



(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)



1-0053354

(51)^{2020.01} H04W 8/26; H04W 12/04; H04W 12/06 (13) B

(21) 1-2020-06415

(22) 04/04/2019

(86) PCT/EP2019/058530 04/04/2019

(87) WO2019/193105 10/10/2019

(30) 201841013099 05/04/2018 IN

(45) 25/11/2025 452

(43) 25/03/2021 396A

(73) NOKIA TECHNOLOGIES OY (FI)

Karakaari 7, 02610 Espoo, Finland

(72) NAIR, Suresh (US); JERICHOW, Anja (DE); BYKAMPADI, Nagendra S (IN);
SCHOINIANAKIS, Dimitrios (DE).

(74) Công ty Luật TNHH ROUSE Việt Nam (ROUSE LEGAL VIETNAM LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ NGƯỜI DÙNG ĐỂ QUẢN LÝ MÃ ĐỊNH DANH
THUÊ BAO THỐNG NHẤT TRONG CÁC HỆ THỐNG TRUYỀN THÔNG

(21) 1-2020-06415

(57) Sáng chế đề xuất phương pháp bao gồm bước sau. Ở thiết bị người sử dụng cụ thể trong hệ thống truyền thông, cấu trúc dữ liệu mã định danh thuê bao thống nhất được xây dựng. Cấu trúc dữ liệu mã định danh thuê bao thống nhất bao gồm nhiều trường mà xác định thông tin cho một loại được chọn trong số hai hoặc nhiều loại mã định danh thuê bao và các tham số có thể chọn được kết hợp với loại mã định danh thuê bao đã chọn, và trong đó thông tin trong cấu trúc dữ liệu mã định danh thuê bao thống nhất có thể sử dụng được bởi thiết bị người dùng cụ thể để truy cập một hoặc nhiều mạng được kết hợp với hệ thống truyền thông dựa trên kịch bản xác thực tương ứng với loại mã định danh thuê bao đã chọn. Ví dụ, trong các kịch bản xác thực khác nhau, thiết bị người dùng cụ thể sử dụng cấu trúc dữ liệu mã định danh thuê bao thống nhất để cung cấp mã định danh thuê bao phù hợp (ví dụ, SUPI, SUCI hoặc IMSI) và các tham số kết hợp cho kịch bản xác thực cho trước.

Trường	Độ dài (bit)
Loại mã định danh (SUPI, SUCI, IMSI) <u>414</u>	2 bit
Tắt/bật sự mã hóa <u>408</u>	1 bit
Mã định danh thuật toán MÃ HÓA <u>426</u>	4 bit
Đường cong ECIES được chọn cho sự mã hóa <u>416</u>	4 bit
Khóa công khai tạm thời của người gửi <u>418</u>	256 bit
Độ dài của MSIN được mã hóa <u>420</u>	4 (128 bit , 192 bit , 256 bit , 512 bit)
MSIN được mã hóa <u>422</u>	(Độ dài được quy định trong trường 420)
MSIN MAC (Sự xác thực bản tin của trường MSIN được tính bằng cách sử dụng các đường cong ECIES) <u>424</u>	256bit
Tham số lựa chọn UDM <u>406</u>	8 bit
MCC <u>402</u>	24 bit (3 chữ số)
MNC <u>404</u>	24 bit (3 chữ số)
KDF được sử dụng cho sự mã hóa <u>410</u>	3bit
Các tham số tùy chọn KDF <u>412</u>	n bit

FIG. 5

Lĩnh vực kỹ thuật được đề cập

Sáng chế nói chung đề cập đến các hệ thống truyền thông, và cụ thể hơn, nhưng không dành riêng, đề cập đến quản lý mã định danh thuê bao người dùng trong các hệ thống đó.

Tình trạng kỹ thuật của sáng chế

Phần này giới thiệu các khía cạnh mà có thể giúp cho dễ dàng hiểu rõ hơn về sáng chế. Theo đó, các nội dung của phần này cần được hiểu theo góc độ này và không được hiểu là sự thừa nhận về những gì có trong kỹ thuật trước đó hoặc những gì không có trong kỹ thuật trước đó.

Công nghệ viễn thông di động không dây thế hệ thứ tư (4G), còn được gọi là công nghệ tiến hóa dài hạn (Long Term Evolution - LTE), được thiết kế để cung cấp đa phương tiện di động dung lượng cao với các tốc độ dữ liệu cao, đặc biệt cho sự tương tác của con người. Công nghệ thế hệ tiếp theo hoặc thế hệ thứ năm (5G) hướng đến không chỉ được sử dụng cho sự tương tác giữa con người mà còn cho các giao tiếp kiểu máy móc trong các mạng được gọi là Internet vạn vật (Internet of Things - IoT).

Trong khi các mạng 5G được nhằm để kích hoạt các dịch vụ IoT quy mô lớn (ví dụ, số lượng rất lớn các thiết bị có dung lượng hạn chế) và các dịch vụ IoT nhiệm vụ then chốt (ví dụ, yêu cầu độ tin cậy cao), các cải tiến đối với các dịch vụ truyền thông di động kế thừa được hỗ trợ dưới dạng các dịch vụ băng thông rộng di động nâng cao (enhanced mobile broadband - eMBB) cung cấp truy cập Internet không dây được cải thiện cho các thiết bị di động.

Trong hệ thống truyền thông làm ví dụ, thiết bị người dùng (UE 5G trong mạng 5G hoặc, rộng hơn là, UE) chẳng hạn như thiết bị đầu cuối di động (thuê bao) giao tiếp qua giao diện vô tuyến với trạm gốc hoặc điểm truy cập được gọi là gNB trong mạng 5G. Điểm truy cập (ví dụ, gNB) là một phần minh họa của mạng truy cập của hệ thống truyền thông. Ví dụ, trong mạng 5G, mạng truy cập được gọi là hệ thống 5G và được mô tả trong chỉ dẫn kỹ thuật (Technical Specification - TS) 3GPP 23.501, V15.0.0, có tiêu đề “Các dịch vụ nhóm và các khía cạnh hệ thống của chỉ dẫn kỹ thuật; kiến trúc hệ thống cho hệ thống 5G”, phần nội dung của nó được kết hợp trong toàn bộ tài liệu này bằng cách viện dẫn. Nói chung, điểm truy cập (ví dụ, gNB) cung cấp sự truy cập cho UE vào mạng lõi (core network - CN), mà sau đó cung cấp sự truy cập cho UE tới các

UE khác và/hoặc mạng dữ liệu chẳng hạn như mạng dữ liệu gói (ví dụ, Internet). Hơn nữa, các thủ tục truy cập mạng 5G được mô tả trong chỉ dẫn kỹ thuật (TS) 3GPP 23.502, V15.1.0, có tựa đề “Các dịch vụ nhóm và các khía cạnh hệ thống của chỉ dẫn kỹ thuật; các thủ tục cho hệ thống 5G”, phần nội dung của nó được kết hợp trong toàn bộ tài liệu này bằng cách viện dẫn. Tiếp nữa, chỉ dẫn kỹ thuật (TS) 3GPP 33.501, V0.7.0, có tựa đề “Các dịch vụ nhóm và các khía cạnh hệ thống của chỉ dẫn kỹ thuật; kiến trúc bảo mật và các thủ tục cho hệ thống 5G”, phần nội dung của nó được kết hợp trong toàn bộ tài liệu này bằng cách viện dẫn, còn mô tả các chi tiết về quản lý bảo mật kết hợp với mạng 5G.

Trong các mạng 5G, UE tương thích 5G có thể bao gồm mã định danh thuê bao ẩn (Concealed Subscription Identifier - SUCI) như được mô tả trong tài liệu 3GPP TS 33.501 trong thủ tục yêu cầu đăng ký được mô tả trong tài liệu 3GPP TS 23.502. SUCI là dạng ẩn (được mã hóa) của mã định danh thường trực của thuê bao (Subscriber Permanent Identifier - SUPI). Trong các mạng (LTE) 4G kế thừa, mã định danh thuê bao được sử dụng là mã định danh trạm di động quốc tế (International Mobile Station Identifier - IMSI) như được định nghĩa trong chỉ dẫn kỹ thuật (TS) 3GPP 23.003, V15.3.0, có tựa đề “Mạng lõi nhóm và các thiết bị đầu cuối trong chỉ dẫn kỹ thuật; đánh số, đánh địa chỉ và nhận dạng”, phần nội dung của nó được kết hợp trong toàn bộ tài liệu này bằng cách viện dẫn. Việc quản lý các mã định danh thuê bao như vậy có thể có những thách thức đáng kể.

3GPP; mạng lõi nhóm và các thiết bị đầu cuối trong chỉ dẫn kỹ thuật; giao thức tầng không truy cập cho các hệ thống 5G (5G Systems - 5GS); giai đoạn 3 (Bản phát hành 15) bộc lộ phương pháp dùng cho thiết bị người dùng yêu cầu và có được một loại cụ thể trong số các loại mã định danh thuê bao di động hiện có.

