(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) **1-0047462**

(51)[2020.01] **H04W 12/06**; H04W 12/04

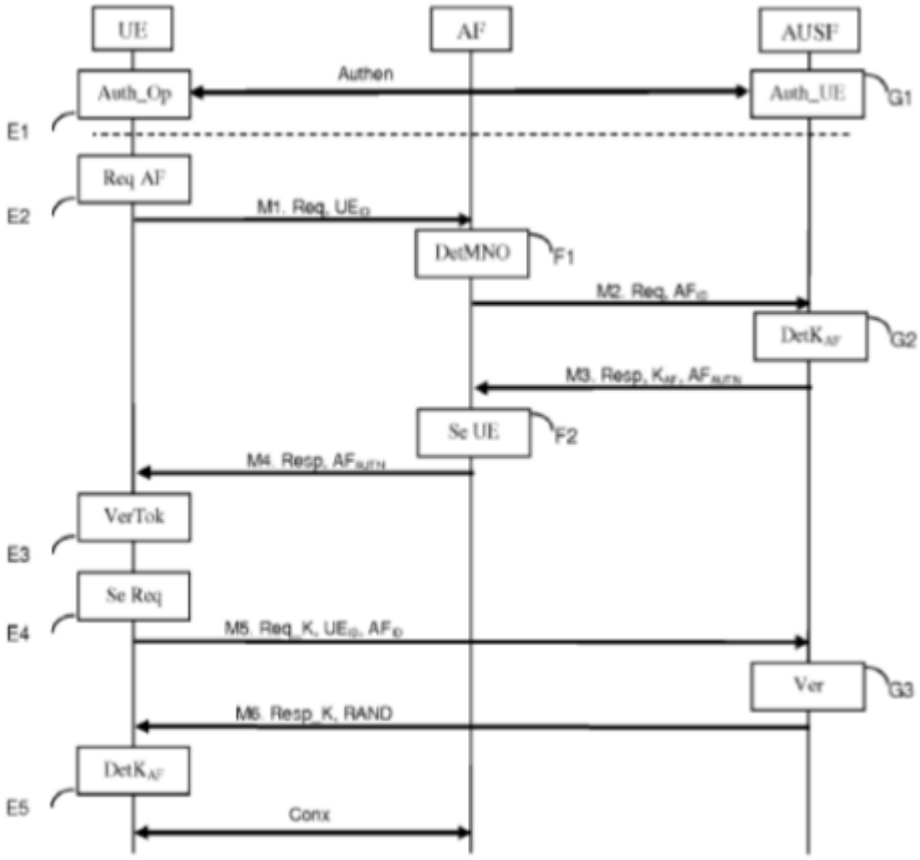
(13) **B**

(21) 1-2020-04354
(22) 11/01/2019
(86) PCT/FR2019/050056 11/01/2019
(87) WO 2019/141924 25/07/2019
(30) 1850440 19/01/2018 FR
(45) 25/06/2025 447
(43) 25/03/2021 396A
(73) ORANGE (FR)
78 rue Olivier de Serres, 75015 Paris, France
(72) GAMISHEV, Todor (FR).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG XÁC ĐỊNH KHOÁ NHẰM TẠO RA TRUYỀN THÔNG GIỮA THIẾT BỊ NGƯỜI DÙNG VÀ MÁY CHỦ ỨNG DỤNG MỘT CÁCH AN TOÀN, THIẾT BỊ NGƯỜI DÙNG, VÀ MÁY CHỦ XÁC THỰC CỦA MẠNG TRUYỀN THÔNG DI ĐỘNG

(21) 1-2020-04354

(57) Sáng chế đề cập đến phương pháp xác định khoá để đảm bảo an toàn truyền thông giữa thiết bị người dùng (10) và máy chủ ứng dụng (40). Máy chủ xác thực (20) của mạng truyền thông di động và thiết bị người dùng tạo ra khoá chính bí mật trong thủ tục xác thực. Thiết bị người dùng này gửi đến máy chủ xác thực yêu cầu khoá để truyền thông với máy chủ ứng dụng và tiếp nhận biến ngẫu nhiên. Máy chủ xác thực và thiết bị người dùng tính toán khoá được yêu cầu bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và máy chủ ứng dụng mã nhận diện bằng cách sử dụng khoá chính.



HÌNH 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực viễn thông nói chung.

Cụ thể hơn, sáng chế đề cập đến kỹ thuật để xác định khoá nhằm tạo ra sự truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn.

Kỹ thuật để xác định khoá có thể áp dụng được cho lĩnh vực mạng truyền thông di động.

Tình trạng kỹ thuật của sáng chế

Để cho phép thiết bị người dùng UE (còn được gọi là thiết bị đầu cuối) truyền thông một cách an toàn với máy chủ ứng dụng, kiến trúc được gọi là kiến trúc tự khởi động (generic bootstrapping architecture - GBA) đã được định nghĩa bởi tổ chức chuẩn hoá 3GPP, trong nội dung về mạng di động, ví dụ mạng di động thế hệ thứ tư. Kiến trúc này được định nghĩa trong phần thông số kỹ thuật được tham chiếu 3GPP TS 33.220 phiên bản V15.1.0, có tiêu đề là "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Phát hành lần thứ 15)". Trong GBA, điều khoản được tạo ra cho hàm máy chủ tự khởi động (bootstrapping server function - BSF), mà tiến hành sự xác thực của thiết bị đầu cuối và cho phép khoá chính Ks được liên kết với mã nhận diện giao dịch tự khởi động B_TID được xác định. Khi khoá chính Ks này đã được xác định, thiết bị đầu cuối và BSF lấy khoá Ks_NAF từ khoá chính Ks để tạo ra sự trao đổi với máy chủ ứng dụng NAF một cách an toàn. Chính xác hơn là, khoá Ks_NAF này được lấy từ khoá chính Ks bằng cách sử dụng hàm phát sinh khoá KDF cho các tham số phát sinh khoá. Cụ thể là các tham số này bao gồm mã nhận diện NAF_Id của máy chủ ứng dụng và số ngẫu nhiên RAND được sử dụng trong quá trình xác thực. Khi kết thúc các hành động này, thiết bị đầu cuối và BSF chia sẻ khoá Ks_NAF nhằm sử dụng để tạo ra các trao đổi giữa thiết bị đầu cuối và máy chủ ứng dụng NAF một cách an toàn. Sau đó, máy chủ ứng dụng NAF yêu cầu khoá Ks_NAF liên kết với mã nhận diện giao dịch B_TID từ BSF. Sau đó, thiết bị đầu cuối và máy chủ ứng dụng NAF có thể truyền thông một cách an toàn bằng khoá Ks_NAF.

Trong ngữ cảnh này, nhà khai thác mạng di động là trung gian mà sử dụng các bí mật được chia sẻ giữa máy chủ thuê bao thường trú (home subscriber system - HSS) và môđun an toàn của thiết bị đầu cuối để đảm bảo an toàn của liên kết giữa máy chủ ứng dụng NAF và thiết bị đầu cuối UE mà không cần hai thực thể này chia sẻ bí mật.

Việc đưa GBA này vào trong mạng của nhà khai thác di động dẫn đến các chi phí đáng kể, cụ thể là do việc đưa BSF vào và do sự giao tiếp của chúng với mạng di động.

Hơn nữa, hiện nay điều khoản không được được tạo ra cho hàm tương tự với hàm GBA này ở các mạng di động thế hệ thứ năm (5G), mà đang trong quá trình được chuẩn hoá bởi tổ chức 3GPP.

Bản chất kỹ thuật của sáng chế

Một trong những mục đích của sáng chế là khắc phục những thiếu sót/nhược điểm của các giải pháp kỹ thuật đã biết, và/hoặc đưa ra những cải thiện đối với chúng.

Theo khía cạnh thứ nhất, một đối tượng của sáng chế là phương pháp xác định khoá nhằm tạo ra sự truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn. Phương pháp này bao gồm bước, trong thiết bị người dùng:

- xác thực thiết bị người dùng bằng máy chủ xác thực của mạng truyền thông di động, khoá chính bí mật được tạo ra, trong suốt quá trình xác thực đã nêu, bởi thiết bị người dùng và máy chủ xác thực;

- gửi bởi thiết bị người dùng, đến máy chủ xác thực yêu cầu khoá với mục đích truyền thông với máy chủ ứng dụng;

- tính toán khoá này bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính, biến ngẫu nhiên này đang được tiếp nhận bởi thiết bị người dùng từ máy chủ xác thực.

Tương ứng là, phương pháp xác định khoá nhằm tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn bao gồm bước, trong máy chủ xác thực:

- xác thực thiết bị người dùng bằng máy chủ xác thực của mạng truyền thông di động, khoá chính bí mật được tạo ra, trong suốt quá trình xác thực đã nêu, bởi thiết bị người dùng và máy chủ xác thực;

- tiếp nhận bởi máy chủ xác thực yêu cầu khoá mà đã được gửi bởi thiết bị người dùng với mục đích truyền thông với máy chủ ứng dụng;

- gửi biến ngẫu nhiên bởi máy chủ xác thực đến thiết bị người dùng;

- tính toán khoá này bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính.

