(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) **1-0035720**

(51)[7] **H04L 63/10**

(13) **B**

(21) 1-2018-05134

(22) 16/11/2018

(30) 17202176.8 16/11/2017 EP

(45) 25/05/2023 422

(43) 27/05/2019 374A

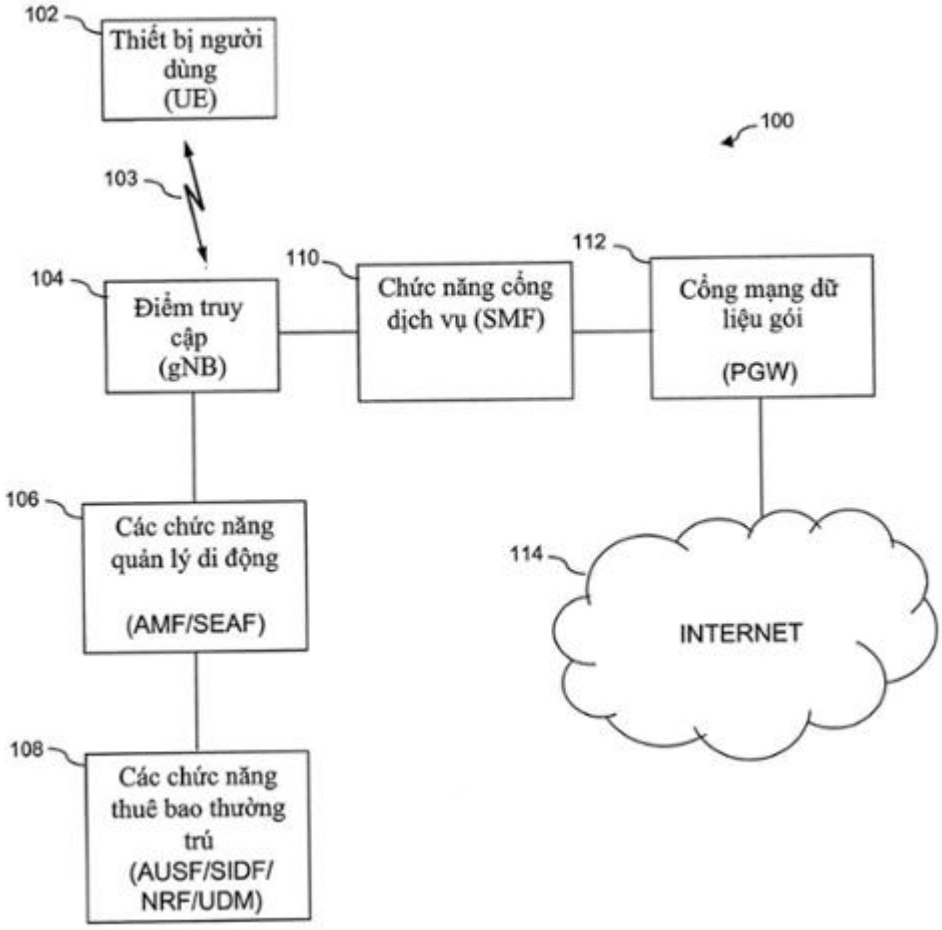
(73) Nokia Technologies Oy (FI)
Karaportti 3, Espoo 02610, Finland

(72) Anja Jerichow (DE).

(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP, THIẾT BỊ VÀ VẬT PHẨM ĐỂ TRUYỀN THÔNG

(57) Sáng chế đề cập đến phương pháp và thiết bị truyền thông. Một cách cụ thể, trong mạng gia đình của hệ thống truyền thông, trong đó một hoặc nhiều cặp khóa mật mã được cung cấp để sử dụng bởi các thuê bao của mạng gia đình để che giấu các thông tin nhận dạng thuê bao được cung cấp cho một hoặc nhiều điểm truy cập trong hệ thông truyền thông, phương pháp truyền thông bao gồm bước cung cấp một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật để sử dụng bởi các thuê bao khi cung cấp các thông tin nhận dạng thuê bao được che giấu của họ cho hệ thống truyền thông. Mỗi trong số một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật nhận dạng thực thể quản lý bảo mật đã biết trong hệ thống truyền thông được tạo cấu hình để trích xuất thông tin nhận dạng thuê bao đã biết.


102
Thiết bị người dùng (UE)
100
103
110
Chức năng cổng dịch vụ (SMF)
112
Cổng mạng dữ liệu gói (PGW)
104
Điểm truy cập (gNB)
106
Các chức năng quản lý di động (AMF/SEAF)
114
INTERNET
108
Các chức năng thuê bao thường trú (AUSF/SIDF/ NRF/UDM)

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập chung đến hệ thống truyền thông, và cụ thể hơn là đề cập đến, nhưng không phải là duy nhất, các kỹ thuật quản lý bảo mật thuê bao trong các hệ thống này.

Tình trạng kỹ thuật của sáng chế

Phần này giới thiệu các khía cạnh có thể hữu ích cho việc hỗ trợ hiểu sáng chế rõ hơn. Do đó, các phần trình bày trong phần này cần được đọc trên góc độ này và không được hiểu là sự thừa nhận về việc phần nào giải pháp kỹ thuật đã biết, phần nào không phải là giải pháp kỹ thuật đã biết.

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), đã 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 hay thế hệ thứ năm (5G) được dự định được sử dụng không chỉ cho sự tương tác của con người, mà còn cho việc truyền thông kiểu máy trong các mạng được gọi là Mạng Internet vạn vật (Internet of Things - IoT).

Mặc dù các mạng 5G được dự định cho phép các dịch vụ IoT quy mô lớn (ví dụ, số lượng rất lớn các thiết bị dung lượng có giới hạn) và các dịch vụ IoT then chốt (ví dụ, đòi hỏi độ tin cậy cao), các sự cải tiến so với các dịch vụ truyền thông di động kế thừa được hỗ trợ dưới dạng các dịch vụ băng rộng di động nâng cao (enhanced mobile broadband - eMBB) cung cấp sự truy cập Internet không dây cải tiến cho các thiết bị di động.

Trong hệ thống truyền thông làm ví dụ, thiết bị người dùng (5G UE trong mạng 5G hoặc, rộng hơn là UE) như thiết bị đầu cuối di động (thuê bao) truyền thông qua giao diện vô tuyến với trạm cơ sở hoặc điểm truy cập (access point) được gọi là gNB trong mạng 5G. Điểm truy cập (ví dụ, gNB) là 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 Tài liệu mô tả kỹ thuật 5G (TS) 23.501, V1.5.0, có tên "Technical Specification Group Services and System Aspects; System Architecture for the 5G System", tài liệu này được kết hợp bằng cách viện dẫn toàn bộ ở đây. Nói chung, điểm truy cập (ví dụ,

gNB) cung cấp sự truy cập cho UE vào mạng lõi (CN), mà sau đó cung cấp sự truy cập cho UE vào các UE khác và/hoặc mạng dữ liệu như mạng dữ liệu gói (ví dụ, Internet).

Bảo mật là sự đánh giá quan trọng trong hệ thống truyền thông bất kỳ. Bảo mật được giải quyết rộng rãi trong báo cáo kỹ thuật 5G (TR) 33.899, V1.1.0, có tên "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14)", tài liệu này được kết hợp bằng cách viện dẫn toàn bộ ở đây. Cụ thể là, TR 33.899 nhận dạng sự bảo mật thuê bao (UE) như là một trong số các vùng bảo mật quan trọng nhất cần được giải quyết trong các mạng 5G. Tài liệu mô tả kỹ thuật 5G (TS) 33.501, V0.3.0, có tên "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System (Release 15)", tài liệu này được kết hợp bằng cách viện dẫn toàn bộ ở đây, cung cấp phần mô tả bảo mật quy chuẩn.

Bản chất kỹ thuật của sáng chế

Các phương án minh họa đề xuất các kỹ thuật để cung cấp sự bảo mật thuê bao trong các hệ thống truyền thông.

Ví dụ, theo một phương án minh họa, phương pháp bao gồm bước sau đây. Trong mạng gia đình của hệ thống truyền thông, trong đó một hoặc nhiều cặp khóa mật mã được cung cấp để sử dụng bởi các thuê bao của mạng gia đình để che giấu các thông tin nhận dạng thuê bao được cung cấp cho một hoặc nhiều điểm truy cập trong hệ thống truyền thông, phương pháp này bao gồm bước cung cấp một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật để sử dụng bởi các thuê bao khi cung cấp các thông tin nhận dạng thuê bao được che giấu của họ cho hệ thống truyền thông. Mỗi trong số một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật nhận dạng thực thể quản lý bảo mật đã biết trong hệ thống truyền thông được tạo cấu hình để trích xuất thông tin nhận dạng thuê bao đã biết.

Theo các phương án minh họa khác, phương pháp này bao gồm bước chọn thực thể quản lý bảo mật từ các thực thể quản lý bảo mật trong hệ thống truyền thông dựa trên thông tin nhận dạng thực thể quản lý bảo mật đã biết được nhận từ thuê bao đã biết, và trích xuất thông tin nhận dạng thuê bao đã biết tại thực thể quản lý bảo mật được chọn. Theo một phương án minh họa, dữ liệu xác thực thuê bao được yêu cầu đồng thời với

bước chọn thực thể quản lý bảo mật. Theo một phương án minh họa khác, dữ liệu xác thực thuê bao được yêu cầu theo sau bước trích xuất.

Theo phương án hệ thống truyền thông 5G, ít nhất một trong số các thực thể quản lý bảo mật được thực thi trong hệ thống truyền thông như là chức năng trích xuất thông tin nhận dạng thuê bao (subscription identifier de-concealing function - SIDF). SIDF có thể được thực thi trong hệ thống truyền thông như là dịch vụ được đề nghị bởi chức năng quản lý dữ liệu người dùng (user data management - UDM). SIDF có thể được định vị cùng với chức năng UDM hoặc chức năng xác thực và bảo mật (authentication and security function - AUSF).

Theo một phương án minh họa khác nữa, trong thiết bị người dùng, phương pháp lưu trữ: (i) ít nhất một khóa công khai kết hợp với ít nhất một cặp khóa mật mã, cặp khóa mật mã được cung cấp bởi mạng gia đình của hệ thống truyền thông để sử dụng bởi thiết bị người dùng nhằm che giấu thông tin nhận dạng thuê bao sẽ được cung cấp cho một hoặc nhiều điểm truy cập trong mạng truyền thông; và (ii) ít nhất một thông tin nhận dạng thực thể quản lý bảo mật để sử dụng bởi thiết bị người dùng khi cung cấp thông tin nhận dạng thuê bao được che giấu cho hệ thống truyền thông, trong đó thông tin nhận dạng thực thể quản lý bảo mật nhận dạng thực thể quản lý bảo mật đã biết trong hệ thống truyền thông được tạo cấu hình để trích xuất thông tin nhận dạng thuê bao được che giấu.

