(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) **1-0047797**

(51)[2019.01] **H04W 12/06**; H04L 9/32

(13) **B**

(21) 1-2020-01129
(22) 07/08/2018
(86) PCT/CN2018/099197 07/08/2018
(87) WO/2019/029531 14/02/2019
(30) 201710667037.3 07/08/2017 CN
(45) 25/06/2025 447
(43) 25/05/2020 386A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) LI, He (CN); CHEN, Jing (CN); LI, Huan (CN); WU, Yizhuang (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP, THIẾT BỊ VÀ HỆ THỐNG KÍCH HOẠT XÁC THỰC MẠNG, PHƯƠNG PHÁP KÍCH HOẠT VIỆC XÁC THỰC, THIẾT BỊ MẠNG THỨ NHẤT, THỰC THỂ CHỨC NĂNG BẢO MẬT THỨ NHẤT, THIẾT BỊ TRUYỀN THÔNG, VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BỞI MÁY TÍNH

(21) 1-2020-01129

(57) Sáng chế đề cập đến lĩnh vực về các công nghệ truyền thông, và bộc lộ phương pháp kích hoạt xác thực mạng, phương pháp kích hoạt việc xác thực, thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất, thiết bị đầu cuối, hệ thống truyền thông, và phương tiện lưu trữ đọc được bởi máy tính. Phương pháp bao gồm các bước: thu tin nhắn thứ nhất từ thiết bị đầu cuối, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng, thông tin nhận dạng thứ nhất là thông tin nhận dạng được mã hóa, và thông tin ký hiệu nhận dạng được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; và gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin ký hiệu nhận dạng. Sáng chế đề xuất giải pháp kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa.

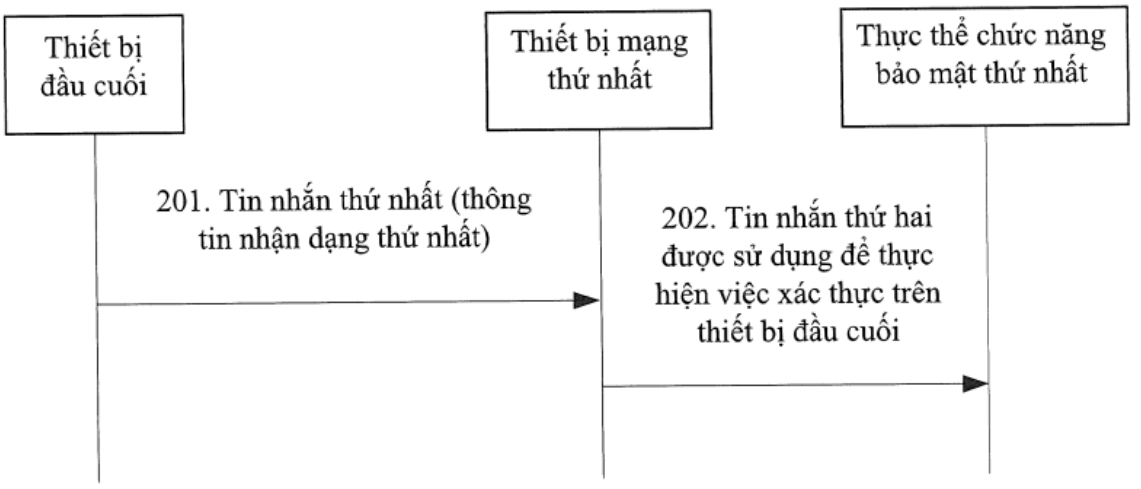

FIG. 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực về các công nghệ truyền thông, và cụ thể là, đến phương pháp kích hoạt xác thực mạng và thiết bị liên quan.

Tình trạng kỹ thuật của sáng chế

Hiện nay, thiết bị đầu cuối có thể truy cập mạng nhờ sử dụng công nghệ 3GPP hoặc nhờ sử dụng công nghệ không phải 3GPP. Khi thiết bị đầu cuối truy cập mạng 5G và được đăng ký lần thứ nhất, bất kể việc thiết bị đầu cuối truy cập mạng 5G nhờ sử dụng công nghệ 3GPP hoặc nhờ sử dụng công nghệ không phải 3GPP, thiết bị đầu cuối cần phải gửi, đến thiết bị trong mạng lõi, tin nhắn kèm theo mang thông tin nhận dạng lâu dài, sao cho thiết bị trong mạng lõi kích hoạt quy trình xác thực theo tin nhắn kèm theo, để thực hiện việc xác thực cho thiết bị đầu cuối.

Trong công nghệ liên quan, khi thiết bị đầu cuối truy cập mạng 5G và thực hiện việc đăng ký ban đầu, thiết bị đầu cuối có thể gửi thông tin nhận dạng lâu dài của thiết bị đầu cuối đến thực thể quản lý di động và truy cập (access and mobility management function, viết tắt là AMF) trong mạng lõi qua nút B thế hệ tiếp theo (next generation NodeB, viết tắt là gNB) hoặc thực thể chức năng liên kết mạng không phải 3GPP (non-3GPP interworking function, viết tắt là N3IWF). Khi thực thể AMF thu thông tin nhận dạng lâu dài của thiết bị đầu cuối, thực thể AMF kích hoạt quy trình xác thực, và sau đó thực thể AMF có thể lựa chọn thực thể chức năng máy chủ xác thực (authentication server function, viết tắt là AUSF) dựa vào thông tin nhận dạng lâu dài của thiết bị đầu cuối, để khởi tạo việc xác thực và việc kiểm chứng của thiết bị đầu cuối.

Trong công nghệ liên quan nêu trên, khi thiết bị đầu cuối gửi thông tin nhận dạng lâu dài đến thực thể AMF qua gNB hoặc N3IWF, để kích hoạt quy trình xác

thực, không có việc xử lý mã hóa được thực hiện trên thông tin nhận dạng lâu dài. Trong trường hợp này, thông tin nhận dạng lâu dài dễ dàng bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối bị đe dọa.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất phương pháp kích hoạt xác thực mạng và thiết bị liên quan, để giải quyết vấn đề trong công nghệ liên quan là tính bảo mật của thiết bị đầu cuối bị đe dọa vì thông tin nhận dạng lâu dài được cung cấp bởi thiết bị đầu cuối cho thực thể AMF không được mã hóa khi quy trình xác thực được kích hoạt. Các giải pháp kỹ thuật là như sau đây:

Theo khía cạnh thứ nhất, phương pháp kích hoạt xác thực mạng được đề xuất. Phương pháp bao gồm các bước:

thu, bởi thiết bị mạng thứ nhất, tin nhắn thứ nhất từ thiết bị đầu cuối, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, và thông tin ký hiệu nhận dạng được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; và gửi, bởi thiết bị mạng thứ nhất, tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất theo thông tin nhận dạng thứ nhất, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối.

Theo giải pháp của phương án này của sáng chế, thiết bị mạng thứ nhất có thể gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất theo thông tin nhận dạng thứ nhất, để kích hoạt việc xác thực cho thiết bị đầu cuối. Có thể hiểu rằng phương án này của sáng chế đề xuất giải pháp kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối được đảm bảo.

Hơn nữa, trong quá trình thực hiện sáng chế, tin nhắn thứ nhất mang thông tin ký

hiệu nhận dạng, để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất, sao cho thực thể chức năng được sử dụng để giải mã thông tin nhận dạng thứ nhất có thể giải mã thông tin nhận dạng thứ nhất nhanh hơn và thuận tiện hơn.

Theo thiết kế có thể, khóa công khai được lưu trữ trong thiết bị đầu cuối, hoặc được lưu trữ trong thẻ nằm trong thiết bị đầu cuối và được sử dụng để lưu trữ khóa dài hạn.

Theo thiết kế có thể, thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ nhất, và ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không; hoặc

thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ hai, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; hoặc

thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ ba, và ký hiệu nhận dạng thứ ba được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; hoặc

thông tin ký hiệu nhận dạng bao gồm ký hiệu nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai, ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất.

Theo thiết kế có thể, thiết bị mạng thứ nhất gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất; thiết bị mạng thứ nhất thu tin nhắn đáp lại nhận dạng lâu dài từ thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn đáp lại nhận dạng lâu dài mang thông tin nhận dạng thứ hai, và thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất; và thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ hai mang thông tin nhận dạng thứ hai.

Theo thiết kế có thể, theo cách khác, thiết bị mạng thứ nhất có thể gửi tin nhắn yêu cầu nhận dạng lâu dài đến thiết bị mạng thứ hai, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất; thiết bị mạng thứ nhất thu tin nhắn đáp lại nhận dạng lâu dài từ thiết bị mạng thứ hai, trong đó tin nhắn đáp lại nhận dạng lâu dài mang thông tin nhận dạng thứ hai, và thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất; và thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ hai mang thông tin nhận dạng thứ hai.

Theo thiết kế có thể, thông tin nhận dạng thứ hai được thu nhận bởi thiết bị mạng thứ hai bằng cách giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân được lưu trữ; hoặc thông tin nhận dạng thứ hai được thu nhận sau khi thiết bị mạng thứ hai chuyển thông tin nhận dạng thứ nhất đến thiết bị mạng thứ ba và thiết bị mạng thứ ba giải mã thông tin nhận dạng thứ nhất.

Theo thiết kế có thể, thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ hai mang thông tin nhận dạng thứ nhất; sau đó thiết bị mạng thứ nhất thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, trong đó thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất, trong đó

việc thu, bởi thiết bị mạng thứ nhất, thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất bao gồm một trong số các trường hợp sau:

thu, bởi thiết bị mạng thứ nhất, tin nhắn thứ ba từ thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ ba mang tin nhắn phản hồi xác thực, tin nhắn phản hồi xác thực mang thông tin nhận dạng thứ hai và vectơ xác thực, và vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối; hoặc tin nhắn thứ ba mang thông tin nhận dạng thứ hai và tin nhắn phản hồi xác thực, tin nhắn phản hồi xác thực mang vectơ xác thực, và vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối; hoặc tin nhắn thứ ba mang tin nhắn thành công xác thực, và tin nhắn thành công xác thực mang thông tin nhận dạng thứ hai; hoặc tin nhắn thứ ba mang thông tin nhận dạng thứ hai và tin nhắn thành công xác thực; hoặc

thu, bởi thiết bị mạng thứ nhất, tin nhắn thứ tư được gửi bởi thực thể chức năng

bảo mật thứ nhất, trong đó tin nhắn thứ tư mang vectơ xác thực và thông tin nhận dạng thứ hai, và vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối.

Theo thiết kế có thể, trước khi thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, thiết bị mạng thứ nhất thu vectơ xác thực được gửi bởi thực thể chức năng bảo mật thứ nhất, thực hiện việc xác thực cho thiết bị đầu cuối nhờ sử dụng vectơ xác thực, và gửi tin nhắn báo nhận xác thực đến thực thể chức năng bảo mật thứ nhất sau khi việc xác thực cho thiết bị đầu cuối thành công.

Theo thiết kế có thể, sau khi thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, thiết bị mạng thứ nhất có thể lưu trữ thông tin nhận dạng thứ hai.

Theo thiết kế có thể, thiết bị mạng thứ hai là bất kỳ một trong số thực thể chức năng xử lý và chứa chứng nhận xác thực, thực thể quản lý dữ liệu hợp nhất, máy chủ quản lý khóa, hoặc trung tâm kiểm chứng.

Theo khía cạnh thứ hai, phương pháp kích hoạt xác thực mạng được đề xuất. Phương pháp bao gồm các bước: thu, bởi thực thể chức năng bảo mật thứ nhất, tin nhắn thứ hai từ thiết bị mạng thứ nhất, trong đó tin nhắn thứ hai được gửi bởi thiết bị mạng thứ nhất dựa vào thông tin nhận dạng thứ nhất được mang trong tin nhắn thứ nhất của thiết bị đầu cuối, tin nhắn thứ hai được sử dụng để kích hoạt quy trình xác thực cho thiết bị đầu cuối, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, tin nhắn thứ hai mang thông tin ký hiệu nhận dạng, và thông tin ký hiệu nhận dạng được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất. Theo giải pháp của phương án này của sáng chế, sau khi thu tin nhắn thứ hai, thực thể chức năng bảo mật thứ nhất có thể kích hoạt việc xác thực cho thiết bị đầu cuối. Ngoài ra, vì tin nhắn thứ hai mang thông tin ký hiệu nhận dạng, thực thể chức năng bảo mật thứ nhất có thể xác định, dựa vào thông tin ký hiệu nhận dạng, việc tin nhắn thứ hai có mang thông tin nhận dạng được mã hóa hay không, để xác định có thực hiện việc giải mã hay không.

Theo thiết kế có thể, khóa công khai được lưu trữ trong thiết bị đầu cuối, hoặc được lưu trữ trong thẻ nằm trong thiết bị đầu cuối và được sử dụng để lưu trữ khóa dài hạn.

Theo thiết kế có thể, thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ nhất, và ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không; hoặc thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ hai, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; hoặc thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ ba, và ký hiệu nhận dạng thứ ba được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; hoặc thông tin ký hiệu nhận dạng bao gồm ký hiệu nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai, ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất.

Theo thiết kế có thể, tin nhắn thứ hai mang thông tin nhận dạng thứ hai, và thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất.

Một cách tương ứng, trước khi thu tin nhắn thứ hai từ thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất thu tin nhắn yêu cầu nhận dạng lâu dài từ thiết bị mạng thứ nhất, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất; thực thể chức năng bảo mật thứ nhất thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất; và thực thể chức năng bảo mật thứ nhất gửi tin nhắn đáp lại nhận dạng lâu dài đến thiết bị mạng thứ nhất, trong đó tin nhắn đáp lại nhận dạng lâu dài mang thông tin nhận dạng thứ hai.

Theo thiết kế có thể, tin nhắn thứ hai mang thông tin nhận dạng thứ nhất, và sau khi thu tin nhắn thứ hai từ thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất, trong đó thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất, trong đó

việc thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất bao gồm một trong số các trường hợp sau:

thực thể chức năng bảo mật thứ nhất thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai, trong đó vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối; và thực thể chức năng bảo mật thứ nhất gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất, trong đó tin nhắn thứ ba mang tin nhắn phản hồi xác thực, và tin nhắn phản hồi xác thực mang vectơ xác thực và thông tin nhận dạng thứ hai, hoặc tin nhắn thứ ba mang tin nhắn phản hồi xác thực và thông tin nhận dạng thứ hai, và tin nhắn phản hồi xác thực mang vectơ xác thực; hoặc

thực thể chức năng bảo mật thứ nhất thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai, trong đó vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối; và thực thể chức năng bảo mật thứ nhất thực hiện việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực, và gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất sau khi việc xác thực cho thiết bị đầu cuối thành công, trong đó tin nhắn thứ ba mang tin nhắn thành công xác thực, và tin nhắn thành công xác thực mang thông tin nhận dạng thứ hai, hoặc tin nhắn thứ ba mang tin nhắn thành công xác thực và thông tin nhận dạng thứ hai; hoặc

thực thể chức năng bảo mật thứ nhất thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai, trong đó vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối; và thực thể chức năng bảo mật thứ nhất gửi tin nhắn thứ tư đến thiết bị mạng thứ nhất, trong đó tin nhắn thứ tư mang vectơ xác thực và thông tin nhận dạng thứ hai; hoặc

thực thể chức năng bảo mật thứ nhất thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai, trong đó vectơ xác thực được sử dụng để thực hiện việc xác thực cho thiết bị đầu cuối; thực thể chức năng bảo mật thứ nhất gửi vectơ xác thực đến thiết bị mạng thứ nhất; và thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi thu tin nhắn báo nhận xác thực được gửi bởi thiết bị mạng thứ nhất.

Theo thiết kế có thể, quy trình trong đó thực thể chức năng bảo mật thứ nhất thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai có thể bao gồm các bước: gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ hai đến thực

thể chức năng bảo mật thứ hai; và thu, bởi thực thể chức năng bảo mật thứ nhất, vectơ xác thực từ thực thể chức năng bảo mật thứ hai.

Theo thiết kế có thể, trước khi gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất có thể còn thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất.

Theo thiết kế có thể, quy trình trong đó thực thể chức năng bảo mật thứ nhất thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất có thể bao gồm các bước: giải mã, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất dựa vào khóa cá nhân, để thu nhận thông tin nhận dạng thứ hai; hoặc

gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất đến thiết bị mạng thứ hai, và thu thông tin nhận dạng thứ hai được gửi bởi thiết bị mạng thứ hai, trong đó thông tin nhận dạng thứ hai được thu nhận bởi thiết bị mạng thứ hai bằng cách giải mã thông tin nhận dạng thứ nhất dựa vào khóa cá nhân được lưu trữ, hoặc thông tin nhận dạng thứ hai được thu nhận sau khi thiết bị mạng thứ hai chuyển thông tin nhận dạng thứ nhất đến thiết bị mạng thứ ba và thiết bị mạng thứ ba giải mã thông tin nhận dạng thứ nhất.

Theo thiết kế có thể, thiết bị mạng thứ hai là bất kỳ một trong số thực thể chức năng xử lý và chứa chứng nhận xác thực, thực thể quản lý dữ liệu hợp nhất, máy chủ quản lý khóa, hoặc trung tâm kiểm chứng.