WO 2014/053197 A1 bộc lộ phương pháp quản lý chính sách và còn bộc lộ các thiết bị nâng cao cho phép hỗ trợ quản lý hồ sơ cộng đồng của người dùng đăng ký cho nhiều thuê bao. Thêm nữa, đơn này còn bộc lộ cách thức tạo và thực thi chức năng chính sách và quy định tính phí cộng đồng có nguồn gốc từ các hồ sơ cộng đồng của người dùng và tốt hơn là được cài đặt trong lúc thiết lập phiên cho người dùng đầu tiên. Các phiên cần được thiết lập cho những người dùng tiếp theo trong số nhiều người dùng có thể được thực thi bởi chức năng chính sách và quy định tính phí cộng đồng nêu trên có thể được cho phép mà không cần xử lý hồ sơ của họ trên cơ sở từng cá nhân.

3GPP; 23.501: hiệu chỉnh thuật ngữ SUPI; bản dự thảo 3GPP bộc lộ “mã định danh thường trực của thuê bao” để có thể phân bổ mã định danh thường trực của thuê bao (SUPI) 5G duy nhất trên toàn cầu cho mỗi thuê bao trong hệ thống 5G.

3GPP; SA WG3; LS về các khía cạnh bảo mật của ECIES để làm ẩn IMSI hoặc SUPI bộc lộ sự tạo thành các mạng di động tiếp theo (sau đây gọi là 5G). Một thuật ngữ mới và dùng chung cho SUPI (mã định danh thường trực của thuê bao) được bộc lộ mà được đề xuất sử dụng để biểu thị mã định danh thường trực của thuê bao 5G duy nhất trên toàn cầu. D4 còn đề xuất việc làm ẩn IMSI hoặc SUPI qua song vô tuyến trong hệ thống 5G theo ECIES (Elliptic Curve Integrated Encryption Scheme - sơ đồ mã hóa tích hợp đường cong elip).

Bản chất kỹ thuật của sáng chế

Các phương án minh họa đề xuất các kỹ thuật cải tiến để quản lý các mã định danh thuê bao trong các hệ thống truyền thông.

Ví dụ, theo một phương án minh họa, phương pháp bao gồm bước sau. Ở thiết bị người sử dụng cụ thể trong hệ thống truyền thông, cấu trúc dữ liệu mã định danh thuê bao thống nhất được xây dựng. Cấu trúc dữ liệu mã định danh thuê bao thống nhất bao gồm nhiều trường mà xác định thông tin cho một loại được chọn trong số hai hoặc nhiều loại mã định danh thuê bao và các tham số có thể chọn được kết hợp với loại mã định danh thuê bao đã chọn, và trong đó thông tin trong cấu trúc dữ liệu mã định danh thuê bao thống nhất có thể sử dụng được bởi thiết bị người dùng cụ thể để truy cập một hoặc nhiều mạng được kết hợp với hệ thống truyền thông dựa trên kịch bản xác thực tương ứng với loại mã định danh thuê bao đã chọn.

Các phương án minh họa khác được đề xuất dưới dạng phương tiện lưu trữ có thể đọc được bằng máy tính không tạm thời có chứa trong đó mã chương trình có thể thực thi mà khi được thực thi bởi bộ xử lý làm cho bộ xử lý thực hiện các bước ở trên. Các phương án minh họa khác nữa bao gồm thiết bị với bộ xử lý và bộ nhớ được cấu hình để thực hiện các bước ở trên.

Ưu điểm là, trong các kịch bản xác thực khác nhau, thiết bị người dùng cụ thể sử dụng cấu trúc dữ liệu mã định danh thuê bao thống nhất để tạo ra mã định danh thuê bao phù hợp (ví dụ, SUPI, SUCI hoặc IMSI) và các tham số kết hợp cho kịch bản xác thực cho trước.

Các ưu điểm và các dấu hiệu này và các ưu điểm và các dấu hiệu khác của các phương án được mô tả ở đây sẽ trở nên rõ ràng hơn từ các hình vẽ kèm theo và phần mô tả chi tiết sau đây.

Mô tả vắn tắt các hình vẽ

Fig.1 minh họa hệ thống truyền thông mà với hệ thống này một hoặc nhiều phương án minh họa có thể được thực hiện.

Fig.2 minh họa thiết bị người dùng và phần tử/chức năng mạng để cung cấp sự quản lý mã định danh thuê bao trong các thủ tục xác thực mà với chúng một hoặc nhiều phương án minh họa có thể được thực hiện.

Fig.3A minh họa định dạng IMSI mà với định dạng này một hoặc nhiều phương án minh họa có thể được thực hiện.

Fig.3B minh họa định dạng SUPI mà với định dạng này một hoặc nhiều phương án minh họa có thể được thực hiện.

Fig.3C minh họa định dạng SUCI mà với định dạng này một hoặc nhiều phương án minh họa có thể được thực hiện.

Fig.4 minh họa định dạng mã định danh thuê bao thống nhất, theo phương án minh họa.

Fig.5 minh họa các độ dài trường làm ví dụ của định dạng mã định danh thuê bao thống nhất, theo phương án minh họa.

Fig.6 minh họa định dạng mã định danh thuê bao thống nhất, theo phương án minh họa khác.

Fig.7 minh họa phương pháp luận thiết bị người dùng để sử dụng định dạng mã định danh thuê bao thống nhất, theo phương án minh họa.

Fig.8 minh họa phương pháp luận thực thể mạng để sử dụng định dạng mã định danh thuê bao thống nhất, theo phương án minh họa.

Mô tả chi tiết sáng chế

Các phương án sẽ được minh họa ở đây cùng với các hệ thống truyền thông làm ví dụ và các kỹ thuật liên quan để tạo ra sự quản lý mã định danh thuê bao trong các thủ tục xác thực và các thủ tục khác trong các hệ thống truyền thông. Tuy nhiên, cần hiểu là phạm vi của các yêu cầu bảo hộ không bị giới hạn ở các loại cụ thể của các hệ thống truyền thông và/hoặc các quy trình xử lý được bộc lộ. Các phương án có thể được thực hiện trong nhiều loại hệ thống truyền thông khác, sử dụng các quy trình và hoạt động thay thế. Ví dụ, mặc dù được minh họa trong ngữ cảnh là các hệ thống di động không dây sử dụng các phần tử hệ thống 3GPP như hệ thống 3GPP thế hệ tiếp theo (5G), các phương án được bộc lộ có thể được làm cho phù hợp một cách đơn giản cho nhiều loại hệ thống truyền thông khác.

Theo các phương án minh họa được thực hiện trong môi trường hệ thống truyền thông 5G, một hoặc nhiều chỉ dẫn kỹ thuật 3GPP (technical specifications - TS) và các báo cáo kỹ thuật (technical reports - TR) có thể cung cấp sự giải thích thêm về các phần tử/chức năng mạng và/hoặc các hoạt động mà có thể tương tác với các phần của các giải pháp sáng chế, ví dụ, 3GPP TS 23.003 23.501, 23.502 và 33.501 được viện dẫn ở trên. Các tài liệu 3GPP TS/TR khác có thể cung cấp các chi tiết thông thường khác mà người có trình độ trung bình trong lĩnh vực kỹ thuật sẽ nhận ra. Tuy nhiên, mặc dù rất phù hợp với các tiêu chuẩn 3GPP liên quan đến 5G, nhưng các phương án không nhất thiết nhằm giới hạn vào các tiêu chuẩn cụ thể bất kỳ.

Các phương án minh họa đề cập đến sự quản lý mã định danh thuê bao được liên kết với mạng 5G. Trước khi mô tả các phương án minh họa như vậy, phần mô tả chung về các thành phần chính của mạng 5G sẽ được mô tả ở dưới theo ngữ cảnh của các hình vẽ Fig.1 và Fig.2.

Fig.1 thể hiện hệ thống truyền thông 100 mà các phương án minh họa được thực hiện ở trong hệ thống này. Cần phải hiểu rằng các phần tử được thể hiện trong hệ thống truyền thông 100 nhằm biểu diễn cho các chức năng chính được cung cấp trong hệ thống, ví dụ, chức năng truy cập UE, chức năng quản lý di động, chức năng xác thực, chức năng công dịch vụ, v.v. Như, các khối được thể hiện trên Fig.1 giới thiệu các phần tử cụ thể trong các mạng 5G mà cung cấp các chức năng chính này. Tuy nhiên, các phần tử mạng khác có thể được sử dụng để thực hiện một số hoặc tất cả các chức năng chính được biểu diễn. Đồng thời, cần hiểu rằng không phải tất cả các chức năng của mạng 5G đều được mô tả trên Fig.1. Thay vào đó, các chức năng mà giúp giải thích các phương án minh họa được biểu diễn. Các hình vẽ tiếp theo có thể mô tả một số phần tử/chức năng bổ sung.

