(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) **1-0036626**

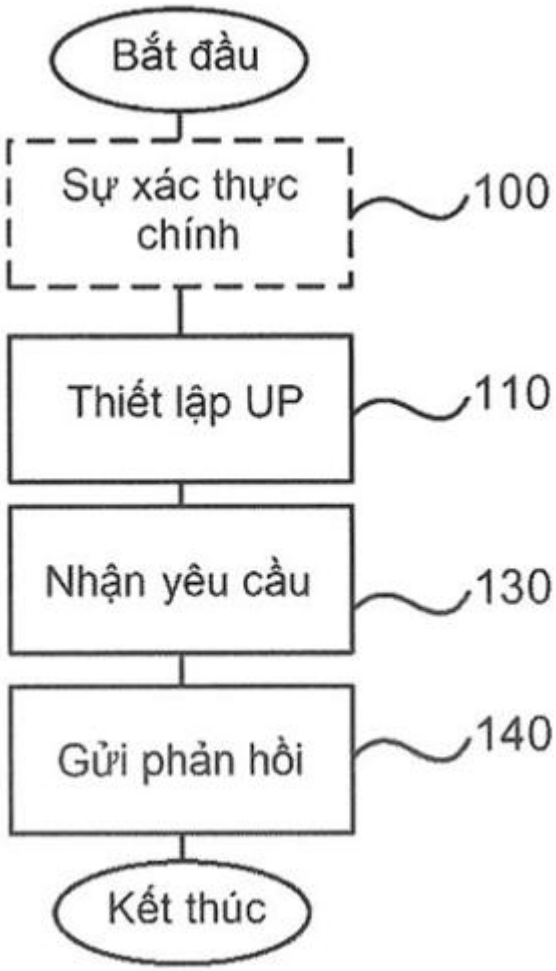
(51)[8] **H04W 12/06**; H04L 29/06

(13) **B**

(21) 1-2019-02794
(22) 25/10/2017
(86) PCT/EP2017/077330 25/10/2017
(87) WO2018/077960 03/05/2018
(30) 62/415,006 31/10/2016 US
(45) 25/08/2023 425
(43) 26/08/2019 377A
(73) TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (SE)
SE-164 83 Stockholm, Sweden
(72) BEN HENDA, Noamen (SE); LEHTOVIRTA, Vesa (FI); CASTELLANOS ZAMORA, David (ES).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP ĐỂ XÁC THỰC PHỤ, THIẾT BỊ NGƯỜI DÙNG VÀ THIẾT BỊ CHỨC NĂNG MẶT PHẲNG NGƯỜI DÙNG ĐỂ HOẠT ĐỘNG TRONG MẠNG

(57) Sáng chế đề xuất các phương pháp và thiết bị để xác thực phụ trong mạng. Phương pháp được thực hiện bởi thiết bị người dùng (user equipment (UE)) bao gồm thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP (UP function (UPF)), nhận yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ UPF và gửi phản hồi xác thực dựa trên EAP đến UPF. Phương pháp được thực hiện bởi thiết bị chức năng mặt phẳng người dùng (user plane UP function (UPF)) bao gồm thiết lập phiên hoặc kết nối UP đối với thiết bị người dùng (user equipment (UE)), gửi yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE, và nhận phản hồi xác thực dựa trên EAP từ UE.


Bắt đầu
Sự xác thực chính
100
Thiết lập UP
110
Nhận yêu cầu
130
Gửi phản hồi
140
Kết thúc

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp và thiết bị để xác thực phụ trong mạng.

Tình trạng kỹ thuật của sáng chế

Dự án đối tác thế hệ thứ ba (3rd Generation Partnership Project (3GPP)) hiện đang phát triển các chuẩn cho 5G, cũng được biết đến như các hệ thống thế hệ tiếp theo (next generation (NG)). Có dự tính là 5G sẽ hỗ trợ nhiều tình huống và trường hợp sử dụng mới và sẽ là phần tử tạo ra khả năng cho Internet vạn vật (Internet of things (IoT)). Có dự tính là các hệ thống NG sẽ cung cấp khả năng kết nối cho khoảng rộng của các thiết bị mới như các cảm biến, các thiết bị mang được thông minh, phương tiện giao thông, máy, v.v.. Tính linh hoạt theo đó là đặc tính chính trong các hệ thống NG. Điều này được phản ánh trong yêu cầu an toàn cho truy nhập mạng mà đang ủy thác cho sự hỗ trợ của các phương pháp xác thực thay thế và các loại khác nhau của các giấy ủy nhiệm (credential), được so sánh với các giấy ủy nhiệm thỏa thuận chính và xác thực (authentication and key agreement (AKA)) thông thường được cung cấp trước bởi nhà điều hành và được lưu trữ theo cách an toàn trong thẻ mạch tích hợp toàn cầu (universal integrated circuit card (UICC)). Điều này sẽ cho phép các chủ nhà máy hoặc các doanh nghiệp tác dụng đòn bẩy đối với các hệ thống quản lý giấy ủy nhiệm và nhận dạng của chính họ cho sự an toàn mạng truy nhập và xác thực.

Trong số các dấu hiệu mới trong các hệ thống NG có khái niệm về tạo lát mạng. Lát mạng (network slice (NS)) về cơ bản là thực thể của mạng lõi được dành riêng để cung cấp dịch vụ riêng. Điều này sẽ cho phép các nhà điều hành thao tác sự đa dạng rộng của các trường hợp sử dụng mới, mỗi trường hợp với các yêu cầu dịch vụ khác nhau liên quan tới Chất lượng của dịch vụ (Quality of Service (QoS)). Ví dụ, nhà điều hành có thể đang chạy NS cho các dịch vụ băng rộng di động (mobile broadband (MBB)) thông thường, song song với NS tới hạn nhiệm vụ cho các dịch vụ an toàn

công cộng (như ấn nút để nói tới hạn nhiệm vụ (Mission-critical push-to-talk (MCPTT))) yêu cầu độ chờ rất thấp, còn song song với IoT NS cho các đồng hồ đo điện với băng thông rất thấp.

Trong số các chủ đề đang được nghiên cứu liên quan đến Tạo lát mạng (Network Slicing) có sự tách của các thủ tục xác thực và cấp phép để truy nhập các NS khác nhau.

Bản chất kỹ thuật của sáng chế

Mục đích của các phương án được trình bày ở đây nhằm làm cho có khả năng tách sự xác thực trong các hệ thống thế hệ tiếp theo.

Theo khía cạnh thứ nhất, phương pháp để xác thực phụ trong mạng được đề xuất. Phương pháp được thực hiện bởi thiết bị người dùng (user equipment (UE)), và bao gồm thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP (UP function (UPF)), nhận yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ UPF và gửi phản hồi xác thực dựa trên EAP đến UPF.

Phương pháp có thể còn bao gồm thiết lập sự xác thực chính với chức năng neo an toàn (security anchor function (SEAF)).

Phương pháp có thể còn bao gồm nhận kết quả xác thực dựa trên EAP từ UPF.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ hai, phương pháp để xác thực phụ trong mạng được đề xuất. Phương pháp được thực hiện bởi thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)), và bao gồm thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị người dùng (user equipment (UE)), gửi yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE, và nhận phản hồi xác thực dựa trên EAP từ UE.

Phương pháp có thể còn bao gồm gửi yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)), và nhận phản hồi xác nhận từ máy chủ AAA.

Phương pháp có thể còn bao gồm gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ ba, thiết bị người dùng (user equipment (UE)) để hoạt động trong mạng được đề xuất. UE bao gồm bộ xử lý, và sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho UE thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP (UP function (UPF)), nhận yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ UPF, và gửi phản hồi xác thực dựa trên EAP đến UPF.

UE có thể còn được làm cho thiết lập sự xác thực chính với chức năng neo an toàn (security anchor function (SEAF)).

UE có thể còn được làm cho nhận kết quả xác thực dựa trên EAP từ UPF.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ tư, thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)) hoạt động trong mạng được đề xuất. UPF bao gồm bộ xử lý, và sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho UPF thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị người dùng (user equipment (UE)), gửi yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible

authentication protocol (EAP)) đến UE và nhận phản hồi xác thực dựa trên EAP từ UE.

UPF có thể còn được làm cho gửi yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)), và nhận phản hồi xác nhận từ máy chủ AAA.

UPF có thể còn được làm cho gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ năm, thiết bị người dùng (user equipment (UE)) để hoạt động trong mạng được đề xuất. UE bao gồm phương tiện để thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP (UP function (UPF)), phương tiện nhận yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ UPF, và phương tiện để gửi phản hồi xác thực dựa trên EAP đến UPF.

UE có thể còn bao gồm phương tiện để thiết lập sự xác thực chính với chức năng neo an toàn (security anchor function (SEAF)).

UE có thể còn bao gồm phương tiện để nhận kết quả xác thực dựa trên EAP từ UPF.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ sáu, thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)) hoạt động trong mạng được đề xuất. UPF bao gồm phương tiện để thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị người dùng (user equipment (UE)), phương tiện để gửi yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE, và phương tiện để nhận phản hồi xác thực dựa trên EAP từ UE.

UPF có thể còn bao gồm phương tiện để gửi yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)); và phương tiện để nhận phản hồi xác nhận từ máy chủ AAA.

