(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) **1-0043555**

(51)[2019.01] **G06F 21/32**; H04L 29/06; G06K 9/00; H04L 12/58; G06F 21/44; G06F 21/45

(13) **B**

(21) 1-2020-00963
(22) 22/08/2018
(86) PCT/KR2018/009667 22/08/2018
(87) WO2019/039865 28/02/2019
(30) 10-2017-0106614 23/08/2017 KR
(45) 25/02/2025 443
(43) 25/08/2020 389A
(76) YOON, Tae Sik (KR)
102-1104, 80, Eojeong-ro, Giheung-gu, Yongin-si, Gyeonggi-do 16994, Republic of Korea
(74) Công ty Luật TNHH quốc tế BMVN (BMVN INTERNATIONAL LLC)

(54) HỆ THỐNG XÁC THỰC VÀ PHƯƠNG PHÁP XÁC THỰC

(21) 1-2020-00963

(57) Sáng chế liên quan đến đầu cuối xác thực, thiết bị xác thực, phương pháp và hệ thống xác thực sử dụng đầu cuối xác thực này và thiết bị xác thực này, và cụ thể hơn là liên quan đến hệ thống và phương pháp xác thực người dùng và cho phép các giao dịch thông qua việc vận chuyển thông tin giữa đầu cuối người dùng, đầu cuối xác thực và thiết bị xác thực.

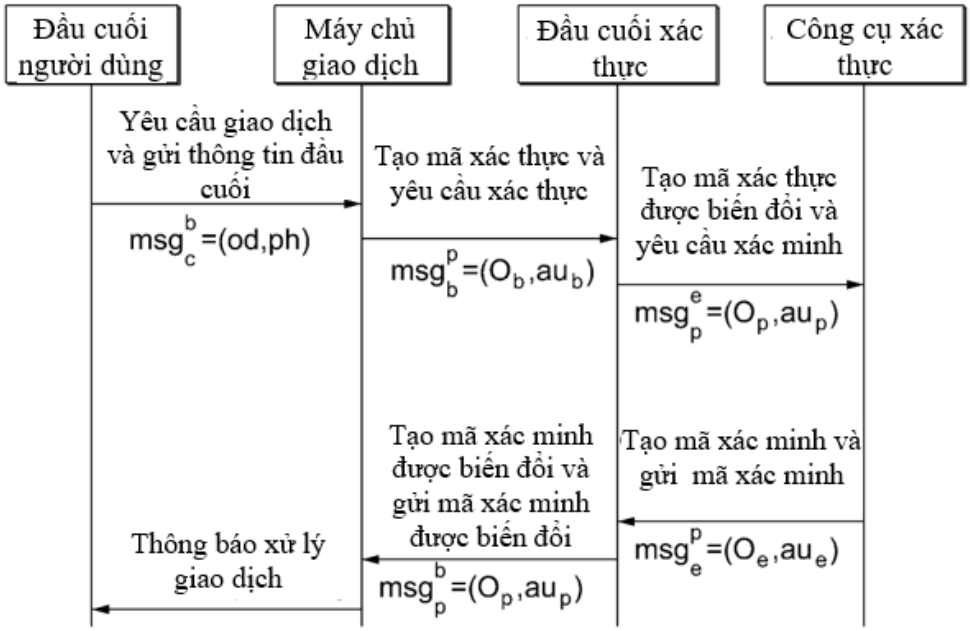

FIG. 6

Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến đầu cuối xác thực, thiết bị xác thực, và phương pháp và hệ thống xác thực sử dụng đầu cuối xác thực này và thiết bị xác thực này, và cụ thể hơn là đến thiết bị và phương pháp xác thực người dùng và cho phép các giao dịch thông qua vận chuyển thông tin trong số đầu cuối người dùng, đầu cuối xác thực và thiết bị xác thực.

Tình trạng kỹ thuật của sáng chế

Gần đây, đã phát triển các phương pháp dịch vụ giao dịch tài chính sử dụng thiết bị truyền thông không dây cá nhân xách tay, ví dụ như, phương pháp xác thực sử dụng thiết bị truyền thông không dây cá nhân xách tay, và việc sử dụng các thiết bị truyền thông không dây cá nhân xách tay đã tăng lên đáng kể do sự phát triển của công nghệ Internet không dây. Do đó, tầm quan trọng của an toàn và xác thực của các thiết bị truyền thông không dây cá nhân xách tay trở nên lớn hơn nhiều so với trường hợp sử dụng các thiết bị này để truyền thông đơn giản như trước kia.

Mặt khác, cho đến gần đây, phương pháp xác thực người dùng trong dịch vụ giao dịch tài chính xác nhận nhân dạng của người dùng khi người dùng này nhập ID và mật khẩu chính xác, nhờ đó cung cấp cho người dùng này các dịch vụ tài chính qua Internet. Tuy nhiên, độ tin cậy của phương pháp này tương đối thấp, nên các giao dịch tài chính chẳng hạn như chuyển khoản tiền bị hạn chế trong trường hợp này.

Do đó, nếu người dùng muốn sử dụng các dịch vụ giao dịch tài chính chẳng hạn như chuyển khoản tiền, cần có quy trình xác thực trong đó người dùng nhận được một chứng nhận người dùng, có thể là thẻ cư dân trên Internet, từ Công ty tài chính viễn thông và thanh toán bù trừ Hàn Quốc – Korea Financial Telecommunications and Clearings Institute (KFTC), đăng ký chứng nhận người dùng này trên trang web của một hãng dịch vụ tài chính, và nhập mật khẩu để ký số, nhờ đó kiểm tra nhân dạng này.

Tuy nhiên, quy trình xác thực thông thường được mô tả trên đây là phương pháp xác minh nhân dạng của người dùng bằng cách nhập mật khẩu của chứng nhận người dùng này vào, và do chứng nhận người dùng này có thể được sao chép từ môi trường chứa chứng nhận người dùng này, có khả năng bị đánh cắp cao nếu chỉ có mật khẩu này được nhập vào.

Do đó, các hãng tài chính sử dụng phương pháp làm giảm khả năng bị đánh cắp, tức là, cung cấp cho người dùng phương tiện xác thực bổ sung cho các dịch vụ quan trọng chẳng hạn như chuyển khoản tiền, ví dụ như, xác thực kép bao gồm nhập số thẻ an ninh hoặc số mật khẩu sử dụng một lần (one-time password - OTP) hoặc xác thực qua điện thoại sau khi người dùng này nhập mật khẩu tài khoản trên màn hình chuyển khoản tiền. Tuy nhiên, có vấn đề là trách nhiệm đối với việc rò rỉ thông tin liên quan đến xác thực được chuyển cho người dùng này. Ngoài ra, nếu thiết bị OTP bị mất, có thể xảy ra sự cố, và thông tin liên quan đến xác thực chẳng hạn như chứng nhận người dùng được lưu giữ trong thiết bị lưu trữ xách tay của người dùng hoặc đĩa cứng máy tính có nguy cơ cao bị đánh

cắp.

Ngoài ra, có vấn đề là người dùng này không được cung cấp quy trình xác thực nhanh, nên có thể tốn nhiều thời gian và gây ách tắc.

Theo sáng chế, để giải quyết các vấn đề nêu trên, thực hiện xác thực bằng cách sử dụng công nghệ mã hóa đường cong eliptic (elliptic curve cryptography - ECC). ECC là một trong các phương pháp mã hóa khóa công khai (public key cryptography) dựa vào lý thuyết đường cong eliptic, và phương pháp này có ưu điểm là tạo ra mức độ an toàn tương tự, trong khi sử dụng khóa ngắn hơn so với Rivest-Shamir-Adleman (RSA) hoặc Elgamal.

Dựa vào các ưu điểm này, ECC được sử dụng chủ yếu trong môi trường ràng buộc có lưu lượng truyền dẫn và tính toán hạn chế, chẳng hạn như môi trường không dây. Trong ECC, công nghệ mã hóa này được thiết kế chủ yếu dựa vào bài toán đại số rời rạc đường cong eliptic.

Hệ thống mã hóa sử dụng thuật toán ECC thực hiện trong dãy mà hệ thống này chia sẻ, với mỗi đầu cuối, khóa công khai thu được bằng cách kết hợp với số ngẫu nhiên và đồng bộ hóa mỗi đầu cuối này bằng khóa bí mật không thể bị kẻ tấn công can thiệp vào.

Để thực hiện hệ thống mã hóa này, cần phải cấu hình thuật toán phân bố khóa và thuật toán mã hóa tin nhắn. Ví dụ đại diện cho sơ đồ phân bố khóa dựa vào mã hóa đường cong eliptic là thuật toán Diffie-Hellman dựa trên đường cong eliptic (elliptic curve Diffie-Hellman - ECDH).

Bản chất kỹ thuật của sáng chế

Các khía cạnh của các phương án của sáng chế đề cập đến đầu cuối xác thực và thiết bị xác thực có thể giảm thiểu đáng kể nguy cơ lấy thông tin cá nhân hoặc thông tin liên quan đến xác thực bị đánh cắp, bằng cách sử dụng thuật toán Diffie-Hellman đường cong eliptic (elliptic curve Diffie-Hellman - ECDH) dựa vào thuật toán mã hóa đường cong eliptic (elliptic curve cryptography - ECC), và đề cập đến phương pháp xác thực và hệ thống xác thực sử dụng đầu cuối xác thực và thiết bị xác thực này.

Các khía cạnh của các phương án của sáng chế cũng đề cập đến đầu cuối xác thực và thiết bị xác thực có thể đảm bảo ổn định hơn so với máy chủ giao dịch ngay cả khi thông tin cá nhân bị lộ từ máy chủ xác thực, và đề cập đến phương pháp xác thực và hệ thống xác thực sử dụng đầu cuối xác thực và thiết bị xác thực này.

Các khía cạnh của các phương án của sáng chế cũng đề cập đến đầu cuối xác thực và thiết bị xác thực có thể trích xuất mức độ hoạt động của thay đổi cử động của các tuyến mồ hôi theo hình dạng các đường vân tay của người dùng để sử dụng mức độ hoạt động này làm phương tiện xác thực người dùng mà không thể bị trùng lặp và loại trừ sự rắc rối của quy trình xác thực này, và đề cập đến phương pháp xác thực và hệ thống xác thực sử dụng đầu cuối xác thực và thiết bị xác thực này.

Các khía cạnh của các phương án của sáng chế cũng đề cập đến phương pháp xác thực và hệ thống xác thực có thể khắc phục các điểm yếu trong quy trình xác thực thông thường trong đó có thể phỏng đoán ID hoặc mật khẩu của người dùng dựa vào thông tin cá nhân của người dùng này, các giá trị truyền thông hoặc các giá trị được lưu trữ trên máy

chủ này, có thể đảm bảo độ an toàn chống lại sự phỏng đoán tấn công vào các giá trị chính của thông tin nhận dạng cá nhân của người dùng, và có thể loại trừ rắc rối của các thủ tục xác thực, trong các quy trình xác thực người dùng trong các loại môi trường khác nhau chẳng hạn như hệ thống đám mây, hệ thống kiểm soát, Internet Vạn Vật (Internet of Things - IOT) và thẻ thông minh.

