua từ khi bắt đầu năm định trước. Ví dụ, số phút theo lịch Giu-liêng cho ngày 15 tháng 1 năm 2015 có thể là giá trị "21600", được tính bằng cách nhân 15 tương ứng với mười lăm ngày, 24 tương ứng với hai mươi bốn giờ, và 60 tương ứng với sáu mươi phút.

Máy chủ tạo mã thẻ 300 có thể tạo ra khóa thời gian giao dịch, mà là khóa duy nhất, sử dụng số phút theo lịch Giu-liêng phút dựa trên thời gian hiện tại tại đó việc xác

thực người dùng được hoàn thành, và có thể tạo ra giá trị kiểm tra sử dụng khóa thời gian giao dịch đã tạo. Nghĩa là, máy chủ tạo mã thẻ 300 có thể tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại như điểm bắt đầu.

Máy chủ tạo mã thẻ 300 có thể tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ và cấp số thẻ ảo đã tạo tới đầu cuối người dùng 100.

Theo một phương án, mã thẻ, dưới dạng số thẻ ảo được chỉ định sử dụng trong dịch vụ thanh toán, có thể là mã thẻ sử dụng một lần có sẵn cho sử dụng trước khi hạn sử dụng mã thẻ định trước hết hạn, và hạn sử dụng mã thẻ có thể được tạo trong dạng YYMM sử dụng bốn số từ 0 tới 4 phụ thuộc vào chiều dài của mã thẻ được hỗ trợ. Ví dụ, số thẻ ảo có thể gồm có hai mươi mốt số bao gồm mười sáu số cho mã thẻ và năm số cho giá trị kiểm tra. Tuy nhiên, dạng số thẻ ảo không bị giới hạn ở đó. Số thẻ ảo có thể gồm có các dạng khác nhau.

Máy chủ kiểm chứng mã thẻ 400 có thể tiếp nhận yêu cầu xác thực từ đầu cuối thương mại 200 và có thể tạo ra giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tạo mã thẻ như điểm bắt đầu.

Khi tạo lại giá trị kiểm tra, máy chủ kiểm chứng mã thẻ 400 có thể tạo lại giá trị kiểm tra qua quá trình tạo ra khóa thời gian giao dịch, mà là khóa duy nhất, bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian tại đó số thẻ ảo được tạo ra bởi máy chủ tạo mã thẻ 300, như được mô tả nêu trên.

Máy chủ kiểm chứng mã thẻ 400 có thể thực hiện việc xác thực trên mã thẻ bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo, nghĩa là, với giá trị kiểm tra tạo ra bởi máy chủ tạo mã thẻ 300. Trong trường hợp này, giá trị kiểm tra tạo ra bởi máy chủ tạo mã thẻ 300 và giá trị kiểm tra tạo ra bởi máy chủ kiểm chứng mã thẻ 400 có thể đồng nhất hoặc tương ứng với nhau. Máy chủ kiểm chứng mã thẻ 400 hoàn thành việc xác thực mã thẻ bằng cách so sánh các giá trị kiểm tra, khi xác định được rằng các giá trị kiểm tra đồng nhất hoặc tương ứng với nhau như kết quả so sánh.

Ví dụ, có thể giả sử rằng khi hạn sử dụng được đặt bằng 3 phút trong số thẻ ảo, máy chủ tạo mã thẻ 300 tạo ra giá trị kiểm tra thứ nhất dựa trên thời gian hiện tại là 10:05, và cấp số thẻ ảo bao gồm số kiểm tra thứ nhất và mã thẻ, và máy chủ kiểm chứng mã thẻ 400 tiếp nhận yêu cầu xác thực từ đầu cuối thương mại 200 ở 10:08.

Trước hết, máy chủ kiểm chứng mã thẻ 400 có thể tạo ra giá trị kiểm tra thứ hai dựa trên 10:07, mà nằm trong hạn sử dụng 3 phút từ 10:05, và so sánh giá trị kiểm tra thứ nhất với giá trị kiểm tra thứ hai này. Trong trường hợp này, do giá trị kiểm tra thứ nhất được tạo ra dựa trên 10:05 và giá trị kiểm tra thứ hai được tạo ra dựa trên 10:07, nên các giá trị kiểm tra thứ nhất và thứ hai có thể được xác định là không trùng với nhau như kết quả so sánh.

Sau đó, máy chủ kiểm chứng mã thẻ 400 có thể tạo ra giá trị kiểm tra thứ hai dựa trên 10:06, mà sớm hơn một phút so với 10:07, và so sánh giá trị kiểm tra thứ nhất với giá trị kiểm tra thứ hai. Ngay cả trong trường hợp này, các giá trị kiểm tra thứ nhất và thứ hai có thể được xác định là không trùng nhau như kết quả so sánh.