UPF có thể còn bao gồm phương tiện để gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ bảy, chương trình máy tính để xác thực phụ trong mạng được đề xuất. Chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên thiết bị người dùng (user equipment (UE)), làm cho UE thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP (UP function (UPF)), nhận yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ UPF, và gửi phản hồi xác thực dựa trên EAP đến UPF.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ tám, chương trình máy tính để xác thực phụ trong mạng được đề xuất. Chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)), làm cho UPF thiết lập phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị người dùng (user equipment (UE)), gửi yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE, và nhận phản hồi xác thực dựa trên EAP từ UE.

UE còn có thể là UE thế hệ tiếp theo (next generation (NG)). UPF còn có thể là NG UPF.

Theo khía cạnh thứ chín, sản phẩm chương trình máy tính được đề xuất. Sản phẩm chương trình máy tính bao gồm chương trình máy tính và phương tiện lưu trữ đọc được bởi máy tính mà trên đó chương trình máy tính được lưu trữ. Nói chung, tất cả các thuật ngữ được sử dụng trong các điểm yêu cầu bảo hộ là để được diễn dịch theo ý nghĩa thông thường của chúng trong lĩnh vực kỹ thuật, trừ khi được định nghĩa rõ ràng theo cách khác ở đây. Tất cả các tham chiếu đến "phần tử, thiết bị, thành phần, phương tiện, bước, v.v." là để được diễn dịch theo cách mở như tham chiếu đến ít nhất một thực thể của phần tử, thiết bị, thành phần, phương tiện, bước, v.v., trừ khi được nêu rõ ràng theo cách khác. Các bước của phương pháp bất kỳ được bộc lộ ở đây không cần phải được thực hiện theo thứ tự chính xác được bộc lộ, trừ khi được nêu rõ ràng.

Mô tả vắn tắt các hình vẽ kèm theo

Khái niệm sáng chế sau đây được mô tả, theo cách ví dụ, có tham chiếu đến các hình vẽ kèm theo, trong đó:

Fig.1 là sơ đồ giản lược minh họa môi trường trong đó các phương án được trình bày ở đây có thể được áp dụng;

Fig.2 là hình vẽ thể hiện giản lược tiến trình để xác thực phụ trong LTE;

Fig.3 là hình vẽ thể hiện giản lược tiến trình để xác thực phụ dựa trên EAP trong các hệ thống thế hệ tiếp theo;

Fig.4-Fig.5 là các hình vẽ thể hiện giản lược các kiến trúc giao thức để xác thực phụ dựa trên EAP cho các phương án được trình bày ở đây;

Fig.6A-Fig.6B là các biểu đồ tiến trình minh họa các phương pháp cho các phương án được trình bày ở đây;

Fig.7-Fig.8 là các sơ đồ giản lược minh họa một số thành phần của các thiết bị được trình bày ở đây; và

Fig.9-Fig.10 là các sơ đồ giản lược thể hiện các môđun chức năng của các thiết bị được trình bày ở đây.

Mô tả chi tiết sáng chế

Khái niệm sáng chế sau đây sẽ được mô tả đầy đủ hơn sau đây có tham chiếu đến các hình vẽ kèm theo, trong đó các phương án nhất định của khái niệm theo sáng chế được thể hiện. Tuy nhiên, khái niệm theo sáng chế này có thể được biểu hiện trong nhiều dạng khác nhau và không được hiểu là bị giới hạn vào các phương án được đưa ra ở đây; đúng hơn là, các phương án này được cung cấp theo cách ví dụ sao cho sáng chế sẽ thấu đáo và toàn diện, và sẽ chuyển tải đầy đủ phạm vi của khái niệm theo sáng chế đến những người có hiểu biết trung bình trong lĩnh vực. Các số chỉ dẫn giống nhau tham chiếu đến các phần tử giống nhau trong toàn bộ phần mô tả.

Một tình huống có thể có để tách các thủ tục xác thực và cấp phép để truy nhập các lát mạng (network slice (NS)) khác nhau là như sau. Để cho thiết bị người dùng thế hệ tiếp theo (NG-user equipment (UE)) truy nhập NS riêng, nhà điều hành trước tiên sẽ chạy sự xác thực chính (thông thường) cho truy nhập mạng ban đầu được theo sau bởi sự xác thực đặc trưng cho NS phụ. Có thể là sự xác thực đặc trưng cho NS phụ có thể dưới sự điều khiển của bên thứ ba. Ở đây đang giả định sự tin cậy giữa nhà cung cấp dịch vụ bên thứ ba và nhà vận hành mạng di động (mobile network operator (MNO)) mà ví dụ đang đưa ra các dịch vụ truy nhập và vận chuyển cho bên thứ ba này trong thực thể NS được dành riêng.

Trong sự cải tiến dài hạn (long term evolution (LTE)), có cơ chế mà có thể có liên quan đến tình huống được mô tả. Cơ chế này được mô tả trong điều khoản 5.3.2 từ TS 23.401. Nó được dựa trên yêu cầu được gọi là yêu cầu tùy chọn được mật mã hóa và sử dụng phần tử thông tin được gọi là các tùy chọn tạo kết cấu giao thức (protocol configuration option (PCO)).

PCO là một trong các phần tử thông tin trong các tin nhắn tầng không truy nhập (non-access stratum (NAS)). PCO có thể được sử dụng trong một vài loại của các tin nhắn như yêu cầu khả năng kết nối mạng dữ liệu gói (packet mạng dữ liệu (PDN)) để

gửi thông tin theo cách trong suốt qua Thực thể quản lý tính di động (Mobility Management Entity (MME)) và cổng nối phục vụ (serving gateway (S-GW)) đến PDN-GW. Ví dụ, PCO có thể bao gồm sự ưu tiên cấp phát địa chỉ chỉ thị là UE ưu tiên để thu được địa chỉ phiên bản giao thức Internet 4 (Internet protocol version 4 (IPv4)) chỉ sau sự kích hoạt phần tử mang (bearer) mặc định bằng phiên bản giao thức tạo kết cấu máy chủ động bốn (dynamic host configuration protocol version four (DHCPv4)).

Một trường hợp sử dụng của PCO là sự chuyển tải của các tên người dùng và mật khẩu của giao thức xác thực mật khẩu (password authentication protocol (PAP)) và giao thức xác thực bắt tay thử thách (challenge handshake authentication protocol (CHAP)) đến PDN-GW, mà tiếp đó chạy chúng qua máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) để xác thực truy nhập. Máy chủ AAA có thể được đặt trong miền ngoài. Do các tên người dùng và mật khẩu là nhạy cảm và cần được bảo vệ, nếu UE dự định gửi PCO mà yêu cầu mật mã hóa (ví dụ, các tên người dùng và mật khẩu PAP/CHAP), UE sẽ thiết đặt cờ chuyển tải các tùy chọn được mật mã hóa trong tin nhắn yêu cầu gắn và gửi PCO chỉ sau khi sự thiết đặt an toàn NAS và xác thực đã được hoàn thành.

Fig.2 thể hiện tiến trình tin nhắn được yêu cầu để chạy thủ tục xác thực bổ sung (nghĩa là phụ) như vậy qua PDN-GW trong LTE. Trong phần sau đây, mô tả chi tiết hơn về các bước trong đó được cung cấp.

UE nằm trong miền UE. MME, S-GW, máy chủ thuê bao gia đình (home subscriber server (HSS)), và PDN-GW nằm trong miền MNO. Máy chủ AAA nằm trong miền bên thứ ba.

Trong bước 1 UE gửi tin nhắn yêu cầu gắn với tập hợp cờ chuyển tải các tùy chọn được mật mã hóa đến MME.

Trong bước 2 thủ tục thỏa thuận chính và xác thực (authentication and key agreement (AKA)) được chạy giữa UE và HSS. Vào lúc xác thực thành công các bước tiếp theo được thực thi.

Trong bước 3 sự an toàn NAS được cài đặt, sử dụng lệnh chế độ an toàn (secure mode command (SMC)). Sau khi sự an toàn NAS đã được cài đặt, tất cả các tin nhắn NAS được bảo vệ tính bảo mật và tính toàn vẹn.

Trong bước 4 MME gửi tin nhắn yêu cầu các tùy chọn được mật mã hóa đến UE cho sự lấy lại của PCO.

Trong bước 5 UE trả lời với tin nhắn phản hồi các tùy chọn được mật mã hóa bao gồm tên người dùng và mật khẩu PAP/CHAP trong phần tử thông tin PCO. Trong trường hợp UE có các sự thuê bao đối với nhiều PDN, thì UE cũng bao gồm tên điểm truy nhập (access point name (APN)) trong tin nhắn.

Trong bước 6 MME giải mật mã dữ liệu được nhận, sử dụng APN được cung cấp có thể có để nhận dạng PDN-GW, và chuyển tiếp PCO qua S-GW đến PDN-GW đích trong tin nhắn yêu cầu tạo ra phiên (create session request message).

Trong bước 7 PDN-GW gửi thông tin PAP/CHAP được nhận trong tin nhắn yêu cầu truy nhập đường kính/bán kính đến máy chủ AAA ngoài. Vào lúc thành công, thủ tục tạo ra phiên tiếp diễn như thường lệ.

Các bước 4-7 trên theo đó biểu diễn sự xác thực phụ, được thực hiện sau khi sự xác thực thứ nhất trong bước 2 đã được hoàn thành. Tuy nhiên, để sử dụng cơ chế này trong hoặc sự mở rộng vào trong các hệ thống NG sẽ cung cấp một số nhược điểm.

Trước tiên, cơ chế rất bị giới hạn liên quan tới các phương pháp xác thực có thể có. Hiện thời chỉ có sự hỗ trợ cho PAP và CHAP. Nhưng do PAP ngày nay đã lỗi thời từ quan điểm về tính an toàn, chỉ có CHAP về cơ bản là có thể sử dụng.

