(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) **1-0047793**

(51)[2022.01] **H04L 9/32**; G06Q 20/40; G06F 21/31; G06Q 20/36

(13) **B**

(21) 1-2022-07472
(22) 20/04/2021
(86) PCT/SG2021/050225 20/04/2021
(87) WO2021/216003 28/10/2021
(30) 10202003630V 21/04/2020 SG
(45) 25/06/2025 447
(43) 26/06/2023 423A
(73) GRABTAXI HOLDINGS PTE. LTD. (SG)
3 MEDIA CLOSE, #01-03/06, SINGAPORE 138498, SINGAPORE
(72) MEDVINSKY, Gennady (US); LINGAMALLU, Surya Anil (US); DOSHI, Hardik Bipinbhai (IN); KANAGASABAI, Prasanna (IN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) THIẾT BỊ TRUYỀN THÔNG, PHƯƠNG PHÁP ĐỂ SINH RA TIN NHẮN NGƯỜI DÙNG, PHƯƠNG PHÁP ĐỂ XÁC MINH SỰ KHẲNG ĐỊNH TRONG TIN NHẮN NGƯỜI DÙNG, VÀ PHƯƠNG TIỆN LƯU TRỮ KHÔNG CHUYỂN TIẾP

(21) 1-2022-07472

(57) Thiết bị truyền thông khách và phương pháp để sinh ra tin nhắn người dùng bao gồm sự khẳng định cho sự xác minh bởi thiết bị máy chủ từ xa được mô tả. Dữ liệu tải tin cho tin nhắn người dùng như được sinh ra bởi ứng dụng an toàn lưu trú trên thiết bị truyền thông được nhận. Sự xác thực sinh trắc học của người dùng được thực hiện như cơ chế về sự an toàn mức thứ nhất. Nếu sự xác thực sinh trắc học của người dùng là thành công, thì chữ ký số được sinh ra dựa trên tải tin tin nhắn như cơ chế về sự an toàn mức thứ hai. Chữ ký số được sinh ra sử dụng khóa chữ ký riêng được lưu trữ trong phần tử an toàn của thiết bị khách. Cơ chế về sự an toàn mức thứ ba được áp dụng nhờ xác thực tin nhắn người dùng sử dụng khóa cụ thể cho ứng dụng an toàn. Trong các sự thi hành, chữ ký số được sinh ra trong môi trường an toàn của thiết bị khách mà có sự truy nhập duy nhất đối với phần tử an toàn sau sự xác thực sinh trắc học thành công. Tin nhắn người dùng bao gồm tải tin tin nhắn và chữ ký số được sinh ra để gửi đến thiết bị máy chủ từ xa. Sự xác minh có thể được đòi hỏi trong lúc giao dịch tài chính. Phương pháp và thiết bị truyền thông máy chủ tương ứng cũng được mô tả. Phương pháp để xác minh sự khẳng định trong tin nhắn người dùng, và phương tiện lưu trữ không chuyển tiếp cũng được mô tả.

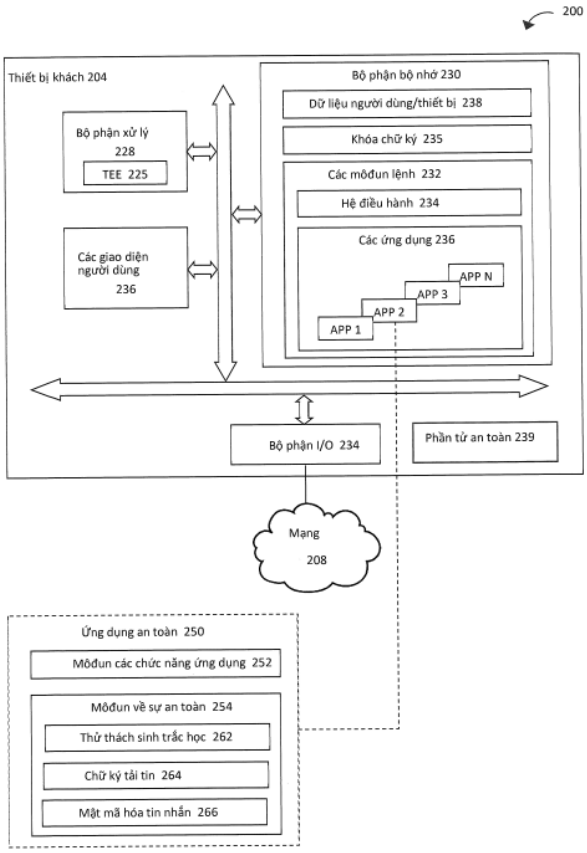

FIG. 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế nói chung đề cập đến lĩnh vực truyền thông. Một khía cạnh của sáng chế đề cập đến các kỹ thuật cho sự xác thực người dùng trong các hệ thống truyền thông. Khía cạnh khác của sáng chế đề cập đến các kỹ thuật để xác nhận tính hợp lệ các sự tryền thông. Khía cạnh khác nữa của sáng chế đề cập đến môđun về sự an toàn và ứng dụng khách được thi hành trên thiết bị khách để cung cấp các sự khẳng định cho thiết bị máy chủ cho sự xác thực hoặc sự xác nhận tính hợp lệ. Sáng chế theo cách riêng biệt, mặc dù không phải theo cách dành riêng, có thể áp dụng được đối với sự xác thực hoặc sự xác nhận tính hợp lệ của các sự khẳng định người dùng trong lúc các giao dịch tài chính qua mạng truyền thông.

Tình trạng kỹ thuật của sáng chế

Trong các hệ thống truyền thông, người dùng của thiết bị khách được đòi hỏi theo cách thường xuyên để cung cấp thông tin xác thực qua mạng truyền thông, để truyền thông và thực hiện các giao dịch trực tuyến với thiết bị máy chủ. Thông tin xác thực được sử dụng để xác minh nhận dạng của người dùng, để xác minh là người dùng là thật (genuine) và được cho quyền để truy nhập thiết bị máy chủ và thực hiện giao dịch. Sự xác thực của người dùng có thể là cần thiết cho các giao dịch mà cho phép sự truy nhập đối với dữ liệu bí mật (confidential data) qua mạng truyền thông, các giao dịch mà cho quyền sự thanh toán tài chính qua mạng truyền thông và vân vân. Thông tin xác thực có thể ở dưới dạng của các giấy chứng nhận (credentials) người dùng truyền thống, như tên người dùng và mật khẩu chỉ được biết đối với người dùng. Tuy nhiên, các giấy chứng nhận người dùng truyền thống dễ bị tấn công bởi sự ăn trộm (theft), bị bẻ khóa (cracked) và các dạng tấn công khác. Theo đó, các kỹ thuật xác thực mà chỉ dựa vào các giấy chứng nhận người dùng không xác minh theo cách tin cậy người dùng, ví dụ với mức bí mật (level of confidence) được mong muốn. Các kỹ thuật xác thực tinh vi hơn đòi hỏi

người dùng để nhập mật khẩu một lần (one-time password, OTP), mà được gửi trong thời gian thực bởi thiết bị máy chủ đến thiết bị của người dùng, để cung cấp mức thứ hai của sự xác thực người dùng. Tuy nhiên, các kỹ thuật xác thực mà dựa vào OTP có thể dễ bị tấn công bởi sự chiếm quyền điều khiển (hijack) bởi các thiết bị và các ứng dụng gian lận.

Theo đó, các kỹ thuật xác thực hiện có có thể không có năng lực để xác minh người dùng với đủ độ tin cậy hoặc sự bí mật cho một số mục đích, như các sự truyền thông bao hàm các giao dịch giá trị cao hơn hoặc các giao dịch trên các tài khoản người dùng mà được xem xét để đòi hỏi sự an toàn được tăng cường, như các giao dịch có nguy cơ cao về hoạt động gian lận.

Bản chất kỹ thuật của sáng chế

Các khía cạnh của sáng chế được trình bày trong các điểm yêu cầu bảo hộ độc lập. Một số dấu hiệu tùy chọn được định nghĩa trong các điểm yêu cầu bảo hộ phụ thuộc.

Sự thi hành của các kỹ thuật được bộc lộ ở đây có thể cung cấp các ưu điểm kỹ thuật đáng kể. Nói riêng, các kỹ thuật dẫn đến sự xác thực người dùng tin cậy hơn và sự xác nhận tính hợp lệ của thông tin về sự an toàn (security information) cho sự an toàn được cải thiện trong các hệ thống và các mạng truyền thông.

Trong các sự thi hành ví dụ, môđun về sự an toàn của ứng dụng khách trên thiết bị khách dẫn đến sự xác thực người dùng tin cậy hơn nhờ thực hiện sự xác thực sinh trắc học như điều kiện tiên quyết đối với sự sinh ra của các tin nhắn người dùng. Tải tin tin nhắn (message payload) được ký nhờ sinh ra chữ ký số sử dụng khóa riêng của cặp khóa chữ ký công khai-riêng, mà có thể chỉ được truy nhập sau sự xác thực sinh trắc học thành công. Điều này tạo ra sự kết hợp liên kết giữa thông tin sinh trắc học của người dùng và cặp khóa chữ ký bằng mật mã được sử dụng để xác nhận người gửi của tin nhắn và xác minh tính toàn vẹn của chúng. Môđun xác thực và về sự an toàn của thiết bị máy chủ, ví dụ máy chủ xác thực, có thể xác thực người gửi của tin nhắn với độ bí mật lớn hơn, đơn giản là nhờ xác nhận tính hợp lệ chữ ký được gắn với tải tin tin nhắn sử dụng khóa chữ ký công khai của cặp khóa chữ ký. Thêm nữa, sự sử dụng của cơ chế về sự an toàn

mức thứ ba như cơ chế mật mã hóa sử dụng khóa cụ thể cho ứng dụng như được mô tả ở dưới mà tận dụng khóa mật mã hóa được làm tối có thể giúp bảo đảm để cung cấp sự xác nhận tính hợp lệ là tin nhắn đã bắt nguồn từ môđun về sự an toàn thật được kết hợp với ứng dụng với độ bí mật lớn hơn, và có thể giảm bớt nguy cơ về các ứng dụng gian lận chiếm quyền điều khiển các quy trình xác thực.

Trong một số sự thi hành, chữ ký số được sinh ra trong môi trường an toàn, như Môi trường thực thi được tin tưởng, của thiết bị khách. Sự truy nhập đối với khóa chữ ký riêng được giới hạn chỉ đối với môi trường an toàn của thiết bị truyền thông. Điều này tăng cường thêm nữa sự an toàn và tính toàn vẹn của các tin nhắn người dùng được gửi bởi thiết bị khách.

Trong các sự thi hành ví dụ, môđun về sự an toàn của ứng dụng khách mật mã hóa các tin nhắn người dùng với khóa mật mã hóa, trước khi gửi đến thiết bị máy chủ. Sự giải mật mã thành công của tin nhắn người dùng được nhận bởi máy chủ xác thực sử dụng khóa giải mật mã tương ứng làm cho có khả năng có sự xác nhận tính hợp lệ là tin nhắn đã bắt nguồn từ môđun về sự an toàn thật được kết hợp với ứng dụng với độ bí mật lớn hơn.

Do đó, trong ít nhất một số sự thi hành, các kỹ thuật được bộc lộ ở đây tạo điều kiện thuận lợi cho sự xác nhận tính hợp lệ thông tin xác thực và về sự an toàn người dùng được cải thiện, dẫn đến sự an toàn được cải thiện trong các hệ thống truyền thông được so sánh với các kỹ thuật hiện có, nhờ thi hành thủ tục ba giai đoạn trong ứng dụng khách chạy trên thiết bị khách. Các chi tiết thêm nữa được mô tả ở dưới.

Trong các sự thi hành, phần chức năng của các kỹ thuật được bộc lộ ở đây có thể được thi hành trong phần mềm chạy trên thiết bị truyền thông cầm tay, như điện thoại di động (ở đây cũng được tham chiếu đến như "thiết bị người dùng" hoặc "thiết bị khách"). Phần mềm mà thi hành phần chức năng của các kỹ thuật được bộc lộ ở đây có thể được chứa trong ứng dụng khách được biết như "ứng dụng" ("app") – chương trình máy tính, hoặc sản phẩm chương trình máy tính – mà người dùng đã tải xuống từ cửa hàng trực tuyến. Khi chạy trên, ví dụ, điện thoại di động của người dùng, các dấu hiệu phần cứng của điện thoại di động có thể được sử dụng để thi hành phần chức năng được

mô tả ở dưới, như sử dụng các thành phần bộ truyền nhận của điện thoại di động để thành lập kênh truyền thông với máy chủ xác thực như được mô tả ở đây.

Mô tả vắn tắt các hình vẽ kèm theo

Các sự thi hành của sáng chế này sẽ tiếp đây được mô tả, chỉ theo cách ví dụ, và với tham chiếu đến các hình vẽ kèm theo trong đó:

Fig.1 là sơ đồ khối dưới dạng giản đồ minh họa hệ thống truyền thông bao gồm thiết bị máy chủ để xác thực người dùng của thiết bị khách phù hợp với các sự thi hành ví dụ của sáng chế này;

Fig.2 là sơ đồ khối dưới dạng giản đồ minh họa thiết bị khách bao gồm ứng dụng khách an toàn phù hợp với các sự thi hành ví dụ của sáng chế này;

Fig.3 là sơ đồ khối dưới dạng giản đồ minh họa thiết bị máy chủ bao gồm phần chức năng xác thực an toàn phù hợp với các sự thi hành ví dụ của sáng chế này;

Fig.4 là lưu đồ minh họa phương pháp cho sự kết nạp của người dùng của ứng dụng khách an toàn trong thiết bị khách phù hợp với các sự thi hành ví dụ của sáng chế này;

Fig.5 là lưu đồ minh họa phương pháp cho sự kết nạp của người dùng của ứng dụng khách an toàn trong thiết bị máy chủ phù hợp với các sự thi hành ví dụ của sáng chế này;

Fig.6 là lưu đồ minh họa phương pháp cho sự xác thực của người dùng của ứng dụng khách an toàn trong thiết bị khách phù hợp với các sự thi hành ví dụ của sáng chế này; và

Fig.7 là lưu đồ minh họa phương pháp cho sự xác thực của người dùng của ứng dụng khách an toàn trong thiết bị máy chủ phù hợp với các sự thi hành ví dụ của sáng chế này.

Trên các hình vẽ, các ký hiệu tham chiếu tương tự được sử dụng để biểu thị các dấu hiệu tương tự.