Sau đó, máy chủ kiểm chứng mã thẻ 400 có thể tạo ra giá trị kiểm tra thứ hai dựa trên 10:05, mà sớm hơn một phút so với 10:06, và so sánh giá trị kiểm tra thứ nhất với giá trị kiểm tra thứ hai. Trong trường hợp này, do cả giá trị kiểm tra thứ nhất lẫn thứ hai được tạo ra dựa trên 10:05, các giá trị kiểm tra thứ nhất và thứ hai có thể được xác định là trùng nhau như kết quả so sánh. Nhờ đó, việc xác thực mã thẻ được hoàn thành.

Nghĩa là, máy chủ kiểm chứng mã thẻ 400 liên tục tạo ra giá trị kiểm tra dựa trên thời gian đưa ra trước một phút bắt đầu ở thời gian khi yêu cầu xác thực được tiếp nhận cho đến khi hạn sử dụng, được đặt trong số thẻ ảo, hết, và xác thực mã thẻ bằng cách so sánh các giá trị kiểm tra.

Nhờ đó, trong việc tạo số thẻ ảo bao gồm mã thẻ và việc xác thực mã thẻ, việc tạo ra giá trị kiểm tra là có thể chỉ khi biết dữ liệu cơ sở và thuật toán khiến cho việc tạo và xác thực không cần phải được thực hiện bởi một đối tượng. Do đó, việc tách giữa máy chủ tạo mã thẻ 300 và máy chủ kiểm chứng mã thẻ 400, như thể hiện trên Fig.5, là có thể. Tuy nhiên, sáng chế không bị giới hạn ở đó, và máy chủ tạo mã thẻ 300 và máy chủ kiểm chứng mã thẻ 400 có thể được lắp đặt trong một máy chủ hợp nhất.

Khi việc xác thực mã thẻ được hoàn thành, máy chủ kiểm chứng mã thẻ 400 có thể gửi yêu cầu thanh toán tới máy chủ thanh toán 500. Trong trường hợp này, máy chủ kiểm chứng mã thẻ 400 có thể sử dụng thông tin nhận dạng chứa trong yêu cầu xác thực tiếp nhận từ đầu cuối thương mại 200 để xác định mã thẻ chứa trong số thẻ ảo tương ứng với thông tin nhận dạng, và có thể gửi yêu cầu thanh toán bao gồm mã thẻ tới máy chủ thanh toán 500.

Máy chủ thanh toán 500 có thể tiếp nhận yêu cầu thanh toán bao gồm mã thẻ từ máy chủ kiểm chứng mã thẻ 400 mà hoàn thành việc xác thực mã thẻ, kiểm tra phương tiện thanh toán phù hợp với mã thẻ, và thực hiện thanh toán sử dụng phương tiện thanh toán.

Khi việc thanh toán được hoàn thành, máy chủ thanh toán 500 có thể gửi các chi tiết của việc thanh toán hoàn thành tới đầu cuối người dùng 100 hoặc đầu cuối thương mại 200.

Fig.2 là hình vẽ thể hiện quá trình tiến hành thanh toán qua việc xác thực mã thẻ theo một phương án; và

Fig.2 thể hiện quá trình hoạt động của mỗi một trong số máy chủ tạo mã thẻ 300 và máy chủ kiểm chứng mã thẻ 400, nhưng sáng chế không bị giới hạn ở đó. Máy chủ tạo mã thẻ 300 và máy chủ kiểm chứng mã thẻ 400 có thể được lắp đặt trong một máy chủ hợp nhất để thực hiện hoạt động của nó, hoặc cả máy chủ tạo mã thẻ 300 và máy chủ kiểm chứng mã thẻ 400 có thể được chứa trong máy chủ thanh toán 500 sao cho tất cả các hoạt động được thực hiện trong máy chủ thanh toán 500.

Trước hết, trong bước S201, đầu cuối người dùng 100 có thể thực hiện việc xác thực người dùng sử dụng phương pháp xác thực cá nhân, như SMS, giấy chứng nhận, mật khẩu thanh toán, hoặc tương tự.

Trong bước S202, đầu cuối người dùng 100 có thể gửi tới máy chủ tạo mã thẻ 300 thông tin về việc xác thực người dùng đã hoàn thành để thông báo cho máy chủ tạo mã thẻ 300 rằng việc xác thực người dùng được hoàn thành. Khi đầu cuối người dùng 100 thực hiện việc xác thực người dùng sử dụng mật khẩu thanh toán và tương tự qua máy chủ thanh toán 500 trong bước S201, máy chủ tạo mã thẻ 300 có thể tiếp nhận thông tin về việc xác thực người dùng đã hoàn thành từ máy chủ thanh toán 500.