Thứ hai, để hỗ trợ các phương pháp khác và sử dụng phần tử thông tin PCO cho sự vận chuyển của thông tin xác thực, cơ chế sẽ được yêu cầu chỉ rõ các tin nhắn đặc biệt giữa MME và S-GW và S-GW và PDN-GW được dành riêng cho mục đích này. Nghĩa là để thao tác các phương pháp xác thực mà yêu cầu nhiều hơn chỉ một chuyến đi và về.

Hơn nữa, khó khăn để thấy được cách thức cơ chế này sẽ khớp với kiến trúc NG, mà sắp được phân nhỏ thêm nữa. Trên thực tế, xem xét đến các dấu hiệu kiến trúc mới (TR 23.799), có khả năng sẽ có nhiều bước nhảy trong đường giữa UE và PDN-GW, ví dụ liên quan đến công việc đang tiến hành về tách MME thành chức năng quản lý tính di động (mobility management function (MMF) và chức năng quản lý phiên (session management function SMF) (TR 23.799) và công việc tách riêng mặt phẳng người dùng và điều khiển (control and user plane separation (CUPS)) cho sự tách mặt phẳng người dùng và điều khiển (TR 23.714). Điều này bao hàm nhiều sự quá tải và báo hiệu hơn trong mạng lõi (core network (CN)).

Cuối cùng, cơ chế này là giải pháp thay thế bởi vì không có giao thức trực tiếp giữa UE và PDN-GW. Việc làm cho nó đủ chung để hỗ trợ các phương pháp xác thực khác sẽ là thử thách về mặt kỹ thuật, đặc biệt là do nhiều phương pháp có các khuyến nghị và yêu cầu chặt chẽ trên lớp vận chuyển.

Việc chạy sự xác thực phụ trên mặt phẳng người dùng (user plane (UP)), một khi nó được cài đặt được trình bày. Phiên UP được giới hạn có thể được chạy cho thủ tục xác thực phụ, hơn là cho phép truy nhập đầy đủ đối với PDN. Một khi sự xác thực phụ được hoàn thành, phiên UP được giới hạn có thể được nâng cấp thành một phiên có truy nhập đầy đủ đối với mạng dữ liệu. Sự sử dụng giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)), như được định nghĩa trong RFC3748, cũng được trình bày. EAP được sử dụng để xác thực giữa UE và máy chủ AAA ngoài có tiềm năng, trong đó thiết bị chức năng UP thế hệ tiếp theo (NG-UP function (UPF)), đóng vai trò tương tự như nó của PDN-GW trong LTE, chứng thực (endorse) vai trò của bộ xác thực EAP. Các tải EAP sẽ được mang bởi giao thức để mang sự xác thực cho truy nhập mạng (protocol for carrying authentication for network access (PANA)), như được định nghĩa trong RFC5191, giao thức mà được dựa trên IP. Một phương án thay thế khác là NG-UPF chứng thực vai trò của máy chủ EAP.

Giải pháp được trình bày sử dụng EAP mà được sử dụng rộng rãi và cung cấp hỗ trợ cho nhiều phương pháp xác thực như EAP-sự an toàn lớp vận chuyển (transport layer security (TLS)), EAP-thỏa thuận chính và xác thực (authentication and key

agreement (AKA)), EAP-TLS được tạo hầm (tunneled TLS (TTLS)) và EAP-giao thức xác thực có thể mở rộng được bảo vệ (protected extensible authentication protocol (PEAP)). Giải pháp được trình bày dựa trên IP và theo đó là không thể biết đối với loại của mạng truy nhập (access network (AN)). Thêm nữa, do nó được dựa trên UP, sự xác thực phụ có thể được thực hiện theo cách độc lập trên cơ sở đặc trưng cho NS ngay cả đối với các tình huống trong đó NG-UE hỗ trợ nhiều khả năng kết nối NS đồng thời có thể. Nhờ sử dụng EAP, giải pháp cũng hỗ trợ các loại khác nhau của các giấy ủy nhiệm và các phương pháp xác thực. Sự trao đổi EAP có thể có lợi từ sự bảo vệ qua giao diện không khí.

Sự xác thực phụ theo đó là sự chạy của các phần tử mang UP một khi NG-UE được cấp phát địa chỉ IP. EAP tiếp đó được sử dụng để xác thực giữa NG-UE và máy chủ AAA (ngoài có tiềm năng) trong đó NG-UPF chứng thực vai trò của bộ xác thực EAP.

Phương án trong đó NG-UPF hành động như bộ xác thực EAP được trình bày với tham chiếu đến Fig.3.

Fig.3 thể hiện tiến trình trong đó sự xác thực phụ dựa trên UP được chạy với máy chủ AAA ngoài. NG-UE ở trong miền UE. Chức năng quản lý tính di động thế hệ tiếp theo (NG mobility management function (MMF)), chức năng quản lý phiên thế hệ tiếp theo (NG session management function (SMF)), chức năng neo an toàn thế hệ tiếp theo (NG security anchor function (SEAF)) và NG-UPF ở trong miền MNO. NG-UPF là UPF tương ứng với PDN-GW trong LTE. Máy chủ AAA ở trong miền bên thứ ba. Các yêu cầu về NG-UPF là để bao gồm hỗ trợ của PANA và EAP, có thể ngoài sự hỗ trợ của tất cả các dấu hiệu UP cần thiết của PDN-GW trong LTE như sự hỗ trợ của giao diện SGi. Nói chung, tiền tố-NG được sử dụng cho chức năng hệ thống NG tương ứng với các khái niệm LTE.

Trong bước 1 NG-UE gửi yêu cầu gắn khởi đầu thủ tục gắn. Giải pháp được trình bày ở đây không phụ thuộc vào cách thức sự tạo lát mạng được hỗ trợ, ví dụ cách thức các thực thể NS được lựa chọn và cách thức NG-UE được hướng đến những cái thích hợp.

Trong bước 2 NG-UE chạy sự xác thực chính với NG SEAF. NG SEAF có thể còn được kết nối với chức năng máy chủ xác thực thế hệ tiếp theo (NG authentication server function (AUSF)). Sự xác thực phụ, sau này không phụ thuộc vào cách thức NG SEAF và NG MMF được triển khai (nghĩa là được sắp xếp vào cùng một chỗ hoặc tách) cũng không phụ thuộc vào địa điểm của NG SEAF (mạng di động mặt đất công cộng (public land mobile network (PLMN)) gia đình hoặc được thăm).

Trong bước 3 sự an toàn mặt phẳng điều khiển được thiết lập giữa NG-UE và điểm cuối của NG NAS. Điểm cuối của NG NAS có thể ví dụ là NG MMF hoặc NG SMF.

Trong bước 4 phiên đơn vị dữ liệu giao thức (protocol data unit (PDU)) sau đó được thiết lập cho sự vận chuyển của dữ liệu UP giữa NG-UE và mạng dữ liệu thông qua NG-UPF. Bước 4 có thể là phiên được giới hạn chỉ cho phép chạy thủ tục xác thực phụ. Sự xác thực phụ, sau này phụ thuộc vào UP được cài đặt, do nó thiết lập khả năng kết nối IP giữa NG-UE và NG-UPF.

Trong bước 5 sự xác thực dựa trên EAP phụ được chạy giữa NG-UE và NG-UPF, ở đây chứng thực vai trò của bộ xác thực EAP và dựa vào máy chủ AAA ngoài phía sau. NG-UE sau đó được cấp truy nhập trong mạng dữ liệu dựa trên kết quả của thủ tục xác thực này.

Giải pháp được trình bày này là không thể biết về cách thức truy nhập không phải 3GPP sẽ được tích hợp và liệu các bước 1 đến 3 được thực thi theo cách chính xác như được miêu tả ở đây hoặc theo cách khác. Miễn là khả năng kết nối IP được thiết lập giữa NG-UE và NG-UPF, mà đạt được trong bước 4, thì sự xác thực dựa trên EAP có thể được chạy trong bước 5. Trong trường hợp sự an toàn mạng truy nhập radio (radio access network (RAN)) đã được thiết lập trước bước 5, thì sự trao đổi EAP cũng sẽ được bảo vệ trên giao diện không khí.

Fig.4 thể hiện kiến trúc giao thức cho sự xác thực phụ dựa trên EAP, giữa NG-UPF và NG-UE với NG-UPF như bộ xác thực EAP, như được mô tả với tham chiếu đến Fig.3. Kiến trúc được thể hiện trên Fig.4 tương tự với kiến trúc của LTE liên quan

đến sự vận chuyển của lưu lượng UP giữa UE và PDN-GW. Các ô được tô màu xám nêu bật các lớp giao thức bổ sung được yêu cầu để cung cấp sự xác thực phụ dựa trên EAP được mô tả trên đây.

Phương án với kiến trúc giao thức để xác thực phụ dựa trên EAP với NG-UPF như máy chủ EAP được trình bày với tham chiếu đến Fig.5.

Theo phương án này NG-UPF kết thúc sự trao đổi EAP và chứng thực vai trò của máy chủ EAP hoàn chỉnh. Tiến trình tin nhắn cho phương án này theo đó tương tự với tiến trình tin nhắn trên Fig.3, ngoại trừ là trong bước 5 máy chủ AAA ngoài không được tiếp xúc.

Cơ chế để xác thực bổ sung hoặc phụ trong các hệ thống NG giữa NG-UE và NG-UPF kết thúc lưu lượng UP trong mạng lõi và có thể tương tác với máy chủ AAA ngoài đã được trình bày. NG-UPF tương ứng với PDN-GW trong LTE. Cơ chế được dựa trên EAP qua IP qua lưu lượng UP sao cho NG-UPF chứng thực vai trò bộ xác thực EAP hoặc vai trò máy chủ EAP.