Nhờ kỹ thuật này, khoá cho phép truyền thông giữa thiết bị người dùng và máy chủ ứng dụng được tạo ra một cách an toàn thu được từ khoá chính được tạo ra trong quá trình xác thực được thực hiện bởi máy chủ xác thực của mạng truyền thông di động. Do đó, kỹ thuật được thực hiện bởi máy chủ xác thực mà đã được tích hợp vào và do đó được giao tiếp với mạng truyền thông di động, và cụ thể là với máy chủ mà quản lý dữ liệu người dùng. Không cần phải cung cấp máy chủ chuyên dụng, tức là máy chủ được gọi là máy chủ tự khởi động, để xác định khoá này. Ngoài ra, khoá này được tính một cách độc lập với quá trình xác thực: biến ngẫu nhiên được sử dụng để tính toán một cách độc lập khoá với khoá được sử dụng để xác thực. Do đó, khoá chính và khoá thu được được tách riêng ra, các biến ngẫu nhiên phân biệt đã được sử dụng. Do đó có khả năng thu được nhiều khoá theo yêu cầu, miễn là khoá chính chưa bị hết hạn. Khi đã thu được khoá, khoá này vẫn giữ hiệu lực thậm chí khi khoá chính được thay đổi. Sự truyền thông an toàn bởi khoá được tính sau đó có thể được thiết lập giữa thiết bị người dùng và máy chủ ứng dụng.

Các phương án hoặc các dấu hiệu khác nhau được đề cập dưới đây có thể được bổ sung một cách độc lập hoặc được kết hợp với nhau vào phương pháp như được xác định trên đây để xác định khoá.

Theo một phương án cụ thể, máy chủ xác thực phân phối đến máy chủ ứng dụng khoá mà đã được tính toán.

Theo một phương án cụ thể về phương pháp xác định khoá, quá trình xác thực này được kích hoạt trong quá trình đăng ký của thiết bị người dùng với mạng truyền thông di động.

Do đó, kỹ thuật được đề xuất lấy ưu điểm của việc xác thực mà được thực hiện trong quá quá trình đăng ký của thiết bị người dùng với mạng truyền thông di động. Cụ thể là, trong

thủ tục xác thực hiện tại trong quy trình chuẩn hoá bởi tổ chức 3GPP đối với các hệ thống thế hệ thứ năm (5G), mà thủ tục được xác định trong tài liệu kỹ thuật 3GPP TS 33.501 V0.6.0 (2017-12) "Security Architecture and Procedures for 5G System (Phát hành lần thứ 15)", khoá chính K_{AUSF} được xác định bởi thiết bị người dùng và máy chủ thực thi hàm máy chủ xác thực (AUSF). Đối với quá trình xác thực EAP-AKA', khoá chính K_{AUSF} được xác định từ khoá phiên chính mở rộng (extended master session key - EMSK). Đối với sự xác thực 5G AKA, khoá chính K_{AUSF} thu được từ sự mã hoá và các khoá toàn vẹn. Trong phiên bản hiện tại của nó, và cụ thể là đoạn 6.2.2.1, tài liệu kỹ thuật TS 33.501 chỉ ra rằng máy chủ xác thực có khả năng lưu trữ khoá chính K_{AUSF} này, mà được tạo ra giữa thủ tục xác thực và các thủ tục được tiến hành giữa các thực thể của mạng truyền thông di động và thiết bị người dùng để đồng ý các khoá này, trong bộ nhớ. tài liệu kỹ thuật này cũng chỉ ra, trong đoạn 6.2.1, trong lưu ý của soạn giả, rằng khi máy chủ xác thực lưu trữ khoá chính K_{AUSF} này trong bộ nhớ, việc thiết bị người dùng có cần lưu trữ nó trong bộ nhớ hay không là đối tượng của nghiên cứu trong tương lai. Sẽ được hiểu rằng, để thực hiện kỹ thuật xác định được đề xuất, khoá chính K_{AUSF} phải được lưu trữ trong bộ nhớ cả bởi máy chủ xác thực và thiết bị người dùng. Vì khoá chính K_{AUSF} này được sử dụng để lấy khoá nhằm tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, cần thiết phải tiến hành thủ tục xác thực mới riêng cho truyền thông này với máy chủ ứng dụng, không giống như trong thủ tục GBA hiện tại mà thủ tục xác thực mới được yêu cầu. Do đó không cần phải yêu cầu bộ phận an toàn của thiết bị người dùng mỗi lần thiết bị người dùng muốn truyền thông với máy chủ ứng dụng. Kỹ thuật này cũng đơn giản để thực hiện trong mạng truyền thông di động 5G, trong chừng mực đủ để tích hợp dịch vụ mới vào trong máy chủ xác thực. Máy chủ xác thực sẽ hiển thị dịch vụ mới này và có thể được tiếp xúc bởi máy chủ ứng dụng để xác định khoá được nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn.

Theo một phương án cụ thể về phương pháp xác định, thiết bị người dùng gửi, đến máy chủ ứng dụng, yêu cầu truy cập và tiếp nhận, từ máy chủ ứng dụng, bằng chứng được chuẩn bị bởi máy chủ xác thực và nhằm cho thiết bị người dùng, việc yêu cầu khoá có được gửi hay không phụ thuộc vào việc xác minh bằng chứng này bởi thiết bị người dùng.

Tương ứng là, máy chủ xác thực chuyển đến máy chủ ứng dụng bằng chứng đã chuẩn bị nhằm cho thiết bị người dùng, bằng chứng này được dành để gửi, bởi máy chủ ứng dụng, đến thiết bị người dùng đáp lại yêu cầu truy cập được gửi bởi thiết bị người dùng, việc yêu

cầu khoá có được gửi bởi máy chủ xác thực hay không phụ thuộc vào việc xác minh bằng chứng đã nêu bởi thiết bị người dùng.

Bằng chứng này ví dụ được chứa trong dấu hiệu xác thực. Bằng chứng này, mà được chuẩn bị bởi máy chủ xác thực và được phân phối bởi máy chủ ứng dụng đến thiết bị người dùng, cho phép thiết bị người dùng xác minh rằng máy chủ ứng dụng quả thực được cấp quyền và thực hiện trước khi thực hiện bất kỳ sự phát sinh khoá nào trong thiết bị người dùng. Trong thủ tục GBA hiện tại, thiết bị người dùng lấy khoá thậm chí trước khi chắc chắn rằng máy chủ ứng dụng được cấp quyền. Máy chủ ứng dụng này có thể không được cấp quyền bởi máy chủ BSF và do đó không có sẵn khoá thu được cho nó.

Tương ứng là, sau khi tiếp nhận yêu cầu truy cập từ thiết bị người dùng, máy chủ ứng dụng tiếp nhận bằng chứng đã chuẩn bị nhằm cho thiết bị người dùng và gửi bằng chứng này đến thiết bị người dùng, việc yêu cầu khoá có được gửi đến máy chủ xác thực hay không phụ thuộc vào việc xác minh bằng chứng đã nêu bởi thiết bị người dùng.

Theo một phương án cụ thể, máy chủ xác thực xác minh rằng đã tính toán khoá nhằm tạo ra truyền thông giữa thiết bị người dùng đã nêu và máy chủ ứng dụng đã nêu một cách an toàn, việc biến ngẫu nhiên có được gửi đến thiết bị người dùng hay không phụ thuộc vào sự xác minh này.

Do đó, thiết bị người dùng này không lấy khoá khi máy chủ ứng dụng không được mời trước máy chủ xác thực cho thiết bị người dùng này.

Theo khía cạnh thứ hai, sáng chế đề cập đến thiết bị người dùng, được bố trí để truyền thông với máy chủ ứng dụng qua mạng truyền thông di động, thiết bị này bao gồm:

- môđun xác thực cho phép máy chủ xác thực của mạng truyền thông di động thực hiện xác thực thiết bị người dùng, khoá chính bí mật được tạo ra, trong quá trình xác thực này, bởi thiết bị người dùng và máy chủ xác thực;

- môđun gửi cho phép thiết bị người dùng gửi, đến máy chủ xác thực, yêu cầu khoá với mục đích truyền thông với máy chủ ứng dụng;

- môđun tính toán cho phép khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn được tính toán bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ

ứng dụng và sử dụng khoá chính, biến ngẫu nhiên này đã được tiếp nhận bởi thiết bị người dùng từ máy chủ xác thực.

Các ưu điểm được đề cập đối với phương pháp xác định khoá theo khía cạnh thứ nhất có thể chuyển vị trực tiếp đến thiết bị người dùng.

Thiết bị người dùng này dĩ nhiên có thể bao gồm, về mặt cấu trúc, các dấu hiệu khác nhau của phương pháp như được mô tả trên đây để xác định khoá, mà các dấu hiệu có thể được kết hợp hoặc được thực hiện riêng rẽ.

Theo khía cạnh thứ ba, sáng chế đề cập đến máy chủ xác thực của mạng truyền thông di động, máy chủ xác thực này bao gồm:

- môđun xác thực, được bố trí để thực hiện sự xác thực thiết bị người dùng, khoá chính bí mật được tạo ra, trong quá trình xác thực này, bởi thiết bị người dùng và máy chủ xác thực;

- môđun tiếp nhận để tiếp nhận yêu cầu khoá mà được gửi bởi thiết bị người dùng với mục đích truyền thông với máy chủ ứng dụng;

- môđun gửi cho phép máy chủ xác thực gửi biến ngẫu nhiên đến thiết bị người dùng;

- môđun tính toán để tính toán khoá nhằm tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, khoá này được tính bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính.

Các ưu điểm được đề cập đối với phương pháp xác định khoá theo khía cạnh thứ nhất có thể chuyển vị trực tiếp đến máy chủ xác thực.