Máy chủ tạo mã thẻ 300 có thể xác định rằng việc xác thực người dùng được hoàn thành trong đầu cuối người dùng 100 sử dụng thông tin về việc xác thực người dùng đã hoàn thành tiếp nhận trong bước S202.

Trong bước S203, máy chủ tạo mã thẻ 300 có thể tạo ra khóa thời gian giao dịch dựa trên thời gian hiện tại, nghĩa là, khóa duy nhất có thời gian hiện tại là điểm bắt đầu,

tạo ra giá trị kiểm tra sử dụng khóa thời gian giao dịch, thông tin người dùng, hoặc thông tin thanh toán, và tạo ra số thẻ ảo bao gồm mã thẻ và giá trị kiểm tra.

Ví dụ, máy chủ tạo mã thẻ 300 có thể tạo ra số thẻ ảo 21 số bao gồm mã thẻ 16 số tương ứng với số thẻ thực cấp cho người dùng và giá trị kiểm tra 5 số tạo ra dựa trên thời gian hiện tại.

Máy chủ tạo mã thẻ 300 có thể sử dụng giá trị kiểu mã hóa, giá trị phân loại giao dịch, số tài khoản chính (PAN), hạn sử dụng của PAN, khóa dẫn xuất chính (MD), và tương tự khi tạo ra số thẻ ảo.

Theo một phương án, giá trị kiểu mã hóa có thể xem là giá trị biểu thị sự mã hóa cho việc tạo ra giá trị kiểm tra và việc xác thực dịch vụ thanh toán và biểu thị kiểu và chiều dài của dữ liệu được sử dụng, và giá trị kiểu mã hóa này biểu thị định dạng mã hóa hiệu quả nhất theo môi trường trong đó số thẻ ảo được cấp và được phân loại thành các kiểu.

Theo một phương án, giá trị phân loại giao dịch là giá trị mã để phân loại các kiểu giao dịch của dịch vụ thanh toán, và giá trị mã được ấn định bổ sung vào mỗi phương pháp thanh toán.

Theo một phương án, PAN là số thẻ thực mà phù hợp với mã thẻ, và hạn sử dụng của PAN là hạn sử dụng của thẻ đặt trong thẻ thực theo dạng YYMM. Khóa MD là khóa MD mà có thể được chứa trong bộ nhớ tốc độ cao (HSM).

Trong bước S204, máy chủ tạo mã thẻ 300 có thể cấp và truyền số thẻ ảo tạo ra trong bước S203 tới đầu cuối người dùng 100.

Trong bước S205, đầu cuối người dùng 100 có thể sử dụng số thẻ ảo cấp bởi máy chủ tạo mã thẻ 300 để tạo ra thông tin nhận dạng tương ứng với số thẻ ảo. Nghĩa là, đầu cuối người dùng 100 có thể tạo ra thông tin nhận dạng tương ứng với số thẻ ảo sao cho thông tin nhận dạng có thể được sử dụng với các phương pháp thanh toán khác nhau, như âm thanh, ký tự, mã vạch, mã QR, NFC, và tương tự.

Trong bước S206, đầu cuối người dùng 100 có thể gửi thông tin nhận dạng tới đầu cuối thương mại 200, và đầu cuối thương mại 200 có thể nhận ra thông tin nhận dạng này.

Một cách chi tiết, khi đầu cuối người dùng 100 trực tiếp gửi thông tin nhận dạng tới đầu cuối thương mại 200, như thẻ NFC và tương tự, sử dụng truyền thông không dây

phạm vi ngắn, đầu cuối thương mại 200 có thể nhận ra thông tin nhận dạng này, và khi đầu cuối người dùng 100 hiển thị thông tin nhận dạng, như mã vạch, mã QR, và tương tự, trên màn hình, đầu cuối thương mại 200 có thể nhận ra thông tin nhận dạng bằng cách sử dụng bộ đọc nối với đầu cuối thương mại 200.

Trong bước S207, đầu cuối thương mại 200 có thể gửi tới máy chủ kiểm chứng mã thẻ 400, yêu cầu xác thực bao gồm thông tin nhận dạng nhận ra từ đầu cuối người dùng 100. Trong trường hợp này, đầu cuối thương mại 200 có thể gửi yêu cầu xác thực tới máy chủ kiểm chứng mã thẻ 400 qua mạng bổ sung giá trị (VAN) hoặc kế hoạch chấp nhận trực tiếp.

