(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) **1-0053060**

(51)[2021.01] **H04W 12/041**; H04W 12/72; H04W 12/0431; H04L 9/08

(13) **B**

(21) 1-2022-05531
(22) 28/01/2021
(86) PCT/CN2021/074160 28/01/2021
(87) WO/2021/155758 12/08/2021
(30) 202010079720.7 04/02/2020 CN
(45) 25/11/2025 452
(43) 25/10/2022 415A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) DENG, Juan (CN); ZHANG, Bo (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP, THIẾT BỊ VÀ HỆ THỐNG THU THẬP KHOÁ, THIẾT BỊ TRUYỀN THÔNG, VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2022-05531

(57) Sáng chế bộc lộ phương pháp thu thập khoá, trong đó phương pháp này bao gồm các bước: thu thập, bởi AUSF (AUthentication Server Function - chức năng máy chủ xác thực), khoá AKMA (Authentication and Key Management for Applications anchor function - chức năng mỏ neo xác thực và quản lý khoá dành cho các ứng dụng) và/hoặc bộ nhận dạng khoá (Key IDentifier - KID) duy nhất của khoá AKMA này; thu thập, bởi AMF/SEAF (Access and Mobility management Function/SEcurity Anchor Function - chức năng quản lý truy cập và quản lý tính di động/chức năng mỏ neo bảo mật), thông điệp thứ tư từ AUSF; và gửi thông điệp thứ năm đến UE (User Equipment - thiết bị người dùng) dựa trên thông điệp thứ tư này, để UE thu thập KID và/hoặc khoá AKMA dựa trên thông điệp thứ năm này. Các phương án của sáng chế bộc lộ phương pháp thu thập hoặc tạo ra khoá AKMA và bộ nhận dạng khoá duy nhất tương ứng với khoá AKMA này, để bảo đảm sự thương lượng khoá trơn tru giữa UE và AF (Application Function - chức năng ứng dụng) và cải thiện sự bảo mật truyền thông giữa UE và AF. Thiết bị thu thập khoá, hệ thống thu thập khoá, thiết bị truyền thông, và phương tiện lưu trữ đọc được bằng máy tính cũng được bộc lộ.

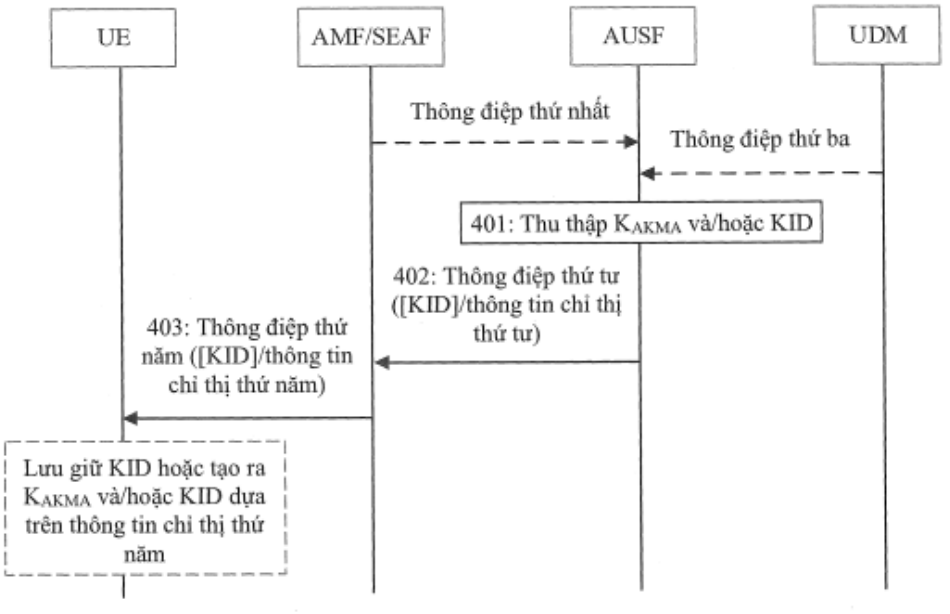


Fig.4A

Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến các công nghệ truyền thông, và cụ thể là đề cập đến phương pháp và thiết bị thu thập khoá.

Tình trạng kỹ thuật của sáng chế

Trong kiến trúc khoá để xác thực và quản lý khoá dành cho các ứng dụng (Authentication and Key Management for Applications - AKMA), thì các khoá khác nhau được tạo ra ở mỗi trong số phía thiết bị người dùng (User Equipment - UE) và phía mạng. Ở phía mạng, sau khi UE hoàn tất việc xác thực sơ cấp, thì chức năng máy chủ xác thực (Authentication Server Function - AUSF) có thể tạo ra khoá AKMA K_{AKMA} dựa trên khoá AUSF K_{AUSF} mà được tạo ra trong tiến trình xác thực sơ cấp. K_{AKMA} là khoá trên mỗi UE (nói cách khác, mỗi UE đều có K_{AKMA} được dành riêng). AUSF truyền K_{AKMA} được tạo ra đến chức năng mỏ neo AKMA (AKMA Anchor Function - AAnF). Sau đó, AAnF tạo ra khoá ứng dụng K_{AF} cho chức năng ứng dụng (Application Function - AF) dựa trên K_{AKMA}. K_{AF} là khoá trên mỗi UE và trên mỗi ứng dụng (nói cách khác, một UE sử dụng K_{AF} được dành riêng khi truy cập một AF). Ở phía UE, thì UE sử dụng các thông số và thuật toán giống như ở phía mạng để tạo ra K_{AUSF} trong tiến trình xác thực. Sau khi việc xác thực thành công, thì UE có thể tạo ra K_{AKMA} dựa trên K_{AUSF} nhờ sử dụng các thông số và thuật toán giống như ở phía mạng, và tạo ra K_{AF} dựa trên K_{AKMA} nhờ sử dụng các thông số và thuật toán giống như ở phía mạng. Sau đó, ở phía UE và phía mạng, thì việc bảo vệ lưu lượng được thực hiện giữa UE và AF dựa trên K_{AF}.

Trong tiến trình này, thì mỗi K_{AKMA} là được nhận dạng bởi bộ nhận dạng khoá duy nhất K_{AKMA} ID (được gọi là KID theo sáng chế). Khi UE truy cập AF, thì UE gửi KID đến AF, để chỉ thị K_{AKMA} được sử dụng bởi UE. Sau khi nhận được KID, thì AF gửi KID đến AAnF. Sau đó, AAnF tạo ra K_{AF} nhờ sử dụng K_{AKMA} được nhận dạng bởi KID và gửi K_{AF} đến AF. Theo cách này, thì bảo đảm được rằng UE và AF sử dụng K_{AF} giống nhau, tức là, K_{AF} là được tạo ra nhờ sử dụng K_{AKMA} mà được nhận dạng bởi

KID, nhờ đó thực hiện việc thương lượng khoá giữa UE và AF. Không có nghiên cứu nào về việc tạo ra và cập nhật KID theo công nghệ thông thường. Do đó, việc thương lượng khoá giữa UE và AF không thể được thực hiện.

Bản chất kỹ thuật của sáng chế

Theo các phương án, sáng chế đề xuất phương pháp và thiết bị thu thập khoá, để thu thập khoá trong tiến trình truyền thông giữa thiết bị đầu cuối người dùng và chức năng ứng dụng.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp thu thập khoá, trong đó phương pháp này được áp dụng cho chức năng máy chủ xác thực (AUthentication Server Function - AUSF). Phương pháp này bao gồm các bước:

thu thập khoá mỏ neo của tiến trình xác thực và quản lý khoá dành cho các ứng dụng K_{AKMA} và/hoặc bộ nhận dạng khoá KID duy nhất của K_{AKMA}.

Theo thiết kế khả thi, thì bước thu thập khoá mỏ neo của tiến trình xác thực và quản lý khoá dành cho các ứng dụng K_{AKMA} và/hoặc bộ nhận dạng khoá KID duy nhất của K_{AKMA} là bao gồm các bước:

nhận thông điệp thứ nhất được gửi bởi chức năng quản lý truy cập và quản lý tính di động hoặc chức năng mỏ neo bảo mật (Access and Mobility management Function / SEcurity Anchor Function AMF/SEAF), và thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất này.

Theo thiết kế khả thi, thì thông điệp thứ nhất bao gồm KID, và bước thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất là bao gồm các bước: thu thập KID trong thông điệp thứ nhất và/hoặc tạo ra K_{AKMA} dựa trên KID.

Theo thiết kế khả thi, thì thông điệp thứ nhất bao gồm thông tin chỉ thị thứ hai, và bước thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất là bao gồm bước:

tạo ra KID và/hoặc K_{AKMA} dựa trên thông tin chỉ thị thứ hai, trong đó thông tin chỉ thị thứ hai này được dùng để yêu cầu hoặc chỉ thị cho AUSF tạo ra KID và/hoặc K_{AKMA}.

Theo phương án này của sáng chế, thì UE chủ động gửi KID hoặc thông tin chỉ thị thứ nhất đến AMF/SEAF, và AMF/SEAF chuyển tiếp KID đến AUSF hoặc gửi thông tin chỉ thị thứ hai đến AUSF dựa trên thông tin chỉ thị thứ nhất. Sau đó, AUSF tạo ra K_{AKMA} dựa trên KID nhận được, hoặc tạo ra KID và/hoặc K_{AKMA} dựa trên thông

tin chỉ thị thứ hai. Thông tin chỉ thị thứ nhất được dùng để yêu cầu hoặc chỉ thị tạo ra KID và/hoặc K_{AKMA}. Trong tiến trình này, thì KID và/hoặc K_{AKMA} có thể được tạo ra dựa trên yêu cầu của UE. Điều này thực hiện việc tạo ra khoá dựa trên yêu cầu, và tránh việc tạo ra, lưu giữ, và quản lý khoá không cần thiết.

Theo thiết kế khả thi, sau khi thông điệp thứ nhất được nhận, thì bước thu thập KID và/hoặc KAKMA dựa trên thông điệp thứ nhất còn bao gồm các bước:

gửi thông điệp thứ hai đến chức năng quản lý dữ liệu hợp nhất (Unified Data Management - UDM) dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai này bao gồm chỉ thị thu thập sự cho phép, chỉ thị thu thập sự cho phép này được dùng để thu thập thông tin cho phép thứ nhất của UE, và thông tin cho phép thứ nhất này được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ xác thực và quản lý khoá dành cho các ứng dụng (Authentication and Key MAnagement - AKMA); và

khi xác định được rằng thông tin cho phép thứ nhất của UE đã được thu thập, thì tạo ra KID và/hoặc K_{AKMA}.

Theo phương án này của sáng chế, thì AUSF chủ động gửi chỉ thị thu thập sự cho phép đến UDM, để thu thập thông tin cho phép thứ nhất, trong đó thông tin cho phép thứ nhất này được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ xác thực và quản lý khoá dành cho các ứng dụng (Authentication and Key MAnagement - AKMA). Sau đó, AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất thu được. Điều này có thể bảo đảm rằng khoá chỉ được tạo ra cho thiết bị người dùng được phép ở phía mạng và tránh việc tạo ra khoá không được phép.

Theo thiết kế khả thi, thì thông điệp thứ nhất là yêu cầu dịch vụ xác thực, và yêu cầu dịch vụ xác thực này được dùng để yêu cầu AUSF thực hiện việc xác thực trên UE.

Theo thiết kế khả thi, thì yêu cầu dịch vụ xác thực này bao gồm đáp ứng xác thực thu được khi AMF/SEAF khởi tạo yêu cầu xác thực đến UE.

Theo thiết kế khả thi, thì thông điệp thứ hai được dùng để yêu cầu vectơ xác thực của UE từ UDM, hoặc thông điệp thứ hai được dùng để thông báo cho UDM về kết quả xác thực.

Theo thiết kế khả thi, thì bước thu thập khoá mỏ neo của tiến trình xác thực và quản lý khoá dành cho các ứng dụng K_{AKMA} và/hoặc bộ nhận dạng khoá KID duy nhất của K_{AKMA} là bao gồm các bước:

nhận thông điệp thứ ba được gửi bởi UDM, và tạo ra KID và/hoặc K_{AKMA} dựa trên thông điệp thứ ba này.

Theo thiết kế khả thi, thì thông điệp thứ ba bao gồm thông tin chỉ thị thứ ba hoặc thông tin cho phép thứ nhất, và thông tin chỉ thị thứ ba này được dùng để chỉ thị cho AUSF tạo ra KID và/hoặc K_{AKMA}. Bước tạo ra KID và/hoặc K_{AKMA} dựa trên thông điệp thứ ba bao gồm bước tạo ra KID và/hoặc K_{AKMA} dựa trên thông tin chỉ thị thứ ba hoặc thông tin cho phép thứ nhất.

Theo phương án này của sáng chế, thì UDM chủ động thu thập thông tin cho phép thứ nhất của UE, và gửi thông tin cho phép thứ nhất này hoặc thông tin chỉ thị thứ ba đến AUSF nhờ sử dụng thông điệp thứ ba, để AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất hoặc thông tin chỉ thị thứ ba này. Trước khi UE khởi tạo ứng dụng, thì UDM có thể chủ động nhắc AUSF tạo ra trước K_{AKMA} và/hoặc KID, để tăng hiệu quả thu thập khoá.

Theo thiết kế khả thi, thì thông điệp thứ ba là thông điệp đáp ứng dịch vụ xác thực, và được dùng để gửi vectơ xác thực của UE đến AUSF.

Theo thiết kế khả thi, thì thông điệp thứ ba là thông điệp đáp ứng xác nhận kết quả xác thực, và được dùng để đáp lại thông điệp yêu cầu xác nhận kết quả xác thực được gửi bởi AUSF.

Theo khía cạnh thứ hai, sáng chế đề xuất phương pháp thu thập khoá, trong đó phương pháp này được áp dụng cho việc quản lý truy cập và quản lý tính di động hoặc chức năng mỏ neo bảo mật (Access and Mobility management/SEcurity Anchor Function - AMF/SEAF). Phương pháp này bao gồm các bước:

thu thập thông điệp thứ tư từ AUSF; và

gửi thông điệp thứ năm đến UE dựa trên thông điệp thứ tư này, để UE thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ năm này.

Theo thiết kế khả thi, thì thông điệp thứ năm bao gồm KID, và được dùng để cho phép UE thu thập KID trong thông điệp thứ năm, và/hoặc tạo ra K_{AKMA} dựa trên KID.

Theo thiết kế khả thi, thì thông điệp thứ năm bao gồm thông tin chỉ thị thứ năm, và thông tin chỉ thị thứ năm này được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}.

Theo thiết kế khả thi, trước khi thông điệp thứ tư được nhận, thì phương pháp

này còn bao gồm bước:

gửi thông điệp thứ nhất đến AUSF, để AUSF tạo ra KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất.

Theo khía cạnh thứ ba, sáng chế đề xuất phần tử mạng AUSF, trong đó phần tử này bao gồm môđun xử lý. Môđun xử lý được tạo cấu hình để:

thu thập khoá mỏ neo của tiến trình xác thực và quản lý khoá dành cho các ứng dụng K_{AKMA} và/hoặc bộ nhận dạng khoá KID duy nhất của K_{AKMA}.

Theo thiết kế khả thi, thì phần tử mạng AUSF này còn bao gồm môđun nhận, được tạo cấu hình để nhận thông điệp thứ nhất được gửi bởi chức năng quản lý truy cập và quản lý tính di động hoặc chức năng mỏ neo bảo mật (Access and Mobility management Function/SEcurity Anchor Function - AMF/SEAF); và

môđun xử lý được tạo cấu hình để thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất.

Theo thiết kế khả thi, thì thông điệp thứ nhất bao gồm KID, và môđun xử lý được tạo cấu hình cụ thể để:

thu thập KID trong thông điệp thứ nhất, và/hoặc tạo ra K_{AKMA} dựa trên KID.

Theo thiết kế khả thi, thì thông điệp thứ nhất bao gồm thông tin chỉ thị thứ nhất, và môđun xử lý được tạo cấu hình cụ thể để tạo ra KID và/hoặc K_{AKMA} dựa trên thông tin chỉ thị thứ nhất.

Theo thiết kế khả thi, thì phần tử mạng AUSF còn bao gồm môđun gửi, được tạo cấu hình để gửi thông điệp thứ hai đến chức năng quản lý dữ liệu hợp nhất (Unified Data Management - UDM) dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai này bao gồm chỉ thị thu thập sự cho phép, chỉ thị thu thập sự cho phép này được dùng để thu thập thông tin cho phép thứ nhất của UE, và thông tin cho phép thứ nhất này được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ xác thực và quản lý khoá dành cho các ứng dụng (Authentication and Key MAnagement - AKMA); và

môđun xử lý được tạo cấu hình để: khi xác định được rằng thông tin cho phép thứ nhất của UE đã được thu thập, thì tạo ra KID và/hoặc K_{AKMA}.

Theo thiết kế khả thi, thì môđun nhận được tạo cấu hình để nhận thông điệp thứ ba được gửi bởi UDM, trong đó thông điệp thứ ba này bao gồm thông tin chỉ thị thứ ba; và

môđun xử lý được tạo cấu hình để tạo ra KID và/hoặc K_{AKMA} dựa trên thông

tin chỉ thị thứ ba.

Theo khía cạnh thứ tư, sáng chế đề xuất phần tử mạng AMF/SEAF. Phần tử mạng này bao gồm:

môđun nhận, được tạo cấu hình để thu thập thông điệp thứ tư từ AUSF; và

môđun gửi, được tạo cấu hình để gửi thông điệp thứ năm đến UE dựa trên thông điệp thứ tư này, để UE thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ năm này.

Theo thiết kế khả thi, thì môđun gửi còn được tạo cấu hình để gửi thông điệp thứ nhất đến AUSF, để AUSF tạo ra KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất.

Theo khía cạnh thứ năm, theo một phương án, sáng chế đề xuất thiết bị truyền thông. Thiết bị này có chức năng thực hiện thiết bị đầu cuối theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất, hoặc có chức năng thực hiện phần tử mạng mặt phẳng điều khiển theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất.

Thiết bị này có thể là thiết bị đầu cuối, hoặc có thể là con chip được bao gồm trong thiết bị đầu cuối. Chức năng của thiết bị truyền thông này có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần cứng bằng cách thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng này.

Thiết bị này có thể là thiết bị mạng, hoặc có thể là con chip được bao gồm trong thiết bị mạng. Chức năng của thiết bị truyền thông này có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần cứng bằng cách thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng này.

Theo thiết kế khả thi, thì cấu trúc của thiết bị này bao gồm môđun xử lý và môđun thu phát. Môđun xử lý được tạo cấu hình để hỗ trợ thiết bị này để thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất, hoặc thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ hai hoặc những cách thức thực hiện khả thi của khía cạnh thứ hai.

Theo thiết kế khả thi khác, thì cấu trúc của thiết bị này bao gồm bộ xử lý, và có thể còn bao gồm bộ nhớ. Bộ xử lý được ghép nối đến bộ nhớ, và có thể được tạo cấu hình để thực thi các chỉ dẫn chương trình máy tính được lưu giữ trong bộ nhớ, để cho

phép thiết bị này thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất, hoặc thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ hai hoặc những cách thức thực hiện khả thi của khía cạnh thứ hai. Tuỳ ý, thiết bị này còn bao gồm giao diện truyền thông, và bộ xử lý được ghép nối vào giao diện truyền thông này. Khi thiết bị này là thiết bị mạng, thì giao diện truyền thông này có thể là bộ thu phát hoặc giao diện vào/ra. Khi thiết bị này là con chip được bao gồm trong thiết bị mạng này, thì giao diện truyền thông này có thể là giao diện vào/ra của con chip này. Tuỳ ý, bộ thu phát có thể là mạch thu phát, và giao diện vào/ra có thể là mạch vào/ra.

Theo khía cạnh thứ sáu, theo một phương án, sáng chế đề xuất hệ thống chip. Hệ thống chip này bao gồm bộ xử lý, và bộ xử lý này được ghép nối đến bộ nhớ. Bộ nhớ được tạo cấu hình để lưu giữ các chương trình hoặc các chỉ dẫn, và khi các chương trình hoặc các chỉ dẫn này được thực thi bởi bộ xử lý, thì hệ thống chip này được cho phép thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất, hoặc thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ hai hoặc những cách thức thực hiện khả thi của khía cạnh thứ hai.

Tuỳ ý, hệ thống chip này còn bao gồm mạch giao diện, và mạch giao diện này được tạo cấu hình để trao đổi các chỉ dẫn mã đến bộ xử lý.

Tuỳ ý, có thể có một hoặc nhiều bộ xử lý trong hệ thống chip này, và bộ xử lý này có thể được thực hiện bằng phần cứng hoặc có thể được thực hiện bằng phần mềm. Khi bộ xử lý được thực hiện bằng phần cứng, thì bộ xử lý có thể là mạch logic, mạch tích hợp, v.v.. Khi bộ xử lý được thực hiện bằng phần mềm, thì bộ xử lý có thể là bộ xử lý thông dụng, và được thực hiện bằng cách đọc mã phần mềm được lưu giữ trong bộ nhớ.

Tuỳ ý, có thể có một hoặc nhiều bộ nhớ trong hệ thống chip này. Bộ nhớ có thể được tích hợp với bộ xử lý, hoặc có thể được bố trí tách biệt khỏi bộ xử lý. Điều này không bị giới hạn theo sáng chế. Ví dụ, bộ nhớ có thể là bộ xử lý phi nhất thời, ví dụ, bộ nhớ chỉ đọc (Read-Only Memory - ROM). Bộ nhớ và bộ xử lý có thể được tích hợp vào cùng một con chip, hoặc có thể được bố trí riêng biệt trên các con chip khác nhau. Chủng loại bộ nhớ và cách bố trí bộ nhớ và bộ xử lý là không bị giới hạn cụ thể theo sáng chế.

Theo khía cạnh thứ bảy, theo một phương án, sáng chế đề xuất phương tiện lưu trữ đọc được bằng máy tính. Phương tiện lưu trữ đọc được bằng máy tính này lưu giữ các chương trình máy tính hoặc các chỉ dẫn, và khi các chương trình máy tính hoặc các chỉ dẫn này được thực thi, thì máy tính được cho phép thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất, hoặc thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ hai hoặc những cách thức thực hiện khả thi của khía cạnh thứ hai.

Theo khía cạnh thứ tám, theo một phương án, sáng chế đề xuất sản phẩm chương trình máy tính. Khi máy tính đọc và thực thi sản phẩm chương trình máy tính này, thì máy tính đó được cho phép thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ nhất hoặc những cách thức thực hiện khả thi của khía cạnh thứ nhất, hoặc thực hiện phương pháp theo bất kỳ trong số khía cạnh thứ hai hoặc những cách thức thực hiện khả thi của khía cạnh thứ hai.

Theo khía cạnh thứ chín, theo một phương án, sáng chế đề xuất hệ thống truyền thông. Hệ thống truyền thông này bao gồm một hoặc nhiều phần tử mạng xử lý và phần tử mạng quản lý nêu trên. Tuỳ ý, hệ thống truyền thông này có thể còn bao gồm thiết bị mặt phẳng điều khiển, thiết bị mạng khác, và/hoặc thiết bị đầu cuối.

Mô tả vắn tắt các hình vẽ

Để mô tả các giải pháp kỹ thuật theo các phương án của sáng chế hoặc công nghệ thông thường một cách rõ ràng hơn, thì phần sau đây mô tả vắn tắt các hình vẽ kèm theo mà được sử dụng khi mô tả các phương án.

Fig.1 là hình vẽ thể hiện sơ đồ kiến trúc mạng AKMA theo một phương án của sáng chế;

Fig.2 là hình vẽ thể hiện sơ đồ kiến trúc khoá AKMA theo một phương án của sáng chế;

Fig.3 là hình vẽ thể hiện sơ đồ thương lượng khoá khi UE truy cập AF theo một phương án của sáng chế;

Fig.4A là hình vẽ thể hiện lưu đồ của phương pháp thu thập khoá theo một phương án của sáng chế;

Fig.4B là hình vẽ thể hiện lưu đồ của phương pháp thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế;

Fig.4C là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập K_{AKMA} và/hoặc KID theo một phương án của sáng chế;

Fig.4D là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế;

Fig.4E là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế;

Fig.4F là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế;

Fig.5 là hình vẽ thể hiện lưu đồ của phương pháp xác thực danh tính UE theo một phương án của sáng chế;

Fig.6A là hình vẽ thể hiện lưu đồ của phương pháp cập nhật KID và/hoặc K_{AKMA} theo một phương án của sáng chế;

Fig.6B là hình vẽ thể hiện lưu đồ của phương pháp khác để cập nhật KID và/hoặc K_{AKMA} theo một phương án của sáng chế;

Fig.7 là hình vẽ thể hiện sơ đồ khối cấu trúc của thiết bị truyền thông theo một phương án của sáng chế;

Fig.8 là hình vẽ thể hiện sơ đồ khối cấu trúc của thiết bị truyền thông khác theo một phương án của sáng chế; và

Fig.9 là hình vẽ thể hiện sơ đồ cấu trúc phần cứng của thiết bị truyền thông theo một phương án của sáng chế.