Mô tả chi tiết sáng chế

Tham chiếu trước tiên đến Fig.1, hệ thống truyền thông 100 được minh họa. Hệ thống truyền thông 100 bao gồm máy máy chủ truyền thông (thiết bị máy chủ) 102, máy truyền thông khách thứ nhất (thiết bị khách thứ nhất) 104 và máy truyền thông khách thứ hai (thiết bị khách thứ hai) 106 được kết nối với mạng truyền thông 108 (ví dụ Internet) qua các liên kết truyền thông tương ứng 110, 112, 114 thi hành, ví dụ, internet hoặc các giao thức truyền thông dữ liệu khác. Mạng truyền thông 108 có thể bao gồm mạng truyền thông có dây và/hoặc không dây bất kỳ hoặc sự kết hợp của các mạng. Theo đó, các thiết bị khách 104, 106 có thể có năng lực để truyền thông với thiết bị máy chủ 102 qua những mạng truyền thông khác nhau, như các mạng điện thoại chuyển mạch công cộng (các mạng PSTN), các mạng truyền thông dạng ô di động (các mạng 3G, 4G hoặc LTE), các mạng có dây và không dây cục bộ (các mạng LAN, WLAN, WiFi) và tương tự.

Thiết bị máy chủ 102 có thể là máy chủ đơn như được minh họa dưới dạng giản đồ trên Fig.1, hoặc phần chức năng của nó có thể được phân bố qua nhiều máy chủ. Ví dụ, thiết bị máy chủ 102 có thể bao gồm nhiều máy chủ gồm có, ví dụ, máy chủ xác thực để cung cấp phần chức năng về sự an toàn/sự xác thực người dùng, máy chủ tài khoản để cung cấp phần chức năng quản lý tài khoản người dùng và máy chủ web để cung cấp phần chức năng xử lý giao dịch người dùng. Một sự sắp xếp như vậy được minh họa trên Fig.3, mà được thảo luận chi tiết thêm nữa ở dưới. Trong ví dụ trên Fig.1, thiết bị máy chủ 102 có thể bao gồm một số những thành phần riêng lẻ gồm có, nhưng không được giới hạn vào, một hoặc nhiều bộ vi xử lý 116, bộ nhớ 118 (ví dụ bộ nhớ khả biến như RAM) cho sự tải của các lệnh có thể thực thi 120, các lệnh có thể thực thi định nghĩa phần chức năng của máy chủ 102 tiến hành dưới sự điều khiển của bộ xử lý 116. Thiết bị máy chủ 102 cũng bao gồm môđun đầu vào/đầu ra (input/output, I/O) 122 cho phép máy chủ truyền thông qua mạng truyền thông 108. Giao diện người dùng 124 được cung cấp cho sự điều khiển người dùng và có thể bao gồm, ví dụ, các thiết bị ngoại vi tính toán như các màn hình hiển thị, các bàn phím máy tính và tương tự. Thiết bị máy chủ 102 có thể cũng bao gồm cơ sở dữ liệu 126, mục đích của nó sẽ dễ dàng trở nên rõ ràng từ sự thảo luận sau đây.

Thiết bị khách thứ nhất 104 có thể bao gồm một số những thành phần riêng lẻ gồm có, nhưng không được giới hạn vào, một hoặc nhiều bộ vi xử lý 128, bộ nhớ 130 (ví dụ bộ nhớ khả biến như RAM) cho sự tải của các lệnh có thể thực thi 132, các lệnh có thể thực thi định nghĩa phần chức năng mà thiết bị khách 104 tiến hành dưới sự điều khiển của bộ xử lý 128. Thiết bị khách thứ nhất 104 cũng bao gồm môđun I/O 134 cho phép thiết bị khách 104 truyền thông qua mạng truyền thông 108. Các giao diện người dùng 136 được cung cấp cho sự điều khiển người dùng. Nếu thiết bị khách thứ nhất 104 là, nói là, thiết bị truyền thông khả chuyển như điện thoại thông minh hoặc thiết bị bảng (tablet device), thì các giao diện người dùng 136 sẽ có bộ hiển thị panen chạm như phổ biến trong nhiều điện thoại thông minh và các thiết bị cầm tay khác. Như một sự lựa chọn, nếu thiết bị khách thứ nhất là, nói là, máy tính để bàn hoặc laptop, thì giao diện người dùng có thể có, ví dụ, các thiết bị ngoại vi tính toán như các màn hình hiển thị, các bàn phím máy tính và tương tự. Các giao diện người dùng 136 có thể cũng bao gồm micrô và tương tự.

Thiết bị khách thứ hai 106 có thể là, ví dụ, điện thoại thông minh hoặc thiết bị bảng với kiến trúc phần cứng giống hoặc tương tự với kiến trúc phần cứng của thiết bị khách thứ nhất 104. Trong các sự thi hành ví dụ, thiết bị khách thứ nhất 104 có thể là thiết bị người dùng của người tiêu dùng của dịch vụ được kết hợp với thiết bị máy chủ 102, và thiết bị khách thứ hai 106 có thể là thiết bị người dùng của nhà cung cấp dịch vụ của dịch vụ được kết hợp với thiết bị máy chủ 102. Trong các sự thi hành ví dụ khác, các thiết bị khách thứ nhất và thứ hai 102, 104 có thể là các thiết bị người dùng của các hạng mục giống hoặc khác nhau của người dùng được kết hợp với một hoặc nhiều phần chức năng của thiết bị máy chủ 102.

Fig.2 minh họa thiết bị khách 204 phù hợp với các sự thi hành ví dụ của sáng chế này. Ví dụ, thiết bị khách 204 có thể được sử dụng như thiết bị khách thứ nhất 106 hoặc thiết bị khách thứ hai 106 của hệ thống truyền thông 100 được minh họa trên Fig.1. Thiết bị khách 204 bao gồm bộ phận xử lý 228, bộ phận bộ nhớ 230, bộ phận I/O 234 và các giao diện người dùng 236, như được mô tả ở trên trong sự liên quan đến Fig.1. Thêm vào, thiết bị khách 204 có thể bao gồm các thành phần khác (không được thể hiện) điển hình là được gồm có trong thiết bị truyền thông khả chuyển, như môđun truyền thông

tiếng nói, camera, gia tốc kế, bộ định vị vị trí (ví dụ, môđun hệ thống vệ tinh dẫn đường toàn cầu) và tương tự.

Bộ phận bộ nhớ 230 lưu trữ nhiều môđun lệnh 232 bao gồm các lệnh có thể thực thi gồm có hệ điều hành 234 và các ứng dụng khách ("các ứng dụng" ("apps")) 236. Thêm vào, bộ phận bộ nhớ 230 lưu trữ dữ liệu người dùng và thiết bị 238. Hệ điều hành 234 quản lý sự vận hành tổng thể của thiết bị khách 204 và cung cấp các dịch vụ chung cho các ứng dụng khách 236. Phù hợp với sáng chế này, hệ điều hành 234 bao gồm phần chức năng xác thực sinh trắc học cho sự an toàn thiết bị, mà giới hạn sự truy nhập đối với thiết bị khách 204, ví dụ, đối với người dùng được xác thực về sinh trắc học đơn mà đã cung cấp thông tin sinh trắc học của họ trên thiết lập hoặc sau đó. Các ví dụ của phần chức năng xác thực sinh trắc học của hệ điều hành 234 gồm có sự nhận biết dấu vân tay, sự nhận biết khuôn mặt, sự nhận biết mống mắt/võng mạc và tương tự. Người dùng có thể ban đầu cung cấp thông tin sinh trắc học sử dụng, ví dụ, camera của thiết bị khách 204 hoặc màn hình chạm của thiết bị khách 204 kết hợp bộ quét dấu vân tay. Các hệ điều hành di động, như Android và iOS của Apple Inc., điển hình là gồm có ít nhất một phần chức năng xác thực sinh trắc học thêm vào phần chức năng xác thực truyền thống dựa trên các giấy chứng nhận người dùng cho sự an toàn của thiết bị khách 204. Thiết bị khách 204 bao gồm thêm nữa phần tử an toàn 239, được thảo luận chi tiết thêm nữa ở dưới. Trong khi phần tử an toàn 239 có thể được thi hành trong hoặc là phần cứng hoặc phần mềm, trong ví dụ trên Fig.2, nó được thi hành trong phần cứng.

Các ứng dụng khách 236 có thể bao gồm các ứng dụng di động riêng lẻ mà cung cấp các chức năng người dùng cụ thể trong thiết bị khách 204. Các ứng dụng khách 236 có thể cũng bao gồm các ứng dụng web mà truyền thông với thiết bị máy chủ (không được thể hiện trên hình vẽ này) qua mạng để cung cấp các chức năng người dùng cụ thể mà có thể bao hàm các sự truyền thông an toàn, các giao dịch trực tuyến và tương tự như được mô tả ở đây. Các ứng dụng khách 236 có thể được cài đặt trước trong thiết bị khách 236 bởi người bán, hoặc có thể được tải xuống và được cài đặt bởi người dùng từ cái được gọi là "Cửa hàng ứng dụng" ("App store").

Trong lúc sự vận hành của thiết bị khách 204, bộ phận xử lý 228 thực thi các lệnh của hệ điều hành 234 và có thể thực thi một hoặc nhiều ứng dụng khách 236, được khởi chạy (launched) bởi người dùng và chạy trên thiết bị khách 204, dưới sự điều khiển của hệ điều hành 234. Bộ phận xử lý 228 có thể gồm có một hoặc nhiều bộ xử lý trung tâm, như bộ vi xử lý, gồm có Môi trường thực thi được tin tưởng (Trusted Execution Environment, TEE) 225. TEE 225 bao gồm môi trường thực thi được cách ly mà cung cấp các dấu hiệu về sự an toàn như được biết trong lĩnh vực. Bộ phận xử lý 228 có thể cũng bao gồm các bộ xử lý khác như bộ xử lý đồ họa, bộ xử lý hình ảnh và vân vân (không được thể hiện).

Thiết bị khách 204 được minh họa được cài đặt với ứng dụng an toàn 250, mà điển hình là được tải xuống và được cài đặt bởi người dùng như được mô tả ở trên, phù hợp với sáng chế này. Nói riêng, ứng dụng an toàn 250 bao gồm môđun các chức năng ứng dụng 252 và môđun về sự an toàn 254. Môđun các chức năng ứng dụng 252 bao gồm các lệnh để thực thi phần chức năng của ứng dụng khách (nghĩa là, các chức năng ứng dụng), mà gồm có các sự truyền thông dữ liệu với thiết bị máy chủ được kết hợp (không được thể hiện trên hình vẽ này) qua bộ phận I/O 234 qua mạng 208. Các ví dụ của các chức năng ứng dụng gồm có các ứng dụng mua sắm trực tuyến, các ứng dụng đặt dịch vụ trực tuyến, các ứng dụng ngân hàng trực tuyến và tương tự. Môđun về sự an toàn 254 bao gồm công cụ về sự an toàn được tích hợp mà thực thi các lệnh mà cung cấp phần chức năng về sự an toàn được dành riêng cho ứng dụng an toàn 250. Trong ứng dụng an toàn 250 được minh họa, môđun về sự an toàn 254 thi hành cơ chế về sự an toàn được tạo ba lớp cho sự cung cấp của thông tin xác thực và về sự an toàn người dùng trong các sự truyền thông dữ liệu được gửi đến thiết bị máy chủ. Nói riêng, môđun thử thách sinh trắc học 262 cung cấp cơ chế về sự an toàn mức thứ nhất, môđun chữ ký tải tin 264 cung cấp cơ chế về sự an toàn mức thứ hai và môđun mật mã hóa tin nhắn 266 cung cấp cơ chế về sự an toàn mức thứ ba. Môđun thử thách sinh trắc học 262, môđun chữ ký tải tin 264 và môđun mật mã hóa tin nhắn 266 bao gồm dữ liệu và các lệnh như được mô tả ở dưới. Trong sự sắp xếp lựa chọn, cơ chế về sự an toàn mức thứ ba có thể được cung cấp bởi ứng dụng của chữ ký số thứ hai. Đây có thể là giải pháp hợp hơn nếu tính bí mật của tin nhắn người dùng – như có thể được cung cấp nếu cơ chế về sự an toàn mức thứ ba là cơ chế mật mã hóa – không được đòi hỏi.

Môđun về sự an toàn 254 thi hành thủ tục xác thực an toàn khi người dùng vận hành ứng dụng an toàn 250, và, nói riêng, gửi yêu cầu giao dịch ứng dụng hoặc sự truyền thông tương tự đến thiết bị máy chủ được kết hợp đòi hỏi sự xác thực người dùng. Nói riêng, môđun các chức năng ứng dụng 252 có thể khởi đầu sự sinh ra của tin nhắn yêu cầu giao dịch để đáp lại dữ liệu được nhập bởi người dùng có liên quan đến giao dịch được yêu cầu. Ví dụ, giao dịch có thể tìm để đặt dịch vụ ở thời gian và địa điểm riêng biệt, và như vậy người dùng có thể nhập dữ liệu định rõ dịch vụ, thời gian và địa điểm được đòi hỏi. Môđun các chức năng ứng dụng 252 có thể xác định là tin nhắn yêu cầu giao dịch riêng biệt đòi hỏi sự xác thực an toàn trước khi yêu cầu giao dịch được gửi đến thiết bị máy chủ được kết hợp. Do đó, môđun các chức năng ứng dụng 252 có thể khởi động thủ tục xác thực an toàn của môđun về sự an toàn 254.

Trong giai đoạn thứ nhất của thủ tục xác thực, môđun thử thách sinh trắc học 262 cung cấp thử thách sinh trắc học cho người dùng của thiết bị khách 204. Nói riêng, môđun thử thách sinh trắc học 262 có thể gọi ra phần chức năng xác thực sinh trắc học của hệ điều hành 234, như được mô tả ở trên. Phần chức năng xác thực sinh trắc học có thể cung cấp giao diện người dùng đồ họa (graphical user interface, GUI) yêu cầu người dùng để cung cấp thông tin sinh trắc học, so sánh thông tin sinh trắc học được cung cấp bởi người dùng với thông tin sinh trắc học được lưu trữ trước, và, nếu có sự so khớp, thì xác nhận tính hợp lệ nhận dạng của người dùng. Nếu nhận dạng của người dùng được xác nhận tính hợp lệ, thì thủ tục xác thực tiến hành giai đoạn thứ hai.