Mạng truyền thông 4, trong đó các phương án được mô tả ở đây có thể được thực hiện được trình bày trên Fig.1. Thiết bị người dùng (user equipment (UE)) 1 có thể kết nối được theo cách không dây với trạm cơ sở (base station (BS)) 2. BS 2 được kết nối với mạng lõi (core network (CN)) 3.

Phương pháp, theo phương án, để xác thực phụ trong mạng được trình bày với tham chiếu đến Fig.6A. Phương pháp được thực hiện bởi thiết bị người dùng thế hệ tiếp theo (next generation (NG) user equipment (UE)), và bao gồm thiết lập 110 phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP thế hệ tiếp theo (NG-UP function (UPF)), nhận 130 yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ NG-UPF, và gửi 140 phản hồi xác thực dựa trên EAP đến NG-UPF.

Phương pháp có thể còn bao gồm thiết lập 100 sự xác thực chính với NG SEAF.

Phương pháp có thể còn bao gồm nhận kết quả xác thực dựa trên EAP từ UPF.

Phương pháp, theo phương án, để xác thực phụ trong mạng lõi được trình bày với tham chiếu đến Fig.6B. Phương pháp được thực hiện bởi thiết bị chức năng mặt phẳng người dùng thế hệ tiếp theo (next generation (NG)-user plane (UP) function (UPF)), và bao gồm thiết lập 110 phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị người dùng thế hệ tiếp theo (NG user equipment (UE)), gửi 120 yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến NG UE, và nhận 150 phản hồi xác thực dựa trên EAP từ NG UE.

Phương pháp có thể còn bao gồm gửi 160 yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)), và nhận 170 phản hồi xác nhận từ máy chủ AAA.

Phương pháp có thể còn bao gồm gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

NG UE, theo phương án, để hoạt động trong mạng được trình bày với tham chiếu đến Fig.7. NG UE 1 bao gồm bộ xử lý 10, và sản phẩm chương trình máy tính 12, 13. Sản phẩm chương trình máy tính lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho NG UE thiết lập 110 phiên hoặc kết nối UP với NG-UPF, nhận 130 yêu cầu xác thực dựa trên EAP từ NG-UPF, và gửi 140 phản hồi xác thực dựa trên EAP đến NG-UPF.

NG-UPF theo phương án, hoạt động trong mạng lõi được trình bày với tham chiếu đến Fig.8. NG-UPF bao gồm bộ xử lý 10, và sản phẩm chương trình máy tính 12, 13 lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho NG-UPF thiết lập 110 phiên hoặc kết nối UP đối với NG UE, gửi 120 yêu cầu xác thực dựa trên EAP đến NG UE, và nhận 150 phản hồi xác thực dựa trên EAP từ NG UE.

NG UE, theo phương án, để hoạt động trong mạng, được trình bày với tham chiếu đến Fig.9. NG UE bao gồm bộ quản lý truyền thông 61 để thiết lập 110 phiên

hoặc kết nối UP với NG-UPF, nhận 130 yêu cầu xác thực dựa trên EAP từ NG-UPF, và để gửi 140 phản hồi xác thực dựa trên EAP đến NG-UPF.

NG-UPF, theo phương án, hoạt động trong mạng được trình bày với tham chiếu đến Fig.10. NG-UPF bao gồm bộ quản lý truyền thông 71 để thiết lập 110 phiên hoặc kết nối UP với NG UE, gửi 120 yêu cầu xác thực dựa trên EAP đến NG UE, và để nhận 150 phản hồi xác thực dựa trên EAP từ NG UE.

Chương trình máy tính 14, 15, theo phương án, để xác thực phụ trong mạng được trình bày. Chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên NG UE, làm cho NG UE thiết lập 110 phiên hoặc kết nối UP với NG-UPF, nhận 130 yêu cầu xác thực dựa trên EAP từ NG-UPF, và gửi 140 phản hồi xác thực dựa trên EAP đến NG-UPF.

Chương trình máy tính 14, 15, theo phương án, để xác thực phụ trong mạng được trình bày. Chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên NG-UPF, làm cho NG-UPF thiết lập 110 phiên hoặc kết nối UP với NG UE, gửi 120 yêu cầu xác thực dựa trên EAP đến NG UE, và nhận 150 phản hồi xác thực dựa trên EAP từ NG UE.

Sản phẩm chương trình máy tính 12, 13, theo phương án, được trình bày. Sản phẩm chương trình máy tính bao gồm chương trình máy tính 14, 15 như được trình bày trên đây và phương tiện lưu trữ đọc được bởi máy tính mà trên đó chương trình máy tính 14, 15 được lưu trữ.

Fig.7 là sơ đồ giản lược thể hiện một số thành phần của NG UE 1. Bộ xử lý 10 có thể được cung cấp sử dụng sự kết hợp bất kỳ của một hoặc nhiều trong bộ phận xử lý trung tâm (central processing unit (CPU)), bộ đa xử lý, bộ vi điều khiển, bộ xử lý tín hiệu số (digital signal processor (DSP)), mạch tích hợp đặc trưng cho ứng dụng thích hợp v.v., có khả năng thực thi các lệnh phần mềm của chương trình máy tính 14 được lưu trữ trong bộ nhớ. Bộ nhớ có thể theo đó được xem là hoặc tạo thành một phần của sản phẩm chương trình máy tính 12. Bộ xử lý 10 có thể được tạo kết cấu để thực thi các phương pháp được mô tả ở đây với tham chiếu đến Fig.12 và Fig.13.

Bộ nhớ có thể là sự kết hợp bất kỳ của bộ nhớ đọc và ghi và bộ nhớ chỉ đọc (read only memory (ROM)). Bộ nhớ cũng có thể bao gồm bộ lưu trữ bền vững, mà, ví dụ, có thể là một bộ nhớ đơn bất kỳ hoặc sự kết hợp của bộ nhớ từ tính, bộ nhớ quang, bộ nhớ thể rắn hoặc thậm chí bộ nhớ được lắp từ xa.

Sản phẩm chương trình máy tính thứ hai 13 dưới dạng bộ nhớ dữ liệu cũng có thể được cung cấp, ví dụ để đọc và/hoặc lưu trữ dữ liệu trong khi thực thi các lệnh phần mềm trong bộ xử lý 10. Bộ nhớ dữ liệu có thể là sự kết hợp bất kỳ của bộ nhớ đọc và ghi và bộ nhớ chỉ đọc (read only memory (ROM)), và cũng có thể bao gồm bộ lưu trữ bền vững, mà, ví dụ, có thể là một bộ nhớ đơn bất kỳ hoặc sự kết hợp của bộ nhớ từ tính, bộ nhớ quang, bộ nhớ thể rắn hoặc thậm chí bộ nhớ được lắp từ xa. Bộ nhớ dữ liệu có thể ví dụ giữ các lệnh phần mềm 15 khác, để cải thiện chức năng cho NG UE 1.

NG UE 1 có thể còn bao gồm giao diện đầu vào/đầu ra (input/output (I/O)) 11 bao gồm ví dụ giao diện người dùng. NG UE 1 có thể còn bao gồm bộ nhận được tạo kết cấu để nhận báo hiệu từ các nút khác, và bộ truyền được tạo kết cấu để truyền báo hiệu đến các nút khác (không được minh họa). Các thành phần khác của NG UE 1 được bỏ qua để không làm rối các khái niệm được trình bày ở đây.

Fig.9 là sơ đồ giản lược thể hiện các khối chức năng của NG UE 1. Các môđun có thể được thực hiện như chỉ các lệnh phần mềm như chương trình máy tính thực thi trong máy chủ cache hoặc chỉ phần cứng, như các mạch tích hợp đặc trưng cho ứng dụng, các mảng cổng lập trình được theo trường, các thành phần logic rời rạc, các bộ truyền nhận, v.v. hoặc như sự kết hợp của chúng. Theo phương án thay thế, một số trong các khối chức năng có thể được thực hiện bởi phần mềm và khối khác bởi phần cứng. Các môđun tương ứng với các bước trong phương pháp được minh họa trên Fig.6A, bao gồm bộ phận bộ quản lý truyền thông 61 và bộ phận môđun xác định 60. Theo các phương án trong đó một hoặc nhiều trong các môđun được thực hiện bởi chương trình máy tính, sẽ cần hiểu là các môđun này không nhất thiết tương ứng với các môđun quy trình, mà có thể được ghi như các lệnh theo ngôn ngữ lập trình trong

đó chúng sẽ được thực hiện, do một số ngôn ngữ lập trình đặc trưng là không chứa các môđun quy trình.

Bộ quản lý truyền thông 61 là để hoạt động trong mạng. Môđun này tương ứng với bước thiết lập UP 110, bước nhận yêu cầu 130 và bước gửi phản hồi 140 trên Fig.6A. Môđun này có thể ví dụ được thực hiện bởi bộ xử lý 10 trên Fig.7, khi chạy chương trình máy tính.

Bộ quản lý xác định 60 là để hoạt động trong mạng. Môđun này tương ứng với bước xác thực chính 100 trên Fig.6A. Môđun này có thể ví dụ được thực hiện bởi bộ xử lý 10 trên Fig.7, khi chạy chương trình máy tính.