Theo khía cạnh thứ ba, phương pháp kích hoạt xác thực mạng được đề xuất. Phương pháp bao gồm các bước: thu, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất từ thiết bị mạng thứ nhất, trong đó thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai; gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ hai; và thu, bởi thực thể chức năng bảo mật thứ nhất, vectơ xác thực và thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ hai, và kích hoạt quy trình xác thực cho thiết bị đầu cuối, trong đó thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất, và vectơ xác thực được thu nhận bởi thực thể chức năng bảo mật thứ hai dựa vào thông tin nhận dạng thứ hai. Giải pháp của phương án này của sáng chế đề xuất quy trình thực

hiện cụ thể của việc kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Ngoài ra, theo giải pháp của phương án này của sáng chế, thực thể chức năng bảo mật thứ nhất kích hoạt việc xác thực cho thiết bị đầu cuối. Vì quy trình xác thực cho thiết bị đầu cuối được kích hoạt bởi thực thể chức năng bảo mật thứ nhất khi thiết bị đầu cuối truy cập mạng nhờ sử dụng công nghệ 3GPP, nên việc xử lý đối với công nghệ 3GPP và việc xử lý đối với công nghệ không phải 3GPP trong quy trình xác thực cho thiết bị đầu cuối là thống nhất theo giải pháp của phương án này, nhờ đó làm giảm độ phức tạp xử lý của thiết bị mạng.

Theo thiết kế có thể, thông tin nhận dạng thứ hai được thu nhận bởi thực thể chức năng bảo mật thứ hai bằng cách giải mã thông tin nhận dạng thứ nhất dựa vào khóa cá nhân được lưu trữ; hoặc thông tin nhận dạng thứ hai được thu nhận sau khi thực thể chức năng bảo mật thứ hai chuyển thông tin nhận dạng thứ nhất đến thiết bị mạng thứ hai và thiết bị mạng thứ hai giải mã thông tin nhận dạng thứ nhất; hoặc thông tin nhận dạng thứ hai được thu nhận sau khi thực thể chức năng bảo mật thứ hai chuyển thông tin nhận dạng thứ nhất đến thiết bị mạng thứ hai, thiết bị mạng thứ hai chuyển thông tin nhận dạng thứ nhất đến thiết bị mạng thứ ba, và thiết bị mạng thứ ba giải mã thông tin nhận dạng thứ nhất.

Theo thiết kế có thể, sau khi kích hoạt quy trình xác thực cho thiết bị đầu cuối, thực thể chức năng bảo mật thứ nhất có thể gửi vectơ xác thực đến thiết bị mạng thứ nhất, thu tin nhắn báo nhận xác thực từ thiết bị mạng thứ nhất, và gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất.

Theo khía cạnh thứ tư, phương án của sáng chế đề xuất thiết bị mạng thứ nhất. Thiết bị mạng thứ nhất có chức năng thực hiện cách xử lý của thiết bị mạng thứ nhất theo thiết kế về phương pháp nêu trên. Chức năng có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên.

Theo thiết kế có thể, thiết bị mạng thứ nhất bao gồm bộ xử lý, và bộ xử lý được tạo cấu hình để hỗ trợ thiết bị mạng thứ nhất trong việc thực hiện chức năng tương ứng theo phương pháp nêu trên. Hơn nữa, thiết bị mạng thứ nhất có thể còn bao gồm giao diện truyền thông. Giao diện truyền thông được tạo cấu hình để hỗ trợ

thiết bị mạng thứ nhất trong việc giao tiếp với thực thể chức năng bảo mật thứ nhất, thiết bị đầu cuối, hoặc thiết bị mạng khác. Hơn nữa, thiết bị mạng thứ nhất có thể còn bao gồm bộ nhớ. Bộ nhớ được ghép đôi với bộ xử lý và được tạo cấu hình để lưu trữ dữ liệu và lệnh chương trình mà cần thiết đối với thiết bị mạng thứ nhất.

Theo khía cạnh thứ năm, phương án của sáng chế đề xuất thực thể chức năng bảo mật thứ nhất. Thực thể chức năng bảo mật thứ nhất có chức năng thực hiện cách xử lý của thực thể chức năng bảo mật thứ nhất theo thiết kế về phương pháp nêu trên. Chức năng có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên.

Theo thiết kế có thể, thực thể chức năng bảo mật thứ nhất bao gồm bộ xử lý, và bộ xử lý được tạo cấu hình để hỗ trợ thực thể chức năng bảo mật thứ nhất trong việc thực hiện chức năng tương ứng theo phương pháp nêu trên. Hơn nữa, thực thể chức năng bảo mật thứ nhất có thể còn bao gồm giao diện truyền thông. Giao diện truyền thông được tạo cấu hình để hỗ trợ thực thể chức năng bảo mật thứ nhất trong việc giao tiếp với thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ hai, hoặc thiết bị mạng khác. Hơn nữa, thực thể chức năng bảo mật thứ nhất có thể còn bao gồm bộ nhớ. Bộ nhớ được ghép đôi với bộ xử lý và được tạo cấu hình để lưu trữ dữ liệu và lệnh chương trình mà cần thiết đối với thực thể chức năng bảo mật thứ nhất.

Theo khía cạnh thứ sáu, phương án của sáng chế đề xuất thực thể chức năng bảo mật thứ hai. Thực thể chức năng bảo mật thứ hai có chức năng thực hiện cách xử lý của thực thể chức năng bảo mật thứ hai theo thiết kế về phương pháp nêu trên. Chức năng có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên.

Theo thiết kế có thể, thực thể chức năng bảo mật thứ hai bao gồm bộ xử lý, và bộ xử lý được tạo cấu hình để hỗ trợ thực thể chức năng bảo mật thứ hai trong việc thực hiện chức năng tương ứng theo phương pháp nêu trên. Hơn nữa, thực thể chức năng bảo mật thứ hai có thể còn bao gồm giao diện truyền thông. Giao diện truyền thông được tạo cấu hình để hỗ trợ thực thể chức năng bảo mật thứ hai trong việc giao tiếp với thực thể chức năng bảo mật thứ nhất hoặc thiết bị mạng khác. Hơn

nữa, thực thể chức năng bảo mật thứ hai có thể còn bao gồm bộ nhớ. Bộ nhớ được ghép đôi với bộ xử lý và được tạo cấu hình để lưu trữ dữ liệu và lệnh chương trình mà cần thiết đối với thực thể chức năng bảo mật thứ hai.

Theo khía cạnh thứ bảy, phương án của sáng chế đề xuất thiết bị đầu cuối. Thiết bị đầu cuối có chức năng thực hiện cách xử lý của thiết bị đầu cuối theo thiết kế về phương pháp nêu trên. Chức năng có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên.

Theo thiết kế có thể, thiết bị đầu cuối bao gồm bộ xử lý. Bộ xử lý được tạo cấu hình để hỗ trợ thiết bị đầu cuối trong việc thực hiện chức năng tương ứng theo phương pháp nêu trên. Hơn nữa, thiết bị đầu cuối có thể còn bao gồm giao diện truyền thông. Giao diện truyền thông được tạo cấu hình để hỗ trợ thiết bị đầu cuối trong việc giao tiếp với thiết bị mạng thứ nhất hoặc thiết bị mạng khác. Hơn nữa, thiết bị đầu cuối có thể còn bao gồm bộ nhớ. Bộ nhớ được ghép đôi với bộ xử lý và được tạo cấu hình để lưu trữ dữ liệu và lệnh chương trình mà cần thiết đối với thiết bị đầu cuối.

Theo khía cạnh thứ tám, phương án của sáng chế đề xuất hệ thống truyền thông. Hệ thống bao gồm thiết bị đầu cuối, thiết bị mạng thứ nhất, và thực thể chức năng bảo mật thứ nhất theo các khía cạnh nêu trên.

Theo khía cạnh khác, phương án của sáng chế đề xuất phương tiện lưu trữ đọc được bởi máy tính. Phương tiện lưu trữ đọc được bởi máy tính lưu trữ lệnh, và khi các lệnh chạy trên máy tính, máy tính thực hiện các phương pháp theo các khía cạnh nêu trên.

Theo khía cạnh khác, phương án của sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh. Khi lệnh chạy trên máy tính, máy tính thực hiện các phương pháp theo các khía cạnh nêu trên.

So với kỹ thuật đã biết, các giải pháp của các phương án của sáng chế đề xuất giải pháp kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất là thông tin nhận dạng được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối

được đảm bảo.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ giản lược của kiến trúc mạng có thể theo phương án của sáng chế;

Fig.2 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.3 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.4 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.5 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.6a là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.6b là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.6c là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.6d là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.7a là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.7b là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng theo phương án của sáng chế;

Fig.8a là sơ đồ khối giản lược của thiết bị mạng thứ nhất theo phương án của sáng chế;

Fig.8b là sơ đồ cấu trúc giản lược của thiết bị mạng thứ nhất theo phương án của sáng chế;

Fig.9a là sơ đồ khối giản lược của thực thể chức năng bảo mật thứ nhất theo phương án của sáng chế;

Fig.9b là sơ đồ cấu trúc giản lược của thực thể chức năng bảo mật thứ nhất theo phương án của sáng chế;

Fig.10a là sơ đồ khối giản lược của thực thể chức năng bảo mật thứ hai theo phương án của sáng chế; và

Fig.10b là sơ đồ cấu trúc giản lược của thực thể chức năng bảo mật thứ hai theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần sau đây mô tả chi tiết hơn các phương án của sáng chế dựa vào các hình vẽ kèm theo.

Trước khi các phương án của sáng chế được mô tả chi tiết, các kịch bản ứng dụng theo các phương án của sáng chế được mô tả trước tiên. Hiện nay, thiết bị đầu cuối có thể truy cập mạng nhờ sử dụng công nghệ 3GPP hoặc nhờ sử dụng công nghệ không phải 3GPP. Công nghệ 3GPP là công nghệ giao diện không gian được đưa ra bởi chuẩn 3GPP. Ví dụ, các công nghệ truy cập giao diện không gian phổ biến của các mạng 3G, 4G, và 5G là công nghệ 3GPP. Công nghệ không phải 3GPP là công nghệ truy cập giao diện không gian được đưa ra bởi chuẩn không phải 3GPP, ví dụ, công nghệ giao diện không gian được đại diện bởi điểm truy cập mạng không dây sử dụng sóng vô tuyến (Wireless Fidelity access point, viết tắt là WiFi AP). Khi thiết bị đầu cuối truy cập mạng 5G, bất kể việc thiết bị đầu cuối truy cập mạng 5G nhờ sử dụng công nghệ 3GPP hoặc nhờ sử dụng công nghệ không phải 3GPP, thiết bị đầu cuối cần gửi tin nhắn kèm theo mang thông tin nhận dạng lâu dài đến thiết bị trong mạng lõi, sao cho thiết bị trong mạng lõi có thể kích hoạt quy trình xác thực, dựa vào tin nhắn kèm theo và thông tin nhận dạng lâu dài, để thực hiện việc xác thực cho thiết bị đầu cuối. Phương pháp kích hoạt xác thực mạng được đề xuất theo các phương án của sáng chế có thể được ứng dụng cho kịch bản nêu trên, để kích hoạt quy trình xác thực cho thiết bị đầu cuối, nhờ đó thực hiện việc xác thực cho thiết bị đầu cuối.

Phương pháp thu nhận sự nhận dạng của thiết bị đầu cuối theo các phương án của sáng chế có thể được ứng dụng cho hệ thống truyền thông bất kỳ có nhu cầu thu nhận sự nhận dạng của thiết bị đầu cuối, ví dụ, có thể được ứng dụng cho hệ

thống 5G như được thể hiện trên Fig.1.

Như được thể hiện trên Fig.1, hệ thống 5G có thể bao gồm thiết bị đầu cuối, thiết bị truy cập (access network, viết tắt là AN)/ mạng truy cập rađio (radio access network, viết tắt là RAN), mạng dữ liệu (data network, viết tắt là DN), và các chức năng mạng (network function, viết tắt là NF) bao gồm chức năng máy chủ xác thực (authentication server function, viết tắt là AUSF), chức năng xử lý và chứa chứng nhận xác thực (authentication repository and processing function, viết tắt là ARPF), chức năng quản lý di động và truy cập (access and mobility management function, viết tắt là AMF), chức năng quản lý phiên (session management function, viết tắt là SMF), PCF, chức năng ứng dụng (application function, viết tắt là AF), và chức năng mặt phẳng người dùng (user plane function, viết tắt là UPF). Có thể hiểu rằng Fig.1 chỉ là sơ đồ kiến trúc ví dụ. Ngoài các thực thể chức năng như được thể hiện trên Fig.1, hệ thống 5G có thể còn bao gồm các thực thể chức năng khác, và điều này không giới hạn theo phương án này của sáng chế.

Trong hệ thống 5G như được thể hiện trên Fig.1, sự kết nối có thể được thiết lập giữa các thực thể chức năng nhờ sử dụng giao diện thế hệ tiếp theo (next generation, viết tắt là NG) để thực hiện việc truyền thông. Ví dụ, thiết bị đầu cuối có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến AMF nhờ sử dụng giao diện N 1 (viết tắt là N1). AN/RAN có thể thiết lập sự kết nối dữ liệu mặt phẳng người dùng đến UPF nhờ sử dụng giao diện N 3 (viết tắt là N3). AN/RAN có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến AMF nhờ sử dụng giao diện N 2 (viết tắt là N2). UPF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến SMF nhờ sử dụng giao diện N 4 (viết tắt là N4). UPF có thể trao đổi dữ liệu mặt phẳng người dùng với DN nhờ sử dụng giao diện N 6 (viết tắt là N6). AMF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến ARPF nhờ sử dụng giao diện N 8 (viết tắt là N8). AMF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến AUSF nhờ sử dụng giao diện N 12 (viết tắt là N12). AMF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến SMF nhờ sử dụng giao diện N 11 (viết tắt là N11). SMF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến PCF nhờ sử dụng giao diện N 7 (viết tắt là N7). PCF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến

AF nhờ sử dụng giao diện N 5 (viết tắt là N5). AUSF có thể thiết lập sự kết nối truyền tín hiệu mặt phẳng điều khiển đến ARPF nhờ sử dụng giao diện N 13 (viết tắt là N13).

Thiết bị đầu cuối trên Fig.1 có thể là UE, hoặc có thể là điện thoại di động, điện thoại không dây, điện thoại giao thức khởi tạo phiên (session initiation protocol, viết tắt là SIP), điện thoại thông minh, trạm lặp cục bộ không dây (wireless local loop, viết tắt là WLL), hỗ trợ số cá nhân (personal digital assistant, viết tắt là PDA), máy tính xách tay, thiết bị truyền thông cầm tay, thiết bị tính cầm tay, thiết bị rađio vệ tinh, thẻ môđem không dây, và/hoặc thiết bị khác được tạo cấu hình để thực hiện việc truyền thông trong hệ thống rađio. AN/RAN là mạng bao gồm các 5G-AN/các 5G-RAN, và được tạo cấu hình để thực hiện chức năng lớp vật lý rađio, chức năng quản lý tài nguyên rađio và lập lịch tài nguyên, chức năng điều khiển truy cập rađio, và chức năng quản lý di động. 5G-AN/5G-RAN có thể là điểm truy cập, nút B thế hệ tiếp theo NodeB, N3IWF, điểm thu truyền (transmission reception point, viết tắt là TRP), điểm truyền (transmission point, viết tắt là TP), hoặc thiết bị mạng truy cập khác. ARPF, AUSF, PCF, AMF, SMF, và UPF có thể được gọi chung là NF. Trong NF, AMF và PCF có thể được gọi là chức năng mặt phẳng điều khiển (control plane, viết tắt là CP), và UPF có thể được gọi là chức năng mặt phẳng người dùng (user plane function, viết tắt là UPF). NF, ngoại trừ UPF, có thể làm việc độc lập, hoặc có thể được kết hợp để thực hiện chức năng điều khiển. Ví dụ, NF được kết hợp có thể kết thúc chức năng quản lý di động và điều khiển truy cập chẳng hạn như xác thực truy cập, mã hóa bảo mật, và đăng ký vị trí của thiết bị đầu cuối, chức năng quản lý phiên chẳng hạn như thiết lập, ngắt, và thay đổi đường truyền mặt phẳng người dùng, và chức năng phân tích dữ liệu liên quan đến một số ngăn (slice) (ví dụ, sự tắc nghẽn) và dữ liệu liên quan đến thiết bị đầu cuối. UPF chủ yếu kết thúc chức năng chẳng hạn như định tuyến và chuyển của dữ liệu mặt phẳng người dùng, ví dụ, chịu trách nhiệm về việc lọc gói dữ liệu, truyền/chuyển dữ liệu, điều khiển tốc độ, tạo ra thông tin tính cước, và tương tự cho thiết bị đầu cuối.

Cụ thể là, AMF chủ yếu chịu trách nhiệm về việc quản lý di động. Hiện nay, môđun chức năng neo bảo mật (security anchor function, viết tắt là SEAF) còn

được tích hợp vào AMF. Môđun SEAF chủ yếu chịu trách nhiệm về việc khởi tạo yêu cầu xác thực đến AUSF, và kết thúc việc xác thực cho thiết bị đầu cuối ở phía mạng trong quy trình xác thực của hệ thống gói được cải tiến. Chức năng chính của AUSF là thu yêu cầu xác thực được gửi bởi môđun SEAF, và lựa chọn phương pháp xác thực. Khi phương pháp xác thực của giao thức xác thực có thể mở rộng được sử dụng, AUSF chủ yếu chịu trách nhiệm về kết thúc việc xác thực cho thiết bị đầu cuối trên thiết bị mạng. Ngoài ra, AUSF có thể yêu cầu vectơ xác thực từ ARPF, và trả lời môđun SEAF với phản hồi xác thực. Chức năng chính của ARPF là lưu trữ khóa dài hạn, thu vectơ xác thực yêu cầu được gửi bởi AUSF, tính vectơ xác thực nhờ sử dụng khóa dài hạn được lưu trữ, và gửi vectơ xác thực đến AUSF.