Máy chủ xác thực này dĩ nhiên có thể bao gồm, về mặt cấu trúc, các dấu hiệu khác nhau của phương pháp như được mô tả trên đây để xác định khoá, mà các dấu hiệu có thể được kết hợp hoặc được thực hiện riêng rẽ.

Theo khía cạnh thứ tư, sáng chế đề cập đến hệ thống xác định khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, hệ thống này bao gồm ít nhất thiết bị người dùng theo khía cạnh thứ hai và máy chủ xác thực theo khía cạnh thứ ba.

Các ưu điểm được đề cập đối với phương pháp xác định khoá theo khía cạnh thứ nhất có thể chuyển vị trực tiếp đến hệ thống xác định khoá.

Theo một phương án cụ thể, hệ thống này còn bao gồm máy chủ ứng dụng, máy chủ ứng dụng này bao gồm môđun truyền thông, được bố trí để tiếp nhận khoá đã nêu từ máy chủ xác thực.

Theo khía cạnh thứ năm, sáng chế đề cập đến chương trình cho thiết bị người dùng, chứa các câu lệnh mã hoá chương trình nhằm để ra lệnh thực thi các câu lệnh của các bước của phương pháp xác định khoá được mô tả trên đây mà được thực hiện bởi thiết bị người dùng khi chương trình này được thực thi bởi thiết bị này và vật ghi mà đọc được bởi thiết bị người dùng, trên đó lưu trữ chương trình cho thiết bị người dùng.

Các ưu điểm được đề cập đối với phương pháp xác định khoá theo khía cạnh thứ nhất có thể chuyển vị trực tiếp đến chương trình cho thiết bị người dùng và đến vật ghi.

Theo khía cạnh thứ sáu, sáng chế đề cập đến chương trình cho máy chủ xác thực, chứa các câu lệnh mã hoá chương trình nhằm để ra lệnh thực thi các câu lệnh của các bước của phương pháp xác định khoá được mô tả trên đây mà được thực hiện bởi máy chủ xác thực khi chương trình này được thực thi bởi máy chủ này và vật ghi mà đọc được bởi máy chủ, trên đó lưu trữ chương trình cho máy chủ.

Các ưu điểm được đề cập đối với phương pháp xác định khoá theo khía cạnh thứ nhất có thể chuyển vị trực tiếp đến chương trình cho máy chủ xác thực và đến vật ghi.

Mô tả vắn tắt các hình vẽ kèm theo

Kỹ thuật để xác định khoá nhằm tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn sẽ được hiểu rõ hơn bằng phần mô tả các phương án cụ thể sau đây, mà được đưa ra với sự tham chiếu đến các hình vẽ kèm theo, trong đó:

- Hình 1 thể hiện mạng truyền thông di động trong đó phương pháp xác định khoá theo một phương án cụ thể được thực hiện;
- Hình 2 minh hoạ các bước của phương pháp xác định khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn theo một phương án cụ thể;
- Hình 3 thể hiện thiết bị người dùng theo một phương án cụ thể;

- Hình 4 thể hiện máy chủ xác thực theo một phương án cụ thể;
- Hình 5 thể hiện máy chủ ứng dụng theo một phương án cụ thể.

Mô tả chi tiết các phương án thực hiện sáng chế

Hình 1 thể hiện mạng truyền thông di động trong đó phương pháp xác định khoá theo một phương án cụ thể được thực hiện.

Hình 1 thể hiện kiến trúc của hệ thống thế hệ thứ năm (5G) trong mạng truyền thông di động trong quy trình được chuẩn hoá, trong trường hợp trong đó thiết bị người dùng ở trong mạng danh nghĩa của nó. Tương ứng với Hình 4.2.3-1 của tài liệu kỹ thuật 3GPP TS 23.501 V2.0.1 (2017-12), với tiêu đề "System Architecture for the 5G System; Stage 2 (Phát hành lần thứ 15)". Kiến trúc hệ thống 5G này bao gồm nhiều chức năng mạng, mà được mô tả chi tiết hơn về mặt chức năng trong phần 6 của tài liệu kỹ thuật TS 23.501 này. Các lược ngữ khác nhau của các chức năng mạng này được đưa ra trong phần phụ lục. Chỉ các chức năng mạng mà đóng góp vào việc thực hiện phương pháp xác định khoá K_{AF} nhằm để tạo ra truyền thông giữa thiết bị người dùng UE và máy chủ ứng dụng AF (AF viết tắt cho hàm ứng dụng) một cách an toàn được mô tả chi tiết dưới đây.

Do đó, với sự tham chiếu đến Hình 1, sự truyền thông an toàn phải được thiết lập giữa thiết bị người dùng 10 và máy chủ ứng dụng 40 để thực hiện ứng dụng.

Thiết bị người dùng UE (còn được gọi là thiết bị đầu cuối) được bố trí để truy cập vào mạng truyền thông di động (được thể hiện trên Hình 1). Trong kiến trúc thông thường của thiết bị người dùng như vậy, môi trường thực thi bao gồm hệ thống hàm thích hợp để thực thi các ứng dụng của người dùng, môi trường thực thi chịu trách nhiệm đối với các truyền thông mạng và được gọi là "dải tần cơ sở" và bộ phận an toàn, là luôn được phân biệt ở giữa. Bộ phận an toàn này là thẻ mạch tích hợp phổ dụng (universal integrated circuit card - UICC) hay thẻ mạch tích hợp phổ dụng được nhúng (embedded universal integrated circuit card - eUICC). Ví dụ về môđun an toàn là môđun nhận dạng thuê bao phổ dụng (universal subscriber identity module - USIM) được cài vào trong thiết bị người dùng và được sử dụng cho điện thoại di động. Bộ phận an toàn được bố trí để lưu trữ và xử lý dữ liệu nhạy, ví dụ ứng dụng cho phép truy cập vào mạng và các dữ liệu xác thực liên kết (các thông tin đã được nói đến) như các thuật toán mật mã và các khoá. Dữ liệu này được nhằm để sử dụng bởi giao thức xác thực cho mạng trong quá trình truy cập vào mạng. Không có giới hạn được đặt cho thiết bị

người dùng loại này và theo phương án làm ví dụ khác, bộ phận an toàn của thiết bị người dùng là vùng phần mềm an toàn được bố trí để xử lý dữ liệu truy cập mạng nhạy cảm. Thiết bị người dùng là thiết bị di động, ví dụ thiết bị đầu cuối thông minh như điện thoại thông minh, máy tính bảng, v.v.. Người dùng thiết bị người dùng đã đưa ra với nhà khai thác sự thuê bao cho phép anh ta truy cập vào mạng di động của nhà khai thác. Cuối cùng, thiết bị người dùng 10 bao gồm dữ liệu an toàn mà tạo ra hồ sơ truy cập mạng. Hồ sơ truy cập mạng bao gồm bộ dữ liệu mà cho phép mạng này được truy cập theo cách an toàn. Chính xác hơn là, hồ sơ truy cập này bao gồm ít nhất một mã nhận diện của thiết bị người dùng 10, mã nhận diện của mạng mà anh ta có thể truy cập vào bằng thuê bao của anh ta, và dữ liệu nhằm để sử dụng trong giai đoạn xác thực đối với mạng, như xác thực khoá, thường được ký hiệu là K.

Thiết bị người dùng 10 truy cập vào các thực thể mạng qua mạng truy cập được ký hiệu là (R)AN trên Hình 1. Mạng truy cập này bao gồm các trạm cơ sở, mà được bố trí để quản lý sự phát và tiếp nhận sóng vô tuyến với thiết bị người dùng 10.

Kiến trúc hệ thống 5G này được dựa trên máy chủ. Chính xác hơn là các bộ phận kiến trúc được xác định dưới dạng chức năng mạng mà tạo ra các dịch vụ của chúng qua các giao diện để phát triển cơ sở hạ tầng thông thường cho các chức năng mạng khác mà được cấp quyền để sử dụng chúng. Hàm lưu trữ mạng (network repository function - NRF) cho phép mỗi chức năng mạng khám phá các dịch vụ được cung cấp bởi các chức năng mạng khác. Hơn nữa, hàm hiển thị mạng (network exposure function - NEF) tiếp nhận thông tin từ các chức năng mạng khác phụ thuộc vào khả năng được hiển thị nhờ đó. NEF lưu trữ thông tin được tiếp nhận trong bộ nhớ dưới dạng dữ liệu được tạo cấu trúc bằng giao diện được chuẩn hoá với sự lưu trữ dữ liệu thống nhất (unified data repository - UDR).

Mạng truyền thông di động cụ thể bao gồm máy chủ quản lý dữ liệu thống nhất (unified-data-management - UDM), ký hiệu là 30. Máy chủ quản lý 30 này cụ thể thực hiện các chức năng sau đây:

- tạo ra dữ liệu xác thực và tán thành khoá 3GPP (AKA);

- lưu trong bộ nhớ và quản lý mã nhận diện cố định sự thuê bao (subscription permanent identifier - SUPI) đối với mỗi thuê bao của hệ thống 5G;

- cấp phép truy cập phụ thuộc vào dữ liệu thuê bao;

- quản lý đăng ký chức năng mạng để liên kết thiết bị người dùng;

- quản lý thuê bao.

Mạng truyền thông di động cũng bao gồm máy chủ xác thực AUSF (đối với hàm máy chủ xác thực), ký hiệu là 20, và thích hợp để xác thực các thiết bị người dùng.