Mô tả chi tiết các phương án thực hiện sáng chế

Trong bản mô tả, các điểm yêu cầu bảo hộ, và các hình vẽ kèm theo của đơn này, thì các từ ngữ "thứ nhất", "thứ hai", "thứ ba", "thứ tư", v.v., là nhằm để phân biệt giữa các đối tượng khác nhau chứ không biểu thị thứ tự cụ thể. Ngoài ra, các từ ngữ "bao gồm", "có", và biến thể bất kỳ khác của chúng, là nhằm bao trùm cả sự bao gồm không loại trừ. Ví dụ, tiến trình, phương pháp, hệ thống, sản phẩm, hoặc thiết bị mà bao gồm một loạt các bước hoặc các đơn vị thì không chỉ giới hạn ở các bước hoặc các đơn vị được liệt kê đó, mà tuỳ ý, còn bao gồm bước hoặc đơn vị không được liệt kê, hoặc tuỳ ý, còn bao gồm bước hoặc đơn vị vốn có khác của tiến trình, phương pháp, sản phẩm, hoặc thiết bị đó.

Việc đề cập đến "phương án" trong bản mô tả này có nghĩa là việc đặc điểm,

cấu trúc, hoặc dấu hiệu cụ thể mà được mô tả dựa vào phương án đó là có thể được bao gồm trong ít nhất một phương án của sáng chế. Cụm từ này được thể hiện ở các vị trí khác nhau trong bản mô tả này có thể không nhất thiết chỉ cùng một phương án, và không phải là phương án độc lập hoặc phương án tuỳ ý loại trừ phương án khác. Người có hiểu biết trung bình trong lĩnh vực cần hiểu một cách tường minh và không tường minh rằng các phương án được mô tả trong bản mô tả này là có thể được kết hợp với phương án khác.

"Nhiều" là hai hoặc nhiều hơn hai. Từ ngữ "và/hoặc" mô tả mối quan hệ liên kết để mô tả các đối tượng liên quan và thể hiện rằng có thể tồn tại ba mối quan hệ. Ví dụ, A và/hoặc B có thể biểu thị ba trường hợp sau đây: Chỉ A tồn tại, cả A và B đều tồn tại, và chỉ B tồn tại. Ký tự "/" nói chung là thể hiện mối quan hệ "hoặc" giữa các đối tượng được liên kết.

Phần sau đây mô tả các thuật ngữ theo các phương án của sáng chế nhờ sử dụng Fig.1 làm ví dụ.

Fig.1 là hình vẽ thể hiện sơ đồ kiến trúc mạng AKMA theo một phương án của sáng chế. So với kiến trúc công nghệ truyền thông di động thế hệ thứ năm (5th Generation Mobile Network - 5G) thông thường, thì chức năng mạng (Network Function - NF) mới, tức là, chức năng mỏ neo AKMA (AKMA Anchor Function - AAnF) 100 là được bổ sung trong kiến trúc mạng AKMA. AAnF có thể là NF được triển khai độc lập, hoặc có thể cùng được triển khai với NF khác. AAnF được dùng để hỗ trợ khoá mỏ neo AKMA (K_{AKMA}) và tạo ra khoá ứng dụng (K_{AF}). Ngoài ra, các phần khác trên Fig.1 và các chức năng mạng theo các phương án của sáng chế là như sau:

Thiết bị đầu cuối 110 cũng có thể được gọi là thiết bị người dùng (User Equipment - UE), đầu cuối, v.v.. Thiết bị đầu cuối này là thiết bị có chức năng thu phát không dây, và có thể truyền thông với một hoặc nhiều mạng lõi (Core Network - CN) nhờ sử dụng thiết bị mạng truy cập trong mạng truy cập (vô tuyến) ((Radio) Access Network - (R)AN) 120. Thiết bị đầu cuối này có thể được triển khai trên đất liền, bao gồm thiết bị đầu cuối trong nhà, thiết bị đầu cuối ngoài trời, thiết bị đầu cuối cầm tay, thiết bị đầu cuối đeo được, hoặc thiết bị đầu cuối được gắn trên xe. Theo cách khác, thiết bị đầu cuối này có thể được triển khai trên mặt nước, ví dụ, trên tàu chạy bằng hơi nước. Theo cách khác, thiết bị đầu cuối này có thể được triển khai trên không, ví dụ, trên máy bay, khí cầu, hoặc vệ tinh. Thiết bị đầu cuối này có thể là điện thoại di động

(Mobile Phone), máy tính bảng (Pad), máy tính có chức năng thu phát không dây, thiết bị đầu cuối thực tế ảo (Virtual Reality - VR), thiết bị đầu cuối thực tế tăng cường (Augmented Reality - AR), thiết bị đầu cuối không dây trong lĩnh vực điều khiển công nghiệp (Industrial Control), thiết bị đầu cuối không dây trong lĩnh vực xe tự hành (self driving), thiết bị đầu cuối không dây trong lĩnh vực y tế từ xa (remote medical), thiết bị đầu cuối không dây trong lưới điện thông minh (smart grid), thiết bị đầu cuối không dây trong lĩnh vực an toàn vận tải (transportation safety), thiết bị đầu cuối không dây trong thành phố thông minh (smart city), thiết bị đầu cuối không dây trong lĩnh vực nhà thông minh (smart home), v.v..

Mạng truy cập (vô tuyến) ((Radio) Access Network - (R)AN) 120 được dùng để cung cấp chức năng truy cập mạng cho các thiết bị người dùng được phép trong vùng cụ thể, và có thể sử dụng các đường hầm truyền có chất lượng biến thiên dựa trên các mức, các yêu cầu dịch vụ, v.v., của các thiết bị người dùng. Ví dụ, (R)AN có thể quản lý tài nguyên vô tuyến, cung cấp dịch vụ truy cập cho thiết bị người dùng, và còn thực hiện việc chuyển tiếp thông tin điều khiển và/hoặc thông tin dữ liệu giữa thiết bị người dùng và mạng lõi (Core Network - CN). Thiết bị mạng truy cập theo phương án này của sáng chế là thiết bị cung cấp chức năng truyền thông không dây cho thiết bị đầu cuối, và cũng có thể được gọi là thiết bị mạng. Ví dụ, thiết bị mạng truy cập có thể bao gồm NodeB thế hệ tiếp theo (Next Generation Node Basestation - gNB) trong hệ thống 5G, NodeB cải tiến (evolved NodeB - eNB) trong LTE (Long Term Evolution - phát triển lâu dài), bộ điều khiển mạng vô tuyến (Radio Network Controller - RNC), NodeB (nút B - NB), bộ điều khiển trạm gốc (Base Station Controller - BSC), trạm thu phát gốc (Base Transceiver Station - BTS), trạm gốc thường trú (ví dụ, NodeB cải tiến thường trú, hoặc nút B thường trú (Home Node B - HNB)), đơn vị băng gốc (Base Band Unit - BBU), điểm truyền nhận (Transmitting and Receiving Point - TRP), điểm truyền (Transmitting Point - TP), thiết bị tế bào nhỏ (pico), trung tâm chuyển mạch di động, thiết bị mạng trong mạng tương lai, v.v.. Có thể hiểu rằng chủng loại cụ thể của thiết bị mạng truy cập là không bị giới hạn theo phương án này của sáng chế. Trong các hệ thống sử dụng các công nghệ truy cập vô tuyến khác nhau, thì các thiết bị mà có chức năng của thiết bị mạng truy cập là có thể có các tên gọi khác nhau.

Chức năng mạng AMF (Access and Mobility Management Function - chức năng quản lý truy cập và quản lý tính di động) 130 là chủ yếu được sử dụng cho việc

quản lý tính di động, quản lý truy cập, v.v., và có thể được dùng để thực hiện các chức năng không phải là chức năng quản lý phiên trong các chức năng MME (Mobility Management Entity - thực thể quản lý tính di động), chẳng hạn chức năng ngăn chặn theo luật và chức năng cho phép/xác thực truy cập. Có thể hiểu rằng chức năng mạng AMF được gọi ngắn gọn là AMF sau đây.

Chức năng máy chủ xác thực (AUthentication Server Function - AUSF) 140 được dùng để xác thực các dịch vụ, tạo ra các khoá, và thực hiện việc xác thực hai chiều trên thiết bị người dùng; và hỗ trợ khung xác thực hợp nhất. Theo phương án này của sáng chế, thì chức năng máy chủ xác thực là chủ yếu được tạo cấu hình để thực hiện việc xác thực lẫn nhau giữa UE và mạng, và tạo ra khoá bảo mật để sử dụng trong thủ tục sau đó.

Chức năng ứng dụng (Application Function - AF) 150 được dùng để thực hiện việc định tuyến dữ liệu bị ảnh hưởng bởi ứng dụng, truy cập chức năng bộc lộ mạng 160, tương tác với khung chính sách để thực hiện việc điều khiển chính sách, v.v..

Chức năng bộc lộ mạng (Network Exposure Function - NEF) 160 được dùng để thu thập, phân tích, và tái lắp ráp các khả năng mạng, và mở các khả năng mạng. AF có thể truy cập mạng lõi 5G nhờ sử dụng NEF.

Chức năng mạng UDM (Unified Data Management - quản lý dữ liệu hợp nhất) 170 có thể được dùng để xử lý danh tính thiết bị người dùng, xác thực truy cập, đăng ký, quản lý tính di động, v.v.. Có thể hiểu rằng chức năng mạng UDM được gọi ngắn gọn là UDM sau đây.

Chức năng mạng SEAF (SEcurity Anchor Function - chức năng mỏ neo bảo mật) được dùng để chia sẻ khoá K_{SEAF} với UE, và khoá này được dùng để trích xuất khoá bất kỳ khác, ví dụ, khoá để bảo vệ mặt phẳng điều khiển và khoá để bảo vệ giao diện vô tuyến. Sau đó, giả định rằng SEAF nằm ở vị trí an toàn và rằng K_{SEAF} sẽ không bao giờ rời khỏi SEAF. Do đó, mỗi lần UE ở trạng thái không tải và sau đó được kích hoạt lại, thì UE có thể thực hiện việc truy cập nhờ sử dụng khoá được chia sẻ. Điều này tránh được việc xác thực lại. SEAF có thể được triển khai độc lập, hoặc có thể cùng được triển khai với chức năng mạng AMF 130.

Để cho việc mô tả được dễ dàng, thì theo các phương án của sáng chế, chức năng mạng AMF (Access and Mobility management Function - chức năng quản lý truy cập và quản lý tính di động) 130 được lấy làm ví dụ để mô tả. Ngoài ra, chức năng mạng

AMF 130 được gọi ngắn gọn là AMF, và thiết bị đầu cuối 110 được gọi là UE. Nói cách khác, theo các phương án của sáng chế, thì tất cả các AMF được mô tả dưới đây là có thể được thay thế bằng chức năng mạng quản lý truy cập và quản lý tính di động, và tất cả các UE là có thể được thay thế bằng thiết bị đầu cuối.

Fig.2 là hình vẽ thể hiện sơ đồ kiến trúc khoá AKMA theo một phương án của sáng chế. Như được thể hiện trên Fig.2, UE và phía mạng thực hiện việc xác thực sơ cấp, và tạo ra khoá bảo mật để sử dụng trong thủ tục sau đó. Việc xác thực sơ cấp này còn bao gồm AMF/SEAF, AUSF, và UDM mà là ở phía mạng (theo sáng chế, AMF/SEAF biểu thị AMF, SEAF, hoặc SEAF và AMF). Khoá bảo mật được tạo ra trong tiến trình xác thực sơ cấp là bao gồm K_{AUSF} mà là khoá được chia sẻ giữa AUSF và UE. Ngoài ra, mỗi trong số UE và AUSF có thể còn tạo ra khoá AKMA K_{AKMA}, để UE và AF thực hiện, dựa trên K_{AF} mà được tạo ra dựa trên K_{AKMA}, việc bảo vệ lưu lượng giữa UE và AF. Ngoài ra, KID là bộ nhận dạng khoá duy nhất tương ứng với K_{AKMA}.

Sau khi UE và AUSF thu thập riêng biệt K_{AKMA} và KID, thì xem Fig.3. Fig.3 là hình vẽ thể hiện sơ đồ thương lượng khoá khi UE truy cập AF theo một phương án của sáng chế. Như được thể hiện trên Fig.3, UE khởi tạo thông điệp yêu cầu phiên dịch vụ đến AF. Thông điệp yêu cầu phiên dịch vụ này bao gồm KID. Sau khi nhận được thông điệp yêu cầu phiên dịch vụ, thì AF gửi thông điệp yêu cầu khoá ứng dụng đến AAnF để thu thập K_{AF}, trong đó thông điệp yêu cầu khoá ứng dụng này cũng bao gồm KID nhận được. Sau khi nhận được yêu cầu khoá ứng dụng, thì AAnF kiểm tra xem K_{AF} được tạo ra dựa trên K_{AKMA} tương ứng với KID này có tồn tại cục bộ hay không. Nếu K_{AF} này tồn tại, thì AAnF gửi K_{AF} này đến AF. Nếu K_{AF} này không tồn tại, thì AAnF kiểm tra xem K_{AKMA} tương ứng với KID này có tồn tại cục bộ hay không. Nếu K_{AKMA} này tồn tại, thì AAnF tạo ra K_{AF} dựa trên K_{AKMA} này, và gửi K_{AF} này đến AF. Nếu K_{AKMA} này không tồn tại, thì AAnF gửi thông điệp yêu cầu khoá AKMA đến AUSF, trong đó thông điệp yêu cầu khoá AKMA này mang KID nhận được. Sau khi nhận được thông điệp yêu cầu khoá AKMA mang KID này, thì AUSF trả về K_{AKMA} tương ứng với KID này cho AAnF. AAnF thu thập K_{AF} thông qua việc tính toán dựa trên K_{AKMA} nhận được và gửi K_{AF} này đến AF. Theo cách này, thì AF và UE có thể bảo vệ hoạt động truyền thông dựa trên K_{AF}.

Có thể thấy từ những phần mô tả tương ứng với Fig.2 và Fig.3 rằng mỗi trong số UE và AUSF đều cần phải thu thập K_{AKMA} và KID, và trước khi tạo ra K_{AF} dựa trên

K_{AKMA} và KID này, thì cần xác định rằng K_{AKMA} và KID này là được tạo ra ở mỗi trong số UE và AUSF. Để giải quyết vấn đề này, thì xem Fig.4A. Fig.4A là hình vẽ thể hiện lưu đồ của phương pháp thu thập khoá theo một phương án của sáng chế. Như được thể hiện trên Fig.4A, phương pháp này bao gồm các bước sau đây.

401: AUSF thu thập khoá mỏ neo của tiến trình xác thực và quản lý khoá dành cho các ứng dụng K_{AKMA} và/hoặc bộ nhận dạng khoá KID duy nhất của K_{AKMA}.

Phương pháp thu thập K_{AKMA} và/hoặc KID bởi AUSF có thể là AUSF tạo ra K_{AKMA} và/hoặc KID sau khi thu thập các thông số liên quan để tạo ra K_{AKMA}, ví dụ, K_{AUSF}.

Theo cách khác, phương pháp thu thập K_{AKMA} và/hoặc KID bởi AUSF có thể là thu thập KID từ AMF/SEAF, và sau đó tạo ra K_{AKMA} bởi AUSF dựa trên KID này.

Theo cách khác, phương pháp thu thập K_{AKMA} và/hoặc KID bởi AUSF có thể là thu thập thông tin chỉ thị thứ hai từ AMF/SEAF, trong đó thông tin chỉ thị thứ hai này được dùng để chỉ thị cho AUSF tạo ra K_{AKMA} và/hoặc KID. AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin chỉ thị thứ hai này.

Theo cách khác, phương pháp thu thập K_{AKMA} và/hoặc KID bởi AUSF có thể là thu thập thông tin chỉ thị thứ ba hoặc thông tin cho phép thứ nhất từ UDM, trong đó thông tin chỉ thị thứ ba này được dùng để chỉ thị cho AUSF tạo ra K_{AKMA} và/hoặc KID, và thông tin cho phép thứ nhất này được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ AKMA. AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin chỉ thị thứ ba hoặc thông tin cho phép thứ nhất này.

Theo sáng chế, thì thông tin chỉ thị thứ ba và thông tin cho phép thứ nhất biểu diễn nội dung giống nhau, và có thể được sử dụng luân phiên. Có thể coi rằng thông tin chỉ thị thứ ba là thông tin cho phép thứ nhất.

Việc AUSF thu thập KID hoặc thông tin chỉ thị thứ hai từ AMF/SEAF có thể là việc AUSF nhận thông điệp thứ nhất được gửi bởi AMF/SEAF, trong đó thông điệp thứ nhất này bao gồm KID hoặc thông tin chỉ thị thứ hai này.

Việc AUSF thu thập thông tin chỉ thị thứ ba hoặc thông tin cho phép thứ nhất từ UDM có thể là việc AUSF nhận thông điệp thứ ba được gửi bởi UDM, trong đó thông điệp thứ ba này bao gồm thông tin chỉ thị thứ ba hoặc thông tin cho phép thứ nhất này.

402: AUSF gửi thông tin chỉ thị thứ tư hoặc KID đến AMF/SEAF, trong đó thông tin chỉ thị thứ tư này được dùng để chỉ thị cho UE tạo ra K_{AKMA} và/hoặc KID.

Việc AUSF gửi thông tin chỉ thị thứ tư hoặc KID đến AMF/SEAF có thể là việc AUSF gửi thông điệp thứ tư đến AMF/SEAF, trong đó thông điệp thứ tư này bao gồm thông tin chỉ thị thứ tư hoặc KID này.

403: Sau khi nhận được thông tin chỉ thị thứ tư hoặc KID này, thì AMF/SEAF gửi KID nhận được hoặc thông tin chỉ thị thứ năm đến UE, trong đó thông tin chỉ thị thứ năm này được dùng để chỉ thị cho UE tạo ra K_{AKMA} và/hoặc KID này.

Việc AMF/SEAF gửi KID hoặc thông tin chỉ thị thứ năm đến UE có thể là việc AMF/SEAF gửi thông điệp thứ năm đến UE, trong đó thông điệp thứ năm này bao gồm KID hoặc thông tin chỉ thị thứ năm này.

Nếu UE nhận được KID này, thì UE lưu giữ KID này và tạo ra K_{AKMA}. Nếu UE nhận được thông tin chỉ thị thứ năm, thì UE tạo ra KID và/hoặc K_{AKMA} này.

Cụ thể là, xem Fig.4B. Fig.4B là hình vẽ thể hiện lưu đồ của phương pháp thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế. Như được thể hiện trên Fig.4B, theo phương pháp này, thì AUSF nhận thông điệp thứ nhất từ AMF/SEAF. Thông điệp thứ nhất này là thông điệp yêu cầu dịch vụ xác thực trong tiến trình xác thực sơ cấp, và thông điệp thứ nhất này bao gồm KID hoặc thông tin chỉ thị thứ hai. AUSF thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất này, KID trong thông điệp thứ nhất này, hoặc thông tin chỉ thị thứ nhất trong thông điệp thứ nhất này. Các bước sau đây được bao gồm cụ thể.

411: UE gửi thông điệp yêu cầu đăng ký đến AMF/SEAF, trong đó thông điệp yêu cầu đăng ký này bao gồm KID hoặc thông tin chỉ thị thứ nhất.

Trước khi gửi KID, thì UE tạo ra KID.

412: AMF/SEAF gửi thông điệp thứ nhất đến AUSF. Theo phương án này, thì thông điệp thứ nhất là thông điệp yêu cầu dịch vụ xác thực, ví dụ, Nausf_UEAuthentication_Authenticate Request. Thông điệp thứ nhất này bao gồm KID hoặc thông tin chỉ thị thứ hai. Tương ứng theo đó, AUSF nhận thông điệp thứ nhất này.

Nếu AMF/SEAF nhận được KID này, thì AMF/SEAF bao gồm KID này trong thông điệp thứ nhất này. Nếu AMF/SEAF nhận được thông tin chỉ thị thứ nhất, thì AMF/SEAF bao gồm thông tin chỉ thị thứ hai trong thông điệp thứ nhất.

Thông tin chỉ thị thứ nhất và thông tin chỉ thị thứ hai có thể là các thông tin chỉ thị giống nhau hoặc các thông tin chỉ thị khác nhau.

413: AUSF gửi thông điệp yêu cầu dịch vụ xác thực (ví dụ, Nudm_UEAuthentication_Get Request), mà được dùng để yêu cầu vectơ xác thực của UE, đến UDM. Tương ứng theo đó, UDM nhận yêu cầu dịch vụ xác thực này.

414: UDM gửi vectơ xác thực đến AUSF. AUSF nhận vectơ xác thực được gửi bởi UDM.

415: AUSF tạo ra K_{AKMA} và/hoặc KID, hoặc tạo ra K_{AKMA} dựa trên KID được bao gồm trong thông điệp thứ nhất, hoặc tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin chỉ thị thứ hai được bao gồm trong thông điệp thứ nhất.

AUSF có thể tạo ra K_{AKMA} và/hoặc KID tại thời điểm bất kỳ sau khi AUSF nhận được vectơ xác thực được gửi bởi UDM. Điều này không bị giới hạn theo sáng chế.

Trong một số trường hợp, như được thể hiện trên Fig.4B, thông điệp thứ nhất mà được gửi bởi AMF/SEAF đến AUSF là bao gồm thông tin chỉ thị thứ hai, và thông tin chỉ thị thứ hai này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây:

việc AUSF tạo ra K_{AKMA} và/hoặc KID; việc UE hỗ trợ chức năng AKMA; việc UE yêu cầu tạo ra K_{AKMA} và/hoặc KID; việc UE có khả năng sử dụng chức năng AKMA; và việc UE có khả năng sử dụng dịch vụ 3GPP (3rd Generation Partnership Project - dự án hợp tác thế hệ thứ ba).

Theo sáng chế, thì "dịch vụ 3GPP", "ứng dụng 3GPP", "ứng dụng", và "dịch vụ" đều biểu thị cùng một ý nghĩa, và có thể được sử dụng luân phiên.

Thông điệp yêu cầu đăng ký mà được gửi bởi UE đến AMF/SEAF là bao gồm thông tin chỉ thị thứ nhất, và thông tin chỉ thị thứ nhất này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây:

việc AUSF tạo ra K_{AKMA} và/hoặc KID; việc UE hỗ trợ chức năng AKMA; việc UE yêu cầu tạo ra K_{AKMA} và/hoặc KID; việc UE có khả năng sử dụng dịch vụ AKMA; và việc UE có khả năng sử dụng dịch vụ 3GPP (3rd Generation Partnership Project - dự án hợp tác thế hệ thứ ba).

Trong các trường hợp khác, như được thể hiện trên Fig.4B, thông điệp thứ nhất mà được gửi bởi AMF/SEAF đến AUSF là bao gồm KID, và KID này có thể được tạo ra bởi UE và được gửi đến AMF/SEAF nhờ sử dụng thông điệp yêu cầu đăng ký này. AMF/SEAF gửi KID nhận được đến AUSF, và AUSF tạo ra K_{AKMA} dựa trên KID

này.

Sau khi nhận được thông điệp yêu cầu đăng ký được gửi bởi UE, thì AMF/SEAF yêu cầu dịch vụ xác thực từ AUSF, cụ thể là, AMF/SEAF gửi thông điệp thứ nhất đến AUSF. Sau khi nhận được thông điệp thứ nhất được gửi bởi AMF/SEAF, thì AUSF yêu cầu dịch vụ xác thực từ UDM. Sau khi nhận được thông điệp yêu cầu dịch vụ xác thực từ AUSF, thì UDM chọn phương pháp xác thực, tạo ra vectơ xác thực của UE, và gửi vectơ xác thực của UE đến AUSF.

Vectơ xác thực này có thể bao gồm số ngẫu nhiên (RANDom number - RAND), thẻ bài xác thực (AUthentication TokeN - AUTN), khoá mật mã trung gian (intermediate Cipher Key - CK'), khoá toàn vẹn trung gian (intermediate Integrity Key - IK'), và đáp ứng được kỳ vọng (eXpected RESponse - XRES). Ở vectơ xác thực, thì khoá mật mã trung gian CK' là được tạo ra dựa trên khoá mật mã (Cipher Key/Encryption Key - CK) và khoá toàn vẹn (Integrity Key - IK), và khoá toàn vẹn trung gian IK' cũng được tạo ra dựa trên khoá mật mã và khoá toàn vẹn này. AUTN bao gồm phép toán HOẶC loại trừ (exclusive OR) của số tuần tự (Sequence Number - SQN) và khoá ẩn danh (Anonymity Key - AK) (tức là, SQN xor AK), trường quản lý xác thực (Authentication Management Field - AMF), và mã xác thực thông điệp (Message Authentication Code - MAC) được tạo ra bởi khoá dài hạn (K), RAND, SQN, và AMF. Một phần của vectơ xác thực là một hoặc nhiều phần bất kỳ trong số các phần sau đây: RAND, AUTN, CK, IK, CK', IK', XRES, AK, AMF, K, SQN, và MAC. CK, IK, AK, và XRES là được tạo ra dựa trên khoá dài hạn (K) và số ngẫu nhiên (RAND). Theo cách khác, phần đó của vectơ xác thực có thể là kết quả của phép toán bất kỳ được thực hiện trên một hoặc nhiều phần bất kỳ trong số RAND, AUTN, CK, IK, CK', IK', XRES, AK, AMF, K, SQN, và MAC. Phép toán này bao gồm, nhưng không chỉ giới hạn ở, phép toán HOẶC loại trừ, phép toán nối, phép toán băm, v.v..