Trong bước S208, máy chủ kiểm chứng mã thẻ 400 có thể tạo ra khóa duy nhất có thời gian tạo là điểm bắt đầu dựa trên thời gian tạo tại đó số thẻ ảo được tạo ra trong bước S203, và có thể tạo lại giá trị kiểm tra bằng cách sử dụng khóa duy nhất đã tạo.

Sau đó, máy chủ kiểm chứng mã thẻ 400 kiểm tra số thẻ ảo tương ứng với thông tin nhận dạng chứa trong yêu cầu xác thực tiếp nhận trong bước S207, và thực hiện việc xác thực mã thẻ bằng cách so sánh giá trị kiểm tra chứa trong số thẻ ảo với ảo giá trị đã tạo lại. Trong trường hợp này, khi các giá trị ảo trùng với nhau, việc xác thực mã thẻ được hoàn thành và việc giao dịch để thanh toán được cho phép.

Theo một phương án, dữ liệu sử dụng để xác thực mã thẻ có thể là mã thẻ, hạn sử dụng mã thẻ, số phút theo lịch Giu-liêng, giá trị kiểm tra, giá trị POS, giá trị kiểu mã hóa, giá trị phân loại giao dịch, và dữ liệu tương tự.

Trong bước S209, khi việc xác thực mã thẻ được hoàn thành, máy chủ kiểm chứng mã thẻ 400 được tạo kết cấu để gửi yêu cầu thanh toán bao gồm mã thẻ tiếp nhận trong bước S207 tới máy chủ thanh toán 500.

Trong bước S210, máy chủ thanh toán 500 có thể kiểm tra mã thẻ chứa trong yêu cầu thanh toán theo yêu cầu thanh toán tiếp nhận trong bước S209, và thực hiện việc thanh toán bằng phương tiện thanh toán mà phù hợp với mã thẻ này.

Sau đó, máy chủ thanh toán 500 có thể gửi các chi tiết của việc thanh toán hoàn thành tới đầu cuối người dùng 100 hoặc đầu cuối thương mại 200.

Fig.3 là hình vẽ thể hiện quá trình thực hiện việc thanh toán nhờ xác thực mã thẻ theo một phương án khác.

Như được thể hiện trên Fig.3, quá trình tạo số thẻ ảo trong đầu cuối người dùng 100 được thể hiện. Các chi tiết của phần mô tả giống với phần mô tả trên Fig.2 sẽ được bỏ qua.

Trước hết, trong bước S301, đầu cuối người dùng 100 có thể thực hiện việc xác thực người dùng, như trong bước S201.

Khi đầu cuối người dùng 100 được trang bị bộ nhớ mã thẻ an toàn đảm bảo sự an toàn hoặc đầu cuối người dùng 100 được nối với bộ nhớ mã thẻ, máy chủ tạo mã thẻ 300 không trực tiếp tạo ra số thẻ ảo mà thực hiện quá trình yêu cầu rằng mã thẻ được cấp ngay khi việc xác thực người dùng được hoàn thành. Ví dụ, máy chủ tạo mã thẻ 300 có thể gửi thông tin tạo khóa tới đầu cuối người dùng 100, mà là dữ liệu cơ sở cần để tạo ra khóa.

Trong bước S302, đầu cuối người dùng 100 có thể thực hiện hoạt động tương tự với hoạt động của máy chủ tạo mã thẻ 300 thực hiện trong bước S203, nghĩa là, hoạt động tạo khóa duy nhất bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại, tạo ra giá trị kiểm tra sử dụng khóa duy nhất đã tạo, tạo ra số thẻ ảo bao gồm giá trị kiểm tra và mã thẻ, và cấp số thẻ ảo đã tạo tới bộ nhớ mã thẻ.

Khi tạo ra số thẻ ảo, đầu cuối người dùng 100 có thể tự tạo ra giá trị kiểm tra nhờ sử dụng thông tin tạo khóa tiếp nhận trước từ máy chủ tạo mã thẻ 300. Nhờ đó, đầu cuối người dùng 100 không cần phải tiếp nhận giá trị kiểm tra tạo ra bởi máy chủ tạo mã thẻ 300 ở mọi thời gian việc giao dịch được yêu cầu, nhờ đó cho phép số thẻ ảo được tạo ra ngay cả khi đầu cuối người dùng 100 ở trạng thái ngoại tuyến.

Trong bước S303, đầu cuối người dùng 100 có thể tạo ra thông tin nhận dạng tương ứng với số thẻ ảo, như trong bước S205.

Trong bước S304, đầu cuối người dùng 100 có thể gửi thông tin nhận dạng tới đầu cuối thương mại 200, như trong bước S206.