Thông thường, và đối với mục đích truy cập mạng, môđun an toàn của thiết bị người dùng 10 đã lưu trữ trong bộ nhớ khoá xác thực, thường được ký hiệu là K, mà được chia sẻ với máy chủ quản lý dữ liệu thống nhất 30. Khoá xác thực K được nhằm để sử dụng cho việc tạo dữ liệu xác thực và thu được các khoá như khoá K_{AUSF}, K_{SEAF}, K_{AMF} và các khoá để tạo mật mã truyền tín hiệu, dữ liệu trong mặt phẳng người dùng, kiểm soát các tài nguyên sóng vô tuyến và các khoá được gọi là khoá trung gian. Thứ bậc của các khoá này ví dụ được thể hiện trong Hình 6.2.1-1 của tài liệu kỹ thuật 3GPP TS 33.501 V0.6.0 (2017-12) "Security Architecture and Procedures for 5G System (Phát hành lần thứ 15)". Trong thủ tục xác thực này, biến ngẫu nhiên RAND được sử dụng.

Khoá chính K_{AUSF} là khoá bí mật được chia sẻ giữa máy chủ xác thực 20 và thiết bị người dùng 10. Theo phương án được mô tả, hai thiết bị này lưu khoá chính K_{AUSF} này trong bộ nhớ tại thời điểm cuối của thủ tục xác thực.

Đối với quá trình xác thực EAP-AKA', khoá chính K_{AUSF} được xác định từ khoá phiên chính mở rộng (EMSK) bởi thiết bị người dùng 10 và máy chủ xác thực 20. Chi tiết hơn xem, đoạn 6.1.3.1 của tài liệu TS 33.501 mô tả chi tiết hơn thủ tục xác thực EAP-AKA' này. Đối với quá trình xác thực 5G AKA, khoá chính K_{AUSF} được xác định từ các khoá CK/IK (CK viết tắt của khoá số không và IK viết tắt của khoá toàn vẹn) bởi thiết bị người dùng 10 và máy chủ xác thực 20. Khoá chính K_{AUSF} thu được từ các khoá CK/IK, như được chỉ rõ trong đoạn A.2, phụ lục A của tài liệu TS 33.501, bằng cách sử dụng hàm phát sinh khoá (KDF) để nhập các tham số. Chi tiết hơn, xem đoạn 6.1.3.2 của tài liệu TS 33.501 mô tả chi tiết hơn thủ tục xác thực 5G AKA này.

Dưới đây, KDF tương ứng với hàm được chỉ rõ trong tài liệu kỹ thuật 3GPP TS 33.220 V15.1.0 (2018-01) "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Phát hành lần thứ 15)". Tài liệu này chỉ ra cụ thể cách để xây dựng, đối với KDF, chuỗi đầu vào S, mà, với khoá cần biết, tạo thành bộ phận của các tham số đầu vào.

Để thực hiện phương pháp được đề xuất, dịch vụ UE_AF_comm được hiển thị bởi máy chủ xác thực 20, mà ví dụ được ký hiệu là Nausf_UE_AF_comm (yêu cầu), ngoài Nausf_UEAuthentication dịch vụ. Nausf tương ứng với tên được đưa ra cho giao diện giữa máy chủ xác thực AUSF và các hàm khác của mạng. Cũng vậy, tUE_AF_comm dịch vụ được hiển thị bởi máy chủ ứng dụng 40, mà ví dụ được ký hiệu là Naf_UE_AF_comm (UE_ausf_notify). Naf tương ứng với tên được đưa ra cho giao diện giữa máy chủ ứng dụng AF và các hàm khác của mạng. Các dịch vụ được hiển thị bởi các chức năng mạng khác nhau được mô tả chi tiết trong tài liệu kỹ thuật 3GPP TS 23.502 V2.0.0 (2017-12) "Procedures for the 5G System; Stage 2 (Phát hành lần thứ 15)".

Máy chủ ứng dụng 40 có thể được quản lý bởi nhà khai thác mạng truyền thông di động hoặc bởi bên thứ ba.

Hệ thống 1 để xác định khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn bao gồm ít nhất thiết bị người dùng 10 và máy chủ xác thực 20.

Theo một phương án cụ thể, hệ thống 1 còn bao gồm máy chủ ứng dụng 40.

Phương pháp xác định khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, trong đó phương pháp này được thực hiện bởi thiết bị người dùng 10, máy chủ ứng dụng 40 và máy chủ xác thực 20, bây giờ sẽ được mô tả với sự tham chiếu đến **Hình 2**.

Dưới đây, nội dung là nội dung về mạng truyền thông di động 5G như được mô tả trên đây.

Thủ tục xác thực được thực hiện bởi thiết bị người dùng 10 ở bước E1 và bởi máy chủ xác thực 20 ở bước G1 trong quá trình đăng ký của thiết bị người dùng với mạng truyền thông di động. Trong thủ tục xác thực này, khoá chính bí mật K_{AUSF} được tạo ra bởi thiết bị người dùng 10 và máy chủ xác thực 20 từ biến ngẫu nhiên RAND1. Cuối bước E1, thiết bị người dùng 10 lưu trữ trong bộ nhớ lưu trữ 105 khoá chính K_{AUSF} được tạo ra. Tương ứng là, cuối bước G1, máy chủ xác thực 20 lưu trữ trong bộ nhớ lưu trữ 205 khoá chính K_{AUSF} được sinh ra.

Thiết bị người dùng 10 gửi, ở bước E2, đến máy chủ ứng dụng 40, yêu cầu truy cập M1. Yêu cầu truy cập M1 này cụ thể bao gồm:

- thông tin cho phép mạng truyền thông được xác định (ví dụ mã quốc gia di động (MCC) và mã mạng di động (MNC)),

- mã nhận diện thiết bị người dùng 10 UE_{ID}, mà sẽ được cung cấp trước bởi nhà khai thác mạng truyền thông.

Mã nhận diện UE_{ID} này là khác với mã nhận diện thuê bao SUPI nhưng nhà khai thác mạng được bố trí để liên kết mã nhận diện người dùng UE_{ID} này với mã nhận diện thuê bao SUPI đối với kết nối đã cho. Mã nhận diện người dùng UE_{ID} này theo một phương án cụ thể được phân bổ bởi nhà khai thác mạng.

Theo một phương án cụ thể, mã nhận diện người dùng UE_{ID} bao gồm thông tin cho phép mạng truyền thông được nhận diện.

Bằng cách minh hoạ, mã nhận diện UE_{ID} lấy từ dạng surname.forename@orange.fr. Mã nhận diện này cho phép thiết bị người dùng được nhận diện và nhà khai thác Orange được nhận diện. Sau đó có thể suy ra từ đó mã nhận diện mạng MCC 208 và MNC 01.

Thông điệp M1 này được tiếp nhận bởi máy chủ ứng dụng 40 ở bước F1. Vẫn trong bước F1 này, máy chủ ứng dụng 40 xác định mã nhận diện mạng và gửi yêu cầu M2 đến máy chủ xác thực 20 của mạng truyền thông của nhà khai thác đã xác định, qua máy chủ chịu trách nhiệm cho NEF khi thích hợp. Yêu cầu M2 này cụ thể bao gồm mã nhận diện máy chủ ứng dụng AF_{ID} và tuỳ ý thời gian hiệu lực $ExpireTime_{AF}$ được yêu cầu. Mã nhận diện máy chủ ứng dụng AF_{ID} ví dụ tương ứng với “service.fr”.

Yêu cầu M2 được tiếp nhận bởi máy chủ xác thực 20 ở bước G2. Vẫn trong bước G2, máy chủ xác thực 20 tính toán khoá K_{AF} được nhằm để tạo ra truyền thông giữa thiết bị người dùng 10 và máy chủ ứng dụng 40 một cách an toàn bằng KDF được áp dụng trên cơ sở khoá chính K_{AUSF}. Chuỗi đầu vào S cụ thể bao gồm mã nhận diện người dùng UE_{ID}, khoảng thời gian hiệu lực $ExpireTime_{AUSF}$, mã nhận diện AF_{ID} của máy chủ ứng dụng và biến ngẫu nhiên RAND2. Biến ngẫu nhiên này được chọn bởi máy chủ xác thực 20 và không có liên quan đến biến ngẫu nhiên RAND1 được sử dụng trong thủ tục xác thực. Thời gian hiệu lực $ExpireTime_{AUSF}$ được xác định bởi máy chủ xác thực 20.

Vẫn trong bước G2 này, máy chủ xác thực 20 chuẩn bị dấu hiệu xác thực AF_{AUTN}, bao gồm mã nhận diện máy chủ ứng dụng AF_{ID} và bằng chứng P để cho thiết bị người dùng. Bằng chứng P này tương ứng với kết quả của hàm f sử dụng như đầu vào khoá chính K_{AUSF}, mã nhận diện máy chủ ứng dụng AF_{ID} và thời gian hiệu lực $ExpireTime_{AUSF}$:

$P = f(K_{AUSF}, AF_{ID}, ExpireTime_{AUSF})$.

Hàm f này được chọn để bảo vệ chống lại việc phát lại.

Do đó, dấu hiệu xác thực AF_{AUTN} tương ứng với AF_{ID} || $f(K_{AUSF}, AF_{ID}, ExpireTime_{AUSF})$, trong đó || tương ứng với toán tử ghép nối. Trong dấu hiệu dấu hiệu xác thực, mã nhận diện máy chủ ứng dụng AF_{ID} là văn bản thuần tuý.