Trong giai đoạn thứ hai của thủ tục xác thực, môđun chữ ký tải tin 264 cung cấp tải tin của yêu cầu giao dịch cho TEE 225. Tải tin gồm có dữ liệu được cung cấp bởi môđun các chức năng ứng dụng 252. Tải tin có thể gồm có thêm nữa dữ liệu bổ sung cho sự an toàn được tăng cường, gồm có sự tham chiếu khóa (như được mô tả ở dưới) và sự kết hợp của dữ liệu cụ thể cho người dùng khác, như mã thông báo đăng nhập (login token), mà là duy nhất đối với ứng dụng an toàn/người dùng 250. TEE 225 thêm nonce và dấu thời gian vào tải tin và ký theo cách an toàn tải tin với "khóa chữ ký" riêng, như khóa riêng của cặp khóa riêng-công khai Viết mật mã đường cong elliptic (Elliptic Curve Cryptography, ECC) hoặc tương tự. Khóa ECC riêng là duy nhất đối với ứng dụng an toàn 250 và được sinh ra trong lúc thủ tục kết nạp người dùng ban đầu với thiết

bị máy chủ mà cung cấp sự tham chiếu khóa được đề cập ở trên. Thủ tục kết nạp được mô tả chi tiết thêm nữa ở dưới. Khóa ECC riêng được lưu trữ trong phần tử an toàn của thiết bị khách 204. Như được biết, phần tử an toàn 239 bao gồm thành phần an toàn được kết hợp với Môi trường thực thi được tin tưởng. Khóa ECC riêng/phần tử an toàn là chỉ có thể truy nhập được đối với TEE 225 sau sự xác thực sinh trắc học thành công trong giai đoạn thứ nhất. Theo đó, khóa ECC riêng là không thể truy nhập được đối với phần bất kỳ của ứng dụng an toàn 250, gồm có môđun chữ ký tải tin 264. TEE 225 cung cấp tải tin được ký cho môđun mật mã hóa tin nhắn 266 cho giai đoạn thứ ba.

Trong giai đoạn thứ ba của thủ tục xác thực, môđun mật mã hóa tin nhắn 266 mật mã hóa tải tin được ký được cung cấp bởi TEE 225 với "khóa mật mã hóa", như khóa thứ nhất của cặp khóa mật mã hóa được kết hợp với thiết bị máy chủ. Khóa mật mã hóa được gồm có trong ứng dụng an toàn 250 được tải xuống đến thiết bị khách 204, và như vậy có thể được xem xét như "khóa mật mã hóa dịch vụ". Trong các sự thi hành ví dụ, khóa mật mã hóa dịch vụ được làm tối trong ứng dụng an toàn 250 nhờ các kỹ thuật mã hóa tốc ký phù hợp để mã hóa theo cách an toàn dữ liệu mật. Theo đó, khóa mật mã hóa dịch vụ được sử dụng cho sự mật mã hóa bởi môđun mật mã hóa tin nhắn 266 là không dễ dàng có thể truy nhập được từ mã của ứng dụng an toàn 250 hoặc dễ bị tấn công bởi các người tấn công. Như người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rõ, khóa mật mã hóa dịch vụ bởi vậy là điều bí mật, nhưng là chung đối với tất cả các phiên bản thật của ứng dụng an toàn 250 chạy trên các thiết bị khách khác nhau để mật mã hóa các tin nhắn được gửi đến thiết bị máy chủ được kết hợp.

Vào lúc sự hoàn thành của giai đoạn thứ ba của thủ tục xác thực, tin nhắn yêu cầu giao dịch được ký và được mật mã hóa được gửi bởi ứng dụng an toàn 250 đến thiết bị máy chủ được kết hợp cho sự xác thực tin cậy của người dùng và sự xác nhận tính hợp lệ của thiết bị khách 204 và/hoặc ứng dụng an toàn 250 như được mô tả ở đây.

Do đó, thủ tục xác thực được tiến hành bởi môđun về sự an toàn 254 phù hợp với các sự thi hành ví dụ được mô tả cung cấp sự an toàn được tăng cường cho các yêu cầu giao dịch người dùng được gửi bởi ứng dụng an toàn 250. Nói riêng, giai đoạn thứ nhất xác thực người dùng nhờ xác nhận tính hợp lệ nhận dạng dựa trên thông tin sinh trắc

học sử dụng phần chức năng hệ điều hành của thiết bị khách 204. Theo đó, thông tin sinh trắc học được giữ theo cách an toàn trên thiết bị khách 204, và sự kết hợp tin tưởng được tạo ra giữa người dùng, thiết bị khách 204 và ứng dụng an toàn 250. Giai đoạn thứ hai có thể thêm dữ liệu thiết bị và/hoặc người dùng duy nhất vào tải tin, và TEE 225 giành được sự truy nhập đối với khóa ECC riêng an toàn và ký tải tin. Theo đó, giai đoạn thứ hai cung cấp sự an toàn được ủng hộ bởi phần cứng cho tải tin được ký sau sự xác thực của người dùng. Giai đoạn thứ ba mật mã hóa tin nhắn được ký sử dụng khóa mật mã hóa dịch vụ được làm tối. Điều này bảo đảm là tin nhắn có thể chỉ đến từ ứng dụng an toàn 250 thật, và giảm bớt nguy cơ về các ứng dụng gian lận chiếm quyền điều khiển các quy trình xác thực.

Fig.3 minh họa thiết bị máy chủ 302 phù hợp với các sự thi hành ví dụ của sáng chế này. Ví dụ, thiết bị máy chủ 302 có thể được kết hợp với ứng dụng an toàn 250 của thiết bị khách 204 được minh họa trên Fig.2. Thiết bị máy chủ 302 bao gồm bộ phận xử lý 316, bộ phận bộ nhớ 318, bộ phận I/O 322, các giao diện người dùng 324 và cơ sở dữ liệu 326, như được mô tả ở trên trong sự liên quan đến Fig.1.

Bộ phận bộ nhớ 318 lưu trữ nhiều môđun lệnh 320 bao gồm các lệnh có thể thực thi để thực hiện các sự vận hành máy chủ mà xử lý các sự truyền thông dữ liệu, như các tin nhắn yêu cầu giao dịch người dùng, được nhận từ các ứng dụng an toàn chạy trên các thiết bị khách (không được thể hiện trên hình vẽ này) qua mạng 308 qua bộ phận I/O 322. Nói riêng, các môđun lệnh 320 gồm có môđun xử lý giao dịch 342, môđun quản lý tài khoản 344 và môđun xác thực và về sự an toàn 360.

Trong lúc sự vận hành của thiết bị máy chủ 302, bộ phận xử lý 316 thực thi các lệnh của môđun xử lý giao dịch 342, môđun quản lý tài khoản 344 và môđun xác thực và về sự an toàn 360 để đáp lại các tin nhắn yêu cầu giao dịch người dùng và các sự truyền thông khác được nhận từ các thiết bị khách (không được thể hiện trên hình vẽ này) qua bộ phận I/O 322 qua mạng 308. Bộ phận xử lý 316 có thể gồm có một hoặc nhiều bộ xử lý trung tâm, như bộ vi xử lý.

Môđun xử lý giao dịch 342 thực hiện sự xử lý được kết hợp với các sự truyền thông gồm có các yêu cầu giao dịch người dùng được nhận từ các ứng dụng an toàn, và

sinh ra các sự đáp lại giao dịch, cho phù hợp. Môđun quản lý tài khoản 342 thực hiện sự xử lý để tạo ra và quản lý các tài khoản người dùng, mà được lưu trữ trong cơ sở dữ liệu 326. Ví dụ, môđun quản lý tài khoản 344 có thể thực hiện sự xử lý để tạo ra và/hoặc quản lý tài khoản người dùng, như trong lúc thủ tục kết nạp như được mô tả ở dưới với tham chiếu đến Fig.4. Thêm vào, môđun quản lý tài khoản 344 có thể kết hợp thông tin có liên quan đến các yêu cầu giao dịch người dùng được nhận và các sự truyền thông khác với các tài khoản người dùng, như được mô tả ở dưới với tham chiếu đến Fig.5. Môđun xác thực và về sự an toàn 360 có thể thực hiện sự xử lý được kết hợp với các chức năng xác thực và về sự an toàn trong sự liên quan đến các yêu cầu giao dịch người dùng được nhận. Ví dụ, môđun xác thực và về sự an toàn 360 có thể xác minh các giấy chứng nhận đăng nhập được kết hợp với người dùng. Thêm vào, môđun xác thực và về sự an toàn 360 có thể thực hiện các quy trình xác thực và về sự an toàn thêm nữa trên các yêu cầu giao dịch người dùng được nhận, như được mô tả ở đây.

Phù hợp với sáng chế này, môđun xác thực và về sự an toàn 360 thi hành thủ tục về sự an toàn để xác nhận tính hợp lệ thông tin xác thực và về sự an toàn trong các sự truyền thông dữ liệu, như các yêu cầu giao dịch người dùng, được nhận từ ứng dụng an toàn chạy trên thiết bị khách như được mô tả ở đây. Nói riêng, môđun xác thực và về sự an toàn 360 thi hành thủ tục về sự an toàn khi nhận các yêu cầu giao dịch nhất định đòi hỏi sự xác thực người dùng và sự xác nhận tính hợp lệ. Ví dụ, yêu cầu giao dịch như vậy có thể được sinh ra bởi ứng dụng an toàn 250 của thiết bị khách 204 trên Fig.2, mà đã được xử lý phù hợp với các giai đoạn thứ nhất, thứ hai và thứ ba của thủ tục xác thực được mô tả ở trên được tiến hành bởi môđun về sự an toàn 254.

Do đó, thủ tục về sự an toàn của môđun xác thực và về sự an toàn 360 của thiết bị máy chủ 302 phản ánh các khía cạnh của thủ tục xác thực ba giai đoạn của môđun về sự an toàn 254 của ứng dụng an toàn 250 của thiết bị khách 204. Nói riêng, môđun xác thực và về sự an toàn 360 bao gồm môđun giải mật mã tin nhắn 376, môđun nhận dạng người dùng 372, môđun xác minh chữ ký 374 và môđun xác nhận tính hợp lệ về sự an toàn 378.

Khi thiết bị máy chủ 302 nhận sự truyền thông để xác nhận tính hợp lệ thông tin xác thực và về sự an toàn, như yêu cầu giao dịch người dùng được mật mã hóa và được ký, tin nhắn được cho đi đến môđun xác thực và về sự an toàn 360 để thực hiện thủ tục về sự an toàn.

Trong giai đoạn thứ nhất của thủ tục về sự an toàn, môđun giải mật mã tin nhắn 376 giải mật mã tin nhắn với khóa thứ hai của cặp khóa mật mã hóa được mô tả ở trên, mà chỉ được biết đối với thiết bị máy chủ 320. Khóa thứ hai có thể được xem xét như "khóa giải mật mã dịch vụ", do nó được sử dụng để giải mật mã các tin nhắn được nhận từ tất cả các phiên bản của ứng dụng an toàn được kết hợp chạy trên các thiết bị khách khác nhau. Sự giải mật mã thành công của tải tin tin nhắn cung cấp sự bảo đảm là tin nhắn đã đến từ ứng dụng an toàn thật, vì khóa mật mã hóa dịch vụ được sử dụng cho sự mật mã hóa được làm tối. Tải tin được giải mật mã gồm có dữ liệu về sự an toàn gồm có sự tham chiếu khóa. Tải tin được giải mật mã có thể gồm có một hoặc nhiều dữ liệu cụ thể cho người dùng khác, như mã thông báo đăng nhập, mà là duy nhất đối với ứng dụng an toàn/người dùng, như được mô tả ở trên.

Trong giai đoạn thứ hai của thủ tục về sự an toàn, môđun xác minh chữ ký 374 tìm kiếm khóa chữ ký công khai, như khóa công khai của cặp khóa riêng-công khai Viết mật mã đường cong elliptic (Elliptic Curve Cryptography, ECC) được mô tả ở trên, và xác minh chữ ký được áp dụng đối với tải tin. Sự xác minh chữ ký xác nhận là khóa ECC riêng đã ký tải tin tin nhắn. Hơn nữa, trong các sự thi hành được mô tả ở đây, sự xác minh chữ ký xác nhận là tải tin đã được ký theo cách an toàn bởi TEE sử dụng phần tử an toàn của thiết bị khách, như được mô tả ở dưới. Theo đó, sự xác minh chữ ký xác minh thiết bị khách và ứng dụng an toàn mà đã ký tin nhắn, và, hệ quả là, xác thực theo cách tin cậy người dùng do sự tin tưởng trong thủ tục xác thực sinh trắc học nhất thiết được thực hiện bởi ứng dụng an toàn của thiết bị khách trước chữ ký.

Trong giai đoạn thứ ba của thủ tục về sự an toàn, mà có thể xảy ra ở thời gian bất kỳ sau giai đoạn thứ nhất, môđun nhận dạng người dùng 372 có thể xác minh người dùng, và theo đó nhận dạng tài khoản của người dùng, ví dụ từ dữ liệu cụ thể cho người

dùng được giải mật mã như các mã thông báo đăng nhập, nhận dạng của ứng dụng an toàn và/hoặc thiết bị khách.

Trong giai đoạn thứ tư của thủ tục về sự an toàn, mà có thể cũng xảy ra ở thời gian bất kỳ sau giai đoạn thứ nhất, môđun về sự an toàn 378 có thể thực hiện các kiểm tra về sự an toàn khác như kiểm tra tính hợp lệ của nonce, và tính chất mới của tin nhắn sử dụng dấu thời gian, được gồm có trong tải tin tin nhắn được ký.

Trong các sự thi hành ở trên, hai cặp khóa được sử dụng cho các sự truyền thông dữ liệu an toàn giữa ứng dụng an toàn chạy trên thiết bị khách và thiết bị máy chủ được kết hợp. Một trong các cặp khóa là cặp "khóa chữ ký" được mô tả ở trên (điển hình là cặp khóa bất đối xứng) và cặp khóa khác là cặp "khóa dịch vụ/mật mã hóa" được mô tả ở trên (cặp khóa đối xứng hoặc bất đối xứng). Một trong hai cặp khóa – cặp khóa "dịch vụ" – được xác định trước và được gồm có trong ứng dụng khách an toàn, và khóa khác trong hai cặp khóa – cặp khóa "chữ ký" – được sinh ra bởi thiết bị khách trong lúc thủ tục kết nạp như được mô tả ở dưới.

Fig.4 là lưu đồ minh họa phương pháp 400 cho sự kết nạp với thiết bị máy chủ được kết hợp với ứng dụng khách an toàn phù hợp với các sự thi hành ví dụ của sáng chế này. Ví dụ, phương pháp 400 có thể được thực hiện bởi ứng dụng an toàn 250 chạy trên thiết bị khách 204 trên Fig.2.