Theo đó, như được thể hiện, hệ thống truyền thông 100 bao gồm thiết bị người dùng (user equipment - UE) 102 mà giao tiếp qua giao diện vô tuyến 103 với điểm truy cập (gNB) 104. UE 102 có thể là trạm di động, và trạm di động này có thể bao gồm, bằng cách ví dụ, điện thoại di động, máy tính hoặc loại thiết bị liên lạc bất kỳ khác. Do đó, thuật ngữ “thiết bị người dùng” như được sử dụng ở đây được nhằm hiểu theo nghĩa rộng, để bao hàm nhiều loại trạm di động, trạm thuê bao khác nhau hoặc, tổng quát hơn, là các thiết bị liên lạc, bao gồm các ví dụ như dạng kết hợp của thẻ dữ liệu được lắp vào máy tính xách tay hoặc thiết bị khác như điện thoại thông minh. Các thiết bị liên lạc như vậy cũng nhằm bao gồm các thiết bị thường được gọi là thiết bị đầu cuối truy cập.

Theo một phương án, UE 102 bao gồm phần thẻ mạch tích hợp toàn cầu (Universal Integrated Circuit Card - UICC) và phần thiết bị di động (Mobile Equipment

- ME). UICC là phần phụ thuộc người dùng của UE và chứa ít nhất một mô đun nhận dạng thuê bao toàn cầu (Universal Subscriber Identity Module - USIM) và phần mềm ứng dụng thích hợp. USIM lưu trữ an toàn mã định danh thuê bao thường trực và khóa liên quan của nó, mà được sử dụng để nhận dạng và xác thực các thuê bao để truy cập các mạng. ME là phần độc lập với người dùng của UE và chứa các chức năng của thiết bị đầu cuối (terminal equipment - TE) và các chức năng đầu cuối di động (mobile termination - MT) khác nhau.

Điểm truy cập 104 là phần minh họa của mạng truy cập của hệ thống truyền thông 100. Mạng truy cập này có thể bao gồm, ví dụ, hệ thống 5G có nhiều trạm gốc và một hoặc nhiều chức năng điều khiển mạng vô tuyến liên quan. Các trạm gốc và các chức năng điều khiển mạng vô tuyến có thể là các thực thể riêng biệt về mặt logic, nhưng theo một số phương án có thể được triển khai trong cùng phần tử mạng vật lý, chẳng hạn như, bộ định tuyến trạm gốc hoặc điểm truy cập di động femto.

Điểm truy cập 104 theo phương án minh họa này được ghép hoạt động với các chức năng quản lý di động 106. Trong mạng 5G, chức năng quản lý di động được thực hiện bởi chức năng quản lý di động và truy cập (Access and Mobility Management Function - AMF). Chức năng neo bảo mật (Security Anchor Function - SEAF) cũng có thể được thực hiện với AMF để cho phép UE kết nối an toàn với chức năng quản lý di động. Chức năng quản lý di động, như được sử dụng ở đây, là phần tử hoặc chức năng (ví dụ, thực thể) trong phần mạng lõi (core network - CN) của hệ thống truyền thông mà quản lý hoặc ngoài ra tham gia vào, trong số các hoạt động mạng khác, các hoạt động truy cập và di động (bao gồm xác thực/cấp quyền) với UE (thông qua điểm truy cập 104). Ở đây, AMF cũng có thể được gọi, một cách tổng quát hơn, là thực thể quản lý di động và truy cập.

AMF 106 theo phương án minh họa này được ghép hoạt động với các chức năng thuê bao thường trú 108, ví dụ, một hoặc nhiều chức năng mà lưu trú trong mạng thường trú của thuê bao. Như được thể hiện, một số chức năng này bao gồm chức năng quản lý dữ liệu thống nhất (Unified Data Management - UDM), cũng như chức năng máy chủ xác thực (Authentication Server Function - AUSF). AUSF và UDM (theo cách riêng hoặc chung cùng với máy chủ quản lý thuê bao thường trú 4G hoặc HSS) cũng có thể được gọi chung ở đây, một cách tổng quát hơn, là thực thể xác thực. Ngoài ra, các chức năng thuê bao thường trú có thể bao gồm, nhưng không giới hạn ở, chức năng lựa chọn ngăn mạng (Network Slice Selection Function - NSSF), chức năng tiếp xúc mạng (Network Exposure Function - NEF), chức năng kho chứa mạng (Network Repository

Function - NRF), chức năng quản lý chính sách (Policy Control Function - PCF) và chức năng ứng dụng (Application Function - AF).

Điểm truy cập 104 cũng được ghép hoạt động với chức năng cổng dịch vụ, ví dụ, chức năng quản lý phiên (Session Management Function - SMF) 110, mà được ghép hoạt động với chức năng mặt phẳng người dùng (User Plane Function - UPF) 112. UPF 112 được ghép hoạt động với mạng dữ liệu gói, ví dụ, Internet 114. Các hoạt động và các chức năng điển hình khác của các phần tử mạng này không được mô tả ở đây do chúng không phải là trọng tâm của các phương án minh họa và có thể được tìm thấy trong tài liệu 3GPP 5G thích hợp.

Cần hiểu là sự bố trí cụ thể này của các phần tử hệ thống chỉ làm ví dụ, và các loại và các sự bố trí khác của các phần tử bổ sung hoặc thay thế có thể được sử dụng để thực hiện hệ thống truyền thông theo các phương án khác. Ví dụ, theo các phương án khác, hệ thống 100 có thể bao gồm các phần tử/chức năng khác không được thể hiện rõ ràng ở đây.

Theo đó, sự bố trí trên Fig.1 chỉ là một cấu hình làm ví dụ của hệ thống di động không dây, và nhiều cấu hình thay thế của các phần tử hệ thống có thể được sử dụng. Ví dụ, mặc dù chỉ các phần tử/chức năng đơn được thể hiện trên phương án của Fig.1, điều này chỉ nhằm mục đích mô tả đơn giản và rõ ràng. Tất nhiên, phương án thay thế cụ thể có thể bao gồm số lượng lớn hơn các phần tử hệ thống như vậy, cũng như các phần tử bổ sung hoặc thay thế thuộc loại thường được kết hợp với sự triển khai hệ thống thông thường.

Cũng cần lưu ý là trong khi Fig.1 minh họa các phần tử hệ thống là các khối chức năng đơn, các mạng con khác nhau mà tạo nên mạng 5G được phân chia thành các phần được gọi là các ngăn mạng. Các ngăn mạng (các phân vùng mạng) bao gồm một loạt các bộ chức năng mạng (network function - NF) (tức là, các chuỗi chức năng) cho từng loại dịch vụ tương ứng mà sử dụng công nghệ ảo hóa chức năng mạng (network function virtualization - NFV) trên cơ sở hạ tầng vật lý chung. Các ngăn mạng được khởi tạo khi cần thiết cho dịch vụ nhất định, ví dụ, dịch vụ eMBB, dịch vụ IoT quy mô lớn và dịch vụ IoT nhiệm vụ then chốt. Do đó, ngăn mạng hoặc chức năng được khởi tạo khi trường hợp là ngăn mạng hoặc chức năng được tạo ra. Theo một số phương án, điều này liên quan đến việc cài đặt hoặc ngoài ra, chạy ngăn mạng hoặc chức năng trên một hoặc nhiều thiết bị máy chủ của cơ sở hạ tầng vật lý bên dưới. UE 102 được cấu hình để truy cập một hoặc nhiều trong số các dịch vụ này qua gNB 104.

Fig.2 là sơ đồ khối của một phần của hệ thống truyền thông 200 bao gồm thiết bị người dùng 202 và phần tử/chức năng mạng 204 để cung cấp quản lý mã định danh thuê bao làm một phần của thủ tục xác thực theo phương án minh họa. Theo một phương án, phần tử/chức năng mạng 204 có thể là UDM (như được mô tả ở trên). Tuy nhiên, cần hiểu là phần tử/chức năng mạng 204 có thể biểu diễn phần tử/chức năng mạng bất kỳ mà có thể cấu hình để cung cấp sự quản lý mã định danh thuê bao và các kỹ thuật xác thực khác được mô tả ở đây.

Thiết bị người dùng 202 bao gồm bộ xử lý 212 được ghép với bộ nhớ 216 và hệ mạch giao diện 210. Bộ xử lý 212 của thiết bị người dùng 202 bao gồm mô đun xử lý xác thực 214 mà có thể được thực hiện ít nhất trong một phần dưới dạng phần mềm được thực thi bởi bộ xử lý. Mô đun xử lý 214 thực hiện quản lý mã định danh thuê bao và các kỹ thuật liên quan khác được mô tả kết hợp với các hình vẽ tiếp theo và các phần khác ở đây. Bộ nhớ 216 của thiết bị người dùng 202 bao gồm mô đun lưu trữ dữ liệu quản lý mã định danh thuê bao 218 mà lưu trữ dữ liệu được tạo ra hoặc ngoài ra được sử dụng trong quản lý mã định danh thuê bao và các hoạt động khác.