Sau đó máy chủ xác thực 20 lưu trong bộ nhớ, trong sự liên kết với khoá chính K_{AUSF} và thuê bao mã nhận diện SUPI, cụ thể là mã nhận diện người dùng UE_{ID} và mã nhận diện máy chủ ứng dụng AF_{ID}.

Tiếp theo, máy chủ xác thực 20 thông báo cho máy chủ ứng dụng 40, qua thông điệp M3 chứa khoá K_{AF} và dấu hiệu xác thực AF_{AUTN}. Do đó, máy chủ xác thực 20 phân phối tới máy chủ ứng dụng 40, khoá K_{AF} đã được tính và bằng chứng được chuẩn bị cho thiết bị người dùng 10, bằng chứng này được nhằm để được gửi, bởi máy chủ ứng dụng 40, đến thiết bị người dùng 10 để đáp lại yêu cầu truy cập M1 được gửi bởi thiết bị người dùng. Theo một phương án cụ thể, thông điệp M3 bao gồm thời gian hiệu lực $ExpireTime_{AUSF}$.

Thông điệp M3 này được tiếp nhận bởi máy chủ ứng dụng 40 ở bước F2. Theo một phương án cụ thể, máy chủ ứng dụng 40 lấy hai khoá, K_{AFenc} để tạo mật mã và K_{AFint} để bảo vệ toàn vẹn, từ K_{AF}.

Trong bước F2 này, máy chủ ứng dụng 40 gửi thông điệp M4 đến thiết bị người dùng 10 để đáp lại yêu cầu truy cập M1 nhận được trong bước F1. Thông điệp M4 này cụ thể bao gồm dấu hiệu xác thực AF_{AUTN} và, khi thích hợp, thời gian hiệu lực $ExpireTime_{AUSF}$. Lưu ý ở đây rằng sự trao đổi giữa thiết bị người dùng 10 và máy chủ ứng dụng 40 được bảo vệ bởi các khoá mạng, vì thiết bị người dùng 10 được xác thực cho mạng.

Ở bước E3, thiết bị người dùng 10 tiếp nhận thông điệp M4 và xác minh bằng chứng của dấu hiệu xác thực AF_{AUTN}. Bằng chứng này cho phép thiết bị người dùng 10 xác minh rằng máy chủ ứng dụng 40 đã được xác định đã được truyền thông thực sự với máy chủ xác

thực 20 và nó thực sự có khoá K_{AF} sẵn có cho nó. Điều này làm cho nó khả thi để xác minh rằng máy chủ ứng dụng 40 thực sự được cấp quyền và thực hiện trước khi phát sinh khoá bất kỳ được diễn ra trong thiết bị người dùng 10. Yêu cầu đối với khoá K_{AF} có được gửi hay không đến máy chủ xác thực 20 tuỳ thuộc vào sự xác minh bằng chứng bởi thiết bị người dùng 10.

Khi bằng chứng là không được xác minh phù hợp, thiết bị người dùng 10 dừng phương pháp xác định khoá K_{AF}.

Khi bằng chứng được xác minh phù hợp, ở bước E4, thiết bị người dùng 10 gửi, đến máy chủ xác thực 20, thông điệp M5 yêu cầu khoá với mục đích truyền thông với máy chủ ứng dụng 40. Thông điệp M5 này cụ thể bao gồm mã nhận diện người dùng UE_{ID} của nó và mã nhận diện máy chủ ứng dụng AF_{ID}. Lưu ý ở đây rằng sự trao đổi giữa thiết bị người dùng 10 và máy chủ xác thực 20 được bảo vệ bởi các khoá mạng, vì thiết bị người dùng 10 được xác thực cho mạng.

Thông điệp yêu cầu khoá M5 này được tiếp nhận bởi máy chủ xác thực 20 ở bước G3. Sau đó máy chủ xác thực xác minh xem việc nó đã tính toán hay chưa khoá K_{AF} được nhằm để tạo ra truyền thông giữa thiết bị người dùng 10 và máy chủ ứng dụng 40 một cách an toàn bởi thông tin được lưu trong bộ nhớ ở bước G2. Biến ngẫu nhiên RAND2 có được gửi hay không đến thiết bị người dùng 10 tuỳ thuộc vào sự xác minh này. Khi sự xác minh là âm, máy chủ xác thực 20 kết thúc phương pháp xác định khoá. Khi sự xác minh là dương, máy chủ xác thực 20 gửi thông điệp đáp lại M6 đến thiết bị người dùng 10. Thông điệp M6 này cụ thể bao gồm mã nhận diện người dùng UE_{ID}, khoảng thời gian hiệu lực $ExpireTime_{AUSF}$, mã nhận diện máy chủ ứng dụng AF_{ID} và biến ngẫu nhiên RAND2 mà được sử dụng bởi máy chủ xác thực 20 để tính toán khoá K_{AF}.

Ở bước E5, thiết bị người dùng 10 tiếp nhận thông điệp M6 và lấy khoá K_{AF} từ khoá chính K_{AUSF} theo cách được mô tả ở bước G2 đối với máy chủ xác thực 20. Theo một phương án cụ thể, thiết bị người dùng 10 lấy hai khoá, K_{AFenc} để tạo mật mã và K_{AFint} để bảo vệ toàn vẹn, từ khoá K_{AF}.

Do đó, cuối bước E5, thiết bị người dùng 10 đã tính toán khoá K_{AF} nhằm để tạo ra truyền thông với máy chủ ứng dụng 40 một cách an toàn. Máy chủ ứng dụng này cũng có khoá K_{AF} này, mà thu được từ máy chủ xác thực, sẵn có cho nó. Khoá này được xác định mà

không cần yêu cầu sự xác thực mới, và do đó không cần yêu cầu lại bộ phận an toàn của thiết bị người dùng.

Sự truyền thông sau đó được thiết lập giữa thiết bị người dùng 10 và máy chủ ứng dụng 40, mà sự truyền thông được tạo ra một cách an toàn bởi khoá K_{AF}, được giới hạn khi thích hợp bởi thời gian hiệu lực $ExpireTime_{AUSF}$. Do đó, phương pháp xác định này có thể được tích hợp vào trong phương pháp thiết lập sự truyền thông an toàn giữa thiết bị người dùng và máy chủ ứng dụng.

Nếu khoá chính K_{AUSF} được thay đổi theo sự xác thực mới, điều này không ảnh hưởng đến sự truyền thông an toàn vì khoá K_{AF} được tách riêng ra khỏi khoá chính K_{AUSF}.

Khoá K_{AF} do đó có thể được xác định cho mỗi truyền thông với máy chủ ứng dụng.

Dịch vụ này dễ dàng được tích hợp vào máy chủ xác thực và máy chủ ứng dụng vì kiến trúc 5G mới, mà được dựa trên dịch vụ. Dịch vụ mới Nausf_UE_AF_comm(yêu cầu) được tạo ra trong máy chủ xác thực. Do đó phương pháp này dựa trên máy chủ xác thực hiện có mà do đó đã được tích hợp sẵn vào trong mạng của nhà khai thác. Do đó phương pháp này có thể được thực hiện dễ dàng hơn kỹ thuật GBA trước đó. Phương pháp này cũng dễ dàng được thực hiện trong thiết bị người dùng. Naf_UE_AF_comm(UE_ausf_notitfy) dịch vụ được tạo ra trong máy chủ ứng dụng. Không có sự trao đổi nào giữa máy chủ xác thực và máy chủ UDM khi thực hiện phương pháp, máy chủ UDM được dựa trên sự xác thực mà đã được thực thi. Chi phí phát triển phương pháp này do đó là thấp.

Phương pháp được mô tả bao gồm máy chủ xác thực chuẩn bị bằng chứng để cho thiết bị người dùng. Bằng chứng này được phân phối bởi máy chủ ứng dụng đến thiết bị người dùng và được xác minh bởi thiết bị người dùng. Sự chuẩn bị bằng chứng này và quá trình xác minh nó không được thực hiện theo phương án cụ thể khác.

Phương án được mô tả này xác định các tham số đầu vào của hàm phát sinh khoá. Lưu ý rằng, theo các phương án nhất định, các tham số nhất định có thể vắng mặt hoặc thực vậy các tham số khác có thể được bổ sung.

Được hiểu rằng kỹ thuật này để xác định khoá cho phép thủ tục tạo truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn được đơn giản hoá. Khi, thiết bị người dùng đã được cấp quyền cho máy chủ xác thực của nhà khai thác mạng di động của nó,

dễ dàng xác định được khoá này đồng thời loại bỏ các hạn chế của kỹ thuật GBA trước đây. Sự tích hợp kỹ thuật này vào mạng truyền thông di động 5G cũng được thúc đẩy.

Không có giới hạn được đặt ra đối với các phương án khác nhau này và người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể xác định các phương án khác từ đó cho phép khoá này được xác định, phụ thuộc vào khoá chính được chia sẻ giữa máy chủ xác thực và thiết bị người dùng, bằng cách sử dụng biến ngẫu nhiên khác biệt với biến được sử dụng trong thủ tục xác thực.

Hình 3 minh hoạ theo sơ đồ thiết bị người dùng 10 theo một phương án cụ thể.