Trong bước S305, đầu cuối thương mại 200 có thể gửi yêu cầu xác thực bao gồm thông tin nhận dạng tới máy chủ kiểm chứng mã thẻ 400, như trong bước S207.

Trong bước S306, máy chủ kiểm chứng mã thẻ 400 có thể thực hiện việc xác thực trên mã thẻ, như trong bước S208.

Trong bước S307, máy chủ kiểm chứng mã thẻ 400 có thể gửi yêu cầu thanh toán tới máy chủ thanh toán 500, như trong bước S209.

Trong bước S308, máy chủ thanh toán 500 có thể thực hiện thanh toán theo yêu cầu thanh toán, như trong bước S210.

Phần mô tả sáng chế nêu trên chỉ nhằm mục đích minh họa, và người có hiểu biết trung bình trong lĩnh vực kỹ thuật này sẽ hiểu rằng các biến thể khác có thể được thực hiện một cách dễ dàng mà không nằm ngoài phạm vi của sáng chế. Do đó, các phương án nêu trên chỉ nhằm mục đích minh họa chứ không giới hạn phạm vi của sáng chế. Ví dụ, các chi tiết cấu thành mà đã được mô tả dưới dạng một cụm có thể được sử dụng trong dạng tách biệt và các chi tiết cấu thành đã được mô tả dưới dạng tách biệt có thể được sử dụng trong dạng kết hợp. Phạm vi của sáng chế không được xác định bởi phần mô tả chi tiết nêu trên được xác định bởi các yêu cầu bảo hộ kèm theo của sáng chế. Cần hiểu rằng tất cả các thay đổi hoặc các biến thể thu được từ phạm vi của các điểm yêu cầu bảo hộ và các phần tương đương của chúng sẽ nằm trong phạm vi của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xác thực mã thẻ sử dụng giá trị kiểm tra tạo ra dựa trên thời gian hiện tại trong hệ thống xác thực mã thẻ, phương pháp xác thực mã thẻ này bao gồm các bước:

tạo ra, bằng máy chủ tạo mã thẻ, giá trị kiểm tra để kiểm tra xem liệu mã thẻ có được cấp theo cách thông thường hay không bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ phù hợp với phương tiện thanh toán, và cấp số thẻ ảo đã tạo tới đầu cuối người dùng;

tiếp nhận, bằng máy chủ kiểm chứng mã thẻ, yêu cầu xác thực bao gồm thông tin nhận dạng tương ứng với số thẻ ảo qua đầu cuối thương mại mà nhận ra thông tin nhận dạng từ đầu cuối người dùng;

tạo lại, bằng máy chủ kiểm chứng mã thẻ, giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và

khi việc xác thực mã thẻ được hoàn thành, truyền, bằng máy chủ kiểm chứng mã thẻ, yêu cầu thanh toán bao gồm mã thẻ tới máy chủ thanh toán khiến cho việc thanh toán được thực hiện bằng phương tiện thanh toán phù hợp với mã thẻ.

2. Phương pháp xác thực mã thẻ theo điểm 1, trong đó việc cấp số thẻ ảo bao gồm, tạo ra, bằng máy chủ tạo mã thẻ, khóa duy nhất bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

3. Phương pháp xác thực mã thẻ sử dụng giá trị kiểm tra tạo ra dựa trên thời gian hiện tại trong hệ thống xác thực mã thẻ, phương pháp xác thực mã thẻ này bao gồm các bước:

tiếp nhận, bằng đầu cuối người dùng, thông tin tạo khóa từ máy chủ tạo mã thẻ, tạo ra giá trị kiểm tra để kiểm tra xem liệu mã thẻ có được cấp theo cách thông thường hay không bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại từ thông tin tạo khóa, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ phù hợp với phương tiện thanh toán, và cấp số thẻ ảo đã tạo tới bộ nhớ mã thẻ nối với đầu cuối người dùng;

tiếp nhận, bằng máy chủ kiểm chứng mã thẻ, yêu cầu xác thực bao gồm thông tin nhận dạng tương ứng với số thẻ ảo qua đầu cuối thương mại mà nhận ra thông tin nhận dạng từ đầu cuối người dùng;

tạo lại, bằng máy chủ kiểm chứng mã thẻ, giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và

khi việc xác thực mã thẻ được hoàn thành, truyền, bằng máy chủ kiểm chứng mã thẻ, yêu cầu thanh toán bao gồm mã thẻ tới máy chủ thanh toán khiến cho việc thanh toán được thực hiện bằng phương tiện thanh toán phù hợp với mã thẻ.