Theo một phương án, hệ thống xác thực bao gồm đầu cuối người dùng được tạo cấu hình để yêu cầu giao dịch bằng cách truyền thông tin người dùng; máy chủ giao dịch được tạo cấu hình để nhận yêu cầu giao dịch này, tạo ra mã xác thực, và yêu cầu xác thực đối với người dùng này; đầu cuối xác thực được tạo cấu hình để tạo ra mã xác thực được biến đổi dựa vào mã xác thực này, tạo ra mã xác minh được biến đổi dựa vào mã xác minh, và truyền mã xác minh được biến đổi này đến máy chủ giao dịch này; và công cụ xác thực được tạo cấu hình để nhận mã xác thực được biến đổi này để xác minh tính hợp pháp của đầu cuối xác thực này, tạo ra mã xác minh này, và truyền mã xác minh này đến đầu cuối xác thực này. Máy chủ giao dịch này xác thực giao dịch này bằng cách xác định xem liệu kết quả tính toán mã xác minh được biến đổi này có khớp với mã xác thực được tạo ra bởi máy chủ giao dịch này hay không.

Đầu cuối người dùng này có thể truyền tin nhắn bao gồm loại giao dịch và số điện thoại của người dùng này đến máy chủ giao dịch này.

Máy chủ giao dịch này có thể lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên này, tạo ra mã xác thực này bằng cách sử dụng thông tin người dùng này, và truyền khóa công khai được tạo ra này và mã xác thực này đến đầu cuối xác thực này.

Đầu cuối xác thực này có thể tạo ra mã xác thực bằng cách sử dụng thông tin người dùng này, và xác định xem liệu mã xác thực này có khớp với mã xác thực nhận được từ máy chủ giao dịch này hay không.

Đầu cuối xác thực này có thể lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên này, tạo ra mã xác thực được biến đổi này bằng cách sử dụng thông tin người dùng này, thông tin sinh trắc học, và mức độ hoạt động của người dùng này, và truyền khóa công khai được tạo ra này và mã xác thực được biến đổi này đến công cụ xác thực này.

Công cụ xác thực này có thể tạo ra mã xác thực bằng cách sử dụng thông tin người dùng này, thông tin sinh trắc học, và mức độ hoạt động của người dùng này, và xác định xem liệu mã xác thực này có khớp với mã xác thực nhận được từ đầu cuối xác thực này hay không.

Công cụ xác thực này có thể lưu trữ dấu vân tay thông thường và dấu vân tay khẩn cấp.

Công cụ xác thực này có thể lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên được chọn này, tạo ra khóa bí mật được chia sẻ bằng cách sử dụng số ngẫu nhiên này và khóa công khai này nhận được từ đầu cuối xác thực này, tạo ra mã xác minh bằng cách sử dụng khóa bí mật được chia sẻ này và thông tin người dùng này, và

truyền khóa công khai được tạo ra này và mã xác minh này đến đầu cuối xác thực này.

Đầu cuối xác thực này có thể tạo ra khóa bí mật được chia sẻ bằng cách sử dụng khóa công khai nhận được từ công cụ xác thực này và xác định xem liệu kết quả tính toán giữa khóa bí mật được chia sẻ được tạo ra này và mã xác minh nhận được từ công cụ xác thực này có khớp với mã xác minh được tạo ra bằng cách sử dụng thông tin người dùng này hay không.

Đầu cuối xác thực này có thể tạo ra khóa bí mật được chia sẻ bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi đầu cuối xác thực này và khóa công khai này nhận được từ máy chủ giao dịch này, tạo ra mã xác minh được biến đổi bằng cách sử dụng khóa bí mật được chia sẻ được tạo ra này, và truyền khóa công khai này và mã xác minh được biến đổi này được tạo ra bởi đầu cuối xác thực này đến máy chủ giao dịch này.

Máy chủ giao dịch này có thể tạo ra khóa bí mật được chia sẻ bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi máy chủ giao dịch này và khóa công khai này nhận được từ đầu cuối xác thực này, và xác định xem liệu kết quả tính toán giữa khóa bí mật được chia sẻ được tạo ra này và mã xác minh được biến đổi này nhận được từ đầu cuối xác thực này có khớp với mã xác minh được tạo ra bằng cách sử dụng thông tin người dùng này hay không.

Theo một phương án, phương pháp xác thực bao gồm đầu cuối người dùng yêu cầu giao dịch bằng cách truyền thông tin người dùng; máy chủ giao dịch nhận yêu cầu giao dịch này và tạo ra mã xác thực; đầu cuối xác thực xác minh tính hợp pháp của máy chủ giao dịch này và tạo ra mã xác thực được biến đổi dựa vào mã xác thực này; công cụ xác thực xác minh tính hợp pháp của đầu cuối xác thực này, tạo ra mã xác minh dựa vào mã xác thực được biến đổi này, và truyền mã xác minh này đến đầu cuối xác thực này; đầu cuối xác thực này tạo ra mã xác minh được biến đổi dựa vào mã xác minh này và truyền mã xác minh được biến đổi này đến máy chủ giao dịch này; và máy chủ giao dịch này xác thực giao dịch này bằng cách xác định xem liệu kết quả tính toán của mã xác minh được biến đổi này có khớp với mã xác thực được tạo ra bởi máy chủ giao dịch này hay không.

Đầu cuối người dùng này có thể truyền tin nhắn bao gồm loại giao dịch và số điện thoại của người dùng này đến máy chủ giao dịch này.

Máy chủ giao dịch này có thể lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên này, tạo ra mã xác thực này bằng cách sử dụng thông tin người dùng này, và truyền khóa công khai được tạo ra này và mã xác thực này đến đầu cuối xác thực này.

Đầu cuối xác thực này có thể tạo ra mã xác thực bằng cách sử dụng thông tin người dùng này, và xác định xem liệu mã xác thực này có khớp với mã xác thực nhận được từ máy chủ giao dịch này hay không.

Đầu cuối xác thực này có thể lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên này, tạo ra mã xác thực được biến đổi này bằng cách sử dụng thông tin người dùng này, thông tin sinh trắc học, và mức độ hoạt động của người dùng này, và truyền khóa công khai được tạo ra này và mã xác thực được biến đổi này đến công

cụ xác thực này.

Công cụ xác thực này có thể lưu trữ dấu vân tay thông thường và dấu vân tay khẩn cấp.

Công cụ xác thực này có thể tạo ra mã xác thực bằng cách sử dụng thông tin người dùng này, và xác định xem liệu mã xác thực này có khớp với mã xác thực nhận được từ đầu cuối xác thực này hay không.

Công cụ xác thực này có thể lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên được chọn này, tạo ra khóa bí mật được chia sẻ bằng cách sử dụng số ngẫu nhiên này và khóa công khai này nhận được từ đầu cuối xác thực này, tạo ra mã xác minh bằng cách sử dụng khóa bí mật được chia sẻ này và thông tin người dùng này, và truyền khóa công khai được tạo ra này và mã xác minh này đến đầu cuối xác thực này.

Đầu cuối xác thực này có thể tạo ra khóa bí mật được chia sẻ bằng cách sử dụng khóa công khai nhận được từ công cụ xác thực này và xác định xem liệu kết quả tính toán giữa khóa bí mật được chia sẻ được tạo ra này và mã xác minh nhận được từ công cụ xác thực này có khớp với mã xác minh được tạo ra bằng cách sử dụng thông tin người dùng này hay không.

Đầu cuối xác thực này có thể tạo ra khóa bí mật được chia sẻ bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi đầu cuối xác thực này và khóa công khai này nhận được từ máy chủ giao dịch này, tạo ra mã xác minh được biến đổi bằng cách sử dụng khóa bí mật được chia sẻ được tạo ra này, và truyền khóa công khai này và mã xác minh được biến đổi này được tạo ra bởi đầu cuối xác thực này đến máy chủ giao dịch này.

Máy chủ giao dịch này có thể tạo ra khóa bí mật được chia sẻ bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi máy chủ giao dịch này và khóa công khai này nhận được từ đầu cuối xác thực này, và xác định xem liệu kết quả tính toán giữa khóa bí mật được chia sẻ được tạo ra này và mã xác minh được biến đổi này nhận được từ đầu cuối xác thực này có khớp với mã xác minh được tạo ra bằng cách sử dụng thông tin người dùng này hay không.

Phương pháp xác thực theo ít nhất một số phương án của sáng chế là nhanh do không có quy trình mã hóa chữ ký số, và bất kỳ ai đều có thể sử dụng phương pháp này bằng cách thay thế mật khẩu bằng chạm dấu vân tay một lần.

Hơn nữa, phương pháp xác thực theo ít nhất một số phương án của sáng chế là an toàn không có nguy cơ rò rỉ thông tin do thông tin cá nhân hoặc thông tin liên quan đến xác thực chỉ được lưu trữ trong đầu cuối xác thực. Ngoài ra, quy trình xác thực này là minh bạch mà không cần nhập dữ liệu cá nhân người dùng vào. Ngoài ra, do sử dụng dấu vân tay hoặc thông tin sinh trắc học được thu thập trực tiếp bởi người dùng này, việc xác minh nhân dạng người dùng này được đảm bảo 100 %.

Hơn nữa, theo phương pháp xác thực theo ít nhất một số phương án của sáng chế, do thông tin cá nhân hoặc thông tin liên quan đến xác thực chỉ được lưu trữ trong đầu cuối xác thực, nguy cơ thông tin cá nhân bị lộ hoặc bị đánh cắp là thấp.

Hơn nữa, phương pháp xác thực theo ít nhất một số phương án của sáng chế có thể

đảm bảo ổn định hơn nhiều do khả năng lộ thông tin khách hàng là thấp hơn so với phương pháp xác thực của máy chủ giao dịch thông thường.

Ngoài ra, phương pháp xác thực theo ít nhất một số phương án của sáng chế có thể tăng tốc độ của quy trình xác minh người dùng này do đầu cuối xác thực có thể nhận mã xác minh không đồng bộ từ công cụ xác thực và ngay lập tức phản hồi yêu cầu xác thực này.

Mô tả vắn tắt các hình vẽ

FIG. 1 là sơ đồ khái niệm minh họa nguyên lý cấu hình tổng thể của hệ thống xác thực theo một phương án của sáng chế.

FIG. 2 là sơ đồ khối minh họa nguyên lý cấu hình của đầu cuối xác thực theo một phương án của sáng chế.

FIG. 3 và FIG. 4 là các sơ đồ khối minh họa nguyên lý cấu hình của công cụ xác thực theo một phương án của sáng chế.

FIG. 5 là lưu đồ minh họa quy trình xác thực theo một phương án của sáng chế.

FIG. 6 là sơ đồ minh họa quy trình truyền tin nhắn trong quy trình xác thực của FIG. 5.

FIG. 7 là sơ đồ minh họa ví dụ thực hiện phương pháp xác thực theo một phương án của sáng chế.

FIG. 8 là sơ đồ minh họa sự bỏ phiếu điện tử thực hiện phương pháp xác thực theo một phương án của sáng chế.

FIG. 9 là sơ đồ minh họa thủ tục mua bán bằng tiền mã hóa thực hiện phương pháp xác thực theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, đầu cuối xác thực, máy chủ xác thực và phương pháp xác thực sử dụng đầu cuối xác thực này và máy chủ xác thực này theo một phương án của sáng chế sẽ được mô tả chi tiết có viện dẫn đến các hình vẽ. Các ưu điểm, các dấu hiệu và các phương pháp để đạt được đầu cuối xác thực, máy chủ xác thực và phương pháp xác thực theo sáng chế sẽ trở nên rõ ràng, có viện dẫn đến các phương án được mô tả chi tiết dưới đây cùng với các hình vẽ kèm theo.

Tuy nhiên, sáng chế không bị giới hạn ở các phương án được mô tả dưới đây, mà có thể được thực hiện dưới nhiều dạng khác nhau, và các phương án này chỉ được đưa ra để hoàn thiện sáng chế và thông tin đầy đủ cho người có trình độ trung bình trong lĩnh vực kỹ thuật này. Cần hiểu rằng sáng chế chỉ bị giới hạn bởi phạm vi của các điểm yêu cầu bảo hộ.