Phần tử/chức năng mạng 204 bao gồm bộ xử lý 222 được ghép với bộ nhớ 226 và hệ mạch giao diện 220. Bộ xử lý 222 của phần tử/chức năng mạng 204 bao gồm mô đun xử lý xác thực 224 mà có thể được thực hiện ít nhất trong một phần dưới dạng phần mềm được thực thi bởi bộ xử lý 222. Mô đun xử lý 224 thực hiện các kỹ thuật xác thực bằng cách sử dụng mã định danh thuê bao được cung cấp bởi UE 202 và các kỹ thuật khác được mô tả kết hợp với các hình vẽ tiếp theo và các phần khác ở đây. Bộ nhớ 226 của phần tử/chức năng mạng 204 bao gồm mô đun lưu trữ dữ liệu xử lý xác thực 228 mà lưu trữ dữ liệu được tạo ra hoặc ngoài ra được sử dụng trong các hoạt động xác thực và các hoạt động khác.

Các bộ xử lý 212 và 222 của thiết bị người dùng tương ứng 202 và phần tử/chức năng mạng 204 có thể bao gồm, ví dụ, các bộ vi xử lý, các mạch tích hợp chuyên dụng (application-specific integrated circuits - ASICs), các mảng cổng lập trình được dạng trường (field programmable gate arrays - FPGAs), các bộ xử lý tín hiệu số (digital signal processors - DSPs) hoặc các loại thiết bị xử lý khác hoặc các mạch tích hợp, cũng như các phần hoặc các dạng kết hợp của các phần tử này. Các thiết bị mạch tích hợp này, cũng như các phần hoặc các dạng kết hợp của chúng, là các ví dụ về “hệ mạch điện” như thuật ngữ đó được sử dụng ở đây. Nhiều cách bố trí khác nhau của phần cứng và phần mềm kết hợp hoặc phần sụn có thể được sử dụng khi thực hiện các phương án minh họa.

Các bộ nhớ 216 và 226 của thiết bị người dùng tương ứng 202 và phần tử/chức năng mạng 204 có thể được sử dụng để lưu trữ một hoặc nhiều chương trình phần mềm mà được thực thi bởi các bộ xử lý tương ứng 212 và 222 để thực hiện ít nhất một phần của chức năng được mô tả ở đây. Ví dụ, các hoạt động quản lý mã định danh thuê bao và chức năng xác thực khác như được mô tả kết hợp với các hình vẽ tiếp theo và các phần khác ở đây có thể được thực hiện theo cách đơn giản bằng cách sử dụng mã phần mềm được thực thi bởi các bộ xử lý 212 và 222.

Do đó, một trong những bộ nhớ 216 hoặc 226 đã cho có thể được xem như ví dụ về những gì thường được đề cập ở đây là sản phẩm chương trình máy tính hoặc nói chung hơn là phương tiện lưu trữ có thể đọc được bằng bộ xử lý mà có mã chương trình có thể thực thi được bao gồm trong đó. Các ví dụ khác về phương tiện lưu trữ có thể đọc được bằng bộ xử lý có thể bao gồm các đĩa hoặc các loại phương tiện từ tính hoặc quang học khác, ở dạng kết hợp bất kỳ. Các phương án minh họa có thể bao gồm các sản phẩm được sản xuất bao gồm các sản phẩm chương trình máy tính như vậy hoặc phương tiện lưu trữ có thể đọc được bằng bộ xử lý khác.

Cụ thể hơn, bộ nhớ 216 hoặc 226 có thể bao gồm, ví dụ, bộ nhớ truy cập ngẫu nhiên (random access memory - RAM) điện tử như RAM tĩnh (static RAM - SRAM), RAM động (dynamic RAM - DRAM) hoặc các loại bộ nhớ điện tử khả biến hoặc không khả biến khác. Loại sau có thể bao gồm, ví dụ, các bộ nhớ không khả biến như bộ nhớ chớp, RAM từ tính (magnetic RAM - MRAM), RAM đổi pha (phase-change RAM - PC-RAM) hoặc RAM điện sắt (ferroelectric RAM - FRAM). Thuật ngữ “bộ nhớ” như được sử dụng ở đây được nhằm hiểu theo nghĩa rộng, và có thể ngoài ra hoặc theo cách khác bao hàm, ví dụ, bộ nhớ chỉ đọc (read-only memory - ROM), bộ nhớ dựa trên đĩa, hoặc loại thiết bị lưu trữ khác, cũng như các phần hoặc các dạng kết hợp của các thiết bị này.

Các hệ mạch giao diện 210 và 220 của thiết bị người dùng tương ứng 202 và phần tử/chức năng mạng 204 bao gồm theo cách minh họa các bộ thu phát hoặc phần cứng hoặc phần sụn giao tiếp khác mà cho phép các phần tử hệ thống kết hợp để giao tiếp với nhau theo cách được mô tả ở đây.

Thấy rõ từ Fig.2 là thiết bị người dùng 202 được cấu hình để giao tiếp với phần tử/chức năng mạng 204 và ngược lại qua các hệ mạch giao diện tương ứng của chúng 210 và 220. Trong trường hợp mà phần tử/chức năng mạng 204 là UDM, thiết bị người dùng và UDM được ghép hoạt động qua và giao tiếp qua gNB 104 và AMF 106 (như được thể hiện trên Fig.1). Sự giao tiếp này bao gồm thiết bị người dùng 202 gửi dữ liệu đến phần tử/chức năng mạng 204, và phần tử/chức năng mạng 204 gửi dữ liệu đến thiết

bị người dùng 202. Tuy nhiên, theo các phương án thay thế, nhiều hơn hoặc ít hơn các phần tử mạng (ngoài hoặc thay thế cho, gNB và AMF) có thể được ghép hoạt động giữa các phần tử/chức năng mạng 202 và 204. Thuật ngữ “dữ liệu” như được sử dụng ở đây được nhằm hiểu theo nghĩa rộng, để bao hàm loại thông tin bất kỳ mà có thể được gửi giữa thiết bị người dùng và một hoặc nhiều phần tử/chức năng mạng bao gồm, nhưng không giới hạn ở, các bản tin, mã định danh, khóa, chỉ báo, dữ liệu người dùng, dữ liệu điều khiển, v.v.

Cần hiểu là sự bố trí cụ thể của các thành phần được thể hiện trên Fig.2 chỉ làm ví dụ, và nhiều cấu hình thay thế có thể được sử dụng theo các phương án khác. Ví dụ, phần tử/chức năng mạng cụ thể bất kỳ có thể được cấu hình để kết hợp các thành phần bổ sung hoặc thay thế và để hỗ trợ các giao thức truyền thông khác.

Các phần tử hệ thống khác (như, nhưng không giới hạn ở, các phần tử khác được thể hiện trên Fig.1) có thể mỗi phần tử cũng được cấu hình để bao gồm các thành phần như bộ xử lý, bộ nhớ và giao diện mạng. Các phần tử này không cần được thực hiện trên các nền tảng xử lý độc lập riêng biệt, mà có thể thay vào đó, ví dụ, thể hiện các phần chức năng khác nhau của nền tảng xử lý chung duy nhất.

Các khái niệm chung đã đưa ra được mô tả ở trên, các phương án minh họa mà giải quyết các vấn đề quản lý mã định danh thuê bao bây giờ sẽ được mô tả.

Như được đề cập ở trên, trong hệ thống truyền thông (LTE) 4G kế thừa, mã định danh thuê bao thường trực thường là mã định danh trạm di động quốc tế hoặc IMSI của UE. Như được định nghĩa trong tài liệu 3GPP TS 23.003 được viện dẫn ở trên, IMSI gồm có mã di động quốc gia (Mobile Country Code - MCC), mã mạng di động (Mobile Network Code - MNC), và số nhận dạng trạm di động (Mobile Station Identification Number - MSIN). Thông thường, nếu mã định danh thuê bao cần được bảo vệ, chỉ phần MSIN của IMSI cần được mã hóa. Các phần MNC và MCC cung cấp thông tin định tuyến, được sử dụng bởi mạng dịch vụ để định tuyến đến mạng thường trú đúng. Trong hệ thống truyền thông 5G, mã định danh thuê bao thường trực được gọi là mã định danh thường trực của thuê bao hoặc SUPI. Đối với IMSI, SUPI có thể sử dụng MSIN để xác định duy nhất thuê bao. Khi MSIN của SUPI được mã hóa, nó được gọi là mã định danh thuê bao ẩn hoặc SUCI.

Tuy nhiên, được nhận ra ở đây là, trong các kịch bản hoạt động khác nhau, UE có thể cần biểu diễn mã định danh thuê bao như SUCI, SUPI hoặc IMSI. Để giải quyết các vấn đề quản lý mã định danh thuê bao này và các vấn đề khác, các phương án minh họa đề xuất cấu trúc biểu diễn thống nhất cho mã định danh thuê bao.