Thiết bị người dùng 10 cụ thể bao gồm:

- bộ xử lý 100 để thực thi các câu lệnh dạng mã môđun phần mềm;

- môđun truyền thông 101, tạo thành giao diện truyền thông với mạng truyền thông di động, được bố trí để truyền thông với các thiết bị của mạng truyền thông, ví dụ với máy chủ xác thực và máy chủ ứng dụng;

- vùng bộ nhớ 105, được bố trí để lưu trữ chương trình mà chứa các câu lệnh dạng mã để thực hiện các bước của phương pháp xác định này;

- bộ nhớ lưu trữ 106, được bố trí để lưu trữ dữ liệu được sử dụng trong quá trình thực hiện phương pháp xác định này;

- bộ phận an toàn (không được thể hiện trên Hình 3).

Thiết bị người dùng cũng bao gồm:

- môđun xác thực 102 cho phép thiết bị người dùng được cấp quyền bởi máy chủ xác thực 20 của mạng truyền thông di động, khoá chính bí mật được tạo ra trong quá trình xác thực này bởi thiết bị người dùng và máy chủ xác thực;

- môđun tính toán 103 cho phép khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn được tính toán bởi hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính, biến ngẫu nhiên đã nêu đã được tiếp nhận bởi thiết bị người dùng từ máy chủ xác thực;

- môđun kết nối 104, được bố trí để thiết lập sự truyền thông an toàn với máy chủ ứng dụng 40 bằng khoá K_{AF}.

Môđun truyền thông 101 cụ thể được bố trí để gửi, đến máy chủ xác thực, yêu cầu khoá với mục đích truyền thông với máy chủ ứng dụng.

Bộ nhớ lưu trữ 106 cụ thể được bố trí để lưu trữ khoá chính K_{AUSF} được xác định trong thủ tục xác thực. Theo một phương án cụ thể, thủ tục xác thực này được kích hoạt trong quá trình đăng ký của thiết bị người dùng với mạng truyền thông di động.

Theo một phương án cụ thể, môđun truyền thông 101 cụ thể được bố trí để gửi, đến máy chủ ứng dụng, yêu cầu truy cập và để tiếp nhận, từ máy chủ ứng dụng, bằng chứng được chuẩn bị bởi máy chủ xác thực và để cho thiết bị người dùng. Môđun tính toán 103 sau đó được bố trí để xác minh bằng chứng này, xem việc yêu cầu khoá có được gửi hay không tuỳ thuộc vào sự xác minh này.

Theo một phương án cụ thể, môđun tính toán 103 được bố trí để thu được hai khoá, K_{AFenc} để tạo mật mã và K_{AFint} để bảo vệ toàn vẹn, từ K_{AF}.

Lưu ý ở đây rằng thiết bị người dùng 10 cũng bao gồm các môđun xử lý khác (không được thể hiện trên Hình 3) được bố trí để tiến hành nhiều hàm khác nhau của thiết bị người dùng này.

Hình 4 minh hoạ theo sơ đồ máy chủ xác thực 20 theo một phương án cụ thể.

Máy chủ xác thực 20 của mạng truyền thông di động cụ thể bao gồm:

- bộ xử lý 200 để thực thi các câu lệnh dạng mã môđun phần mềm;

- môđun truyền thông 201, mà tạo thành giao diện truyền thông đối với mạng truyền thông di động, được bố trí để truyền thông với các thiết bị của mạng truyền thông, ví dụ với thiết bị người dùng và máy chủ ứng dụng;

- vùng bộ nhớ 204, được bố trí để lưu trữ trong bộ nhớ chương trình mà chứa các câu lệnh dạng mã để thực hiện các bước của phương pháp xác định này;

- bộ nhớ lưu trữ 205, được bố trí để lưu trữ dữ liệu được sử dụng trong quá trình thực hiện phương pháp xác định này.

Máy chủ xác thực 20 cũng bao gồm:

- môđun xác thực 202, được bố trí để tiến hành xác thực thiết bị người dùng, khoá chính bí mật được tạo ra trong quá trình xác thực này bởi thiết bị người dùng và máy chủ xác thực;

- môđun tính toán 203 để tính toán khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, khoá này được tính bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính.

Môđun truyền thông 201 cụ thể được bố trí để tiếp nhận yêu cầu khoá được gửi bởi thiết bị người dùng với mục đích truyền thông với máy chủ ứng dụng và với mục đích cho biến ngẫu nhiên được gửi đến thiết bị người dùng. Môđun truyền thông 201 cũng được bố trí để phân phối, đến máy chủ ứng dụng, khoá được tính.

Bộ nhớ lưu trữ 205 cụ thể được bố trí để lưu trữ khoá chính K_{AUSF} được xác định trong thủ tục xác thực. Theo một phương án cụ thể, thủ tục xác thực này được kích hoạt trong quá trình đăng ký của thiết bị người dùng với mạng truyền thông di động.

Theo một phương án cụ thể, môđun tính toán 203 cụ thể được bố trí để chuẩn bị bằng chứng để cho thiết bị người dùng. Môđun truyền thông 201 sau đó được bố trí để phân phối bằng chứng này đến máy chủ ứng dụng, sao cho máy chủ ứng dụng có thể gửi nó đến thiết bị người dùng để đáp lại yêu cầu truy cập được gửi bởi thiết bị người dùng, việc yêu cầu khoá này có được gửi đến máy chủ xác thực hay không phụ thuộc vào sự xác minh bằng chứng này như được tiến hành bởi thiết bị người dùng.

Theo một phương án cụ thể, bộ nhớ lưu trữ 205 được bố trí để lưu trữ, trong sự liên kết với khoá chính K_{AUSF} và mã nhận diện thuê bao SUPI, cụ thể là mã nhận diện người dùng UE_{ID} và mã nhận diện máy chủ ứng dụng AF_{ID}.

Theo một phương án cụ thể, môđun tính toán 203 cụ thể được bố trí để xác minh rằng đã tính khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, việc biến ngẫu nhiên này có được gửi đến thiết bị người dùng hay không phụ thuộc vào sự xác minh này. Sự xác minh này cụ thể bao gồm việc xây dựng bộ nhớ lưu trữ 205.

Theo một phương án cụ thể, máy chủ xác thực bao gồm môđun được bố trí để hiện thị UE_AF_Comm dịch vụ, như được mô tả trên đây.

Lưu ý ở đây rằng máy chủ xác thực 20 cũng bao gồm các môđun xử lý khác (không được thể hiện trên Hình 4) được bố trí để tiến hành các hàm khác nhau của máy chủ xác thực này.

Hình 5 minh hoạ theo sơ đồ máy chủ ứng dụng 40 theo một phương án cụ thể.

Máy chủ ứng dụng 40 cụ thể bao gồm:

- bộ xử lý 400 để thực thi các câu lệnh dạng mã môđun phần mềm;

- môđun truyền thông 401, tạo thành giao diện truyền thông với mạng truyền thông di động, được bố trí để truyền thông với các thiết bị của mạng truyền thông, ví dụ với thiết bị người dùng và máy chủ xác thực;

- vùng bộ nhớ 404, được bố trí để lưu trữ chương trình mà chứa các câu lệnh dạng mã để thực hiện các bước của phương pháp xác định này;

- bộ nhớ lưu trữ 405, được bố trí để lưu trữ dữ liệu được sử dụng trong quá trình thực hiện phương pháp xác định này.

Máy chủ ứng dụng 40 cũng bao gồm:

- môđun 402 để xác định mã nhận diện mạng, được bố trí để xác định, từ yêu cầu truy cập M1 được tiếp nhận từ thiết bị người dùng, mã nhận diện mạng;

- môđun kết nối 403, được bố trí để thiết lập truyền thông an toàn với thiết bị người dùng 10 bằng khoá K_{AF}.

Môđun truyền thông 40 cụ thể được bố trí để tiếp nhận yêu cầu truy cập M1được gửi bởi thiết bị người dùng và để gửi yêu cầu M2 đến máy chủ xác thực 20 của mạng truyền thông của nhà khai thác được nhận diện. Môđun truyền thông 401 cũng được bố trí để tiếp nhận khoá K_{AF} được nhằm để tạo ra sự truyền thông với thiết bị người dùng một cách an toàn.

Theo một phương án cụ thể, môđun truyền thông 401 được bố trí để tiếp nhận, từ máy chủ xác thực, bằng chứng được chuẩn bị để cho thiết bị người dùng 10 và để gửi bằng chứng này đến thiết bị người dùng 10 để đáp lại yêu cầu truy cập M1 được gửi bởi thiết bị người dùng.

Theo một phương án cụ thể, máy chủ ứng dụng 40 còn bao gồm môđun tính toán, được bố trí để thu được hai khoá, K_{AFenc} để tạo mật mã và K_{AFint} để bảo vệ toàn vẹn, từ K_{AF}.

Theo một phương án cụ thể, bộ nhớ lưu trữ 405 được bố trí để lưu trữ, trong sự liên kết với mã nhận diện người dùng UE_{ID}, khoá K_{AF}.

Theo một phương án cụ thể, máy chủ ứng dụng bao gồm môđun được bố trí để hiện thị UE_AF_Comm dịch vụ, như được mô tả trên đây.

Lưu ý ở đây rằng máy chủ ứng dụng 40 cũng bao gồm các môđun xử lý khác (không được thể hiện trên Hình 5) được bố trí để tiến hành các hàm khác nhau của máy chủ ứng dụng này.