FIG. 1 là sơ đồ khái niệm minh họa nguyên lý cấu hình tổng thể của hệ thống xác thực theo một phương án của sáng chế.

Tham khảo FIG. 1, hệ thống xác thực 100 theo một phương án của sáng chế bao gồm đầu cuối xác thực 110, công cụ xác thực thứ nhất 120, và máy chủ giao dịch 130. Ngoài ra, hệ thống xác thực 100 này theo một phương án của sáng chế có thể còn bao gồm đầu cuối người dùng 140 và công cụ xác thực thứ hai 150.

Đầu cuối người dùng 140 này, là đầu cuối dùng để truy cập vào máy chủ giao dịch 130 này để thực hiện các giao dịch tài chính, có thể bao gồm máy tính cá nhân (personal computer - PC), điện thoại thông minh, máy tính bảng, máy pad, hoặc tất cả các loại đầu cuối có khả năng thực hiện các giao dịch tài chính bằng cách truy cập vào máy chủ giao dịch 130 này không dây hoặc có dây.

Đầu cuối người dùng 140 này truy cập vào máy chủ giao dịch 130 này và yêu cầu giao dịch, sử dụng ứng dụng được cài đặt trên đầu cuối người dùng 140 này hoặc trang mạng được cung cấp bởi máy chủ giao dịch 130 này.

Máy chủ giao dịch 130 này nhận yêu cầu truy cập từ đầu cuối người dùng 140 này và cung cấp màn hình cho đầu cuối người dùng 140 này để đầu cuối người dùng 140 này thực hiện giao dịch.

Đầu cuối người dùng 140 này có thể thực hiện các giao dịch chẳng hạn như xem các chi tiết giao dịch, xem các khoản vay, chuyển tiền, thanh toán lại khoản vay, v.v. bằng cách sử dụng ứng dụng này được cài đặt trên đầu cuối người dùng 140 này hoặc trang mạng này được cung cấp bởi máy chủ giao dịch 130 này.

Máy chủ giao dịch 130 này cần được cài đặt ứng dụng xác thực để thực hiện phương pháp xác thực theo một phương án của sáng chế. Máy chủ giao dịch 130 này có cài đặt ứng dụng xác thực này có thể thực hiện quy trình xác thực nhờ truyền thông dữ liệu với đầu cuối xác thực 110 này và công cụ xác thực thứ hai 150 này.

Khi máy chủ giao dịch 130 này được cài đặt ứng dụng xác thực này nhận được yêu cầu giao dịch từ đầu cuối người dùng 140 này, máy chủ giao dịch 130 này có thể yêu cầu đầu cuối xác thực 110 này, không phải là đầu cuối người dùng 140 này truy cập vào máy chủ giao dịch 130 này, để xác thực người dùng. Người dùng này có thể cho phép thông tin dấu vân tay của người dùng này được nhận diện thông qua đầu cuối xác thực 110 này, nhờ đó xác thực người yêu cầu giao dịch này là người truy cập vào máy chủ giao dịch này.

Đầu cuối xác thực 110 này được cài đặt ứng dụng riêng để xác thực người dùng.

Đầu cuối xác thực 110 này được ghép cặp với đầu cuối người dùng 140 này để có thể truyền thông Bluetooth.

Ngoài ra, đầu cuối xác thực 110 này có thể chính là đầu cuối người dùng 140 này. Trong trường hợp này, đầu cuối xác thực 110 này truy cập vào máy chủ giao dịch 130 này để thực hiện giao dịch tài chính, ngoài chức năng của đầu cuối xác thực 110 này.

Đầu cuối xác thực 110 này nhận yêu cầu xác thực này từ máy chủ giao dịch 130 này và yêu cầu xác minh bằng cách yêu cầu mã xác minh từ công cụ xác thực thứ nhất 120 này.

Công cụ xác thực thứ nhất 120 này có thể được cài đặt trong điện thoại thông minh được đeo bởi người dùng. Ngoài ra, công cụ xác thực thứ hai 150 này có thể được cài đặt trong máy chủ hoặc đám mây.

Một trong số công cụ xác thực thứ nhất 120 này và công cụ xác thực thứ hai 150 này truyền mã xác minh này đến đầu cuối xác thực 110 này, và đầu cuối xác thực 110 này đã nhận được mã xác minh này biến đổi mã xác minh này và sau đó truyền mã xác minh được biến đổi này đến máy chủ giao dịch 130 này.

Hệ thống xác thực theo một phương án của sáng chế có thể bao gồm ít nhất một trong số công cụ xác thực thứ nhất 120 này và công cụ xác thực thứ hai 150 này, và công cụ xác thực thứ nhất 120 này có thể chính là công cụ xác thực thứ hai 150 này. Trong trường hợp trong đó công cụ xác thực thứ nhất 120 này bị mất hoặc công cụ xác thực thứ nhất 120 này không khả dụng, công cụ thứ hai 150 này được dự phòng cho máy chủ này hoặc đám mây này có thể được sử dụng làm công cụ xác thực này.

Máy chủ giao dịch 130 này thực hiện giao dịch được yêu cầu bởi người dùng này sau khi xác minh nhân dạng của người dùng đã yêu cầu giao dịch này bằng cách sử dụng mã xác minh được biến đổi này.

Theo một phương án, nếu người dùng này không có công cụ xác thực thứ nhất 120 này và đầu cuối xác thực 110 này, máy chủ giao dịch 130 này có thể trực tiếp yêu cầu công cụ xác thực thứ hai 150 này cung cấp mã xác minh này, và công cụ xác thực thứ hai 150 này có thể gửi mã xác minh này đến máy chủ giao dịch 130 này.

Như được sử dụng trong bản mô tả này, xác thực đề cập đến quy trình trước khi kiểm tra tính hợp pháp của người dùng này và đầu cuối này, từ máy chủ giao dịch 130 này đến công cụ xác thực 120 và 150 này bằng đầu cuối xác thực 110 này, và xác minh đề cập đến quy trình sau khi kiểm tra tính hợp pháp của người dùng này và đầu cuối này, từ công cụ xác thực 120 và 150 đến máy chủ giao dịch 130 này bằng đầu cuối xác thực 110 này.

Ngoài ra, thông tin xác thực này và thông tin xác minh này trong mỗi quy trình có thể được biến đổi cho mỗi quy trình nhưng có thể bao gồm cùng một thông tin.

FIG. 2 là sơ đồ khối minh họa nguyên lý cấu hình của đầu cuối xác thực 110 theo một phương án của sáng chế, và FIG. 3 và FIG. 4 là các sơ đồ khối minh họa nguyên lý cấu hình của các công cụ xác thực 120 và 150 theo một phương án của sáng chế.

Tham khảo các hình vẽ từ FIG. 1 đến FIG. 4, đầu cuối xác thực 110 này theo một phương án của sáng chế bao gồm khối đầu vào 111, khối quét dấu vân tay 112, khối lưu trữ 113, khối truyền thông 114, khối hiển thị 115, và bộ điều khiển 116. Công cụ xác thực thứ nhất 120 này bao gồm bộ điều khiển 126, khối lưu trữ 123, khối hiển thị 125, và khối truyền thông 124.

Ngoài ra, công cụ xác thực thứ hai 150 này bao gồm bộ điều khiển 156, khối lưu trữ 153, khối hiển thị 155, và khối truyền thông 154.

Đầu cuối xác thực 110 này xác thực người dùng này bằng cách nhận diện thông tin dấu vân tay của người dùng này. Theo phương pháp nhận diện dấu vân tay thông thường, sau khi các đường vân tay của người dùng này được quét và được lưu trữ thành hình ảnh, dấu vân tay của người dùng được quét mỗi khi thực hiện xác thực, và nhân dạng của người dùng này được xác minh theo kết quả so sánh giữa hình ảnh dấu vân tay được quét của người dùng này và hình ảnh dấu vân tay được lưu trữ. Phương pháp nhận dạng dấu vân tay thông thường này chỉ thuần túy so sánh các hình ảnh dấu vân tay này, và do đó nếu dấu vân tay của người dùng bị trùng lặp và được sử dụng, có thể xảy ra lỗi, và có thể được nhận dạng là dấu vân tay của người dùng này.

Để giải quyết lỗi nhận dạng dấu vân tay bị trùng lặp nêu trên, sáng chế sử dụng thực

tế là các tuyến mồ hôi được tạo ra theo hình dạng của các đường vân tay, và các lỗ rỗng hô hấp và di chuyển tỉ mỉ để thoát mồ hôi từ các tuyến mồ hôi này. Cơ thể người luôn luôn thở qua da, nên nếu nhiều hơn một phần ba cơ thể người bị bỏng, con người có thể chết, trong trường hợp này nguyên nhân tử vong là ngạt thở. Tức là, cơ thể người cần thở không chỉ qua mũi và miệng mà còn qua da.

Do đó, theo sáng chế, để xác định xem liệu dấu vân tay này có phải là dấu vân tay bị trùng lặp, phương pháp trích xuất, thành tín hiệu điện của chip bán dẫn, sự thay đổi chuyển động của các tuyến mồ hôi này theo hình dạng của các đường vân tay, tức là, mức độ hoạt động của việc hô hấp qua da và sự thoát mồ hôi, có thể được sử dụng bổ sung cho phương pháp so sánh các hình ảnh dấu vân tay trong quy trình xác thực này, để cho có thể phân biệt được dấu vân tay bị trùng lặp và dấu vân tay sinh trắc học. Do đó, sáng chế có thể phân biệt xác thực chủ động với xác thực do sự trùng lặp các dấu vân tay.

Ngoài ra, người dùng này có thể đăng ký dấu vân tay thông thường được sử dụng cho giao dịch thông thường và dấu vân tay khẩn cấp được sử dụng trong tình huống khẩn cấp trong ít nhất một trong số công cụ xác thực thứ nhất 120 này và công cụ xác thực thứ hai 150 này. Ví dụ như, dấu vân tay của ngón cái có thể được đăng ký làm dấu vân tay thông thường được sử dụng trong giao dịch thông thường, và dấu vân tay của ngón trỏ có thể được đăng ký làm dấu vân tay khẩn cấp được sử dụng trong trường hợp khẩn cấp. Do đó, trong trường hợp trong đó người dùng bị bắt cóc và cần phải xác thực mà không phải là mong muốn của chính người dùng này, người dùng này có thể sử dụng dấu vân tay cho trường hợp khẩn cấp để có thể thực hiện các hành động khẩn cấp, ví dụ như, thông báo cho cảnh sát hoặc gửi thông tin cho cảnh sát.

Khi người dùng này vận hành khối đầu vào 111 này của đầu cuối xác thực 110 này để chuyển sang chế độ đăng ký dấu vân tay này, và sau đó chạm bề mặt dưới của ngón tay có dấu vân tay này vào khối quét dấu vân tay 112 này, khối quét dấu vân tay 112 này quét dấu vân tay này của người dùng này và chuyển đổi các dấu vân tay này thành dữ liệu dấu vân tay tương ứng.

Dữ liệu vân tay được chuyển đổi này được nhập vào từ khối quét dấu vân tay 112 này đến bộ điều khiển 116 này và sau đó được ghi lại trong khối lưu trữ 113 này bằng bộ điều khiển 116 này, và do đó dấu vân tay của người dùng này được đăng ký. Để ngăn chặn sự rò rỉ dữ liệu dấu vân tay này có thể xảy ra khi đầu cuối xác thực 110 này bị mất, dữ liệu dấu vân tay này được mã hóa và được lưu trữ riêng biệt trong các khối lưu trữ 123 và 153 này của các công cụ xác thực 120 và 150 này, và người dùng này trực tiếp quản lý thông tin dấu vân tay của mình.