Phương pháp kết nạp 400 được thực hiện sau sự cài đặt của ứng dụng ("app") an toàn trên thiết bị khách và trước sự sử dụng đầu tiên bởi người dùng. Như được chỉ báo ở trên, ứng dụng an toàn có thể được cài đặt trước trên thiết bị khách hoặc được tải xuống từ cửa hàng ứng dụng. Phù hợp với các sự thi hành ví dụ, ứng dụng an toàn gồm có khóa mật mã hóa dịch vụ, mà được làm tối như được mô tả ở trên, để được sử dụng bởi ứng dụng an toàn để mật mã hóa các sự truyền thông dữ liệu được gửi đến thiết bị máy chủ. Để dễ dàng cho sự mô tả, trong ví dụ sau đây, nó được giả định là người dùng đã thiết lập tài khoản người dùng với thiết bị máy chủ được kết hợp với ứng dụng an toàn, và như vậy có thể giành được sự truy nhập đối với tài khoản sử dụng các giấy chứng nhận đăng nhập thông thường.

Phương pháp 400 bắt đầu ở bước 405. Ví dụ, phương pháp 400 có thể bắt đầu để đáp lại người dùng khởi chạy ứng dụng an toàn trên thiết bị khách cho lần đầu tiên và tương tác với giao diện người dùng đồ họa (graphical user interface, GUI) của màn hình kết nạp của ứng dụng an toàn.

Ở bước 410, người dùng đăng nhập vào tài khoản người dùng của họ với thiết bị máy chủ được kết hợp. Ví dụ, người dùng có thể nhập các giấy chứng nhận đăng nhập, như tên người dùng và mật khẩu, mà có thể được xác minh bởi môđun quản lý tài khoản được kết hợp với thiết bị máy chủ. Thêm vào, mật khẩu một lần có thể được gửi đến người dùng và được nhập thành công để hoàn thành thủ tục đăng nhập. Vào lúc sự hoàn thành thành công của thủ tục đăng nhập, phương pháp tiến hành bước 420.

Ở bước 420, người dùng cung cấp thông tin cho sự xác thực yếu tố thứ hai, cho mục đích để xác nhận tính hợp lệ sự có mặt của người dùng. Nói riêng, người dùng có thể cung cấp thông tin nhận dạng yếu tố thứ hai đủ để khẳng định là người dùng là có mặt, như nhập số nhận dạng cá nhân (personal identification number, PIN) duy nhất chỉ được biết đối với người dùng hoặc chụp ảnh "ảnh tự chụp" ("selfie"). Điều này có thể được sử dụng như sự xác thực mức thứ hai đối với sự xác thực sinh trắc học như được mô tả ở đây.

Ở bước 430, người dùng thực hiện sự xác thực sinh trắc học trên thiết bị khách để kết nạp cho sự xác thực sinh trắc học như được mô tả ở đây. Nói riêng, người dùng được hỏi để cung cấp thông tin xác thực sinh trắc học cho quy trình xác thực sinh trắc học của hệ điều hành của thiết bị khách như được mô tả ở trên. Nếu sự xác thực sinh trắc học là thành công, thì phương pháp tiến hành bước 440.

Ở bước 440, phương pháp sinh ra cặp "khóa chữ ký" bất đối xứng, như cặp khóa ECC như được mô tả ở trên. Bước 440 lưu trữ khóa ECC riêng trong phần tử an toàn của thiết bị khách, mà chỉ có thể truy nhập được đối với TEE của thiết bị khách theo sau sự xác thực sinh trắc học thành công và là không thể truy nhập được đối với các thành phần khác của thiết bị khách. Khóa ECC riêng/phần tử an toàn được lưu trữ cho các mục đích để ký tải tin tin nhắn. Trong các sự thi hành ví dụ, khóa ECC riêng/phần tử an toàn được làm mất hiệu lực nếu đặc tính bất kỳ trong các đặc tính về sự an toàn của thiết bị

khách được thay đổi, như PIN thiết bị và thông tin sinh trắc học người dùng được sử dụng để giành được sự truy nhập đối với thiết bị khách.

Ở bước 450, phương pháp sinh ra tin nhắn yêu cầu kết nạp. Tin nhắn yêu cầu kết nạp gồm có tải tin bao gồm khóa ECC công khai được sinh ra trong bước 440 và thông tin nhận dạng yếu tố thứ hai được cung cấp bởi người dùng trong bước 420. Tải tin có thể gồm có thông tin bổ sung như nonce và dấu thời gian.

Ở bước 460, phương pháp mật mã hóa tin nhắn kết nạp với khóa mật mã hóa dịch vụ (được làm tối), và gửi yêu cầu kết nạp được mật mã hóa đến thiết bị máy chủ được kết hợp cho sự xử lý kết nạp.

Thiết bị máy chủ bao gồm máy chủ xác thực mà thực hiện thủ tục về sự an toàn, để xác nhận tính hợp lệ thông tin xác thực và về sự an toàn, như một phần của sự xử lý kết nạp. Nói riêng, máy chủ xác thực có thể thực hiện phương pháp được mô tả ở dưới với tham chiếu đến Fig.5. Theo cách vắn tắt, máy chủ xác thực giải mật mã tải tin sử dụng khóa mật mã hóa riêng. Tải tin được giải mật mã có thể được xác nhận tính hợp lệ, ví dụ nhờ kiểm tra nonce và dấu thời gian, và xác nhận tính hợp lệ thông tin xác thực yếu tố thứ hai cho người dùng. Thiết bị máy chủ sau đó lưu trữ khóa ECC công khai với dữ liệu người dùng khác, ví dụ trong tài khoản người dùng hiện có, và sinh ra "sự tham chiếu khóa" tương ứng mà nhận dạng theo cách duy nhất cặp khóa ECC chữ ký. Thiết bị dịch vụ chúng sinh ra tin nhắn đáp lại kết nạp mật mã hóa gồm có sự tham chiếu khóa. Trong các sự thi hành, tin nhắn đáp lại kết nạp mật mã hóa có thể được mật mã hóa sử dụng khóa mật mã hóa dịch vụ/riêng chỉ được biết đối với thiết bị máy chủ.

Ở bước 470, phương pháp nhận sự đáp lại kết nạp mật mã hóa từ thiết bị máy chủ, và, nếu thích hợp, có thể thực hiện sự giải mật mã của tải tin tin nhắn sử dụng khóa mật mã hóa.

Ở bước 470, phương pháp lưu trữ sự tham chiếu khóa cho cặp khóa ECC được chứa trong tin nhắn đáp lại kết nạp mật mã hóa cho sự sử dụng trong các phiên bản tiếp theo của các quy trình xác thực bởi thiết bị khách. Phương pháp sau đó kết thúc ở bước 485.

Fig.5 là lưu đồ minh họa phương pháp 500 cho sự kết nạp của người dùng của ứng dụng khách an toàn bởi thiết bị máy chủ phù hợp với các sự thi hành ví dụ của sáng chế này. Ví dụ, phương pháp 500 có thể được thực hiện bởi môđun xác thực và về sự an toàn 360 của thiết bị máy chủ 302 trên Fig.3. Trong sự mô tả sau đây, để dễ dàng cho sự tham chiếu, môđun xác thực và về sự an toàn 360 được gọi là máy chủ xác thực. Phương pháp 500 có thể được thực hiện bởi thiết bị máy chủ chung với phương pháp 400 trên Fig.4 được thực hiện bởi thiết bị khách. Phương pháp 500 thực hiện thủ tục về sự an toàn như một phần của sự xử lý kết nạp.

Phương pháp 500 bắt đầu ở bước 505. Phương pháp 500 có thể bắt đầu để đáp lại thiết bị máy chủ nhận tin nhắn yêu cầu kết nạp từ ứng dụng an toàn được kết hợp chạy trên thiết bị khách, và cho yêu cầu đi đến máy chủ xác thực.

Ở bước 510, máy chủ xác thực giải mật mã tải tin của tin nhắn yêu cầu kết nạp được nhận sử dụng khóa giải mật mã dịch vụ.

Bước 520 xem xét liệu sự giải mật mã trong bước 510 đã thành công. Nếu bước 520 xác định là sự giải mật mã đã thành công, thì tin nhắn yêu cầu kết nạp được nhận đã bắt nguồn từ ứng dụng an toàn thật trên thiết bị khách và phương pháp tiến hành bước 530. Nếu không thì, tin nhắn yêu cầu được nhận thất bại trong thủ tục về sự an toàn và phương pháp kết thúc ở bước 565.

Ở bước 530, máy chủ xác thực xác nhận tính hợp lệ tải tin được giải mật mã. Ví dụ, máy chủ xác thực có thể kiểm tra tính hợp lệ của nonce và tính chất mới của dấu thời gian. Máy chủ xác thực có thể xác nhận tính hợp lệ thông tin xác thực yếu tố thứ hai cho người dùng.

Bước 540 xem xét liệu tất cả các kiểm tra xác nhận tính hợp lệ được thực hiện trong bước 530 đã thành công để cho tải tin được xác nhận tính hợp lệ. Nếu bước 540 xác định là tải tin được giải mật mã được xác nhận tính hợp lệ bởi tất cả các kiểm tra xác nhận tính hợp lệ trong bước 530, thì tin nhắn được nhận vượt qua thủ tục về sự an toàn và phương pháp tiến hành bước 550. Nếu không thì, yêu cầu được nhận thất bại trong thủ tục về sự an toàn và phương pháp kết thúc ở bước 565.

Ở bước 550, máy chủ xác thực lưu trữ khóa ECC công khai được chứa trong tải tin được giải mật mã, với dữ liệu người dùng khác cho người dùng, ví dụ trong tài khoản người dùng. Nói riêng, khóa ECC công khai được lưu trữ như khóa chữ ký công khai để xác nhận tính hợp lệ người dùng/thiết bị khách như được mô tả ở đây. Thêm vào, máy chủ sinh ra "sự tham chiếu khóa" tương ứng mà nhận dạng theo cách duy nhất cặp khóa công khai-riêng chữ ký (ECC). Điều này hoàn thành sự kết nạp của người dùng và ứng dụng an toàn cho sự sử dụng với sự xác thực sinh trắc học như được mô tả ở đây.

Ở bước 560, máy chủ xác thực sinh ra tin nhắn đáp lại kết nạp mật mã hóa gồm có sự tham chiếu khóa trong tải tin tin nhắn, và gửi sự đáp lại đến thiết bị khách. Trong các sự thi hành, tin nhắn đáp lại kết nạp mật mã hóa có thể được mật mã hóa sử dụng khóa mật mã hóa dịch vụ. Phương pháp kết thúc ở bước 565.

Fig.6 là lưu đồ minh họa phương pháp 600 cho sự xác thực của người dùng với thiết bị máy chủ được kết hợp với ứng dụng khách an toàn phù hợp với các sự thi hành ví dụ của sáng chế này. Ví dụ, phương pháp 600 có thể được thực hiện bởi ứng dụng an toàn 250 chạy trên thiết bị khách 204 trên Fig.2. Phương pháp 600 có thể được thực hiện khi ứng dụng an toàn gửi các sự truyền thông dữ liệu, như các yêu cầu giao dịch và các tin nhắn khác mà đòi hỏi sự xác thực và sự xác nhận tính hợp lệ, đến thiết bị máy chủ được kết hợp sau thủ tục kết nạp trên Fig.4.

Phương pháp 600 bắt đầu ở bước 605. Ví dụ, phương pháp 600 có thể bắt đầu để đáp lại người dùng khởi chạy ứng dụng an toàn trên thiết bị khách, đăng nhập vào tài khoản người dùng và nhập dữ liệu người dùng cho yêu cầu giao dịch (nghĩa là, thông tin giao dịch) sử dụng giao diện người dùng đồ họa (graphical user interface, GUI) của màn hình được kết hợp của ứng dụng an toàn. Trong một số sự thi hành, phương pháp 600 có thể được khởi động bởi các loại nhất định của các giao dịch người dùng, như tất cả hoặc các giao dịch tài chính có giá trị tương đối cao (ví dụ, sự sử dụng cho quyền sự thanh toán tài chính). Trong các sự thi hành khác, phương pháp 600 có thể được khởi động cho một số hoặc tất cả các giao dịch người dùng của người dùng hoặc thiết bị khách mà đã được nhận dạng như đòi hỏi sự an toàn bổ sung, như có nguy cơ cao về

gian lận. Theo đó, bước 605 có thể gồm có nhận thông tin giao dịch đầu vào người dùng để tạo thành ít nhất một phần của tải tin của tin nhắn yêu cầu giao dịch.

Ở bước 610, người dùng thực hiện sự xác thực sinh trắc học. Nói riêng, người dùng được hỏi bởi ứng dụng an toàn để cung cấp thông tin xác thực sinh trắc học cho quy trình xác thực sinh trắc học của hệ điều hành của thiết bị khách như được mô tả ở trên.

Ở bước 620, phương pháp xác định liệu sự xác thực sinh trắc học trong bước 610 đã thành công. Nếu bước 620 xác định là sự xác thực sinh trắc học trong bước 610 đã thành công, thì phương pháp tiến hành bước 630. Tuy nhiên, nếu bước 630 xác định là sự xác thực sinh trắc học trong bước 610 đã không thành công, thì người dùng có thể được thông báo là yêu cầu giao dịch được hủy bỏ và phương pháp kết thúc ở bước 665.

Ở bước 630, ứng dụng an toàn tạo ra tải tin tin nhắn yêu cầu giao dịch và cung cấp nó cho TEE của thiết bị khách. Nói riêng, ứng dụng an toàn tạo ra tải tin gồm có thông tin giao dịch đầu vào người dùng và sự tham chiếu khóa được mô tả ở trên. Tải tin có thể gồm có thông tin bổ sung như thông tin đăng nhập chính của người dùng và tùy chọn là thông tin xác thực yếu tố thứ hai được nhập bởi người dùng. Trong các sự thi hành ví dụ, tải tin gồm có sự kết hợp của dữ liệu người dùng, như mã thông báo đăng nhập, mà là duy nhất đối với ứng dụng an toàn người dùng, như được mô tả ở trên.

Ở bước 640, TEE có thể thêm nonce và dấu thời gian vào tải tin và ký theo cách an toàn tải tin với khóa chữ ký riêng (ECC) được lưu trữ trong phần tử an toàn của thiết bị khách. Ví dụ, TEE có thể sinh ra chữ ký số nhờ băm tải tin tin nhắn để tạo ra trị số băm và mật mã hóa trị số băm với khóa chữ ký riêng (ECC)/phần tử an toàn, và có thể thêm chữ ký số để ký theo cách an toàn tin nhắn. Vì bước 620 đã xác định là sự xác thực sinh trắc học trong bước 610 đã thành công, TEE có thể giành được sự truy nhập đối với khóa ECC riêng/phần tử an toàn của thiết bị khách như được mô tả ở trên. Trong một số sự thi hành, sự tham chiếu khóa được thêm vào tải tin tin nhắn sau khi TEE đã sinh ra chữ ký số của tải tin tin nhắn. Phương pháp sau đó tiến hành bước 650.