Kháng thể để xác định khoá được thực hiện bằng các phần mềm và/hoặc phần cứng. Trong ngữ cảnh này, thuật ngữ "môđun" có thể tương ứng, trong tài liệu này, với phần mềm hoặc phần cứng hoặc tập hợp các phần cứng và/hoặc phần mềm, có khả năng tiến hành hàm hoặc tập hợp các hàm, theo phần mô tả được đưa ra trên đây đối với môđun được xem xét.

Phần mềm tương ứng với một hoặc nhiều chương trình máy tính, một hoặc nhiều chương trình con của chương trình máy tính, phổ biến hơn là với bộ phận bất kỳ của chương trình hoặc gói phần mềm. Phần mềm này được lưu trong bộ nhớ sau khi được nạp và được thực thi bởi bộ xử lý dữ liệu của thực thể vật lý và có khả năng truy cập vào tài nguyên phần cứng của thực thể vật lý (bộ nhớ, vật ghi, các buýt truyền thông, các bảng mạch vào/ra, các giao diện người dùng, v.v..).

Theo cùng cách, phần cứng tương ứng với bộ phận bất kỳ của kết cấu phần cứng. Nó có thể là câu hỏi về phần cứng lập trình được hoặc không lập trình được có hoặc không có bộ xử lý được tích hợp để thực thi phần mềm. Nó ví dụ là câu hỏi về mạch tích hợp, về thẻ chip, về bảng mạch để thực thi phần sụn, v.v..

Theo một phương án cụ thể, các môđun 101, 102, 103, 104 được bố trí để thực thi các bước của phương pháp xác định được mô tả trên đây mà được thực thi bởi thiết bị người dùng. Tốt hơn là nó là câu hỏi về các môđun phần mềm chứa các câu lệnh phần mềm để làm cho nó thực thi các lệnh của các bước (hoặc của các hoạt động) của phương pháp xác định được mô tả trên đây mà được thực hiện bởi thiết bị người dùng. Do đó, sáng chế cũng đề cập đến:

- chương trình cho thiết bị người dùng, chứa các câu lệnh mã chương trình nhằm để ra lệnh thực thi các lệnh của các bước (hoặc của các hoạt động) của phương pháp xác định như được mô tả trên đây, khi chương trình này được thực thi bởi thiết bị người dùng này;

- vật ghi mà đọc được bằng thiết bị người dùng mà trên đó chương trình cho thiết bị được lưu trữ.

Theo một phương án cụ thể, các môđun 201, 202, 203 được bố trí để thực hiện các bước của phương pháp xác định được mô tả trên đây mà được thực hiện bởi máy chủ xác thực. Tốt hơn là nó là câu hỏi về các môđun phần mềm chứa các câu lệnh phần mềm để làm cho nó thực thi các lệnh của các bước (hoặc của các hoạt động) của phương pháp xác định được mô tả trên đây mà được thực hiện bởi máy chủ xác thực. Do đó, sáng chế cũng đề cập đến:

- chương trình cho máy chủ xác thực, chứa các câu lệnh mã chương trình nhằm ra lệnh việc thực thi các câu lệnh của các bước (hoặc của các hoạt động) của phương pháp xác định được mô tả trên đây, khi chương trình này được thực thi bởi máy chủ xác thực này;

- vật ghi mà đọc được bằng máy chủ xác thực mà trên đó chương trình cho máy chủ được lưu trữ.

Theo một phương án cụ thể, các môđun 401, 402, 403 được bố trí để thực hiện các bước của phương pháp xác định được mô tả trên đây mà được thực hiện bởi máy chủ ứng dụng. Tốt hơn là nó là câu hỏi về các môđun phần mềm chứa các câu lệnh phần mềm để làm cho nó thực thi các lệnh của các bước (hoặc của các hoạt động) của phương pháp xác định được mô tả trên đây mà được thực hiện bởi máy chủ ứng dụng. Do đó, sáng chế cũng đề cập đến:

- chương trình cho máy chủ ứng dụng, chứa các câu lệnh mã chương trình nhằm ra lệnh việc thực thi các câu lệnh của các bước (hoặc của các hoạt động) của phương pháp xác định được mô tả trên đây, khi chương trình này được thực thi bởi máy chủ ứng dụng này;

- vật ghi mà đọc được bằng máy chủ ứng dụng mà trên đó chương trình cho máy chủ được lưu trữ.

Các môđun phần mềm có thể được lưu trữ trong hoặc được truyền qua vật ghi dữ liệu. Vật ghi dữ liệu này có thể vật ghi phần cứng, ví dụ CD-ROM, đĩa mềm hoặc ổ cứng, hoặc

thực sự là phương tiện truyền dẫn như tín hiệu điện, quang hoặc vô tuyến, hoặc mạng viễn thông.

Phụ lục

- Hàm máy chủ xác thực (AUSF)
- Hàm quản lý truy cập và di động (AMF)
- Mạng dữ liệu (DN), ví dụ các dịch vụ vận hành, truy cập mở rộng vào mạng truyền thông hoặc thực sự là các dịch vụ của bên thứ ba
- Hàm hiển thị mạng (NEF)
- Hàm lưu trữ NF (NRF)
- Hàm chọn lọc mạng mỏng (NSSF)
- Hàm kiểm soát chính sách (PCF)
- Hàm quản lý phiên (SMF)
- Quản lý dữ liệu thống nhất (UDM)
- Hàm mặt phẳng người dùng (UPF)
- Hàm ứng dụng (AF)
- Thiết bị người dùng (UE)
- Mạng truy cập (sóng vô tuyến) ((R)AN)

YÊU CẦU BẢO HỘ

1. Phương pháp xác định khoá nhằm tạo ra truyền thông giữa thiết bị người dùng (10) và máy chủ ứng dụng (40) một cách an toàn, phương pháp này bao gồm bước:

- xác thực (E1) thiết bị người dùng bằng máy chủ xác thực (20) của mạng truyền thông di động, khoá chính bí mật được tạo ra, trong suốt quá trình xác thực đã nêu, bởi thiết bị người dùng và máy chủ xác thực;

- gửi (E4) bởi thiết bị người dùng đến máy chủ xác thực, yêu cầu khoá với mục đích giao tiếp với máy chủ ứng dụng;

- tính toán (E5) khoá này bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính, biến ngẫu nhiên này đang được tiếp nhận bởi thiết bị người dùng từ máy chủ xác thực.

2. Phương pháp xác định theo điểm 1, trong đó sự xác thực đã nêu được kích hoạt trong quá trình đăng ký thiết bị người dùng với mạng truyền thông di động.

3. Phương pháp xác định theo điểm 1, trong đó thiết bị người dùng gửi (E2), đến máy chủ ứng dụng, yêu cầu truy cập và tiếp nhận, từ máy chủ ứng dụng, bằng chứng được chuẩn bị bởi máy chủ xác thực và nhằm cho thiết bị người dùng, việc yêu cầu khoá có được gửi hay không phụ thuộc vào sự xác minh (E3) bằng chứng đã nêu bởi thiết bị người dùng.

4. Phương pháp xác định khoá nhằm tạo ra truyền thông giữa thiết bị người dùng (10) và máy chủ ứng dụng (40) một cách an toàn, phương pháp này bao gồm bước:

- xác thực (G1) thiết bị người dùng bằng máy chủ xác thực (20) của mạng truyền thông di động, khoá chính bí mật được tạo ra, trong suốt quá trình xác thực đã nêu, bởi thiết bị người dùng và máy chủ xác thực;

- tiếp nhận (G3) bởi máy chủ xác thực yêu cầu khoá mà đã được gửi bởi thiết bị người dùng với mục đích truyền thông với máy chủ ứng dụng;

- gửi (G3) biến ngẫu nhiên bởi máy chủ xác thực đến thiết bị người dùng;

- tính toán (G2) khoá này bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính.

5. Phương pháp xác định theo điểm 4, trong đó máy chủ xác thực phân phối (G2) đến máy chủ ứng dụng bằng chứng đã chuẩn bị nhằm cho thiết bị người dùng, bằng chứng này được dành để gửi, bởi máy chủ ứng dụng, đến thiết bị người dùng đáp lại yêu cầu truy cập được gửi bởi thiết bị người dùng, việc yêu cầu khoá có được gửi bởi máy chủ xác thực hay không phụ thuộc vào việc xác minh bằng chứng đã nêu bởi thiết bị người dùng.

6. Phương pháp xác định theo điểm 4, trong đó máy chủ xác thực xác minh (G3) rằng đã tính toán khoá nhằm tạo ra truyền thông giữa thiết bị người dùng đã nêu và máy chủ ứng dụng đã nêu một cách an toàn, việc biến ngẫu nhiên có được gửi đến thiết bị người dùng hay không phụ thuộc vào sự xác minh này.

7. Thiết bị người dùng (10), được bố trí để truyền thông với máy chủ ứng dụng (40) qua mạng truyền thông di động, thiết bị này bao gồm:

- môđun xác thực (102) cho phép máy chủ xác thực (20) của mạng truyền thông di động thực hiện xác thực thiết bị người dùng, khoá chính bí mật được tạo ra, trong quá trình xác thực này, bởi thiết bị người dùng và máy chủ xác thực;

- môđun gửi (101) cho phép thiết bị người dùng gửi, đến máy chủ xác thực, yêu cầu khoá với mục đích truyền thông với máy chủ ứng dụng;

- môđun tính toán (103) cho phép khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn được tính toán bởi hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính, biến ngẫu nhiên đã nêu đã được tiếp nhận bởi thiết bị người dùng từ máy chủ xác thực.