Theo cách khác, vectơ xác thực có thể bao gồm: RAND, AUTN, K_{AUSF}, và đáp ứng được kỳ vọng 5G AKA (Authentication and Key Agreement (xác thực và thoả thuận khoá) Expected Response - XRES*). Ở vectơ xác thực, thì AUTN bao gồm phép toán HOẶC loại trừ của SQN và AK (tức là, SQN xor AK), AMF, và MAC mà được tạo ra dựa trên khoá dài hạn (K), RAND, SQN, và AMF. XRES* là được tạo ra dựa trên CK, IK, RAND, XRES, và tên mạng dịch vụ (Service Network name - SN name (tên SN)). K_{AUSF} là được tạo ra dựa trên CK, IK, SQN xor AK, và tên SN. Phần đó của vectơ

xác thực là một hoặc nhiều trong số các phần sau đây: RAND, AUTN, K_{AUSF}, XRES*, XRES, CK, IK, AK, AMF, K, SQN, MAC, và tên SN. Theo cách khác, phần đó của vectơ xác thực có thể là kết quả của phép toán bất kỳ được thực hiện trên một hoặc nhiều phần bất kỳ trong số RAND, AUTN, K_{AUSF}, XRES*, XRES, CK, IK, AK, AMF, K, SQN, MAC, và tên SN. Phép toán này bao gồm, nhưng không chỉ giới hạn ở, phép toán HOẶC loại trừ, phép toán nối, phép toán băm, v.v..

Sau khi thu được vectơ xác thực, thì AUSF thu thập K_{AUSF} từ vectơ xác thực, hoặc tạo ra K_{AUSF} dựa trên vectơ xác thực. AUSF tạo ra K_{AKMA} và/hoặc KID. Các thông số được dùng để tạo ra K_{AKMA} và/hoặc KID là bao gồm một hoặc nhiều thành phần bất kỳ trong số các thành phần sau đây:

thông số độ tươi, bao gồm, nhưng không chỉ giới hạn ở, số ngẫu nhiên (RAND), SQN, số đếm (Count), vectơ xác thực, phần nêu trên của vectơ xác thực, v.v.;

bộ nhận dạng của UE, bao gồm, nhưng không chỉ giới hạn ở, bộ nhận dạng đăng ký cố định (SUbscription Permanent Identifier - SUPI), bộ nhận dạng tạm thời duy nhất toàn cầu 5G (5G Globally Unique Temporary Identifier - 5G-GUTI), bộ nhận dạng đăng ký ẩn (SUbscription Concealed Identifier - SUCI), bộ nhận dạng đăng ký công khai chung (Generic Public Subscription Identifier - GPSI), v.v.;

khoá được chia sẻ giữa UE và phía mạng, bao gồm, nhưng không chỉ giới hạn ở, K_{AUSF}, K_{AKMA}, khoá mật mã CK, khoá toàn vẹn IK, khoá ẩn danh AK, khoá dài hạn K, và khoá được tạo ra bởi một hoặc nhiều thành phần bất kỳ trong số K_{AUSF}, K_{AKMA}, CK, IK, AK, và K, ví dụ, khoá SEAF K_{SEAF}, trong đó K_{SEAF} này là được tạo ra dựa trên K_{AUSF};

khoá công khai và khoá bí mật, bao gồm, nhưng không chỉ giới hạn ở, khoá công khai của UE, khoá bí mật của UE, khoá công khai của mạng thường trú của UE, khoá bí mật của mạng thường trú của UE, v.v.; và

thông tin định tuyến của AUSF, bao gồm, nhưng không chỉ giới hạn ở, bộ nhận dạng mạng di động đất liền công cộng (Public Land Mobile Network IDentifier - PLMN ID), mã quốc gia di động (Mobile Country Code - MCC), mã mạng di động (Mobile Network Code - MNC), bộ chỉ thị định tuyến (Routing Indicator), bộ nhận dạng thực thể AUSF (AUSF Instance ID), bộ nhận dạng nhóm AUSF (AUSF Group ID), v.v..

Sau khi tạo ra K_{AKMA} và/hoặc KID, thì AUSF gửi K_{AKMA} được tạo ra và/hoặc KID được tạo ra đến AAnF.

Sau khi tạo ra KID, thì AUSF có thể gửi KID được tạo ra đến AMF/SEAF (xem số chỉ dẫn 416 trên Fig.4B), và AMF/SEAF gửi KID nhận được đến UE (xem số chỉ dẫn 417 trên Fig.4B). AUSF có thể gửi KID này đến AMF/SEAF bằng cách gửi thông điệp thứ tư đến AMF/SEAF, trong đó thông điệp thứ tư này bao gồm KID này. Theo phương án này, thì thông điệp thứ tư là thông điệp đáp ứng dịch vụ xác thực, ví dụ, Nausf_UEAuthentication_Authenticate Response. AMF/SEAF có thể gửi KID này đến UE bằng cách gửi thông điệp thứ năm đến UE, trong đó thông điệp thứ năm này bao gồm KID này. Theo phương án này, thì thông điệp thứ năm này là thông điệp yêu cầu xác thực. Sau khi nhận được KID này, thì UE lưu giữ KID này và tạo ra K_{AKMA}.

Sau khi tạo ra KID và/hoặc K_{AKMA}, thì AUSF có thể gửi thông tin chỉ thị thứ tư đến AMF/SEAF (xem số chỉ dẫn 416 trên Fig.4B). Thông tin chỉ thị thứ tư này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: được dùng để chỉ thị cho AMF/SEAF gửi, đến UE, thông tin chỉ thị mà được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}; được dùng để thông báo cho UE rằng AUSF tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị rằng UE có khả năng sử dụng chức năng AKMA; được dùng để chỉ thị rằng phía mạng hỗ trợ chức năng AKMA; và được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ. AUSF có thể gửi thông tin chỉ thị thứ tư đến AMF/SEAF bằng cách gửi thông điệp thứ tư đến AMF/SEAF, trong đó thông điệp thứ tư này bao gồm thông tin chỉ thị thứ tư này. Theo phương án này, thì thông điệp thứ tư là thông điệp đáp ứng dịch vụ xác thực, ví dụ, Nausf_UEAuthentication_Authenticate Response. Sau khi nhận được thông tin chỉ thị thứ tư này, thì AMF/SEAF gửi thông tin chỉ thị thứ năm đến UE (xem số chỉ dẫn 417 trên Fig.4B). Thông tin chỉ thị thứ năm này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}; được dùng để thông báo cho UE rằng AUSF tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị rằng UE có khả năng sử dụng chức năng AKMA; được dùng để chỉ thị rằng phía mạng hỗ trợ chức năng AKMA; và được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ. AMF/SEAF có thể gửi thông tin chỉ thị thứ năm này đến UE nhờ sử dụng thông điệp thứ năm được gửi đến UE, trong đó thông điệp thứ năm này bao gồm thông tin chỉ thị thứ năm này. Sau khi nhận được thông điệp thứ năm hoặc thông tin chỉ thị thứ năm này, thì UE tạo ra KID và/hoặc K_{AKMA}. Thông tin chỉ thị thứ tư và thông tin chỉ thị thứ năm có thể là các thông tin chỉ thị giống nhau hoặc các thông

tin chỉ thị khác nhau. Thông tin chỉ thị thứ tư và thông tin chỉ thị thứ năm có thể chỉ thị nội dung giống nhau hoặc nội dung khác nhau.

Theo sáng chế, thì UE tạo ra KID và/hoặc K_{AKMA} nhờ sử dụng các thông số và thuật toán giống như của AUSF. UE có thể tạo ra KID và/hoặc K_{AKMA} tại thời điểm bất kỳ sau khi nhận được thông điệp thứ năm hoặc thông tin chỉ thị thứ năm. Điều này không bị giới hạn theo sáng chế.

Theo phương án này của sáng chế, thì UE chủ động gửi KID hoặc thông tin chỉ thị thứ nhất đến AMF/SEAF, AMF/SEAF chuyển tiếp KID này đến AUSF hoặc gửi thông tin chỉ thị thứ hai đến AUSF dựa trên thông tin chỉ thị thứ nhất, và sau đó AUSF thu thập KID này hoặc tạo ra KID này và/hoặc K_{AKMA} dựa trên thông tin chỉ thị thứ hai. Trong tiến trình này, thì KID và/hoặc K_{AKMA} có thể được tạo ra dựa trên yêu cầu của UE. Theo cách này, thì KID và/hoặc K_{AKMA} là được tạo ra dựa trên yêu cầu. Điều này tránh việc tạo ra KID không cần thiết và/hoặc K_{AKMA} không cần thiết và giảm bớt việc lưu giữ và quản lý KID và/hoặc K_{AKMA}.

Trong một số trường hợp, thì AUSF khởi tạo chỉ thị thu thập sự cho phép đến UDM, để thu thập thông tin cho phép thứ nhất của UE. Sau đó, AUSF tạo ra K_{AKMA} và/hoặc KID tương ứng với UE dựa trên thông tin cho phép thứ nhất thu được.

Fig.4C là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập K_{AKMA} và/hoặc KID theo một phương án của sáng chế. Theo phương pháp này, thì AUSF nhận thông điệp thứ nhất từ AMF/SEAF. Theo phương án này, thì thông điệp thứ nhất là thông điệp yêu cầu dịch vụ xác thực (ví dụ, Nausf_UEAuthentication_Authenticate Request). Sau khi nhận được thông điệp thứ nhất, thì AUSF gửi thông điệp thứ hai đến UDM. Theo phương án này của sáng chế, thì thông điệp thứ hai là thông điệp yêu cầu dịch vụ xác thực (ví dụ, Nudm_UEAuthentication_Get Request), và được dùng để yêu cầu vectơ xác thực của UE từ UDM. Thông điệp thứ hai này bao gồm chỉ thị thu thập sự cho phép, và được AUSF dùng để thu thập thông tin cho phép thứ nhất từ UDM, để xác định xem UE có sự cho phép thứ nhất hay không. Nếu UE có sự cho phép thứ nhất, thì KID và/hoặc K_{AKMA} là được tạo ra. Các bước sau đây được bao gồm cụ thể.

421: UE gửi thông điệp yêu cầu đăng ký đến AMF/SEAF. Tương ứng theo đó, AMF/SEAF nhận thông điệp yêu cầu đăng ký được gửi bởi UE.

422: AMF/SEAF gửi yêu cầu dịch vụ xác thực (thông điệp thứ nhất) đến AUSF dựa trên thông tin yêu cầu đăng ký của UE, trong đó thông điệp thứ nhất mang

bộ nhận dạng của UE, SUCI, hoặc SUPI. Tương ứng theo đó, AUSF nhận thông điệp thứ nhất này.

423: AUSF gửi thông điệp thứ hai đến UDM. Theo phương án này, thì thông điệp thứ hai này là thông điệp yêu cầu dịch vụ xác thực. AUSF bao gồm, trong thông điệp thứ hai, chỉ thị yêu cầu sự cho phép, và chỉ thị yêu cầu sự cho phép này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: được dùng để chỉ thị yêu cầu tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị yêu cầu sử dụng dịch vụ AKMA; được dùng để chỉ thị yêu cầu sử dụng dịch vụ 3GPP; được dùng để chỉ thị rằng UE hỗ trợ chức năng AKMA; được dùng để chỉ thị rằng AUSF hỗ trợ chức năng AKMA; được dùng để chỉ thị yêu cầu truy vấn xem UE có sự cho phép thứ nhất hay không. Sự cho phép thứ nhất là một hoặc nhiều việc bất kỳ trong số những việc sau đây: UE hỗ trợ chức năng AKMA; UE có khả năng sử dụng dịch vụ 3GPP; UE có khả năng sử dụng chức năng AKMA; và KID và/hoặc K_{AKMA} có thể được tạo ra cho UE. Tương ứng theo đó, UDM nhận thông điệp thứ hai bao gồm chỉ thị yêu cầu sự cho phép này. UDM thu thập thông tin cho phép thứ nhất dựa trên chỉ thị yêu cầu sự cho phép này.

424: UDM gửi thông điệp đáp ứng thứ hai đến AUSF.

Theo phương án này, thì thông điệp đáp ứng thứ hai này là thông điệp đáp ứng dịch vụ xác thực. Thông điệp đáp ứng thứ hai này bao gồm thông tin cho phép thứ nhất, và thông tin cho phép thứ nhất này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc UE có khả năng sử dụng AKMA; việc KID và/hoặc K_{AKMA} được tạo ra cho UE; việc UE có khả năng sử dụng dịch vụ 3GPP; và việc UE hỗ trợ AKMA.

425: AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất hoặc thông điệp đáp ứng thứ hai.

Các thông số được dùng để tạo ra K_{AKMA} và/hoặc KID là được mô tả trên Fig.4B, và các chi tiết không được mô tả lại ở đây.

AUSF có thể tạo ra K_{AKMA} và/hoặc KID tại thời điểm bất kỳ sau khi nhận được thông tin cho phép thứ nhất hoặc thông điệp đáp ứng thứ hai. Điều này không bị giới hạn theo sáng chế.

Sau khi nhận được chỉ thị yêu cầu sự cho phép, thì UDM trả về thông tin cho phép thứ nhất cho AUSF dựa trên dữ liệu liên quan của UE.

Trong một số trường hợp, thì AUSF có thể gửi chỉ thị yêu cầu sự cho phép

đến UDM dựa trên một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc AUSF nhận thông điệp thứ nhất được gửi bởi AMF/SEAF; và việc AUSF nhận thông điệp thứ nhất được gửi bởi AMF/SEAF, trong đó thông điệp thứ nhất này bao gồm thông tin chỉ thị thứ hai hoặc KID. Trong trường hợp này, khi AMF/SEAF gửi thông điệp thứ nhất đến AUSF, thì thông điệp thứ nhất này bao gồm thông tin chỉ thị thứ hai hoặc KID. Việc AMF/SEAF gửi thông tin chỉ thị thứ hai, KID, thông điệp thứ nhất bao gồm thông tin chỉ thị thứ hai, hoặc thông điệp thứ nhất bao gồm KID đến AUSF có thể là dựa trên việc AMF/SEAF nhận thông tin chỉ thị thứ nhất hoặc KID được gửi bởi UE. Trong trường hợp này, UE gửi thông điệp yêu cầu đăng ký đến AMF/SEAF, trong đó thông điệp yêu cầu đăng ký này mang thông tin chỉ thị thứ nhất hoặc KID này. Về những phần mô tả của thông điệp thứ nhất, thông tin chỉ thị thứ hai, và thông tin chỉ thị thứ nhất, thì xem những phần mô tả trên Fig.4B. Các chi tiết không được mô tả lại ở đây.

Sau khi tạo ra K_{AKMA} và/hoặc KID, thì AUSF gửi K_{AKMA} được tạo ra và/hoặc KID được tạo ra đến AAnF.

426: Xem những phần mô tả của bước 416 trên Fig.4B, và các chi tiết không được mô tả lại ở đây.

427: Xem những phần mô tả của bước 417 trên Fig.4B, và các chi tiết không được mô tả lại ở đây.

Theo phương án này của sáng chế, thì AUSF chủ động gửi chỉ thị thu thập sự cho phép đến UDM, để thu thập thông tin cho phép thứ nhất, trong đó thông tin cho phép thứ nhất này được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ xác thực và quản lý khoá dành cho các ứng dụng (Authentication and Key MAnagement - AKMA). Sau đó, AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất thu được. Điều này có thể bảo đảm rằng việc tạo ra K_{AKMA} và/hoặc KID là được phép và tránh được việc tạo ra K_{AKMA} không được phép và/hoặc KID không được phép.

Theo phương án tuỳ ý, xem Fig.4D. Fig.4D là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế. Theo phương pháp này, thì AUSF nhận thông điệp thứ nhất từ AMF/SEAF. Thông điệp thứ nhất bao gồm KID hoặc thông tin chỉ thị thứ hai. Theo phương án này, thì thông điệp thứ nhất là yêu cầu dịch vụ xác thực (ví dụ, Nausf_UEAuthentication_Authenticate Request), và yêu cầu dịch vụ xác thực này bao gồm đáp ứng RES hoặc đáp ứng 5G AKA RES*. Sau khi nhận được thông điệp thứ nhất, thì AUSF gửi thông điệp thứ hai

đến UDM. Theo phương án này, thông điệp thứ hai là thông điệp yêu cầu xác nhận kết quả xác thực (ví dụ, Nudm_UEAuthentication_ResultConfirmation Request). Thông điệp thứ hai có thể bao gồm chỉ thị thu thập sự cho phép, và được AUSF dùng để thu thập thông tin cho phép thứ nhất từ UDM và tạo ra KID và/hoặc K_{AKMA} dựa trên thông tin cho phép thứ nhất. Như được thể hiện trên Fig.4D, phương pháp này bao gồm các bước sau đây.

431: UE gửi thông điệp đáp ứng xác thực đến AMF/SEAF, trong đó thông điệp đáp ứng xác thực này mang đáp ứng RES hoặc RES*, và thông điệp đáp ứng xác thực này bao gồm KID hoặc thông tin chỉ thị thứ nhất. Tương ứng theo đó, AMF/SEAF nhận thông điệp đáp ứng xác thực mà được gửi bởi UE và bao gồm KID hoặc thông tin chỉ thị thứ nhất. UE tạo ra KID trước khi gửi KID.

432: AMF/SEAF gửi thông điệp thứ nhất đến AUSF. Thông điệp thứ nhất này bao gồm đáp ứng xác thực RES hoặc RES* nhận được. Nếu AMF/SEAF nhận được KID này từ UE, thì AMF/SEAF bao gồm KID này trong thông điệp thứ nhất này. Nếu AMF/SEAF nhận được thông tin chỉ thị thứ nhất từ UE, thì AMF/SEAF bao gồm thông tin chỉ thị thứ hai trong thông điệp thứ nhất. Theo phương án này, thì thông điệp thứ nhất này là thông điệp yêu cầu dịch vụ xác thực.

Tương ứng theo đó, AUSF nhận thông điệp thứ nhất mà được gửi bởi AMF/SEAF và bao gồm KID hoặc thông tin chỉ thị thứ hai.

433: AUSF xác minh RES hoặc RES* nhận được.

434: Sau khi việc xác minh thành công, thì AUSF tạo ra K_{AKMA} và/hoặc KID. Theo cách khác, sau khi việc xác minh thành công, thì AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin chỉ thị thứ hai hoặc KID. Các thông số được AUSF dùng để tạo ra K_{AKMA} và/hoặc KID là được mô tả trên Fig.4B, và các chi tiết không được mô tả lại ở đây.

AUSF có thể tạo ra K_{AKMA} và/hoặc KID tại thời điểm bất kỳ sau khi AUSF xác minh thành công RES hoặc RES*. Điều này không bị giới hạn theo sáng chế.

Khi UE gửi, đến AMF/SEAF, thông điệp đáp ứng xác thực mà mang đáp ứng RES hoặc RES*, thì thông điệp này bao gồm thông tin chỉ thị thứ nhất hoặc KID. Thông tin chỉ thị thứ nhất được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc AUSF tạo ra K_{AKMA} và/hoặc KID; việc UE hỗ trợ chức năng AKMA; việc UE yêu cầu tạo ra K_{AKMA} và/hoặc KID; việc UE có khả năng sử dụng dịch vụ AKMA;

và việc UE có khả năng sử dụng dịch vụ 3GPP (3rd Generation Partnership Project - dự án hợp tác thế hệ thứ ba).

Sau khi nhận được thông điệp đáp ứng xác thực được gửi bởi UE, thì AMF/SEAF gửi thông điệp thứ nhất đến AUSF. Thông điệp thứ nhất này bao gồm KID hoặc thông tin chỉ thị thứ hai. Thông tin chỉ thị thứ hai được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc AUSF tạo ra K_{AKMA} và/hoặc KID; việc UE hỗ trợ chức năng AKMA; việc UE yêu cầu tạo ra K_{AKMA} và/hoặc KID; việc UE có khả năng sử dụng dịch vụ AKMA; và việc UE có khả năng sử dụng dịch vụ 3GPP (3rd Generation Partnership Project - dự án hợp tác thế hệ thứ ba).

Thông tin chỉ thị thứ nhất và thông tin chỉ thị thứ hai có thể là các thông tin chỉ thị giống nhau hoặc các thông tin chỉ thị khác nhau.

Sau khi việc xác minh trên đáp ứng RES hoặc RES* thành công, thì AUSF tạo ra K_{AKMA} và/hoặc KID, hoặc tạo ra K_{AKMA} dựa trên KID nhận được, hoặc tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin chỉ thị thứ hai nhận được hoặc thông điệp thứ nhất nhận được.

Theo cách khác, như được thể hiện trên Fig.4D, phương pháp này có thể còn bao gồm các bước sau đây.

434: Sau khi xác minh RES hoặc RES*, thì AUSF gửi thông điệp thứ hai đến UDM, trong đó thông điệp thứ hai này bao gồm chỉ thị thu thập sự cho phép. Thông điệp thứ hai này có thể là thông điệp yêu cầu xác nhận kết quả xác thực. Tương ứng theo đó, UDM nhận thông điệp thứ hai bao gồm chỉ thị thu thập sự cho phép này. Chỉ thị thu thập sự cho phép này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: yêu cầu tạo ra KID và/hoặc K_{AKMA}; yêu cầu sử dụng dịch vụ AKMA; yêu cầu sử dụng dịch vụ 3GPP; việc UE hỗ trợ chức năng AKMA; việc AUSF hỗ trợ chức năng AKMA; và yêu cầu truy vấn xem UE có sự cho phép thứ nhất hay không. Sự cho phép thứ nhất là một hoặc nhiều việc bất kỳ trong số những việc sau đây: UE hỗ trợ chức năng AKMA; UE có khả năng sử dụng dịch vụ 3GPP; UE có khả năng sử dụng chức năng AKMA; và KID và/hoặc K_{AKMA} có thể được tạo ra cho UE. Tương ứng theo đó, UDM nhận thông điệp thứ hai bao gồm chỉ thị thu thập sự cho phép này.

435: UDM gửi thông tin cho phép thứ nhất đến AUSF dựa trên chỉ thị thu thập sự cho phép này, trong đó thông tin cho phép thứ nhất này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc UE có khả năng sử dụng

AKMA; việc KID và/hoặc K_{AKMA} có thể được tạo ra cho UE; việc UE đã đăng ký dịch vụ 3GPP; và việc UE hỗ trợ AKMA. Tương ứng theo đó, AUSF nhận thông tin cho phép thứ nhất từ UDM. UDM gửi thông tin cho phép thứ nhất đến AUSF, và đáp ứng thông điệp thứ hai mà được gửi đến AUSF là có thể bao gồm thông tin cho phép thứ nhất. Đáp ứng thông điệp thứ hai này có thể là thông điệp đáp ứng xác nhận kết quả xác thực (ví dụ, Nudm_UEAuthentication_ResultConfirmation Response).

436: AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất nhận được. Phương pháp và các thông số được AUSF dùng để tạo ra K_{AKMA} và/hoặc KID là được mô tả trên Fig.4B, và các chi tiết không được mô tả lại ở đây.

AUSF có thể tạo ra K_{AKMA} và/hoặc KID tại thời điểm bất kỳ sau khi AUSF thu thập thông tin cho phép thứ nhất. Điều này không bị giới hạn theo sáng chế.

Sau khi tạo ra K_{AKMA} và/hoặc KID, thì AUSF gửi K_{AKMA} được tạo ra và/hoặc KID được tạo ra đến AAnF.

Sau khi tạo ra KID, thì AUSF có thể gửi KID được tạo ra đến AMF/SEAF (xem số chỉ dẫn 437 trên Fig.4D), và AMF/SEAF gửi KID nhận được đến UE (xem số chỉ dẫn 438 trên Fig.4D). AUSF có thể gửi KID này đến AMF/SEAF bằng cách gửi thông điệp thứ tư đến AMF/SEAF, trong đó thông điệp thứ tư này bao gồm KID này. Theo phương án này, thì thông điệp thứ tư là thông điệp đáp ứng dịch vụ xác thực, ví dụ, Nausf_UEAuthentication_Authenticate Response. AMF/SEAF có thể gửi KID này đến UE bằng cách gửi thông điệp thứ năm đến UE, trong đó thông điệp thứ năm này bao gồm KID này. Theo phương án này, thì thông điệp thứ năm là thông điệp N1 (ví dụ, thông điệp kết quả xác thực hoặc thông điệp lệnh chế độ bảo mật tầng không truy cập). Sau khi nhận được KID này, thì UE lưu giữ KID này và tạo ra K_{AKMA}.