Ở bước 650, ứng dụng an toàn mật mã hóa tin nhắn yêu cầu giao dịch được ký với khóa mật mã hóa dịch vụ, và gửi yêu cầu được mật mã hóa đến thiết bị máy chủ được kết hợp để xử lý yêu cầu giao dịch.

Thiết bị máy chủ có thể bao gồm máy chủ xác thực mà thực hiện thủ tục về sự an toàn như một phần của sự xử lý yêu cầu giao dịch. Nói riêng, máy chủ xác thực có thể thực hiện phương pháp được mô tả ở dưới với tham chiếu đến Fig.7. Theo cách vắn tắt, máy chủ xác thực giải mật mã tải tin sử dụng khóa giải mật mã (nghĩa là, khóa giải mật mã dịch vụ). Vì tải tin được giải mật mã gồm có sự tham chiếu khóa, máy chủ có thể tìm kiếm khóa chữ ký công khai được kết hợp và xác nhận tính hợp lệ chữ ký. Máy chủ xác thực có thể thực hiện các quy trình về sự an toàn khác sử dụng thông tin khác trong tải tin được giải mật mã, như kiểm tra nonce và dấu thời gian, và xác nhận tính hợp lệ sự xác thực yếu tố chính hoặc thứ hai bất kỳ đối với phần tử nhận dạng được kết hợp cho người dùng. Vào lúc sự hoàn thành thành công của thủ tục về sự an toàn, máy chủ xác thực có thể sinh ra mã thông báo mà được trả về cho ứng dụng an toàn của thiết bị khách (hoặc, như một sự lựa chọn, thay đổi trạng thái phiên cho phù hợp). Thiết bị máy chủ sau đó có thể tiến hành để xử lý yêu cầu giao dịch.

Ở bước 660, ứng dụng an toàn có thể nhận sự đáp lại từ thiết bị máy chủ, xác nhận sự xác thực thành công. Phương pháp sau đó kết thúc ở bước 665.

Do đó, có được cung cấp thiết bị truyền thông khách để sinh ra tin nhắn người dùng bao gồm sự khẳng định cho sự xác minh bởi thiết bị máy chủ từ xa. Thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ. Thiết bị truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để: nhận dữ liệu tải tin cho tin nhắn người dùng; thực hiện sự xác thực sinh trắc học của người dùng, sự xác thực sinh trắc học bao gồm nhận thông tin sinh trắc học đầu vào từ người dùng và xác nhận tính hợp lệ thông tin sinh trắc học đầu vào đối với thông tin sinh trắc học cho người dùng được lưu trữ trước đó trong bộ nhớ; để đáp lại sự xác thực sinh trắc học thành công của người dùng, sinh ra chữ ký số dựa trên tải tin tin nhắn, trong đó chữ ký số được sinh ra sử dụng khóa chữ ký riêng được lưu trữ trong phần tử an toàn của thiết bị truyền thông, trong đó khóa riêng là có thể truy nhập được chỉ khi sự xác thực sinh

trắc học của người dùng là thành công, và sinh ra tin nhắn người dùng để gửi đến thiết bị từ xa, tin nhắn người dùng bao gồm tải tin tin nhắn và chữ ký số. Phương pháp tương ứng cũng được cung cấp.

Fig.7 là lưu đồ minh họa phương pháp 700 để xác thực và xác nhận tính hợp lệ các yêu cầu giao dịch của người dùng của ứng dụng khách an toàn bởi thiết bị máy chủ phù hợp với các sự thi hành ví dụ của sáng chế này. Ví dụ, phương pháp 700 có thể được thực hiện bởi môđun xác thực và về sự an toàn 360 của thiết bị máy chủ 302 trên Fig.3. Trong sự mô tả sau đây, để dễ dàng cho sự tham chiếu, môđun xác thực và về sự an toàn 360 được gọi là máy chủ xác thực. Phương pháp 700 có thể được thực hiện bởi thiết bị máy chủ chung với phương pháp 600 trên Fig.6 được thực hiện bởi thiết bị khách. Phương pháp 700 thực hiện thủ tục về sự an toàn trước khi xử lý yêu cầu giao dịch được nhận.

Phương pháp 700 bắt đầu ở bước 705. Phương pháp 700 có thể bắt đầu để đáp lại thiết bị máy chủ nhận tin nhắn yêu cầu giao dịch từ ứng dụng an toàn được kết hợp chạy trên thiết bị khách, và cho yêu cầu đi đến máy chủ xác thực.

Ở bước 710 máy chủ xác thực giải mật mã tải tin tin nhắn của tin nhắn yêu cầu giao dịch được nhận sử dụng khóa giải mật mã dịch vụ.

Bước 720 xem xét liệu sự giải mật mã trong bước 710 đã thành công. Nếu bước 720 xác định là sự giải mật mã trong bước 710 đã thành công, thì tin nhắn yêu cầu giao dịch được nhận đã bắt nguồn từ ứng dụng an toàn thật trên thiết bị khách và phương pháp tiến hành bước 730. Nếu không thì, tin nhắn yêu cầu được nhận thất bại trong thủ tục xác thực và về sự an toàn và phương pháp kết thúc ở bước 775.

Ở bước 730, máy chủ xác thực sử dụng sự tham chiếu khóa được gồm có trong tải tin tin nhắn được giải mật mã để tìm kiếm khóa ECC chữ ký công khai được kết hợp và xác nhận tính hợp lệ chữ ký của tải tin được ký. Ví dụ, máy chủ xác thực có thể sinh ra chữ ký số sử dụng khóa ECC công khai dựa trên tải tin tin nhắn, và so sánh chữ ký được sinh ra với chữ ký được nhận trong tải tin được ký; nếu sự so sánh chỉ báo sự so khớp, thì chữ ký trong tin nhắn là hợp lệ.

Bước 740 xem xét liệu chữ ký đã được xác nhận tính hợp lệ trong bước 730. Nếu bước 740 xác định là chữ ký là hợp lệ, thì phương pháp có thể tin tưởng là người dùng đã được xác thực về sinh trắc học ở thiết bị khách và phương pháp tiến hành bước 750. Nếu không thì, tin nhắn yêu cầu được nhận thất bại trong thủ tục xác thực và về sự an toàn và phương pháp kết thúc ở bước 775.

Ở bước 750, máy chủ xác thực xác nhận tính hợp lệ tải tin được giải mật mã. Ví dụ, máy chủ xác thực có thể kiểm tra tính hợp lệ của nonce và tính chất mới của dấu thời gian, và có thể xác nhận tính hợp lệ thông tin xác thực yếu tố thứ hai và tương tự cho người dùng.

Bước 760 xem xét liệu tất cả các kiểm tra xác nhận tính hợp lệ được thực hiện trong bước 750 đã thành công để cho tải tin được xác nhận tính hợp lệ. Nếu bước 760 xác định là tải tin được giải mật mã và được xác minh chữ ký được xác nhận tính hợp lệ bởi tất cả các kiểm tra xác nhận tính hợp lệ trong bước 750, thì tin nhắn yêu cầu được nhận vượt qua thủ tục về sự an toàn và phương pháp tiến hành bước 770. Nếu không thì, yêu cầu được nhận thất bại trong thủ tục về sự an toàn và phương pháp kết thúc ở bước 575.

Ở bước 770, máy chủ xác thực sinh ra mã thông báo, mà có thể được trả về cho ứng dụng an toàn của thiết bị khách, chỉ báo là tin nhắn được nhận đã vượt qua các kiểm tra xác thực và về sự an toàn (hoặc, như một sự lựa chọn, trạng thái phiên được thay đổi cho phù hợp). Thiết bị máy chủ sau đó có thể tiến hành để xử lý yêu cầu giao dịch. Phương pháp sau đó kết thúc ở bước 775.

Do đó, có được cung cấp thiết bị truyền thông máy chủ để xác minh sự khẳng định trong tin nhắn người dùng được nhận từ thiết bị khách từ xa. Thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ. Thiết bị truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để: xác nhận tính hợp lệ chữ ký số trong tải tin của tin nhắn người dùng được nhận, sử dụng khóa chữ ký công khai và tải tin tin nhắn, và nếu chữ ký số được xác nhận tính hợp lệ, thì xác định là người dùng của thiết bị từ xa đã được xác thực về sinh trắc học ở thiết bị từ xa. Trong các sự thi hành ví dụ, thiết bị truyền thông được tạo cấu hình thêm nữa, dưới sự điều khiển của

bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để: nhận dạng sự tham chiếu khóa trong tải tin của tin nhắn người dùng được nhận, và tìm kiếm khóa chữ ký công khai tương ứng với sự tham chiếu khóa được lưu trữ trong bộ nhớ của thiết bị truyền thông.

Tóm lại, thiết bị truyền thông khách và phương pháp để sinh ra tin nhắn người dùng bao gồm sự khẳng định cho sự xác minh bởi thiết bị máy chủ từ xa được mô tả. Dữ liệu tải tin cho tin nhắn người dùng được nhận. Sự xác thực sinh trắc học của người dùng được thực hiện. Nếu sự xác thực sinh trắc học của người dùng là thành công, thì chữ ký số được sinh ra dựa trên tải tin tin nhắn. Chữ ký số được sinh ra sử dụng khóa chữ ký riêng được lưu trữ trong phần tử an toàn của thiết bị khách. Trong các sự thi hành, chữ ký số được sinh ra trong môi trường an toàn của thiết bị khách mà có sự truy nhập duy nhất đối với phần tử an toàn sau sự xác thực sinh trắc học thành công. Tin nhắn người dùng bao gồm tải tin tin nhắn và chữ ký số được sinh ra để gửi đến thiết bị máy chủ từ xa. Phương pháp và thiết bị truyền thông máy chủ tương ứng cũng được mô tả.

Các sự thi hành ví dụ của sáng chế này được mô tả ở đây làm cho có khả năng có sự an toàn được cải thiện trong các hệ thống truyền thông. Nói riêng, sự kết hợp liên kết được tạo ra giữa sự xác thực sinh trắc học của người dùng và chữ ký của sự khẳng định được ký (tải tin tin nhắn), vì chữ ký hợp lệ có thể chỉ được áp dụng vào lúc sự xác thực sinh trắc học thành công. Theo đó, máy chủ có thể tin tưởng là người dùng đã được xác thực về sinh trắc học chỉ vào lúc sự xác nhận tính hợp lệ thành công của chữ ký được áp dụng đối với sự khẳng định (tải tin tin nhắn). Sự sử dụng của sự xác thực sinh trắc học cung cấp giải pháp đơn giản hơn, an toàn hơn và chi phí thấp trong các kịch bản xác thực, nhờ tận dụng phần chức năng hiện có của thiết bị khách. Dạng bất kỳ của sự xác thực sinh trắc học là có thể, mà có thể được lựa chọn bởi người dùng trong lúc sự kết nạp. Theo đó, ứng dụng an toàn được mô tả có thể được thi hành trên loại bất kỳ của thiết bị khách từ mức vào (entry-level) đến cao cấp (high-end), với điều kiện là ít nhất một dạng của cơ chế xác thực sinh trắc học là khả dụng. Sự sử dụng của sự xác thực sinh trắc học là thuận tiện hơn đối với người dùng vì nó không dựa vào việc nhớ các giấy chứng nhận người dùng chi tiết. Sự kết hợp liên kết được ủng hộ bởi phần cứng

thêm nữa, vì các sự khẳng định được ký trong môi trường an toàn, như TEE, của thiết bị khách.

Hơn nữa, các sự khẳng định được ký như các tin nhắn yêu cầu giao dịch người dùng được mật mã hóa trước sự truyền thông. Sự an toàn mật mã hóa được tăng cường vì khóa mật mã hóa được làm tối; các ứng dụng không phải thật bởi vậy không thể thực hiện theo cách hợp lệ sự mật mã hóa mà không được phát hiện bởi thiết bị máy chủ.

Cuối cùng, một số sự thi hành ví dụ gồm có các dấu hiệu về sự an toàn khác, như nonce và/hoặc dấu thời gian, và/hoặc sự kết hợp của dữ liệu mà là duy nhất đối với ứng dụng an toàn/người dùng, trong tải tin tin nhắn cho sự xác minh. Điều này tăng cường sự an toàn đối với các ứng dụng/các thiết bị giả và các người dùng bị cấm, mà có thể được phát hiện theo cách tự động bởi thủ tục về sự an toàn được thực hiện ở thiết bị máy chủ. Theo đó, cơ chế về sự an toàn ba mức phù hợp với sáng chế này ngăn theo cách mạnh mẽ hơn sự truy nhập không thích hợp đối với các tài khoản người dùng và giảm thiểu khả năng của sự giành quyền kiểm soát tài khoản thành công bởi các người tấn công.

Các khía cạnh của sáng chế này được mô tả ở đây với tham chiếu đến các lưu đồ. Nó sẽ được hiểu là các bước trong các sự thi hành được minh họa là theo cách ví dụ. Các bước có thể được tiến hành theo thứ tự phù hợp bất kỳ, và một số trong các bước có thể được bỏ qua cho phù hợp đối với các sự đòi hỏi ứng dụng. Nó sẽ được hiểu là các bước của các lưu đồ, và các sự kết hợp của các bước, có thể được thi hành bởi các lệnh chương trình đọc được bởi máy tính.

Nó sẽ được hiểu rõ là sáng chế đã được mô tả chỉ theo cách ví dụ. Những sự sửa đổi khác nhau có thể được thực hiện đối với các kỹ thuật được mô tả ở đây và các tương đương của chúng mà không lệch khỏi ý đồ và phạm vi của các điểm yêu cầu bảo hộ kèm theo. Các kỹ thuật được bộc lộ bao gồm các kỹ thuật mà có thể được cung cấp theo cách độc lập, hoặc trong sự kết hợp với nhau. Bởi vậy, các dấu hiệu được mô tả đối với một kỹ thuật có thể cũng được trình bày trong sự kết hợp với kỹ thuật khác.