Theo một phương án, thuật toán thích hợp đối với khả năng hoặc công năng của đầu cuối xác thực 110 được sử dụng có thể được chọn làm thuật toán mã hóa được sử dụng để mã hóa dữ liệu dấu vân tay này. Khi dữ liệu dấu vân tay này được lưu trữ trong công cụ xác thực thứ hai 150 này, dữ liệu dấu vân tay này có thể được truyền dẫn qua kênh truyền thông an toàn có áp dụng bảo mật tầng giao vận (Transport Layer Security - TLS), tầng socket bảo mật (Secure Sockets Layer - SSL), hoặc bảo mật tầng giao vận gói dữ liệu

(Datagram Transport Layer Security - DTLS).

Khi người dùng này thực hiện giao dịch tài chính, người dùng này cho mặt dưới của ngón tay có dấu vân tay này tiếp xúc với khối quét dấu vân tay 112 này, và khối quét dấu vân tay 112 này quét dấu vân tay của người dùng này và chuyển các dấu vân tay này thành dữ liệu dấu vân tay tương ứng. Dữ liệu dấu vân tay được chuyển đổi bởi khối quét dấu vân tay 112 này được nhập vào bộ điều khiển 116 này.

Trong trường hợp này, bộ điều khiển 116 này so sánh dữ liệu dấu vân tay được nhập vào từ khối quét dấu vân tay 112 này với dữ liệu dấu vân tay được lưu trữ trong khối lưu trữ 113 này để xác định xem liệu người dùng hiện tại có phải là người dùng đã được đăng ký hay không. Nếu người dùng hiện tại này không phải là người dùng đã được đăng ký, việc xác thực dấu vân tay này bị hủy và tin nhắn thông báo rằng việc xác thực dấu vân tay bị hủy được hiển thị qua khối hiển thị 115 này.

Ngoài ra, khi thông tin dấu vân tay đã được mã hóa này được lưu trữ trong khối lưu trữ 113 này được giải mã để so sánh dữ liệu dấu vân tay được nhập vào từ khối quét dấu vân tay 112 này với dữ liệu dấu vân tay được lưu trữ trong khối lưu trữ 113 này, dữ liệu dấu vân tay được giải mã này được lưu trữ tạm thời trong không gian an toàn và bị xóa đồng thời khi quy trình xác thực này kết thúc.

Theo một phương án, khi xác định được rằng người dùng có dấu vân tay đã bị truy vấn là người dùng đã được đăng ký này như kết quả xác định này, bộ điều khiển 116 này mã hóa tín hiệu xác thực dấu vân tay chỉ báo rằng dấu vân tay này đã được xác thực, dữ liệu thời gian chỉ báo thời gian hiện tại, dữ liệu dấu vân tay được xác thực, và tương tự theo thuật toán mã hóa đã được xác định trước được lưu trữ trong khối lưu trữ 113 này và xuất chúng vào khối truyền thông 114 này, và tin nhắn chỉ báo rằng dấu vân tay đã được xác thực được hiển thị trên khối hiển thị 115 này.

Nếu không có thao tác chính nào trong khoảng thời gian được xác định trước sau khi thực hiện xác thực dấu vân tay này, dữ liệu dấu vân tay đã được xác thực trước đó sẽ bị vô hiệu và cần phải được xác thực lại để sử dụng đầu cuối xác thực 110 này. Do đó, có thể giải quyết được các vấn đề tình cờ khởi động việc xác thực dấu vân tay này, do đó để cho đầu cuối xác thực 110 này không bị chạm vào.

Mặt khác, theo thứ tự ngược lại, khi thực hiện xác thực dấu vân tay này sau khi thực hiện xong thao tác chính này, và khi dữ liệu tương ứng với thao tác chính trước đó được truyền dẫn cùng với dữ liệu xác thực dấu vân tay này, bên nhận có thể xử lý tất cả các dữ liệu được truyền từ đầu cuối xác thực 110 này.

FIG. 5 là lưu đồ minh họa quy trình xác thực theo một phương án của sáng chế. FIG. 6 là sơ đồ minh họa quy trình truyền tin nhắn trong quy trình xác thực của FIG. 5.

Để giải thích quy trình xác thực này và quy trình truyền tin nhắn theo sáng chế, mỗi dữ liệu trong các dữ liệu được sử dụng trong sáng chế sẽ được biểu diễn bởi các ký hiệu sau.

ph: số điện thoại, im: IMEI, pid: công cụ xác thực ID

od: loại giao dịch, msg_s^d: tin nhắn

dur: khoảng thời gian, t_{now}: thời gian hiện tại

h (): hàm băm, au: mã xác thực, ve_d: mã xác minh

n_d: số ngẫu nhiên, Q_d: khóa công khai, K_s^d : khóa bí mật được chia sẻ

Nhóm đường cong eliptic: kích cỡ-q (số nguyên tố lớn), thông số sản xuất-G

Chỉ số dưới d biểu thị điểm đến và s biểu thị nguồn. P có nghĩa là điện thoại, e có nghĩa là công cụ, b có nghĩa là ngân hàng, và c có nghĩa là máy tính cá nhân. Thông tin cần cho việc xác thực được truyền qua khóa công khai này và mã xác thực này.

Đầu cuối người dùng này có thể là bất kỳ một trong số máy tính (PC), điện thoại thông minh, và máy tính bảng của người dùng.

Ngoài ra, đầu cuối người dùng này có thể chính là đầu cuối xác thực này. Trong trường hợp này, đầu cuối người dùng này thực hiện đồng thời chức năng của đầu cuối xác thực này.

Máy chủ giao dịch này có thể bao gồm máy chủ của ngân hàng.

1. Yêu cầu giao dịch và truyền thông tin đầu cuối

- Đầu cuối người dùng -> Máy chủ giao dịch

Khi đầu cuối người dùng truy cập vào trang mạng (web) của máy chủ giao dịch này yêu cầu máy chủ giao dịch này giao dịch tài chính, tin nhắn bao gồm các loại giao dịch, thông tin người dùng chẳng hạn như số điện thoại, hoặc thông tin đầu cuối được gửi. Tin nhắn là như sau.

$msg_s^d=(od,ph)$

2. Tạo ra mã xác minh và yêu cầu xác thực

Máy chủ giao dịch

Máy chủ giao dịch này thực hiện phép toán AND giữa chuỗi bit của thời gian hiện tại và khoảng thời gian trong đó phần đặc trưng được đặt là 0 (zero). Ví dụ như, nếu thời gian hiện tại = (năm, tháng, ngày, giờ, phút, giây, mili giây) và khoảng thời gian = ((1). (1). (1). (1). (0). (0)), khoảng thời gian này có nghĩa là một phút. Nếu phép toán AND này được thực hiện trên thời gian hiện tại này và khoảng thời gian này, (giây. mili giây) trở thành 0, và do đó giá trị của phép toán AND này được thực hiện trên thời gian hiện tại này và khoảng thời gian này trong 1 phút luôn luôn là cùng một giá trị.

$t=t_{now}*dur$, trong đó t là thời gian.

Máy chủ giao dịch này băm chuỗi bit <số điện thoại, im, thời gian> để tạo ra mã xác thực_máy chủ giao dịch, có nghĩa là mã xác thực của máy chủ giao dịch này. Như được sử dụng trong bản mô tả này, im là ký hiệu biểu thị mã số nhận dạng thiết bị di động quốc tế (international mobile equipment identity - IMEI), là mã số duy nhất của đầu cuối thể hiện thông tin chẳng hạn như nhà sản xuất và model của đầu cuối này. IMEI này có thể nhận được từ đầu cuối người dùng này.

$au_b=h(<ph,im,t)$

Máy chủ giao dịch này lựa chọn số ngẫu nhiên và sử dụng nó làm khóa riêng cần được lưu trữ. Khóa công khai được tính toán dựa vào khóa riêng này. Số ngẫu nhiên này

được tạo ra nhờ thiết bị tạo số ngẫu nhiên (random number generator - RNG), thiết bị tạo số ngẫu nhiên giả (pseudo random number generator - PRNG), hoặc thiết bị tạo số ngẫu nhiên thực được sử dụng làm khóa riêng. Khóa công khai này được tính toán dựa vào khóa riêng này bằng cách sử dụng thuật toán mã hóa đường cong eliptic (elliptic curve cryptography - ECC). Trong trường hợp này, kích thước của khóa này được tạo ra bởi thuật toán ECC cần phải ít nhất là 160 bit. Khóa riêng được tạo ra này cần được lưu trữ trong vùng an toàn.

$0 < n_b < q, Q_b = n_b G$

Máy chủ giao dịch-> Đầu cuối xác thực

Máy chủ giao dịch này gửi tin nhắn bao gồm (khóa công khai, mã xác thực_máy chủ giao dịch) để yêu cầu xác thực và giao dịch cho người dùng này.

$msg_b^p = (Q_b, au_b)$

3. Tạo ra mã xác thực được biến đổi và yêu cầu xác minh

Đầu cuối xác thực

Đầu cuối xác thực này kiểm tra tính hợp pháp của máy chủ giao dịch này. Đầu cuối xác thực này thiết lập thời gian hiện tại bằng cách thực hiện phép toán AND với khoảng thời gian này. Khi mã xác thực_đầu cuối xác thực này được lưu trữ trước trong đầu cuối xác thực này và mã xác thực_máy chủ giao dịch này nhận được từ máy chủ giao dịch này khớp với nhau, đầu cuối xác thực này xác định rằng máy chủ giao dịch này là hợp pháp.

$t = t_{now} * dur$, trong đó t là thời gian.

$au_b = h(ph, im, t>)$

If $au_p = U_b$, valid

Ngoài ra, đầu cuối xác thực này tạo ra mã xác thực được biến đổi dựa vào mã xác thực nhận được từ máy chủ giao dịch này. Đầu cuối xác thực này tạo ra mã xác thực được biến đổi này bằng cách băm <số điện thoại, im, thông tin bio, thời gian> dựa vào ít nhất một trong số thông tin sinh trắc học và mức độ hoạt động sinh học được trích xuất bởi phương tiện sinh trắc học của đầu cuối xác thực này và mã xác thực_đầu cuối xác thực (au_p) nhận được này.

Thông tin sinh trắc học này có thể bao gồm ít nhất một thông tin được chọn từ nhóm bao gồm dấu vân tay, mống mắt, chất sinh lý (ví dụ, mồ hôi, nước mắt, nước tiểu, v.v.) được xuất ra từ cơ thể người và chỉ báo mức độ hoạt động của con người.

Ngoài ra, đầu cuối xác thực này lựa chọn số ngẫu nhiên cần được lưu trữ làm khóa riêng và tính toán khóa công khai dựa vào số ngẫu nhiên này. Số ngẫu nhiên này được tạo ra nhờ thiết bị tạo số ngẫu nhiên (RNG), thiết bị tạo số ngẫu nhiên giả (PRNG), hoặc thiết bị tạo số ngẫu nhiên thật và được sử dụng làm khóa riêng này. Khóa công khai này được tính toán dựa vào khóa riêng này bằng cách sử dụng thuật toán mã hóa đường cong eliptic (ECC). Trong trường hợp này, kích thước của khóa này được tạo ra bởi thuật thoán ECC này cần phải ít nhất là 160 bit. Khóa riêng được tạo ra này cần được lưu trữ trong vùng an toàn.

au=h(<ph,im,or,ac,t>)

$0<n_p=q, Q_p=n_pG$

Đầu cuối xác thực -> Công cụ xác thực

Đầu cuối xác thực này gửi mã xác thực được biến đổi này (khóa công khai, thông tin sinh trắc học, mã xác thực_đầu cuối xác thực) đến công cụ xác thực này và yêu cầu mã xác minh.

$$msg_p^e=(Q_p,au_p)$$

4. Tạo mã xác minh và gửi mã xác minh

Công cụ xác thực

Công cụ xác thực này kiểm tra tính hợp pháp của đầu cuối xác thực này. Công cụ xác thực này có thể thiết lập thời gian hiện tại bằng cách thực hiện phép toán AND với khoảng thời gian này và trích xuất thông tin sinh trắc học có trong mã xác thực được biến đổi nhận được từ đầu cuối xác thực này.