Sau khi tạo ra KID và/hoặc K_{AKMA}, thì AUSF có thể gửi thông tin chỉ thị thứ tư đến AMF/SEAF (xem số chỉ dẫn 437 trên Fig.4D). Thông tin chỉ thị thứ tư này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: được dùng để chỉ thị cho AMF/SEAF gửi, đến UE, thông tin chỉ thị mà được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}; được dùng để thông báo cho UE rằng AUSF tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị rằng UE có khả năng sử dụng chức năng AKMA; được dùng để chỉ thị rằng phía mạng hỗ trợ chức năng AKMA; và được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ. AUSF có thể gửi thông tin chỉ thị thứ tư đến AMF/SEAF bằng cách gửi thông

điệp thứ tư đến AMF/SEAF, trong đó thông điệp thứ tư này bao gồm thông tin chỉ thị thứ tư này. Theo phương án này, thì thông điệp thứ tư là thông điệp đáp ứng dịch vụ xác thực, ví dụ, Nausf_UEAuthentication_Authenticate Response. Sau khi nhận được thông tin chỉ thị thứ tư này, thì AMF/SEAF gửi thông tin chỉ thị thứ năm đến UE (xem số chỉ dẫn 438 trên Fig.4D). Thông tin chỉ thị thứ năm này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}; được dùng để thông báo cho UE rằng AUSF tạo ra KID và/hoặc K_{AKMA}; được dùng để chỉ thị rằng UE có khả năng sử dụng chức năng AKMA; được dùng để chỉ thị rằng phía mạng hỗ trợ chức năng AKMA; và được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ. AMF/SEAF có thể gửi thông tin chỉ thị thứ năm này đến UE nhờ sử dụng thông điệp thứ năm được gửi đến UE, trong đó thông điệp thứ năm này bao gồm thông tin chỉ thị thứ năm này. Theo phương án này, thì thông điệp thứ năm là thông điệp N1 (ví dụ, thông điệp kết quả xác thực hoặc thông điệp lệnh chế độ bảo mật tầng không truy cập). Sau khi nhận được thông tin chỉ thị thứ năm hoặc thông điệp thứ năm, thì UE tạo ra KID và/hoặc K_{AKMA}. Thông tin chỉ thị thứ tư và thông tin chỉ thị thứ năm có thể là các thông tin chỉ thị giống nhau hoặc các thông tin chỉ thị khác nhau. Thông tin chỉ thị thứ tư và thông tin chỉ thị thứ năm có thể chỉ thị nội dung giống nhau.

Trong một số trường hợp, theo cách khác thì UDM có thể gửi thông điệp thứ ba đến AUSF, để kích hoạt AUSF tạo ra KID và/hoặc K_{AKMA}. Fig.4E là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế. Như được thể hiện trên Fig.4E, phương pháp này bao gồm các bước sau đây.

451: AUSF gửi thông điệp yêu cầu dịch vụ xác thực, ví dụ, Nudm_UEAuthentication_Get Request, đến UDM dựa trên yêu cầu dịch vụ xác thực nhận được, trong đó yêu cầu dịch vụ xác thực này được dùng để yêu cầu thu thập vectơ xác thực. Tương ứng theo đó, UDM nhận thông điệp yêu cầu dịch vụ xác thực này.

452: UDM gửi thông điệp thứ ba đến AUSF. UDM bao gồm thông tin cho phép thứ nhất trong thông điệp thứ ba này, và thông tin cho phép thứ nhất này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc UE có khả năng sử dụng AKMA; việc KID và/hoặc K_{AKMA} được tạo ra cho UE; việc UE có khả năng sử dụng dịch vụ 3GPP; và việc UE hỗ trợ AKMA. Theo phương án này, thì thông điệp thứ ba này là thông điệp đáp ứng dịch vụ xác thực, ví dụ, Nudm_UEAuthentication_Get Response.

Tương ứng theo đó, AUSF nhận thông điệp thứ ba mà được gửi bởi UDM và bao gồm thông tin cho phép thứ nhất.

453: AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất hoặc thông điệp thứ ba. Phương pháp và các thông số được AUSF dùng để tạo ra K_{AKMA} và/hoặc KID là được mô tả trên Fig.4B, và các chi tiết không được mô tả lại ở đây. AUSF có thể tạo ra K_{AKMA} và/hoặc KID tại thời điểm bất kỳ sau khi nhận được thông điệp thứ ba hoặc thông tin cho phép thứ nhất. Điều này không bị giới hạn theo sáng chế.

Sau khi tạo ra K_{AKMA} và/hoặc KID, thì AUSF gửi K_{AKMA} được tạo ra và/hoặc KID được tạo ra đến AAnF.

454: Xem những phần mô tả của bước 416 trên Fig.4B, và các chi tiết không được mô tả ở đây.

455: Xem những phần mô tả của bước 417 trên Fig.4B, và các chi tiết không được mô tả ở đây.

Theo phương án này của sáng chế, thì UDM chủ động thu thập thông tin cho phép thứ nhất của UE, và gửi thông tin cho phép thứ nhất này đến AUSF, để AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất này. Điều này bảo đảm rằng AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên sự cho phép và tránh việc tạo ra K_{AKMA} không được phép và/hoặc KID không được phép.

Theo cách khác, trong một số trường hợp, UDM cũng gửi thông tin cho phép thứ nhất đến AUSF, để kích hoạt AUSF tạo ra KID và/hoặc K_{AKMA}. Thông tin thứ ba mà được gửi bởi UDM đến AUSF là bao gồm thông tin cho phép thứ nhất, nhưng thông tin thứ ba này là thông tin đáp ứng xác nhận kết quả xác thực. Chi tiết xem Fig.4F. Fig.4F là hình vẽ thể hiện lưu đồ của phương pháp khác để thu thập KID và/hoặc K_{AKMA} theo một phương án của sáng chế. Như được thể hiện trên Fig.4F, phương pháp này bao gồm các bước sau đây.

461: AMF/SEAF gửi thông điệp yêu cầu dịch vụ xác thực, có mang RES hoặc RES*, đến AUSF. AUSF nhận thông điệp yêu cầu dịch vụ xác thực được gửi bởi AMF/SEAF này, và AUSF xác minh RES hoặc RES*.

462: AUSF gửi thông điệp yêu cầu xác nhận kết quả xác thực, ví dụ, Nudm_UEAuthentication_ ResultConfirmation Request, đến UDM, để thông báo cho UDM về kết quả xác thực của UE.

463: UDM gửi thông điệp thứ ba đến AUSF, trong đó thông điệp thứ ba này

bao gồm thông tin cho phép thứ nhất. Thông tin cho phép thứ nhất này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc UE có khả năng sử dụng AKMA; việc KID và/hoặc K_{AKMA} được tạo ra cho UE; việc UE có khả năng sử dụng dịch vụ 3GPP; và việc UE hỗ trợ chức năng AKMA. Theo phương án này, thì thông điệp thứ ba là thông điệp đáp ứng xác nhận kết quả xác thực, ví dụ, Nudm_UEAuthentication_ResultConfirmation Response. Tương ứng theo đó, AUSF nhận thông điệp thứ ba bao gồm thông tin cho phép thứ nhất này.

464: AUSF tạo ra K_{AKMA} và/hoặc KID dựa trên thông tin cho phép thứ nhất hoặc thông điệp thứ ba. Phương pháp và các thông số được AUSF dùng để tạo ra K_{AKMA} và/hoặc KID là được mô tả trên Fig.4B, và các chi tiết không được mô tả lại ở đây. AUSF có thể tạo ra K_{AKMA} và/hoặc KID tại thời điểm bất kỳ sau khi nhận được thông điệp thứ ba hoặc thông tin cho phép thứ nhất. Điều này không bị giới hạn theo sáng chế.

Sau khi tạo ra K_{AKMA} và/hoặc KID, thì AUSF gửi K_{AKMA} được tạo ra và/hoặc KID được tạo ra đến AAnF.

465: Xem những phần mô tả của bước 437 trên Fig.4D, và các chi tiết không được mô tả ở đây.

466: Xem những phần mô tả của bước 438 trên Fig.4D, và các chi tiết không được mô tả ở đây.

Theo các phương án trên Fig.4B đến Fig.4F, thì AMF/SEAF gửi KID hoặc thông tin chỉ thị thứ hai đến AUSF bằng cách gửi thông điệp thứ nhất đến AUSF, trong đó thông điệp thứ nhất này bao gồm thông tin chỉ thị thứ hai. Thông điệp thứ nhất này có thể là thông điệp yêu cầu dịch vụ xác thực. Cần lưu ý rằng loại của thông điệp thứ nhất là không chỉ giới hạn ở nội dung được đề cập ở các phương án nêu trên. Theo cách khác, thông điệp thứ nhất này có thể là thông điệp truyền thông hiện có bất kỳ khác giữa AMF/SEAF và AUSF, hoặc có thể là thông điệp truyền thông được thiết lập mới giữa AMF/SEAF và AUSF.

Theo các phương án trên Fig.4B đến Fig.4F, thì AUSF gửi chỉ thị thu thập sự cho phép đến UDM bằng cách gửi thông điệp thứ hai, trong đó thông điệp thứ hai này bao gồm chỉ thị thu thập sự cho phép này. Thông điệp thứ hai này có thể là thông điệp yêu cầu dịch vụ xác thực, hoặc có thể là thông điệp yêu cầu xác nhận kết quả xác thực. Cần lưu ý rằng loại của thông điệp thứ hai là không chỉ giới hạn ở nội dung được đề cập ở các phương án nêu trên. Theo cách khác, thông điệp thứ hai có thể là thông điệp truyền

thông hiện có bất kỳ khác giữa AUSF và UDM, hoặc có thể là thông điệp truyền thông được thiết lập mới giữa AUSF và the UDM.

Theo các phương án trên Fig.4B đến Fig.4F, thì UDM gửi thông tin cho phép thứ nhất đến AUSF bằng cách gửi thông điệp thứ ba đến UDM, trong đó thông điệp thứ ba này bao gồm thông tin cho phép thứ nhất này. Thông điệp thứ ba này có thể là thông điệp đáp ứng dịch vụ xác thực, hoặc có thể là thông điệp đáp ứng xác nhận kết quả xác thực. Cần lưu ý rằng loại của thông điệp thứ ba là không chỉ giới hạn ở nội dung được đề cập ở các phương án nêu trên. Theo cách khác, thông điệp thứ ba có thể là thông điệp truyền thông hiện có bất kỳ khác giữa UDM và AUSF, hoặc có thể là thông điệp truyền thông được thiết lập mới giữa AUSF và the UDM.

Theo các phương án trên Fig.4B đến Fig.4F, sau khi thu thập K_{AKMA} và KID, thì AUSF gửi thông điệp thứ tư đến AMF/SEAF, trong đó thông điệp thứ tư này bao gồm KID hoặc thông tin chỉ thị thứ tư. AMF/SEAF gửi thông điệp thứ năm đến UE, trong đó thông điệp thứ năm này bao gồm KID hoặc thông tin chỉ thị thứ năm. Thông điệp thứ tư có thể là thông điệp đáp ứng dịch vụ xác thực được gửi bởi AUSF đến AMF/SEAF được thể hiện trên Fig.4B và Fig.4C, và thông điệp thứ năm có thể là thông điệp yêu cầu xác thực được gửi bởi AMF/SEAF đến UE. Theo cách khác, thông điệp thứ tư có thể là thông điệp đáp ứng dịch vụ xác thực được thể hiện trên Fig.4D, và thông điệp thứ năm có thể là thông điệp N1, ví dụ, thông điệp kết quả xác thực hoặc thông điệp lệnh chế độ bảo mật tầng không truy cập. Cần lưu ý rằng loại của thông điệp thứ tư là không chỉ giới hạn ở nội dung được đề cập ở các phương án nêu trên. Theo cách khác, thông điệp thứ tư này có thể là thông điệp truyền thông hiện có khác giữa AMF/SEAF và AUSF, hoặc có thể là thông điệp truyền thông được thiết lập mới giữa AMF/SEAF và AUSF. Loại của thông điệp thứ năm là không chỉ giới hạn ở nội dung được đề cập ở các phương án nêu trên. Theo cách khác, thông điệp thứ năm có thể là thông điệp N1 hiện có bất kỳ khác giữa AMF/SEAF và UE, hoặc có thể là thông điệp N1 được thiết lập mới giữa AMF/SEAF và UE.

Có thể thấy rằng, theo các phương án của sáng chế, thì AUSF hoặc UE thu thập khoá AKMA K_{AKMA} và/hoặc KID, trong đó khoá AKMA này được dùng để tạo ra K_{AF}. Sáng chế bộc lộ phương pháp và các thông số được sử dụng bởi AUSF hoặc UE để thu thập khoá AKMA K_{AKMA} và/hoặc KID, và điều kiện kích hoạt và cơ hội để AUSF hoặc UE thu thập K_{AKMA} và/hoặc KID.

UE khởi tạo yêu cầu phiên dịch vụ đến AF để thiết lập hoạt động truyền thông giữa hai bên. Trong tiến trình này, thì việc xác thực danh tính có thể còn được thực hiện trên UE. Cụ thể là, xem Fig.5. Fig.5 là hình vẽ thể hiện lưu đồ của phương pháp xác thực danh tính UE theo một phương án của sáng chế. Như được thể hiện trên Fig.5, phương pháp này bao gồm các bước sau đây.

501: UE gửi yêu cầu thiết lập phiên dịch vụ đến AF, trong đó yêu cầu thiết lập phiên dịch vụ này bao gồm KID và Token (thẻ bài).

Theo phương án này của sáng chế, thì yêu cầu phiên dịch vụ này bao gồm thẻ bài Token. Token này được dùng để xác minh danh tính của UE hoặc danh tính của người dùng ứng dụng. Nếu UE gửi Token này đến AF, thì UE thu thập hoặc tạo ra Token này trước khi gửi Token này.

Theo cách khả thi, thì yêu cầu phiên dịch vụ này có thể còn bao gồm bộ nhận dạng người dùng ứng dụng (User IDentifier - User-ID) và/hoặc bộ nhận dạng UE (UE IDentifier - UE-ID). User-ID là danh tính được sử dụng bởi người dùng ứng dụng để truy cập AF, và được sử dụng bởi AF để nhận dạng người dùng ứng dụng. UE-ID là danh tính được sử dụng khi UE truy cập mạng, và được sử dụng bởi phía mạng (ví dụ, AUSF, UDM, hoặc AAnF) để nhận dạng UE. Theo sáng chế, thì User-ID bao gồm, nhưng không chỉ giới hạn ở, GPSI, tên người dùng, v.v.. UE-ID bao gồm, nhưng không chỉ giới hạn ở, SUPI, 5G-GUTI, SUCI, GPSI, v.v., của UE.

Theo cách khả thi, thì yêu cầu phiên dịch vụ này bao gồm Token, và Token này bao gồm User-ID và/hoặc UE-ID.

502: AF gửi yêu cầu khoá ứng dụng đến AAnF để thu thập K_{AF}, trong đó yêu cầu khoá này bao gồm KID và Token.

Nếu AF nhận được Token này từ UE, thì AF thực hiện hoạt động bất kỳ trong số các hoạt động sau đây:

AF xác minh Token nhận được, và sau khi việc xác minh thành công, thì AF gửi yêu cầu khoá ứng dụng này đến AAnF để thu thập K_{AF}, trong đó yêu cầu khoá này bao gồm KID.

AF gửi yêu cầu khoá ứng dụng này đến AAnF để thu thập K_{AF}, trong đó yêu cầu khoá này bao gồm KID và Token nhận được.

Theo cách khả thi, thì AF nhận dạng, dựa trên User-ID nhận được, người dùng ứng dụng mà yêu cầu dịch vụ.

Theo cách khả thi, theo cách khác thì AF có thể bao gồm User-ID nhận được và/hoặc UE-ID nhận được trong yêu cầu khoá ứng dụng này.

503: AAnF gửi yêu cầu khoá AKMA đến AUSF để thu thập K_{AKMA}, trong đó yêu cầu khoá AKMA này bao gồm KID và Token này.

Trước khi AAnF gửi yêu cầu khoá AKMA đến AUSF, thì AAnF cần chọn AUSF dựa trên thông tin định tuyến AUSF được bao gồm trong KID nhận được.

Nếu AAnF nhận được Token này từ AF, thì AAnF còn thực hiện hoạt động bất kỳ trong số các hoạt động sau đây:

AAnF xác minh Token nhận được, và sau khi việc xác minh thành công, thì AF gửi yêu cầu khoá ứng dụng đến AUSF để thu thập K_{AF}, trong đó yêu cầu khoá này bao gồm KID.

AF gửi yêu cầu khoá ứng dụng này đến AAnF để thu thập K_{AF}, trong đó yêu cầu khoá này bao gồm KID và Token nhận được.

Nếu AAnF nhận được User-ID và/hoặc UE-ID nêu trên, thì AAnF bao gồm User-ID nhận được và/hoặc UE-ID nhận được này trong yêu cầu khoá AKMA.

504: Nếu AUSF nhận Token nêu trên, thì AUSF xác minh Token nhận được này, hoặc AUSF gửi Token này đến UDM, và UDM xác minh Token nhận được này.

AUSF xác minh Token nhận được, và có thể xác minh Token này nhờ sử dụng thông tin khoá được chia sẻ bởi AUSF và UE. Thông tin khoá được chia sẻ bởi AUSF và UE có thể là một hoặc nhiều thành phần bất kỳ trong số các thành phần sau đây: K_{AUSF}, K_{AKMA}, khoá mật mã CK, khoá toàn vẹn IK, khoá dài hạn K, và khoá được tạo ra dựa trên khoá mật mã CK và/hoặc khoá toàn vẹn IK, vectơ xác thực, một phần của vectơ xác thực, v.v.. Trước khi xác minh Token nhận được, thì AUSF có thể cần nhận dạng UE hoặc người dùng ứng dụng mà khởi tạo yêu cầu này. AUSF có thể nhận dạng UE hoặc người dùng ứng dụng theo cách bất kỳ trong số những cách sau đây:

AUSF nhận dạng UE dựa trên KID nhận được, và thu thập UE-ID và/hoặc User-ID của UE.

AUSF thu thập UE-ID hoặc User-ID được bao gồm trong Token.

AUSF có thể gửi UE-ID thu được và/hoặc User-ID thu được đến UDM.

Việc AUSF gửi Token đến UDM có thể là việc AUSF gửi thông điệp thứ x đến UDM, trong đó thông điệp thứ x này bao gồm Token này. UDM nhận thông điệp thứ x bao gồm Token này, xác minh Token này, và trả về kết quả xác minh của Token

này cho AUSF. UDM có thể gửi kết quả xác minh của Token này đến AUSF bằng cách gửi thông điệp đáp ứng thứ x đến AUSF bởi UDM này, trong đó thông điệp đáp ứng thứ x này bao gồm kết quả xác minh này. Trước khi xác minh Token nhận được, thì UDM có thể cần nhận dạng UE hoặc người dùng ứng dụng mà khởi tạo yêu cầu này. UDM có thể nhận dạng UE hoặc người dùng ứng dụng theo cách bất kỳ trong số những cách sau đây:

UDM nhận dạng UE hoặc người dùng ứng dụng dựa trên UE-ID hoặc User-ID được bao gồm trong Token này.

UDM nhận dạng UE hoặc người dùng ứng dụng dựa trên UE-ID hoặc User-ID nhận được từ AUSF.

UDM có thể xác minh Token này nhờ sử dụng thông tin khoá được chia sẻ bởi UDM và UE. Thông tin khoá được chia sẻ bởi UDM và UE có thể là một hoặc nhiều thành phần bất kỳ trong số các thành phần sau đây: K_{AUSF}, K_{AKMA}, khoá mật mã CK, khoá toàn vẹn IK, khoá dài hạn K, khoá được tạo ra dựa trên khoá mật mã CK và/hoặc khoá toàn vẹn IK, vectơ xác thực, phần nêu trên của vectơ xác thực, v.v.. Theo cách khác, UDM có thể xác minh Token này nhờ sử dụng khoá công khai của UE, khoá bí mật của UE, khoá công khai của mạng thường trú, khoá bí mật của mạng thường trú, v.v..

UDM có thể gửi User-ID và/hoặc UE-ID của UE đến AUSF.

505: AUSF thu thập hoặc tạo ra K_{AKMA} tương ứng dựa trên KID nhận được. Theo cách khác, nếu AUSF xác minh thành công Token này, thì AUSF thu thập hoặc tạo ra K_{AKMA} tương ứng dựa trên KID nhận được. Theo cách khác, nếu AUSF nhận được kết quả xác minh mà được gửi bởi UDM và chỉ thị rằng việc xác minh trên Token này là thành công, thì AUSF thu thập hoặc tạo ra K_{AKMA} tương ứng dựa trên KID nhận được. AUSF bao gồm K_{AKMA} trong đáp ứng khoá AKMA và gửi đáp ứng khoá AKMA này đến AAnF.

Khi AUSF gửi K_{AKMA} đến AAnF, thì AUSF có thể còn gửi User-ID hoặc UE-ID đến AAnF, nói cách khác, là AUSF bao gồm UE-ID hoặc User-ID này trong đáp ứng khoá AKMA.

AAnF gửi UE-ID nhận được hoặc User-ID nhận được đến AF.

Trong tiến trình này, thì việc xác thực danh tính được thực hiện trên UE hoặc người dùng ứng dụng nhờ sử dụng AF, AAnF, AUSF, hoặc UDM, để xác định danh

tính của UE. AUSF gửi K_{AKMA} đến AAnF, để AAnF tạo ra khoá ứng dụng K_{AF} tương ứng với AF dựa trên K_{AKMA}, trong đó K_{AF} được sử dụng cho việc bảo vệ lưu lượng giữa UE và AF.

Theo phương án này, thì Token nêu trên được dùng để xác thực UE hoặc người dùng ứng dụng. Trong một số trường hợp, theo cách khác thì cách xác thực khác có thể được sử dụng, ví dụ, KID, sự rút gọn (digest), hoặc mã xác thực thông điệp (Message Authentication Code - MAC). Như được thể hiện trên Fig.5, KID được sử dụng làm ví dụ.

Sau khi nhận được KID được gửi bởi AAnF, thì AUSF xác minh KID, hoặc gửi KID đến UDM. Sau khi nhận được KID, thì UDM xác minh KID và trả về kết quả xác minh cho AUSF. Nếu AUSF xác minh thành công KID, hoặc AUSF nhận được kết quả xác minh mà được gửi bởi UDM và chỉ thị rằng việc xác minh trên KID là thành công, thì AUSF gửi K_{AKMA} đến AAnF.

AUSF có thể xác minh Token này nhờ sử dụng thông tin khoá được chia sẻ bởi AUSF và UE. Thông tin khoá được chia sẻ bởi AUSF và UE có thể là một hoặc nhiều thành phần bất kỳ trong số các thành phần sau đây: K_{AUSF}, K_{AKMA}, khoá mật mã CK, khoá toàn vẹn IK, khoá dài hạn K, khoá được tạo ra dựa trên khoá mật mã CK và/hoặc khoá toàn vẹn IK, vectơ xác thực, phần nêu trên của vectơ xác thực, v.v..

UDM có thể xác minh KID nhờ sử dụng thông tin khoá được chia sẻ bởi UDM và UE. Thông tin khoá được chia sẻ bởi UDM và UE có thể là một hoặc nhiều thành phần bất kỳ trong số các thành phần sau đây: K_{AUSF}, K_{AKMA}, khoá mật mã CK, khoá toàn vẹn IK, khoá dài hạn K, khoá được tạo ra dựa trên khoá mật mã CK và/hoặc khoá toàn vẹn IK, vectơ xác thực, phần nêu trên của vectơ xác thực, v.v.. Theo cách khác, UDM có thể xác minh KID này nhờ sử dụng khoá công khai của UE, khoá bí mật của UE, khoá công khai của mạng thường trú, khoá bí mật của mạng thường trú, v.v..

Ngoài ra, KID ở UE và AUSF có thể được cập nhật để ngăn không cho kẻ tấn công theo dõi UE bằng cách theo dõi KID. Fig.6A là hình vẽ thể hiện lưu đồ của phương pháp cập nhật KID và/hoặc K_{AKMA} theo một phương án của sáng chế. Như được thể hiện trên Fig.6A, phương pháp này bao gồm các bước sau đây.

601: UE gửi yêu cầu thiết lập phiên dịch vụ đến AF, trong đó yêu cầu thiết lập phiên dịch vụ này bao gồm KID này.

602: AF gửi yêu cầu khoá ứng dụng đến AAnF để thu thập K_{AF}, trong đó yêu

cầu khoá này bao gồm KID này. AAnF thu thập K_{AF} tương ứng dựa trên KID nhận được. Việc AAnF thu thập K_{AF} tương ứng có thể là việc AAnF thu thập K_{AF} một cách cục bộ dựa trên KID, hoặc việc AAnF tạo ra K_{AF} dựa trên K_{AKMA} tương ứng với KID, hoặc việc AAnF gửi yêu cầu khoá AKMA mang KID nhận được đến AUSF, nhận K_{AKMA} được trả về bởi AUSF, và tạo ra K_{AF} dựa trên K_{AKMA} nhận được.

603: AAnF ghi lại số lần mà KID được sử dụng.

AAnF ghi lại số lần mà KID được sử dụng. Bộ đếm có thể được tạo ra bởi AAnF, và giá trị khởi đầu của bộ đếm này là 0. Khi KID này được sử dụng một lần, thì bộ đếm này được tăng thêm một. Bộ đếm này có thể được tăng thêm một dựa trên yêu cầu khoá ứng dụng mà AAnF nhận được. Theo cách khác, bộ đếm này có thể được tăng thêm một dựa trên yêu cầu khoá AKMA mà AAnF gửi đến AUSF. Theo cách khác, bộ đếm này có thể được tăng thêm một dựa trên K_{AKMA} hoặc đáp ứng khoá AKMA mà AAnF thu được từ AUSF. Theo cách khác, bộ đếm này có thể được tăng thêm một dựa trên KID nhận được hoặc thông điệp nhận được bao gồm KID này.

604: Khi AAnF xác định được rằng số lần mà KID được sử dụng (hoặc giá trị của bộ đếm) là lớn hơn ngưỡng được thiết đặt trước, thì AAnF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA} đến AUSF, để thông báo cho AUSF cập nhật KID và/hoặc K_{AKMA}, và tạo ra KID mới và/hoặc K_{AKMA} mới. AAnF có thể còn gửi UE-ID hoặc User-ID đến AUSF cùng một lúc. Dựa trên UE-ID nhận được hoặc User-ID nhận được, thì AUSF xác định UE mà cần cập nhật KID và/hoặc K_{AKMA}.