YÊU CẦU BẢO HỘ

1. Thiết bị truyền thông để sinh ra tin nhắn người dùng bao gồm sự khẳng định cho sự xác minh bởi thiết bị từ xa, thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ, thiết bị truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

nhận dữ liệu tải tin cho tin nhắn người dùng, dữ liệu tải tin đã được sinh ra bởi ứng dụng an toàn lưu trú trên thiết bị truyền thông;

áp dụng cơ chế về sự an toàn mức thứ nhất của sự xác thực sinh trắc học của người dùng, sự xác thực sinh trắc học bao gồm nhận thông tin sinh trắc học đầu vào từ người dùng và xác nhận tính hợp lệ thông tin sinh trắc học đầu vào đối với thông tin sinh trắc học cho người dùng được lưu trữ trước đó trong bộ nhớ;

để đáp lại sự xác thực sinh trắc học thành công của người dùng, áp dụng cơ chế về sự an toàn mức thứ hai để sinh ra chữ ký số dựa trên tải tin tin nhắn, trong đó chữ ký số được sinh ra sử dụng khóa chữ ký riêng được lưu trữ trong phần tử an toàn của thiết bị truyền thông, trong đó khóa riêng là có thể truy nhập được chỉ khi sự xác thực sinh trắc học của người dùng là thành công;

sinh ra tin nhắn người dùng để gửi đến thiết bị từ xa, tin nhắn người dùng bao gồm tải tin tin nhắn và chữ ký số;

áp dụng cơ chế mật mã hóa về sự an toàn mức thứ ba nhờ xác thực tin nhắn người dùng sử dụng khóa mật mã hóa cụ thể cho ứng dụng an toàn; và

mật mã hóa tin nhắn người dùng với khóa mật mã hóa, trong đó khóa mật mã hóa được làm tối trong bộ nhớ được kết hợp với các lệnh trong thiết bị truyền thông.

2. Thiết bị truyền thông theo điểm 1, được tạo cấu hình cho chữ ký số để được sinh ra trong môi trường an toàn của thiết bị truyền thông.

3. Thiết bị truyền thông theo điểm 2, được tạo cấu hình cho sự truy nhập đối với khóa chữ ký riêng để được giới hạn chỉ đối với môi trường an toàn của thiết bị truyền thông.

4. Thiết bị truyền thông theo điểm nêu trên bất kỳ, được tạo cấu hình cho tải tin tin nhắn để bao gồm một hoặc nhiều trong: sự tham chiếu khóa; dữ liệu xác thực người dùng; dữ liệu nhận dạng thiết bị khách, và dữ liệu ứng dụng khách, và/hoặc được tạo cấu hình cho tin nhắn người dùng để bao gồm thêm nữa một hoặc nhiều trong: nonce và dấu thời gian.

5. Thiết bị truyền thông theo điểm nêu trên bất kỳ, được tạo cấu hình cho chữ ký số để được sinh ra nhờ băm tải tin tin nhắn để tạo ra trị số băm, và mật mã hóa trị số băm với khóa chữ ký riêng để sinh ra chữ ký số.

6. Thiết bị truyền thông theo điểm nêu trên bất kỳ, trong đó thiết bị truyền thông được tạo cấu hình thêm nữa để sinh ra tin nhắn kết nạp bao gồm sự khẳng định cho sự xác minh bởi thiết bị từ xa, trong đó thiết bị truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

nhận dữ liệu tải tin cho tin nhắn kết nạp, để đáp lại sự xác thực của người dùng bởi thiết bị từ xa;

thực hiện sự xác thực sinh trắc học của người dùng;

để đáp lại sự xác thực sinh trắc học thành công của người dùng, sinh ra cặp khóa chữ ký bất đối xứng bao gồm khóa chữ ký riêng để sinh ra chữ ký số và khóa chữ ký công khai tương ứng;

lưu trữ khóa chữ ký riêng trong phần tử an toàn, và

sinh ra tin nhắn kết nạp để gửi đến thiết bị từ xa, tin nhắn kết nạp bao gồm dữ liệu tải tin và khóa chữ ký công khai.

7. Thiết bị truyền thông theo điểm 6, trong đó thiết bị truyền thông được tạo cấu hình thêm nữa, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

mật mã hóa tin nhắn kết nạp với khóa mật mã hóa.

8. Thiết bị truyền thông theo điểm 6 hoặc điểm 7, trong đó thiết bị truyền thông được tạo cấu hình thêm nữa, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

nhận tin nhắn đáp lại từ thiết bị từ xa, tin nhắn đáp lại chỉ báo sự kết nạp thành công bởi thiết bị từ xa, và

lưu trữ sự tham chiếu khóa được kết hợp với cặp khóa chữ ký bất đối xứng được chứa trong tải tin của tin nhắn đáp lại.

9. Thiết bị truyền thông để xác minh sự khẳng định trong tin nhắn người dùng được nhận từ thiết bị từ xa, tin nhắn người dùng đã được sinh ra bởi ứng dụng an toàn lưu trú trên thiết bị từ xa và được xác thực sử dụng khóa mật mã hóa cụ thể cho ứng dụng an toàn được làm tối trong bộ nhớ được kết hợp với ứng dụng an toàn, thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ, thiết bị truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

xác nhận tính hợp lệ khóa cụ thể cho ứng dụng an toàn được sử dụng bởi thiết bị từ xa để xác thực tin nhắn người dùng được nhận nhờ giải mật mã thành công tải tin của tin nhắn người dùng sử dụng khóa giải mật mã dịch vụ;

nếu khóa cụ thể cho ứng dụng an toàn được xác nhận tính hợp lệ, thì xác định là tin nhắn người dùng được nhận đã bắt nguồn từ ứng dụng an toàn thật;

xác nhận tính hợp lệ chữ ký số trong tải tin của tin nhắn người dùng được nhận, sử dụng khóa chữ ký công khai và tải tin tin nhắn, và

nếu chữ ký số được xác nhận tính hợp lệ, thì xác định là người dùng của thiết bị từ xa đã được xác thực về sinh trắc học ở thiết bị từ xa.

10. Thiết bị truyền thông theo điểm 9, thiết bị truyền thông được tạo cấu hình thêm nữa, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

nhận dạng sự tham chiếu khóa trong tải tin của tin nhắn người dùng được nhận, và

tìm kiếm khóa chữ ký công khai tương ứng với sự tham chiếu khóa được lưu trữ trong bộ nhớ của thiết bị truyền thông.

11. Thiết bị truyền thông theo điểm 9 hoặc điểm 10, thiết bị truyền thông được tạo cấu hình thêm nữa, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để thực hiện một hoặc nhiều trong:

xác định tính hợp lệ của nonce hoặc dấu thời gian trong tin nhắn người dùng được nhận, và

xác định tính hợp lệ của dữ liệu xác thực người dùng; dữ liệu nhận dạng thiết bị khách, và/hoặc dữ liệu ứng dụng khách trong tải tin của tin nhắn người dùng được nhận.

12. Thiết bị truyền thông theo điểm 9, 10 hoặc 11, trong đó thiết bị truyền thông được tạo cấu hình thêm nữa để xác minh sự khẳng định trong tin nhắn kết nạp được nhận từ thiết bị từ xa, thiết bị truyền thông được tạo cấu hình thêm nữa, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

nhận tin nhắn kết nạp từ thiết bị từ xa;

xác nhận tính hợp lệ dữ liệu trong tải tin tin nhắn, dữ liệu được xác nhận tính hợp lệ nhận dạng người dùng của thiết bị từ xa mà đã gửi tin nhắn kết nạp;

nhận dạng khóa chữ ký công khai trong tải tin tin nhắn;

lưu trữ khóa chữ ký công khai trong bộ nhớ của thiết bị truyền thông, và

sinh ra sự tham chiếu khóa cho khóa chữ ký công khai để gửi trong tin nhắn đáp lại đến thiết bị từ xa.

13. Thiết bị truyền thông để sinh ra tin nhắn người dùng bao gồm sự khẳng định cho sự xác minh bởi thiết bị từ xa trong giao dịch tài chính, thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ, thiết bị truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh được lưu trữ trong bộ nhớ để:

nhận dữ liệu tải tin cho tin nhắn người dùng, dữ liệu tải tin đã được sinh ra bởi ứng dụng an toàn lưu trú trên thiết bị truyền thông;

áp dụng cơ chế về sự an toàn mức thứ nhất của sự xác thực sinh trắc học của người dùng, sự xác thực sinh trắc học bao gồm nhận thông tin sinh trắc học đầu vào từ người dùng và xác nhận tính hợp lệ thông tin sinh trắc học đầu vào đối với thông tin sinh trắc học cho người dùng được lưu trữ trước đó trong bộ nhớ;

để đáp lại sự xác thực sinh trắc học thành công của người dùng, áp dụng cơ chế về sự an toàn mức thứ hai để sinh ra chữ ký số dựa trên tải tin tin nhắn, trong đó chữ ký số được sinh ra sử dụng khóa chữ ký riêng được lưu trữ trong phần tử an toàn của thiết bị truyền thông, trong đó khóa riêng là có thể truy nhập được chỉ khi sự xác thực sinh trắc học của người dùng là thành công;

sinh ra tin nhắn người dùng để gửi đến thiết bị từ xa, tin nhắn người dùng bao gồm tải tin tin nhắn và chữ ký số; và

áp dụng cơ chế mật mã hóa về sự an toàn mức thứ ba nhờ xác thực tin nhắn người dùng sử dụng khóa mật mã hóa cụ thể cho ứng dụng an toàn; và

để mật mã hóa tin nhắn người dùng với khóa mật mã hóa, trong đó khóa mật mã hóa được làm tối trong bộ nhớ được kết hợp với các lệnh trong thiết bị truyền thông.

14. Phương pháp, được thực hiện trong thiết bị truyền thông khách, để sinh ra tin nhắn người dùng bao gồm sự khẳng định cho sự xác minh bởi thiết bị máy chủ từ xa, phương pháp này bao gồm, dưới sự điều khiển của bộ xử lý của thiết bị truyền thông khách:

nhận dữ liệu tải tin cho tin nhắn người dùng, dữ liệu tải tin đã được sinh ra bởi ứng dụng an toàn lưu trú trên thiết bị truyền thông;

áp dụng cơ chế về sự an toàn mức thứ nhất của sự xác thực sinh trắc học của người dùng, sự xác thực sinh trắc học bao gồm nhận thông tin sinh trắc học đầu vào từ người dùng và xác nhận tính hợp lệ thông tin sinh trắc học đầu vào đối với thông tin sinh trắc học cho người dùng được lưu trữ trước đó trong bộ nhớ;

để đáp lại sự xác thực sinh trắc học thành công của người dùng, áp dụng cơ chế về sự an toàn mức thứ hai nhờ sinh ra chữ ký số dựa trên tải tin tin nhắn, trong đó chữ ký số được sinh ra sử dụng khóa chữ ký riêng được lưu trữ trong phần tử an toàn của thiết bị truyền thông khách, trong đó khóa riêng là có thể truy nhập được chỉ khi sự xác thực sinh trắc học của người dùng là thành công;

sinh ra tin nhắn người dùng để gửi đến thiết bị máy chủ từ xa, tin nhắn người dùng bao gồm tải tin tin nhắn và chữ ký số; và

áp dụng cơ chế mật mã hóa về sự an toàn mức thứ ba nhờ xác thực tin nhắn người dùng sử dụng khóa mật mã hóa cụ thể cho ứng dụng an toàn; và

mật mã hóa tin nhắn người dùng với khóa mật mã hóa, trong đó khóa mật mã hóa được làm tối trong bộ nhớ được kết hợp với các lệnh trong thiết bị truyền thông khách.

15. Phương pháp theo điểm 14, phương pháp này bao gồm bước:

sinh ra chữ ký số trong môi trường an toàn của thiết bị truyền thông khách, và/hoặc

giới hạn sự truy nhập đối với khóa chữ ký riêng chỉ đối với môi trường an toàn của thiết bị truyền thông khách.

16. Phương tiện lưu trữ không chuyển tiếp lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho bộ xử lý thực hiện phương pháp theo điểm bất kỳ trong các điểm từ 14 đến 15.

17. Phương pháp, được thực hiện trong thiết bị truyền thông máy chủ, để xác minh sự khẳng định trong tin nhắn người dùng được nhận từ thiết bị khách từ xa, tin nhắn người dùng đã được sinh ra bởi ứng dụng an toàn lưu trú trên thiết bị khách từ xa và

được xác thực với khóa mật mã hóa cụ thể cho ứng dụng an toàn được làm tối trong bộ nhớ được kết hợp với ứng dụng an toàn, phương pháp này bao gồm, dưới sự điều khiển của bộ xử lý của thiết bị truyền thông máy chủ:

xác nhận tính hợp lệ khóa cụ thể cho ứng dụng an toàn được sử dụng bởi thiết bị từ xa để xác thực tin nhắn người dùng được nhận nhờ giải mật mã thành công tải tin của tin nhắn người dùng sử dụng khóa giải mật mã dịch vụ;

nếu khóa cụ thể cho ứng dụng an toàn được xác nhận tính hợp lệ, thì xác định là tin nhắn người dùng được nhận đã bắt nguồn từ ứng dụng an toàn thật;

xác nhận tính hợp lệ chữ ký số trong tải tin của tin nhắn người dùng được nhận, sử dụng khóa chữ ký công khai và tải tin tin nhắn, và

nếu chữ ký số được xác nhận tính hợp lệ, thì xác định là người dùng của thiết bị khách đã được xác thực về sinh trắc học ở thiết bị khách từ xa.

18. Phương tiện lưu trữ không chuyển tiếp lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho bộ xử lý thực hiện phương pháp theo điểm 17.