Công cụ xác thực này so sánh thông tin sinh trắc học và mức độ hoạt động được lưu trữ của người dùng này với thông tin sinh trắc học nhận được từ đầu cuối xác thực này và khi chúng khớp với nhau, công cụ xác thực này xác định rằng đầu cuối xác thực này là hợp pháp.

Phương án khác là, để xác định tính hợp pháp của đầu cuối xác thực này, công cụ xác thực này có thể thiết lập thời gian hiện tại bằng cách thực hiện phép toán AND với khoảng thời gian này và tính toán mã xác thực_công cụ xác thực này bằng cách sử dụng thông tin sinh trắc học được lưu trữ trước trong công cụ xác thực này. Tiếp theo, công cụ xác thực này có thể so sánh mã xác thực_công cụ xác thực được tính toán với mã xác thực_đầu cuối xác thực được biến đổi nhận được từ đầu cuối xác thực này và khi chúng khớp với nhau, công cụ xác thực này có thể xác định rằng đầu cuối xác thực này là hợp pháp.

$t=t_{now}$*dur, trong đó t là thời gian.

au_e=h(<ph,im,or,ac,t>)

If $au_e=au_p$, valid

Ngoài ra, công cụ xác thực này tạo ra mã xác minh sẽ được gửi đến đầu cuối xác thực này dựa vào mã xác thực được biến đổi này. Công cụ xác thực này lựa chọn số ngẫu nhiên làm khóa riêng và tạo ra khóa công khai bằng cách sử dụng khóa riêng này. Ngoài ra, công cụ xác thực này tính toán khóa bí mật được chia sẻ bằng cách nhân khóa công khai này từ đầu cuối xác thực này với khóa riêng này được tạo ra bởi công cụ xác thực này. Khóa bí mật này cần phải trùng nhau trên đầu cuối xác thực này và công cụ xác thực này. Công cụ xác thực này tạo ra mã xác minh này bằng phép XOR kết quả của việc băm <số điện thoại, im, thời gian, ID công cụ xác thực > và khóa bí mật được chia sẻ này.

$$0 < n_e < q, Q_e = n_eG, K_p^e=n_eQ_p=n_en_pG$$

$$ve_e = h(< ph,im,t,pid >) \oplus K_p^e$$

Công cụ xác thực -> Đầu cuối xác thực

Khóa công khai này và mã xác minh này của công cụ xác thực này được truyền đến

đầu cuối xác thực này.

$$msg_e^p=(Q_e,ve_e)$$

5. Tạo ra mã xác minh được biến đổi và gửi mã xác minh được biến đổi

Đầu cuối xác thực

Đầu cuối xác thực này tạo ra khóa bí mật được chia sẻ bằng cách nhân khóa công khai này của công cụ xác thực này với khóa riêng của chính đầu cuối xác thực này và tạo ra mã xác minh được biến đổi bằng phép XOR mã xác minh nhận được từ công cụ xác thực này bằng khóa bí mật được chia sẻ này.

Đầu cuối xác thực này tạo ra mã xác minh của chính đầu cuối xác thực này và xác định rằng công cụ xác thực này là hợp pháp khi kết quả của phép XOR khóa bí mật được chia sẻ này và mã xác minh nhận được từ công cụ xác thực này khớp với mã xác minh được tạo ra dựa vào thông tin được lưu trữ trong chính đầu cuối xác thực này.

$K_{p\,e'}=n_pQ_e=n_pn_eG$

$ve'_e=ve_eK_{p\,e'}=h(<ph,im,t,pid>)$

$ve_p=h(<ph_p,im_pt,pid>)$

If $ve'_e=ve_p$, OK

Đầu cuối xác thực này tạo ra mã xác minh được biến đổi. Đầu cuối xác thực này tính toán khóa bí mật được chia sẻ bằng cách nhân khóa công khai này của máy chủ giao dịch này với khóa riêng này của đầu cuối xác thực này. Đầu cuối xác thực này tạo ra mã xác minh được biến đổi này, sẽ được truyền đến máy chủ giao dịch này, bằng phép XOR kết quả của việc băm <số điện thoại, im, thời gian, ID công cụ xác thực> và khóa bí mật được chia sẻ này.

$K_b^P=n_pQ_b=n_p\tilde{n_b}G$

$ve_p=h(<ph,im,t,pid>)\oplus K_b^P$

Đầu cuối xác thực -> Máy chủ giao dịch

Đầu cuối xác thực này gửi (khóa công khai, mã xác minh được biến đổi) đến máy chủ giao dịch này.

$$msg_p^b=(Q_p,ve_p)$$

6. Thông báo xử lý giao dịch

Máy chủ giao dịch

Máy chủ giao dịch này tính toán khóa bí mật được chia sẻ bằng cách nhân khóa công khai này nhận được từ đầu cuối xác thực này với khóa riêng của máy chủ giao dịch này và so sánh kết quả của phép XOR khóa bí mật được chia sẻ này và mã xác minh được biến đổi này nhận được từ đầu cuối xác thực này với kết quả của hàm băm <số điện thoại, im, thời gian, ID công cụ xác thực> có trong mã xác thực này được lưu trữ trong máy chủ giao dịch này. Máy chủ giao dịch này thông báo xử lý giao dịch này nếu các kết quả so sánh trùng khớp.

$k_p{}^{b'}=n_b q_p=n_b n_p G$
$ve_b=h(<ph_b.im_b.t_b.pid_b>)$
If $ve_p \oplus K_b{}^{p'}=ve_b.OK$

Sáng chế dựa vào tính ổn định của thuật toán Diffie-Hellman đường cong eliptic (ECDH), và số ngẫu nhiên này không thể được xác định bởi riêng khóa công khai này. Phương pháp xác thực theo sáng chế có thể chia sẻ cùng một khóa bí mật bằng cách trao đổi các khóa công khai của cả hai bên, và kẻ ăn cắp không thể tìm được số ngẫu nhiên chỉ bởi khóa công khai này.

FIG. 7 là sơ đồ minh họa một ví dụ thực hiện phương pháp xác thực theo một phương án của sáng chế. Các số được mô tả trong phương án này của sáng chế được đơn giản hóa và được mô tả tùy ý để giúp hiểu rõ sáng chế.

Tham khảo FIG. 7, trong 701, người dùng yêu cầu truy cập vào máy chủ qua máy tính (PC) của người dùng. Máy chủ này truyền trang để người dùng này nhập số điện thoại di động vào và người dùng này nhập số điện thoại này vào.

Trong 702, máy chủ này đã nhận được số điện thoại di động này gửi số được tạo ra ngẫu nhiên 9 và yêu cầu điện thoại di động này xác thực người dùng này.

Trong 703, khi người dùng này ấn nút chấp thuận, số 9 này nhận được bởi điện thoại di động này được gửi đến công cụ xác thực này để yêu cầu xác minh.

Công cụ xác thực được yêu cầu để xác minh tạo ra mã ngẫu nhiên 12345. Hơn nữa, công cụ xác thực này tạo ra mã xác minh 111105 bằng cách nhân số ngẫu nhiên 9 này nhận được từ máy chủ này với 12345 được tạo ra bởi công cụ xác thực này.

Trong 704, công cụ xác thực này gửi mã xác minh được tạo ra 111105 này đến điện thoại di động này.

Trong 705, điện thoại di động này tạo ra mã xác minh được biến đổi 9 bằng cách cộng mỗi chữ số của mã xác minh này nhận được từ công cụ xác thực này và gửi mã xác minh được biến đổi 9 này đến máy chủ này.

Trong 706, máy chủ này xác định xem liệu mã xác minh 9 được biến đổi nhận được này và số ngẫu nhiên 9 này được xuất ra từ máy chủ này có khớp với nhau không. Do mã xác minh 9 được biến đổi nhận được này và số ngẫu nhiên 9 này được xuất ra từ máy chủ này khớp với nhau, máy chủ này thông báo cho PC của người dùng này thực hiện kết nối.

Trong quy trình xác thực đăng nhập thực hiện phương pháp xác thực theo một phương án của sáng chế, do quy trình đăng ký là không cần thiết, không cần phải lưu trữ thông tin cá nhân trong máy chủ này, nên không có nguy cơ rò rỉ thông tin cá nhân.

Ngoài ra, do các mã ngẫu nhiên luôn được tạo ra trong máy chủ này và phía người dùng này, không có số cố định, và mã ngẫu nhiên bất quy tắc được tạo ra khiến cho khó rò rỉ thông tin.

Ngoài ra, do loại bỏ quy trình mã hóa, phương pháp theo sáng chế không bị quá tải, và tất cả các tính toán được thực hiện trong vòng 1 giây.

FIG. 8 là sơ đồ minh họa sự bỏ phiếu điện tử thực hiện phương pháp xác thực theo một phương án của sáng chế.

Tham khảo FIG. 8, trong 801, người bỏ phiếu yêu cầu truy cập bằng cách nộp đơn yêu cầu bỏ phiếu điện tử cho ủy ban quản lý bầu cử thông qua máy tính (PC) hoặc điện thoại di động của người bỏ phiếu.

Khi nhận được yêu cầu truy cập này trong 802, máy chủ này của ủy ban quản lý bầu cử này gửi số ngẫu nhiên 9 để nhận dạng và danh sách bỏ phiếu điện tử đến điện thoại di động của người bỏ phiếu này để yêu cầu xác thực.

Trong 803, khi người bỏ phiếu này bỏ phiếu cho một trong số các ứng viên trong danh sách bỏ phiếu điện tử này và ấn nút chấp thuận, điện thoại di động này gửi số ngẫu nhiên này và kết quả bỏ phiếu điện tử này đến công cụ xác thực này và yêu cầu xác minh.

Trong 804, công cụ xác thực này tạo ra mã ngẫu nhiên 12345, nhân số ngẫu nhiên 9 này nhận được từ máy chủ của ủy ban quản lý bầu cử này với 12345 được tạo ra bởi công cụ xác thực này, và truyền kết quả này cùng với kết quả bỏ phiếu điện tử này đến điện thoại di động này.

Trong 805, điện thoại di động này cộng mỗi chữ số của 111105 nhận được từ công cụ xác thực này, nhờ đó tạo ra mã xác minh được biến đổi 9, và truyền kết quả này đến máy chủ của ủy ban quản lý bầu cử này cùng với kết quả bỏ phiếu điện tử này.

Trong 806, máy chủ của ủy ban quản lý bầu cử này so sánh số ngẫu nhiên 9 này được gửi bởi máy chủ của ủy ban quản lý bầu cử này với mã xác minh được biến đổi này nhận được từ điện thoại di động này, xác định nhân dạng của người dùng bỏ phiếu điện tử này, và lưu trữ kết quả bỏ phiếu điện tử này.

Việc bỏ phiếu điện tử thực hiện phương pháp xác thực theo một phương án của sáng chế có thể được quản lý bởi máy chủ của ủy ban quản lý bầu cử này và có thể kỳ vọng làm tăng tỷ lệ người bầu cử.

Ngoài ra, do luôn sử dụng các mã ngẫu nhiên, không có nguy cơ rò rỉ thông tin, không thể bỏ phiếu ủy nhiệm, và loại bỏ quy trình mã hóa, nên không có nguy cơ máy chủ bị quá tải, và thông tin bỏ phiếu không thể bị can thiệp vào.