Thuận lợi là, các phương án minh họa cho phép chọn SIDF thích hợp trong hệ thống truyền thông, đặc biệt khi nhà khai thác mạng gia đình (nhà khai thác mạng di động hoặc MNO) có một vài đối tượng UDM và/hoặc cũng có một hoặc nhiều nhà khai thác mạng di động ảo hoặc các MVNO được ký hợp đồng mà có thể lưu trữ các cặp khóa công khai/bảo mật của chính chúng nhằm mục đích che giấu thông tin nhận dạng thuê bao.

Các phương án khác được đề xuất dưới dạng vật ghi lâu dài đọc được bằng máy tính có chứa trong đó mã chương trình thực thi được mà khi được thực thi bởi bộ xử lý làm cho bộ xử lý thực hiện các bước trên đây. Các phương án khác nữa bao gồm thiết bị có bộ xử lý và bộ nhớ được tạo cấu hình để thực hiện các bước trên đây.

Các dấu hiệu và ưu điểm này và các dấu hiệu và ưu điểm 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 là sơ đồ khối của hệ thống truyền thông theo phương án minh họa.

Fig.2 là sơ đồ khối của các phần tử/các chức năng mạng để cung cấp sự quản lý bảo mật thuê bao theo phương án minh họa.

Fig.3 là lưu đồ của phương pháp quản lý bảo mật thuê bao theo phương án minh họa.

Fig.4 là sơ đồ khối của ít nhất một phần của hệ thống truyền thông thực hiện sự quản lý bảo mật thuê bao theo phương án minh họa.

Fig.5 là sơ đồ khối của ít nhất một phần của hệ thống truyền thông thực hiện sự quản lý bảo mật thuê bao theo một phương án minh họa khác.

Mô tả chi tiết sáng chế

Các phương án sẽ được minh họa ở đây kết hợp với các hệ thống truyền thông làm ví dụ và các kỹ thuật kết hợp để cung cấp sự quản lý bảo mật thuê bao trong các hệ thống truyền thông. Tuy nhiên, cần hiểu rằng phạm vi yêu cầu bảo hộ không bị giới hạn ở các loại hệ thống truyền thông cụ thể và/hoặc các quy trình được trích xuất. Các phương án có thể được thực hiện trong rất nhiều loại hệ thống truyền thông khác, sử dụng các quy trình hoặc các hoạt động khác. Ví dụ, mặc dù được minh họa trong ngữ cảnh của các hệ thống tế bào 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 thích ứng theo cách đơn giản cho nhiều loại hệ thống truyền thông khác bao gồm, nhưng không bị giới hạn ở, các hệ thống WiMAX và các hệ thống Wi-Fi, cũng như các hệ thống 3GPP có trước hệ thống 5G (LTE, v.v.).

Theo các phương án minh họa được thực thi trong môi trường hệ thống truyền thông 5G, một hoặc nhiều tài liệu mô tả kỹ thuật (TS) và báo cáo kỹ thuật (TR) 3GPP sau đây có thể cung cấp các sự giải thích thêm về các phần tử/các chức năng mạng và/hoặc các hoạt động mà có thể tương tác với các phần của các giải pháp sáng tạo: 3GPP TS 23.501, 3GPP TS 23.502, 3GPP TS 33.501, và 3GPP TR 33.899, các phần bộc lộ của chúng được kết hợp bằng cách viện dẫn toàn bộ ở đây. Các tài liệu 3GPP TS/TR khác có thể cung cấp các thông tin chi tiết thông thường khác mà người có hiểu biết trung bình trong lĩnh vực kỹ thuật liên quan sẽ thực hiện. Tuy nhiên, mặc dù hoàn toàn thích hợp

cho các tiêu chuẩn 3GPP liên quan đến 5G, các phương án không nhất thiết được dự định là bị giới hạn ở các tiêu chuẩn cụ thể bất kỳ.

Như được nêu trên đây, sự bảo mật của các thông tin nhận dạng thuê bao khi được truyền thông qua giao diện vô tuyến giữa thiết bị người dùng và điểm truy cập mạng là vấn đề đáng chú ý đối với các hệ thống truyền thông. Đã có nhiều sự nỗ lực được thực hiện trong các mạng 5G để giải quyết vấn đề đáng chú ý này.

Ví dụ, đã biết rằng các đối tượng ác ý cố gắng lấy các thông tin nhận dạng thuê bao nhờ nghe trộm thụ động (công cụ thu gom thụ động – passive catcher) qua giao diện vô tuyến giữa UE và gNB hoặc yêu cầu chủ động (công cụ thu gom chủ động - active catcher) yêu cầu thông tin nhận dạng thuê bao.

Các giải pháp để cung cấp sự bảo mật qua giao diện vô tuyến có thể được nhóm chung thành ba lớp giải pháp: (1) các giải pháp biệt hiệu dựa trên các hệ thống mật mã đối xứng, mà đòi hỏi máy chủ/chức năng thuê bao thường trú của mạng gia đình của UE ánh xạ biệt hiệu thay đổi đến thông tin nhận dạng thuê bao vĩnh viễn của UE; (2) sự mã hóa thông tin nhận dạng thuê bao vĩnh viễn của UE sử dụng khóa công khai của nhà khai thác mạng gia đình; và (3) sự mã hóa thông tin nhận dạng thuê bao vĩnh viễn của UE sử dụng khóa công khai của nhà khai thác mạng phục vụ.

Mặc dù các phương án có thể được làm thích ứng đối với giải pháp bất kỳ trong số các giải pháp nêu trên, các phương án minh họa đề xuất các kỹ thuật quản lý bảo mật thuê bao theo quan điểm của giải pháp 2 (sự mã hóa thông tin nhận dạng thuê bao vĩnh viễn của UE sử dụng khóa công khai của nhà khai thác mạng gia đình).

Cần lưu ý rằng, trong một ví dụ, nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identity - IMSI) là thông tin nhận dạng thuê bao vĩnh viễn (nhận dạng thuê bao) của UE. Theo một phương án, IMSI có độ dài 15 chữ số cố định và bao gồm mã quốc gia di động (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 9 chữ số (Mobile Station Identification Number - MSIN).

Trong hệ thống truyền thông 5G, IMSI được gọi là thông tin nhận dạng vĩnh viễn thuê bao (Subscription Permanent Identifier - SUPI). SUPI không bao giờ được gửi qua giao diện vô tuyến (trừ khi trong các trường hợp khẩn cấp). Trong trường hợp IMSI dưới dạng SUPI, MSIN cung cấp nhận dạng thuê bao. Vì vậy, chỉ phần MSIN của IMSI cần

được mã hóa. Các phần MNC và MCC của IMSI cung cấp thông tin định tuyến, được sử dụng bởi mạng phục vụ để định tuyến đến mạng gia đình chính xác. SUPI được bảo vệ bằng mã hóa được gọi là thông tin nhận dạng thuê bao được che giấu (Subscription Concealed Identifier - SUCI). Nhà khai thác mạng gia đình (nhà khai thác mạng di động hoặc MNO) tạo ra một hoặc nhiều cặp khóa công khai/bảo mật nhằm mục đích cho phép che giấu SUPI. Khóa công khai của cặp khóa đã biết được cung cấp cho tất cả các thuê bao MNO và được sử dụng để che giấu SUPI. Chỉ MNO có thể trích xuất SUPI, do MNO có khóa bảo mật tương ứng.

Các SUPI thường được lưu trữ trong phần quản lý dữ liệu người dùng/kho lưu trữ dữ liệu người dùng (User Data Management/User Data Repository - UDM/UDR) và được quản lý bởi MNO. MNO có thể có một số đối tượng UDM truy cập được qua phần trước (front end) UDM, mỗi trong số chúng liên quan đến một nhóm thuê bao riêng biệt. Ngoài ra, MNO có thể đã ký hợp đồng tài nguyên với nhà khai thác mạng di động ảo (Mobile Virtual Network Operator - MVNO), mà cũng có thể có phần được cấp phát của UDM.

Theo quan điểm MVNO, MNO chia sẻ/cung cấp các tài nguyên của nó cho MVNO, nhưng MVNO có cơ sở dữ liệu của riêng nó. Có thể MNO quản lý thuê bao thay cho MVNO, nhưng với trường hợp này, nó sẽ thường sử dụng đối tượng UDM riêng biệt.

Trước khi đối tượng UDM chính xác có thể được định địa chỉ, SUCI cần được giải mã (hoặc trích xuất). Thực thể mới được gọi là chức năng trích xuất thông tin nhận dạng thuê bao (SIDF) đã được giới thiệu trong 3GPP TS 33.501 nhằm trích xuất SUCI.

3GPP TS 33.501 không định địa chỉ nơi nào trong mạng SIDF nên được đặt. Nên hiểu là SIDF và UDM có thể được đặt cùng và/hoặc SIDF có thể được đề nghị dưới dạng dịch vụ được cung cấp bởi UDM. SIDF có thể được lưu trữ bởi mỗi đối tượng UDM. Theo cách khác, SIDF có thể được đặt cùng với chức năng xác thực và bảo mật (Authentication and Security Function - AUSF), hoặc một số phần tử/chức năng mạng khác.

Không phân biệt nơi mà SIDF được thực thi thực tế, điều thấy được là vấn đề tồn tại là cách để chọn SIDF thích hợp trong hệ thống truyền thông. Vấn đề này gây rắc rối cụ thể nếu MNO có một số đối tượng UDM và cũng có các MVNO được ký hợp đồng mà có cặp khóa công khai/bảo mật của riêng chúng cho các hoạt động liên quan đến bảo

mật. Trong trường hợp MNO có các hợp đồng MVNO, mỗi MNO và các MVNO có thể muốn thao tác các SIDF của riêng chúng, một SIDF cho mỗi trong số các MNO/MVNO. Hơn nữa, một trường hợp sử dụng khác là chỉ có một SIDF toàn cầu hoặc trung tâm cho MNO, nhưng một số cặp khóa công khai được lưu trữ. Vì vậy, các MVNO có thể cung cấp cặp khóa công khai/bảo mật của chính chúng cho các thuê bao của chúng, nhưng việc quản lý vẫn thuộc về MNO. Đối với tùy chọn thứ ba, cặp khóa công khai/bảo mật của MNO cũng có thể là hợp lệ đối với các MVNO.