Sau khi kịch bản ứng dụng và kiến trúc hệ thống theo các phương án của sáng chế được mô tả, phần sau đây mô tả chi tiết các giải pháp của các phương án của sáng chế.

Trong giải pháp hiện có, khi thiết bị đầu cuối gửi thông tin nhận dạng lâu dài đến AMF qua gNB hoặc N3IWF, để kích hoạt quy trình xác thực, không có việc xử lý mã hóa được thực hiện trên thông tin nhận dạng lâu dài. Trong trường hợp này, thông tin nhận dạng lâu dài dễ dàng bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối bị đe dọa.

Từ quan điểm này, các phương án của sáng chế đề xuất phương pháp kích hoạt xác thực mạng, và thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất, và hệ thống dựa vào phương pháp này. Phương pháp bao gồm các bước: thu, bởi thiết bị mạng thứ nhất, tin nhắn thứ nhất từ thiết bị đầu cuối, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất, và thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai; gửi, bởi thiết bị mạng thứ nhất, tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất theo thông tin nhận dạng thứ nhất, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối. Ví dụ, phương pháp có thể như được thể hiện trên Fig.2. Theo các giải pháp được đề xuất theo các phương án của sáng chế, sau khi thu thông tin nhận dạng thứ nhất được gửi bởi thiết bị đầu cuối, thiết bị mạng thứ nhất có thể gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất dựa vào thông tin nhận dạng

thứ nhất, để kích hoạt việc xác thực cho thiết bị đầu cuối. Thông tin nhận dạng thứ nhất được thu nhận bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài. Nói cách khác, các phương án của sáng chế đề xuất giải pháp kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất là thông tin nhận dạng được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối được đảm bảo.

Theo cách thực hiện có thể, tin nhắn thứ nhất có thể còn mang một hoặc tất cả trong số thông tin ký hiệu nhận dạng và thông tin định tuyến. Phần sau đây mô tả thông tin ký hiệu nhận dạng và thông tin định tuyến.

Thông tin ký hiệu nhận dạng được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất. Ví dụ, thông tin ký hiệu nhận dạng có thể là ký hiệu nhận dạng thứ nhất, và ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không; hoặc thông tin ký hiệu nhận dạng có thể là ký hiệu nhận dạng thứ hai, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; hoặc thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ ba, và ký hiệu nhận dạng thứ ba được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất; hoặc thông tin ký hiệu nhận dạng có thể bao gồm ký hiệu nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai, ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất.

Thông tin định tuyến có thể là thông tin định tuyến thứ nhất, và thông tin định tuyến thứ nhất có thể được sử dụng bởi thiết bị mạng thứ nhất để xác định mạng gia đình của thiết bị đầu cuối, sao cho thiết bị mạng thứ nhất có thể lựa chọn thực thể chức năng bảo mật thứ nhất trong mạng gia đình của thiết bị đầu cuối. Theo cách khác, thông tin định tuyến có thể là thông tin định tuyến thứ hai, và thông tin định

tuyến thứ hai được sử dụng để xác định thực thể chức năng giải mã thông tin nhận dạng thứ nhất.

Theo cách thực hiện này, khi tin nhắn thứ nhất mang thông tin ký hiệu nhận dạng, tin nhắn thứ hai mang thông tin ký hiệu nhận dạng.

Theo các phương án của sáng chế, thiết bị mạng thứ nhất có thể kích hoạt quy trình xác thực cho thiết bị đầu cuối sau khi thu nhận thông tin nhận dạng thứ hai tương ứng với thông tin nhận dạng thứ nhất, hoặc có thể thu nhận thông tin nhận dạng thứ hai sau khi kích hoạt quy trình xác thực. Thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất. Phần sau đây mô tả trường hợp thứ nhất dựa vào các hình vẽ từ Fig.3 đến Fig.5.

Fig.3 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng khác theo phương án của sáng chế. Dựa vào Fig.3, phương pháp bao gồm các bước sau đây.

Bước 301. Thiết bị đầu cuối gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất qua trạm gốc, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, và thông tin ký hiệu nhận dạng được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất.

Thiết bị đầu cuối có thể là thiết bị đầu cuối trong kiến trúc mạng 5G như được thể hiện trên Fig.1, và thực thể chức năng trạm gốc có thể là thực thể chức năng trạm gốc 3GPP, hoặc có thể là thực thể chức năng trạm gốc không phải 3GPP. Cụ thể là, khi thiết bị đầu cuối truy cập mạng 5G nhờ sử dụng công nghệ 3GPP, thực thể chức năng trạm gốc có thể là thực thể chức năng gNB, hoặc thực thể chức năng eNB, hoặc thực thể chức năng NB. Khi thiết bị đầu cuối truy cập mạng nhờ sử dụng công nghệ không phải 3GPP, ví dụ, qua WiFi, thực thể chức năng trạm gốc có thể bao gồm thực thể chức năng N3IWF. Khi môđun SEAF được tích hợp vào thực thể chức năng AMF, thiết bị mạng thứ nhất có thể là thực thể chức năng AMF, hoặc có thể là môđun SEAF trong thực thể chức năng AMF. Khi AMF và SEAF

không phải là một thực thể chức năng, thiết bị mạng thứ nhất có thể là thực thể chức năng AMF, hoặc thực thể chức năng MME, hoặc thực thể khác có chức năng quản lý di động và truy cập.

Khi thiết bị đầu cuối truy cập mạng hoặc khi việc xác thực được thực hiện trên thiết bị đầu cuối, thiết bị đầu cuối có thể gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất qua trạm gốc. Tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất, và thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài nhờ sử dụng khóa công khai, ví dụ, SUCI (ký hiệu nhận dạng được giấu của sự thuê bao- subscription concealed identifier, sự nhận dạng lâu dài được mã hóa). Khóa công khai mã hóa có thể được lưu trữ trong thiết bị đầu cuối, hoặc có thể được lưu trữ trong thẻ nằm trong thiết bị đầu cuối và được sử dụng để lưu trữ khóa dài hạn, ví dụ, môđun nhận dạng thuê bao (subscriber identification module, viết tắt là SIM), môđun nhận dạng thuê bao đa năng (universal subscriber identity module, viết tắt là USIM), thẻ mạch tích hợp đa năng (universal integrated circuit card, viết tắt là UICC), thẻ mạch tích hợp đa năng được nhúng (embedded universal integrated circuit card, viết tắt là eUICC), hoặc thẻ mạch tích hợp đa năng 5G (5G–universal integrated circuit card, viết tắt là 5G-UICC). Nhận dạng lâu dài có thể là nhận dạng thuê bao di động quốc tế (international mobile subscriber identification number, viết tắt là IMSI), ký hiệu nhận dạng lâu dài thuê bao (subscription permanent identifier), hoặc thông tin nhận dạng khác có chức năng nhận dạng duy nhất trên toàn cầu của thiết bị đầu cuối. Cụ thể là, khi sự nhận dạng lâu dài là IMSI, IMSI bao gồm số nhận dạng thuê bao di động (international mobile subscriber identification number, viết tắt là MSIN) và thông tin định tuyến. Do đó, thiết bị đầu cuối có thể mã hóa MSIN trong IMSI nhờ sử dụng khóa công khai, để thu nhận thông tin nhận dạng thứ nhất. Khi sự nhận dạng lâu dài không được dựa vào cấu trúc IMSI, thông tin nhận dạng thứ nhất có thể là thông tin nhận dạng được thu nhận bằng cách mã hóa toàn bộ sự nhận dạng lâu dài, hoặc có thể là thông tin được thu nhận bằng cách mã hóa chỉ một phần được sử dụng để nhận dạng duy nhất thiết bị đầu cuối trong sự nhận dạng lâu dài.

Ngoài ra, tin nhắn thứ nhất có thể mang thông tin định tuyến thứ nhất, và thông tin định tuyến thứ nhất có thể được sử dụng bởi thiết bị mạng thứ nhất để xác định

mạng gia đình của thiết bị đầu cuối, sao cho thiết bị mạng thứ nhất lựa chọn thực thể chức năng bảo mật thứ nhất trong mạng gia đình của thiết bị đầu cuối.

Một cách tùy ý, tin nhắn thứ nhất có thể còn mang thông tin định tuyến thứ hai, trong đó thông tin định tuyến thứ hai được sử dụng để xác định thực thể chức năng giải mã thông tin nhận dạng thứ nhất.

Một cách tùy ý, tin nhắn thứ nhất có thể mang thông tin ký hiệu nhận dạng. Cụ thể là, thông tin ký hiệu nhận dạng có thể là ký hiệu nhận dạng thứ nhất, và ký hiệu nhận dạng thứ nhất được sử dụng để nhận dạng thông tin nhận dạng thứ nhất được mang trong tin nhắn thứ nhất có phải là thông tin nhận dạng được mã hóa hay không.

Theo cách thực hiện tùy ý, khi thông tin nhận dạng được mang bởi thiết bị đầu cuối không phải là thông tin nhận dạng thứ nhất mà là thông tin nhận dạng tạm thời, thông tin nhận dạng tạm thời có thể được sử dụng là ký hiệu nhận dạng thứ nhất. Thông tin nhận dạng tạm thời của thiết bị đầu cuối được cung cấp đến thiết bị đầu cuối bởi thực thể chức năng quản lý di động sau khi thực thể chức năng quản lý di động kiểm chứng thiết bị đầu cuối. Theo cách này, khả năng rò rỉ của thông tin nhận dạng lâu dài có thể được làm giảm, và việc bảo vệ quyền riêng tư có thể được nâng cao. Thông tin nhận dạng tạm thời của thiết bị đầu cuối có thể là thông tin nhận dạng 5G tạm thời, hoặc thông tin nhận dạng LTE tạm thời, ví dụ, nhận dạng thiết bị người dùng tạm thời duy nhất trên toàn cầu thế hệ thứ năm (5th-generation globally unique temporary user equipment identity, viết tắt là 5G-GUTI), nhận dạng tạm thời duy nhất trên toàn cầu (globally unique temporary identity, viết tắt là GUTI), nhận dạng thuê bao di động tạm thời-sự phát triển kiến trúc hệ thống (System Architecture Evolution –temporary mobile subscriber identity, viết tắt là S-TMSI), hoặc nhận dạng thuê bao di động tạm thời (temporary mobile subscriber identity, viết tắt là TMSI).

Theo cách thực hiện tùy ý khác, ký hiệu nhận dạng thứ nhất có thể là thông tin bit. Ví dụ, 0 biểu diễn "không được mã hóa", và 1 biểu diễn "được mã hóa".

Một cách tùy ý, thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất có thể là ký hiệu nhận dạng thứ hai, và ký hiệu nhận dạng thứ hai được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất. Ví dụ, cách thức mã

hóa có thể là công nghệ mã hóa đường cong êlip. Theo cách khác, cách thức mã hóa có thể là cách thức mã hóa được định trước khác ở phía UE và phía mạng gia đình. Một cách tùy ý, các cách thức mã hóa có thể được tạo cấu hình, và mỗi cách thức mã hóa có thể tương ứng với một ký hiệu nhận dạng thứ hai. Thực thể chức năng được sử dụng để giải mã thông tin nhận dạng thứ nhất có thể xác định cách thức mã hóa của thông tin nhận dạng thứ nhất dựa vào ký hiệu nhận dạng thứ hai được mang trong tin nhắn thứ nhất, để xác định thêm cách thức giải mã của thông tin nhận dạng thứ nhất.

Một cách tùy ý, thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất có thể là ký hiệu nhận dạng thứ ba, và ký hiệu nhận dạng thứ ba được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất. Ví dụ, ký hiệu nhận dạng thứ ba có thể là thông tin 8 bit. Bốn bit đầu tiên của thông tin được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không, và bốn bit sau cùng của thông tin được sử dụng để nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất. Khi thông tin nhận dạng thứ nhất là thông tin nhận dạng không được mã hóa, tất cả bốn bit sau cùng của thông tin có thể là 0.

Một cách tùy ý, thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất có thể bao gồm cả ký hiệu nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai. Ký hiệu chỉ báo hợp nhất chỉ báo thông tin nhận dạng được mang trong tin nhắn thứ nhất có phải là thông tin nhận dạng được mã hóa hay không. Ngoài ra, khi thông tin nhận dạng được mang trong tin nhắn thứ nhất là thông tin nhận dạng được mã hóa, ký hiệu chỉ báo hợp nhất có thể còn chỉ báo cách thức mã hóa được sử dụng để thu nhận thông tin nhận dạng được mã hóa.

Cần hiểu thêm rằng tin nhắn thứ nhất có thể là bất kỳ một trong số tin nhắn yêu cầu đăng ký, tin nhắn yêu cầu kèm theo, tin nhắn cập nhật vùng vị trí, tin nhắn yêu cầu dịch vụ, và tin nhắn phản hồi sự nhận dạng.

Bước 302. Thiết bị mạng thứ nhất gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất khi thu tin nhắn thứ nhất, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất.

Thực thể chức năng bảo mật thứ nhất có thể là thực thể chức năng AUSF trong kiến trúc mạng 5G như được thể hiện trên Fig.1. Ngoài ra, nếu AMF và SEAF là hai thực thể chức năng khác nhau, thực thể chức năng bảo mật thứ nhất có thể theo cách khác là SEAF.

Sau khi thu tin nhắn thứ nhất, thiết bị mạng thứ nhất có thể thu nhận thông tin nhận dạng thứ nhất được mang trong tin nhắn thứ nhất. Vì thông tin nhận dạng thứ nhất được mã hóa, thiết bị mạng thứ nhất có thể gửi tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất, để thu nhận thông tin nhận dạng thứ hai mà được giải mã từ thông tin nhận dạng thứ nhất. Tin nhắn yêu cầu nhận dạng lâu dài có thể là tin nhắn yêu cầu SUPI, hoặc có thể là tin nhắn yêu cầu cập nhật vị trí.

Một cách tùy ý, khi tin nhắn thứ nhất mang thông tin định tuyến thứ nhất, thiết bị mạng thứ nhất có thể xác định mạng gia đình của thiết bị đầu cuối dựa vào thông tin định tuyến thứ nhất, để xác định thực thể chức năng bảo mật thứ nhất trong mạng gia đình. Cụ thể là, thiết bị mạng thứ nhất có thể xác định thực thể chức năng giải mã được tạo cấu hình trước là thực thể chức năng bảo mật thứ nhất, và gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất.

Một cách tùy ý, khi tin nhắn thứ nhất mang thông tin định tuyến thứ hai, thiết bị mạng thứ nhất có thể xác định, dựa vào thông tin định tuyến thứ hai, thực thể chức năng được sử dụng để giải mã thông tin nhận dạng thứ nhất. Theo cách khác, thiết bị mạng thứ nhất có thể bổ sung thông tin định tuyến thứ hai vào tin nhắn yêu cầu nhận dạng lâu dài, và gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất.

Một cách tùy ý, khi thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất là ký hiệu nhận dạng thứ nhất, và ký hiệu nhận dạng thứ nhất không phải là thông tin nhận dạng tạm thời, thiết bị mạng thứ nhất có thể gửi, đến thực thể chức năng bảo mật thứ nhất, tin nhắn yêu cầu xác thực được sử dụng để yêu cầu thực hiện việc xác thực cho thiết bị đầu cuối, trong đó tin nhắn yêu cầu xác thực mang thông tin nhận dạng thứ nhất. Nếu tin nhắn thứ nhất mang ký hiệu nhận dạng thứ nhất, ký hiệu nhận dạng thứ nhất là thông tin nhận dạng tạm thời, và thiết bị mạng thứ nhất có thể thu nhận thông tin bối cảnh của thiết bị đầu cuối dựa vào thông tin

nhận dạng tạm thời, thiết bị mạng thứ nhất không kích hoạt việc xác thực. Nếu thiết bị mạng thứ nhất không thể thu nhận bối cảnh của thiết bị đầu cuối dựa vào thông tin nhận dạng tạm thời, thiết bị mạng thứ nhất có thể gửi tin nhắn yêu cầu nhận dạng (identity request) đến thiết bị đầu cuối, để yêu cầu nhận dạng lâu dài của thiết bị đầu cuối. Sau đó, thiết bị đầu cuối có thể gửi thông tin nhận dạng thứ nhất đến thiết bị mạng thứ nhất theo tin nhắn yêu cầu nhận dạng, và thiết bị mạng thứ nhất có thể kích hoạt việc xác thực cho thiết bị đầu cuối dựa vào thông tin nhận dạng thứ nhất.

Một cách tùy ý, khi ký hiệu nhận dạng thứ nhất là thông tin bit, thiết bị mạng thứ nhất có thể không phân tách ký hiệu nhận dạng thứ nhất khi thu tin nhắn thứ nhất, mà chuyển ký hiệu nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất. Theo cách khác, thiết bị mạng thứ nhất có thể phân tách ký hiệu nhận dạng thứ nhất, và gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất sau khi xác định rằng, nhờ sử dụng ký hiệu nhận dạng thứ nhất, thông tin nhận dạng thứ nhất là thông tin nhận dạng được mã hóa.