Ngoài ra, việc bỏ phiếu điện tử thực hiện phương pháp xác thực theo một phương án của sáng chế có thể ngay lập tức giảm các chi phí bầu cử và các chi phí kiểm đếm do có kết quả bỏ phiếu ngay sau khi kết thúc bỏ phiếu.

FIG. 9 là sơ đồ minh họa thủ tục mua bán bằng tiền mã hóa thực hiện phương pháp xác thực theo một phương án của sáng chế.

Tham khảo FIG. 9, trong 901, công cụ xác thực của người dùng này tạo ra mã ngẫu nhiên và yêu cầu điện thoại di động của người dùng này chuyển tiền.

Trong 902, khi người dùng này nhập số lượng tiền cần phải chuyển đến điện thoại di động của người dùng này, điện thoại di động của người dùng này tạo ra số ngẫu nhiên 9. Điện thoại di động của người dùng này gửi số ngẫu nhiên 9 được tạo ra này đến điện thoại di động của bên đối tác.

Trong 903, bên đối tác này xác nhận số lượng tiền cần chuyển và ấn nút chấp thuận. Điện thoại di động của bên đối tác này gửi số ngẫu nhiên nhận được này và thông tin về lượng tiền chuyển đến công cụ xác thực của bên đối tác này và yêu cầu xác minh.

Trong 904, công cụ xác thực của bên đối tác này tạo ra mã ngẫu nhiên 12345. Công cụ xác thực của bên đối tác này gửi kết quả của phép nhân số ngẫu nhiên 9 nhận được này với 12345 được tạo ra bởi công cụ xác thực này và lượng tiền cần chuyển đến điện thoại di động của bên đối tác này.

Trong 905, điện thoại di động của bên đối tác này tạo ra mã xác minh được biến đổi bằng cách cộng mỗi chữ số của 111105 nhận được từ công cụ xác thực này và gửi mã xác minh được biến đổi này đến điện thoại di động của người dùng này.

Trong 906, so sánh số ngẫu nhiên 9 được gửi ban đầu và mã xác minh 9 được biến đổi nhận được này, và tiền điện tử được chuyển này được lưu trữ trong công cụ xác thực của người dùng này.

Thủ tục giao dịch tiền mã hóa để thực hiện phương pháp xác thực theo một phương án của sáng chế là sơ đồ chuỗi khối riêng (private blockchain scheme) với phương pháp chuyển tiền 1:1. Do người giao dịch tự động tạo ra và sử dụng mã ngẫu nhiên, không có nguy cơ bị rò rỉ thông tin, và không thể đánh cắp. Ngoài ra, việc loại bỏ quy trình mã hóa, nên không có sự quá tải, không có khả năng bị can thiệp và không phát sinh phí mua bán bằng thẻ tín dụng.

Mặc dù sáng chế được mô tả trên đây đã được mô tả có viện dẫn đến các hình vẽ minh họa, là rõ ràng đối với người có trình độ trung bình trong lĩnh vực kỹ thuật này, sáng chế không bị giới hạn ở các phương án được mô tả này và có thể được biến đổi và thay đổi khác nhau mà không nằm ngoài nguyên lý và phạm vi của sáng chế. Do đó, cần hiểu rằng các biến đổi hoặc các thay đổi như vậy đều thuộc phạm vi của các điểm yêu cầu bảo hộ của sáng chế, và phạm vi của sáng chế cần được diễn giải căn cứ vào các điểm yêu cầu bảo hộ kèm theo.

YÊU CẦU BẢO HỘ

1. Hệ thống xác thực, bao gồm:

đầu cuối người dùng được tạo cấu hình để truy cập máy chủ giao dịch bằng cách sử dụng ứng dụng được cài đặt trong đầu cuối người dùng này hoặc trang mạng (web) được cung cấp bởi máy chủ giao dịch này, và yêu cầu giao dịch bằng cách truyền thông tin người dùng;

máy chủ giao dịch được tạo cấu hình để nhận yêu cầu giao dịch này được truyền từ đầu cuối người dùng này, tạo ra mã xác thực_máy chủ giao dịch bằng cách băm chuỗi bít <số điện thoại, nhận dạng thiết bị di động quốc tế (international mobile equipment identity - IMEI), thời gian>, và yêu cầu xác thực đối với đầu cuối người dùng này bằng cách truyền mã xác thực_máy chủ giao dịch được tạo ra này đến đầu cuối xác thực này;

đầu cuối xác thực được tạo cấu hình để tạo ra mã xác thực được biến đổi bằng cách băm chuỗi bít <số điện thoại, IMEI, thời gian> này dựa vào mã xác thực_đầu cuối xác thực, khi mã xác thực_máy chủ giao dịch được tạo ra này được truyền từ máy chủ giao dịch này được khớp với mã xác thực_đầu cuối xác thực đã được lưu trữ trước, và yêu cầu mã xác minh bằng cách truyền mã xác thực được biến đổi được tạo ra này đến máy chủ giao dịch này; và

bộ xử lý xác thực được tạo cấu hình để trích xuất thông tin sinh sắc học có trong mã xác thực được biến đổi này nhận được từ đầu cuối xác thực này, tạo ra mã xác minh này bằng phép XOR kết quả của việc băm <số điện thoại, IMEI, thời gian, ID bộ xử lý xác thực> bằng khóa bí mật được chia sẻ này dựa vào mã xác thực được biến đổi này, khi thông tin sinh sắc học được trích xuất này được khớp với thông tin sinh sắc học được lưu trữ trước và thông tin hoạt động của người dùng này, và truyền mã xác minh được tạo ra này đến đầu cuối xác thực này,

trong đó đầu cuối xác thực này tạo ra khóa bí mật được chia sẻ này bằng cách nhân khóa công khai của bộ xử lý xác thực này với khóa riêng của đầu cuối xác thực này, tạo ra mã xác minh được biến đổi bằng phép XOR kết quả của việc băm <số điện thoại, IMEI, thời gian, ID bộ xử lý xác thực> này bằng khóa bí mật được chia sẻ được tạo ra này, và truyền mã xác minh được biến đổi được tạo ra này đến máy chủ giao dịch này, và

trong đó máy chủ giao dịch này tạo ra khóa bí mật được chia sẻ này bằng cách nhân khóa công khai này nhận được từ đầu cuối xác thực này với khóa riêng của máy chủ giao dịch này, so sánh kết quả của phép XOR khóa bí mật được chia sẻ này và mã xác minh được biến đổi này nhận được từ đầu cuối xác thực này với kết quả của việc băm <số điện thoại, IMEI, thời gian, ID bộ xử lý xác thực> này có trong mã xác thực được lưu trữ trong máy chủ giao dịch này, và thông báo xử lý giao dịch nếu các kết quả so sánh này trùng khớp.

2. Hệ thống xác thực theo điểm 1, trong đó đầu cuối người dùng này truyền tin nhắn bao gồm loại giao dịch và số điện thoại của người dùng này đến máy chủ giao dịch này.

3. Hệ thống xác thực theo điểm 2, trong đó máy chủ giao dịch này lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên này, tạo ra mã xác thực_máy chủ giao dịch này bằng cách sử dụng thông tin người dùng này, và truyền khóa công khai được tạo ra này và mã xác thực_máy chủ giao dịch này đến đầu cuối xác thực này.

4. Hệ thống xác thực theo điểm 1, trong đó đầu cuối xác thực này lựa chọn số ngẫu nhiên, tạo ra khóa công khai này bằng cách sử dụng số ngẫu nhiên này, và truyền khóa công khai được tạo ra này và mã xác thực được biến đổi này đến bộ xử lý xác thực này.

5. Hệ thống xác thực theo điểm 1, trong đó bộ xử lý xác thực này lưu trữ dấu vân tay thông thường và dấu vân tay khẩn cấp.

6. Hệ thống xác thực theo điểm 4, trong đó bộ xử lý xác thực này lựa chọn số ngẫu nhiên, tạo ra khóa bí mật được chia sẻ này bằng cách sử dụng số ngẫu nhiên được lựa chọn này và khóa công khai này nhận được từ đầu cuối xác thực này, và truyền khóa công khai được tạo ra này đến đầu cuối xác thực này.

7. Hệ thống xác thực theo điểm 6, trong đó đầu cuối xác thực này xác định liệu kết quả tính toán giữa khóa bí mật được chia sẻ được tạo ra này và mã xác minh được biến đổi này nhận được từ bộ xử lý xác thực này có khớp với mã xác minh này được tạo ra bằng cách sử dụng thông tin người dùng này hay không.

8. Hệ thống xác thực theo điểm 7, trong đó đầu cuối xác thực này tạo ra khóa bí mật được chia sẻ này bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi đầu cuối xác thực này và khóa công khai nhận được từ máy chủ giao dịch này, và truyền khóa công khai này và khóa bí mật được chia sẻ được tạo ra này đến máy chủ giao dịch này.

9. Hệ thống xác thực theo điểm 8, trong đó máy chủ giao dịch này tạo ra khóa bí mật được chia sẻ này bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi máy chủ giao dịch này và khóa công khai này nhận được từ đầu cuối xác thực này.

10. Phương pháp xác thực được thực hiện bởi hệ thống xác thực bao gồm đầu cuối người dùng, máy chủ giao dịch, đầu cuối xác thực, và bộ xử lý xác thực, phương pháp xác thực này bao gồm:

bằng đầu cuối người dùng này, truy cập máy chủ giao dịch này bằng cách sử dụng ứng dụng được cài đặt trong đầu cuối người dùng này hoặc trang web được cung cấp bởi máy chủ giao dịch này, và yêu cầu giao dịch bằng cách truyền thông tin người dùng;

bằng máy chủ giao dịch này nhận yêu cầu giao dịch này được truyền từ đầu cuối người dùng này, tạo ra mã xác thực_máy chủ giao dịch bằng cách băm chuỗi bít <số điện thoại, nhận dạng thiết bị di động quốc tế (international mobile equipment identity – IMEI), thời gian>, và yêu cầu xác thực đối với đầu cuối người dùng này bằng cách truyền mã xác thực_máy chủ giao dịch được tạo ra này đến đầu cuối xác thực này;

bằng đầu cuối xác thực này, tạo ra mã xác thực được biến đổi bằng cách băm chuỗi bít <số điện thoại, IMEI, thời gian> này dựa vào mã xác thực_đầu cuối xác thực, khi mã xác thực_máy chủ giao dịch được tạo ra này được truyền từ máy chủ giao dịch này được khớp với mã xác thực_đầu cuối xác thực đã được lưu trữ trước, và yêu cầu mã xác minh bằng cách truyền mã xác thực được biến đổi được tạo ra này đến máy chủ giao dịch này; và

bằng bộ xử lý xác thực này, xác minh tính hợp pháp của đầu cuối xác thực này, tạo ra mã xác minh dựa vào mã xác thực được biến đổi này trích xuất thông tin sinh sắc học có trong mã xác thực được biến đổi này nhận được từ đầu cuối xác thực này, tạo ra mã xác minh này bằng phép XOR kết quả của việc băm <số điện thoại, IMEI, thời gian, ID bộ xử lý xác thực> bằng khóa bí mật được chia sẻ này dựa vào mã xác thực được biến đổi này, khi thông tin sinh sắc học được trích xuất này được khớp với thông tin sinh sắc học được lưu trữ trước và thông tin hoạt động của người dùng này, và truyền mã xác minh được tạo ra này đến đầu cuối xác thực này,

trong đó đầu cuối xác thực này tạo ra khóa bí mật được chia sẻ này bằng cách nhân khóa công khai của bộ xử lý xác thực này với khóa riêng của đầu cuối xác thực này, tạo ra mã xác minh được biến đổi bằng phép XOR kết quả của việc băm <số điện thoại, IMEI, thời gian, ID bộ xử lý xác thực> này bằng khóa bí mật được chia sẻ được tạo ra này, và truyền mã xác minh được biến đổi được tạo ra này đến máy chủ giao dịch này, và

trong đó máy chủ giao dịch này tạo ra khóa bí mật được chia sẻ này bằng cách nhân khóa công khai này nhận được từ đầu cuối xác thực này với khóa riêng của máy chủ giao dịch này, so sánh kết quả của phép XOR khóa bí mật được chia sẻ này và mã xác minh được biến đổi này nhận được từ đầu cuối xác thực này với kết quả của việc băm <số điện thoại, IMEI, thời gian, ID bộ xử lý xác thực> này có trong mã xác thực này được lưu trữ trong máy chủ giao dịch này, và thông báo xử lý giao dịch nếu các kết quả so sánh này trùng khớp.