Fig.8 là sơ đồ giản lược thể hiện một số thành phần của NG–UPF 3. Bộ xử lý 10 có thể được cung cấp sử dụng sự kết hợp bất kỳ của một hoặc nhiều trong bộ phận xử lý trung tâm (central processing unit (CPU)), bộ đa xử lý, bộ vi điều khiển, bộ xử lý tín hiệu số (digital signal processor (DSP)), mạch tích hợp đặc trưng cho ứng dụng thích hợp v.v., có khả năng thực thi các lệnh phần mềm của chương trình máy tính 14 được lưu trữ trong bộ nhớ. Bộ nhớ có thể theo đó được xem là hoặc tạo thành một phần của sản phẩm chương trình máy tính 12. Bộ xử lý 10 có thể được tạo kết cấu để thực thi các phương pháp được mô tả ở đây với tham chiếu đến Fig.6B.

Bộ nhớ có thể là sự kết hợp bất kỳ của bộ nhớ đọc và ghi, RAM, và bộ nhớ chỉ đọc (read only memory (ROM)). Bộ nhớ cũng có thể bao gồm bộ lưu trữ bền vững, mà, ví dụ, có thể là một bộ nhớ đơn bất kỳ hoặc sự kết hợp của bộ nhớ từ tính, bộ nhớ quang, bộ nhớ thể rắn hoặc thậm chí bộ nhớ được lắp từ xa.

Sản phẩm chương trình máy tính thứ hai 13 dưới dạng bộ nhớ dữ liệu cũng có thể được cung cấp, ví dụ để đọc và/hoặc lưu trữ dữ liệu trong khi thực thi các lệnh phần mềm trong bộ xử lý 10. Bộ nhớ dữ liệu có thể là sự kết hợp bất kỳ của bộ nhớ đọc và ghi, RAM, và bộ nhớ chỉ đọc (read only memory (ROM)), và cũng có thể bao gồm bộ lưu trữ bền vững, mà, ví dụ, có thể là một bộ nhớ đơn bất kỳ hoặc sự kết hợp của bộ nhớ từ tính, bộ nhớ quang, bộ nhớ thể rắn hoặc thậm chí bộ nhớ được lắp từ xa.

Bộ nhớ dữ liệu có thể ví dụ giữ các lệnh phần mềm 15 khác, để cải thiện chức năng cho NG-UPF 3.

NG-UPF 3 có thể còn bao gồm giao diện đầu vào/đầu ra (input/output (I/O)) 11 bao gồm ví dụ giao diện người dùng. NG-UPF 3 có thể còn bao gồm bộ nhận được tạo kết cấu để nhận báo hiệu từ các nút khác, và bộ truyền được tạo kết cấu để truyền báo hiệu đến các nút khác (không được minh họa). Các thành phần khác của NG-UPF 3 được bỏ qua để không làm rối các khái niệm được trình bày ở đây.

Fig.10 là sơ đồ giản lược thể hiện các khối chức năng của NG-UPF 3. Các môđun có thể được thực hiện như chỉ các lệnh phần mềm như chương trình máy tính thực thi trong máy chủ cache hoặc chỉ phần cứng, như các mạch tích hợp đặc trưng cho ứng dụng, các mảng cổng lập trình được theo trường, các thành phần logic rời rạc, các bộ truyền nhận, v.v. hoặc như sự kết hợp của chúng. Theo phương án thay thế, một số trong các khối chức năng có thể được thực hiện bởi phần mềm và khối khác bởi phần cứng. Các môđun tương ứng với các bước trong các phương pháp được minh họa trên Fig.6B, bao gồm bộ phận bộ quản lý truyền thông 71 và bộ phận bộ quản lý xác định 70. Theo các phương án trong đó một hoặc nhiều trong các môđun được thực hiện bởi chương trình máy tính, sẽ cần hiểu là các môđun này không nhất thiết tương ứng với các môđun quy trình, mà có thể được ghi như các lệnh theo ngôn ngữ lập trình trong đó chúng sẽ được thực hiện, do một số ngôn ngữ lập trình đặc trưng là không chứa các môđun quy trình.

Bộ quản lý truyền thông 71 là để hoạt động trong mạng lõi. Môđun này tương ứng với bước thiết lập UP 110, bước gửi yêu cầu 120, và bước nhận phản hồi 150 trên Fig.6B. Môđun này có thể ví dụ được thực hiện bởi bộ xử lý 10 trên Fig.8, khi chạy chương trình máy tính.

Bộ phận bộ quản lý xác định 70 là để hoạt động trong mạng lõi. Môđun này tương ứng với bước yêu cầu xác nhận 160 và bước phản hồi xác nhận 170 trên Fig.6B. Môđun này có thể ví dụ được thực hiện bởi bộ xử lý 10 trên Fig.8, khi chạy chương trình máy tính.

Khái niệm sáng chế đã chủ yếu được mô tả trên đây có tham chiếu đến một vài phương án. Tuy nhiên, như người có hiểu biết trung bình trong lĩnh vực dễ dàng hiểu rõ, các phương án khác với các phương án được bộc lộ trên đây là có thể thực hiện được ngang nhau nằm trong phạm vi của khái niệm theo sáng chế, như được định nghĩa bởi các điểm yêu cầu bảo hộ kèm theo.

Sau đây là các phương án được liệt kê nhất định minh họa thêm nữa các khía cạnh khác nhau của đối tượng được bộc lộ.

1. Phương pháp để xác thực phụ trong mạng, được thực hiện bởi thiết bị người dùng thế hệ tiếp theo (next generation (NG) user equipment (UE)), phương pháp này bao gồm các bước:

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP thế hệ tiếp theo (NG-UP function (UPF));

nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ UP NG-UPF; và

gửi (140) phản hồi xác thực dựa trên EAP đến UP NG-UPF.

2. Phương pháp theo mục 1, còn bao gồm:

thiết lập (100) sự xác thực chính với NG-chức năng neo an toàn (security anchor function (SEAF)).

3. Phương pháp để xác thực phụ trong mạng, được thực hiện bởi thiết bị chức năng mặt phẳng người dùng thế hệ tiếp theo (next generation (NG)-user plane UP function (UPF)), phương pháp này bao gồm các bước:

thiết lập (110) phiên hoặc kết nối UP đối với thiết bị người dùng thế hệ tiếp theo (NG-user equipment (UE));

gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến NG UE; và

nhận (150) phản hồi xác thực dựa trên EAP từ NG UE.

4. Phương pháp theo mục 3, còn bao gồm:

gửi (160) yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)); và

nhận (170) phản hồi xác nhận từ máy chủ AAA.

5. Thiết bị người dùng thế hệ tiếp theo (next generation (NG) user equipment (UE)) để hoạt động trong mạng, NG UE bao gồm:

bộ xử lý (10); và

sản phẩm chương trình máy tính (12, 13) lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho NG UE:

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP thế hệ tiếp theo (NG-UP function (UPF));

nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ NG-UPF; và

gửi (140) phản hồi xác thực dựa trên EAP đến NG-UPF.

6. Thiết bị người dùng thế hệ tiếp theo (NG user equipment (UE)) theo mục 5, NG UE còn được làm cho:

thiết lập (100) sự xác thực chính với NG chức năng neo an toàn (security anchor function (SEAF)).

7. Thiết bị chức năng mặt phẳng người dùng thế hệ tiếp theo (next generation (NG)-user plane (UP) function (UPF)) hoạt động trong mạng, NG-UPF bao gồm:

bộ xử lý (10); và

sản phẩm chương trình máy tính (12, 13) lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho NG-UPF:

thiết lập (110) phiên hoặc kết nối UP với thiết bị người dùng thế hệ tiếp theo (NG-user equipment (UE));

gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến NG UE; và

nhận (150) phản hồi xác thực dựa trên EAP từ NG UE.

8. Thiết bị chức năng mặt phẳng người dùng thế hệ tiếp theo (NG user plane (UP) function (UPF)) theo mục 7, NG-UPF còn được làm cho:

gửi (160) yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)); và

nhận (170) phản hồi xác nhận từ máy chủ AAA.

9. Thiết bị người dùng thế hệ tiếp theo (next generation (NG) user equipment (UE)) để hoạt động trong mạng, NG UE bao gồm:

bộ quản lý truyền thông (61) để thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP thế hệ tiếp theo (NG-UP function (UPF)), nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ NG-UPF, và gửi (140) phản hồi xác thực dựa trên EAP đến NG-UPF.

10. Thiết bị chức năng mặt phẳng người dùng thế hệ tiếp theo (next generation (NG)-user plane (UP) function (UPF)) hoạt động trong mạng, NG-UPF bao gồm:

bộ quản lý truyền thông (71) để thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị người dùng thế hệ tiếp theo (NG user equipment (UE)), gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở

rộng (extensible authentication protocol (EAP)) đến NG UE, và nhận (150) phản hồi xác thực dựa trên EAP từ NG UE.

11. Chương trình máy tính (14, 15) để xác thực phụ trong mạng, chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên thiết bị người dùng thế hệ tiếp theo (next generation (NG) user equipment (UE)), làm cho NG UE:

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với thiết bị chức năng UP thế hệ tiếp theo (NG-UP function (UPF));

nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) từ NG-UPF; và

gửi (140) phản hồi xác thực dựa trên EAP đến NG-UPF.

12. Chương trình máy tính (14, 15) để xác thực phụ trong mạng, chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên thiết bị chức năng mặt phẳng người dùng thế hệ tiếp theo (next generation (NG)-user plane (UP) function (UPF)), làm cho NG-UPF:

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) đối với thiết bị người dùng thế hệ tiếp theo (NG user equipment (UE));

gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến NG UE; và

nhận (150) phản hồi xác thực dựa trên EAP từ NG UE.