Một cách tùy ý, khi thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất là ký hiệu nhận dạng thứ hai, thiết bị mạng thứ nhất có thể bổ sung ký hiệu nhận dạng thứ hai vào tin nhắn yêu cầu nhận dạng lâu dài được gửi đến thực thể chức năng bảo mật thứ nhất.

Một cách tùy ý, khi thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất là ký hiệu nhận dạng thứ ba, thiết bị mạng thứ nhất có thể phân tách ký hiệu nhận dạng thứ ba. Khi xác định, nhờ sử dụng ký hiệu nhận dạng thứ ba, rằng thông tin nhận dạng thứ nhất là thông tin nhận dạng được mã hóa, thiết bị mạng thứ nhất có thể gửi tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất và ký hiệu nhận dạng thứ ba đến thực thể chức năng bảo mật thứ nhất.

Một cách tùy ý, khi thông tin ký hiệu nhận dạng được mang trong tin nhắn thứ nhất bao gồm ký hiệu nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai, thiết bị mạng thứ nhất có thể gửi tin nhắn yêu cầu nhận dạng lâu dài mang ký hiệu nhận dạng thứ hai và thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất sau khi xác định, nhờ sử dụng ký hiệu nhận dạng thứ nhất, thông tin nhận dạng thứ nhất là thông tin nhận dạng được mã hóa.

Bước 303. Thực thể chức năng bảo mật thứ nhất gửi tin nhắn đáp lại nhận dạng lâu dài, trong đó tin nhắn đáp lại nhận dạng lâu dài mang thông tin nhận dạng thứ hai.

Sau khi thu tin nhắn yêu cầu nhận dạng lâu dài, thực thể chức năng bảo mật thứ nhất có thể thu nhận thông tin nhận dạng thứ hai và gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất. Tin nhắn đáp lại nhận dạng lâu dài có thể là tin nhắn phản hồi SUPI, hoặc có thể là tin nhắn phản hồi cập nhật vị trí.

Thực thể chức năng bảo mật thứ nhất có thể thu nhận thông tin nhận dạng thứ hai nhờ sử dụng một vài phương pháp sau đây.

(1) Thực thể chức năng bảo mật thứ nhất giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân được lưu trữ, để thu nhận thông tin nhận dạng thứ hai.

(2) Thực thể chức năng bảo mật thứ nhất có thể chuyển thông tin nhận dạng thứ nhất thu được đến thiết bị mạng thứ hai, và thiết bị mạng thứ hai giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai. Sau đó, thiết bị mạng thứ hai gửi lại thông tin nhận dạng thứ hai được thu nhận đến thực thể chức năng bảo mật thứ nhất. Thiết bị mạng thứ hai lưu trữ khóa cá nhân, và thiết bị mạng thứ hai có thể là bất kỳ một trong số thực thể chức năng xử lý và chứa chứng nhận xác thực (authentication repository and processing function, viết tắt là ARPF), thực thể quản lý dữ liệu hợp nhất (unified data management, viết tắt là UDM), thực thể chức năng giải mã nhận dạng (identity decryption function, viết tắt là IDF), máy chủ quản lý khóa (key management server, viết tắt là KMS), trung tâm xác thực (authentication center, viết tắt là AuC), hoặc thực thể chức năng lưu trữ khóa và được sử dụng cho việc giải mã.

Một cách tùy ý, khi tin nhắn yêu cầu nhận dạng lâu dài mang thông tin định tuyến thứ nhất, thực thể chức năng bảo mật thứ nhất có thể chuyển thông tin nhận dạng thứ nhất và thông tin định tuyến thứ nhất cùng với thiết bị mạng thứ hai. Khi thiết bị mạng thứ hai là thiết bị mạng lưu trữ các khóa giải mã cá nhân của các mạng điều hành khác nhau, thiết bị mạng thứ hai có thể thu nhận khóa cá nhân của mạng gia đình của thiết bị đầu cuối dựa vào thông tin định tuyến thứ nhất, và giải mã thông tin nhận dạng thứ nhất dựa vào khóa cá nhân thu nhận được.

Theo cách thực hiện có thể khác, thực thể chức năng bảo mật thứ nhất có thể

chuyển trực tiếp tin nhắn yêu cầu nhận dạng lâu dài thu được đến thiết bị mạng thứ hai, để yêu cầu thông tin nhận dạng thứ hai từ thiết bị mạng thứ hai.

(3) Thực thể chức năng bảo mật thứ nhất có thể chuyển thông tin nhận dạng thứ nhất thu được đến thiết bị mạng thứ hai. Khi thiết bị mạng thứ hai không thể tìm thấy khóa cá nhân, thiết bị mạng thứ hai có thể gửi yêu cầu đến thiết bị mạng thứ ba, và thiết bị mạng thứ ba giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai. Sau đó thiết bị mạng thứ ba truyền thông tin nhận dạng thứ hai đến thực thể chức năng bảo mật thứ nhất nhờ sử dụng thiết bị mạng thứ hai. Thiết bị mạng thứ ba lưu trữ khóa cá nhân.

(4) Thực thể chức năng bảo mật thứ nhất có thể thu nhận khóa giải mã cá nhân dựa vào thông tin định tuyến, và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa giải mã cá nhân thu nhận được, để thu nhận thông tin nhận dạng thứ hai. Thông tin định tuyến là thông tin định tuyến được mang trong tin nhắn yêu cầu nhận dạng lâu dài được thu bởi thực thể chức năng bảo mật thứ nhất, và thông tin định tuyến có thể là thông tin định tuyến thứ nhất và/hoặc thông tin định tuyến thứ hai.

Ví dụ, thực thể chức năng bảo mật thứ nhất là thực thể SEAF, thiết bị mạng thứ hai là thực thể AUSF, và thiết bị mạng thứ ba là thực thể ARPF. Sau đó, khóa cá nhân được lưu trữ trong ARPF, và thực thể ARPF giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai. Sau đó, thực thể ARPF gửi thông tin nhận dạng thứ hai đến SEAF. Theo ví dụ khác, thực thể chức năng bảo mật thứ nhất là thực thể AUSF, thiết bị mạng thứ hai là thực thể UDM, và thiết bị mạng thứ ba là thực thể AuC trong thực thể UDM hoặc thực thể lưu trữ khóa cá nhân và có chức năng giải mã. Sau đó, AuC hoặc thực thể lưu trữ khóa cá nhân và có chức năng giải mã giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai. Sau đó, thực thể UDM gửi lại thông tin nhận dạng thứ hai đến thực thể AUSF. AuC và thực thể lưu trữ khóa và có chức năng giải mã có thể tương tác nội bộ với nhau.

Một cách tùy ý, khi tin nhắn yêu cầu nhận dạng lâu dài thu được còn mang thông tin định tuyến thứ hai, thực thể chức năng bảo mật thứ nhất có thể xác định, dựa vào thông tin định tuyến thứ hai, thực thể chức năng được sử dụng để giải mã thông

tin nhận dạng thứ nhất. Ví dụ, thông tin định tuyến thứ hai có thể chỉ báo thực thể chức năng bảo mật thứ nhất. Trong trường hợp này, thực thể chức năng bảo mật thứ nhất giải mã thông tin nhận dạng thứ nhất. Theo cách khác, thông tin định tuyến thứ hai có thể chỉ báo thực thể ARPF. Sau đó, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ nhất đến thực thể ARPF, và thực thể ARPF giải mã thông tin nhận dạng thứ nhất.

Một cách tùy ý, khi tin nhắn yêu cầu nhận dạng lâu dài còn mang thông tin ký hiệu nhận dạng, thực thể chức năng bảo mật thứ nhất có thể phân tách thông tin ký hiệu nhận dạng. Cụ thể là, khi thông tin ký hiệu nhận dạng được mang trong tin nhắn yêu cầu nhận dạng lâu dài là ký hiệu nhận dạng thứ nhất, thực thể chức năng bảo mật thứ nhất có thể xác định, dựa vào ký hiệu nhận dạng thứ nhất, thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không. Khi thông tin nhận dạng thứ nhất là thông tin nhận dạng được mã hóa, thực thể chức năng bảo mật thứ nhất có thể thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất nhờ sử dụng phương pháp nêu trên.

Khi thông tin ký hiệu nhận dạng được mang trong tin nhắn yêu cầu nhận dạng lâu dài là ký hiệu nhận dạng thứ hai, thực thể chức năng bảo mật thứ nhất có thể xác định cách thức mã hóa của thông tin nhận dạng thứ nhất dựa vào ký hiệu nhận dạng thứ hai, để giải mã thông tin nhận dạng thứ nhất dựa vào cách thức mã hóa nhờ sử dụng khóa cá nhân được lưu trữ. Theo cách khác, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai đến thiết bị mạng thứ hai, và thiết bị mạng thứ hai xác định cách thức mã hóa của thông tin nhận dạng thứ nhất dựa vào ký hiệu nhận dạng thứ hai và giải mã thông tin nhận dạng thứ nhất dựa vào cách thức mã hóa nhờ sử dụng khóa cá nhân được lưu trữ. Theo cách khác, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai đến thiết bị mạng thứ ba nhờ sử dụng thiết bị mạng thứ hai, và thiết bị mạng thứ ba xác định cách thức mã hóa của thông tin nhận dạng thứ nhất dựa vào ký hiệu nhận dạng thứ hai và giải mã thông tin nhận dạng thứ nhất dựa vào cách thức mã hóa.

Khi thông tin ký hiệu nhận dạng được mang trong tin nhắn yêu cầu nhận dạng lâu dài là ký hiệu nhận dạng thứ ba, thực thể chức năng bảo mật thứ nhất có thể xử

lý ký hiệu nhận dạng thứ ba dựa vào các cách thức nêu trên về việc xử lý ký hiệu nhận dạng thứ nhất và ký hiệu nhận dạng thứ hai, và các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Bước 304. Thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất khi thu tin nhắn đáp lại nhận dạng lâu dài, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ hai.

Sau khi thu tin nhắn đáp lại nhận dạng lâu dài được gửi bởi thực thể chức năng bảo mật thứ nhất, thiết bị mạng thứ nhất có thể lưu trữ thông tin nhận dạng thứ hai để sử dụng sau đó khi thiết bị đầu cuối được đăng ký lại hoặc yêu cầu dịch vụ. Ngoài ra, thiết bị mạng thứ nhất có thể gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, để kích hoạt quy trình xác thực cho thiết bị đầu cuối. Tin nhắn thứ hai mang thông tin nhận dạng thứ hai, sao cho thực thể chức năng bảo mật thứ nhất yêu cầu vectơ xác thực dựa vào thông tin nhận dạng thứ hai, để thực hiện việc xác thực cho thiết bị đầu cuối. Ngoài ra, tin nhắn thứ hai có thể là tin nhắn yêu cầu khởi tạo xác thực, hoặc có thể là tin nhắn giao thức xác thực có thể mở rộng/yêu cầu nhận dạng (Extensible Authentication Protocol/identity-request, viết tắt là EAP-AKA'/identity-request).

Theo phương án này của sáng chế, khi thiết bị đầu cuối truy cập mạng, thiết bị đầu cuối có thể gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất, và bổ sung thông tin nhận dạng được mã hóa, cụ thể là, thông tin nhận dạng thứ nhất, vào tin nhắn thứ nhất. Khi thu thông tin nhận dạng thứ nhất từ thiết bị đầu cuối, thiết bị mạng thứ nhất có thể trước tiên thu nhận thông tin nhận dạng được mã hóa, cụ thể là, thông tin nhận dạng thứ hai, của thông tin nhận dạng thứ nhất từ thực thể chức năng bảo mật thứ nhất. Sau khi thu nhận thông tin nhận dạng thứ hai, thiết bị mạng thứ nhất có thể gửi, đến thực thể chức năng bảo mật thứ nhất, tin nhắn thứ hai được sử dụng để kích hoạt quy trình xác thực. Nói cách khác, phương án này của sáng chế đề xuất quy trình thực hiện cụ thể của việc kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất là thông tin nhận dạng được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo

mật của thiết bị đầu cuối được đảm bảo. Ngoài ra, trong quá trình thực hiện sáng chế, thiết bị đầu cuối có thể bổ sung thông tin ký hiệu nhận dạng vào tin nhắn thứ nhất, để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất, sao cho thiết bị đầu cuối có thể mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài một cách linh hoạt hơn. Ngoài ra, khi thông tin ký hiệu nhận dạng là ký hiệu nhận dạng thứ hai hoặc ký hiệu nhận dạng thứ ba, thực thể chức năng được sử dụng để giải mã thông tin nhận dạng thứ nhất có thể giải mã thông tin nhận dạng thứ nhất nhanh hơn và thuận tiện hơn.

Phương án nêu trên mô tả quy trình trong đó thiết bị mạng thứ nhất gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất, để yêu cầu thông tin nhận dạng thứ hai, và sau khi thu thông tin nhận dạng thứ hai, gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, để kích hoạt quy trình xác thực. Phần sau đây mô tả phương pháp khác trong đó thiết bị mạng thứ nhất kích hoạt quy trình xác thực cho thiết bị đầu cuối sau khi thu nhận thông tin nhận dạng thứ hai tương ứng với thông tin nhận dạng thứ nhất.

Fig.4 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng khác nữa theo phương án của sáng chế. Như được thể hiện trên Fig.4, phương pháp bao gồm các bước sau đây.

Bước 401. Thiết bị đầu cuối gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất qua trạm gốc, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng, và thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối nhờ sử dụng khóa công khai.

Đối với quá trình thực hiện của bước này, dựa vào bước 301. Các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Bước 402. Thiết bị mạng thứ nhất gửi tin nhắn yêu cầu nhận dạng lâu dài đến thiết bị mạng thứ hai khi thu tin nhắn thứ nhất, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất, và thông tin ký hiệu nhận dạng được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận

dạng thứ nhất.

Sau khi thu tin nhắn thứ nhất, thiết bị mạng thứ nhất có thể yêu cầu thông tin nhận dạng thứ hai từ thiết bị mạng thứ hai dựa vào thông tin nhận dạng thứ nhất được mang trong tin nhắn thứ nhất. Thông tin nhận dạng thứ hai là thông tin nhận dạng được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất.

Thiết bị mạng thứ hai có thể là bất kỳ một trong số thực thể ARPF, thực thể UDM, thực thể IDF, hoặc AuC.

Bước 403. Thiết bị mạng thứ hai gửi tin nhắn đáp lại nhận dạng lâu dài đến thiết bị mạng thứ nhất, trong đó tin nhắn đáp lại nhận dạng lâu dài mang thông tin nhận dạng thứ hai.

Sau khi thu tin nhắn yêu cầu nhận dạng lâu dài, thiết bị mạng thứ hai có thể thu nhận thông tin nhận dạng thứ hai và gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất.

Thiết bị mạng thứ hai có thể thu nhận thông tin nhận dạng thứ hai nhờ sử dụng hai cách thức sau đây:

(1) Khi thiết bị mạng thứ hai lưu trữ khóa cá nhân, thiết bị mạng thứ hai giải mã, dựa vào khóa cá nhân được lưu trữ, thông tin nhận dạng thứ nhất được mang trong tin nhắn yêu cầu nhận dạng lâu dài, để thu nhận thông tin nhận dạng thứ hai.

Một cách tùy ý, tin nhắn yêu cầu nhận dạng lâu dài có thể mang thông tin định tuyến thứ nhất. Khi thiết bị mạng thứ hai là thiết bị mạng lưu trữ các khóa cá nhân của các mạng điều hành khác nhau, thiết bị mạng thứ hai có thể thu nhận khóa cá nhân của mạng gia đình của thiết bị đầu cuối dựa vào thông tin định tuyến thứ nhất và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân thu nhận được.

(2) Khi thiết bị mạng thứ hai không lưu trữ khóa cá nhân, thiết bị mạng thứ hai chuyển thông tin nhận dạng thứ nhất đến thiết bị mạng thứ ba, và thiết bị mạng thứ ba giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai, và gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ hai.

Bước 404. Thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất khi thu tin nhắn đáp lại nhận dạng lâu dài, trong đó tin nhắn thứ hai được sử dụng để kích hoạt quy trình xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ hai.

Đối với bước này, dựa vào bước 305 theo phương án nêu trên. Các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Theo phương án này của sáng chế, khi thiết bị đầu cuối truy cập mạng, thiết bị đầu cuối có thể gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất, và bổ sung thông tin nhận dạng được mã hóa, cụ thể là, thông tin nhận dạng thứ nhất, đến tin nhắn thứ nhất. Khi thu thông tin nhận dạng thứ nhất từ thiết bị đầu cuối, thiết bị mạng thứ nhất có thể trước tiên thu nhận thông tin nhận dạng được mã hóa, cụ thể là, thông tin nhận dạng thứ hai, của thông tin nhận dạng thứ nhất nhờ sử dụng thiết bị mạng thứ hai. Sau khi thu nhận thông tin nhận dạng thứ hai, thiết bị mạng thứ nhất gửi, đến thực thể chức năng bảo mật thứ nhất, tin nhắn thứ hai được sử dụng để kích hoạt quy trình xác thực. Nói cách khác, phương án này của sáng chế đề xuất quy trình thực hiện cụ thể của việc kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất là thông tin nhận dạng được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối được đảm bảo. Ngoài ra, theo phương án này của sáng chế, thiết bị mạng thứ nhất có thể yêu cầu trực tiếp thông tin nhận dạng thứ hai từ thiết bị mạng thứ hai. Theo cách này, so với trường hợp trong đó thiết bị mạng thứ nhất yêu cầu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, và thực thể chức năng bảo mật thứ nhất yêu cầu thông tin nhận dạng thứ hai từ thiết bị mạng thứ hai vì thực thể chức năng bảo mật thứ nhất không lưu trữ khóa giải mã cá nhân, phương pháp này làm giảm việc truyền tín hiệu được trao đổi.