11. Phương pháp xác thực theo điểm 10, trong đó đầu cuối người dùng này truyền tin nhắn bao gồm loại giao dịch và số điện thoại của người dùng này đến máy chủ giao dịch này.

12. Phương pháp xác thực theo điểm 11, trong đó máy chủ giao dịch này lựa chọn số ngẫu nhiên, tạo ra khóa công khai bằng cách sử dụng số ngẫu nhiên này, tạo ra mã xác thực_máy chủ giao dịch này bằng cách sử dụng thông tin người dùng này, và truyền khóa công khai được tạo ra này và mã xác thực_máy chủ giao dịch này đến đầu cuối xác thực này.

13. Phương pháp xác thực theo điểm 10, trong đó đầu cuối xác thực này lựa chọn số ngẫu nhiên, tạo ra khóa công khai này bằng cách sử dụng số ngẫu nhiên này, và truyền khóa công khai được tạo ra này đến bộ xử lý xác thực này.

14. Phương pháp xác thực theo điểm 10, trong đó bộ xử lý xác thực này lưu trữ dấu vân tay thông thường và dấu vân tay khẩn cấp.

15. Phương pháp xác thực theo điểm 13, trong đó bộ xử lý xác thực này lựa chọn số ngẫu nhiên, tạo ra khóa bí mật được chia sẻ này bằng cách sử dụng số ngẫu nhiên được lựa chọn này và khóa công khai này nhận được từ đầu cuối xác thực này, và truyền khóa công khai được tạo ra này đến đầu cuối xác thực này.

16. Phương pháp xác thực theo điểm 15, trong đó đầu cuối xác thực này xác định xem liệu kết quả tính toán giữa khóa bí mật được chia sẻ được tạo ra này và mã xác minh được biến đổi này nhận được từ bộ xử lý xác thực này có khớp với mã xác minh này được tạo ra bằng cách sử dụng thông tin người dùng này hay không.

17. Phương pháp xác thực theo điểm 16, trong đó đầu cuối xác thực này tạo ra khóa bí mật được chia sẻ này bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi đầu cuối xác thực này và khóa công khai nhận được từ máy chủ giao dịch này, và truyền khóa bí mật được chia sẻ được tạo ra này đến máy chủ giao dịch này.

18. Phương pháp xác thực theo điểm 17, trong đó máy chủ giao dịch này tạo ra khóa bí mật được chia sẻ này bằng cách sử dụng số ngẫu nhiên này được tạo ra bởi máy chủ giao dịch này và khóa công khai này nhận được từ đầu cuối xác thực này.

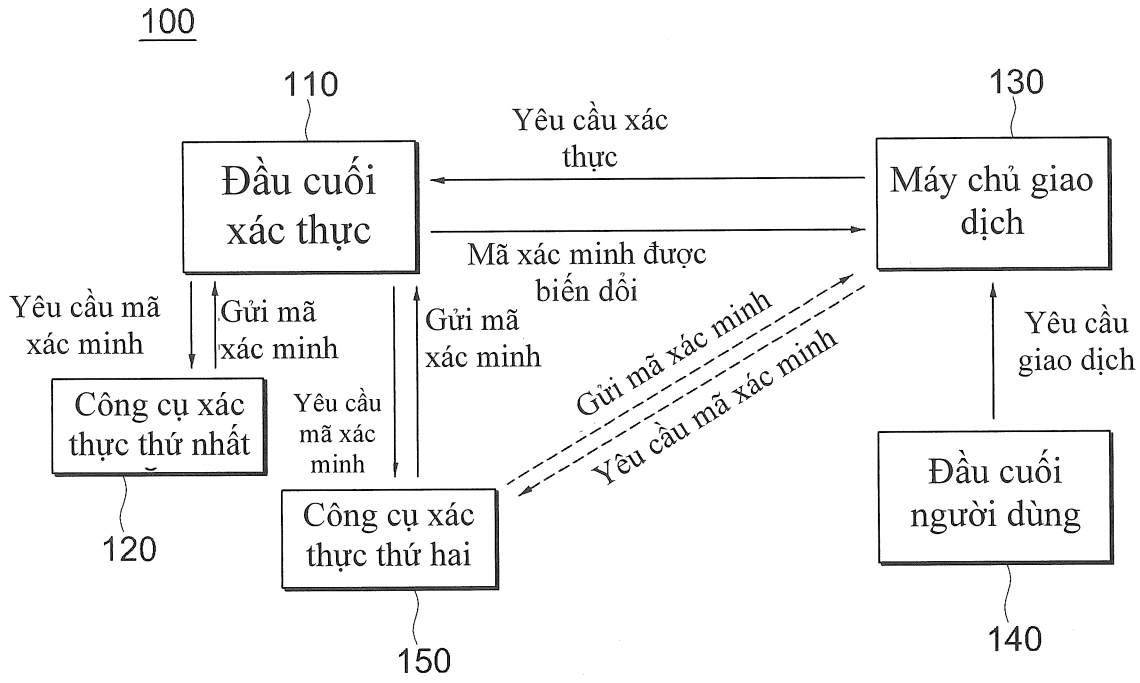
100
110
Đầu cuối xác thực
Yêu cầu xác thực
130
Máy chủ giao dịch
Mã xác minh được biến đổi
Yêu cầu mã xác minh
Gửi mã xác minh
Gửi mã xác minh
Yêu cầu mã xác minh
Gửi mã xác minh
Yêu cầu mã xác minh
Yêu cầu giao dịch
Công cụ xác thực thứ nhất
120
Công cụ xác thực thứ hai
150
Đầu cuối người dùng
140

FIG. 1

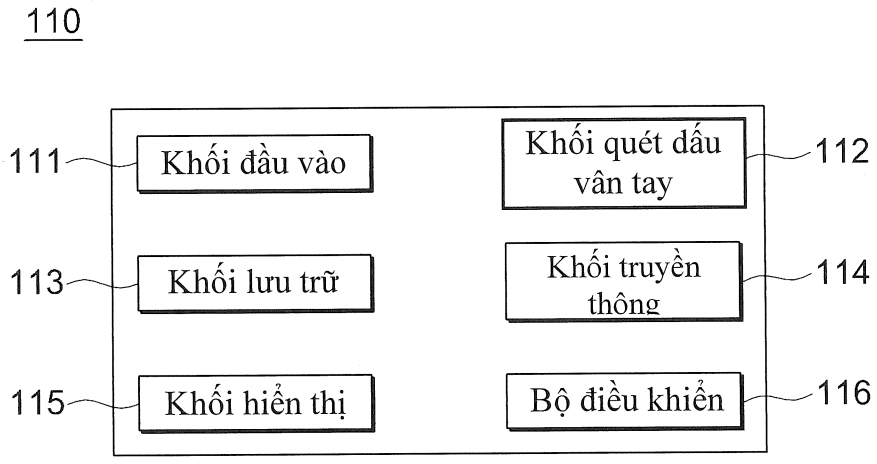
110
111
Khối đầu vào
Khối quét dấu vân tay
112
113
Khối lưu trữ
Khối truyền thông
114
115
Khối hiển thị
Bộ điều khiển
116

FIG. 2

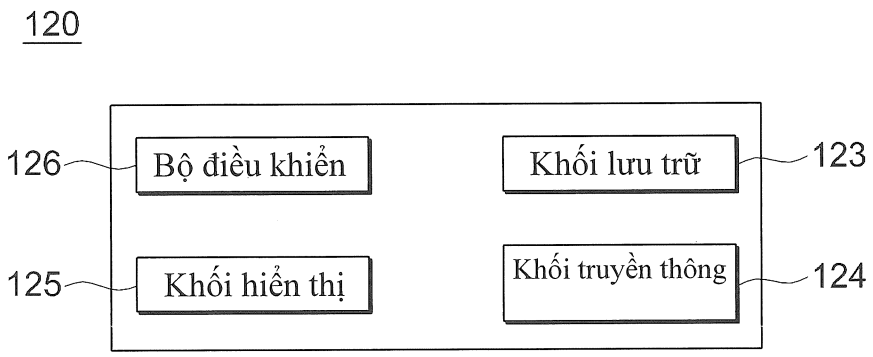
120
126
Bộ điều khiển
Khối lưu trữ
123
125
Khối hiển thị
Khối truyền thông
124

FIG. 3

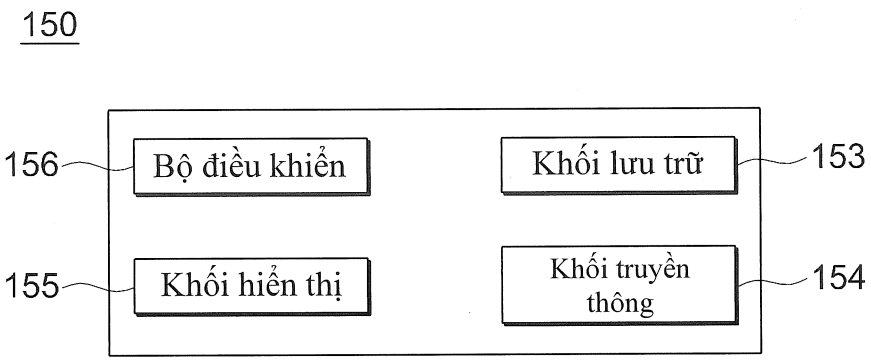
150
156
Bộ điều khiển
Khối lưu trữ
153
155
Khối hiển thị
Khối truyền thông
154

FIG. 4


Đầu cuối người dùng
Máy chủ giao dịch
Đầu cuối xác thực
Công cụ xác thực
Yêu cầu giao dịch và gửi thông tin đầu cuối
Tạo mã xác thực và yêu cầu xác thực
Tạo mã xác thực được biến đổi và yêu cầu xác minh
Tạo mã xác minh được biến đổi và gửi mã xác minh được biến đổi
Tạo mã xác minh và gửi mã xác minh
Thông báo xử lý giao dịch