4. Phương pháp xác thực mã thẻ theo điểm 3, trong đó việc cấp số thẻ ảo bao gồm, tạo ra, bằng đầu cuối người dùng, khóa duy nhất bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

5. Hệ thống xác thực mã thẻ bao gồm:

máy chủ tạo mã thẻ được tạo kết cấu để tạo ra giá trị kiểm tra để kiểm tra xem liệu mã thẻ có được cấp theo cách thông thường hay không bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ phù hợp với phương tiện thanh toán, và cấp số thẻ ảo đã tạo tới đầu cuối người dùng;

đầu cuối thương mại được tạo kết cấu để nhận ra thông tin nhận dạng tương ứng với số thẻ ảo từ đầu cuối người dùng;

máy chủ kiểm chứng mã thẻ được tạo kết cấu để tiếp nhận yêu cầu xác thực bao gồm thông tin nhận dạng dã nhận ra qua đầu cuối thương mại, tạo lại giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra, và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và

máy chủ thanh toán được tạo kết cấu để, khi việc xác thực mã thẻ được hoàn thành, tiếp nhận yêu cầu thanh toán bao gồm mã thẻ từ máy chủ xác thực mã thẻ và thực hiện việc thanh toán bằng phương tiện thanh toán phù hợp với mã thẻ này.

6. Hệ thống xác thực mã thẻ theo điểm 5, trong đó khóa duy nhất được tạo ra bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

7. Hệ thống xác thực mã thẻ bao gồm:

đầu cuối người dùng được tạo kết cấu để tiếp nhận thông tin tạo khóa từ máy chủ tạo mã thẻ, tạo ra giá trị kiểm tra để kiểm tra xem liệu mã thẻ có được cấp theo cách thông thường hay không bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian hiện tại từ thông tin tạo khóa, tạo ra số thẻ ảo bao gồm giá trị kiểm tra đã tạo ra và mã thẻ phù hợp với phương tiện thanh toán, và cấp số thẻ ảo đã tạo tới bộ nhớ mã thẻ;

đầu cuối thương mại được tạo kết cấu để nhận ra thông tin nhận dạng tương ứng với số thẻ ảo từ đầu cuối người dùng;

máy chủ kiểm chứng mã thẻ được tạo kết cấu để tiếp nhận yêu cầu xác thực bao gồm thông tin nhận dạng dã nhận ra qua đầu cuối thương mại, tạo lại giá trị kiểm tra bằng cách sử dụng khóa duy nhất tạo ra dựa trên thời gian tại đó số thẻ ảo được tạo ra, và xác thực mã thẻ chứa trong số thẻ ảo bằng cách so sánh giá trị kiểm tra tạo lại với giá trị kiểm tra chứa trong số thẻ ảo tương ứng với thông tin đã xác định; và

máy chủ thanh toán được tạo kết cấu để, khi việc xác thực mã thẻ được hoàn thành, tiếp nhận yêu cầu thanh toán bao gồm mã thẻ từ máy chủ xác thực mã thẻ và thực hiện việc thanh toán bằng phương tiện thanh toán phù hợp với mã thẻ này.

8. Hệ thống xác thực mã thẻ theo điểm 7, trong đó khóa duy nhất được tạo ra bằng cách sử dụng số phút theo lịch Giu-liêng dựa trên thời gian hiện tại.