Các phương án minh họa khắc phục các vấn đề trên đây và các vấn đề khác kết hợp với việc chọn thực thể quản lý bảo mật thuê bao thích hợp, như SIDF, trong hệ thống truyền thông. Cụ thể hơn, khi cung cấp khóa công khai liên quan đến bảo mật cho tất cả các thuê bao của nhà khai thác mạng gia đình, nhà khai thác mạng gia đình hoặc thực thể cung cấp bao gồm thông tin nhận dạng mới (số nhận dạng, mã, địa chỉ, v.v.) mà nhờ đó thực thể quản lý bảo mật, như chức năng trích xuất SIDF, có thể được đặt trong miền của nhà khai thác. Theo các phương án minh họa, thông tin nhận dạng thực thể quản lý bảo mật có thể chỉ đến vị trí trung tâm hoặc đến đối tượng UDM. Theo một phương án khác, thông tin nhận dạng thực thể quản lý bảo mật có thể có trong thông tin nhận dạng khóa nếu mức bảo mật thấp hơn có thể chấp nhận được. Tuy nhiên, theo các phương án ưu tiên, điều này không phải là tối ưu do thông tin nhận dạng khóa là để tìm khóa chính xác để trích xuất, không nhất thiết là để tìm vị trí của chức năng trích xuất.

Vì vậy, theo các phương án minh họa, định dạng SUCI được cải tiến để truyền thông tin nhận dạng thực thể quản lý bảo mật trong yêu cầu đăng ký khởi tạo UE. Thông tin nhận dạng thực thể quản lý bảo mật có thể được gọi là "thông tin nhận dạng SIDF" hoặc "thông tin nhận dạng MNO/MVNO" mà dẫn đến SIDF chuyên dụng. Điều này là có lợi nếu MNO và MVNO có cùng thông tin định tuyến (MCC+MNC) và MNO cần phải đối hướng đến MVNO. Theo các phương án khác, cần hiểu rằng thông tin định danh SIDF (thông tin nhận dạng) có thể được gửi nằm ngoài định dạng thông báo SUCI.

Fig.1 thể hiện hệ thống truyền thông 100 mà trong đó các phương án minh họa được thực hiện. Cần hiểu rằng các phần tử được thể hiện trong hệ thống truyền thông 100 nhằm thể hiện các chức năng chính được cung cấp trong hệ thống, ví dụ, các chức năng truy cập UE, các chức năng quản lý di động, các chức năng xác thực, các chức năng cổng dịch vụ, v.v.. Như vậy, các khối được thể hiện trên Fig.1 tham chiếu đến các phần tử riêng 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 thi một số hoặc toàn bộ các chức năng được thể hiện. Ngoài ra, cần hiểu rằng không phải tất cả các chức năng của mạng 5G được thể hiện trên Fig.1. Ngoài ra, các chức năng mà hỗ trợ việc giải thích các phương án minh họa được thể hiện. Các hình vẽ tiếp theo có thể thể hiện một số phần tử/chức năng bổ sung.

Do đó, như được thể hiện, hệ thống truyền thông 100 bao gồm thiết bị người dùng (UE) 102 mà truyền thông 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, ví dụ, điện thoại di động, máy tính, hoặc loại thiết bị truyền thông khác bất kỳ. Do đó, thuật ngữ "thiết bị người dùng" như được sử dụng ở đây được dự định là được hiểu theo nghĩa rộng, để bao hàm nhiều loại trạm di động, trạm thuê bao khác nhau hoặc, chung hơn là, các thiết bị truyền thông, bao gồm các ví dụ như sự kết hợp của thẻ dữ liệu được cắm vào máy tính xách tay hoặc thiết bị khác như điện thoại thông minh. Các thiết bị truyền thông này cũng được dự định để bao hàm các thiết bị được gọi chung là các thiết bị đầu cuối truy cập.

Theo một phương án, UE 102 bao gồm UICC và ME. UICC là phần phụ thuộc vào người dùng của UE và chứa ít nhất một môđun nhận dạng thuê bao toàn cầu (Universal Subscriber Identity Module - USIM) và phần mềm ứng dụng thích hợp. USIM lưu trữ bảo mật số IMSI 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 thiết bị đầu cuối (terminal equipment - TE) và các chức năng đầu cuối di động (mobile termination - MT).

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 cơ sở và một hoặc nhiều chức năng điều khiển mạng vô tuyến kết hợp. Các trạm cơ sở và các chức năng điều khiển mạng vô tuyến có thể là các thực thể tách rời về mặt logic, nhưng theo phương án đã biết có thể được thực hiện trong cùng một phần tử mạng vật lý, như, ví dụ, bộ định tuyến trạm cơ sở hoặc điểm truy cập dạng ô femto.

Điểm truy cập 104 theo phương án minh họa này được ghép nối theo cách hoạt động với các chức năng quản lý di động 106. Trong mạng 5G, chức năng quản lý di động được thực thi bởi chức năng quản lý truy cập và di động (Access and Mobility Management Function - AMF). Chức năng neo bảo mật (Security Anchor Function - SEAF) cũng có thể được thực thi với AMF nối UE 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 trong phần mạng lõi (CN) của hệ thống truyền thông mà quản lý, trong số các hoạt động mạng khác, các hoạt động xác thực và truy cập với UE (qua điểm truy cập 104).

AMF 106 theo phương án minh họa này được ghép nối theo cách hoạt động với các chức năng thuê bao thường trú 108, tức là, một hoặc nhiều chức năng có trong mạng gia đình của thuê bao. Như được thể hiện, một số trong số các chức năng này bao gồm các chức năng AUSF, SIDF, và UDM nêu trên, cũng như chức năng kho lưu trữ mạng (Network Repository Function - NRF).

Điểm truy cập 104 cũng được ghép nối theo cách hoạt động với chức năng cổng dịch vụ 110 (ví dụ, chức năng quản lý phiên (Session Management Function - SMF) trong mạng 5G), mà được ghép nối theo cách hoạt động với cổng mạng dữ liệu gói (Packet Data Network - PDN) (PGW) 112. PGW 112 được ghép nối theo cách hoạt động với mạng dữ liệu gói, ví dụ, Internet 114. Các hoạt động và các chức năng đặc trưng khác của các phần tử mạng này không được mô tả ở đây do chúng không phải là trọng điểm của các phương án minh họa và có thể được tìm thấy trong tài liệu 5G 3GPP thích hợp.

Cần hiểu rằng cách bố trí cụ thể này của các phần tử hệ thống chỉ là ví dụ, và các loại và các cách bố trí khác của các phần tử bổ sung hoặc thay thế có thể được sử dụng để thực thi 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/các chức năng khác không được thể hiện rõ ràng ở đây.

Do đó, cách bố trí trên Fig.1 chỉ là một cấu hình ví dụ của hệ thống tế bào 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 UE, gNB, AMF, SEAF, AUSF, SIDF, NRF, UDM, SMF và PGW được thể hiện trong phương án trên Fig.1, nhưng điều này chỉ nhằm mô tả đơn giản và rõ ràng. Phương án thay thế đã biết hiển nhiên là có thể bao gồm số lượng lớn các phần tử hệ thống này, cũng như các phần tử bổ sung hoặc thay thế thuộc loại kết hợp chung với các phương án thực thi hệ thống thông thường.

Cũng cần lưu ý rằng mặc dù Fig.1 minh họa các phần tử hệ thống như là các khối chức năng đơn lẻ, nhưng các mạng con khác nhau mà tạo thành mạng 5G được phân chia thành các lát mạng (network slice). Các lát mạng (các phân vùng mạng) bao gồm một loạt các tập hợp chức năng (tức là, các chuỗi chức năng) cho mỗi loại dịch vụ tương ứng

sử dụng sự ảo hóa chức năng mạng (network function virtualization - NFV) trên cơ sở hạ tầng vật lý chung. Các lát mạng được tạo phiên bản khi cần đối với dịch vụ đã biết, ví dụ, dịch vụ eMBB, dịch vụ IoT quy mô lớn, và dịch vụ IoT then chốt. Vì vậy, lát mạng hoặc chức năng được tạo phiên bản khi trường hợp mà lát mạng hoặc chức năng được tạo ra. Theo một số phương án, điều này bao gồm việc cài đặt hoặc theo cách khác là chạy lát mạng hoặc chức năng trên một hoặc nhiều thiết bị chủ (host device) của cơ sở hạ tầng vật lý ở dưới. UE 102 được tạo cấu hình để truy cập một hoặc nhiều dịch vụ trong số các dịch vụ này qua gNB 104.

Fig.2 là sơ đồ khối của các phần tử/các chức năng mạng để cung cấp sự quản lý bảo mật thuê bao theo phương án minh họa. Hệ thống 200 được thể hiện bao gồm phần tử/chức năng mạng thứ nhất 202 và phần tử/chức năng mạng thứ hai 204. Cần hiểu rằng các phần tử/các chức năng mạng 202 và 204 thể hiện các phần tử/các chức năng mạng bất kỳ nêu trên, ví dụ, AMF, SEAF, AUSF, SIDF, NRF, UDM, mà được tạo cấu hình để cung cấp sự quản lý bảo mật thuê bao và các kỹ thuật khác được mô tả ở đây. Ví dụ, phần tử/chức năng mạng 202 có thể là AUSF và phần tử/chức năng mạng 204 có thể là UDM. Theo cách khác, phần tử/chức năng mạng 202 có thể là UDM và phần tử/chức năng mạng 204 có thể là SIDF.

Phần tử/chức năng mạng 202 bao gồm bộ xử lý 212 được ghép nối với bộ nhớ 216 và mạch giao diện 210. Bộ xử lý 212 của phần tử/chức năng mạng 202 bao gồm môđun xử lý quản lý bảo mật 214 mà có thể được thực hiện ít nhất một phần dưới dạng phần mềm được thực thi bởi bộ xử lý. Môđun xử lý 214 thực hiện quản lý bảo mật được mô tả kết hợp với các hình vẽ tiếp theo và theo cách khác ở đây. Bộ nhớ 216 của phần tử/chức năng mạng 202 bao gồm môđun lưu trữ quản lý bảo mật 218 để lưu trữ dữ liệu được tạo ra hoặc theo cách khác được sử dụng trong các quá trình quản lý bảo mật.