13. Sản phẩm chương trình máy tính (12, 13) bao gồm chương trình máy tính (14, 15) theo một mục bất kỳ trong số các mục 11 đến 12 và phương tiện lưu trữ đọc được bởi máy tính mà trên đó chương trình máy tính (14, 15) được lưu trữ.

YÊU CẦU BẢO HỘ

1. Phương pháp để xác thực phụ trong mạng, được thực hiện bởi thiết bị người dùng (user equipment (UE)), phương pháp này bao gồm các bước:

thiết lập (100) sự xác thực chính với chức năng neo an toàn (security anchor function (SEAF));

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với hoặc thông qua thiết bị chức năng UP (UP function (UPF));

nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) thông qua UPF;

gửi (140) phản hồi xác thực dựa trên EAP đến UPF; và

nhận kết quả xác thực dựa trên EAP thông qua UPF, kết quả xác thực dựa trên EAP dựa trên phản hồi xác nhận từ máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) trong miền bên thứ ba.

2. Phương pháp theo điểm 1, trong đó thiết bị người dùng (user equipment (UE)) là UE thế hệ tiếp theo (next generation (NG)).

3. Phương pháp theo điểm 1, trong đó thiết bị chức năng mặt phẳng người dùng (user plane function (UPF)) là UPF thế hệ tiếp theo (next generation (NG)).

4. Phương pháp theo điểm 1, trong đó SEAF còn được kết nối với chức năng máy chủ xác thực (authentication server function (AUSF)).

5. Phương pháp để xác thực phụ trong mạng, được thực hiện bởi thiết bị chức năng mặt phẳng người dùng (user plane UP function (UPF)), phương pháp này bao gồm các bước:

thiết lập (110) phiên hoặc kết nối UP đối với thiết bị người dùng (user equipment (UE));

gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE;

nhận (150) phản hồi xác thực dựa trên EAP từ UE;

gửi (160) yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) trong miền bên thứ ba;

nhận (170) phản hồi xác nhận từ máy chủ AAA; và

gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

6. Phương pháp theo điểm 5, trong đó thiết bị người dùng (user equipment (UE)) là thiết bị người dùng thế hệ tiếp theo (next generation (NG) user equipment (UE)).

7. Phương pháp theo điểm 5, trong đó thiết bị chức năng mặt phẳng người dùng (user plane function (UPF)) là UPF thế hệ tiếp theo (next generation (NG)).

8. Thiết bị người dùng (user equipment (UE)) để hoạt động trong mạng, UE này bao gồm:

bộ xử lý (10); và

sản phẩm chương trình máy tính (12, 12) lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho UE:

thiết lập (100) sự xác thực chính với chức năng neo an toàn (security anchor function (SEAF));

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với hoặc thông qua thiết bị chức năng UP (UP function (UPF));

nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) thông qua UPF;

gửi (140) phản hồi xác thực dựa trên EAP đến UPF; và

nhận kết quả xác thực dựa trên EAP thông qua UPF, kết quả xác thực dựa trên EAP dựa trên phản hồi xác nhận từ máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) trong miền bên thứ ba.

9. Thiết bị người dùng (user equipment (UE)) theo điểm 8, trong đó UE là UE thế hệ tiếp theo (next generation (NG)).

10. Thiết bị người dùng (user equipment (UE)) theo điểm 8, trong đó UPF là UPF thế hệ tiếp theo (next generation (NG)).

11. Thiết bị người dùng (user equipment (UE)) theo điểm 8, trong đó SEAF còn được kết nối với chức năng máy chủ xác thực (authentication server function (AUSF)).

12. Thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)) hoạt động trong mạng, UPF này bao gồm:

bộ xử lý (10); và

sản phẩm chương trình máy tính (12, 13) lưu trữ các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho UPF:

thiết lập (110) phiên hoặc kết nối UP với thiết bị người dùng (user equipment (UE));

gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE;

nhận (150) phản hồi xác thực dựa trên EAP từ UE;

gửi (160) yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) trong miền bên thứ ba;

nhận (170) phản hồi xác nhận từ máy chủ AAA; và

gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

13. Thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)) theo điểm 12, trong đó UPF là UPF thế hệ tiếp theo (next generation (NG)).

14. Thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)) theo điểm 12, trong đó UE là UE thế hệ tiếp theo (next generation (NG)).

15. Phương tiện lưu trữ đọc được bởi máy tính lưu trữ trong đó chương trình máy tính (14, 15) để xác thực phụ trong mạng, chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên thiết bị người dùng (user equipment (UE)), làm cho UE:

thiết lập (100) sự xác thực chính với chức năng neo an toàn (security anchor function (SEAF));

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) với hoặc thông qua thiết bị chức năng UP (UP function (UPF));

nhận (130) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) thông qua UPF;

gửi (140) phản hồi xác thực dựa trên EAP đến UPF;

và nhận kết quả xác thực dựa trên EAP thông qua UPF, kết quả xác thực dựa trên EAP dựa trên phản hồi xác nhận từ máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) trong miền bên thứ ba.

16. Phương tiện lưu trữ đọc được bởi máy tính lưu trữ trong đó chương trình máy tính (14, 15) để xác thực phụ trong mạng, chương trình máy tính bao gồm mã chương trình máy tính mà, khi được chạy trên thiết bị chức năng mặt phẳng người dùng (user plane (UP) function (UPF)), làm cho UPF:

thiết lập (110) phiên hoặc kết nối mặt phẳng người dùng (user plane (UP)) đối với thiết bị người dùng (user equipment (UE));

gửi (120) yêu cầu xác thực dựa trên giao thức xác thực có thể mở rộng (extensible authentication protocol (EAP)) đến UE;

nhận (150) phản hồi xác thực dựa trên EAP từ UE;

gửi (160) yêu cầu xác nhận của phản hồi xác thực dựa trên EAP được nhận đến máy chủ xác thực, cấp phép, và tính cước (authentication, authorization, and accounting (AAA)) trong miền bên thứ ba;

nhận (170) phản hồi xác nhận từ máy chủ AAA; và

gửi kết quả xác thực đến UE, trong đó sự xác thực được dựa trên phản hồi xác nhận từ máy chủ AAA.