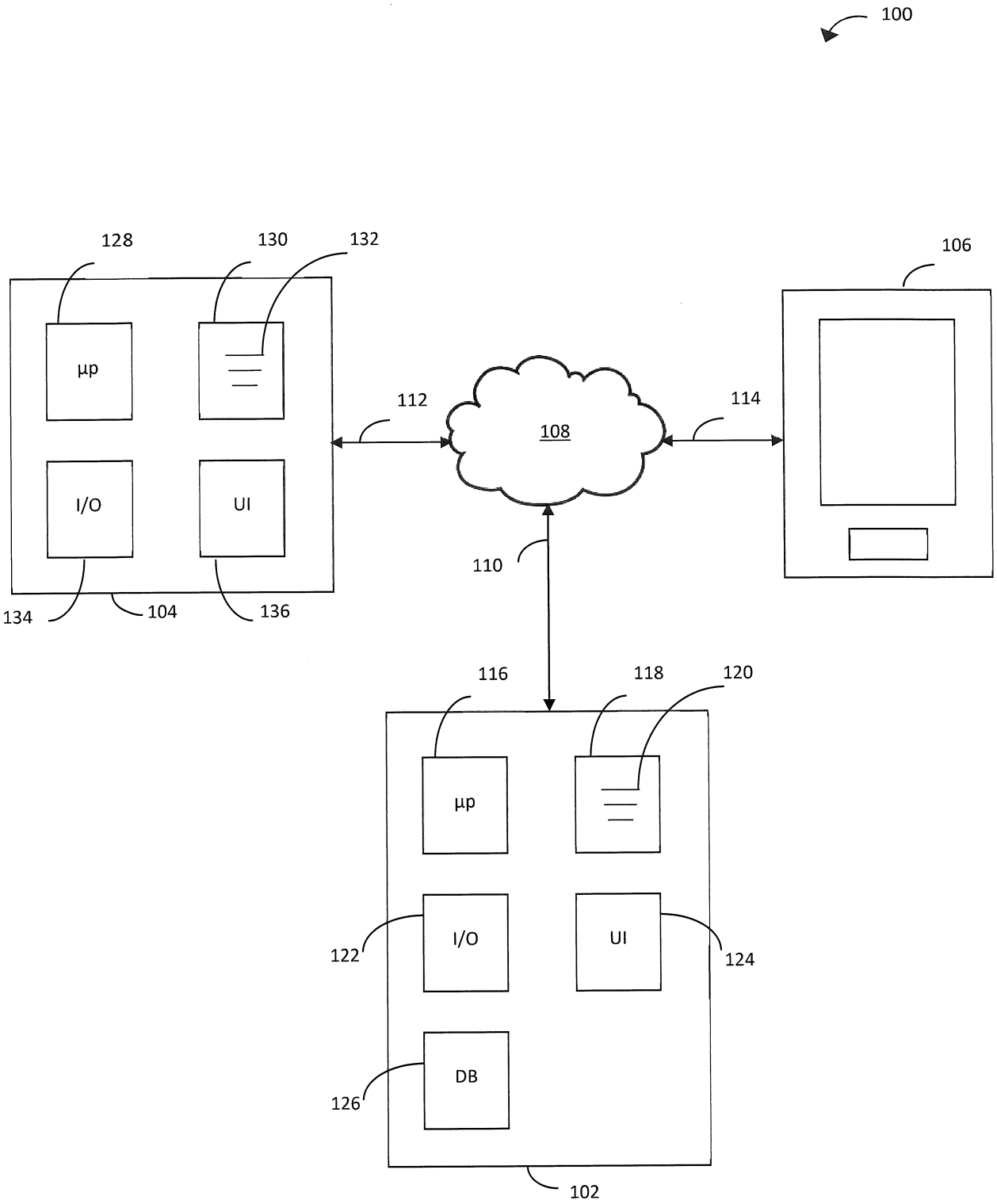
100
128
130
132
106
µp
112
108
114
I/O
UI
110
134
104
136
116
118
120
µp
I/O
UI
122
124
DB
126
102

FIG. 1

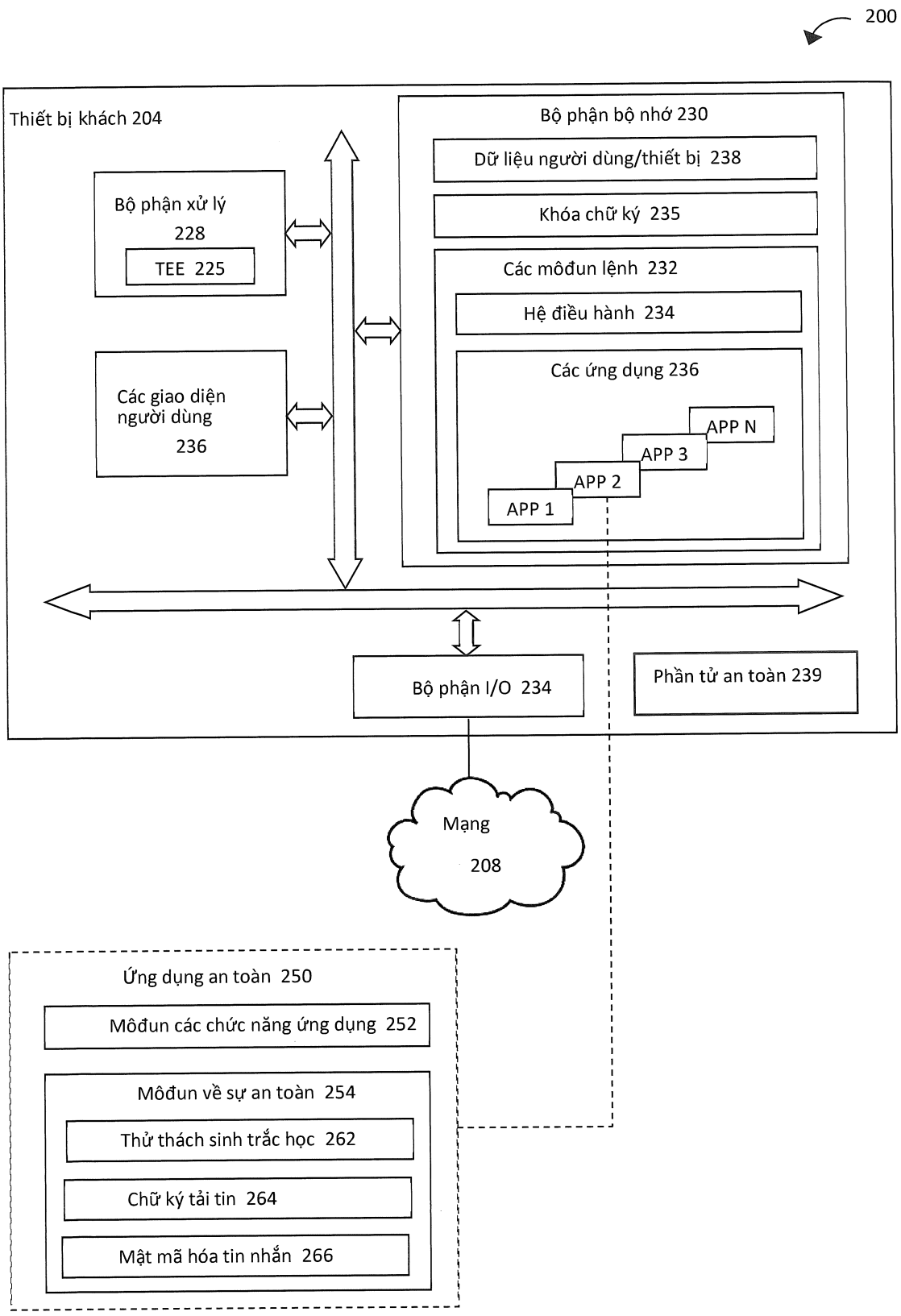
200
Thiết bị khách 204
Bộ phận bộ nhớ 230
Dữ liệu người dùng/thiết bị 238
Khóa chữ ký 235
Bộ phận xử lý
228
TEE 225
Các môđun lệnh 232
Hệ điều hành 234
Các ứng dụng 236
Các giao diện người dùng
236
APP N
APP 3
APP 2
APP 1
Bộ phận I/O 234
Phần tử an toàn 239
Mạng
208
Ứng dụng an toàn 250
Môđun các chức năng ứng dụng 252
Môđun về sự an toàn 254
Thử thách sinh trắc học 262
Chữ ký tải tin 264
Mật mã hóa tin nhắn 266

FIG. 2

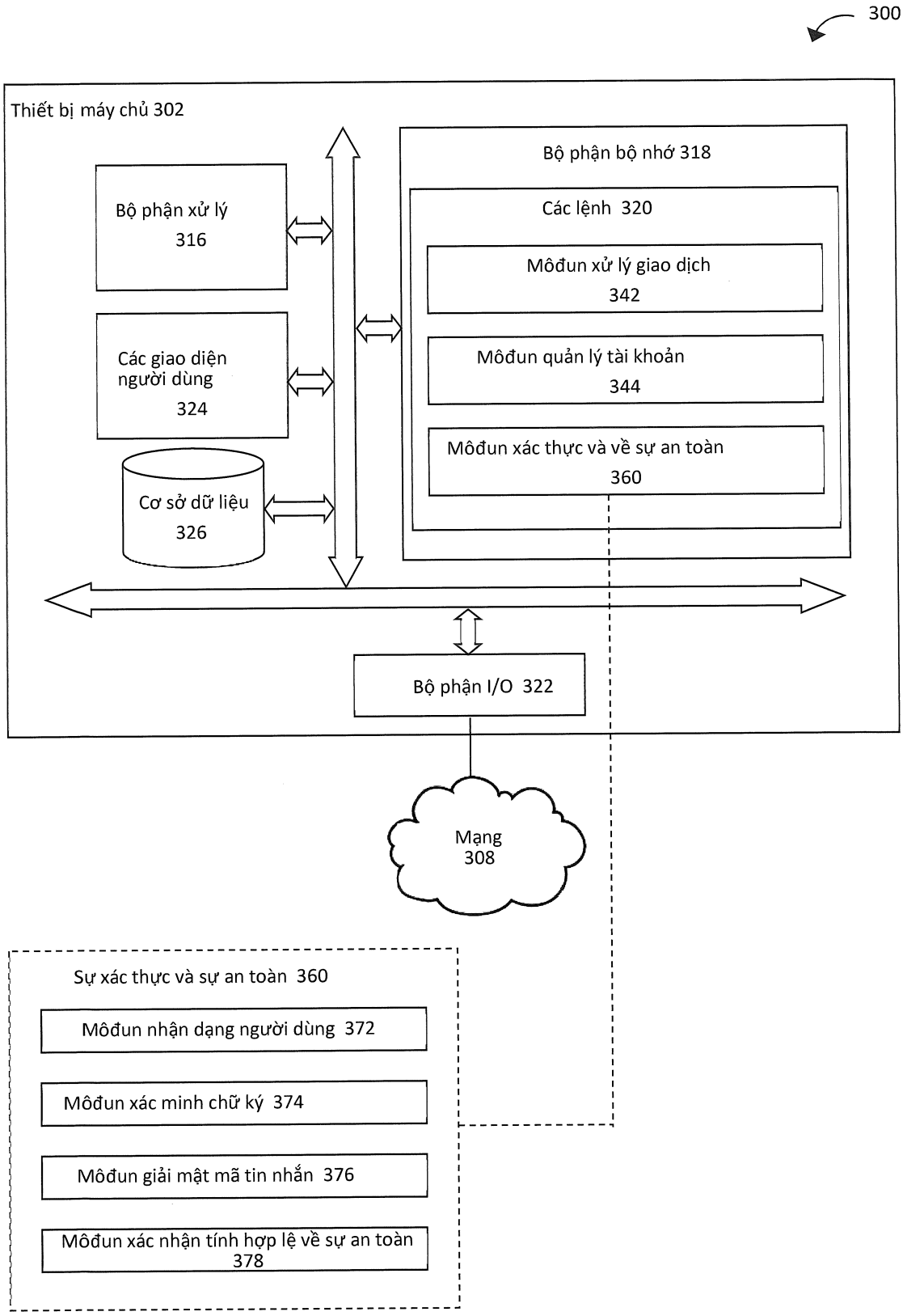
300
Thiết bị máy chủ 302
Bộ phận bộ nhớ 318
Bộ phận xử lý
316
Các lệnh 320
Môđun xử lý giao dịch
342
Các giao diện
người dùng
324
Môđun quản lý tài khoản
344
Môđun xác thực và về sự an toàn
360
Cơ sở dữ liệu
326
Bộ phận I/O 322
Mạng
308
Sự xác thực và sự an toàn 360
Môđun nhận dạng người dùng 372
Môđun xác minh chữ ký 374
Môđun giải mật mã tin nhắn 376
Môđun xác nhận tính hợp lệ về sự an toàn
378

FIG. 3

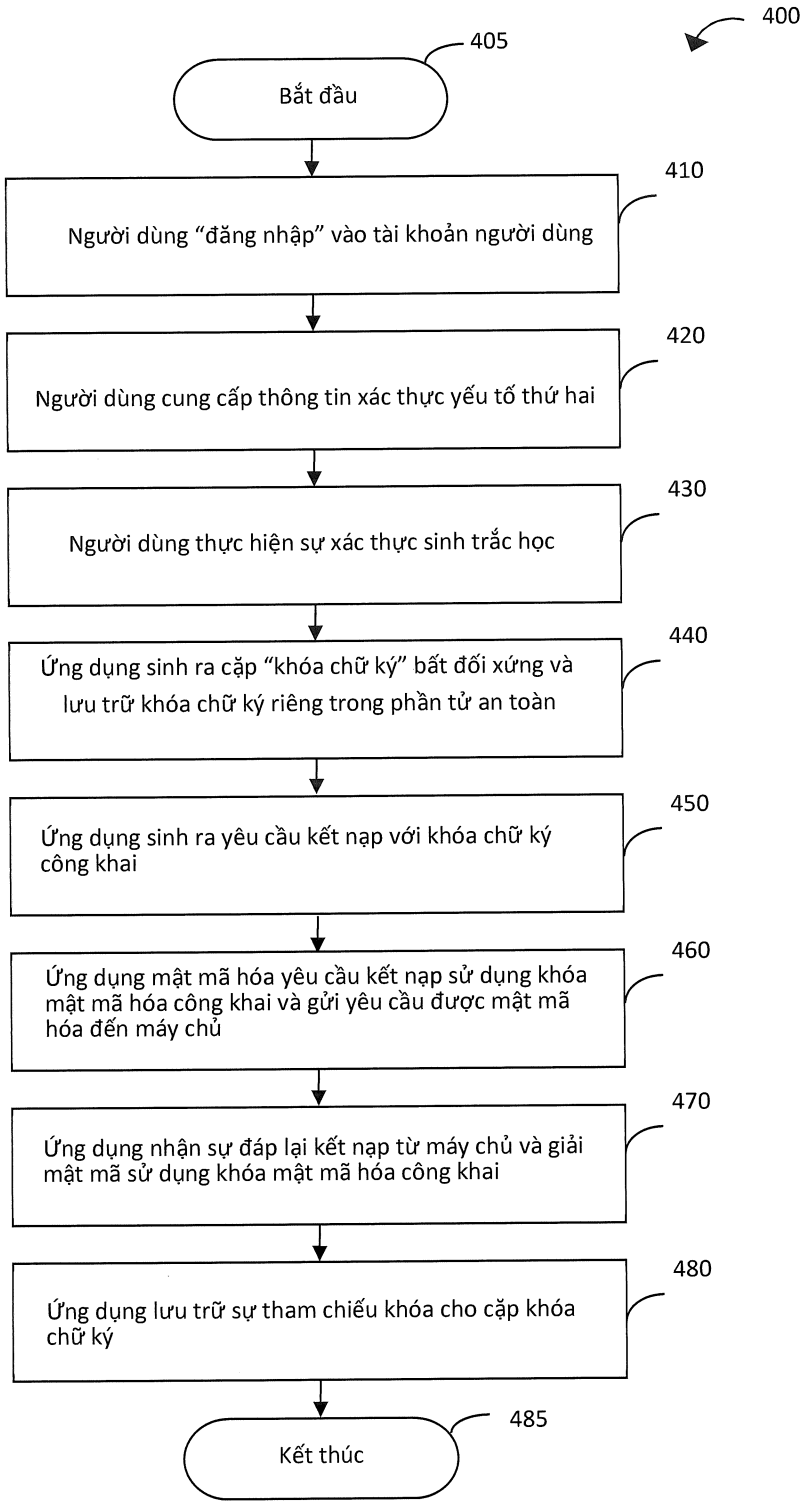
400
405
Bắt đầu
410
Người dùng "đăng nhập" vào tài khoản người dùng
420
Người dùng cung cấp thông tin xác thực yếu tố thứ hai
430
Người dùng thực hiện sự xác thực sinh trắc học
440
Ứng dụng sinh ra cặp "khóa chữ ký" bất đối xứng và lưu trữ khóa chữ ký riêng trong phần tử an toàn
450
Ứng dụng sinh ra yêu cầu kết nạp với khóa chữ ký công khai
460
Ứng dụng mật mã hóa yêu cầu kết nạp sử dụng khóa mật mã hóa công khai và gửi yêu cầu được mật mã hóa đến máy chủ
470
Ứng dụng nhận sự đáp lại kết nạp từ máy chủ và giải mật mã sử dụng khóa mật mã hóa công khai
480
Ứng dụng lưu trữ sự tham chiếu khóa cho cặp khóa chữ ký
485
Kết thúc