Phần tử/chức năng mạng 204 bao gồm bộ xử lý 222 được ghép nối với bộ nhớ 226 và mạch giao diện 220. Bộ xử lý 222 của phần tử/chức năng mạng 204 bao gồm môđun xử lý quản lý bảo mật 224 mà có thể được thực hiện ít nhất một phần dưới dạng phần mềm được thực thi bởi bộ xử lý 222. Môđun xử lý 224 thực hiện quản lý bảo mật được mô tả kết hợp với các hình vẽ tiếp theo và theo cách khác ở đây. Bộ nhớ 226 của phần tử/chức năng mạng 204 bao gồm môđun lưu trữ quản lý bảo mật 228 để lưu trữ dữ liệu được tạo ra hoặc theo cách khác được sử dụng trong các quá trình quản lý bảo mật.

Các bộ xử lý 212 và 222 của các phần tử/các chức năng mạng 202 và 204 tương ứng có thể bao gồm, ví dụ, các bộ vi xử lý, các mạch tích hợp chuyên dụng (ASIC), các bộ xử lý tín hiệu số (DSP) hoặc các loại thiết bị xử lý khác, cũng như các phần hoặc các sự kết hợp của các phần tử này.

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

Do đó, một trong số các bộ nhớ 216 hoặc 226 đã biết có thể được xem là một ví dụ về cái được đề cập chung đến ở đây là sản phẩm chương trình máy tính hoặc được đề cập chung hơn nữa là vật ghi lưu trữ đọc được bằng bộ xử lý có mã chương trình thực thi được được chứa trong đó. Các ví dụ khác về vật ghi lưu trữ đọc được bằng bộ xử lý có thể bao gồm đĩa hoặc các loại vật ghi từ tính hoặc quang học khác, theo sự kết hợp bất kỳ. Các phương án minh họa có thể bao gồm các vật phẩm gồm các sản phẩm chương trình máy tính này hoặc vật ghi lưu trữ đọc được bằng bộ xử lý khác.

Bộ nhớ 216 hoặc 226 cụ thể hơn có thể bao gồm, ví dụ, bộ nhớ truy cập ngẫu nhiên (random access memory - RAM) điện tử như RAM tĩnh (SRAM), RAM động (DRAM) hoặc các loại bộ nhớ điện tử khả biến hoặc không khả biến khác. Bộ nhớ điện tử khả biến hoặc không khả biến có thể bao gồm, ví dụ, các bộ nhớ không khả biến như bộ nhớ nhanh (flash memory), RAM từ tính (MRAM), RAM đổi pha (phase-change RAM - PC-RAM) hoặc RAM sắt điện (ferroelectric RAM - FRAM). Thuật ngữ "bộ nhớ" như được sử dụng ở đây được dự định để được hiểu theo nghĩa rộng, và ngoài ra hoặc theo cách khác có thể bao gồm, ví dụ, bộ nhớ chỉ đọc (read-only memory - ROM), bộ nhớ trên cơ sở đĩa (disk-based memory), hoặc loại thiết bị lưu trữ khác, cũng như các phần hoặc các sự kết hợp của các thiết bị này.

Các mạch giao diện 210 và 220 của các phần tử/các chức năng mạng 202 và 204 tương ứng bao gồm theo cách minh họa các bộ thu phát hoặc phần cứng hoặc phần sụn truyền thông khác mà cho phép các phần tử hệ thống kết hợp truyền thông với nhau theo

cách được mô tả ở đây.

Trên Fig.2, rõ ràng là phần tử/chức năng mạng 202 được tạo cấu hình để truyền thông với phần tử/chức năng mạng 204 và ngược lại qua các mạch giao diện 210 và 220 tương ứng của chúng. Việc truyền thông này bao gồm phần tử/chức năng mạng 202 gửi dữ liệu đến phần tử/chức năng mạng 204, và phần tử/chức năng mạng 204 gửi dữ liệu đến phần tử/chức năng mạng 202. Tuy nhiên, theo các phương án khác, các phần tử mạng khác có thể được ghép nối theo cách hoạt động được giữa các phần tử/các chức năng mạng 202 và 204. Thuật ngữ "dữ liệu" như được sử dụng ở đây được dự định để hiểu theo nghĩa rộng, để bao hàm loại thông tin bất kỳ có thể được gửi giữa các phần tử/các chức năng mạng (cũng như giữa thiết bị người dùng và mạng lõi) bao gồm, nhưng không bị giới hạn ở, dữ liệu nhận dạng, các cặp khóa, các bộ chỉ báo khóa, các thông tin nhận dạng thực thể quản lý bảo mật, dữ liệu xác thực, dữ liệu điều khiển, âm thanh, viđeo, đa phương tiện, v.v.

Cần hiểu rằng cách bố trí cụ thể của các thành phần được thể hiện trên Fig.2 chỉ là ví dụ, và nhiều cấu hình thay thế có thể được sử dụng trong các phương án khác. Ví dụ, phần tử/chức năng mạng đã biết bất kỳ có thể được tạo 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 UE 102 và gNB 104, mỗi phần tử cũng có thể được tạo cấu hình để bao gồm các thành phần như bộ xử lý, bộ nhớ và giao diện mạng. Các phần tử này không cần phải được thực thi trên các nền tảng xử lý độc lập riêng rẽ, mà thay vào đó có thể, ví dụ, biểu diễn các phần chức năng khác của một nền tảng xử lý chung.

Với cấu hình mạng 5G minh họa được mô tả trên đây, theo các phương án minh họa, sau khi AMF của mạng tạm trú (visiting network - VN) đã nhận dạng AUSF (108) của mạng gia đình (HN) của thuê bao đã biết (UE) từ MCC+MNC của SUCI, AMF cung cấp SUCI cho AUSF. Cần lưu ý rằng, theo các phương án minh họa, SUCI ngoài thông tin nhận dạng khóa còn bao gồm thông tin nhận dạng SIDF. Cần hiểu rằng khi có trong thông báo SUCI, thì thông tin nhận dạng SIDF không được che giấu. Như đã nêu trên, theo các phương án khác, thông tin nhận dạng SDF có thể được gửi ở ngoài định dạng SUCI. Ví dụ, thông tin nhận dạng SIDF có thể là một phần tử thông tin khi yêu cầu AV đối với SUCI được gửi.

Nói chung, AUSF có thể nhận các yêu cầu AV với SUPI hoặc SUCI, loại sau trong việc đăng ký ban đầu, loại trước, nếu UE đã được xác thực và AMF hoặc phần tử/chức năng mạng khác biết SUPI. Vì vậy, nếu AUSF nhận thông tin nhận dạng SIDF, thì đó cũng là sự chỉ báo rằng sự bảo mật được sử dụng (tương tự như thông tin nhận dạng khóa). Vì vậy, AUSF được tạo cấu hình để trước tiên yêu cầu dịch vụ SIDF được đề nghị UDM với SUCI bao gồm thông tin nhận dạng SIDF. Sau đó, sau khi AUSF trở lại SUPI, AUSF có thể gửi yêu cầu dữ liệu xác thực (các vectơ xác thực hay các AV) đến UDM (có thể là sau khi liên hệ NRF đối với đối tượng UDM chính xác).

Theo cách khác, AUSF có thể gửi yêu cầu AV với SUCI và nhận lại SUPI với các AV. Trong trường hợp này, UDM đang xử lý việc trích xuất qua SIDF ở bên trong và sử dụng SUPI để hướng yêu cầu đến đối tượng UDM chính xác trước khi đáp lại yêu cầu AV.

Trong trường hợp khác, được giới thiệu là SIDF trong UDM có thông tin nhận dạng định địa chỉ trung tâm. Theo một số phương án, điều được mong muốn là tránh có một số đối tượng dành cho SIDF và gấp đôi các khóa bảo mật từ quan điểm quản lý trong trường hợp cập nhật. Trên thực tế, địa chỉ của SIDF có thể được quy định theo một số phương án nếu sự bảo mật được bật.

Các phần chi tiết thêm liên quan đến việc thực hiện sự quản lý bảo mật thuê bao cùng với việc sử dụng thông tin nhận dạng thực thể quản lý bảo mật sẽ được thảo luận dưới đây có dựa vào các hình vẽ từ Fig.3 đến Fig.5.

Fig.3 là lưu đồ của phương pháp quản lý bảo mật thuê bao theo phương án minh họa. Cụ thể hơn là phương pháp 300 mô tả giai đoạn cung cấp ban đầu nhờ đó các thiết bị thuê bao (UE) được cung cấp dữ liệu bảo mật để cho phép chúng truy cập hệ thống truyền thông qua giao diện vô tuyến mà không để lộ các thông tin nhận dạng vĩnh viễn của chúng. Việc cung cấp dữ liệu bảo mật cho UE có thể xảy ra trực tuyến (ví dụ, UE được kết nối với hệ thống truyền thông), ngoại tuyến (ví dụ, UE không được kết nối với hệ thống truyền thông), hoặc một số sự kết hợp của cả hai loại.

Như được thể hiện, ở bước 302, nhà khai thác mạng gia đình (MNO hoặc thực thể cung cấp khác nào đó) cung cấp cho mỗi thiết bị thuê bao (ví dụ, UE 102): (1) khóa công khai từ cặp khóa công khai/khóa bảo mật để sử dụng khi che giấu thông tin nhận dạng vĩnh viễn; (2) thông tin nhận dạng đối với cặp khóa công khai/khóa bảo mật; và (3) thông

tin nhận dạng đối với thực thể quản lý bảo mật (ví dụ, SIDF) được tạo cấu hình để trích xuất thông tin nhận dạng vĩnh viễn của thuê bao (ví dụ, SUPI).

Sau đó, ở bước 304, mỗi thiết bị thuê bao (ví dụ, UE 102) truy cập mạng gia đình (ví dụ, các chức năng thuê bao thường trú 108) qua mạng tạm trú (ví dụ, các chức năng quản lý di động 106) sử dụng thông tin nhận dạng vĩnh viễn được che giấu (ví dụ, SUCI) bao gồm thông tin nhận dạng khóa và thông tin nhận dạng thực thể quản lý bảo mật (ví dụ, thông tin nhận dạng SIDF).