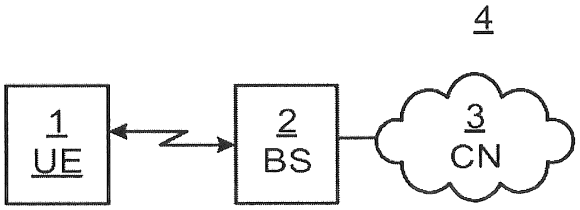

4
1
UE
2
BS
3
CN

Fig. 1

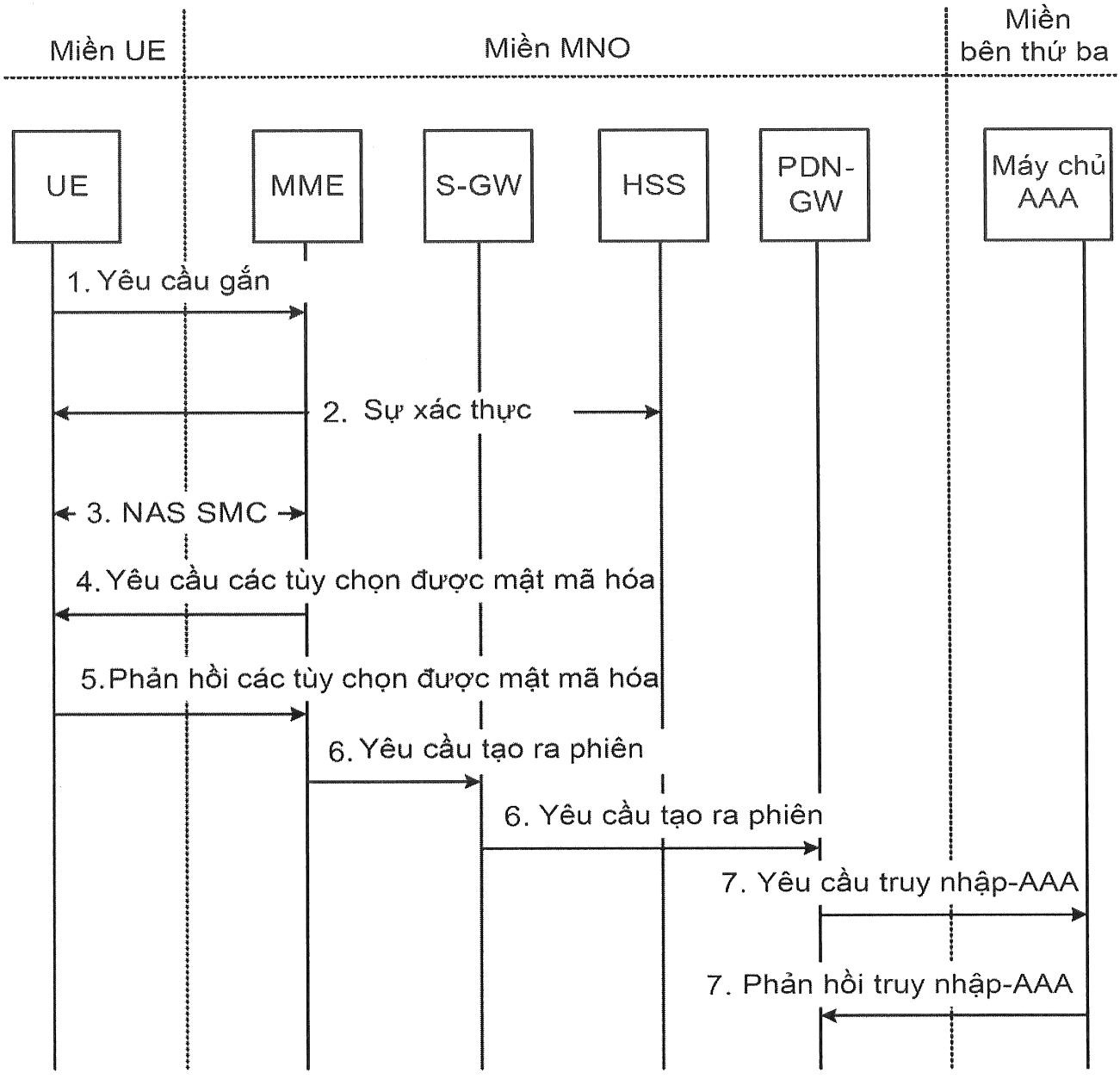

Miền UE
Miền MNO
Miền
bên thứ ba
UE
MME
S-GW
HSS
PDN-
GW
Máy chủ
AAA
1. Yêu cầu gắn
2. Sự xác thực
3. NAS SMC
4. Yêu cầu các tùy chọn được mật mã hóa
5. Phản hồi các tùy chọn được mật mã hóa
6. Yêu cầu tạo ra phiên
6. Yêu cầu tạo ra phiên
7. Yêu cầu truy nhập-AAA
7. Phản hồi truy nhập-AAA

Fig. 2

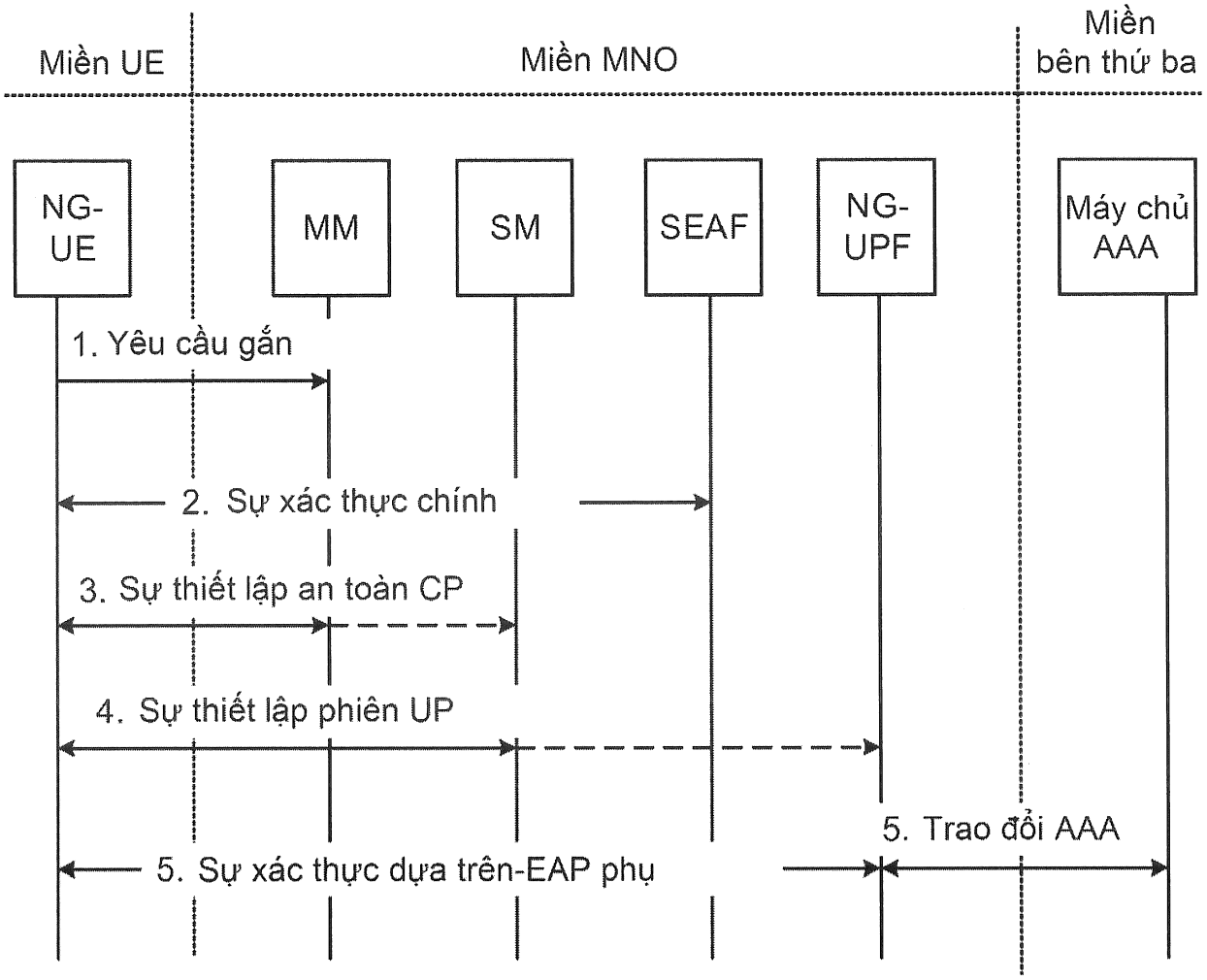

Miền UE
Miền MNO
Miền bên thứ ba
NG-UE
MM
SM
SEAF
NG-UPF
Máy chủ AAA
1. Yêu cầu gắn
2. Sự xác thực chính
3. Sự thiết lập an toàn CP
4. Sự thiết lập phiên UP
5. Trao đổi AAA
5. Sự xác thực dựa trên-EAP phụ

Fig. 3

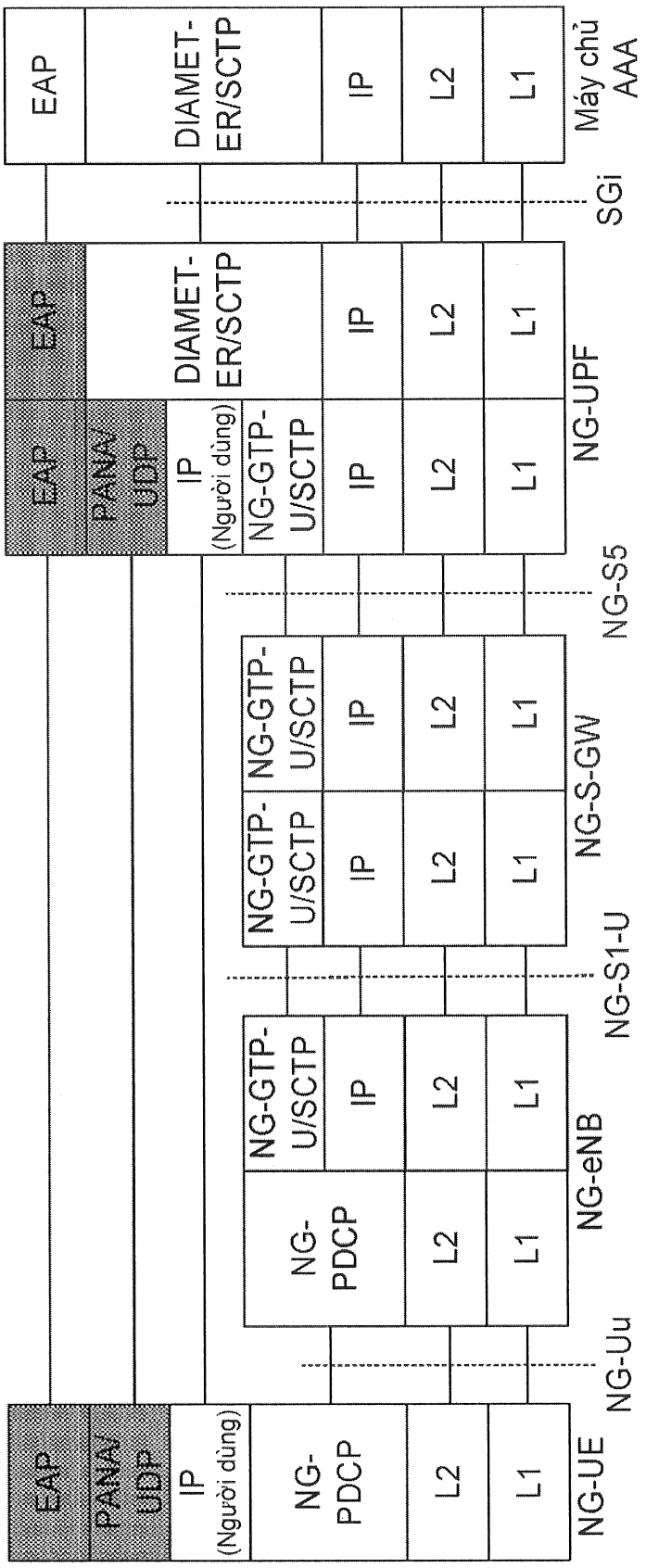

EAP
PANA/ UDP
IP (Người dùng)
NG-PDCP
L2
L1
NG-UE
NG-Uu
NG-GTP-U/SCTP
IP
NG-eNB
NG-S1-U
NG-S-GW
NG-S5
NG-UPF
DIAMET-ER/SCTP
SGi
Máy chủ AAA