605: Sau khi nhận được yêu cầu cập nhật KID và/hoặc K_{AKMA}, thì AUSF có thể thực hiện một hoặc nhiều hoạt động bất kỳ trong số các hoạt động sau đây:

AUSF cập nhật KID và/hoặc K_{AKMA}, và tạo ra KID mới và/hoặc K_{AKMA} mới.

AUSF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID đã được cập nhật, hoặc thông tin chỉ thị thứ bảy đến AMF/SEAF. Thông tin chỉ thị thứ bảy này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: được dùng để chỉ thị cho UE cập nhật KID và/hoặc K_{AKMA}; được dùng để chỉ thị cho UE tạo ra KID mới và/hoặc K_{AKMA}; được dùng để chỉ thị cho AMF/SEAF khởi tạo việc xác thực sơ cấp; và được dùng để chỉ thị cho AMF/SEAF cấp phát 5G-GUTI mới cho UE. AUSF có thể còn gửi UE-ID đến AMF/SEAF cùng một lúc, tức là, bước 606 trên Fig.6A.

AUSF yêu cầu vectơ xác thực từ UDM. Sau khi nhận được vectơ xác thực từ UDM, thì AUSF gửi thông điệp EAP-Request/AKA'-Challenge đến AMF/SEAF, hoặc

gửi vectơ xác thực môi trường dịch vụ 5G đến AMF/SEAF. Vectơ xác thực môi trường dịch vụ 5G này bao gồm RAND, AUTN, và HXRES*.

Sau khi tạo ra KID mới và/hoặc K_{AKMA} mới, thì AUSF gửi KID mới và/hoặc K_{AKMA} mới này đến AAnF.

Theo cách khác, sau khi AUSF hoàn tất việc cập nhật KID và/hoặc K_{AKMA}, thì UE cũng cần cập nhật KID và/hoặc K_{AKMA}. Xem Fig.6A. Tiến trình mà trong đó UE cập nhật KID là có thể bao gồm các bước sau đây.

606: AUSF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID được tạo ra mới, hoặc thông tin chỉ thị thứ bảy, đến AMF/SEAF. Thông tin chỉ thị thứ bảy này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: cập nhật KID và/hoặc K_{AKMA}; tạo ra KID mới và/hoặc K_{AKMA} mới; việc AMF/SEAF khởi tạo việc xác thực sơ cấp; và việc AMF/SEAF cấp phát 5G-GUTI mới cho UE. AUSF có thể còn gửi UE-ID đến AMF/SEAF cùng một lúc, để AMF/SEAF nhận dạng UE mà cần thực hiện việc cập nhật.

607: Dựa trên UE-ID nhận được, thì AMF/SEAF xác định UE mà cần cập nhật KID và/hoặc K_{AKMA}. AMF/SEAF có thể thực hiện một hoặc nhiều hoạt động bất kỳ trong số các hoạt động sau đây dựa trên yêu cầu cập nhật KID và/hoặc K_{AKMA} nhận được, thông tin chỉ thị thứ bảy, hoặc KID này:

AMF/SEAF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA} đến UE; AMF/SEAF gửi thông tin chỉ thị thứ tám đến UE; AMF/SEAF gửi KID đến UE; AMF/SEAF khởi tạo thủ tục xác thực sơ cấp; và AMF/SEAF cấp phát 5G-GUTI mới cho UE và gửi 5G-GUTI mới đến UE.

Thông tin chỉ thị thứ tám được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: cập nhật KID và/hoặc K_{AKMA}; tạo ra KID mới và/hoặc K_{AKMA}; và việc phía mạng (ví dụ, AUSF) đã cập nhật KID và/hoặc K_{AKMA}.

Nếu UE nhận được KID này, thì UE lưu giữ KID này và tạo ra K_{AKMA} mới. Nếu UE nhận được yêu cầu cập nhật KID và/hoặc K_{AKMA} hoặc thông tin chỉ thị thứ tám này, thì UE tạo ra KID mới và/hoặc K_{AKMA} mới.

Theo sáng chế, khi cập nhật KID, thì UE hoặc AUSF có thể tạo ra KID mới dựa trên KID hiện tại. Các thông số khác có thể được sử dụng thay thế để tạo ra KID mới. Điều này không bị giới hạn theo sáng chế. UE và AUSF sử dụng cùng một phương pháp và cùng các thông số để cập nhật KID.

Theo cách khác, trong một số trường hợp khả thi, thì việc cập nhật KID mà được thực hiện bởi UE là có thể được kích hoạt bởi AF. Xem Fig.6A. Tiến trình này bao gồm các bước sau đây.

606': AUSF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID và/hoặc K_{AKMA} được tạo ra mới, hoặc thông tin chỉ thị thứ bảy, đến AAnF. AUSF có thể còn gửi UE-ID hoặc User-ID đến AAnF cùng một lúc. Dựa trên UE-ID nhận được hoặc User-ID nhận được, thì AAnF xác định UE hoặc người dùng ứng dụng mà cần cập nhật KID và/hoặc K_{AKMA}.

607': AAnF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID nhận được, hoặc thông tin chỉ thị thứ tám, đến AF. AAnF có thể còn gửi UE-ID hoặc User-ID đến AF cùng một lúc. Dựa trên UE-ID nhận được hoặc User-ID nhận được, thì AF xác định UE mà cần cập nhật KID và/hoặc K_{AKMA}. Thông tin chỉ thị thứ tám được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: cập nhật KID và/hoặc K_{AKMA}; tạo ra KID mới và/hoặc K_{AKMA} mới; và việc phía mạng (ví dụ, AUSF) đã cập nhật KID và/hoặc K_{AKMA}.

608': AF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID nhận được, hoặc thông tin chỉ thị thứ chín đến UE dựa trên yêu cầu cập nhật KID và/hoặc K_{AKMA} nhận được, KID, hoặc thông tin chỉ thị thứ tám. Thông tin chỉ thị thứ chín được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: cập nhật KID và/hoặc K_{AKMA}; tạo ra KID mới và/hoặc K_{AKMA} mới; và việc phía mạng (ví dụ, AUSF) đã cập nhật KID và/hoặc K_{AKMA}.

UE cập nhật KID và/hoặc K_{AKMA} dựa trên yêu cầu cập nhật KID và/hoặc K_{AKMA} nhận được, KID nhận được, hoặc thông tin chỉ thị thứ chín.

Sau khi hoàn tất việc cập nhật KID, thì AUSF có thể gửi KID mới đến AAnF, và sau đó AAnF chuyển tiếp KID mới này đến AF. AF gửi KID mới này đến UE để hoàn tất việc cập nhật KID được thực hiện bởi UE.

Theo cách khác, AUSF có thể gửi yêu cầu cập nhật KID đến AAnF, AAnF chuyển tiếp yêu cầu cập nhật KID này đến AF, sau đó AF gửi yêu cầu cập nhật KID này đến UE, và UE hoàn tất việc cập nhật KID nhờ sử dụng yêu cầu cập nhật KID này.

Theo cách khác, AUSF có thể gửi thông tin chỉ thị thứ bảy đến AAnF; AAnF tạo ra thông tin chỉ thị thứ tám dựa trên thông tin chỉ thị thứ bảy này và gửi thông tin chỉ thị thứ tám này đến AF; AF tạo ra thông tin chỉ thị thứ chín dựa trên thông tin chỉ

thị thứ tám này và gửi thông tin chỉ thị thứ chín này đến UE; và UE hoàn tất việc cập nhật KID dựa trên thông tin chỉ thị thứ chín này.

Các thông tin chỉ thị chẳng hạn như thông tin chỉ thị thứ bảy, thông tin chỉ thị thứ tám, và thông tin chỉ thị thứ chín là có thể được bao gồm trong yêu cầu cập nhật KID và/hoặc K_{AKMA}, hoặc có thể được bổ sung vào thông điệp truyền thông khác. Nội dung của các thông tin chỉ thị này có thể giống nhau hoặc khác nhau. Bước 606 và bước 607 và bước 606' đến bước 608' trên Fig.6A là hai cách thức thực hiện tuỳ ý, và phương pháp ở bước 601 đến bước 605 có thể được kết hợp với phương pháp bất kỳ trong số hai phương pháp này.

Sau khi cập nhật KID, thì sau đó UE có thể khởi tạo yêu cầu thiết lập phiên ứng dụng đến AF dựa trên KID mới.

Fig.6B là hình vẽ thể hiện lưu đồ của phương pháp khác để cập nhật KID và/hoặc K_{AKMA} theo một phương án của sáng chế. Như được thể hiện trên Fig.6B, phương pháp này bao gồm các bước sau đây.

611: AMF/SEAF xác định cập nhật 5G-GUTI của UE. Tuỳ ý, AMF/SEAF cập nhật 5G-GUTI của UE.

612: AMF/SEAF thực hiện một hoặc nhiều hoạt động bất kỳ trong số các hoạt động sau đây:

AMF/SEAF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA} hoặc thông tin chỉ thị thứ sáu đến AUSF. Thông tin chỉ thị thứ sáu này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc AUSF cập nhật KID và/hoặc K_{AKMA}; và việc 5G-GUTI của UE đã được cập nhật.

AMF/SEAF khởi tạo thủ tục xác thực sơ cấp.

AMF/SEAF gửi yêu cầu dịch vụ xác thực đến AUSF.

AMF/SEAF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA} hoặc thông tin chỉ thị thứ x đến UE. Thông tin chỉ thị thứ x này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: việc UE cập nhật KID và/hoặc K_{AKMA}; việc UE tạo ra KID mới và/hoặc K_{AKMA} mới; và việc phía mạng (ví dụ, AUSF) đã cập nhật KID và/hoặc K_{AKMA}.

613: AUSF cập nhật KID và/hoặc K_{AKMA} dựa trên yêu cầu cập nhật KID và/hoặc K_{AKMA} nhận được hoặc thông tin chỉ thị thứ sáu, và tạo ra KID mới và/hoặc K_{AKMA} mới.

Theo cách khác, AUSF nhận yêu cầu dịch vụ xác thực được gửi bởi AMF/SEAF, và AUSF khởi tạo yêu cầu dịch vụ xác thực đến UDM, trong đó yêu cầu dịch vụ xác thực này được dùng để yêu cầu thu thập vectơ xác thực.

Khi xác định là cập nhật 5G-GUTI và trước hoặc sau khi cập nhật tuỳ ý 5G-GUTI, thì AMF/SEAF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA} hoặc thông tin chỉ thị thứ sáu đến AUSF. AMF/SEAF có thể gửi thông tin chỉ thị thứ sáu này nhờ sử dụng thông điệp truyền thông hiện có giữa AMF/SEAF và AUSF, hoặc AMF/SEAF có thể gửi thông tin chỉ thị thứ sáu này nhờ sử dụng thông điệp truyền thông được xác định mới giữa AMF/SEAF và AUSF.

5G-GUTI là bộ nhận dạng luôn được cập nhật. Việc sử dụng 5G-GUTI có thể giảm bớt việc sử dụng bộ nhận dạng cố định của UE được hiển thị trong quá trình truyền thông, để cải thiện sự bảo mật. Khi 5G-GUTI được cập nhật thì KID cũng được cập nhật. Điều này có thể ngăn không cho UE bị theo dõi nhờ sử dụng KID, và cải thiện sự bảo mật truyền thông của UE.

Tương tự, nếu AUSF cập nhật KID và/hoặc K_{AKMA}, thì UE cũng cần cập nhật KID và/hoặc K_{AKMA}. KID ở UE có thể được cập nhật. Như được thể hiện trên Fig.6B, tiến trình này có thể bao gồm các bước sau đây.

614: Sau khi AUSF tạo ra KID mới và/hoặc K_{AKMA} mới, thì AUSF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID mới này, hoặc thông tin chỉ thị thứ mười, đến AMF/SEAF. Thông tin chỉ thị thứ mười này được dùng để chỉ thị một hoặc nhiều việc bất kỳ trong số những việc sau đây: cập nhật KID và/hoặc K_{AKMA}; tạo ra KID mới và/hoặc K_{AKMA} mới; và việc AMF/SEAF khởi tạo việc xác thực sơ cấp. Sau khi tạo ra KID mới và/hoặc K_{AKMA} mới, thì AUSF gửi KID đã được cập nhật và/hoặc K_{AKMA} đã được cập nhật đến AAnF.

Theo cách khác, sau khi thu thập vectơ xác thực từ UDM, thì AUSF gửi đáp ứng dịch vụ xác thực đến AMF/SEAF.

615: AMF/SEAF gửi yêu cầu cập nhật KID và/hoặc K_{AKMA}, KID nhận được, hoặc thông tin chỉ thị thứ mười một đến UE dựa trên yêu cầu cập nhật KID và/hoặc K_{AKMA} nhận được, KID mới, hoặc thông tin chỉ thị thứ mười.

Theo phương án này, thì UE cập nhật KID và/hoặc K_{AKMA} dựa trên yêu cầu cập nhật KID và/hoặc K_{AKMA} nhận được, thông tin chỉ thị thứ mười một, hoặc thông tin chỉ thị thứ x, và tạo ra KID mới và/hoặc K_{AKMA} mới. Sau khi nhận được KID này, thì

UE lưu giữ và sử dụng KID này, và tạo ra K_{AKMA} mới.

Theo phương án này của sáng chế, theo cách khác thì việc cập nhật KID có thể bao gồm việc cập nhật K_{AKMA} tương ứng. Cụ thể là, sau khi AUSF hoặc UE nhận được yêu cầu cập nhật KID, thì AUSF hoặc UE cập nhật K_{AKMA} và/hoặc KID.

Theo phương án này của sáng chế, thì mối đe doạ từ việc theo dõi UE là được giảm bớt bằng cách cập nhật KID, và sự bảo mật truyền thông được cải thiện.

Phần nêu trên chủ yếu mô tả các giải pháp theo sáng chế từ góc độ sự tương tác giữa các phần tử mạng. Có thể hiểu rằng theo những cách thức thực hiện nêu trên, để thực hiện các chức năng nêu trên, thì các phần tử mạng đó bao gồm các cấu trúc phần cứng và/hoặc các môđun phần mềm tương ứng để thực hiện các chức năng nêu trên. Người có hiểu biết trung bình trong lĩnh vực có thể dễ dàng thấy rằng, kết hợp với các đơn vị và các bước thuật toán của các ví dụ được mô tả theo các phương án được bộc lộ trong bản mô tả này, thì sáng chế có thể được thực hiện bằng phần cứng hoặc tổ hợp của phần cứng và phần mềm máy tính. Việc một chức năng được thực hiện bằng phần cứng hay phần cứng được điều khiển bởi phần mềm máy tính là phụ thuộc vào các ứng dụng cụ thể và các ràng buộc thiết kế của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả đối với mỗi ứng dụng cụ thể, nhưng điều này không được coi là cách thức thực hiện đó nằm ngoài phạm vi của sáng chế.

Theo các phương án của sáng chế, thì thiết bị đầu cuối, phần tử mạng mặt phẳng điều khiển, phần tử mạng chức năng dịch vụ, phần tử mạng chức năng quản lý, hoặc thiết bị mạng khác, là có thể được chia thành các môđun chức năng dựa trên các ví dụ về phương pháp nêu trên. Ví dụ, các môđun chức năng này có thể được chia dựa trên các chức năng, hoặc hai hoặc nhiều chức năng có thể được tích hợp vào một môđun xử lý. Môđun tích hợp này có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng môđun chức năng phần mềm. Cần lưu ý rằng, theo các phương án của sáng chế, thì việc chia thành các môđun là một ví dụ, và chỉ là cách chia theo chức năng logic. Khi thực hiện thực tế thì cách chia khác có thể được sử dụng.

Fig.7 là hình vẽ thể hiện thiết bị truyền thông 700 theo một phương án của sáng chế. Thiết bị truyền thông 700 này có thể được tạo cấu hình để thực hiện phương pháp thu thập khoá và các phương án cụ thể mà được áp dụng cho phần tử mạng AUSF và được thể hiện trên Fig.4A đến Fig.4F. Thiết bị này có thể là thiết bị đầu cuối hoặc

con chip mà có thể được tạo cấu hình trong thiết bị đầu cuối. Theo cách thức thực hiện khả thi, như được thể hiện trên Fig.7, thì thiết bị truyền thông 700 bao gồm môđun xử lý 703.

Môđun xử lý 703 được tạo cấu hình để thu thập khoá mỏ neo của tiến trình xác thực và quản lý khoá dành cho các ứng dụng K_{AKMA} và/hoặc bộ nhận dạng khoá KID duy nhất của K_{AKMA}.

Tuỳ ý, thiết bị truyền thông 700 còn bao gồm môđun nhận 701, được tạo cấu hình để nhận thông điệp thứ nhất được gửi bởi chức năng quản lý truy cập và quản lý tính di động hoặc chức năng mỏ neo bảo mật (Access and Mobility management Function/SEcurity Anchor Function - AMF/SEAF).

Môđun xử lý 703 được tạo cấu hình để thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất.

Tuỳ ý, thông điệp thứ nhất bao gồm KID, và môđun xử lý 703 được tạo cấu hình cụ thể để: thu thập KID trong thông điệp thứ nhất, và/hoặc tạo ra K_{AKMA} dựa trên KID.

Tuỳ ý, thông điệp thứ nhất bao gồm thông tin chỉ thị thứ nhất, và môđun xử lý 703 được tạo cấu hình cụ thể để tạo ra KID và/hoặc K_{AKMA} dựa trên thông tin chỉ thị thứ nhất.

Tuỳ ý, thiết bị truyền thông 700 còn bao gồm môđun gửi 702, được tạo cấu hình để gửi thông điệp thứ hai đến chức năng quản lý dữ liệu hợp nhất (Unified Data Management - UDM) dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai này bao gồm chỉ thị thu thập sự cho phép, chỉ thị thu thập sự cho phép này được dùng để thu thập thông tin cho phép thứ nhất của UE, và thông tin cho phép thứ nhất này được dùng để chỉ thị rằng UE có khả năng sử dụng dịch vụ xác thực và quản lý khoá dành cho các ứng dụng (Authentication and Key MAnagement - AKMA).

Môđun xử lý 703 được tạo cấu hình để: khi xác định được rằng thông tin cho phép thứ nhất của UE đã được thu thập, thì tạo ra KID và/hoặc K_{AKMA}.

Tuỳ ý, môđun nhận 701 được tạo cấu hình để nhận thông điệp thứ ba được gửi bởi UDM, trong đó thông điệp thứ ba này bao gồm thông tin chỉ thị thứ ba. Môđun xử lý 703 được tạo cấu hình để tạo ra KID và/hoặc K_{AKMA} dựa trên thông tin chỉ thị thứ ba.

Tuỳ ý, môđun xử lý 703 có thể là con chip, bộ mã hoá, mạch mã hoá, hoặc

mạch tích hợp khác mà có thể thực hiện phương pháp theo sáng chế.

Môđun nhận 701 có thể là mạch giao diện hoặc bộ thu phát.

Các phương pháp cụ thể và các phương án đã được mô tả trên đây, và thiết bị 700 được tạo cấu hình để thực hiện phương pháp thu thập khoá tương ứng với thiết bị đầu cuối. Do đó, về những phần mô tả cụ thể của phương pháp thu thập khoá, và đặc biệt là chức năng của môđun xử lý 703, thì xem các phần liên quan ở phương án tương ứng. Các chi tiết không được mô tả lại ở đây.

Tuỳ ý, thiết bị 700 có thể còn bao gồm môđun lưu trữ (không được thể hiện trên hình vẽ). Môđun lưu trữ này có thể được tạo cấu hình để lưu giữ dữ liệu và/hoặc báo hiệu. Môđun lưu trữ này có thể được ghép nối đến môđun xử lý 703, hoặc có thể được ghép nối đến môđun nhận 701 hoặc môđun gửi 702. Ví dụ, môđun xử lý 703 có thể được tạo cấu hình để đọc dữ liệu và/hoặc báo hiệu trong môđun lưu trữ, để thực hiện phương pháp thu thập khoá theo các phương án về phương pháp nêu trên.

Tuỳ ý, thiết bị truyền thông 700 có thể được áp dụng cho phương pháp thu thập khoá và các phương án cụ thể mà được áp dụng cho phần tử mạng AUSF trên Fig.5, Fig.6A, hoặc Fig.6B. Các chi tiết không được mô tả lại ở đây.

Fig.8 là hình vẽ thể hiện thiết bị truyền thông 800 khác theo một phương án của sáng chế. Thiết bị truyền thông 800 này có thể được tạo cấu hình để thực hiện phương pháp thu thập khoá và các phương án cụ thể mà được áp dụng cho phần tử mạng AMF/SEAF và được thể hiện trên Fig.4A đến Fig.4F. Thiết bị này có thể là thiết bị đầu cuối hoặc con chip mà có thể được tạo cấu hình trong thiết bị đầu cuối. Theo cách thức thực hiện khả thi, như được thể hiện trên Fig.8, thiết bị truyền thông 800 bao gồm môđun nhận 801 và môđun gửi 802.

Môđun nhận 801 được tạo cấu hình để thu thập thông điệp thứ tư từ AUSF.

Môđun gửi 802 được tạo cấu hình để gửi thông điệp thứ năm đến UE dựa trên thông điệp thứ tư này, để UE thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ năm này.

Tuỳ ý, thiết bị truyền thông 800 bao gồm môđun xử lý 803, được tạo cấu hình để tạo ra thông điệp thứ năm dựa trên thông điệp thứ tư.

Tuỳ ý, môđun gửi 802 còn được tạo cấu hình để gửi thông điệp thứ nhất đến AUSF, để AUSF tạo ra KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất.

Tuỳ ý, môđun xử lý 803 có thể là con chip, bộ mã hoá, mạch mã hoá, hoặc

mạch tích hợp khác mà có thể thực hiện phương pháp theo sáng chế.

Môđun nhận 801 có thể là mạch giao diện hoặc bộ thu phát.

Các phương pháp cụ thể và các phương án đã được mô tả trên đây, và thiết bị 800 được tạo cấu hình để thực hiện phương pháp thu thập khoá tương ứng với thiết bị đầu cuối. Do đó, về những phần mô tả cụ thể của phương pháp thu thập khoá, và đặc biệt là các chức năng của môđun nhận 801 và môđun gửi 802, thì xem các phần liên quan ở các phương án tương ứng. Các chi tiết không được mô tả lại ở đây.

Tuỳ ý, thiết bị 800 có thể còn bao gồm môđun lưu trữ (không được thể hiện trên hình vẽ). Môđun lưu trữ này có thể được tạo cấu hình để lưu giữ dữ liệu và/hoặc báo hiệu. Môđun lưu trữ này có thể được ghép nối đến môđun xử lý 803, hoặc có thể được ghép nối đến môđun nhận 801 hoặc môđun gửi 802. Ví dụ, môđun xử lý 803 có thể được tạo cấu hình để đọc dữ liệu và/hoặc báo hiệu trong môđun lưu trữ, để thực hiện phương pháp thu thập khoá theo các phương án về phương pháp nêu trên.

Tuỳ ý, thiết bị truyền thông 800 có thể được áp dụng cho phương pháp thu thập khoá và các phương án cụ thể mà được áp dụng cho phần tử mạng AMF/SEAF trên Fig.5, Fig.6A, hoặc Fig.6B. Các chi tiết không được mô tả lại ở đây.

Khi môđun xử lý 703 hoặc 803 là bộ xử lý, môđun nhận 701 hoặc 801, và môđun gửi 702 hoặc 802 cấu thành bộ thu phát, thì thiết bị truyền thông 700 hoặc thiết bị truyền thông 800 theo phương án này của sáng chế có thể là thiết bị truyền thông 900 được thể hiện trên Fig.9.

Fig.9 là hình vẽ thể hiện sơ đồ cấu trúc phần cứng của thiết bị truyền thông theo một phương án của sáng chế. Về cấu trúc của phần tử mạng AUSF hoặc AMF/SEAF, thì xem cấu trúc được thể hiện trên Fig.9. Thiết bị truyền thông 900 bao gồm bộ xử lý 111 và bộ thu phát 112, trong đó bộ xử lý 111 và bộ thu phát 112 này được ghép nối điện.

Bộ xử lý 111 được tạo cấu hình để thực thi một số hoặc tất cả trong số các chỉ dẫn chương trình máy tính trong bộ nhớ 113, và khi một số hoặc tất cả trong số các chỉ dẫn chương trình máy tính này được thực thi, thì thiết bị này được cho phép thực hiện phương pháp theo phương án bất kỳ trong số các phương án nêu trên.

Bộ thu phát 112 được tạo cấu hình để truyền thông với thiết bị khác, ví dụ, thu thập thông điệp thứ tư từ AUSF, và gửi thông điệp thứ năm đến UE dựa trên thông điệp thứ tư này, để UE thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ năm này.

Tuỳ ý, thiết bị này còn bao gồm bộ nhớ 113, được tạo cấu hình để lưu giữ các chỉ dẫn chương trình máy tính. Tuỳ ý, bộ nhớ 113 (bộ nhớ #1) được đặt trong thiết bị này, bộ nhớ 113 (bộ nhớ #2) được tích hợp với bộ xử lý 111, hoặc bộ nhớ 113 (bộ nhớ #3) được đặt bên ngoài thiết bị này.