Phương án nêu trên mô tả quy trình trong đó thiết bị mạng thứ nhất gửi tin nhắn yêu cầu nhận dạng lâu dài đến thiết bị mạng thứ hai để yêu cầu thông tin nhận dạng thứ hai, và gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất sau khi thu thông tin nhận dạng thứ hai, để kích hoạt quy trình xác thực. Phần sau đây mô tả phương pháp khác trong đó thiết bị mạng thứ nhất kích hoạt quy trình xác thực cho thiết bị đầu cuối sau khi thu nhận thông tin nhận dạng thứ hai tương ứng với thông tin nhận dạng thứ nhất.

Fig.5 là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng khác nữa theo phương án của sáng chế. Như được thể hiện trên Fig.5, phương pháp

bao gồm các bước sau đây.

Bước 501. Thiết bị đầu cuối gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất qua trạm gốc, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, và thông tin ký hiệu nhận dạng được sử dụng để nhận dạng thông tin nhận dạng thứ nhất có phải là thông tin nhận dạng được mã hóa hay không và/hoặc nhận dạng cách thức mã hóa của thông tin nhận dạng thứ nhất.

Đối với quá trình thực hiện của bước này, dựa vào bước 301. Các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Bước 502. Thiết bị mạng thứ nhất gửi tin nhắn yêu cầu nhận dạng đến thiết bị mạng thứ hai khi thu tin nhắn thứ nhất, trong đó tin nhắn yêu cầu nhận dạng mang thông tin nhận dạng thứ nhất và thông tin định tuyến thứ nhất.

Thông tin định tuyến thứ nhất có thể được sử dụng bởi thiết bị mạng thứ nhất để xác định mạng gia đình của thiết bị đầu cuối.

Sau khi thu tin nhắn thứ nhất, thiết bị mạng thứ nhất có thể xác định mạng gia đình của thiết bị đầu cuối dựa vào thông tin định tuyến thứ nhất, và gửi tin nhắn yêu cầu nhận dạng mang thông tin định tuyến thứ nhất và thông tin nhận dạng thứ nhất đến thiết bị mạng thứ hai được tạo cấu hình trước. Thiết bị mạng thứ hai có thể là thiết bị mạng trong mạng gia đình của thiết bị đầu cuối, hoặc có thể là thiết bị mạng lưu trữ các khóa cá nhân của các mạng điều hành khác nhau.

Thiết bị mạng thứ hai có thể là bất kỳ một trong số thực thể ARPF, thực thể UDM, KMS, hoặc AuC.

Một cách tùy ý, tin nhắn yêu cầu nhận dạng có thể mang thông tin ký hiệu nhận dạng. Đối với phương pháp xử lý cụ thể, dựa vào sự mô tả và giải thích ở bước 302.

Bước 503. Thiết bị mạng thứ hai thu nhận khóa cá nhân dựa vào thông tin định tuyến được mang trong tin nhắn yêu cầu nhận dạng thu được, và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân thu nhận được, để thu nhận thông tin nhận dạng thứ hai.

Khi thiết bị mạng thứ hai là thiết bị mạng trong mạng gia đình của thiết bị đầu

cuối và lưu trữ khóa cá nhân của mạng gia đình, thiết bị mạng thứ hai có thể thu nhận khóa cá nhân, và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân thu nhận được, để thu nhận thông tin nhận dạng thứ hai.

Khi thiết bị mạng thứ hai là thiết bị mạng lưu trữ các khóa cá nhân của các mạng điều hành khác nhau, thiết bị mạng thứ hai có thể thu nhận khóa cá nhân của mạng gia đình của thiết bị đầu cuối dựa vào thông tin định tuyến thứ nhất được mang trong tin nhắn yêu cầu nhận dạng, và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân thu nhận được, để thu nhận thông tin nhận dạng thứ hai.

Một cách tùy ý, khi thiết bị mạng thứ hai không lưu trữ khóa cá nhân, thiết bị mạng thứ hai có thể xác định thiết bị mạng thứ ba dựa vào thông tin định tuyến thứ nhất, và gửi yêu cầu thu nhận khóa cá nhân đến thiết bị mạng thứ ba, trong đó yêu cầu thu nhận khóa cá nhân có thể mang thông tin định tuyến thứ nhất. Sau đó, thiết bị mạng thứ ba có thể thu nhận khóa cá nhân dựa vào thông tin định tuyến thứ nhất và gửi lại khóa cá nhân thu nhận được đến thiết bị mạng thứ hai, và thiết bị mạng thứ hai giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân. Trong trường hợp này, thiết bị mạng thứ hai có thể còn lưu trữ khóa cá nhân, sao cho khi tin nhắn yêu cầu nhận dạng được gửi bởi thiết bị đầu cuối trong mạng gia đình được thu sau đó, thông tin nhận dạng thứ nhất của thiết bị đầu cuối có thể được mã hóa nhờ sử dụng khóa cá nhân.

Ví dụ, thiết bị mạng thứ hai là thực thể AUSF, và thiết bị mạng thứ ba là thực thể ARPF, AuC, hoặc thực thể IDF. Theo cách khác, thiết bị mạng thứ hai là thực thể ARPF, và thiết bị mạng thứ ba là thực thể chức năng chẳng hạn như AuC hoặc thực thể IDF trong ARPF.

Một cách tùy ý, khi tin nhắn yêu cầu nhận dạng còn mang thông tin ký hiệu nhận dạng, thiết bị mạng thứ hai có thể tham khảo phương pháp liên quan trong đó thực thể chức năng bảo mật thứ nhất xử lý thông tin ký hiệu nhận dạng ở bước 303 theo phương án nêu trên, và các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Bước 504. Thiết bị mạng thứ hai gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất.

Bước 505. Thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng

bảo mật thứ nhất, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ hai.

Đối với quá trình thực hiện của bước này, dựa vào bước 301 theo phương án nêu trên. Các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Theo phương án này của sáng chế, khi thiết bị đầu cuối truy cập mạng, thiết bị đầu cuối có thể gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất, và bổ sung thông tin nhận dạng được mã hóa, cụ thể là, thông tin nhận dạng thứ nhất, vào tin nhắn thứ nhất. Khi thu thông tin nhận dạng thứ nhất từ thiết bị đầu cuối, thiết bị mạng thứ nhất có thể trước tiên thu nhận trực tiếp khóa giải mã cá nhân từ thiết bị mạng thứ hai và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa giải mã cá nhân thu nhận được, để thu nhận thông tin nhận dạng thứ hai. Sau khi thu nhận thông tin nhận dạng thứ hai, thiết bị mạng thứ nhất gửi, đến thực thể chức năng bảo mật thứ nhất, tin nhắn thứ hai được sử dụng để kích hoạt quy trình xác thực. Nói cách khác, phương án này của sáng chế đề xuất quy trình thực hiện cụ thể của việc kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất là thông tin nhận dạng được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối được đảm bảo. Ngoài ra, theo phương án này của sáng chế, thiết bị mạng thứ nhất có thể lưu trữ khóa giải mã cá nhân thu nhận được. Theo cách này, khi thiết bị mạng thứ nhất thu thông tin nhận dạng được mã hóa của thiết bị đầu cuối trong cùng mạng điều hành của thiết bị đầu cuối hiện thời, thông tin nhận dạng được mã hóa có thể được mã hóa trực tiếp nhờ sử dụng khóa giải mã cá nhân, nhờ đó đơn giản hóa quá trình thao tác.

Phương án nêu trên mô tả quy trình thực hiện trong đó thiết bị mạng thứ nhất kích hoạt quy trình xác thực cho thiết bị đầu cuối sau khi thu nhận thông tin nhận dạng thứ hai tương ứng với thông tin nhận dạng thứ nhất. Phần sau đây mô tả, dựa vào các hình vẽ từ Fig.6a đến Fig.6d, quy trình thực hiện trong đó thiết bị mạng thứ nhất thu nhận thông tin nhận dạng thứ hai sau khi kích hoạt quy trình xác thực.

Phương án của sáng chế đề xuất sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng. Phương pháp bao gồm các bước sau đây.

Bước 601. Thiết bị đầu cuối gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất qua trạm gốc, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất, và thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối nhờ sử dụng khóa công khai.

Đối với quá trình thực hiện của bước này, dựa vào bước 301. Các sự thể hiện chi tiết không được mô tả lại theo phương án này của sáng chế.

Bước 602. Thiết bị mạng thứ nhất gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất khi thu tin nhắn thứ nhất, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ nhất.

Thiết bị mạng thứ nhất có thể gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất khi thiết bị mạng thứ nhất thu thông tin nhận dạng thứ nhất mà không thu nhận thông tin nhận dạng thứ hai, để kích hoạt quy trình xác thực cho thiết bị đầu cuối.

Bước 603. Thực thể chức năng bảo mật thứ nhất thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất khi thu tin nhắn thứ hai.

Theo phương án này, nếu thực thể chức năng bảo mật thứ nhất là thực thể AUSF, và thiết bị mạng thứ nhất là thực thể chức năng kết hợp AMF và SEAF, không cần phải xác định việc AMF gửi tin nhắn thứ nhất hoặc SEAF gửi tin nhắn thứ nhất. Nếu SEAF là thực thể chức năng độc lập, thiết bị mạng thứ nhất là thực thể SEAF. Trước khi gửi tin nhắn thứ hai, thực thể SEAF cần phải thu thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng trong tin nhắn thứ nhất được gửi bởi thực thể AMF. Nếu thực thể chức năng bảo mật thứ nhất là thực thể SEAF được triển khai độc lập, thực thể SEAF được triển khai trong mạng gia đình của thiết bị đầu cuối.

Sau khi thu thông tin nhận dạng thứ nhất, thực thể chức năng bảo mật thứ nhất có thể thu nhận thông tin nhận dạng thứ hai nhờ sử dụng bất kỳ một trong số ba cách thức sau đây.

(1) Thực thể chức năng bảo mật thứ nhất giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân được lưu trữ, để thu nhận thông tin nhận dạng thứ hai.

(2) Thực thể chức năng bảo mật thứ nhất có thể chuyển thông tin nhận dạng thứ

nhất thu được đến thiết bị mạng thứ hai, và thiết bị mạng thứ hai giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai. Sau đó, thiết bị mạng thứ hai gửi lại thông tin nhận dạng thứ hai thu nhận được đến thực thể chức năng bảo mật thứ nhất. Thiết bị mạng thứ hai lưu trữ khóa cá nhân, hoặc thiết bị mạng thứ hai có thể thu nhận khóa cá nhân từ thiết bị mạng thứ ba dựa vào thông tin định tuyến. Cụ thể là, thiết bị mạng thứ hai có thể là bất kỳ một trong số thực thể ARPF, thực thể UDM, KMS, hoặc AuC.

(3) Thực thể chức năng bảo mật thứ nhất có thể chuyển thông tin nhận dạng thứ nhất thu được đến thiết bị mạng thứ hai. Khi thiết bị mạng thứ hai không thể tìm thấy khóa cá nhân, thiết bị mạng thứ hai có thể gửi yêu cầu đến thiết bị mạng thứ ba, và thiết bị mạng thứ ba giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai. Sau đó thiết bị mạng thứ ba truyền thông tin nhận dạng thứ hai đến thực thể chức năng bảo mật thứ nhất nhờ sử dụng thiết bị mạng thứ hai. Thiết bị mạng thứ ba lưu trữ khóa cá nhân.

Sau khi thu nhận thông tin nhận dạng thứ hai, thực thể chức năng bảo mật thứ nhất có thể xác định phương pháp xác thực. Phương pháp xác thực bao gồm phương pháp xác thực dựa vào giao thức xác thực có thể mở rộng (Extensible Authentication Protocol, viết tắt là EAP) và phương pháp xác thực được nâng cấp của hệ thống gói được cải tiến (evolved packet system, viết tắt là EPS).

Bước 604. Thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thực thể chức năng bảo mật thứ hai.

Một cách tùy ý, nếu ở bước 603, thực thể chức năng bảo mật thứ nhất thu nhận thông tin nhận dạng thứ hai sau khi thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ hai và thực thể chức năng bảo mật thứ hai giải mã thông tin nhận dạng thứ nhất dựa vào khóa cá nhân được lưu trữ, bước này có thể không thể được thực hiện, và bước 605 được thực hiện trực tiếp.

Bước 605. Thực thể chức năng bảo mật thứ hai thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai.

Bước 606. Thực thể chức năng bảo mật thứ hai gửi vectơ xác thực đến thực thể chức năng bảo mật thứ nhất.

Sau khi thu vectơ xác thực, thực thể chức năng bảo mật thứ nhất thực hiện các thao tác khác nhau dựa vào các phương pháp xác thực khác nhau được lựa chọn ở bước 603. Khi thực thể chức năng bảo mật thứ nhất thực hiện việc xác thực nhờ sử dụng phương pháp xác thực EAP, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất nhờ sử dụng hai phương pháp, như được thể hiện trên Fig.6a và Fig.6b. Khi thực thể chức năng bảo mật thứ nhất sử dụng phương pháp xác thực EPS, thực thể chức năng bảo mật thứ nhất có thể cũng gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất nhờ sử dụng hai phương pháp, như được thể hiện trên Fig.6c và Fig.6d.

Như được thể hiện trên Fig.6a, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất trong quy trình xác thực. Đối với quy trình xác thực cụ thể, dựa vào bước 607.

Bước 607. Thực thể chức năng bảo mật thứ nhất gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất khi thu vectơ xác thực, trong đó tin nhắn thứ ba mang thông tin nhận dạng thứ hai.

Khi thu vectơ xác thực, thực thể chức năng bảo mật thứ nhất có thể bắt đầu thực hiện việc xác thực cho thiết bị đầu cuối. Tin nhắn thứ ba có thể mang tin nhắn phản hồi xác thực và thông tin nhận dạng thứ hai, và tin nhắn phản hồi xác thực mang vectơ xác thực hoặc một phần của vectơ xác thực. Theo cách khác, tin nhắn thứ ba mang tin nhắn phản hồi xác thực, tin nhắn phản hồi xác thực mang thông tin nhận dạng thứ hai, và tin nhắn phản hồi xác thực mang vectơ xác thực hoặc một phần của vectơ xác thực.

Một cách tùy ý, tin nhắn phản hồi xác thực là tin nhắn yêu cầu xác thực người dùng, hoặc tin nhắn yêu cầu EAP (thử thách AKA'), hoặc tin nhắn 5G-AIA (câu trả lời khởi tạo xác thực-authentication initiation answer).

Cần hiểu rằng khi quy trình xác thực được kích hoạt theo cách thức được mô tả ở các bước từ 601 đến 607, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai trong khi gửi tin nhắn phản hồi xác thực đến thiết bị mạng thứ nhất. Theo cách này, thiết bị mạng thứ nhất có thể thu nhận thông tin nhận dạng thứ hai trong quy trình xác thực, và phương pháp này làm giảm việc truyền tín hiệu được trao đổi khi so với trường hợp trong đó thiết bị mạng thứ nhất thu nhận thông

tin nhận dạng thứ hai trước khi kích hoạt quy trình xác thực.

Như được thể hiện trên Fig.6b, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất sau khi xác định rằng việc xác thực cho thiết bị đầu cuối thành công. Đối với quy trình cụ thể, dựa vào các bước 608 và 609.

Bước 608. Thực thể chức năng bảo mật thứ nhất thực hiện việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực khi thu vectơ xác thực.

Cụ thể là, thực thể chức năng bảo mật thứ nhất có thể tương tác với thiết bị đầu cuối nhờ sử dụng vectơ xác thực, để thực hiện việc xác thực cho thiết bị đầu cuối.

Bước 609. Thực thể chức năng bảo mật thứ nhất gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất sau khi việc xác thực cho thiết bị đầu cuối thành công, trong đó tin nhắn thứ ba mang thông tin nhận dạng thứ hai.

Cụ thể là, việc xác thực thành công cho thiết bị đầu cuối bởi thực thể chức năng bảo mật thứ nhất có thể được chỉ báo trong các trường hợp sau: thực thể chức năng bảo mật thứ nhất gửi hoặc thu tin nhắn thành công EAP, hoặc kiểm chứng thành công thiết bị đầu cuối, hoặc thu tin nhắn 5G-AC (xác nhận xác thực).

Sau khi xác định rằng việc xác thực cho thiết bị đầu cuối thành công, thực thể chức năng bảo mật thứ nhất có thể gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất. Tin nhắn thứ ba mang tin nhắn thành công xác thực được sử dụng để thông báo cho thiết bị mạng thứ nhất rằng việc xác thực cho thiết bị đầu cuối thành công. Thông tin nhận dạng thứ hai được mang trong tin nhắn thành công xác thực.

Tất nhiên là, thông tin nhận dạng thứ hai có thể không được mang trong tin nhắn thành công xác thực. Nói cách khác, tin nhắn thứ ba có thể mang tin nhắn thành công xác thực và thông tin nhận dạng thứ hai.

Cụ thể là, tin nhắn thành công xác thực có thể là tin nhắn thành công EAP, hoặc tin nhắn 5G-AK (báo nhận xác thực). Tin nhắn 5G-AK là tin nhắn phản hồi được sử dụng để đáp lại tin nhắn 5G-AC.