Cụ thể hơn, các phương án minh họa giải quyết thách thức của việc sử dụng sự biểu diễn mã định danh thuê bao phù hợp, tức là, SUPI hoặc dạng mã hóa của nó SUCI hoặc thậm chí IMSI, trong bản tin yêu cầu đăng ký được gửi bởi UE đến mạng và thủ tục xác thực UE trong mạng 5G (lưu ý là cấu trúc dữ liệu thống nhất giống nhau hoặc tương tự có thể được trao đổi giữa các thực thể mạng). Ví dụ, UE trong khi thực hiện thủ tục thỏa thuận khóa và xác thực 5G (Authentication and Key Agreement - AKA) (xem ví dụ, tài liệu 3GPP TS 33.501 được viện dẫn ở trên) có thể cần để biểu diễn mã định danh thuê bao theo ba định dạng khác nhau SUCI, SUPI hoặc IMSI. Nếu thủ tục xác thực đang sử dụng thủ tục giao thức xác thực mở rộng (Extensible Authentication Protocol - EAP) AKA' (xem ví dụ, tài liệu 3GPP TS 33.501 được viện dẫn ở trên), khi đó sự biểu diễn sử dụng định dạng mã định danh truy cập mạng (Network Access Identifier - NAI), tức là, “joe@example.com” như được định nghĩa trong đề nghị duyệt thảo và bình luận (Request for Comment - RFC) 7542 mà được phê chuẩn bởi lực lượng chuyên trách kỹ thuật internet (Internet Engineering Task Force - IETF), “mã định danh truy cập mạng” tháng 5 năm 2015, phần nội dung của nó được kết hợp trong toàn bộ tài liệu này bằng cách viện dẫn.

Thách thức của các định dạng mã định danh thuê bao khác nhau không được giải quyết trong tài liệu TS 33.501 được viện dẫn ở trên, cũng như không có ở các bản mô tả kỹ thuật giai đoạn 3 bất kỳ khác. Trong chỉ dẫn kỹ thuật (TS) 3GPP 33.401, V15.3.0, có tựa đề “các dịch vụ nhóm và các khía cạnh hệ thống của chỉ dẫn kỹ thuật; sự tiến hóa kiến trúc hệ thống 3GPP (System Architecture Evolution - SAE); kiến trúc hệ thống”, phần nội dung của nó được kết hợp trong toàn bộ tài liệu này bằng cách viện dẫn, định nghĩa chỉ duy nhất việc sử dụng IMSI.

Fig.3A minh họa định dạng IMSI 300 mà với định dạng này một hoặc nhiều phương án minh họa có thể được thực hiện. Như được thể hiện, định dạng 300 bao gồm độ dài 15 chữ số cố định và gồm có mã di động quốc gia (Mobile Country Code - MCC) 3 chữ số, mã mạng di động (Mobile Network Code - MNC) 3 chữ số, và số nhận dạng trạm di động (Mobile Station Identification Number - MSIN) 9 chữ số. Trong một số trường hợp, MNC có thể là 2 chữ số, trong khi MSIN là 10 chữ số. Các chi tiết khác về IMSI được định nghĩa trong tài liệu 3GPP TS 23.003 được viện dẫn ở trên.

Như được giải thích ở trên, nếu thủ tục xác thực đang sử dụng thủ tục EAP-AKA' hoặc thủ tục bảo mật tầng giao vận (Transport Layer Security - TLS) EAP (mỗi thủ tục được định nghĩa trong tài liệu 3GPP TS 33.501 được viện dẫn ở trên), khi đó sự biểu diễn mã định danh thuê bao sử dụng định dạng NAI. RFC 7542 quy định là, đối với 3GPP, phần “tên người dùng” là mã định danh duy nhất mà được suy ra từ thông tin

thiết bị cụ thể và phần “cảnh giới” gồm có thông tin về mạng thường trú theo sau bởi chuỗi cơ sở “3gppnetwork.org”. Ví dụ, mã định danh thuê bao trong định dạng NAI có thể được biểu diễn như sau:

234150999999999@ims.mnc015.mcc234.3gppnetwork.org

Do đó, đối với thủ tục EAP-AKA', UE sẽ mã hóa mã định danh thuê bao SUPI hoặc SUCI của nó theo định dạng NAI như được quy định trong RFC 7542, ví dụ MSIN@mnc.mcc.3gppnetwork.org.

Các hình vẽ Fig.3B và Fig.3C lần lượt minh họa định dạng SUPI 310 và định dạng SUCI 320 mà với các định dạng này một hoặc nhiều phương án minh họa có thể được thực hiện. Trong ví dụ này, định dạng SUPI 310 bao gồm trường MCC (3 chữ số), và trường MNC (3 chữ số), bộ chọn MSIN và UDM (8 bit). Định dạng SUCI 320 là dạng được mã hóa của định dạng SUPI 310 và, như được thể hiện, bao gồm trường MCC (3 chữ số), và trường MNC (3 chữ số), trường bộ chọn UDM, MSIN được mã hóa, và các tham số để giải mã MSIN được mã hóa.

Đã được thỏa thuận trong 3GPP SA3 để hỗ trợ ít nhất hai đường cong elip, sơ đồ mã hóa tích hợp đường cong elip (Elliptic Curve Integrated Encryption Scheme - ECIES) đường cong A và đường cong B để mã hóa phần MSIN của SUPI trong khi mã định danh được mã hóa được sử dụng làm SUCI. Trong các bản phát hành tương lai, 3GPP có thể quy định nhiều hơn hoặc ít hơn các đường cong từ họ mật mã đường cong elip (Elliptic Curve Cryptography - ECC) của các đường cong hoặc có thể cho phép việc sử dụng các đường cong độc quyền cần được sử dụng để mã hóa MSIN. Tuy nhiên, đã nhận ra rằng trong khi ưu tiên sử dụng các sơ đồ tiêu chuẩn hóa, nhà điều hành mạng cũng có thể quyết định sử dụng phương pháp mã hóa cụ thể của riêng mình. Hơn nữa, đặc biệt là trong pha chuyển đổi, nhà điều hành mạng có thể cấu hình các thiết bị để chỉ sử dụng sơ đồ rộng cho SUCI. Sơ đồ rộng được thực hiện sao cho nó trả về cùng một đầu ra như đầu vào, mà áp dụng cho cả sự mã hóa và giải mã (tức là, MSIN không được mã hóa). Sơ đồ rộng được biểu thị bằng mã định danh sơ đồ trong SUCI và do đó, có thể được trình bày bằng định dạng mã định danh thuê bao thống nhất theo cách bình đẳng.

Vì mã định danh thuê bao ẩn SUCI được trao đổi giữa UE (102 trên Fig.1) và UDM (một phần của 108 trên Fig.1) trong mạng lõi, UDM nên được cấu hình để có thể hiểu cách UE đã mã hóa MSIN. Do đó, phương pháp mã hóa nên là một phần của định dạng được trao đổi cùng với chính đầu ra được mã hóa, vì không có các trao đổi bản tin khác giữa UE và UDM trong quá trình xác thực. Do đó, người ta nhận ra rằng sơ đồ để

biểu diễn SUCI nên hỗ trợ sự biểu diễn linh hoạt để phù hợp với nhiều trường, mỗi trường đủ linh hoạt để hỗ trợ nhiều lựa chọn.

Các phương án minh họa giải quyết các thách thức trên và các thách thức khác bằng cách cung cấp cấu trúc thống nhất để biểu diễn mã định danh thuê bao. Ví dụ, cấu trúc thống nhất theo một phương án minh họa có thể biểu diễn các mã định danh thuê bao như SUCI, SUPI và IMSI, cũng như các tùy chọn khác nhau liên quan đến việc sử dụng mỗi mã định danh trong quá trình xác thực và các hoạt động khác.

Fig.4 minh họa định dạng mã định danh thuê bao thống nhất (cấu trúc dữ liệu) 400, theo phương án minh họa. Hơn nữa, Fig.5 minh họa các độ dài trường 500 làm ví dụ cho mỗi trường được thể hiện trong định dạng mã định danh thuê bao thống nhất 400 của Fig.4.

Như được thể hiện, định dạng mã định danh thuê bao thống nhất 400 bao gồm các trường dưới đây (với các độ dài trường làm ví dụ trong các dấu ngoặc đơn):

Trường MCC 402 (24 bit/3 chữ số);

Trường MNC 404 (24 bit/3 chữ số);

Trường tham số lựa chọn UDM 406 (8 bit);

Trường tắt/bật mã hóa 408 (1 bit);

Trường KDF (Key Derivation Function, nghĩa là hàm sinh khóa) 410 (3 bit);

Trường tham số tùy chọn KDF 412 (n bit/tùy thuộc vào tham số tùy chọn);

Trường SUPI/SUCI/IMSI loại mã định danh 414 (2 bit);

Đường cong ECIES được lựa chọn cho trường mã hóa 416 (4 bit);

Trường cặp khóa công khai tạm thời 418 (256 bit);

Độ dài của trường MSIN được mã hóa 420 (4 bit/128, 192, 256, 512 bit/tùy thuộc vào định dạng MSIN);

Trường MSIN hoặc MSIN được mã hóa 422 (độ dài như được quy định trong trường 420);

Trường MSIN MAC (mã xác thực bản tin của trường MSIN được tính bằng cách sử dụng các đường cong ECIES được chọn) 424 (256 bit); và

Trường mã định danh thuật toán mã hóa 426 (4 bit).