FIG. 5

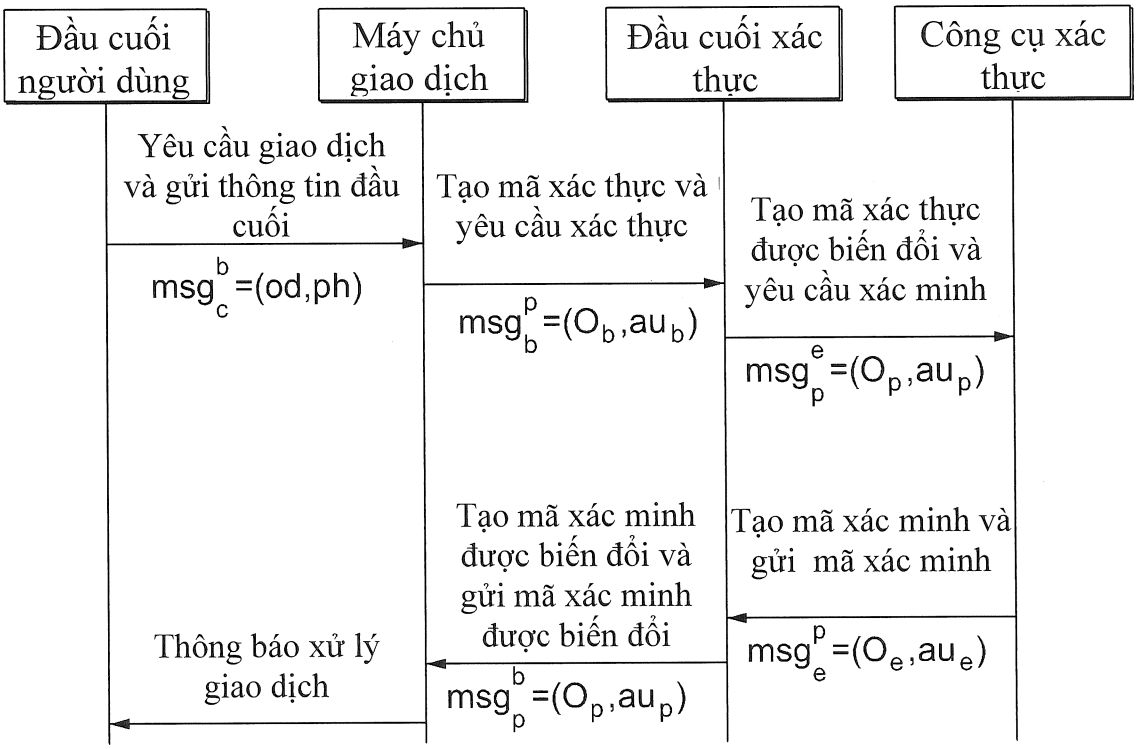
Đầu cuối người dùng
Máy chủ giao dịch
Đầu cuối xác thực
Công cụ xác thực
Yêu cầu giao dịch và gửi thông tin đầu cuối
msg_c^b=(od,ph)
Tạo mã xác thực và yêu cầu xác thực
msg_b^p=(O_b,au_b)
Tạo mã xác thực được biến đổi và yêu cầu xác minh
msg_p^e=(O_p,au_p)
Tạo mã xác minh được biến đổi và gửi mã xác minh được biến đổi
msg_p^b=(O_p,au_p)
Tạo mã xác minh và gửi mã xác minh
msg_e^p=(O_e,au_e)
Thông báo xử lý giao dịch

FIG. 6

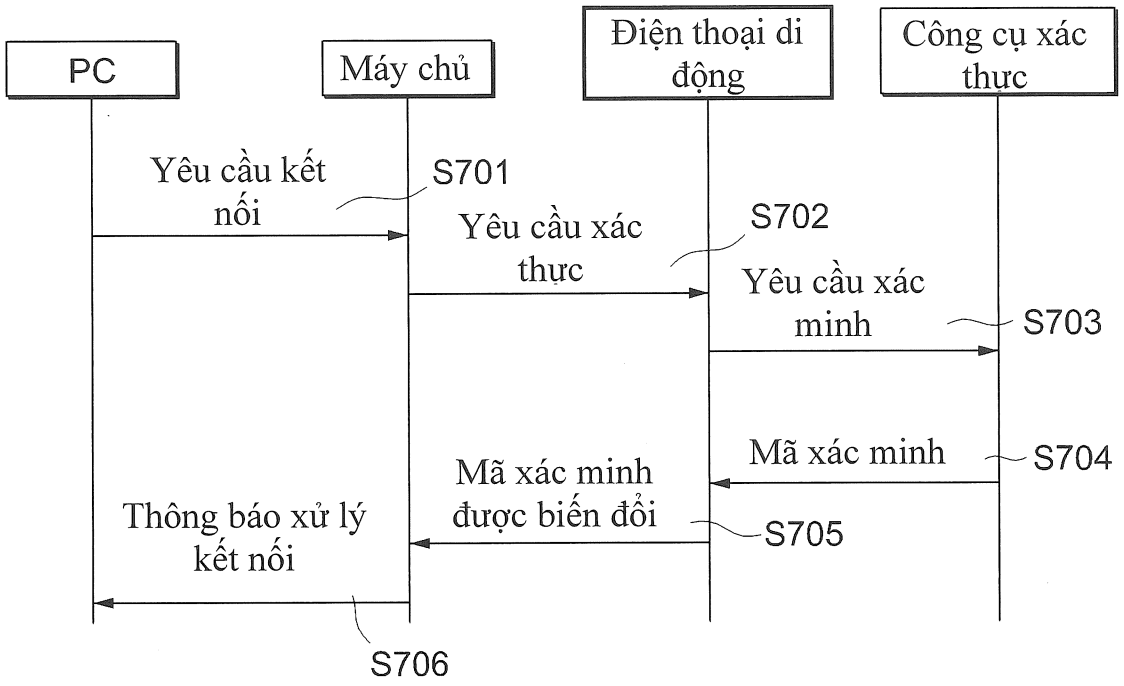
PC
Máy chủ
Điện thoại di động
Công cụ xác thực
Yêu cầu kết nối
S701
Yêu cầu xác thực
S702
Yêu cầu xác minh
S703
Mã xác minh
S704
Mã xác minh được biến đổi
S705
Thông báo xử lý kết nối
S706

FIG. 7

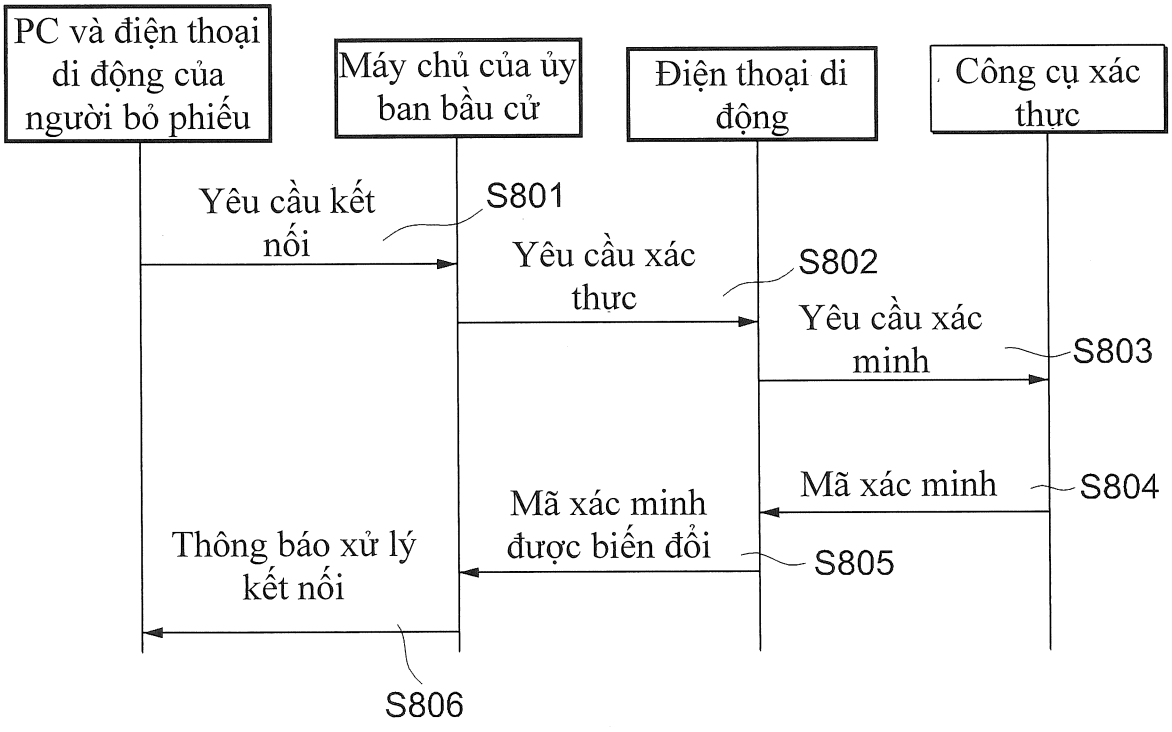
PC và điện thoại di động của người bỏ phiếu
Máy chủ của ủy ban bầu cử
Điện thoại di động
Công cụ xác thực
Yêu cầu kết nối
S801
Yêu cầu xác thực
S802
Yêu cầu xác minh
S803
Mã xác minh
S804
Mã xác minh được biến đổi
S805
Thông báo xử lý kết nối
S806

FIG. 8

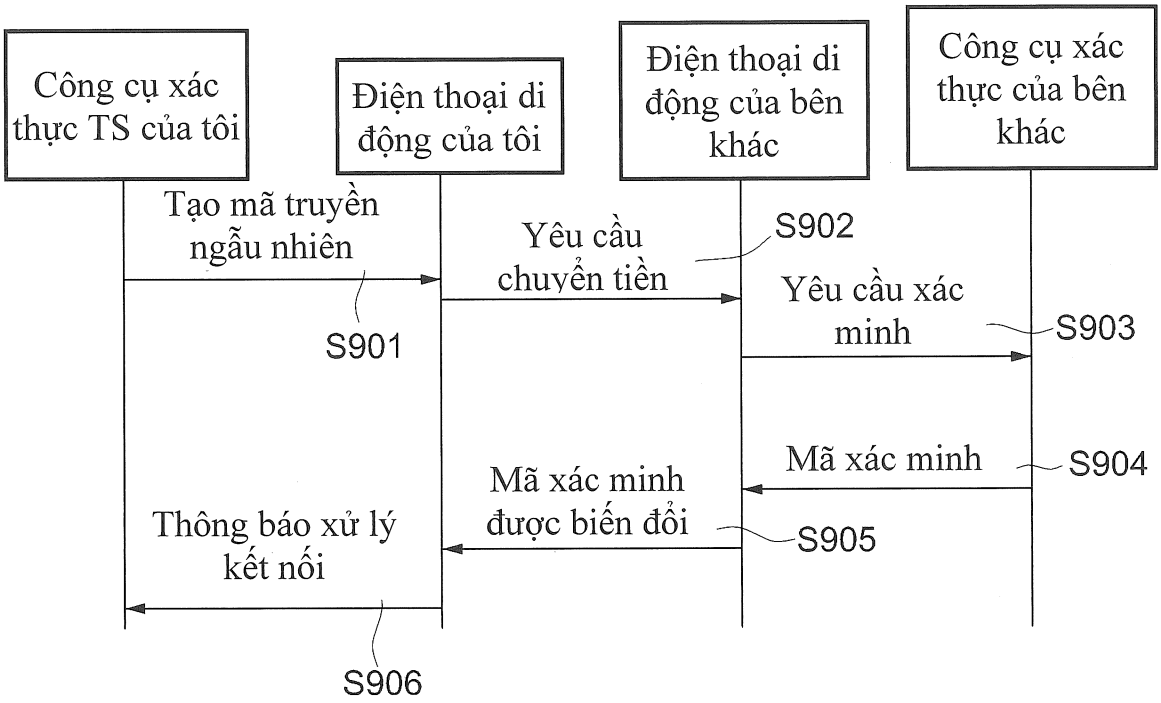
Công cụ xác thực TS của tôi
Điện thoại di động của tôi
Điện thoại di động của bên khác
Công cụ xác thực của bên khác
Tạo mã truyền ngẫu nhiên
S901
Yêu cầu chuyển tiền
S902
Yêu cầu xác minh
S903
Mã xác minh
S904
Mã xác minh được biến đổi
S905
Thông báo xử lý kết nối
S906

FIG. 9