Cần hiểu rằng khi quy trình xác thực được kích hoạt nhờ sử dụng phương pháp được mô tả ở các bước 601 đến 606 và các bước 608 và 609, khi thu thông tin nhận dạng thứ nhất, thiết bị mạng thứ nhất có thể kích hoạt trực tiếp quy trình xác thực. Thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai trong

khi gửi tin nhắn thành công xác thực đến thiết bị mạng thứ nhất sau khi việc xác thực thành công. Theo cách này, quy trình trong đó thiết bị mạng thứ nhất thu nhận thông tin nhận dạng thứ hai được kết thúc cùng với việc xác thực, sao cho việc truyền tín hiệu được trao đổi được làm giảm. Ngoài ra, vì thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai và tin nhắn thành công xác thực cùng với thiết bị mạng thứ nhất sau khi việc xác thực thành công, thông tin nhận dạng của thiết bị đầu cuối có thể được bảo vệ không bị rò rỉ một cách tốt hơn, và tính bảo mật của thiết bị đầu cuối được nâng cao.

Phần trên đây mô tả, dựa vào Fig.6a và Fig.6b, hai phương pháp gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi thực thể chức năng bảo mật thứ nhất thực hiện việc xác thực nhờ sử dụng phương pháp xác thực EAP. Phần sau đây mô tả hai phương pháp gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi thực thể chức năng bảo mật thứ nhất sử dụng phương pháp xác thực EPS. Khi phương pháp xác thực EPS được sử dụng, thực thể chức năng bảo mật thứ nhất cần phải gửi vectơ xác thực đến thiết bị mạng thứ nhất, và thiết bị mạng thứ nhất thực hiện việc xác thực cho thiết bị đầu cuối.

Như được thể hiện trên Fig.6c, thực thể chức năng bảo mật thứ nhất có thể gửi vectơ xác thực và thông tin nhận dạng thứ hai cùng với thiết bị mạng thứ nhất. Đối với quy trình cụ thể, dựa vào bước 610.

Bước 610. Thực thể chức năng bảo mật thứ nhất gửi vectơ xác thực và thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi thu vectơ xác thực.

Một cách tùy ý, thực thể chức năng bảo mật thứ nhất có thể gửi vectơ xác thực và thông tin nhận dạng thứ hai dưới định dạng cố định. Ví dụ, thông tin nhận dạng thứ hai được đặt trong một vài bit đầu tiên của tin nhắn thứ ba, và số lượng của các bit lớn hơn hoặc bằng với độ dài của thông tin nhận dạng thứ hai. Vectơ xác thực được đặt sau các bit dùng cho thông tin nhận dạng thứ hai. Theo cách khác, vectơ xác thực được đặt trong các bit cố định đầu tiên, và thông tin nhận dạng thứ hai được đặt trong các bit cố định sau cùng.

Bước 611. Khi thu vectơ xác thực và thông tin nhận dạng thứ hai, thiết bị mạng thứ nhất lưu trữ thông tin nhận dạng thứ hai, và thực hiện việc xác thực cho thiết bị

đầu cuối dựa vào vectơ xác thực.

Thiết bị mạng thứ nhất có thể nhận dạng thông tin nhận dạng thứ hai và lưu trữ trực tiếp thông tin nhận dạng thứ hai. Theo cách khác, khi thực thể chức năng bảo mật thứ nhất gửi vectơ xác thực và thông tin nhận dạng thứ hai theo định dạng cố định, thiết bị mạng thứ nhất có thể thu nhận thông tin nhận dạng thứ hai dựa vào các bit cố định theo định dạng cố định, trong đó thông tin trong bit cố định là thông tin nhận dạng thứ hai.

Ngoài ra, vectơ xác thực thường bao gồm các thông số chẳng hạn như phản hồi được mong đợi (expected response, viết tắt là XRES) và mã xác thực tin nhắn (message authentication code, viết tắt là MAC). Khi thiết bị mạng thứ nhất là thực thể chức năng kết hợp SEAF và AMF, sau khi thu vectơ xác thực, thiết bị mạng thứ nhất có thể lưu trữ XRES hoặc MAC trong vectơ xác thực, và gửi các thông số còn lại trong vectơ xác thực đến thiết bị đầu cuối, để tương tác với thiết bị đầu cuối và thực hiện việc xác thực cho thiết bị đầu cuối. Khi thiết bị mạng thứ nhất là SEAF độc lập, sau khi thu vectơ xác thực, thiết bị mạng thứ nhất có thể lưu trữ XRES hoặc MAC trong vectơ xác thực, và gửi thông số còn lại trong vectơ xác thực đến thực thể AMF, và thực thể AMF gửi thông số đến thiết bị đầu cuối.

Cần hiểu rằng khi quy trình xác thực được kích hoạt nhờ sử dụng phương pháp được mô tả ở các bước 601 đến 606 và các bước 610 và 611, khi thu thông tin nhận dạng thứ nhất, thiết bị mạng thứ nhất có thể gửi trực tiếp tin nhắn thứ hai mang thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất, để kích hoạt quy trình xác thực. Sau đó, sau khi thu nhận vectơ xác thực, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai và vectơ xác thực cùng với thiết bị mạng thứ nhất. Theo cách này, thiết bị mạng thứ nhất có thể thu nhận thông tin nhận dạng lâu dài của thiết bị đầu cuối trước khi thực hiện việc xác thực cho thiết bị đầu cuối, và phương pháp này làm giảm việc truyền tín hiệu được trao đổi khi so với trường hợp trong đó thiết bị mạng thứ nhất thu nhận thông tin nhận dạng thứ hai trước khi kích hoạt quy trình xác thực.

Như được thể hiện trên Fig.6d, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất sau khi xác định rằng việc xác thực cho thiết bị đầu cuối thành công, nhờ đó nâng cao độ bảo mật. Đối với quy

trình cụ thể, dựa vào các bước từ 611 đến 614. Cần hiểu rằng ở các bước từ 611 đến 614, thực thể chức năng bảo mật thứ nhất có thể là thực thể AUSF, và thiết bị mạng thứ nhất tương ứng có thể là thực thể kết hợp AMF và SEAF. Theo cách khác, thực thể chức năng bảo mật thứ nhất có thể là SEAF độc lập, và thiết bị mạng thứ nhất tương ứng là AMF.

Bước 612. Khi thu vectơ xác thực hoặc một phần của vectơ xác thực, thực thể chức năng bảo mật thứ nhất gửi vectơ xác thực hoặc một phần của vectơ xác thực đến thiết bị mạng thứ nhất, để kích hoạt việc xác thực cho thiết bị đầu cuối.

Ví dụ, thực thể chức năng bảo mật thứ nhất có thể gửi tin nhắn thử thách AKA'/yêu cầu EAP đến thiết bị mạng thứ nhất, và tin nhắn thử thách AKA'/yêu cầu EAP mang vectơ xác thực hoặc một phần của vectơ xác thực. Theo cách khác, thực thể chức năng bảo mật thứ nhất gửi tin nhắn 5G-AIA, và tin nhắn 5G-AIA mang vectơ xác thực hoặc một phần của vectơ xác thực.

Bước 613. Thiết bị mạng thứ nhất thực hiện việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực khi thu vectơ xác thực hoặc một phần của vectơ xác thực.

Khi thu vectơ xác thực hoặc một phần của vectơ xác thực, thiết bị mạng thứ nhất có thể gửi vectơ xác thực hoặc một phần của vectơ xác thực đến thiết bị đầu cuối. Sau đó, thiết bị đầu cuối và thiết bị mạng thứ nhất có thể kết thúc việc xác thực nhờ sử dụng vectơ xác thực hoặc một phần của vectơ xác thực.

Cụ thể là, thiết bị mạng thứ nhất có thể bổ sung vectơ xác thực hoặc một phần của vectơ xác thực vào tin nhắn thử thách AKA'/yêu cầu EAP, và gửi tin nhắn thử thách AKA'/yêu cầu EAP đến thiết bị đầu cuối, hoặc có thể bổ sung vectơ xác thực hoặc một phần của vectơ xác thực vào tin nhắn yêu cầu xác thực (authentication request), và gửi tin nhắn yêu cầu xác thực đến thiết bị đầu cuối.

Bước 614. Thiết bị mạng thứ nhất có thể gửi tin nhắn báo nhận xác thực đến thực thể chức năng bảo mật thứ nhất sau khi việc xác thực cho thiết bị đầu cuối thành công.

Tin nhắn báo nhận xác thực được sử dụng để thông báo cho thực thể chức năng bảo mật thứ nhất rằng việc xác thực cho thiết bị đầu cuối thành công. Cụ thể là, tin nhắn báo nhận xác thực có thể là 5G-AC.

Theo cách thực hiện có thể khác, thiết bị mạng thứ nhất có thể gửi tin nhắn báo

nhận xác thực mang tin nhắn phản hồi xác thực đến thực thể chức năng bảo mật thứ nhất, và tin nhắn trả lời xác thực là tin nhắn phản hồi của tin nhắn yêu cầu xác thực. Sau khi thu tin nhắn trả lời xác thực, thực thể chức năng bảo mật thứ nhất có thể xác định rằng, dựa vào tin nhắn trả lời xác thực, việc xác thực cho thiết bị đầu cuối thành công.

Tin nhắn báo nhận xác thực có thể là tin nhắn thử thách AKA'/phản hồi EAP.

Bước 615. Thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi thu tin nhắn báo nhận xác thực được gửi bởi thiết bị mạng thứ nhất.

Khi thu tin nhắn báo nhận xác thực được gửi bởi thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất có thể xác định rằng thiết bị mạng thứ nhất xác thực thành công thiết bị đầu cuối. Trong trường hợp này, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất, nhờ đó nâng cao độ bảo mật.

Một cách tùy ý, khi thu tin nhắn báo nhận xác thực được gửi bởi thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất có thể xác định rằng thiết bị mạng thứ nhất xác thực thành công thiết bị đầu cuối. Trong trường hợp này, thực thể chức năng bảo mật thứ nhất có thể tạo ra tin nhắn thành công xác thực, và gửi tin nhắn thành công xác thực và thông tin nhận dạng thứ hai cùng với thiết bị mạng thứ nhất. Tất nhiên là, thực thể chức năng bảo mật thứ nhất có thể bổ sung thông tin nhận dạng thứ hai đến tin nhắn thành công xác thực và gửi tin nhắn thành công xác thực đến thiết bị mạng thứ nhất. Tin nhắn thành công xác thực có thể là tin nhắn đáp lại nhận dạng lâu dài.

Cần hiểu rằng khi quy trình xác thực được kích hoạt nhờ sử dụng phương pháp được mô tả ở các bước từ 601 đến 606 và các bước từ 612 đến 615, khi thu thông tin nhận dạng thứ nhất, thiết bị mạng thứ nhất có thể gửi trực tiếp tin nhắn thứ hai mang thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất, để kích hoạt quy trình xác thực. Sau đó, sau khi thu nhận thông tin nhận dạng thứ hai và vectơ xác thực, thực thể chức năng bảo mật thứ nhất gửi chỉ vectơ xác thực đến thiết bị mạng thứ nhất, mà không gửi thông tin nhận dạng thứ hai. Sau khi việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực thành công, thiết bị mạng thứ

nhất có thể gửi tin nhắn báo nhận xác thực đến thực thể chức năng bảo mật thứ nhất. Sau khi thu tin nhắn báo nhận xác thực, thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất chỉ khi xác định rằng thiết bị mạng thứ nhất xác thực thành công thiết bị đầu cuối. Theo cách này, thông tin nhận dạng của thiết bị đầu cuối có thể được bảo vệ không bị rò rỉ tốt hơn, và tính bảo mật của thiết bị đầu cuối được nâng cao.

Phương án nêu trên mô tả quy trình thực hiện cụ thể trong đó thiết bị mạng thứ nhất kích hoạt quy trình xác thực cho thiết bị đầu cuối và thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất. Ngoài ra, quy trình xác thực cho thiết bị đầu cuối có thể được kích hoạt bởi thực thể chức năng bảo mật thứ nhất.

Trong kịch bản trong đó thực thể chức năng bảo mật thứ nhất kích hoạt quy trình xác thực cho thiết bị đầu cuối, phương án của sáng chế còn đề xuất phương pháp kích hoạt xác thực mạng, và thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất, thực thể chức năng bảo mật thứ hai, và hệ thống dựa vào phương pháp này. Phương pháp bao gồm các bước: thu, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất từ thiết bị mạng thứ nhất, trong đó thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai; gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ hai; và thu, bởi thực thể chức năng bảo mật thứ nhất, vectơ xác thực và thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ hai, và kích hoạt quy trình xác thực cho thiết bị đầu cuối, trong đó thông tin nhận dạng thứ hai được thu nhận bằng cách giải mã thông tin nhận dạng thứ nhất, và vectơ xác thực được thu nhận bởi thực thể chức năng bảo mật thứ hai dựa vào thông tin nhận dạng thứ hai. Ví dụ, phương pháp có thể như được thể hiện trên Fig.7a. Giải pháp của phương án này của sáng chế đề xuất giải pháp kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Ngoài ra, theo giải pháp của phương án này của sáng chế, thực thể chức năng bảo mật thứ nhất kích hoạt việc xác thực cho thiết bị đầu cuối. Vì quy trình xác thực cho thiết bị đầu cuối cũng được kích hoạt bởi thực thể chức năng bảo mật thứ nhất khi thiết bị đầu cuối truy cập mạng nhờ sử dụng

công nghệ 3GPP, nên việc xử lý đối với công nghệ 3GPP và việc xử lý đối với công nghệ không phải 3GPP trong quy trình xác thực cho thiết bị đầu cuối là thống nhất theo giải pháp của phương án này, nhờ đó làm giảm độ phức tạp xử lý của thiết bị mạng.

Phần sau đây mô tả, chi tiết dựa vào Fig.7b, giải pháp trong đó thực thể chức năng bảo mật thứ nhất kích hoạt quy trình xác thực.

Fig.7b là sơ đồ truyền thông giản lược của phương pháp kích hoạt xác thực mạng khác nữa theo phương án của sáng chế. Như được thể hiện trên Fig.7b, phương pháp bao gồm các bước sau đây.

Bước 701. Thiết bị đầu cuối gửi thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất qua trạm gốc và thiết bị mạng thứ nhất, trong đó thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai.

Khi thiết bị đầu cuối truy cập mạng, thiết bị đầu cuối có thể gửi thông tin nhận dạng thứ nhất đến trạm gốc, và sau đó trạm gốc gửi thông tin nhận dạng thứ nhất đến thiết bị mạng thứ nhất. Khi thu thông tin nhận dạng thứ nhất, thiết bị mạng thứ nhất chuyển thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất. Cần hiểu rằng thiết bị mạng thứ nhất có thể gửi tin nhắn yêu cầu nhận dạng lâu dài đến thực thể chức năng bảo mật thứ nhất, và bổ sung thông tin nhận dạng thứ nhất vào tin nhắn yêu cầu nhận dạng lâu dài.

Khóa công khai có thể được lưu trữ trong thiết bị đầu cuối, hoặc có thể được lưu trữ trong thẻ nằm trong thiết bị đầu cuối và được sử dụng để lưu trữ khóa dài hạn, ví dụ, môđun nhận dạng thuê bao (subscriber identification module, viết tắt là SIM), môđun nhận dạng thuê bao đa năng (universal subscriber identity module, viết tắt là USIM), thẻ mạch tích hợp đa năng (universal integrated circuit card, viết tắt là UICC), thẻ mạch tích hợp đa năng được nhúng (embedded universal integrated circuit card, viết tắt là eUICC), hoặc thẻ mạch tích hợp đa năng 5G (5G–universal integrated circuit card, viết tắt là 5G-UICC). Nhận dạng lâu dài có thể là số nhận dạng thuê bao di động quốc tế (international mobile subscriber identification number, viết tắt là IMSI). Khi nhận dạng lâu dài là IMSI, IMSI bao gồm số nhận dạng thuê bao di động (mobile subscriber identification number, viết tắt là MSIN)

và thông tin định tuyến. Do đó, thiết bị đầu cuối có thể mã hóa MSIN trong IMSI nhờ sử dụng khóa công khai, để thu nhận thông tin nhận dạng thứ nhất.

Ngoài ra, tin nhắn thứ nhất còn mang thông tin định tuyến, và thông tin định tuyến được sử dụng bởi thiết bị mạng thứ nhất để xác định mạng gia đình của thiết bị đầu cuối, sao cho thiết bị mạng thứ nhất xác định thực thể chức năng bảo mật thứ nhất trong mạng gia đình của thiết bị đầu cuối.

Bước 702. Thực thể chức năng bảo mật thứ nhất thu thông tin nhận dạng thứ nhất và gửi thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ hai.

Một cách tùy ý, thực thể chức năng bảo mật thứ nhất có thể là thực thể AUSF.

Bước 703. Thực thể chức năng bảo mật thứ hai thu thông tin nhận dạng thứ nhất, thu nhận thông tin nhận dạng thứ hai, và thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai.