Cần hiểu là các độ dài trường được mô tả ở đây mang tính chất minh họa và do đó không có ý định giới hạn. Tùy thuộc vào các kịch bản hoạt động trong đó UE và chức

năng mạng 5G, các độ dài trường có thể được thiết đặt đến các trị số khác nhau. Cũng cần hiểu là, theo các phương án thay thế, một hoặc nhiều trường khác có thể được bổ sung vào cấu trúc dữ liệu và/hoặc một số các trường ở trên có thể được xóa đi và/hoặc đơn giản là không được sử dụng. Đồng thời, vị trí trường trong định dạng cấu trúc 400 trên Fig.4 mang tính chất ví dụ và do đó, các sự bố trí trường thay thế được dự tính theo các phương án khác. Bằng cách lấy ví dụ, một trường bổ sung mà có thể là một phần của cấu trúc dữ liệu (hoặc được chỉ ra trong sự lựa chọn UDM hoặc trường khác) là trường thông tin hỗ trợ lựa chọn ngăn mạng (Network Slice Selection Assistance Information - NSSAI).

Trong khi một số phương án minh họa đề xuất UE gửi cấu trúc dữ liệu mã định danh thuê bao thống nhất đầy đủ (ví dụ, 400 trên Fig.4) đến UDM cụ thể (hoặc một hoặc nhiều thực thể mạng khác), các phương án minh họa thay thế tránh việc vận chuyển nhiều tham số chỉ định chẳng hạn như, ví dụ, KDF, các tham số tùy chọn KDF, đường cong elip đã chọn, mã định danh thuật toán mã hóa, v.v. để giảm thiểu chi phí truyền dẫn. Do đó, cấu trúc dữ liệu mã định danh thuê bao thống nhất minh họa thay thế 600 được mô tả trên Fig.6. Như được thể hiện, định dạng mã định danh thuê bao thống nhất 600 bao gồm các trường dưới đây (với các độ dài trường làm ví dụ trong các dấu ngoặc đơn):

Trường MCC 602 (24 bit/3 chữ số);

Trường MNC 604 (24 bit/3 chữ số);

Trường tham số lựa chọn UDM 606 (8 bit);

Trường SUPI/SUCI/IMSI loại mã định danh 608 (2 bit);

Độ dài của trường MSIN được mã hóa 610 (4 bit/128, 192, 256, 512 bit/tùy thuộc vào định dạng MSIN);

Trường MSIN hoặc MSIN được mã hóa 612 (độ dài như được quy định trong trường 610);

Trường MSIN MAC (mã xác thực bản tin của trường MSIN được tính bằng cách sử dụng các đường cong ECIES được chọn) 614 (256 bit); và

Trường lựa chọn hồ sơ 616 (4 bit).

Cần hiểu là các độ dài trường được mô tả ở đây mang tính chất minh họa và do đó không có ý định giới hạn. Tùy thuộc vào các kịch bản hoạt động trong đó UE và chức năng mạng 5G, các độ dài trường có thể được thiết đặt đến các trị số khác nhau. Cũng cần hiểu là, theo các phương án thay thế, một hoặc nhiều trường khác có thể được bổ

sung vào cấu trúc dữ liệu và/hoặc một số các trường ở trên có thể được xóa đi và/hoặc đơn giản là không được sử dụng. Đồng thời, vị trí trường trong định dạng cấu trúc 600 trên Fig.6 mang tính chất ví dụ và, do đó, các sự bố trí trường thay thế được dự tính theo các phương án khác. Bằng cách lấy ví dụ, một trường bổ sung mà có thể là một phần của cấu trúc dữ liệu (hoặc được chỉ ra trong sự lựa chọn UDM hoặc trường khác) là trường thông tin hỗ trợ lựa chọn ngăn mạng (Network Slice Selection Assistance Information - NSSAI).

Các trường 602 đến 614 cung cấp cùng thông tin như các bản sao được đặt tên giống nhau trong cấu trúc dữ liệu 400. Tuy nhiên, cấu trúc dữ liệu 600 bao gồm trường lựa chọn hồ sơ 616. Nhận thấy rằng có thể có lợi nếu thiết lập trước một số hồ sơ tiêu chuẩn để được sử dụng trong định dạng biểu diễn mã định danh thuê bao thống nhất giữa UE và UDM. Các hồ sơ được thỏa thuận này có thể được xác định làm các trị số được thiết đặt trước (bằng cách lấy ví dụ, đường cong ECIES 4 bit được lựa chọn cho trường mã hóa). Trong trường hợp như vậy, các trị số đã thỏa thuận từ các hồ sơ sẽ được sử dụng bởi người gửi UE và UDM mà tránh việc trao đổi thực tế của các trị số cho các tham số này.

Ví dụ, trong phiên bản các trường rút gọn dựa trên hồ sơ như vậy của cấu trúc dữ liệu mã định danh thuê bao thống nhất, UDM sẽ được cấu hình để biết là trường lựa chọn hồ sơ đã cho của “0011” (nếu 4 bit) tương ứng với một số cài đặt được xác định trước cho các trường từ định dạng trên Fig.4 mà không được gửi trong phiên bản trường rút gọn của Fig.6, trong khi trường lựa chọn hồ sơ của “1010” có nghĩa là các cài đặt được xác định trước khác nhau, v.v. Do đó, UDM có thể lưu trữ trước (hoặc thu được trong thời gian thực) cấu trúc dữ liệu cho mỗi hồ sơ có thể mà UE có thể gửi (do các UE được cấu hình để chọn các kịch bản xác thực khác nhau).

Các phương án minh họa đề xuất cho tất cả các UE (ví dụ, 102 trên Fig.1) và các phần tử/chức năng mạng như, nhưng không giới hạn ở, gNB (104 trên Fig.1), AMF (một phần của 106 trên Fig.1), SEAF (một phần của 106 trên Fig.1), AUSF (một phần của 108 trên Fig.1) và UDM (một phần của 108 trên Fig.1), để hỗ trợ các định dạng mã định danh thuê bao thống nhất 400 và 600, cũng như các biến thể thay thế.

Fig.7 minh họa phương pháp luận 700 để sử dụng định dạng mã định danh thuê bao thống nhất (ví dụ, cấu trúc dữ liệu 400 của Fig.4 hoặc cấu trúc dữ liệu 600 của Fig.6) từ quan điểm của UE, theo phương án minh họa.

Trong bước 702, UE duy trì mã định danh thuê bao thường trực (permanent subscription identifier - SUPI) hoặc IMSI.

Trong bước 704, UE duy trì khóa công khai của UDM cũng như cặp khóa công khai/riêng tư của chính nó.

Trong bước 706, UE lựa chọn các tham số để mã hóa MSIN (thuật toán, các đường cong, v.v.).

Trong bước 708, UE xây dựng cấu trúc dữ liệu mã định danh thuê bao thống nhất (ví dụ, 400 trên Fig.4) sử dụng loại mã định danh, thuật toán mã hóa, chỉ báo đường cong, khóa công khai, MSIN được mã hóa, MSIN MAC, MCC, MNC, bộ lựa chọn UDM, KDF, các tham số KDF tùy chọn, v.v.

Trong bước 710, UE gửi cấu trúc dữ liệu mã định danh thuê bao thống nhất đến UDM được chọn trong khi yêu cầu truy cập mạng (ví dụ, yêu cầu đăng ký). Theo một phương án, cấu trúc dữ liệu mã định danh thuê bao thống nhất có thể là cấu trúc dữ liệu 400 của Fig.4 (ví dụ, phiên bản được điền tất cả các trường), trong khi theo phương án thay thế, cấu trúc dữ liệu mã định danh thuê bao thống nhất có thể là cấu trúc dữ liệu 600 của Fig.6 (phiên bản các trường rút gọn dựa trên hồ sơ). Các biến thể khác của cấu trúc dữ liệu mã định danh thuê bao thống nhất có thể được gửi theo các phương án thay thế khác. Các thực thể mạng (ví dụ, UDM) cũng được cấu hình để xây dựng hoặc ngoài ra thu được/duy trì các cấu trúc dữ liệu mã định danh thuê bao thống nhất như vậy.

Fig.8 minh họa phương pháp luận 800 để sử dụng định dạng mã định danh thuê bao thống nhất (ví dụ, cấu trúc dữ liệu 400 của Fig.4 hoặc cấu trúc dữ liệu 600 của Fig.6) từ quan điểm của thực thể mạng (ví dụ, một hoặc nhiều trong số các phân tử/chức năng mạng được mô tả ở đây), theo phương án minh họa.