8. Máy chủ xác thực (20) của mạng truyền thông di động, máy chủ xác thực này bao gồm:

- môđun xác thực (202), được bố trí để tiến hành xác thực thiết bị người dùng, khoá chính bí mật được tạo ra, trong quá trình xác thực này, bởi thiết bị người dùng và máy chủ xác thực;

- môđun tiếp nhận (201) để tiếp nhận yêu cầu khoá mà được gửi bởi thiết bị người dùng với mục đích truyền thông với máy chủ ứng dụng;

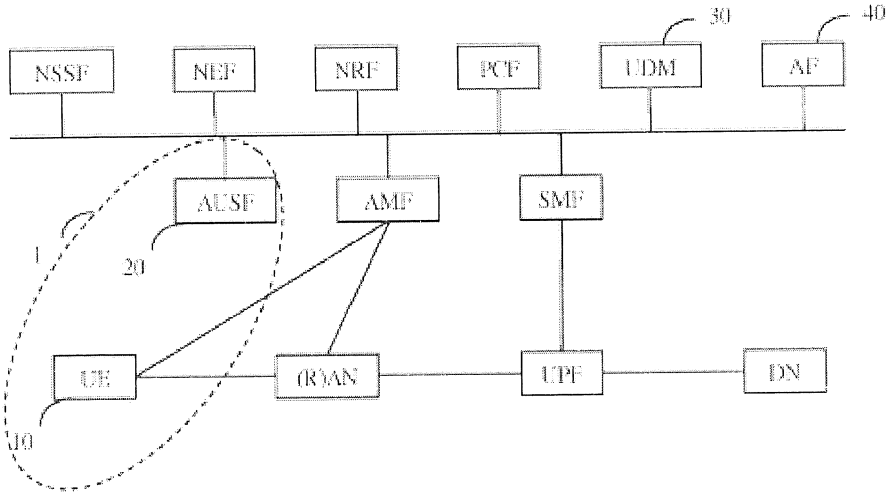
- môđun gửi (201) cho phép máy chủ xác thực gửi biến ngẫu nhiên đến thiết bị người dùng;

- môđun tính toán (203) để tính toán khoá nhằm tạo ra truyền thông giữa thiết bị người dùng và máy chủ ứng dụng một cách an toàn, khoá này được tính bằng hàm phát sinh khoá được áp dụng cho ít nhất biến ngẫu nhiên, mã nhận diện người dùng và mã nhận diện của máy chủ ứng dụng và sử dụng khoá chính.

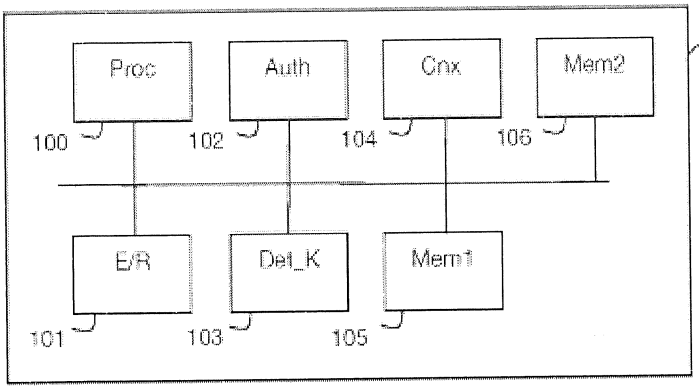
9. Hệ thống (1) để xác định khoá nhằm để tạo ra truyền thông giữa thiết bị người dùng (10) và máy chủ ứng dụng (40) một cách an toàn, hệ thống này bao gồm ít nhất thiết bị người dùng theo điểm 7 và máy chủ xác thực theo điểm 8.

10. Vật ghi đọc được bằng thiết bị người dùng, trên đó được lưu trữ chương trình đối với thiết bị người dùng, chứa các lệnh mã chương trình nhằm để ra lệnh việc thực thi các bước của phương pháp xác định theo điểm bất kỳ trong số các điểm từ 1 đến 3, các bước này được thực thi bởi thiết bị người dùng khi chương trình này được thực thi bởi thiết bị đã nêu.

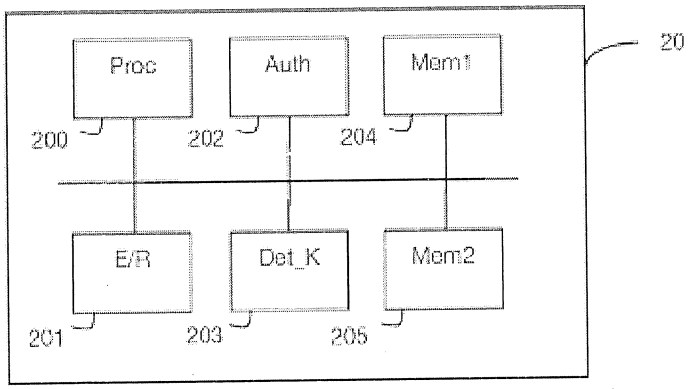
11. Vật ghi đọc được bằng máy chủ xác thực, trên đó được lưu trữ chương trình cho máy chủ xác thực, chứa các câu lệnh mã chương trình nhằm để ra lệnh việc thực thi các bước của phương pháp xác định theo điểm bất kỳ trong số các điểm từ 4 đến 6, các bước này được thực thi bằng máy chủ xác thực khi chương trình đã nêu được thực thi bởi máy chủ đã nêu.



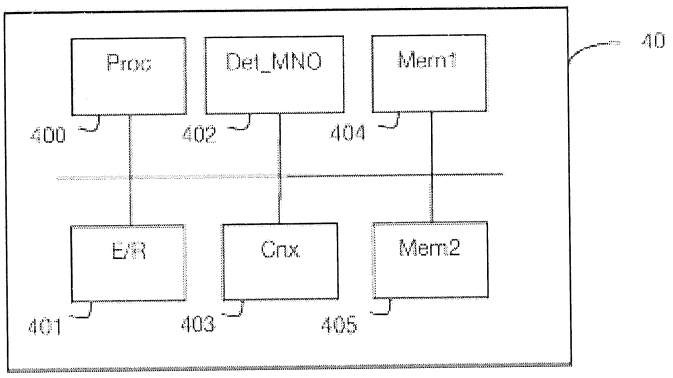
HÌNH 1



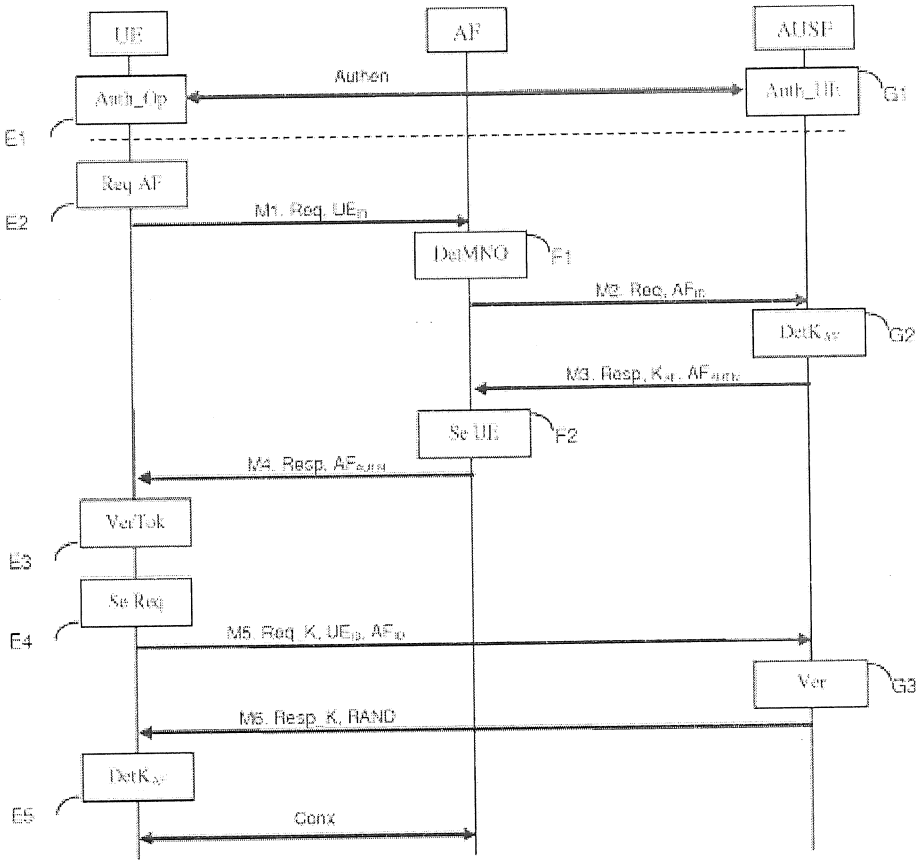
HÌNH 3



HÌNH 4


Proc
Det_MNO
Mem1
40
400
402
404
E/R
Cnx
Mem2
401
403
405

HÌNH 5


UE
AF
AUSP
Authen
Auth_Up
Auth_UE
G1
E1
Req AF
E2
M1. Req. UE
DetMNO
F1
M2. Req. AF
DetK
G2
M3. Resp. K
Se UE
F2
M4. Resp. AF
VerTok
E3
Se Req
E4
M5. Req. K, UE, AF
Ver
G3
M6. Resp. K, RAND
DetK
E5
Conx

HÌNH 2