Fig.4 là sơ đồ khối của ít nhất một phần của hệ thống truyền thông thực hiện sự quản lý bảo mật thuê bao theo phương án minh họa. Cụ thể hơn là Fig.4 minh họa kịch bản 400 nhờ đó dữ liệu xác thực thuê bao được yêu cầu theo sau bước trích xuất. Giả sử rằng UE (102) gửi SUCI (MNC+MCC+ (MSIN) được mã hóa + thông tin nhận dạng khóa + thông tin nhận dạng SIDF) đến AMF (106) của mạng tạm trú. Cần hiểu rằng các thông số có thể được gửi theo thứ tự bất kỳ và có thể liên quan trực tiếp đến SUCI như được thể hiện trên đây hoặc các thông số này có thể là các phần tử thông tin riêng rẽ trong yêu cầu đến AUSF/UDM, nhờ đó yêu cầu có thể là yêu cầu trích xuất hoặc yêu cầu AV. Cũng giả sử rằng AMF trong mạng tạm trú chọn AUSF thích hợp trong mạng gia đình dựa trên MNC+MCC. Giả sử rằng AUSF 402 trên Fig.4 là AUSF được chọn.

AUSF 402 kiểm tra xem liệu SUPI hay SUCI được nhận. Nếu là SUCI thì AUSF 402 chuyển tiếp SUCI đến UDM (phần trước) 404, mà duy trì việc ánh xạ thông tin nhận dạng SIDF đến địa chỉ SIDF.

UDM 404 chọn và gọi SIDF trung tâm 406 dựa trên thông tin nhận dạng SIDF.

SIDF 406 sử dụng khóa bảo mật chính xác liên quan đến thông tin nhận dạng khóa nhận được để trích xuất SUCI. Điều này có nghĩa là, dựa trên thông tin nhận dạng khóa nhận được, SIDF có thể nhận dạng cặp khóa mật mã mà từ đó UE phụ thuộc đã sử dụng khóa công khai tương ứng để mã hóa SUPI của nó.

SIDF 406 cung cấp SUPI trở lại AUSF 402 qua UDM 404.

AUSF 402 có thể yêu cầu NRF (không được thể hiện rõ ràng ngoài phần của các chức năng thuê bao thường trú 108 như được nêu trên) đối với đối tượng UDM chính xác dựa trên SUPI. Như được thể hiện trên Fig.4, có thể có nhiều đối tượng UDM kết hợp với MNO 408, cũng như các đối tượng UDM riêng rẽ đối với nhiều MNVO 410 và 412.

AUSF 402 sau đó yêu cầu dữ liệu xác thực (tức là, các AV) từ đối tượng UDM thích hợp (trong ví dụ này, đối tượng UDM kết hợp với MVNO 410) cùng với SUPI.

Fig.5 là sơ đồ khối của ít nhất một phần của hệ thống truyền thông thực hiện sự quản lý bảo mật thuê bao theo một phương án minh họa khác. Cụ thể hơn, Fig.5 minh họa kịch bản 500 nhờ đó dữ liệu xác thực thuê bao được yêu cầu đồng thời với bước chọn thực thể quản lý bảo mật. Giả sử rằng UE (102) gửi SUCI (MNC+MCC+ (MSIN) được mã hóa + thông tin nhận dạng khóa + thông tin nhận dạng SIDF) đến AMF (106) của mạng tạm trú. Cũng giả sử rằng AMF trong mạng tạm trú chọn AUSF thích hợp trong mạng gia đình dựa trên MNC+MCC. Giả sử rằng AUSF 502 trên Fig.5 là AUSF được chọn.

AUSF 502 kiểm tra liệu SUPI hay SUCI được nhận. Nếu là SUCI, thì AUSF 502 chuyển tiếp SUCI cũng như yêu cầu dữ liệu xác thực (tức là, các AV) đến UDM (phần trước) 504, mà duy trì việc ánh xạ thông tin nhận dạng SIDF đến địa chỉ SIDF.

UDM 504 chọn và gọi SIDF chính xác trong số nhiều SIDF 505, 506 và 507, dựa trên thông tin nhận dạng SIDF. Trong ví dụ này, SIDF được chọn là SIDF 506 tương ứng với MVNO 510. Như được thể hiện trên Fig.5, có thể có nhiều đối tượng UDM kết hợp với MNO 508, cũng như các đối tượng UDM riêng rẽ đối với nhiều MNVO 510 và 512.

SIDF 506 sử dụng khóa bảo mật chính xác liên quan đến thông tin nhận dạng khóa nhận được để trích xuất SUCI. Nghĩa là, dựa trên thông tin nhận dạng khóa nhận được, SIDF 506 có thể nhận dạng cặp khóa mật mã mà từ đó UE phụ thuộc sử dụng khóa công khai tương ứng để mã hóa SUPI của nó.

SIDF 506 yêu cầu dữ liệu xác thực (ví dụ, các AV) từ đối tượng UDM kết hợp với MVNO 510.

Sau đó, SIDF 506 gửi các AV trở lại đến AUSF 502 qua UDM 504.

Theo đó, bằng cách bổ sung thông tin nhận dạng thực thể quản lý bảo mật (ví dụ, SIDF) vào SUCI, theo các phương án minh họa, tất cả các kịch bản cấu hình khác nhau có thể được định địa chỉ, ví dụ, MNO với một SIDF trung tâm (Fig.4), và MNO với SIDF khác đối với một hoặc một số đối tượng UDM (Fig.5).

Cụ thể là, trong trường hợp sử dụng MVNO, MNO có thể ký hợp đồng các phần của cơ sở dữ liệu thuê bao của nó, tức là, một đối tượng UDM. Sau đó, MVNO có thể có

SIDF của riêng nó hoặc nó cũng có thể sử dụng SIDF từ MNO, nhưng với thông tin nhận dạng khóa khác. Nhưng MNO đồng thời có thể muốn có cho các đối tượng UDM khác của nó chỉ một thông tin nhận dạng SIDF. Mỗi trong số các kịch bản này là khả dụng theo các phương án minh họa.

Theo một phương án minh họa khác nữa, một mình thông tin nhận dạng khóa có thể là đủ để đóng vai trò làm thông tin nhận dạng đối với SIDF trung tâm, nếu bắt buộc là nếu bộ chỉ báo bảo mật được thiết lập, thì AUSF hoặc UDM luôn luôn liên hệ với SIDF đầu tiên.

Cần hiểu rằng việc đặt tên các thông tin nhận dạng được nêu ở đây, ví dụ, IMSI, SUPI, SUCI, v.v., chỉ nhằm mục đích minh họa. Nghĩa là, thông tin nhận dạng dùng cho UE có thể có các tên hoặc các chữ viết tắt khác trong các giao thức và các tiêu chuẩn khác đối với các công nghệ mạng truyền thông khác nhau. Như vậy, không có tên hoặc chữ viết tắt cụ thể nào được gắn cho các thông tin nhận dạng ở đây được dự định để giới hạn các phương án theo cách bất kỳ.

Như được nêu trên, các phương án không bị giới hạn ở ngữ cảnh 5G và các kỹ thuật được bộc lộ có thể được làm thích ứng theo cách đơn giản với rất nhiều loại ngữ cảnh hệ thống truyền thông khác bao gồm, nhưng không bị giới hạn ở, các hệ thống 3GPP khác và các hệ thống phi 3GPP khác mà sử dụng nhận dạng (ví dụ, IMSI hoặc tương đương) trong quy trình yêu cầu nhận dạng.

Bộ xử lý, bộ nhớ, bộ điều khiển và các thành phần khác của thiết bị người dùng hoặc phần tử trạm cơ sở của hệ thống truyền thông như được bộc lộ ở đây có thể bao gồm mạch đã biết rộng rãi được cải biến một cách thích hợp để thực thi ít nhất một phần của chức năng yêu cầu nhận dạng được mô tả trên đây.

Như đã nêu trên, các phương án có thể được thực hiện dưới dạng các vật phẩm, mỗi vật phẩm bao gồm một hoặc nhiều chương trình phần mềm được thực thi bởi mạch xử lý của thiết bị người dùng, các trạm cơ sở hoặc các phần tử khác của hệ thống truyền thông. Các khía cạnh thông thường của mạch này đã được biết đến rộng rãi đối với người có hiểu biết trung bình trong lĩnh vực liên quan và do đó sẽ không được mô tả chi tiết ở đây. Ngoài ra, các phương án có thể được thực hiện trong một hoặc nhiều ASIC, FPGA hoặc các loại thiết bị mạch tích hợp khác, theo cách kết hợp bất kỳ. Các thiết bị mạch tích hợp này, cũng như các phần hoặc các sự kết hợp của chúng, là các ví dụ về "mạch" khi

thuật ngữ đó được sử dụng ở đây. Rất nhiều cách bố trí khác của phần cứng và phần mềm hoặc phần sụn kết hợp có thể được sử dụng khi thực hiện các phương án minh họa.

Do đó, cần nhấn mạnh lại rằng các phương án khác nhau được mô tả ở đây được đưa ra chỉ là ví dụ minh họa, và không nên được hiểu làm giới hạn phạm vi yêu cầu bảo hộ. Ví dụ, các phương án thay thế có thể sử dụng các cấu hình hệ thống truyền thông khác, các cấu hình thiết bị người dùng khác, các cấu hình trạm cơ sở khác, các quy trình cung cấp và sử dụng cặp khóa khác, các giao thức gửi thông báo khác và các định dạng thông báo khác với những loại được mô tả trên đây trong ngữ cảnh của các phương án minh họa. Các phương án thay thế này và nhiều phương án thay thế khác nằm trong phạm vi của yêu cầu bảo hộ kèm theo sẽ được hiểu rõ một cách dễ dàng đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật liên quan.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông bao gồm các bước:

trong mạng gia đình của hệ thống truyền thông, trong đó một hoặc nhiều cặp khóa mật mã được cung cấp để sử dụng bởi một hoặc nhiều thuê bao của mạng gia đình để che giấu các thông tin nhận dạng thuê bao được cung cấp cho một hoặc nhiều điểm truy cập trong hệ thống truyền thông;

thu nhận, tại một trong số một hoặc nhiều điểm truy cập từ thiết bị người dùng, yêu cầu dữ liệu xác thực đối với một trong số các thuê bao, yêu cầu dữ liệu xác thực này bao gồm thông tin nhận dạng thuê bao được che giấu và thông tin nhận dạng thực thể quản lý bảo mật, thông tin nhận dạng thực thể quản lý bảo mật nhận dạng một trong số một hoặc nhiều thực thể quản lý bảo mật trong mạng gia đình của hệ thống truyền thông được tạo cấu hình để trích xuất thông tin nhận dạng thuê bao được che giấu;

sử dụng một trong số một hoặc nhiều thực thể quản lý bảo mật này trong mạng gia đình của hệ thống truyền thông được nhận dạng bởi thông tin nhận dạng thực thể quản lý bảo mật trong yêu cầu dữ liệu xác thực để trích xuất thông tin nhận dạng thuê bao được che giấu; và

thu nhận, từ một trong số các đối tượng khác nhau của kho lưu trữ dữ liệu người dùng, dữ liệu xác thực đối với một trong số các thuê bao này sử dụng thông tin nhận dạng được trích xuất, mỗi trong số các đối tượng khác nhau của kho lưu trữ dữ liệu người dùng lưu trữ dữ liệu xác thực đối với tập hợp con khác của các thuê bao của mạng gia đình;

trong đó một trong số một hoặc nhiều thực thể quản lý bảo mật này trong mạng gia đình của hệ thống truyền thông bao gồm một trong số:

thực thể quản lý bảo mật trung tâm trong mạng gia đình mà quản lý việc trích xuất các thông tin nhận dạng thuê bao được che giấu đối với nhà khai thác mạng di động trong mạng gia đình và một hoặc nhiều nhà khai thác mạng di động ảo trong mạng gia đình;

thực thể quản lý bảo mật dành riêng thứ nhất kết hợp với nhà khai thác mạng di động trong mạng gia đình; và

thực thể quản lý bảo mật dành riêng thứ hai kết hợp với một trong số một hoặc nhiều nhà khai thác mạng di động ảo trong mạng gia đình.

2. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước chọn một hoặc nhiều thực thể quản lý bảo mật trong hệ thống truyền thông dựa ít nhất một phần vào thông tin nhận dạng thực thể quản lý bảo mật được nhận trong yêu cầu dữ liệu xác thực.

3. Phương pháp theo điểm 2, phương pháp này còn bao gồm bước trích xuất thông tin nhận dạng thuê bao được che giấu tại thực thể quản lý bảo mật được chọn.

4. Phương pháp theo điểm 3, phương pháp này còn bao gồm bước yêu cầu dữ liệu xác thực thuê bao đồng thời với bước chọn thực thể quản lý bảo mật.

5. Phương pháp theo điểm 4, trong đó chức năng xác thực và bảo mật của hệ thống truyền thông yêu cầu trích xuất thông tin nhận dạng thuê bao được che giấu đồng thời với việc yêu cầu dữ liệu xác thực đối với một trong số các thuê bao này.

6. Phương pháp theo điểm 3, phương pháp này còn bao gồm bước yêu cầu dữ liệu xác thực thuê bao theo sau bước trích xuất.

7. Phương pháp theo điểm 6, trong đó chức năng xác thực và bảo mật của hệ thống truyền thông yêu cầu trích xuất thông tin nhận dạng thuê bao đã biết và, đáp lại việc nhận thông tin nhận dạng thuê bao được trích xuất, thì yêu cầu dữ liệu xác thực đối với một trong số các thuê bao này.

8. Phương pháp theo điểm 1, trong đó ít nhất một trong số một hoặc nhiều thực thể quản lý bảo mật được thực thi trong hệ thống truyền thông dưới dạng chức năng trích xuất thông tin nhận dạng thuê bao.

9. Phương pháp theo điểm 1, trong đó mạng gia đình bao gồm nhiều đối tượng quản lý dữ liệu người dùng.

10. Phương pháp theo điểm 9, trong đó nhiều đối tượng quản lý dữ liệu người dùng này bao gồm một hoặc nhiều đối tượng quản lý dữ liệu người dùng kết hợp với một hoặc nhiều nhà khai thác mạng ảo.

11. Phương pháp theo điểm 9, trong đó thực thể quản lý bảo mật trung tâm được sử dụng cho nhiều đối tượng quản lý dữ liệu người dùng.

12. Phương pháp theo điểm 9, trong đó nhiều thực thể quản lý bảo mật dành riêng được

sử dụng cho nhiều đối tượng quản lý dữ liệu người dùng.

13. Vật phẩm để truyền thông bao gồm vật ghi lâu dài đọc được bằng máy tính có chứa trong đó mã chương trình thực thi được mà khi được thực thi bởi bộ xử lý làm cho bộ xử lý này thực hiện các bước theo điểm 1.

14. Thiết bị truyền thông bao gồm:

trong mạng gia đình của hệ thống truyền thông, trong đó một hoặc nhiều cặp khóa mật mã được cung cấp để sử dụng bởi một hoặc nhiều thuê bao của mạng gia đình để che giấu các thông tin nhận dạng thuê bao được cung cấp cho một hoặc nhiều điểm truy cập trong hệ thống truyền thông;

ít nhất một bộ xử lý;

ít nhất một bộ nhớ gồm mã chương trình máy tính;

ít nhất một bộ nhớ và mã chương trình máy tính được tạo cấu hình để, với ít nhất một bộ xử lý, làm cho thiết bị này ít nhất thực hiện các bước:

thu nhận, tại một trong số một hoặc nhiều điểm truy cập từ thiết bị người dùng, yêu cầu dữ liệu xác thực đối với một trong số các thuê bao, yêu cầu dữ liệu xác thực này bao gồm thông tin nhận dạng thuê bao được che giấu và thông tin nhận dạng thực thể quản lý bảo mật, thông tin nhận dạng thực thể quản lý bảo mật nhận dạng một trong số một hoặc nhiều thực thể quản lý bảo mật trong mạng gia đình của hệ thống truyền thông được tạo cấu hình để trích xuất thông tin nhận dạng thuê bao được che giấu;

sử dụng một trong số một hoặc nhiều thực thể quản lý bảo mật này trong mạng gia đình của hệ thống truyền thông được nhận dạng bởi thông tin nhận dạng thực thể quản lý bảo mật trong yêu cầu dữ liệu xác thực để trích xuất thông tin nhận dạng thuê bao được che giấu; và

thu nhận, từ một trong số các đối tượng khác nhau của kho lưu trữ dữ liệu người dùng, dữ liệu xác thực đối với một trong số các thuê bao này sử dụng thông tin nhận dạng được trích xuất, mỗi trong số các đối tượng khác nhau của kho lưu trữ dữ liệu người dùng lưu trữ dữ liệu xác thực đối với tập hợp con khác của các thuê bao của mạng gia đình;

trong đó một trong số một hoặc nhiều thực thể quản lý bảo mật này trong mạng gia đình của hệ thống truyền thông bao gồm một trong số:

thực thể quản lý bảo mật trung tâm trong mạng gia đình mà quản lý việc trích xuất các thông tin nhận dạng thuê bao được che giấu đối với nhà khai thác mạng di động trong mạng gia đình và một hoặc nhiều nhà khai thác mạng di động ảo trong mạng gia đình;

thực thể quản lý bảo mật dành riêng thứ nhất kết hợp với nhà khai thác mạng di động trong mạng gia đình; và

thực thể quản lý bảo mật dành riêng thứ hai kết hợp với một trong số một hoặc nhiều nhà khai thác mạng di động ảo trong mạng gia đình.

15. Phương pháp truyền thông bao gồm các bước:

trong thiết bị người dùng, lưu trữ: (i) một hoặc nhiều khóa công khai kết hợp với một hoặc nhiều cặp khóa mật mã, một hoặc nhiều cặp khóa mật mã được cung cấp bởi mạng gia đình của hệ thống truyền thông để sử dụng bởi thiết bị người dùng để che giấu thông tin nhận dạng thuê bao sẽ được cung cấp cho một hoặc nhiều điểm truy cập trong mạng truyền thông; và (ii) một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật để sử dụng bởi thiết bị người dùng khi cung cấp thông tin nhận dạng thuê bao được che giấu cho một hoặc nhiều điểm truy cập trong hệ thống truyền thông, trong đó mỗi trong số một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật nhận dạng thực thể quản lý bảo mật trong số một hoặc nhiều thực thể quản lý bảo mật trong mạng gia đình của hệ thống truyền thông được tạo cấu hình để trích xuất thông tin nhận dạng thuê bao được che giấu;

che giấu thông tin nhận dạng thuê bao sử dụng một trong số một hoặc nhiều khóa công khai;

gửi, từ thiết bị người dùng đến một trong số một hoặc nhiều điểm truy cập, yêu cầu dữ liệu xác thực đối với một trong số các thuê bao của mạng gia đình, yêu cầu dữ liệu xác thực bao gồm thông tin nhận dạng thuê bao được che giấu và một trong số một hoặc nhiều thông tin nhận dạng thực thể quản lý bảo mật kết hợp với một trong số một hoặc nhiều thực thể quản lý bảo mật trong mạng gia đình của hệ thống truyền thông; và

thu nhận, tại thiết bị người dùng từ một trong số một hoặc nhiều điểm truy cập này, dữ liệu xác thực đối với một trong số các thuê bao này, dữ liệu xác thực được thu từ một trong số các đối tượng khác nhau của kho lưu trữ dữ liệu người dùng trong mạng gia

đình, mỗi trong số các đối tượng khác nhau của kho lưu trữ dữ liệu người dùng lưu trữ dữ liệu xác thực đối với tập hợp con khác của các thuê bao của mạng gia đình;

trong đó một trong số một hoặc nhiều thực thể quản lý bảo mật này trong mạng gia đình của hệ thống truyền thông bao gồm một trong số:

thực thể quản lý bảo mật trung tâm trong mạng gia đình mà quản lý việc trích xuất các thông tin nhận dạng thuê bao được che giấu đối với nhà khai thác mạng di động trong mạng gia đình và một hoặc nhiều nhà khai thác mạng di động ảo trong mạng gia đình;

thực thể quản lý bảo mật dành riêng thứ nhất kết hợp với nhà khai thác mạng di động trong mạng gia đình; và

thực thể quản lý bảo mật dành riêng thứ hai kết hợp với một trong số một hoặc nhiều nhà khai thác mạng di động ảo trong mạng gia đình.

16. Phương pháp theo điểm 15, trong đó thiết bị người dùng lưu trữ thông tin nhận dạng khóa mà nhận dạng một trong số một hoặc nhiều cặp khóa mật mã được sử dụng bởi thiết bị người dùng để che giấu thông tin nhận dạng thuê bao.

17. Phương pháp theo điểm 16, phương pháp này còn bao gồm bước gửi thông tin nhận dạng khóa đến một trong số một hoặc nhiều điểm truy cập này trong hệ thống truyền thông.

18. Phương pháp theo điểm 17, trong đó thông tin nhận dạng thuê bao được che giấu, thông tin nhận dạng khóa, và thông tin nhận dạng thực thể quản lý bảo mật được gửi trong hai hoặc nhiều thông báo riêng biệt đến một trong số một hoặc nhiều điểm truy cập này.