Trong bước 802, thực thể mạng nhận cấu trúc dữ liệu mã định danh thuê bao thống nhất.

Trong bước 804, thực thể mạng giải mã cấu trúc dữ liệu mã định danh thuê bao thống nhất khi cần.

Trong bước 806, phân tử mạng thực hiện sự xác thực của người gửi UE dựa trên kịch bản xác thực tương ứng với loại mã định danh thuê bao đã chọn trong cấu trúc dữ liệu đã nhận.

Do đó, cần nhấn mạnh lại rằng các phương án khác nhau được mô tả ở đây được trình bày chỉ qua ví dụ minh họa và không nên được hiểu là làm giới hạn phạm vi của các yêu cầu bảo hộ. Ví dụ, các phương án thay thế có thể sử dụng các cấu hình hệ thống truyền thông khác nhau, cấu hình thiết bị người dùng, cấu hình trạm gốc, quy trình sử dụng và cung cấp cặp khóa, giao thức nhắn tin và định dạng bản tin ngoài các cấu hình

được mô tả ở trên trong ngữ cảnh của các phương án minh họa. Những phương án này và nhiều phương án thay thế khác nằm trong phạm vi của các yêu cầu bảo hộ kèm theo là rõ ràng đối với những người có trình độ trong lĩnh vực kỹ thuật tương ứng.

YÊU CẦU BẢO HỘ

1. Thiết bị người dùng (102) cho hệ thống truyền thông không dây (100) bao gồm bộ xử lý (212) và bộ nhớ (216) được cấu hình để thực hiện các bước:

xây dựng, ở thiết bị người dùng (102, 202) trong hệ thống truyền thông không dây (100, 200), cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600),

trong đó cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) bao gồm nhiều trường (402, 404, 406, 422, 424) mà xác định thông tin cho một loại và tham số được chọn trong số hai hoặc nhiều loại mã định danh thuê bao và tham số (408, 410, 412, 416, 418, 420, 426, 610) được kết hợp với loại mã định danh thuê bao đã chọn, và

sử dụng cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) để truy cập một hoặc nhiều mạng được kết hợp với hệ thống truyền thông không dây (100) dựa trên kịch bản xác thực tương ứng với loại mã định danh thuê bao đã chọn;

trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường loại mã định danh thuê bao (414, 608) mà xác định một loại được chọn trong số hai hoặc nhiều loại mã định danh thuê bao; và

trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường tham số lựa chọn quản lý dữ liệu thống nhất (unified data management - UDM) (406, 606), trong đó thực thể mạng là để thực hiện một hoặc nhiều trong số chức năng UDM và chức năng máy chủ xác thực (authentication server function - AUSF).

2. Thiết bị người dùng (102) theo điểm 1, trong đó loại mã định danh thuê bao có thể chọn từ nhóm bao gồm mã định danh thuê bao ẩn (Concealed Subscription Identifier - SUCI), mã định danh thường trực của thuê bao (Subscriber Permanent Identifier - SUPI) và mã định danh trạm di động quốc tế (International Mobile Station Identifier - IMSI).

3. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường bật/tắt mã hoá (408).

4. Thiết bị người dùng (102) theo điểm 3, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường mã định danh thuật toán mã hoá (426).

5. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường hàm sinh khoá (410).

6. Thiết bị người dùng (102) theo điểm 5, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường tham số hàm sinh khoá (412).

7. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường mã di động quốc gia (402).
8. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường mã mạng di động (404).
9. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường xác định đường cong được chọn từ sơ đồ mã hoá tích hợp đường cong elip (416).
10. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường cặp khoá công khai tạm thời (418).
11. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường xác định độ dài của trường số nhận dạng trạm di động (Mobile Station Identification Number - MSIN) được mã hoá (420).
12. Thiết bị người dùng (102) theo điểm 11, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường MSIN được mã hoá (422).
13. Thiết bị người dùng (102) theo điểm 11, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường mã xác thực bản tin MSIN (424).
14. Thiết bị người dùng (102) theo điểm 1, trong đó hệ thống truyền thông không dây (100) bao gồm hệ thống 5G.
15. Thiết bị người dùng (102) theo điểm 1, thiết bị người dùng (102) còn được cấu hình để gửi cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) đến ít nhất một thực thể mạng trong hệ thống truyền thông không dây (100) để có khả năng truy cập vào một hoặc nhiều mạng được kết hợp với hệ thống truyền thông không dây (100).
16. Thiết bị người dùng (102) theo điểm 1, trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường lựa chọn hồ sơ.
17. Thiết bị người dùng (102) theo điểm 16, trong đó trường lựa chọn hồ sơ cho phép thiết bị người dùng (102) thông báo cho một hoặc nhiều thực thể mạng trong một hoặc nhiều mạng được kết hợp với hệ thống truyền thông không dây (100) để sử dụng các trị số được thiết lập trước cho một hoặc nhiều tham số có thể chọn (408, 410, 412, 416, 418, 420, 426, 610) được kết hợp với loại mã định danh thuê bao đã chọn.
18. Thiết bị người dùng (102) theo điểm 17, trong đó thiết bị này còn được cấu hình để gửi cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) với trường lựa chọn hồ sơ và bộ rút gọn của các trường đến ít nhất một trong số một hoặc nhiều thực thể

mạng trong hệ thống truyền thông không dây (100) để có khả năng truy cập vào một hoặc nhiều mạng được kết hợp với hệ thống truyền thông không dây (100).

19. Phương pháp để quản lý mã định danh thuê bao thống nhất, phương pháp này bao gồm các bước:

xây dựng, ở thiết bị người dùng (102) trong hệ thống truyền thông không dây (100), cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600);

trong đó cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) bao gồm nhiều trường (402, 404, 406, 422, 424) mà xác định thông tin cho một loại và tham số được chọn trong số hai hoặc nhiều loại mã định danh thuê bao và tham số có thể chọn (408, 410, 412, 416, 418, 420, 426, 610) được kết hợp với loại mã định danh thuê bao đã chọn, và

sử dụng cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) để truy cập một hoặc nhiều mạng được kết hợp với hệ thống truyền thông không dây (100) dựa trên kịch bản xác thực tương ứng với loại mã định danh thuê bao đã chọn;

trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường loại mã định danh thuê bao (414, 608) mà xác định một loại được chọn trong số hai hoặc nhiều loại mã định danh thuê bao; và

trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường tham số lựa chọn quản lý dữ liệu thống nhất (UDM) (406, 606), trong đó thực thể mạng là để thực hiện một hoặc nhiều trong số chức năng UDM và chức năng máy chủ xác thực (AUSF).

20. Phương tiện lưu trữ có thể đọc được bằng máy tính không tạm thời có chứa trong đó mã chương trình có thể thực thi mà khi được thực thi bởi bộ xử lý của thiết bị người dùng (102) cho hệ thống truyền thông không dây (100), làm cho bộ xử lý thực hiện:

xây dựng cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600);

trong đó cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) bao gồm nhiều trường (402, 404, 406, 422, 424) mà xác định thông tin cho một loại và tham số được chọn trong số hai hoặc nhiều loại mã định danh thuê bao và tham số có thể chọn (408, 410, 412, 416, 418, 420, 426, 610) được kết hợp với loại mã định danh thuê bao đã chọn, và

sử dụng cấu trúc dữ liệu mã định danh thuê bao thống nhất (400, 600) để truy cập một hoặc nhiều mạng được kết hợp với hệ thống truyền thông không dây (100) dựa trên kịch bản xác thực tương ứng với loại mã định danh thuê bao đã chọn;

trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường loại mã định danh thuê bao (414, 608) mà xác định một loại được chọn trong số hai hoặc nhiều loại mã định danh thuê bao; và

trong đó nhiều trường (402, 404, 406, 422, 424) bao gồm trường tham số lựa chọn quản lý dữ liệu thống nhất (UDM) (406, 606), trong đó thực thể mạng là để thực hiện một hoặc nhiều trong số chức năng UDM và chức năng máy chủ xác thực (AUSF).