Cần hiểu rằng thiết bị truyền thông 900 được thể hiện trên Fig.9 có thể là con chip hoặc mạch. Ví dụ, thiết bị truyền thông 900 có thể là con chip hoặc mạch mà có thể được bố trí trong thiết bị đầu cuối hoặc thiết bị truyền thông này. Theo cách khác, bộ thu phát 112 có thể là giao diện truyền thông. Bộ thu phát này bao gồm bộ thu và bộ phát. Ngoài ra, thiết bị truyền thông 900 có thể còn bao gồm hệ thống buýt.

Bộ xử lý 111, bộ nhớ 113, và bộ thu phát 112 được nối qua hệ thống buýt này. Bộ xử lý 111 được tạo cấu hình để thực thi các chỉ dẫn được lưu giữ trong bộ nhớ 113, để điều khiển bộ thu phát để nhận tín hiệu và gửi tín hiệu, và thực hiện các bước của thiết bị thứ nhất hoặc thiết bị thứ hai theo phương pháp thực hiện theo sáng chế. Bộ nhớ 113 có thể được tích hợp vào bộ xử lý 111, hoặc có thể được bố trí tách biệt khỏi bộ xử lý 111.

Theo một cách thức thực hiện, có thể coi rằng các chức năng của bộ thu phát 112 là được thực hiện nhờ sử dụng mạch thu phát hoặc chip thu phát dành riêng. Có thể coi rằng bộ xử lý 111 có thể được thực hiện nhờ sử dụng chip xử lý dành riêng, mạch xử lý, bộ xử lý, hoặc chip thông dụng. Bộ xử lý này có thể là đơn vị xử lý trung tâm (Central Processing Unit - CPU), bộ xử lý mạng (Network Processor - NP), hoặc tổ hợp của CPU và NP. Bộ xử lý này có thể còn bao gồm chip phần cứng hoặc bộ xử lý thông dụng khác. Chip phần cứng này có thể là mạch tích hợp chuyên dụng (Application-Specific Integrated Circuit - ASIC), thiết bị logic lập trình được (Programmable Logic Device - PLD), hoặc tổ hợp của chúng. PLD có thể là thiết bị logic phức lập trình được (Complex Programmable Logic Device - CPLD), mảng cổng lập trình được dạng trường (Field-Programmable Gate Array - FPGA), logic mảng chung (Generic Array Logic - GAL) và thiết bị logic lập trình được khác, cổng rời rạc hoặc thiết bị logic tranzito, thành phần phần cứng rời rạc, hoặc tổ hợp bất kỳ của chúng. Bộ xử lý thông dụng có thể là bộ vi xử lý, hoặc bộ xử lý này có thể là bộ xử lý thông thường bất kỳ, v.v..

Còn có thể hiểu rằng bộ nhớ được đề cập ở các phương án của sáng chế có thể là bộ nhớ khả biến hoặc bộ nhớ bất biến, hoặc có thể bao gồm bộ nhớ khả biến và bộ nhớ bất biến. Bộ nhớ bất biến có thể là bộ nhớ chỉ đọc (Read-Only Memory - ROM),

bộ nhớ chỉ đọc lập trình được (Programmable ROM - PROM), bộ nhớ chỉ đọc lập trình được và xoá được (Erasable PROM - EPROM), bộ nhớ chỉ đọc lập trình được và xoá được bằng điện (Electrically EPROM - EEPROM), hoặc bộ nhớ flash (bộ nhớ chớp nhoáng). Bộ nhớ khả biến có thể là bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM), được sử dụng làm bộ đệm ngoài. Theo ví dụ không phải là phần mô tả nhằm mục đích giới hạn, thì nhiều dạng RAM có thể được sử dụng, ví dụ, RAM tĩnh (Static RAM - SRAM), RAM động (Dynamic RAM - DRAM), DRAM đồng bộ (Synchronous DRAM - SDRAM), SDRAM tốc độ dữ liệu gấp đôi (Double Data Rate SDRAM - DDR SDRAM), SDRAM tăng cường (Enhanced SDRAM - ESDRAM), DRAM liên kết đồng bộ (Synchlink DRAM - SLDRAM), và RAM có Rambus trực tiếp (Direct Rambus RAM - DR RAM). Cần lưu ý rằng bộ nhớ được mô tả theo sáng chế là nhằm bao gồm, nhưng không chỉ giới hạn ở, các bộ nhớ này và bộ nhớ bất kỳ thuộc loại phù hợp khác.

Theo một phương án, sáng chế đề xuất phương tiện lưu trữ của máy tính, lưu giữ các chương trình máy tính. Chương trình máy tính này được dùng để thực hiện phương pháp tương ứng với phần tử mạng AUSF theo các phương án nêu trên.

Theo một phương án, sáng chế đề xuất phương tiện lưu trữ của máy tính, lưu giữ các chương trình máy tính. Chương trình máy tính này được dùng để thực hiện phương pháp tương ứng với phần tử mạng AMF/SEAF theo các phương án nêu trên.

Theo một phương án, sáng chế đề xuất sản phẩm chương trình máy tính bao gồm các chỉ dẫn. Khi sản phẩm chương trình máy tính này chạy trên máy tính, thì máy tính đó được cho phép thực hiện phương pháp tương ứng với phần tử mạng AUSF theo các phương án nêu trên.

Theo một phương án, sáng chế đề xuất sản phẩm chương trình máy tính bao gồm các chỉ dẫn. Khi sản phẩm chương trình máy tính này chạy trên máy tính, thì máy tính đó được cho phép thực hiện phương pháp tương ứng với phần tử mạng AMF/SEAF theo các phương án nêu trên.

Cần hiểu rằng các số tuần tự của các tiến trình nêu trên không có nghĩa là các trình tự thực hiện theo các phương án khác nhau của sáng chế. Các trình tự thực hiện của các tiến trình đó là được xác định dựa trên các chức năng và logic nội tại của các tiến trình đó, chứ không được hiểu là giới hạn nào đối với các tiến trình thực hiện theo các phương án của sáng chế.

Dựa vào các ví dụ được mô tả ở các phương án được bộc lộ trong bản mô tả này, thì người có hiểu biết trung bình trong lĩnh vực có thể thấy rằng các đơn vị và các bước thuật toán là có thể được thực hiện bằng phần cứng điện tử, hoặc tổ hợp của phần mềm máy tính và phần cứng điện tử. Việc các chức năng này được thực hiện bằng phần cứng hay phần mềm là phụ thuộc vào các ứng dụng cụ thể và các ràng buộc về thiết kế của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả đối với mỗi ứng dụng cụ thể, nhưng điều này không được coi là cách thức thực hiện đó nằm ngoài phạm vi của sáng chế.

Người có hiểu biết trung bình trong lĩnh vực có thể hiểu rõ rằng, để cho việc mô tả được thuận tiện và phần mô tả được ngắn gọn, thì quá trình hoạt động chi tiết của hệ thống, thiết bị, và đơn vị nêu trên là có thể được tìm thấy ở quá trình tương ứng theo các phương án về phương pháp nêu trên, và các chi tiết không được mô tả lại ở đây.

Theo một số phương án được cung cấp trong đơn này, thì cần hiểu rằng hệ thống, thiết bị và phương pháp được bộc lộ là có thể được thực hiện theo những cách khác. Ví dụ, phương án về thiết bị được mô tả chỉ là một ví dụ. Ví dụ, việc chia thành các đơn vị chỉ là cách chia theo chức năng logic, và có thể là cách chia khác khi thực hiện thực tế. Ví dụ, nhiều đơn vị hoặc thành phần có thể được kết hợp hoặc được tích hợp vào hệ thống khác, hoặc một số dấu hiệu có thể được bỏ qua hoặc không được thực hiện. Ngoài ra, những sự ghép nối với nhau hoặc những sự ghép nối trực tiếp hoặc các kết nối giao tiếp mà đã được thể hiện hoặc được mô tả nêu trên là có thể được thực hiện thông qua một số giao diện. Những sự ghép nối gián tiếp hoặc các kết nối giao tiếp đó giữa các thiết bị hoặc các đơn vị là có thể được thực hiện về mặt điện tử, cơ học, hoặc các dạng khác.

Các đơn vị mà được mô tả dưới dạng các bộ phận riêng rẽ thì có thể là hoặc không phải là riêng rẽ về mặt vật lý, và các bộ phận mà được thể hiện dưới dạng các đơn vị thì có thể là hoặc không phải là các đơn vị vật lý, có thể được đặt tại một vị trí, hoặc có thể được rải rác trên nhiều đơn vị mạng. Một số hoặc tất cả trong số các đơn vị này có thể được chọn dựa trên các yêu cầu thực tế để đạt được các mục đích của các giải pháp theo các phương án này.

Ngoài ra, các đơn vị chức năng theo các phương án của sáng chế là có thể được tích hợp vào một đơn vị xử lý, hoặc mỗi trong số các đơn vị này có thể tồn tại một

mình về mặt vật lý, hoặc hai hay nhiều đơn vị được tích hợp vào một đơn vị.

Khi các chức năng này được thực hiện dưới dạng đơn vị chức năng phần mềm và được bán hoặc được sử dụng dưới dạng sản phẩm độc lập, thì các chức năng này có thể được lưu giữ trên phương tiện lưu trữ đọc được bằng máy tính. Dựa trên cách hiểu đó, thì các giải pháp kỹ thuật theo sáng chế, hoặc phần đóng góp vào công nghệ thông thường, hoặc một số trong số các giải pháp kỹ thuật này, là có thể được thực hiện dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm máy tính này được lưu giữ trên phương tiện lưu trữ, và bao gồm một số chỉ dẫn để chỉ dẫn cho thiết bị máy tính (có thể là máy tính cá nhân, máy chủ, hoặc thiết bị mạng) thực hiện toàn bộ hoặc một số trong số các bước của các phương pháp đã được mô tả theo các phương án của sáng chế. Phương tiện lưu trữ nêu trên bao gồm phương tiện bất kỳ mà có thể lưu giữ mã chương trình, ví dụ, ổ đĩa flash (ổ đĩa chớp nhoáng) USB (Universal Serial Bus - buýt nối tiếp vạn năng), đĩa cứng tháo ra được, bộ nhớ chỉ đọc (Read Only Memory - ROM), bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM), cơ cấu đĩa từ, hoặc đĩa quang.

Phần mô tả nêu trên chỉ là những cách thức thực hiện cụ thể của sáng chế chứ không nhằm giới hạn phạm vi bảo hộ của sáng chế. Bất kỳ phương án biến thể hoặc phương án thay thế nào mà người có hiểu biết trung bình trong lĩnh vực có thể tạo ra trong phạm vi kỹ thuật được bộc lộ của sáng chế thì cũng nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế là phạm vi bảo hộ của các điểm yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp thu thập khoá, trong đó phương pháp này bao gồm các bước:

gửi, bởi chức năng máy chủ xác thực, thông điệp yêu cầu dịch vụ xác thực đến chức năng quản lý dữ liệu hợp nhất;

nhận, bởi chức năng máy chủ xác thực, thông điệp đáp ứng dịch vụ xác thực được gửi bởi chức năng quản lý dữ liệu hợp nhất, trong đó thông điệp đáp ứng dịch vụ xác thực này bao gồm thông tin cho phép thứ nhất, và thông tin cho phép thứ nhất này được dùng để chỉ thị tạo ra khoá K_{AKMA} dành cho thiết bị người dùng (User Equipment - UE);

tạo ra, bởi chức năng máy chủ xác thực đáp lại thông điệp đáp ứng dịch vụ xác thực, K_{AKMA} và bộ nhận dạng khoá (Key IDentifier - KID) tương ứng với K_{AKMA}, dựa trên thông tin cho phép thứ nhất; và

gửi, bởi chức năng máy chủ xác thực, K_{AKMA} được tạo ra và KID được tạo ra đến chức năng mỏ neo xác thực và quản lý khoá dành cho các ứng dụng.

2. Phương pháp theo điểm 1, trong đó bước tạo ra, bởi chức năng máy chủ xác thực, KID là bao gồm bước:

tạo ra, bởi chức năng máy chủ xác thực, KID dựa trên thông tin định tuyến, bộ nhận dạng của UE, và bộ nhận dạng mạng di động đất liền công cộng (Public Land Mobile Network IDentifier - PLMN ID).

3. Phương pháp theo điểm 2, trong đó bộ nhận dạng của UE là bộ nhận dạng đăng ký cố định (SUbscription Permanent Identifier - SUPI).

4. Phương pháp theo điểm 1, trong đó bước tạo ra, bởi chức năng máy chủ xác thực, K_{AKMA} là bao gồm bước:

tạo ra, bởi chức năng máy chủ xác thực, K_{AKMA} dựa trên khoá K_{AUSF} và bộ nhận dạng của UE.

5. Thiết bị thu thập khoá, trong đó thiết bị này bao gồm:

bộ thu phát, được tạo cấu hình để: gửi thông điệp yêu cầu dịch vụ xác thực đến chức năng quản lý dữ liệu hợp nhất; và nhận thông điệp đáp ứng dịch vụ xác thực được

gửi bởi chức năng quản lý dữ liệu hợp nhất, trong đó thông điệp đáp ứng dịch vụ xác thực này bao gồm thông tin cho phép thứ nhất, và thông tin cho phép thứ nhất này được dùng để chỉ thị tạo ra khoá K_{AKMA} dành cho thiết bị người dùng (User Equipment - UE); và

bộ xử lý, được tạo cấu hình để tạo ra, đáp lại thông điệp đáp ứng dịch vụ xác thực này, K_{AKMA} và bộ nhận dạng khoá (Key IDentifier - KID) tương ứng với K_{AKMA} này, dựa trên thông tin cho phép thứ nhất, trong đó

bộ thu phát còn được tạo cấu hình để gửi K_{AKMA} được tạo ra và KID được tạo ra đến chức năng mỏ neo xác thực và quản lý khoá dành cho các ứng dụng.

6. Thiết bị theo điểm 5, trong đó bộ xử lý được tạo cấu hình cụ thể để tạo ra KID dựa trên thông tin định tuyến, bộ nhận dạng của UE, và bộ nhận dạng mạng di động đất liền công cộng (Public Land Mobile Network IDentifier - PLMN ID).

7. Thiết bị theo điểm 6, trong đó bộ nhận dạng của UE là bộ nhận dạng đăng ký cố định (SUbscription Permanent Identifier - SUPI).

8. Thiết bị theo điểm 5, trong đó bộ xử lý được tạo cấu hình cụ thể để tạo ra K_{AKMA} dựa trên khoá K_{AUSF} và bộ nhận dạng của UE.

9. Phương pháp thu thập khoá, được áp dụng cho chức năng quản lý truy cập và quản lý tính di động hoặc chức năng mỏ neo bảo mật, trong đó phương pháp này bao gồm các bước:

gửi thông điệp thứ nhất đến chức năng máy chủ xác thực, trong đó thông điệp thứ nhất này được sử dụng bởi chức năng máy chủ xác thực để gửi thông điệp thứ hai bao gồm chỉ thị thu thập sự cho phép đến chức năng quản lý dữ liệu hợp nhất và thu thập thông tin cho phép thứ nhất để tạo ra khoá K_{AKMA} và bộ nhận dạng khoá (Key IDentifier - KID) tương ứng với the K_{AKMA};

thu thập thông điệp thứ tư từ chức năng máy chủ xác thực; và

tạo ra thông điệp thứ năm dựa trên thông điệp thứ tư này, và gửi thông điệp thứ năm này đến UE, để UE thu thập KID và/hoặc K_{AKMA} dựa trên thông điệp thứ năm này.

10. Phương pháp theo điểm 9, trong đó thông điệp thứ năm bao gồm KID, và được dùng để cho phép UE thu thập KID trong thông điệp thứ năm, và/hoặc tạo ra K_{AKMA} dựa trên KID.

11. Phương pháp theo điểm 9, trong đó thông điệp thứ năm bao gồm thông tin chỉ thị thứ năm, và thông tin chỉ thị thứ năm này được dùng để chỉ thị cho UE tạo ra KID và/hoặc K_{AKMA}.

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 9 đến 11, trong đó trước khi thông điệp thứ tư được nhận, thì phương pháp này còn bao gồm bước:

gửi thông điệp thứ nhất đến chức năng máy chủ xác thực, để chức năng máy chủ xác thực tạo ra KID và/hoặc K_{AKMA} dựa trên thông điệp thứ nhất.

13. Thiết bị truyền thông, trong đó thiết bị này bao gồm ít nhất một bộ xử lý, và ít nhất một bộ xử lý này được ghép nối đến ít nhất một bộ nhớ; và

ít nhất một bộ xử lý này được tạo cấu hình để thực thi các chương trình máy tính hoặc các chỉ dẫn được lưu giữ trong ít nhất một bộ nhớ này, để cho phép thiết bị này thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 9 đến 12.

14. Phương tiện lưu trữ đọc được bằng máy tính, được tạo cấu hình để lưu giữ các chỉ dẫn, trong đó khi các chỉ dẫn này được thực thi, thì phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4 được thực hiện.

15. Phương tiện lưu trữ đọc được bằng máy tính, được tạo cấu hình để lưu giữ các chỉ dẫn, trong đó khi các chỉ dẫn này được thực thi, thì phương pháp theo điểm bất kỳ trong số các điểm từ 9 đến 12 được thực hiện.

16. Phương pháp thu thập khoá, trong đó phương pháp này bao gồm các bước:

gửi, bởi chức năng máy chủ xác thực, thông điệp yêu cầu dịch vụ xác thực đến chức năng quản lý dữ liệu hợp nhất;

gửi, bởi chức năng quản lý dữ liệu hợp nhất, thông điệp đáp ứng dịch vụ xác thực đến chức năng máy chủ xác thực, trong đó thông điệp đáp ứng dịch vụ xác thực này bao

gồm thông tin cho phép thứ nhất, và thông tin cho phép thứ nhất này được dùng để chỉ thị tạo ra khoá K_{AKMA} dành cho thiết bị người dùng (User Equipment - UE);

tạo ra, bởi chức năng máy chủ xác thực đáp lại thông điệp đáp ứng dịch vụ xác thực, K_{AKMA} và bộ nhận dạng khoá (Key IDentifier - KID) tương ứng với K_{AKMA}, dựa trên thông tin cho phép thứ nhất; và

gửi, bởi chức năng máy chủ xác thực, K_{AKMA} được tạo ra và KID được tạo ra đến chức năng mỏ neo xác thực và quản lý khoá dành cho các ứng dụng.

17. Phương pháp theo điểm 16, trong đó bước tạo ra, bởi chức năng máy chủ xác thực, KID là bao gồm bước:

tạo ra, bởi chức năng máy chủ xác thực, KID dựa trên thông tin định tuyến, bộ nhận dạng của UE, và bộ nhận dạng mạng di động đất liền công cộng (Public Land Mobile Network IDentifier - PLMN ID).

18. Phương pháp theo điểm 17, trong đó bộ nhận dạng của UE là bộ nhận dạng đăng ký cố định (SUbscription Permanent Identifier - SUPI).

19. Phương pháp theo điểm 16, trong đó bước tạo ra, bởi chức năng máy chủ xác thực, K_{AKMA} là bao gồm bước:

tạo ra, bởi chức năng máy chủ xác thực, K_{AKMA} dựa trên khoá K_{AUSF} và bộ nhận dạng của UE.

20. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 19, trong đó trước bước gửi, bởi chức năng máy chủ xác thực, thông điệp yêu cầu dịch vụ xác thực đến chức năng quản lý dữ liệu hợp nhất, thì phương pháp này còn bao gồm bước:

nhận, bởi chức năng máy chủ xác thực, yêu cầu dịch vụ xác thực được gửi bởi chức năng mỏ neo bảo mật.

21. Phương pháp theo điểm 20, trong đó phương pháp này còn bao gồm bước:

gửi, bởi chức năng máy chủ xác thực, đáp ứng dịch vụ xác thực đến chức năng mỏ neo bảo mật.

22. Hệ thống thu thập khoá, trong đó hệ thống này bao gồm:

chức năng máy chủ xác thực được tạo cấu hình để gửi thông điệp yêu cầu dịch vụ xác thực đến chức năng quản lý dữ liệu hợp nhất, trong đó

chức năng quản lý dữ liệu hợp nhất được tạo cấu hình để gửi thông điệp đáp ứng dịch vụ xác thực đến chức năng máy chủ xác thực, trong đó thông điệp đáp ứng dịch vụ xác thực này bao gồm thông tin cho phép thứ nhất, và thông tin cho phép thứ nhất này được dùng để chỉ thị tạo ra khoá K_{AKMA} dành cho thiết bị người dùng (User Equipment - UE); và

chức năng máy chủ xác thực còn được tạo cấu hình để: tạo ra, đáp lại thông điệp đáp ứng dịch vụ xác thực này, K_{AKMA} và bộ nhận dạng khoá (Key IDentifier - KID) tương ứng với K_{AKMA} này, dựa trên thông tin cho phép thứ nhất; và gửi K_{AKMA} được tạo ra và KID được tạo ra đến chức năng mỏ neo xác thực và quản lý khoá dành cho các ứng dụng.

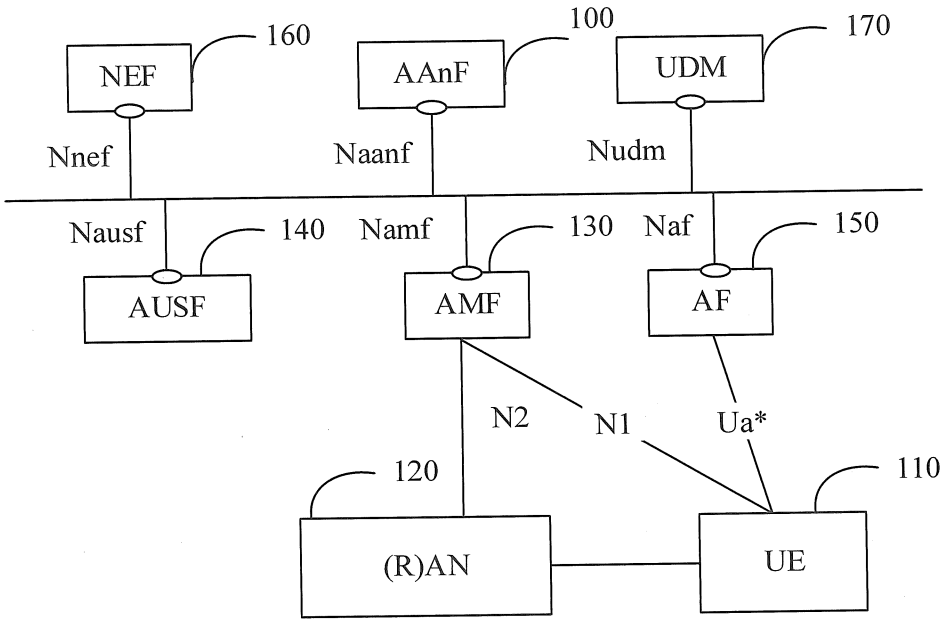
23. Hệ thống theo điểm 22, trong đó bước tạo ra KID là bao gồm bước: tạo ra KID dựa trên thông tin định tuyến, bộ nhận dạng của UE, và bộ nhận dạng mạng di động đất liền công cộng (Public Land Mobile Network IDentifier - PLMN ID).

24. Hệ thống theo điểm 23, trong đó bộ nhận dạng của UE là bộ nhận dạng đăng ký cố định (SUbscription Permanent Identifier - SUPI).

25. Hệ thống theo điểm 22, trong đó bước tạo ra K_{AKMA} là bao gồm bước: tạo ra K_{AKMA} dựa trên khoá K_{AUSF} và bộ nhận dạng của UE.

26. Hệ thống theo điểm bất kỳ trong số các điểm từ 22 đến 25, trong đó chức năng máy chủ xác thực còn được tạo cấu hình để nhận yêu cầu dịch vụ xác thực được gửi bởi chức năng mỏ neo bảo mật.

27. Hệ thống theo điểm 26, trong đó chức năng máy chủ xác thực còn được tạo cấu hình để gửi đáp ứng dịch vụ xác thực đến chức năng mỏ neo bảo mật.