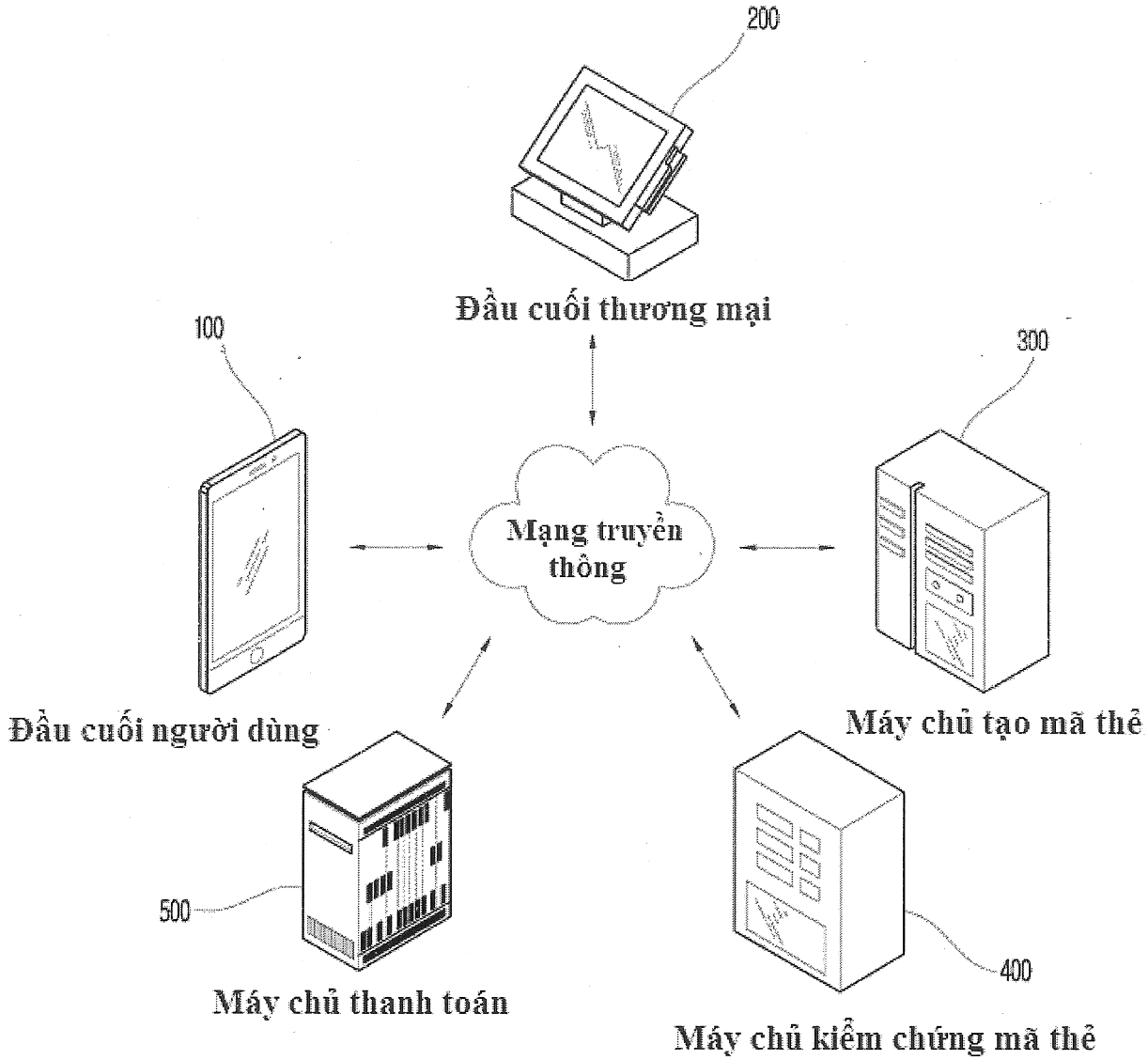

200
Đầu cuối thương mại
100
300
Mạng truyền thông
Đầu cuối người dùng
Máy chủ tạo mã thẻ
500
400
Máy chủ thanh toán
Máy chủ kiểm chứng mã thẻ