1/8

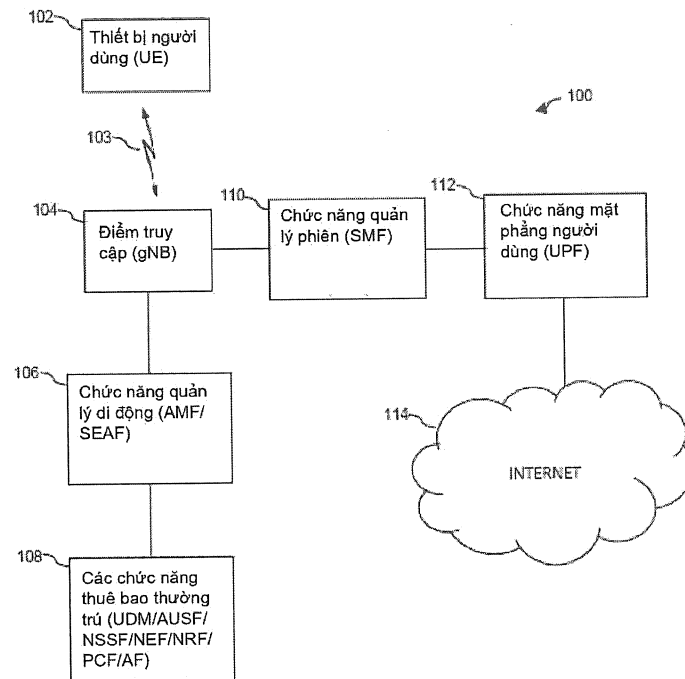


FIG. 1

2/8

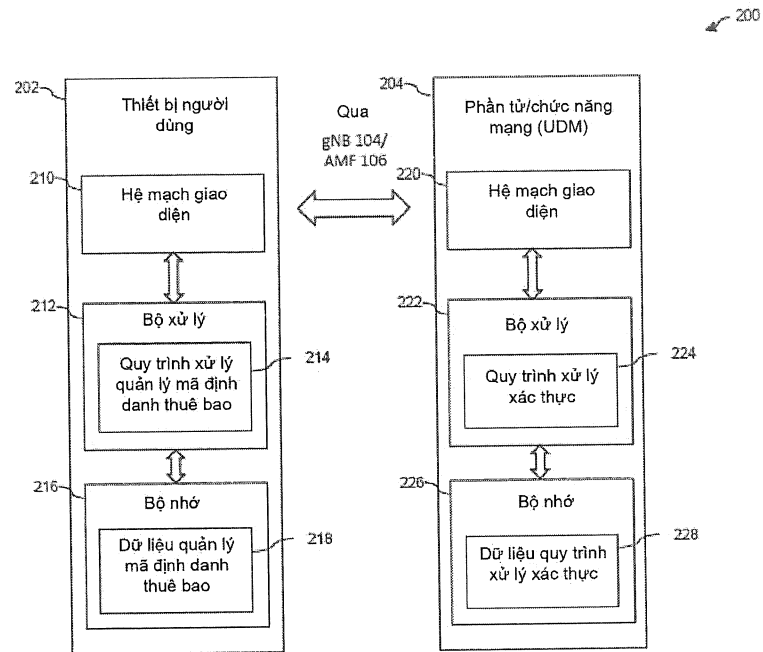


FIG. 2

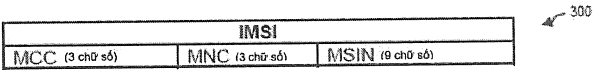


FIG. 3A

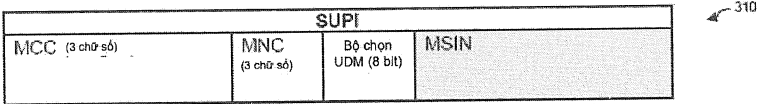


FIG. 3B

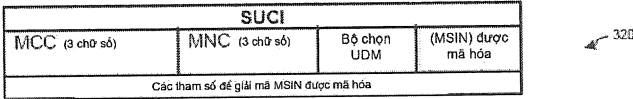


FIG. 3C

400

Mã định danh thuê bao (SUCI, SUPI, IMSI)		
MCC 402	MNC 404	Tham số lựa chọn UDM 406
Tắt/bật sự mã hóa 408	KDF 410	Các tham số tùy chọn KDF 412
Loại mã định danh SUPI/SUCI/IMSI 414	Đường cong ECIES được chọn cho sự mã hóa 416	Cặp khóa công khai tạm thời 418
Độ dài của MSIN được mã hóa 420	MSIN được mã hóa 422	MSIN MAC 424
Trường mã định danh thuật toán mã hóa 426		

FIG. 4

5/8

Trường	Độ dài (bit)
Loại mã định danh (SUPI, SUCI, IMSI) ⁴¹⁴	2 bit
Tắt/bật sự mã hóa ⁴⁰⁸	1 bit
Mã định danh thuật toán MÃ HÓA ⁴²⁶	4 bit
Đường cong ECIES được chọn cho sự mã hóa ⁴¹⁸	4 bit
Khóa công khai tạm thời của người gửi ⁴¹⁸	256 bit
Độ dài của MSIN được mã hóa ⁴²⁰	4 (128 bit , 192 bit , 256 bit , 512 bit)
MSIN được mã hóa ⁴²²	(Độ dài được quy định trong trường 420)
MSIN MAC (Sự xác thực bản tin của trường MSIN được tính bằng cách sử dụng các đường cong ECIES) ⁴²⁴	256bit
Tham số lựa chọn UDM ⁴⁰⁶	8 bit
MCC ⁴⁰²	24 bit (3 chữ số)
MNC ⁴⁰⁴	24 bit (3 chữ số)
KDF được sử dụng cho sự mã hóa ⁴¹⁰	3bit
Các tham số tùy chọn KDF ⁴¹²	n bit

500

FIG. 5

6/8

600

Mã định danh thuê bao (SUCI, SUPI, IMSI)		
MCC 602	MNC 604	Tham số lựa chọn UDM 606
Loại mã định danh SUPI/SUCI/IMSI 608	Độ dài của MSIN được mã hóa 610	MSIN được mã hóa 612
MSIN MAC 614	Sự lựa chọn hồ sơ 616	

FIG. 6

7/8

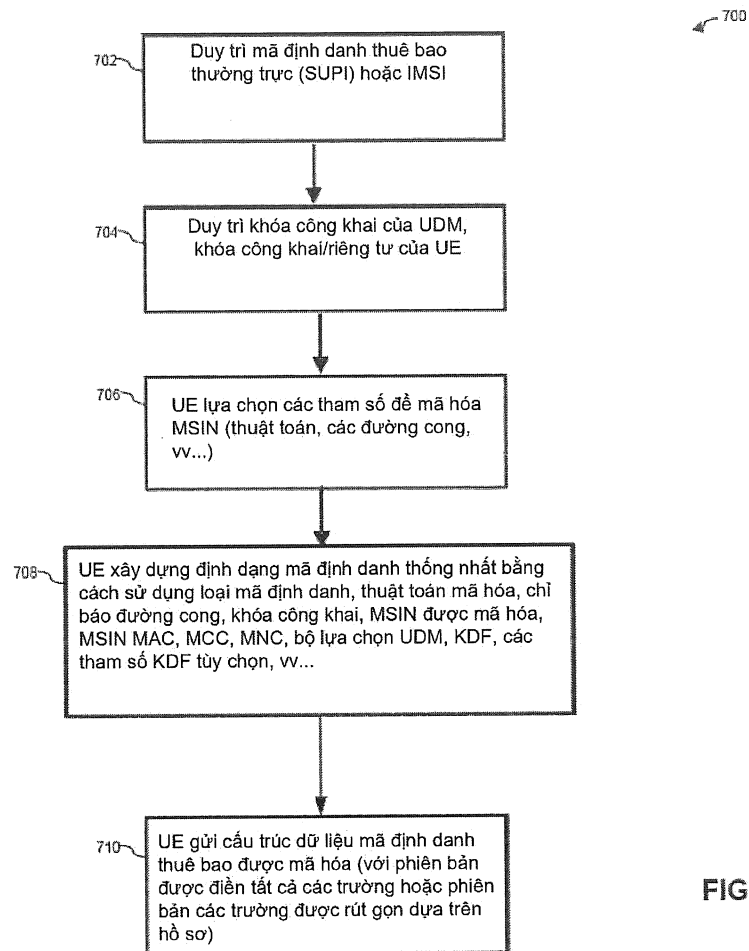


FIG. 7

8/8

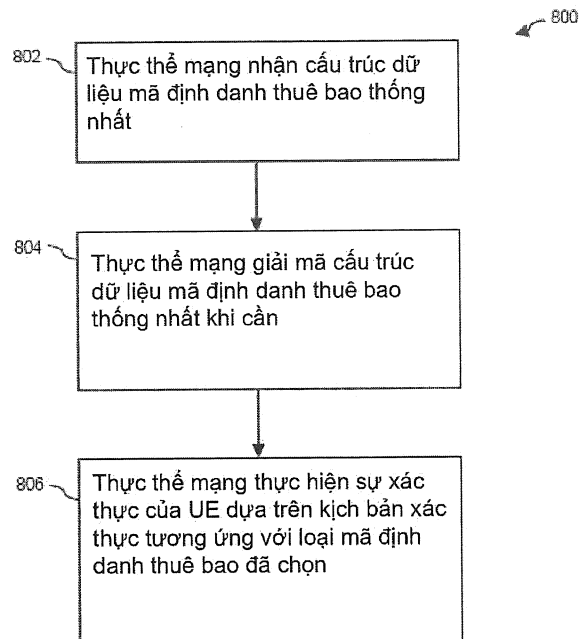


FIG. 8