FIG. 4

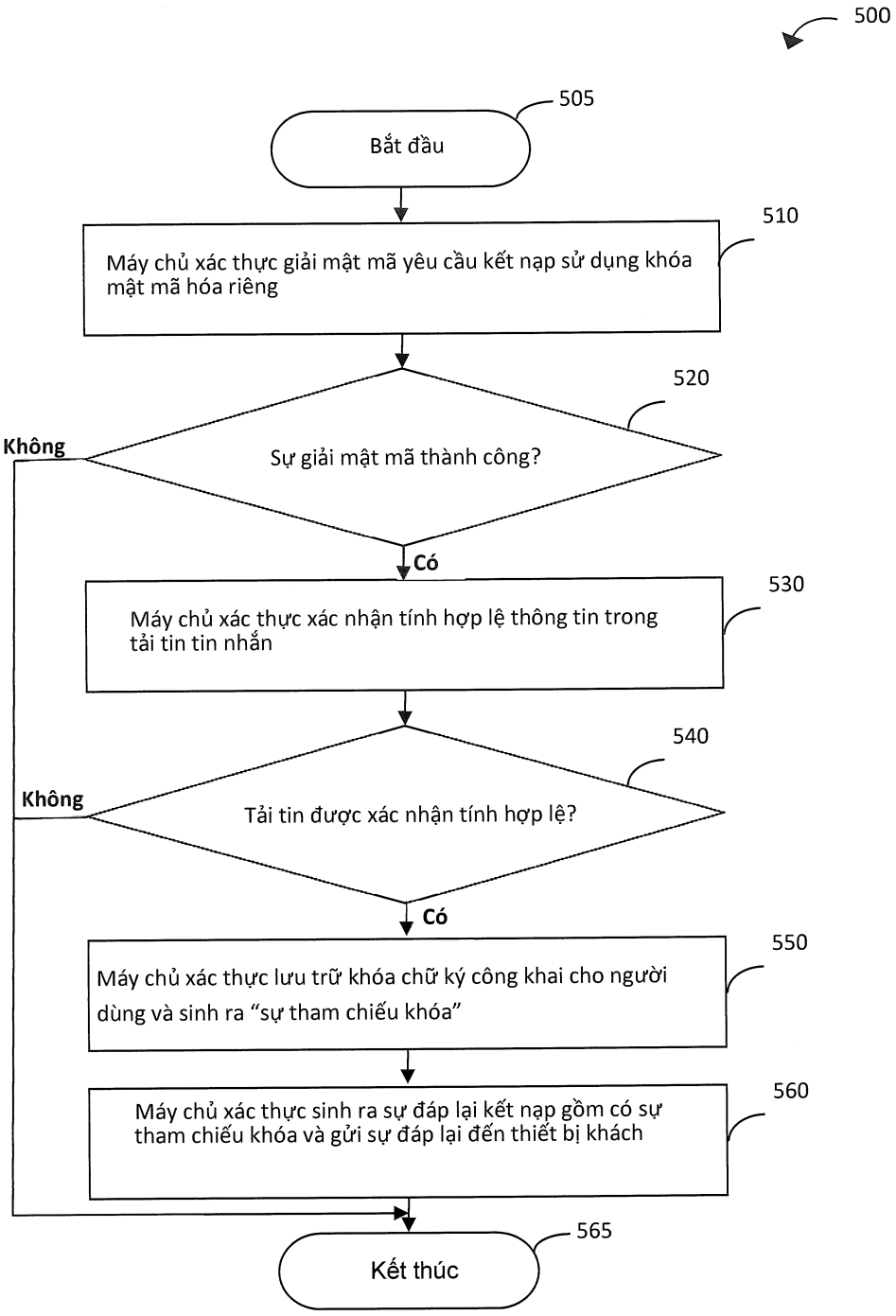
500
505
Bắt đầu
510
Máy chủ xác thực giải mật mã yêu cầu kết nạp sử dụng khóa mật mã hóa riêng
520
Sự giải mật mã thành công?
Không
Có
530
Máy chủ xác thực xác nhận tính hợp lệ thông tin trong tải tin tin nhắn
540
Tải tin được xác nhận tính hợp lệ?
Không
Có
550
Máy chủ xác thực lưu trữ khóa chữ ký công khai cho người dùng và sinh ra "sự tham chiếu khóa"
560
Máy chủ xác thực sinh ra sự đáp lại kết nạp gồm có sự tham chiếu khóa và gửi sự đáp lại đến thiết bị khách
565
Kết thúc

FIG. 5

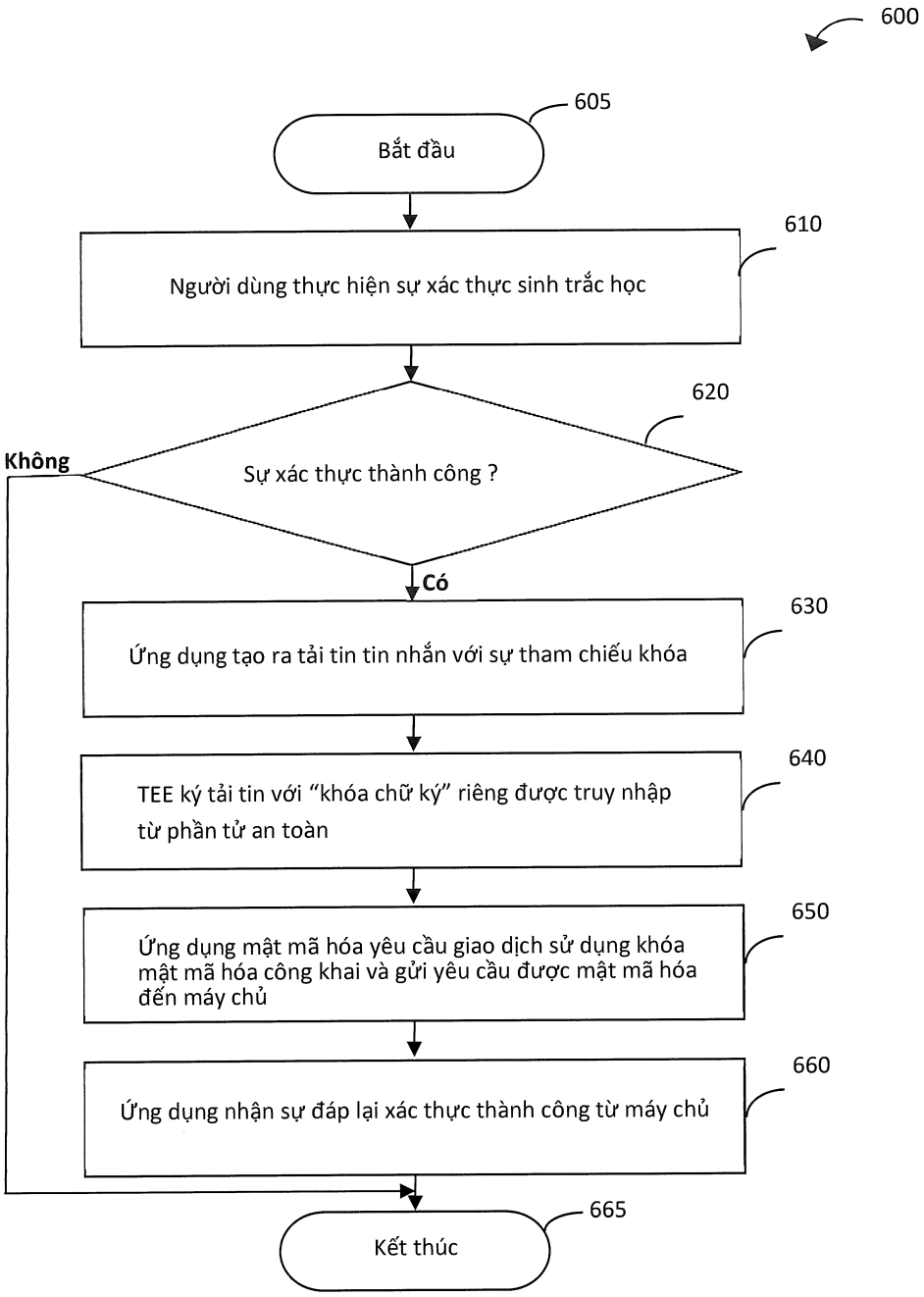
600
605
Bắt đầu
610
Người dùng thực hiện sự xác thực sinh trắc học
620
Sự xác thực thành công ?
Không
Có
630
Ứng dụng tạo ra tải tin tin nhắn với sự tham chiếu khóa
640
TEE ký tải tin với "khóa chữ ký" riêng được truy nhập từ phần tử an toàn
650
Ứng dụng mật mã hóa yêu cầu giao dịch sử dụng khóa mật mã hóa công khai và gửi yêu cầu được mật mã hóa đến máy chủ
660
Ứng dụng nhận sự đáp lại xác thực thành công từ máy chủ
665
Kết thúc

FIG. 6

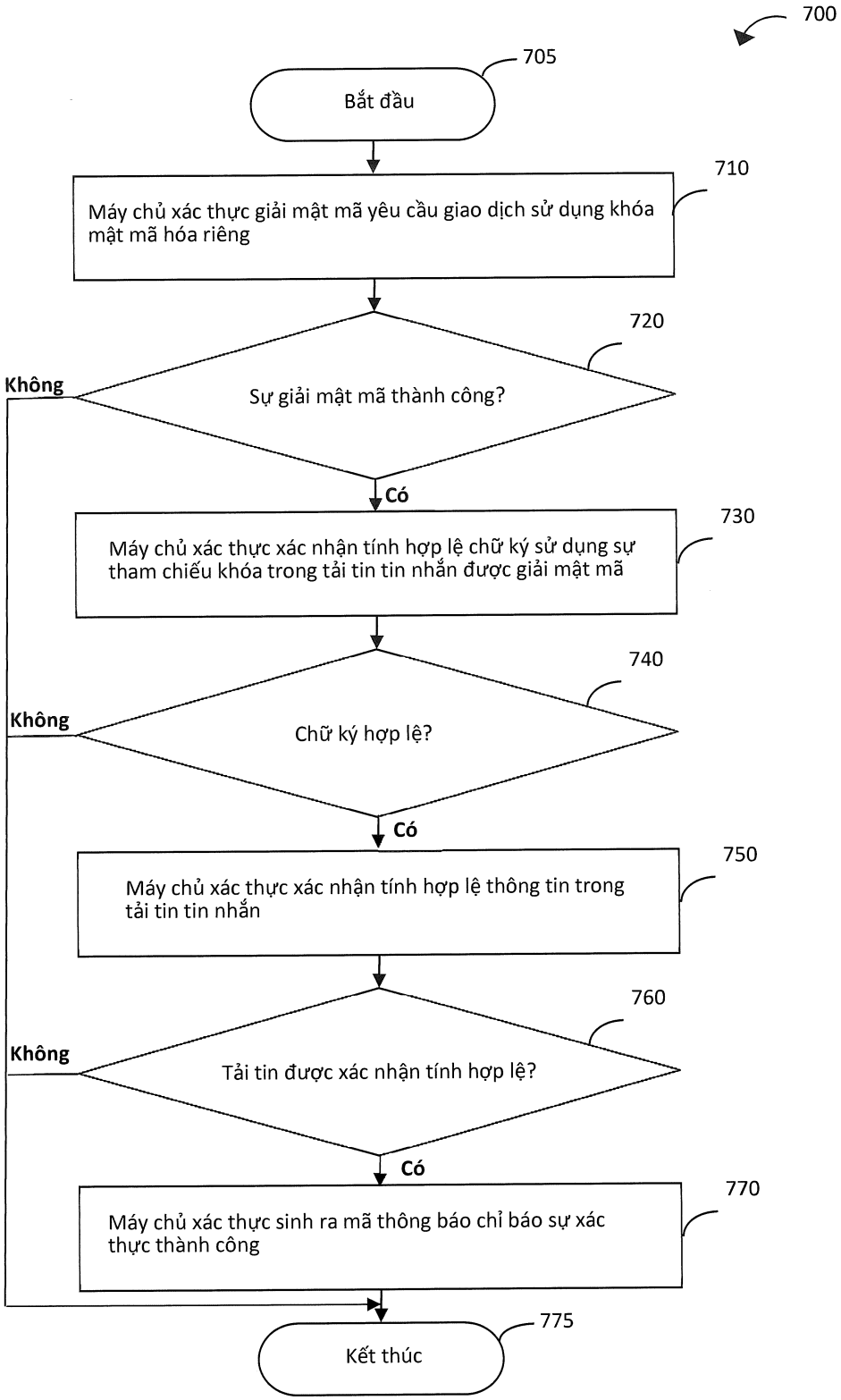
700
705
Bắt đầu
710
Máy chủ xác thực giải mật mã yêu cầu giao dịch sử dụng khóa mật mã hóa riêng
720
Sự giải mật mã thành công?
Không
Có
730
Máy chủ xác thực xác nhận tính hợp lệ chữ ký sử dụng sự tham chiếu khóa trong tải tin tin nhắn được giải mật mã
740
Chữ ký hợp lệ?
Không
Có
750
Máy chủ xác thực xác nhận tính hợp lệ thông tin trong tải tin tin nhắn
760
Tải tin được xác nhận tính hợp lệ?
Không
Có
770
Máy chủ xác thực sinh ra mã thông báo chỉ báo sự xác thực thành công
775
Kết thúc

FIG. 7