Khi thu thông tin nhận dạng thứ nhất, thực thể chức năng bảo mật thứ hai có thể giải mã thông tin nhận dạng thứ nhất dựa vào khóa cá nhân được lưu trữ, để thu nhận thông tin nhận dạng thứ hai. Theo cách khác, thực thể chức năng bảo mật thứ hai có thể gửi thông tin nhận dạng thứ nhất đến thiết bị mạng thứ hai, và thiết bị mạng thứ hai giải mã thông tin nhận dạng thứ nhất để thu nhận thông tin nhận dạng thứ hai, và gửi thông tin nhận dạng thứ hai đến thực thể chức năng bảo mật thứ hai. Theo cách khác, thực thể chức năng bảo mật thứ hai có thể yêu cầu khóa cá nhân từ thiết bị mạng thứ hai, và thiết bị mạng thứ hai xác định khóa cá nhân dựa vào thông tin định tuyến và gửi khóa cá nhân đến thực thể chức năng bảo mật thứ hai.

Một cách tùy ý, thực thể chức năng bảo mật thứ hai có thể là thực thể ARPF, và thiết bị mạng thứ hai có thể là AuC, KMS, hoặc IDF.

Sau khi thu nhận thông tin nhận dạng thứ hai, thực thể chức năng bảo mật thứ hai có thể xác định khóa dài hạn của thiết bị đầu cuối dựa vào thông tin nhận dạng thứ hai, và thu nhận vectơ xác thực dựa vào khóa dài hạn. Vectơ xác thực là thông số được sử dụng bởi thiết bị mạng thứ nhất để thực hiện việc xác thực cho thiết bị đầu cuối. Khóa dài hạn là giống như khóa dài hạn được lưu trữ trong thiết bị đầu cuối.

Bước 704. Thực thể chức năng bảo mật thứ hai gửi vectơ xác thực và thông tin nhận dạng thứ hai đến thực thể chức năng bảo mật thứ nhất.

Bước 705. Thực thể chức năng bảo mật thứ nhất thu vectơ xác thực và thông tin nhận dạng thứ hai, và kích hoạt quy trình xác thực.

Bước 706. Thực thể chức năng bảo mật thứ nhất gửi vectơ xác thực đến thiết bị mạng thứ nhất.

Một cách tùy ý, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai trong khi gửi vectơ xác thực đến thiết bị mạng thứ nhất, nói cách khác, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ hai và vectơ xác thực đến thiết bị mạng thứ nhất ở cùng thời điểm. Trong trường hợp này, bước 707 có thể được thực hiện mà không cần thực hiện bước 708 và bước 709.

Bước 707. Thiết bị mạng thứ nhất thực hiện việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực.

Vectơ xác thực thường bao gồm các thông số chẳng hạn như phản hồi được mong đợi (expected response, viết tắt là XRES) và mã xác thực tin nhắn (message authentication code, viết tắt là MAC). Sau khi thu vectơ xác thực, thiết bị mạng thứ nhất có thể lưu trữ XRES hoặc MAC trong vectơ xác thực, và gửi các thông số còn lại trong vectơ xác thực đến thiết bị đầu cuối, để thực hiện việc xác thực cho thiết bị đầu cuối bằng cách tương tác với thiết bị đầu cuối.

Cần hiểu rằng khi thiết bị mạng thứ nhất còn thu thông tin nhận dạng thứ hai trong khi thu vectơ xác thực, thiết bị mạng thứ nhất có thể thực hiện việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực và lưu trữ thông tin nhận dạng thứ hai thu được. Trong trường hợp này, bước 708 và bước 709 có thể không được thực hiện sau đó.

Bước 708. Thiết bị mạng thứ nhất gửi tin nhắn báo nhận xác thực đến thực thể chức năng bảo mật thứ nhất sau khi việc xác thực cho thiết bị đầu cuối thành công.

Tin nhắn báo nhận xác thực được sử dụng để thông báo cho AUSF rằng việc xác thực cho thiết bị đầu cuối thành công.

Bước 709. Thực thể chức năng bảo mật thứ nhất gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi thu tin nhắn báo nhận xác thực.

Vì khi thu tin nhắn báo nhận xác thực, thực thể chức năng bảo mật thứ nhất có thể xác định rằng việc xác thực cho thiết bị đầu cuối thành công, nếu thông tin nhận dạng thứ hai được gửi đến thiết bị mạng thứ nhất ở thời điểm này, sự nhận dạng lâu

dài của thiết bị đầu cuối có thể được bảo vệ không bị rò rỉ tốt hơn, và tính bảo mật được đảm bảo.

Theo phương án này của sáng chế, khi truy cập mạng, thiết bị đầu cuối có thể gửi thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ nhất nhờ sử dụng trạm gốc và thiết bị mạng thứ nhất. Khi thu thông tin nhận dạng thứ nhất từ thiết bị đầu cuối, thực thể chức năng bảo mật thứ nhất có thể gửi thông tin nhận dạng thứ nhất đến thực thể chức năng bảo mật thứ hai, và thực thể chức năng bảo mật thứ hai có thể thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất, thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai, và sau đó gửi vectơ xác thực và thông tin nhận dạng thứ hai đến thực thể chức năng bảo mật thứ nhất. Khi thu vectơ xác thực và thông tin nhận dạng thứ hai, thực thể chức năng bảo mật thứ nhất kích hoạt quy trình xác thực. Nói cách khác, phương án này của sáng chế đề xuất quy trình thực hiện cụ thể của việc kích hoạt quy trình xác thực khi thông tin nhận dạng được mã hóa. Vì thông tin nhận dạng được gửi bởi thiết bị đầu cuối đến thiết bị mạng thứ nhất là thông tin nhận dạng được mã hóa, thông tin nhận dạng được ngăn ngừa không bị chặn hoặc bị giả mạo trong quá trình truyền, và tính bảo mật của thiết bị đầu cuối được đảm bảo. Ngoài ra, theo phương án này của sáng chế, quy trình xác thực được kích hoạt bởi thực thể chức năng bảo mật thứ nhất khi thực thể chức năng bảo mật thứ nhất thu vectơ xác thực. Trong công nghệ liên quan, khi thiết bị đầu cuối truy cập mạng nhờ sử dụng công nghệ 3GPP, quy trình xác thực cho thiết bị đầu cuối được kích hoạt bởi thực thể chức năng bảo mật thứ nhất. Phương pháp được đề xuất theo phương án này của sáng chế có thể không chỉ được ứng dụng cho công nghệ 3GPP, mà còn được ứng dụng cho công nghệ không phải 3GPP. Theo phương án này của sáng chế, khi thiết bị đầu cuối truy cập mạng nhờ sử dụng công nghệ không phải 3GPP, quy trình xác thực cho thiết bị đầu cuối cũng được kích hoạt bởi thực thể chức năng bảo mật thứ nhất. Nói cách khác, theo phương án này của sáng chế, việc xử lý đối với công nghệ 3GPP và việc xử lý đối với công nghệ không phải 3GPP là thống nhất. Theo cách này, độ phức tạp xử lý của thiết bị mạng có thể được làm giảm.

Phần nêu trên chủ yếu mô tả, từ quan điểm về sự tương tác giữa các thiết bị mạng khác nhau, các giải pháp được đề xuất theo các phương án của sáng chế. Có

thể hiểu rằng để thực hiện các chức năng nêu trên, thiết bị mạng thứ nhất và thực thể chức năng bảo mật thứ nhất đều bao gồm cấu trúc phần cứng tương ứng và/hoặc môđun phần mềm được sử dụng để thực hiện các chức năng. Dựa vào các ví dụ được mô tả theo các phương án được bộc lộ trong sáng chế, các bộ phận và các bước thuật toán có thể được thực hiện bởi phần cứng hoặc sự kết hợp của phần cứng và phần mềm máy tính theo các phương án của sáng chế. Việc chức năng được thực hiện bởi phần cứng hoặc bởi phần mềm máy tính điều khiển phần cứng phụ thuộc vào ứng dụng cụ thể và điều kiện hạn chế thiết kế của giải pháp kỹ thuật. Đối với mỗi ứng dụng cụ thể, 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, nhưng không nên được xem là cách thực hiện vượt quá phạm vi của các giải pháp kỹ thuật theo các phương án của sáng chế.

Theo các phương án của sáng chế, việc phân chia môđun chức năng có thể được thực hiện trên thiết bị mạng thứ nhất và thực thể chức năng bảo mật thứ nhất dựa vào các ví dụ về phương pháp. Ví dụ, mỗi môđun chức năng có thể được thu nhận qua sự phân chia dựa vào chức năng tương ứng, hoặc hai hoặc nhiều hơn hai chức năng có thể được tích hợp vào một môđun xử lý. Môđun được tích hợp có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng môđun chức năng của phần mềm. Cần hiểu rằng sự phân chia môđun theo các phương án của sáng chế là ví dụ và chỉ đơn thuần là phân chia chức năng lôgic. Trong quá trình thực hiện cụ thể, có thể có cách thức phân chia khác.

Khi môđun được tích hợp được sử dụng, Fig.8a là sơ đồ khối giản lược có thể của thiết bị mạng thứ nhất theo phương án của sáng chế. Thiết bị mạng thứ nhất 800 bao gồm môđun xử lý 802 và môđun truyền thông 803. Môđun xử lý 802 được tạo cấu hình để điều khiển và quản lý các hoạt động của thiết bị mạng thứ nhất. Ví dụ, môđun xử lý 802 được tạo cấu hình để hỗ trợ thiết bị mạng thứ nhất trong việc thực hiện các quy trình 201 và 202 trên Fig.2, các quy trình 302 và 304 trên Fig.3, các quy trình 402 và 404 trên Fig.4, các quy trình 502 và 505 trên Fig.5, các quy trình 602, 611, 613, và 614 trên Fig.6a đến Fig.6d, các quy trình 711 đến 714 trên Fig.7a, các quy trình 707 và 708 trên Fig.7b, và/hoặc các quy trình khác sử dụng công nghệ được mô tả trong bản mô tả này. Môđun truyền thông 803 được tạo cấu

hình để hỗ trợ thiết bị mạng thứ nhất trong việc giao tiếp với thực thể chức năng bảo mật thứ nhất hoặc thiết bị mạng khác. Thiết bị mạng thứ nhất có thể còn bao gồm môđun lưu trữ 801, được tạo cấu hình để lưu trữ dữ liệu và mã chương trình của thiết bị mạng thứ nhất.

Môđun xử lý 802 có thể là bộ xử lý hoặc bộ điều khiển, ví dụ, bộ phận xử lý trung tâm (Central Processing Unit, viết tắt là CPU), bộ xử lý mục đích chung, bộ xử lý tín hiệu số (Digital Signal Processor, viết tắt là DSP), mạch tích hợp ứng dụng dành riêng (Application-Specific Integrated Circuit, viết tắt là ASIC), mảng cổng lập trình được dạng trường (Field Programmable Gate Array, viết tắt là FPGA) hoặc thiết bị lôgic lập trình được khác, thiết bị lôgic tranzito, thành phần phần cứng, hoặc sự kết hợp bất kỳ của nó. Môđun xử lý có thể thực hiện hoặc thực thi các khối lôgic ví dụ khác nhau, các môđun, và các mạch được mô tả dựa vào nội dung được bộc lộ theo sáng chế. Theo cách khác, bộ xử lý có thể là sự kết hợp để thực hiện chức năng tính, ví dụ, sự kết hợp của một hoặc nhiều bộ vi xử lý hoặc sự kết hợp của DSP và bộ vi xử lý. Môđun truyền thông 803 có thể là giao diện truyền thông, bộ thu phát, mạch thu phát, hoặc tương tự. Giao diện truyền thông là tên gọi chung, và trong quá trình thực hiện cụ thể, giao diện truyền thông có thể bao gồm các giao diện, ví dụ, có thể bao gồm giao diện giữa thiết bị mạng thứ nhất và thực thể chức năng bảo mật thứ nhất hoặc giữa thiết bị mạng thứ nhất và thiết bị mạng thứ hai và/hoặc giao diện khác. Môđun lưu trữ 801 có thể là bộ nhớ.

Khi môđun xử lý 802 là bộ xử lý, môđun truyền thông 803 là giao diện truyền thông, và môđun lưu trữ 801 là bộ nhớ, thiết bị mạng thứ nhất theo phương án này của sáng chế có thể là thiết bị mạng thứ nhất như được thể hiện trên Fig.8b.

Như được thể hiện trên Fig.8b, thiết bị mạng thứ nhất 810 bao gồm bộ xử lý 812, giao diện truyền thông 813, và bộ nhớ 811. Một cách tùy ý, thiết bị mạng thứ nhất 810 có thể còn bao gồm bus 814. Giao diện truyền thông 813, bộ xử lý 812, và bộ nhớ 811 có thể được kết nối với nhau nhờ sử dụng bus 814. Bus 814 có thể là bus kết nối thành phần ngoại vi (Peripheral Component Interconnect, viết tắt là PCI), bus kiến trúc tiêu chuẩn công nghiệp mở rộng (Extended Industry Standard Architecture, viết tắt là EISA), hoặc tương tự. Bus 814 có thể được phân loại là bus địa chỉ, bus dữ liệu, bus điều khiển, hoặc tương tự. Để dễ biểu diễn, chỉ một đường

thẳng đậm được sử dụng để biểu diễn bus trên Fig.8b, nhưng điều này không có nghĩa là chỉ có một bus hoặc một loại bus.

Thiết bị mạng thứ nhất như được thể hiện trên Fig.8a và Fig.8b có thể là thực thể AMF trong kiến trúc hệ thống trên Fig.1, hoặc có thể là môđun SEAF trong thực thể chức năng AMF. Khi AMF và SEAF không phải là một thực thể chức năng, thiết bị mạng thứ nhất có thể là thực thể chức năng AMF, hoặc thực thể chức năng MME, hoặc thực thể khác có chức năng quản lý di động và truy cập.

Khi môđun được tích hợp được sử dụng, Fig.9a là sơ đồ khối giản lược có thể của thực thể chức năng bảo mật thứ nhất theo phương án của sáng chế. Thực thể chức năng bảo mật thứ nhất 900 bao gồm môđun xử lý 902 và môđun truyền thông 903. Môđun xử lý 902 được tạo cấu hình để điều khiển và quản lý các hoạt động của thực thể chức năng bảo mật thứ nhất. Ví dụ, môđun xử lý 902 được tạo cấu hình để hỗ trợ thực thể chức năng bảo mật thứ nhất trong việc thực hiện quy trình 202 trên Fig.2, quy trình 303 trên Fig.3, quy trình 404 trên Fig.4, quy trình 505 trên Fig.5, các quy trình 603, 604, 607, 608, 609, 610, 612, và 615 trên Fig.6a đến Fig.6d, các quy trình 712 và 713 trên Fig.7a, các quy trình 702, 705, 706, và 709 trên Fig.7b, và/hoặc các quy trình khác sử dụng công nghệ được mô tả trong bản mô tả này. Môđun truyền thông 903 được tạo cấu hình để hỗ trợ thực thể chức năng bảo mật thứ nhất trong việc giao tiếp với thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ hai, hoặc thiết bị mạng khác. Thực thể chức năng bảo mật thứ nhất có thể còn bao gồm môđun lưu trữ 901, được tạo cấu hình để lưu trữ dữ liệu và chương trình và của thực thể chức năng bảo mật thứ nhất.

Môđun xử lý 902 có thể là bộ xử lý hoặc bộ điều khiển, ví dụ, có thể là CPU, bộ xử lý mục đích chung, DSP, ASIC, FPGA hoặc thiết bị lôgic lập trình được khác, thiết bị lôgic tranzito, thành phần phần cứng, hoặc sự kết hợp bất kỳ của nó. Môđun xử lý có thể thực hiện hoặc thực thi các khối, các môđun, và các mạch lôgic ví dụ khác nhau được mô tả dựa vào nội dung được bộc lộ theo sáng chế. Theo cách khác, bộ xử lý có thể là sự kết hợp để thực hiện chức năng tính, ví dụ, sự kết hợp của một hoặc nhiều bộ vi xử lý hoặc sự kết hợp của DSP và bộ vi xử lý. Môđun truyền thông 903 có thể là giao diện truyền thông, bộ thu phát, mạch thu phát, hoặc tương tự. Giao diện truyền thông là tên gọi chung, và trong quá trình thực hiện cụ thể,

giao diện truyền thông có thể bao gồm nhiều giao diện, ví dụ, có thể bao gồm giao diện giữa thực thể chức năng bảo mật thứ nhất và thiết bị mạng thứ nhất hoặc giữa thực thể chức năng bảo mật thứ nhất và thiết bị mạng thứ hai và/hoặc giao diện khác. Môđun lưu trữ 901 có thể là bộ nhớ.

Khi môđun xử lý 902 là bộ xử lý, môđun truyền thông 903 là giao diện truyền thông, và môđun lưu trữ 901 là bộ nhớ, thực thể chức năng bảo mật thứ nhất theo phương án này của sáng chế có thể là thực thể chức năng bảo mật thứ nhất như được thể hiện trên Fig.9b.

Như được thể hiện trên Fig.9b, thực thể chức năng bảo mật thứ nhất 910 bao gồm bộ xử lý 912, giao diện truyền thông 913, và bộ nhớ 911. Một cách tùy ý, thực thể chức năng bảo mật thứ nhất 910 có thể còn bao gồm bus 914. Giao diện truyền thông 913, bộ xử lý 912, và bộ nhớ 911 có thể được kết nối với nhau nhờ sử dụng bus 914. Bus 914 có thể là bus PCI, bus EISA, hoặc tương tự. Bus 914 có thể được phân loại như bus địa chỉ, bus dữ liệu, bus điều khiển, hoặc tương tự. Để dễ biểu diễn, chỉ một đường thẳng đậm được sử dụng để biểu diễn bus trên Fig.9b, nhưng điều này không có nghĩa là chỉ một bus hoặc chỉ một loại bus.