Fig.1

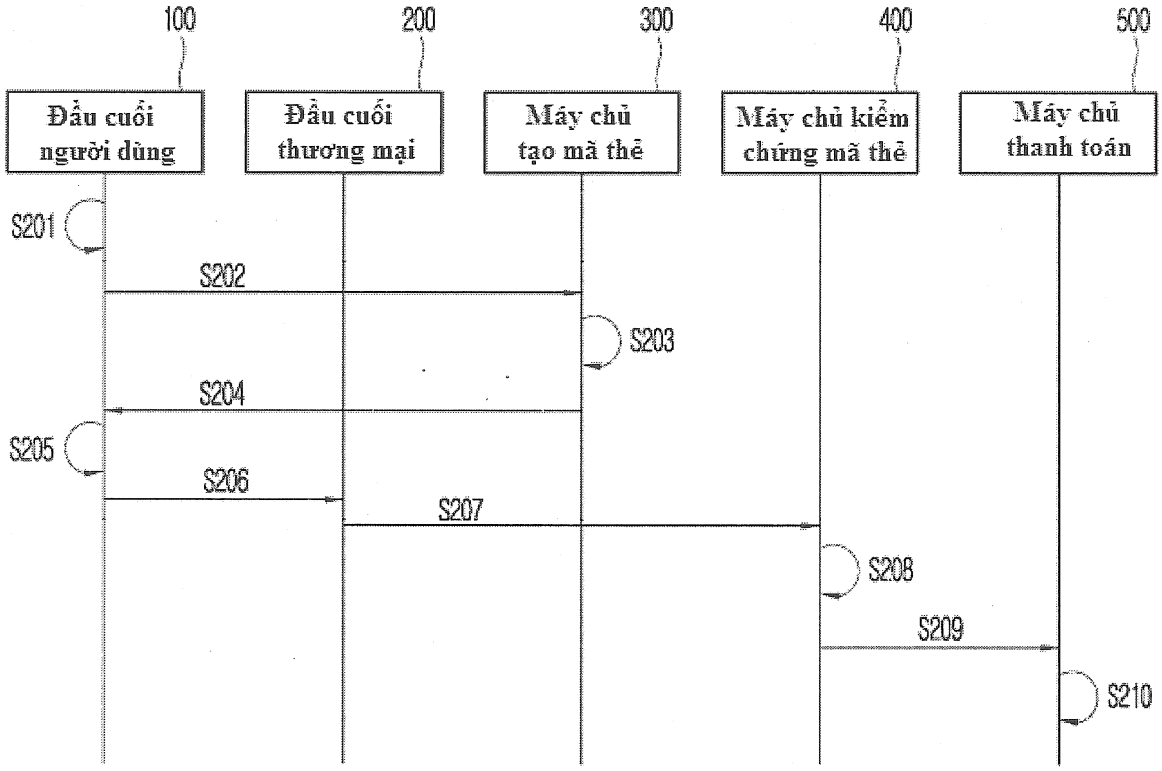

100
200
300
400
500
Đầu cuối người dùng
Đầu cuối thương mại
Máy chủ tạo mã thẻ
Máy chủ kiểm chứng mã thẻ
Máy chủ thanh toán
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210

Fig.2

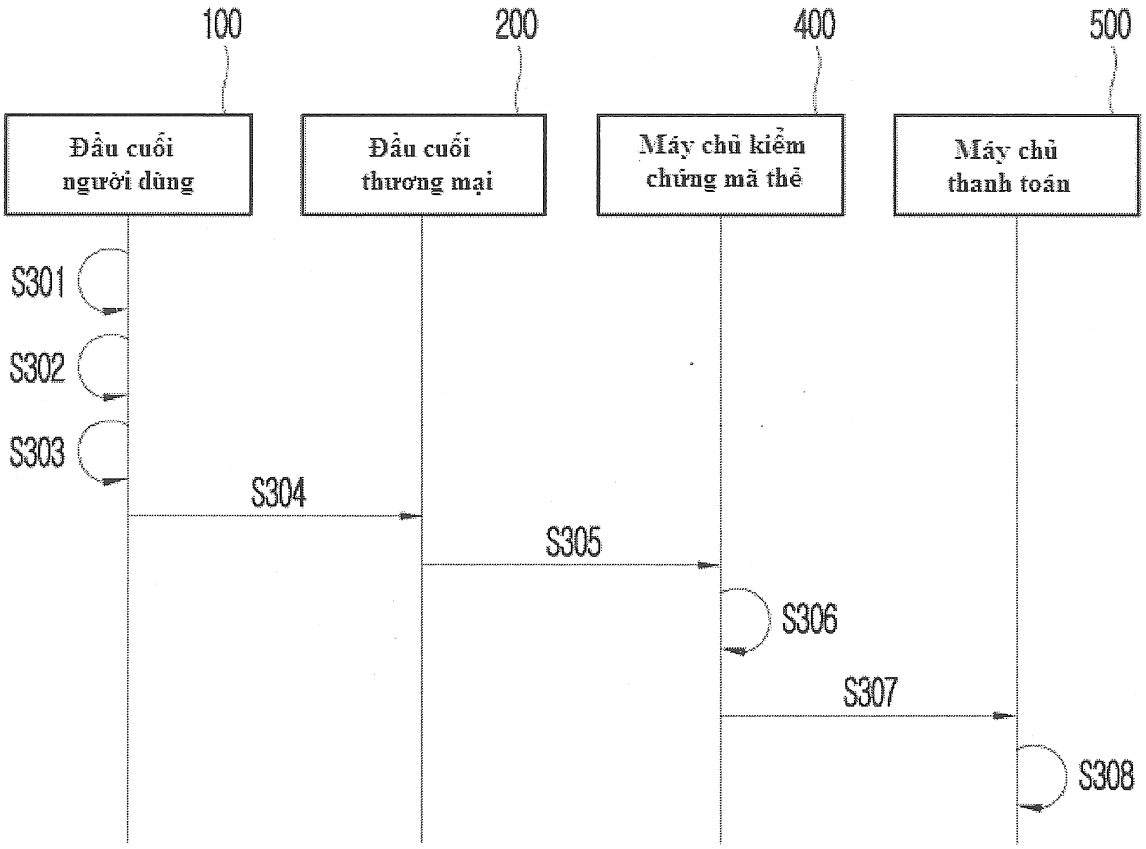

100
200
400
500
Đầu cuối người dùng
Đầu cuối thương mại
Máy chủ kiểm chứng mã thẻ
Máy chủ thanh toán
S301
S302
S303
S304
S305
S306
S307
S308

Fig.3