Fig. 4

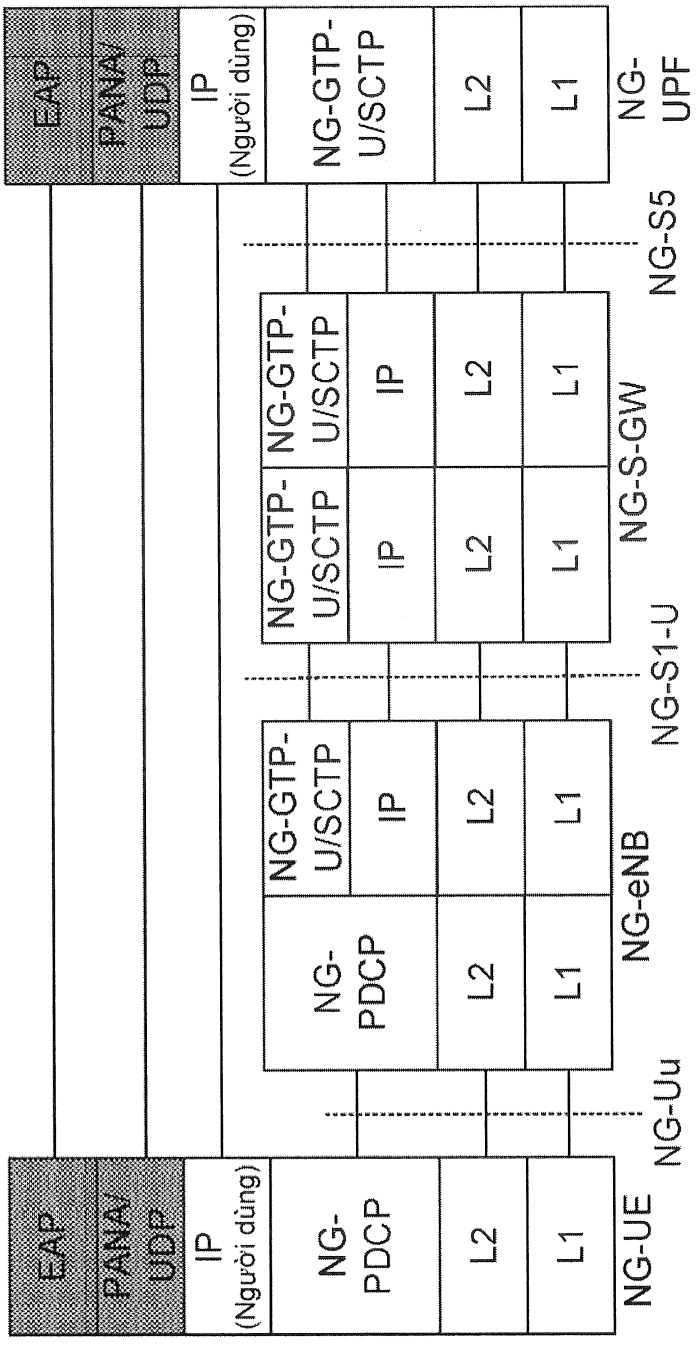

EAP
PANA/
UDP
IP
(Người dùng)
NG-
PDCP
L2
L1
NG-UE
NG-Uu
NG-GTP-
U/SCTP
IP
NG-eNB
NG-S1-U
NG-S-GW
NG-S5
NG-
UPF

Fig. 5

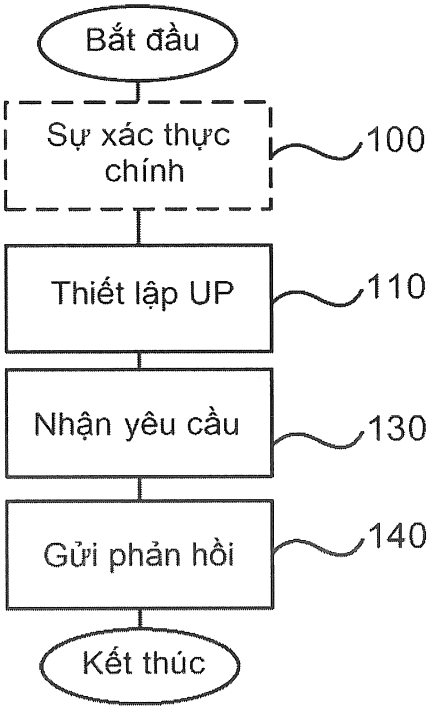

Bắt đầu
Sự xác thực chính
100
Thiết lập UP
110
Nhận yêu cầu
130
Gửi phản hồi
140
Kết thúc

Fig. 6A

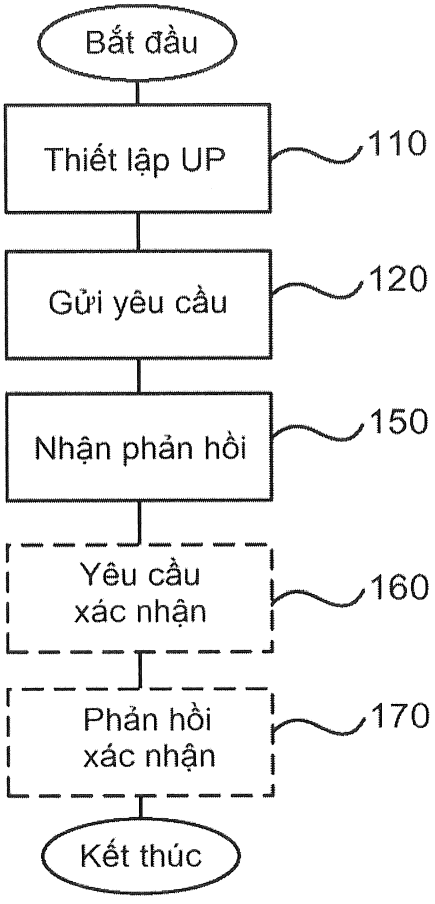

Bắt đầu
Thiết lập UP
110
Gửi yêu cầu
120
Nhận phản hồi
150
Yêu cầu xác nhận
160
Phản hồi xác nhận
170
Kết thúc

Fig. 6B

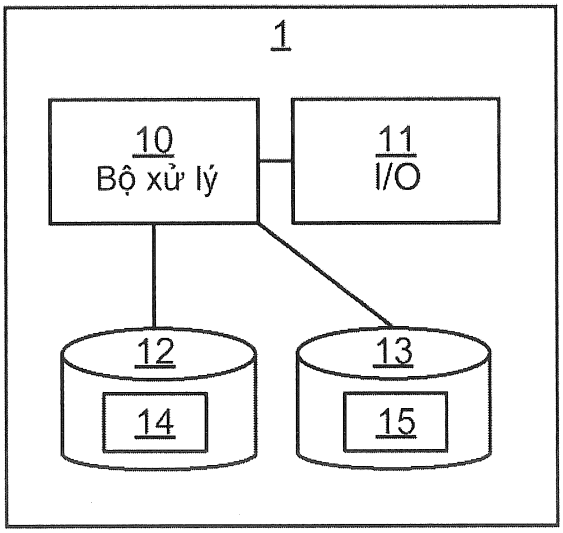


Fig. 7

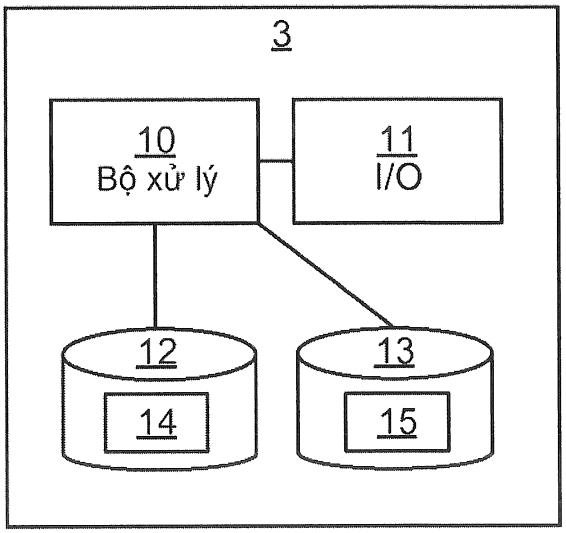


Fig. 8

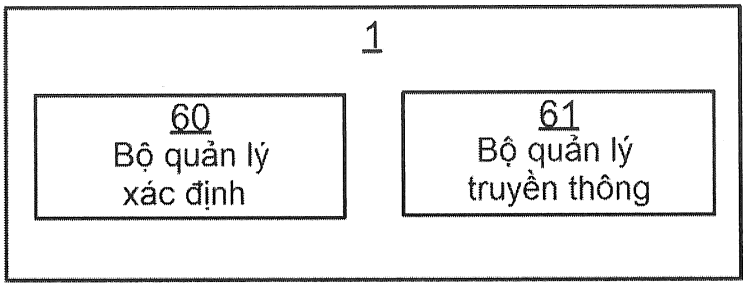


Fig. 9

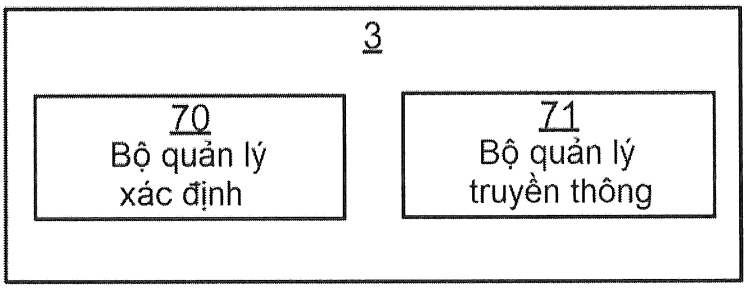


Fig. 10