19. Thiết bị truyền thông bao gồm bộ xử lý được ghép nối theo cách hoạt động được với bộ nhớ và được tạo cấu hình để thực hiện các bước theo điểm 15.

20. Vật phẩm để truyền thông bao gồm vật ghi lâu dài đọc được bằng máy tính có chứa trong đó mã chương trình thực thi được mà khi được thực thi bởi bộ xử lý làm cho bộ xử lý này thực hiện các bước theo điểm 15.

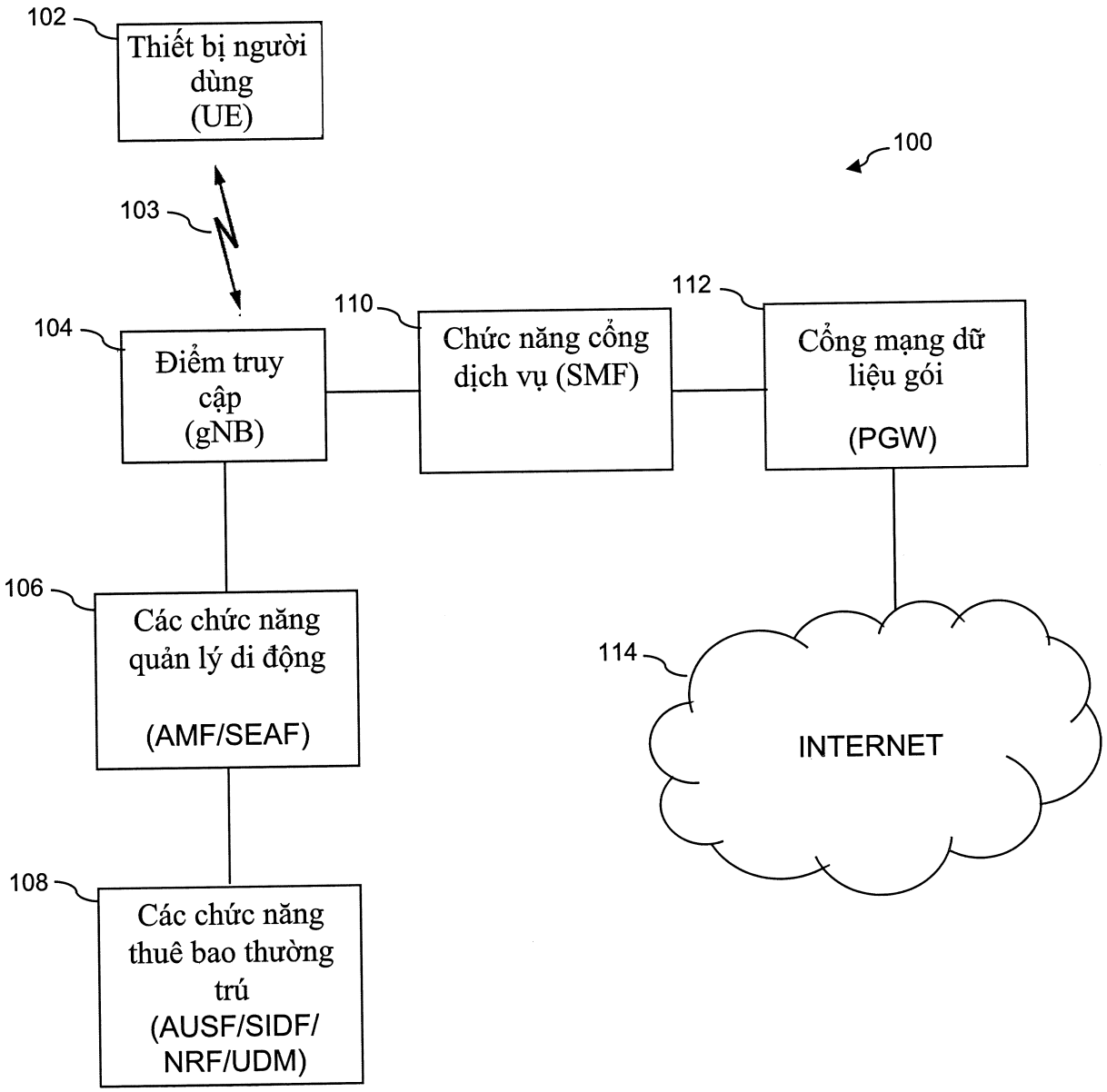

102
Thiết bị người dùng (UE)
100
103
112
110
104
Điểm truy cập (gNB)
Chức năng cổng dịch vụ (SMF)
Cổng mạng dữ liệu gói (PGW)
106
Các chức năng quản lý di động (AMF/SEAF)
114
INTERNET
108
Các chức năng thuê bao thường trú (AUSF/SIDF/ NRF/UDM)

FIG. 1

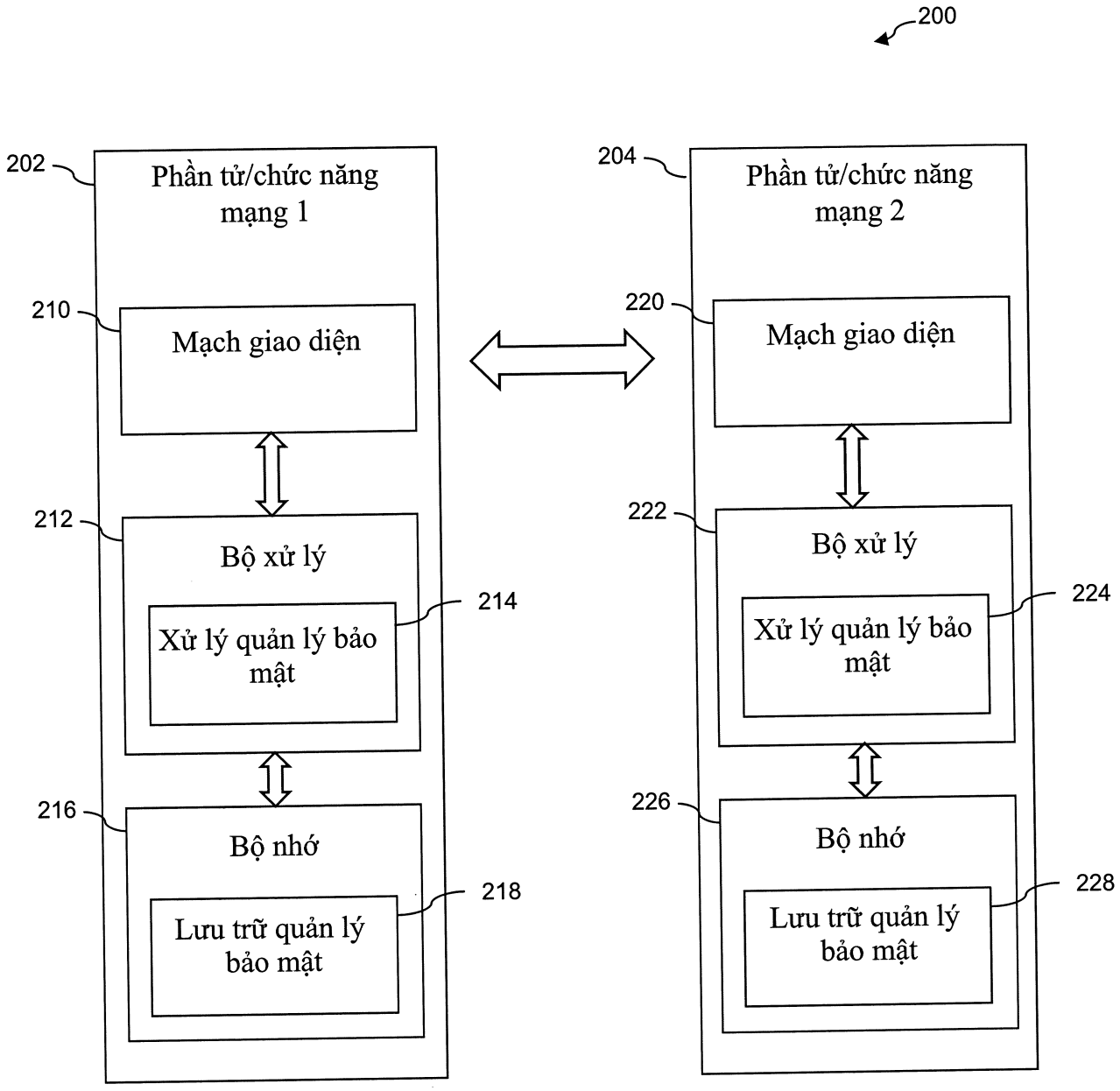

200
202
Phần tử/chức năng mạng 1
210
Mạch giao diện
212
Bộ xử lý
214
Xử lý quản lý bảo mật
216
Bộ nhớ
218
Lưu trữ quản lý bảo mật
204
Phần tử/chức năng mạng 2
220
Mạch giao diện
222
Bộ xử lý
224
Xử lý quản lý bảo mật
226
Bộ nhớ
228
Lưu trữ quản lý bảo mật