NEF: Chức năng bộc lộ mạng

AUSF: Chức năng máy chủ xác thực

AAnF: Chức năng mỏ neo xác thực và quản lý khoá dành cho các ứng dụng

AMF: Chức năng quản lý truy cập và quản lý tính di động

UDM: Quản lý dữ liệu hợp nhất

AF: Chức năng ứng dụng

UE: Thiết bị người dùng

(R)AN: Mạng truy cập (vô tuyến)

Fig.1

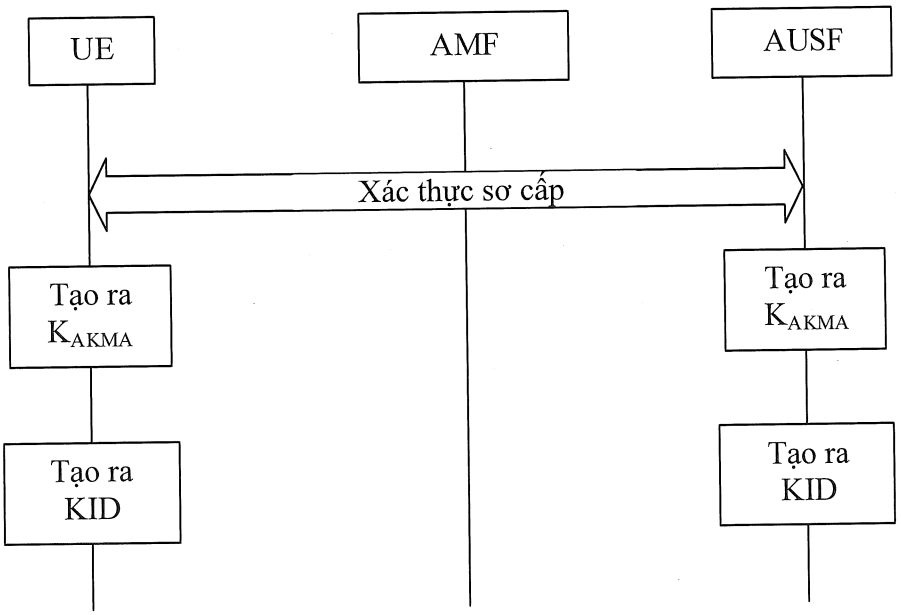


Fig.2

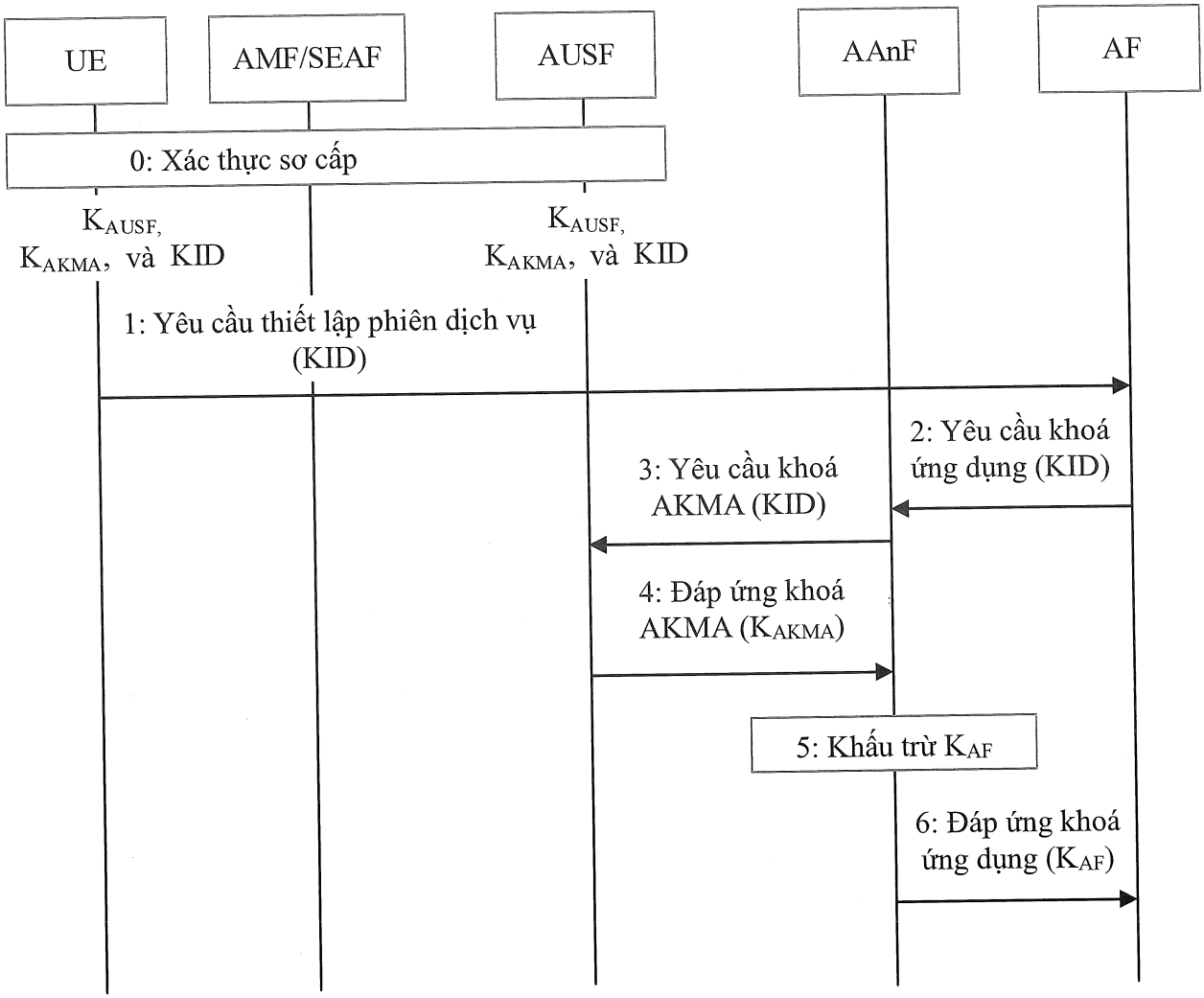

UE
AMF/SEAF
AUSF
AAnF
AF
0: Xác thực sơ cấp
K_{AUSF}, K_{AKMA}, và KID
K_{AUSF}, K_{AKMA}, và KID
1: Yêu cầu thiết lập phiên dịch vụ (KID)
2: Yêu cầu khoá ứng dụng (KID)
3: Yêu cầu khoá AKMA (KID)
4: Đáp ứng khoá AKMA (K_{AKMA})
5: Khấu trừ K_{AF}
6: Đáp ứng khoá ứng dụng (K_{AF})

Fig.3

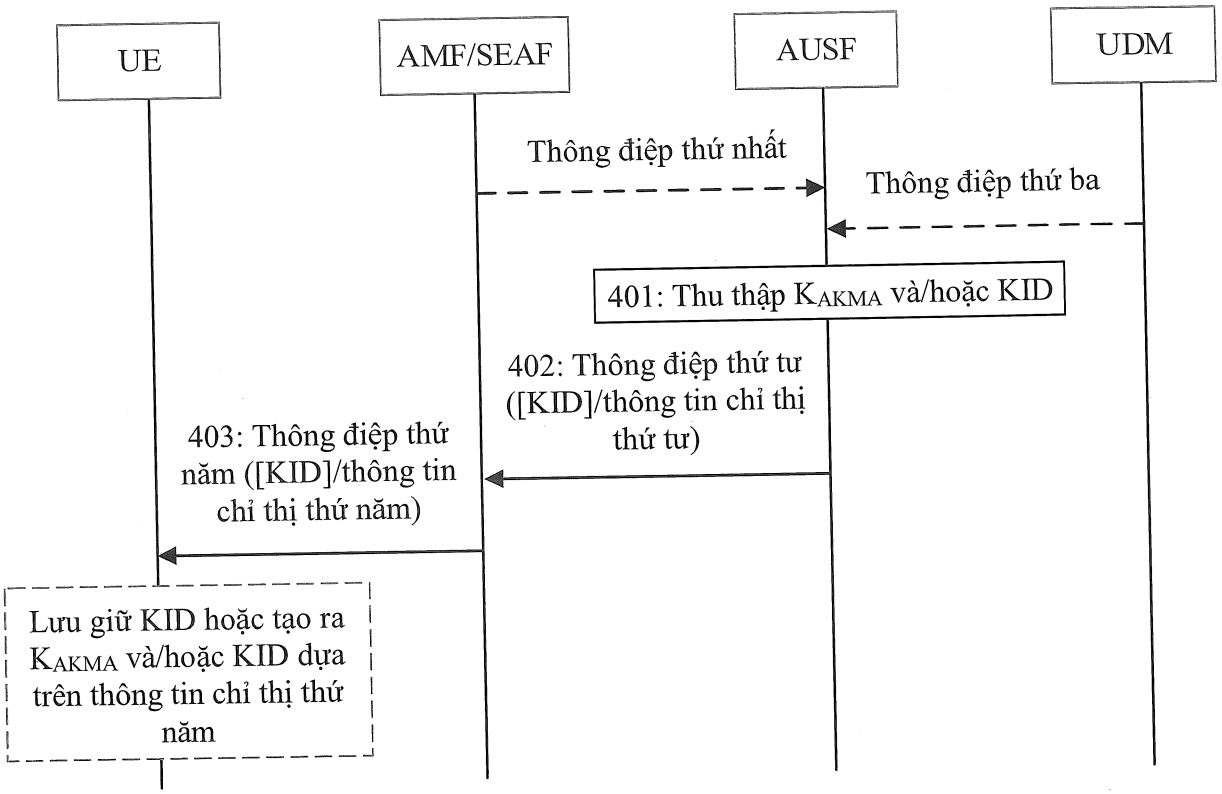

UE
AMF/SEAF
AUSF
UDM
Thông điệp thứ nhất
Thông điệp thứ ba
401: Thu thập KAKMA và/hoặc KID
402: Thông điệp thứ tư ([KID]/thông tin chỉ thị thứ tư)
403: Thông điệp thứ năm ([KID]/thông tin chỉ thị thứ năm)
Lưu giữ KID hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ năm

Fig.4A

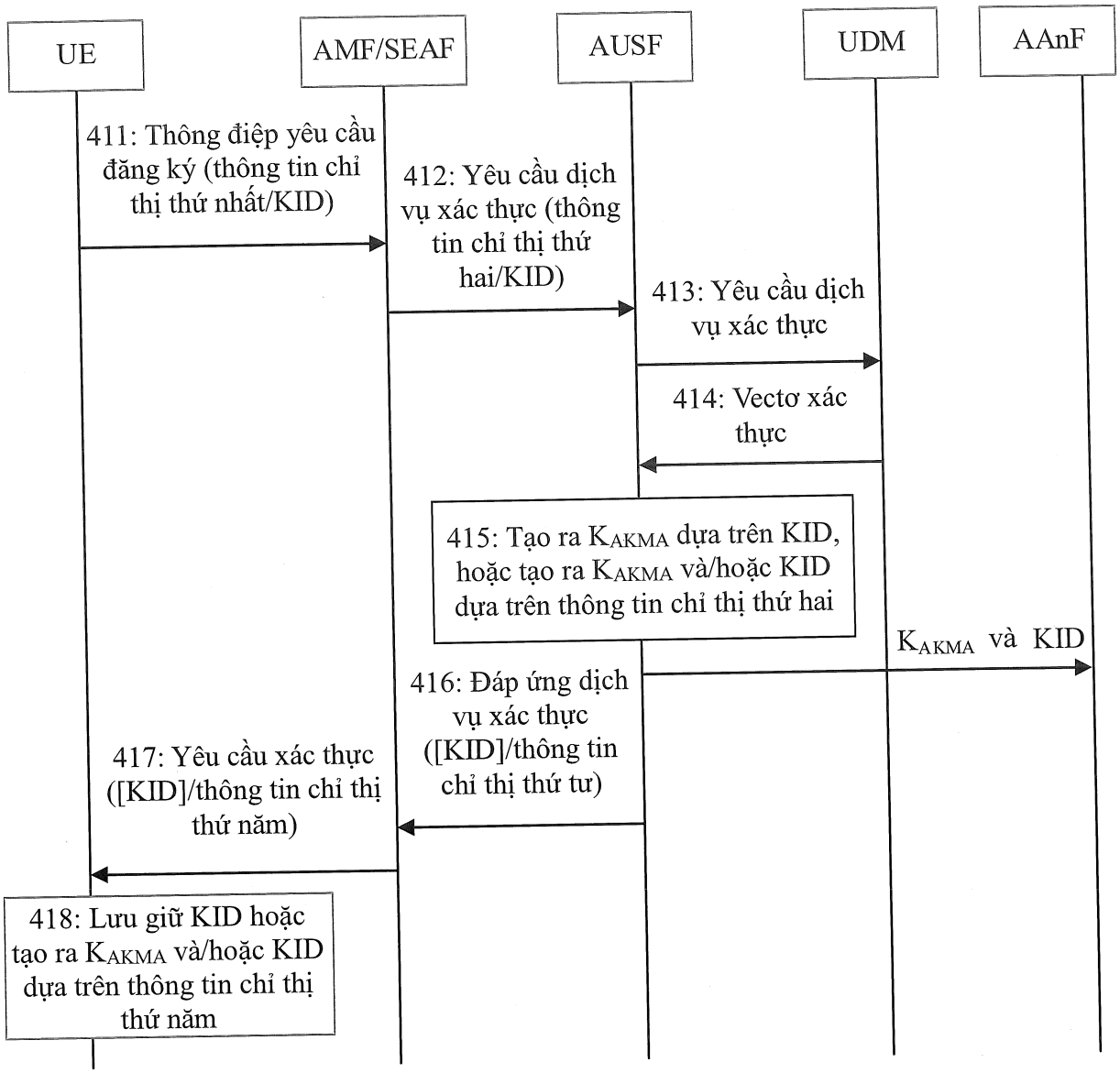

UE
AMF/SEAF
AUSF
UDM
AAnF
411: Thông điệp yêu cầu đăng ký (thông tin chỉ thị thứ nhất/KID)
412: Yêu cầu dịch vụ xác thực (thông tin chỉ thị thứ hai/KID)
413: Yêu cầu dịch vụ xác thực
414: Vectơ xác thực
415: Tạo ra KAKMA dựa trên KID, hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ hai
KAKMA và KID
416: Đáp ứng dịch vụ xác thực ([KID]/thông tin chỉ thị thứ tư)
417: Yêu cầu xác thực ([KID]/thông tin chỉ thị thứ năm)
418: Lưu giữ KID hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ năm

Fig.4B

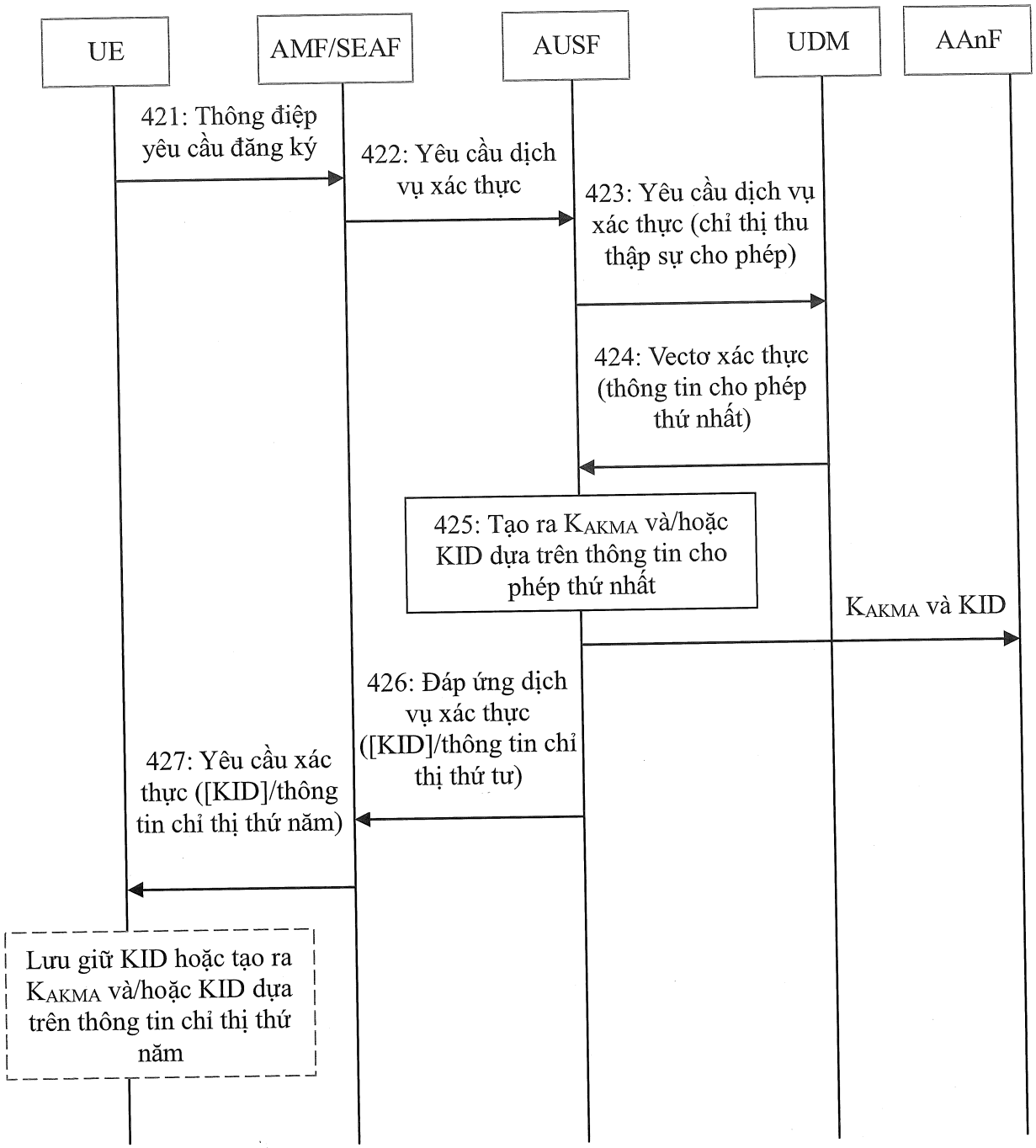

UE
AMF/SEAF
AUSF
UDM
AAnF
421: Thông điệp yêu cầu đăng ký
422: Yêu cầu dịch vụ xác thực
423: Yêu cầu dịch vụ xác thực (chỉ thị thu thập sự cho phép)
424: Vectơ xác thực (thông tin cho phép thứ nhất)
425: Tạo ra KAKMA và/hoặc KID dựa trên thông tin cho phép thứ nhất
KAKMA và KID
426: Đáp ứng dịch vụ xác thực ([KID]/thông tin chỉ thị thứ tư)
427: Yêu cầu xác thực ([KID]/thông tin chỉ thị thứ năm)
Lưu giữ KID hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ năm

Fig.4C

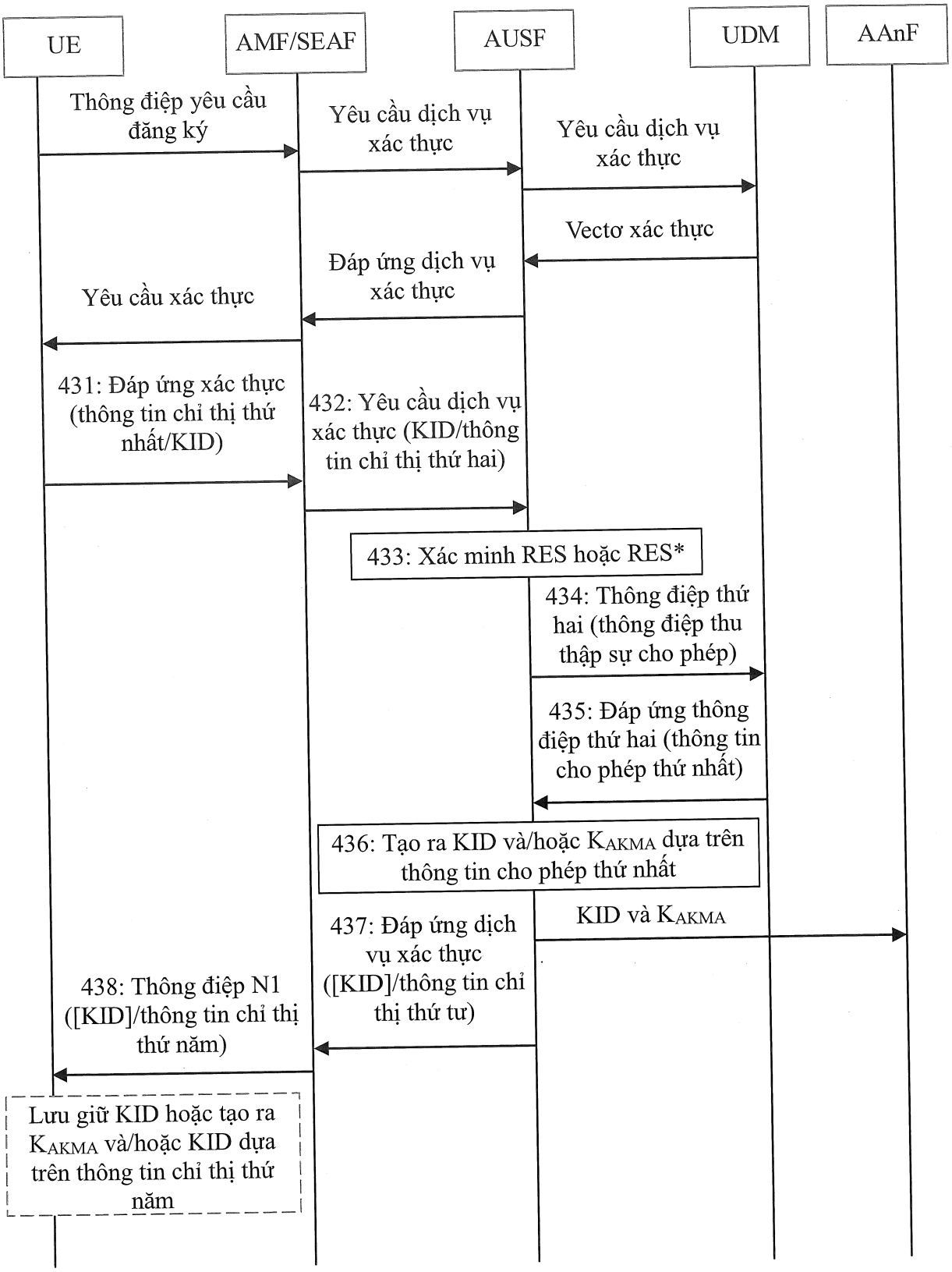

UE
AMF/SEAF
AUSF
UDM
AAnF
Thông điệp yêu cầu đăng ký
Yêu cầu dịch vụ xác thực
Yêu cầu dịch vụ xác thực
Vectơ xác thực
Đáp ứng dịch vụ xác thực
Yêu cầu xác thực
431: Đáp ứng xác thực (thông tin chỉ thị thứ nhất/KID)
432: Yêu cầu dịch vụ xác thực (KID/thông tin chỉ thị thứ hai)
433: Xác minh RES hoặc RES*
434: Thông điệp thứ hai (thông điệp thu thập sự cho phép)
435: Đáp ứng thông điệp thứ hai (thông tin cho phép thứ nhất)
436: Tạo ra KID và/hoặc KAKMA dựa trên thông tin cho phép thứ nhất
KID và KAKMA
437: Đáp ứng dịch vụ xác thực ([KID]/thông tin chỉ thị thứ tư)
438: Thông điệp N1 ([KID]/thông tin chỉ thị thứ năm)
Lưu giữ KID hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ năm

Fig.4D

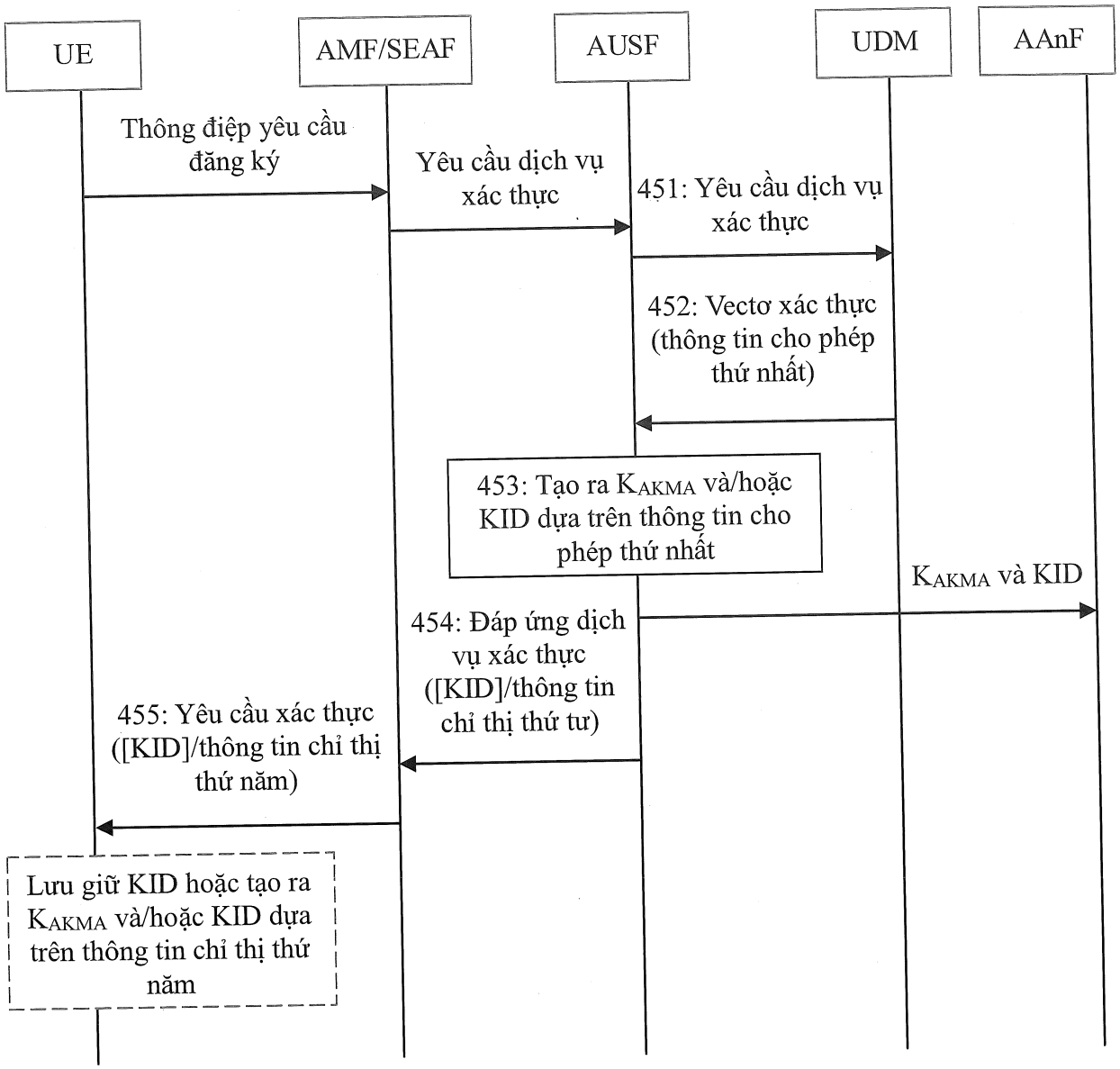

UE
AMF/SEAF
AUSF
UDM
AAnF
Thông điệp yêu cầu đăng ký
Yêu cầu dịch vụ xác thực
451: Yêu cầu dịch vụ xác thực
452: Vectơ xác thực (thông tin cho phép thứ nhất)
453: Tạo ra KAKMA và/hoặc KID dựa trên thông tin cho phép thứ nhất
KAKMA và KID
454: Đáp ứng dịch vụ xác thực ([KID]/thông tin chỉ thị thứ tư)
455: Yêu cầu xác thực ([KID]/thông tin chỉ thị thứ năm)
Lưu giữ KID hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ năm

Fig.4E

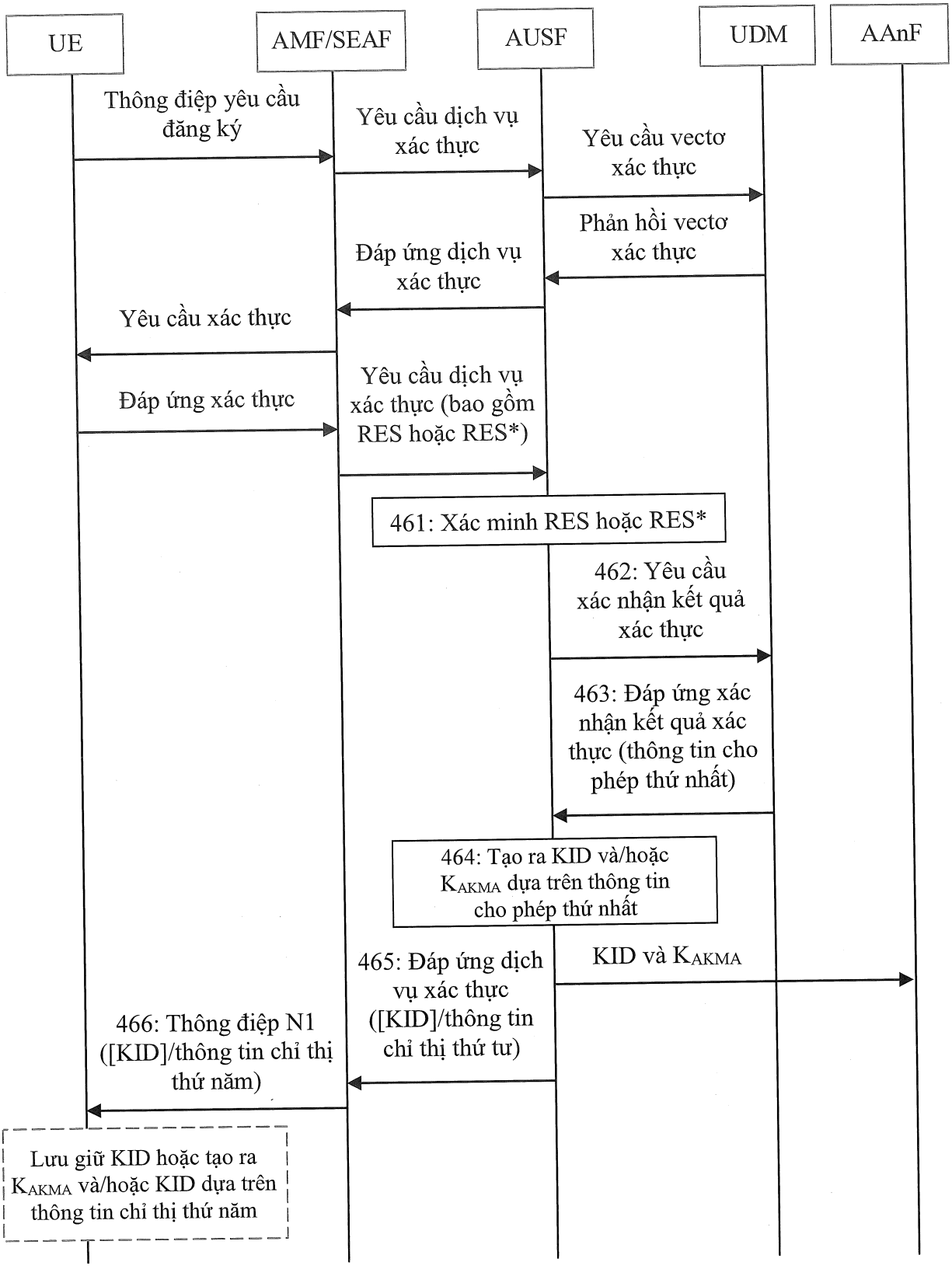

UE
AMF/SEAF
AUSF
UDM
AAnF
Thông điệp yêu cầu đăng ký
Yêu cầu dịch vụ xác thực
Yêu cầu vectơ xác thực
Phản hồi vectơ xác thực
Đáp ứng dịch vụ xác thực
Yêu cầu xác thực
Đáp ứng xác thực
Yêu cầu dịch vụ xác thực (bao gồm RES hoặc RES*)
461: Xác minh RES hoặc RES*
462: Yêu cầu xác nhận kết quả xác thực
463: Đáp ứng xác nhận kết quả xác thực (thông tin cho phép thứ nhất)
464: Tạo ra KID và/hoặc KAKMA dựa trên thông tin cho phép thứ nhất
KID và KAKMA
465: Đáp ứng dịch vụ xác thực ([KID]/thông tin chỉ thị thứ tư)
466: Thông điệp N1 ([KID]/thông tin chỉ thị thứ năm)
Lưu giữ KID hoặc tạo ra KAKMA và/hoặc KID dựa trên thông tin chỉ thị thứ năm

Fig.4F

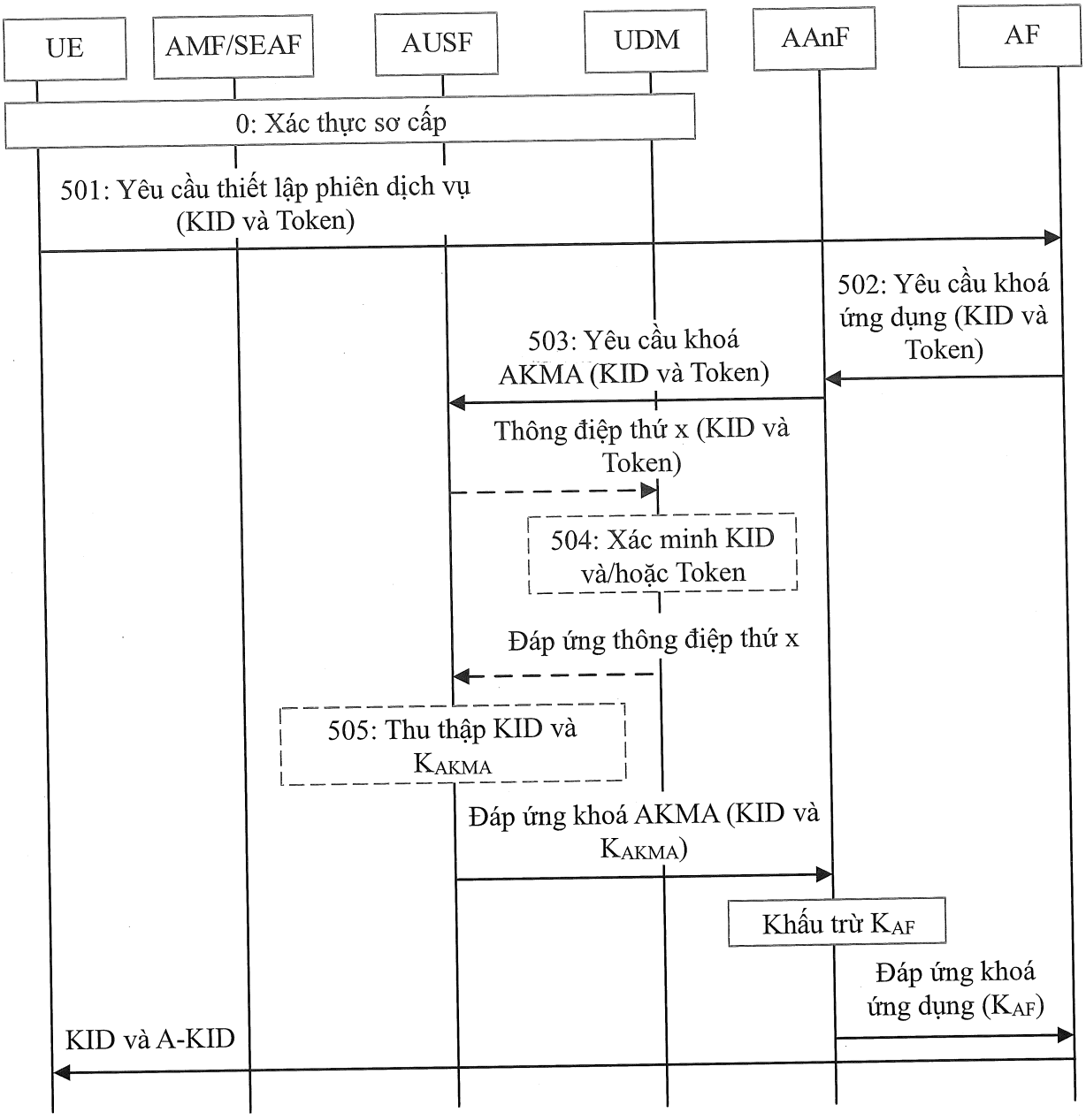

UE
AMF/SEAF
AUSF
UDM
AAnF
AF
0: Xác thực sơ cấp
501: Yêu cầu thiết lập phiên dịch vụ (KID và Token)
502: Yêu cầu khoá ứng dụng (KID và Token)
503: Yêu cầu khoá AKMA (KID và Token)
Thông điệp thứ x (KID và Token)
504: Xác minh KID và/hoặc Token
Đáp ứng thông điệp thứ x
505: Thu thập KID và KAKMA
Đáp ứng khoá AKMA (KID và KAKMA)
Khấu trừ KAF
Đáp ứng khoá ứng dụng (KAF)
KID và A-KID

Fig.5

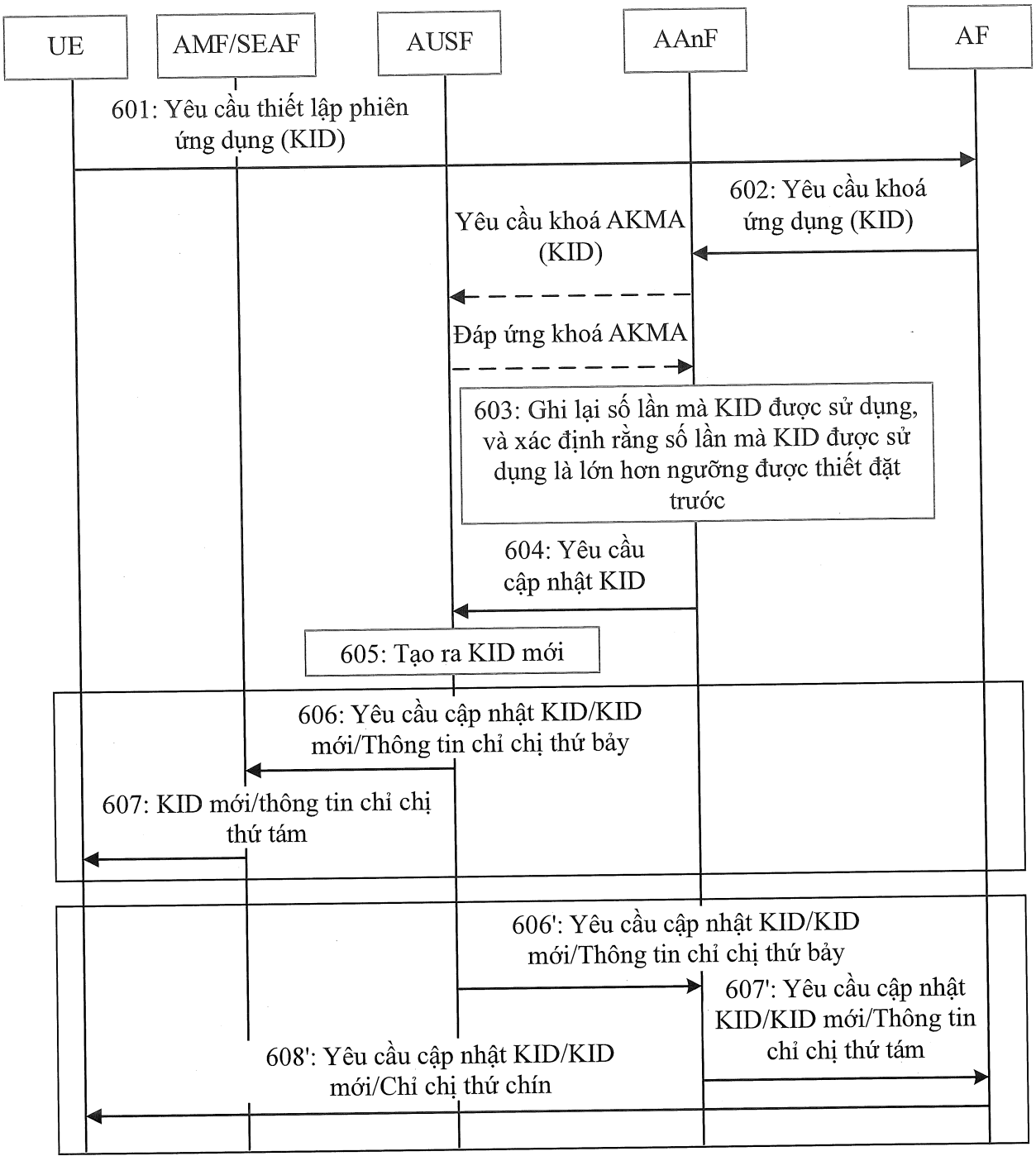

UE
AMF/SEAF
AUSF
AAnF
AF
601: Yêu cầu thiết lập phiên ứng dụng (KID)
602: Yêu cầu khoá ứng dụng (KID)
Yêu cầu khoá AKMA (KID)
Đáp ứng khoá AKMA
603: Ghi lại số lần mà KID được sử dụng, và xác định rằng số lần mà KID được sử dụng là lớn hơn ngưỡng được thiết đặt trước
604: Yêu cầu cập nhật KID
605: Tạo ra KID mới
606: Yêu cầu cập nhật KID/KID mới/Thông tin chỉ chị thứ bảy
607: KID mới/thông tin chỉ chị thứ tám
606': Yêu cầu cập nhật KID/KID mới/Thông tin chỉ chị thứ bảy
607': Yêu cầu cập nhật KID/KID mới/Thông tin chỉ chị thứ tám
608': Yêu cầu cập nhật KID/KID mới/Chỉ chị thứ chín

Fig.6A

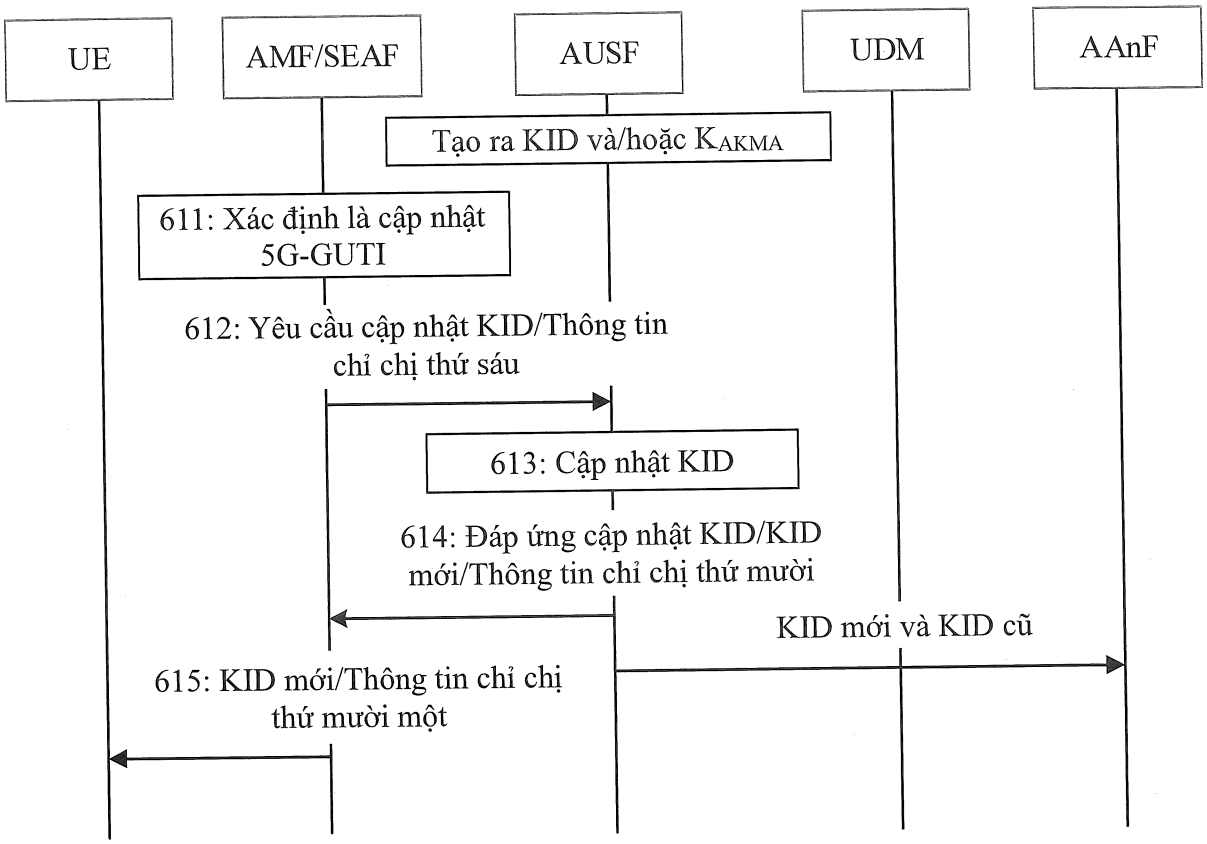

UE
AMF/SEAF
AUSF
UDM
AAnF
Tạo ra KID và/hoặc KAKMA
611: Xác định là cập nhật 5G-GUTI
612: Yêu cầu cập nhật KID/Thông tin chỉ chị thứ sáu
613: Cập nhật KID
614: Đáp ứng cập nhật KID/KID mới/Thông tin chỉ chị thứ mười
KID mới và KID cũ
615: KID mới/Thông tin chỉ chị thứ mười một

Fig.6B

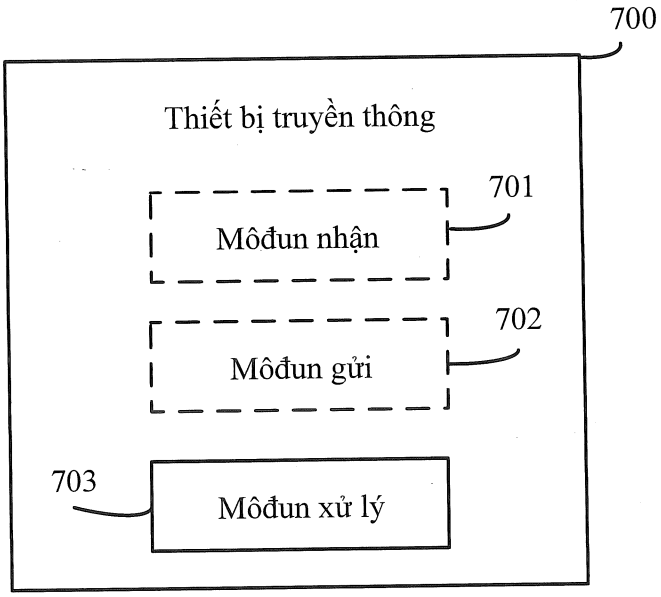

700
Thiết bị truyền thông
701
Môđun nhận
702
Môđun gửi
703
Môđun xử lý

Fig.7

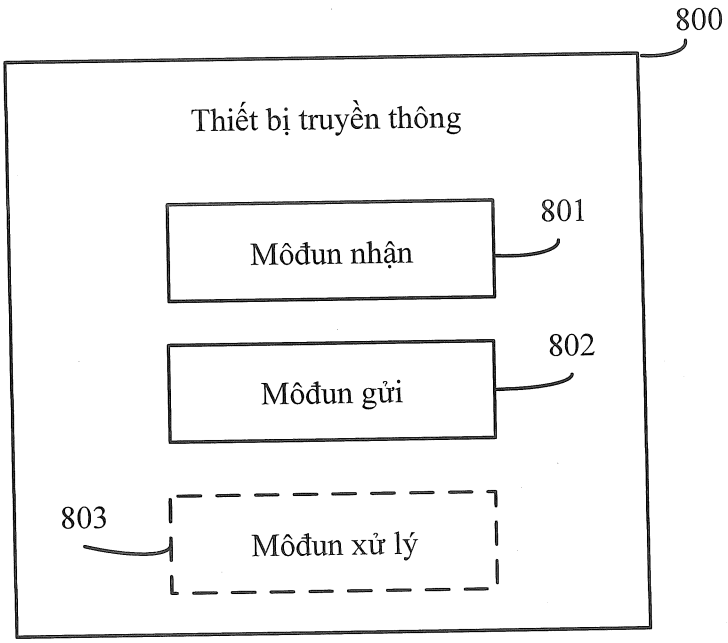

800
Thiết bị truyền thông
801
Môđun nhận
802
Môđun gửi
803
Môđun xử lý

Fig.8

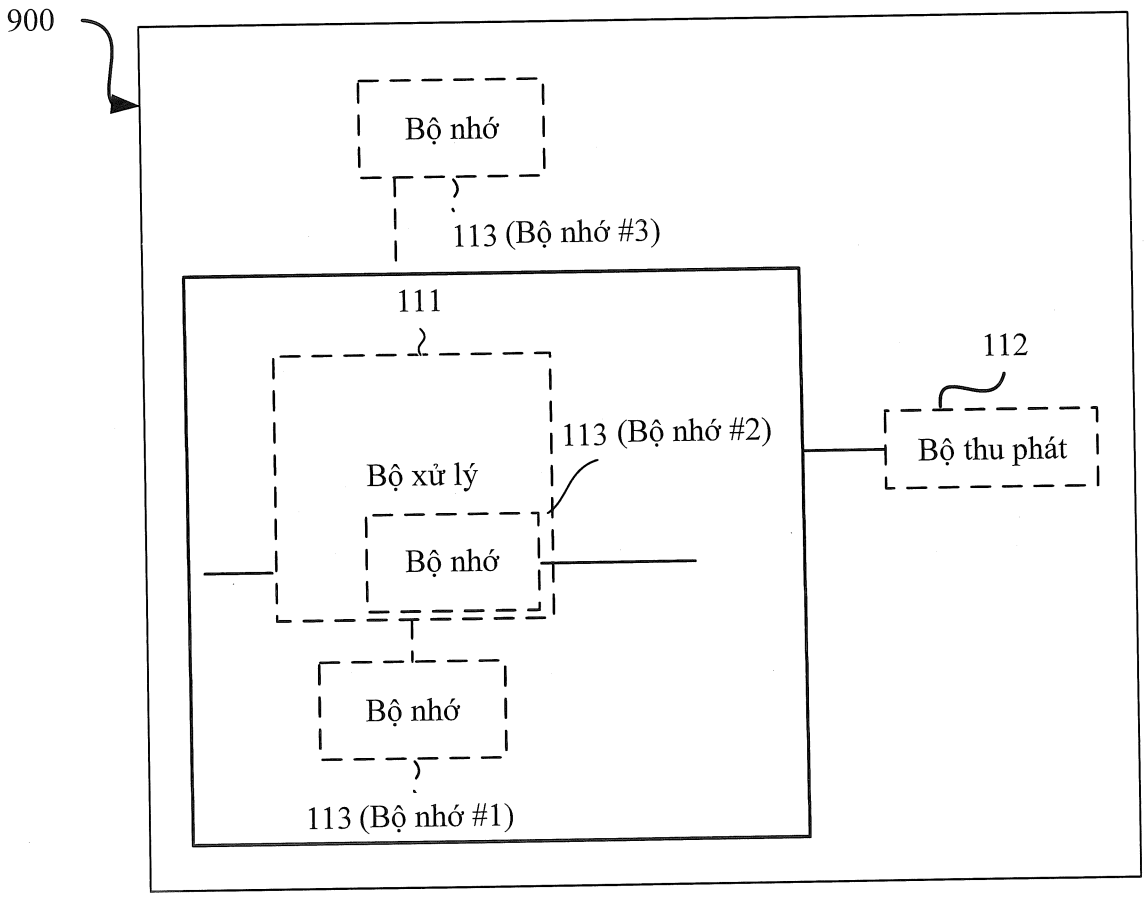

900
Bộ nhớ
113 (Bộ nhớ #3)
111
112
113 (Bộ nhớ #2)
Bộ thu phát
Bộ xử lý
Bộ nhớ
Bộ nhớ
113 (Bộ nhớ #1)

Fig.9