FIG. 2

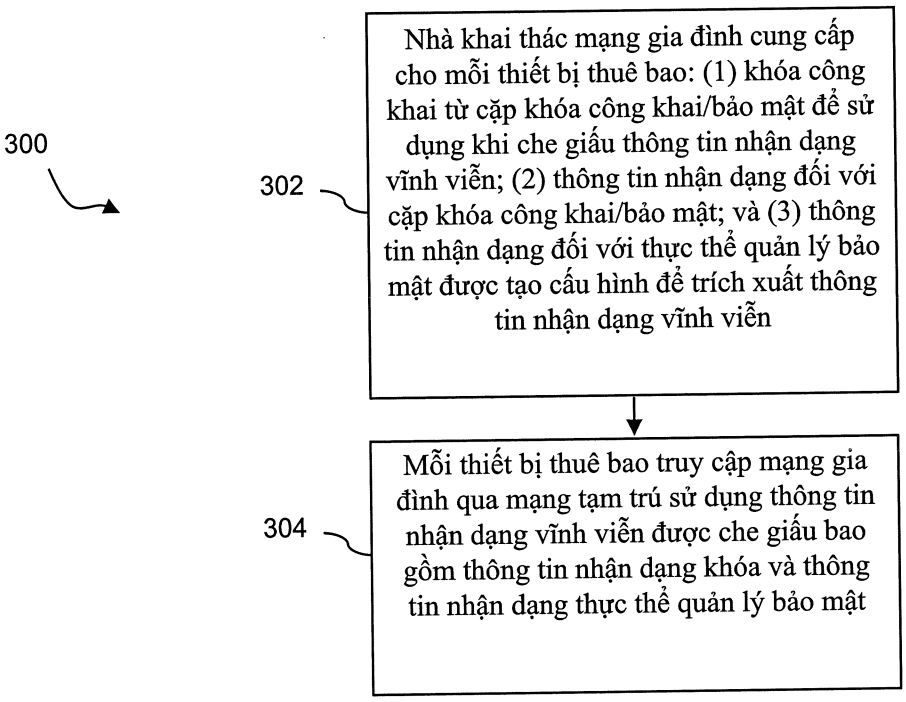

300
302
Nhà khai thác mạng gia đình cung cấp cho mỗi thiết bị thuê bao: (1) khóa công khai từ cặp khóa công khai/bảo mật để sử dụng khi che giấu thông tin nhận dạng vĩnh viễn; (2) thông tin nhận dạng đối với cặp khóa công khai/bảo mật; và (3) thông tin nhận dạng đối với thực thể quản lý bảo mật được tạo cấu hình để trích xuất thông tin nhận dạng vĩnh viễn
304
Mỗi thiết bị thuê bao truy cập mạng gia đình qua mạng tạm trú sử dụng thông tin nhận dạng vĩnh viễn được che giấu bao gồm thông tin nhận dạng khóa và thông tin nhận dạng thực thể quản lý bảo mật

FIG. 3

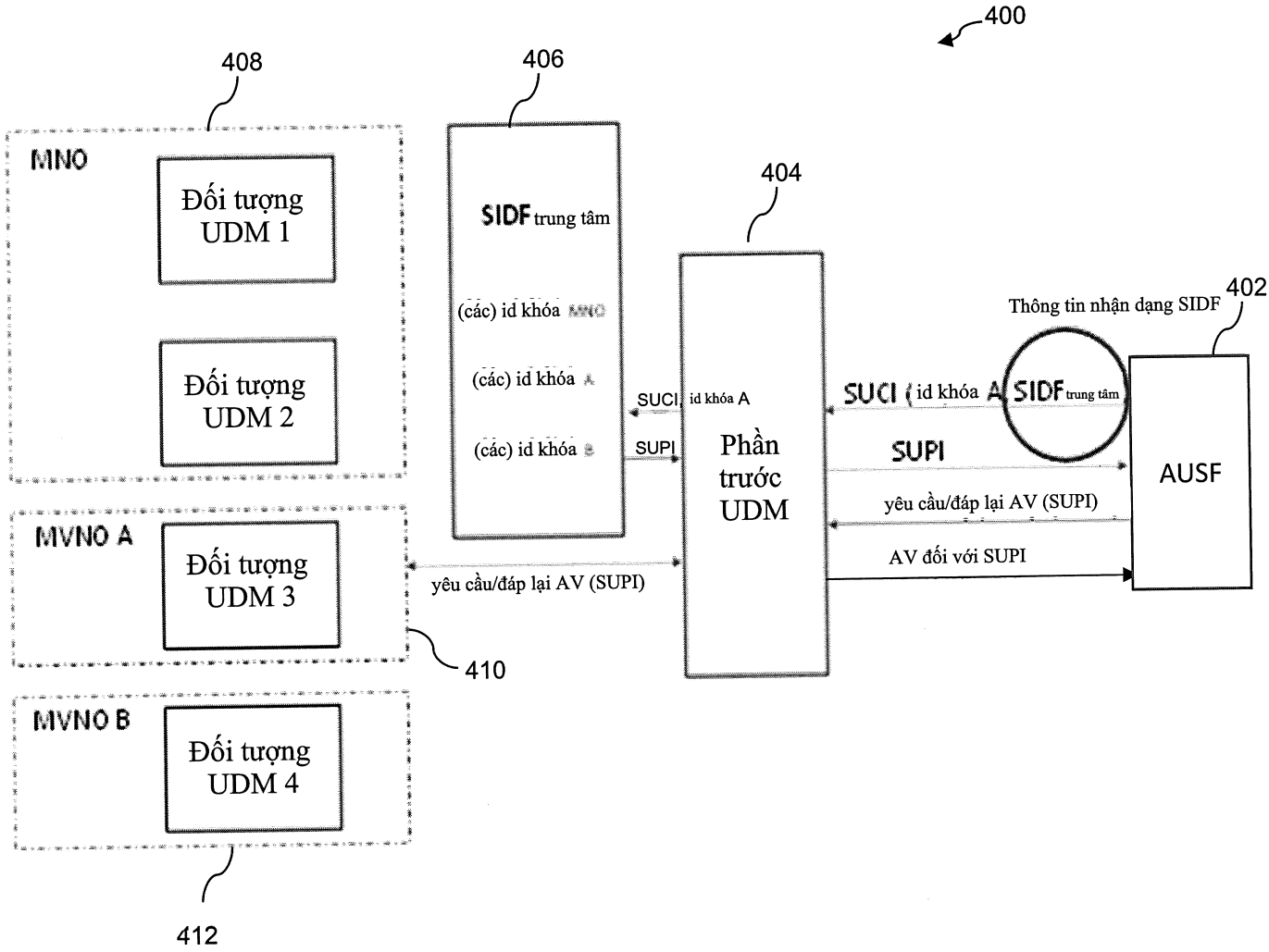

400
408
406
MNO
Đối tượng UDM 1
Đối tượng UDM 2
SIDF trung tâm
(các) id khóa MNO
(các) id khóa A
(các) id khóa B
404
Thông tin nhận dạng SIDF
402
SUCI, id khóa A
SUPI
Phần trước UDM
SUCI (id khóa A, SIDF trung tâm)
SUPI
yêu cầu/đáp lại AV (SUPI)
AV đối với SUPI
AUSF
MVNO A
Đối tượng UDM 3
yêu cầu/đáp lại AV (SUPI)
410
MVNO B
Đối tượng UDM 4
412

FIG. 4

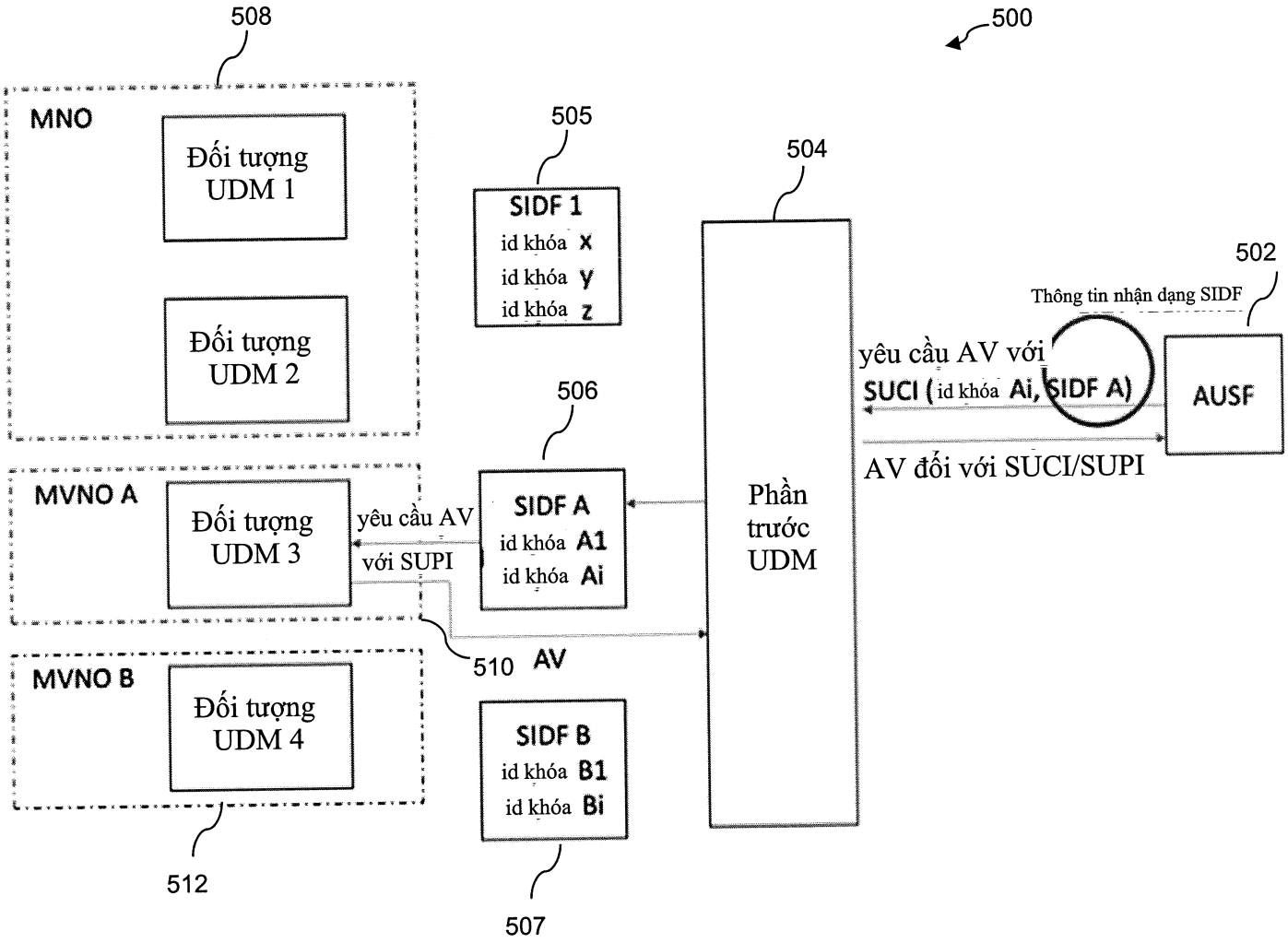

508
500
MNO
Đối tượng UDM 1
Đối tượng UDM 2
505
SIDF 1
id khóa x
id khóa y
id khóa z
504
502
Thông tin nhận dạng SIDF
yêu cầu AV với
SUCI (id khóa Ai, SIDF A)
AUSF
AV đối với SUCI/SUPI
506
MVNO A
Đối tượng UDM 3
yêu cầu AV
với SUPI
SIDF A
id khóa A1
id khóa Ai
Phần trước UDM
510
AV
MVNO B
Đối tượng UDM 4
SIDF B
id khóa B1
id khóa Bi
512
507

FIG. 5