Thực thể chức năng bảo mật thứ nhất như được thể hiện trên Fig.9a và Fig.9b có thể là thực thể AUSF trong kiến trúc hệ thống của Fig.1; hoặc khi AMF trên Fig.1 không bao gồm SEAF, thực thể chức năng bảo mật thứ nhất có thể là SEAF.

Phương án của sáng chế còn đề xuất thực thể chức năng bảo mật thứ hai. Sơ đồ cấu trúc giản lược của thực thể chức năng bảo mật thứ hai là giống như sơ đồ cấu trúc giản lược của thực thể chức năng bảo mật thứ nhất, như được thể hiện trên Fig.10a và Fig.10b. Các môđun hoặc các thành phần được bao gồm trong thực thể chức năng bảo mật thứ hai có thể thực hiện tương ứng các hoạt động được kết thúc bởi thực thể chức năng bảo mật thứ hai trong các phương pháp nêu trên, và các sự thể hiện chi tiết không được mô tả lại ở đây. Thực thể chức năng bảo mật thứ hai như được thể hiện trên Fig.10a hoặc Fig.10b có thể là thực thể ARPF trên Fig.1.

Các phương pháp hoặc các bước thuật toán được mô tả dựa vào nội dung được bộc lộ theo các phương án của sáng chế có thể được thực hiện theo cách thức phần cứng, hoặc có thể được thực hiện theo cách thực thực thi lệnh phần mềm bởi bộ xử lý. Lệnh phần mềm có thể bao gồm môđun phần mềm tương ứng. Môđun phần

mềm có thể được lưu trữ trong bộ nhớ truy cập ngẫu nhiên (Random Access Memory, viết tắt là RAM), bộ nhớ tia chớp, bộ nhớ chỉ đọc (Read-Only Memory, viết tắt là ROM), bộ nhớ chỉ đọc lập trình được xóa được (Erasable Programmable ROM, viết tắt là EPROM), bộ nhớ chỉ độc lập trình được xóa được bằng điện (Electrically EPROM, viết tắt là EEPROM), bộ đăng ký, đĩa cứng, đĩa cứng có thể tháo được, bộ nhớ chỉ đọc-đĩa compact (CD-ROM), hoặc phương tiện lưu trữ dưới các dạng khác bất kỳ đã biết trong lĩnh vực. Phương tiện lưu trữ được sử dụng làm ví dụ được ghép đôi với bộ xử lý, sao cho bộ xử lý có thể đọc thông tin từ phương tiện lưu trữ, và có thể ghi thông tin vào phương tiện lưu trữ. Tất nhiên là, phương tiện lưu trữ có thể là thành phần của bộ xử lý. Bộ xử lý và phương tiện lưu trữ có thể được nằm trong ASIC. Ngoài ra, ASIC có thể được nằm trong thiết bị mạng thứ nhất hoặc thực thể chức năng bảo mật thứ nhất. Tất nhiên là, bộ xử lý và phương tiện lưu trữ có thể tồn tại trong thiết bị mạng thứ nhất hoặc thực thể chức năng bảo mật thứ nhất như các thành phần rời rạc.

Người có hiểu biết trung bình trong lĩnh vực sẽ nhận biết rằng, theo một hoặc nhiều trong số các ví dụ nêu trên, các chức năng được mô tả theo các phương án của sáng chế có thể được thực hiện toàn bộ hoặc từng phần nhờ sử dụng phần mềm, phần cứng, phần sụn, hoặc sự kết hợp bất kỳ của nó. Khi phần mềm được sử dụng để thực hiện các phương án, các phương án có thể được thực hiện toàn bộ hoặc từng phần dưới dạng sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính bao gồm một hoặc nhiều lệnh máy tính. Khi các lệnh chương trình máy tính được tải và được thực hiện trên máy tính, các thủ tục hoặc các chức năng theo các phương án của sáng chế được tạo ra toàn bộ hoặc từng phần. Máy tính có thể là máy tính mục đích chung, máy tính dành riêng, mạng máy tính, hoặc thiết bị lập trình được khác. Lệnh máy tính có thể được lưu trữ trong phương tiện lưu trữ đọc được bởi máy tính, hoặc có thể được truyền từ phương tiện lưu trữ đọc được bởi máy tính này đến phương tiện lưu trữ đọc được bởi máy tính khác. Ví dụ, lệnh máy tính có thể được truyền từ trang mạng, máy tính, máy chủ, hoặc trung tâm dữ liệu đến trang mạng khác, máy tính khác, máy chủ khác, hoặc trung tâm dữ liệu khác theo cách thức có dây (ví dụ, cáp đồng trục, cáp quang, hoặc đường dây thuê bao số (Digital Subscriber Line, viết tắt là DSL)) hoặc không dây (ví dụ, hồng ngoại, rađio,

hoặc vi ba). Phương tiện lưu trữ đọc được bởi máy tính có thể là phương tiện có thể sử dụng được bất kỳ có thể truy cập được bởi máy tính, hoặc thiết bị lưu trữ dữ liệu, chẳng hạn như máy chủ hoặc trung tâm dữ liệu, tích hợp một hoặc nhiều phương tiện có thể sử dụng được. Phương tiện có thể sử dụng được có thể là phương tiện từ (ví dụ, đĩa mềm, đĩa cứng, hoặc băng từ), phương tiện quang (ví dụ, đĩa viđeo số (Digital Video Disc, viết tắt là DVD)), phương tiện bán dẫn (ví dụ, đĩa trạng thái rắn (Solid State Disk, viết tắt là SSD), hoặc tương tự.

Các mục đích, các giải pháp kỹ thuật, và các hiệu quả có lợi của các phương án của sáng chế còn được mô tả chi tiết theo các cách thực hiện cụ thể nêu trên. Cần hiểu rằng, các phần mô tả nêu trên chỉ là các cách thực hiện cụ thể của các phương án của sáng chế, nhưng không nhằm giới hạn ở phạm vi bảo hộ của các phương án của sáng chế. Bất kỳ sự cải biến, thay thế tương đương, hoặc sự cải tiến được tạo ra dựa vào các giải pháp kỹ thuật theo các phương án của sáng chế sẽ nằm trong phạm vi bảo hộ của các phương án của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp kích hoạt xác thực mạng, trong đó phương pháp này bao gồm các bước:

thu, bởi thiết bị mạng thứ nhất, tin nhắn thứ nhất từ thiết bị đầu cuối, trong đó tin nhắn thứ nhất này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, và thông tin ký hiệu nhận dạng được sử dụng để chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất; thông tin định tuyến bao gồm thông tin định tuyến thứ nhất và thông tin định tuyến thứ hai, thông tin định tuyến thứ hai được sử dụng để xác định thực thể chức năng giải mã thông tin nhận dạng thứ nhất; và

xác định, bởi thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất nằm trong mạng gia đình của thiết bị đầu cuối theo thông tin định tuyến thứ nhất;

gửi, bởi thiết bị mạng thứ nhất, tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ hai này được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến thứ hai; và

thu, bởi thiết bị mạng thứ nhất, thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, trong đó thông tin nhận dạng thứ hai này được giải mã từ thông tin nhận dạng thứ nhất.

2. Phương pháp theo điểm 1, trong đó bước thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất là bao gồm bước:

thu, bởi thiết bị mạng thứ nhất, tin nhắn thứ ba từ thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ ba này mang thông tin nhận dạng thứ hai và tin nhắn thành công xác thực.

3. Phương pháp theo điểm 2, trong đó trước bước thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, thì phương pháp này bao gồm bước:

thu, bởi thiết bị mạng thứ nhất, vectơ xác thực từ thực thể chức năng bảo mật thứ nhất, và thực hiện việc xác thực cho thiết bị đầu cuối nhờ sử dụng vectơ xác thực này.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó sự nhận dạng lâu dài của thiết bị đầu cuối là sự nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identity - IMSI), và IMSI bao gồm số nhận dạng thuê bao di động (Mobile Subscriber Identification Number - MSIN) và thông tin định tuyến thứ nhất; trong đó thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối là MSIN.

5. Phương pháp kích hoạt xác thực mạng, trong đó phương pháp này bao gồm các bước:

thu, bởi thực thể chức năng bảo mật thứ nhất, tin nhắn thứ hai từ thiết bị mạng thứ nhất, trong đó tin nhắn thứ hai này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến thứ hai; thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, thông tin ký hiệu nhận dạng chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất;

xác định, bởi thực thể chức năng bảo mật thứ nhất theo thông tin định tuyến thứ hai được mang trong tin nhắn thứ hai thu được, thiết bị mạng thứ hai;

gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng đến thiết bị mạng thứ hai;

thu, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ hai và vectơ xác thực từ thiết bị mạng thứ hai; trong đó thông tin nhận dạng thứ hai này được giải mã từ thông tin nhận dạng thứ nhất; và vectơ xác thực này được thu nhận theo thông tin nhận dạng thứ hai;

gửi, bởi thực thể chức năng bảo mật thứ nhất, thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi việc xác thực cho thiết bị đầu cuối thành công.

6. Phương pháp theo điểm 5, trong đó phương pháp này bao gồm bước:

gửi, bởi thực thể chức năng bảo mật thứ nhất, vectơ xác thực đến thiết bị mạng thứ nhất.

7. Phương pháp theo điểm 5 hoặc 6, trong đó thực thể chức năng bảo mật thứ nhất là thực thể chức năng máy chủ xác thực (AUthentication Server Function - AUSF), thiết bị mạng thứ nhất là thực thể chức năng neo bảo mật (SEcurity Anchor Function - SEAF) hoặc thực thể chức năng kết hợp thực thể quản lý di động và truy cập (Access and Mobility Management - AMF) và thực thể SEAF; và thiết bị mạng thứ hai là thực thể quản lý dữ liệu hợp nhất (Unified Data Management - UDM).

8. Phương pháp kích hoạt việc xác thực, trong đó phương pháp này bao gồm các bước:

thu nhận, bởi thiết bị đầu cuối, thông tin nhận dạng thứ nhất bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối nhờ sử dụng khóa công khai;

gửi, bởi thiết bị đầu cuối này, tin nhắn thứ nhất đến thiết bị mạng thứ nhất; trong đó tin nhắn thứ nhất này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến, thông tin ký hiệu nhận dạng chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất, và thông tin định tuyến bao gồm thông tin định tuyến thứ nhất mà chỉ báo mạng gia đình của thiết bị đầu cuối và thông tin định tuyến thứ hai mà chỉ báo thực thể chức năng được sử dụng để giải mã thông tin nhận dạng thứ nhất.

9. Phương pháp theo điểm 8, trong đó sự nhận dạng lâu dài của thiết bị đầu cuối là sự nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identity - IMSI), và IMSI bao gồm số nhận dạng thuê bao di động (Mobile Subscriber Identification Number - MSIN) và thông tin định tuyến thứ nhất; trong đó thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối là MSIN.

10. Phương pháp theo điểm 8 hoặc 9, trong đó khóa công khai được lưu trữ trong môđun nhận dạng thuê bao đa năng (Universal Subscriber Identity Module - USIM)

của thiết bị đầu cuối.

11. Phương pháp theo điểm 8 hoặc 9, trong đó tin nhắn thứ nhất là tin nhắn yêu cầu đăng ký.

12. Phương pháp theo điểm 8 hoặc 9, trong đó thiết bị mạng thứ nhất là thực thể chức năng neo bảo mật (SEcurity Anchor Function - SEAF) hoặc thực thể chức năng kết hợp thực thể quản lý di động và truy cập (Access and Mobility Management - AMF) và thực thể SEAF.

13. Thiết bị mạng thứ nhất, trong đó thiết bị mạng thứ nhất này bao gồm môđun xử lý và môđun truyền thông, trong đó

môđun xử lý được tạo cấu hình để: thu, nhờ sử dụng môđun truyền thông, tin nhắn thứ nhất từ thiết bị đầu cuối, trong đó tin nhắn thứ nhất này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, và thông tin ký hiệu nhận dạng chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất; thông tin định tuyến bao gồm thông tin định tuyến thứ nhất và thông tin định tuyến thứ hai, và thông tin định tuyến thứ hai được sử dụng để xác định thực thể chức năng giải mã thông tin nhận dạng thứ nhất; xác định thực thể chức năng bảo mật thứ nhất nằm trong mạng gia đình của thiết bị đầu cuối theo thông tin định tuyến thứ nhất; và gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất nhờ sử dụng môđun truyền thông, trong đó tin nhắn thứ hai này được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến thứ hai; trong đó môđun xử lý được tạo cấu hình để thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất nhờ sử dụng môđun truyền thông này, trong đó thông tin nhận dạng thứ hai này được giải mã từ thông tin nhận dạng thứ nhất.

14. Thiết bị mạng thứ nhất theo điểm 13, trong đó môđun xử lý được tạo cấu hình cụ thể để nhận tin nhắn thứ ba từ thực thể chức năng bảo mật thứ nhất nhờ sử dụng môđun truyền thông, trong đó tin nhắn thứ ba này mang thông tin nhận dạng thứ hai và tin nhắn thành công xác thực.

15. Thiết bị mạng thứ nhất theo điểm 14, trong đó môđun xử lý được tạo cấu hình để: thu, nhờ sử dụng môđun truyền thông, vectơ xác thực được gửi bởi thực thể chức năng bảo mật thứ nhất; thực hiện việc xác thực cho thiết bị đầu cuối nhờ sử dụng vectơ xác thực này.

16. Thiết bị mạng thứ nhất theo điểm bất kỳ trong số các điểm từ 13 đến 15, trong đó sự nhận dạng lâu dài của thiết bị đầu cuối là sự nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identity - IMSI), và IMSI bao gồm số nhận dạng thuê bao di động (Mobile Subscriber Identification Number - MSIN) và thông tin định tuyến thứ nhất; trong đó thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối là MSIN.

17. Thực thể chức năng bảo mật thứ nhất, trong đó thực thể chức năng bảo mật thứ nhất này bao gồm môđun xử lý và môđun truyền thông, trong đó

môđun xử lý được tạo cấu hình để thu tin nhắn thứ hai từ thiết bị mạng thứ nhất nhờ sử dụng môđun truyền thông, trong đó tin nhắn thứ hai này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến thứ hai; thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, thông tin ký hiệu nhận dạng chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất; xác định thiết bị mạng thứ hai theo thông tin định tuyến thứ hai được mang trong tin nhắn thứ hai thu được; gửi thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng đến thiết bị mạng thứ hai nhờ sử dụng môđun truyền thông; và thu thông tin nhận dạng thứ hai và vectơ xác thực từ thiết bị mạng thứ hai nhờ sử dụng môđun truyền thông; trong đó thông tin nhận dạng thứ hai được giải mã từ thông tin nhận dạng thứ nhất; và vectơ xác thực được thu nhận theo thông tin

nhận dạng thứ hai khi gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất nhờ sử dụng môđun truyền thông khi việc xác thực cho thiết bị đầu cuối thành công.

18. Thực thể chức năng bảo mật thứ nhất theo điểm 17, trong đó môđun xử lý còn được tạo cấu hình để gửi, nhờ sử dụng môđun truyền thông, vectơ xác thực đến thiết bị mạng thứ nhất.

19. Thực thể chức năng bảo mật thứ nhất theo điểm 17 hoặc 18, trong đó thực thể chức năng bảo mật thứ nhất là thực thể chức năng máy chủ xác thực (AUthentication Server Function - AUSF), thiết bị mạng thứ nhất là thực thể chức năng neo bảo mật (SEcurity Anchor Function - SEAF) hoặc thực thể chức năng kết hợp thực thể quản lý di động và truy cập (Access and Mobility Management - AMF) và thực thể SEAF; và thiết bị mạng thứ hai là thực thể quản lý dữ liệu hợp nhất (Unified Data Management - UDM).

20. Thiết bị kích hoạt xác thực mạng, trong đó thiết bị này bao gồm môđun xử lý và môđun truyền thông, trong đó

môđun xử lý được tạo cấu hình để thu nhận thông tin nhận dạng thứ nhất bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị này nhờ sử dụng khóa công khai; gửi tin nhắn thứ nhất đến thiết bị mạng thứ nhất nhờ sử dụng môđun truyền thông; trong đó tin nhắn thứ nhất này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến, thông tin ký hiệu nhận dạng chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất, và thông tin định tuyến bao gồm thông tin định tuyến thứ nhất mà chỉ báo mạng gia đình của thiết bị đầu cuối và thông tin định tuyến thứ hai mà chỉ báo thực thể chức năng được sử dụng để giải mã thông tin nhận dạng thứ nhất.

21. Thiết bị theo điểm 20, trong đó sự nhận dạng lâu dài của thiết bị này là sự nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identity - IMSI), và IMSI bao gồm số nhận dạng thuê bao di động (Mobile Subscriber Identification

Number - MSIN) và thông tin định tuyến thứ nhất; trong đó thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối là MSIN.

22. Thiết bị theo điểm 20 hoặc 21, trong đó khóa công khai được lưu trữ trong môđun nhận dạng thuê bao đa năng (Universal Subscriber Identity Module - USIM) của thiết bị này.

23. Thiết bị truyền thông, bao gồm bộ nhớ lưu trữ các lệnh chương trình, và bộ xử lý được ghép đôi với bộ nhớ và được tạo cấu hình để thực hiện các lệnh này để khiến thiết bị này thực hiện phương pháp theo điểm bất kỳ trong số các điểm 1 đến 4.

24. Thiết bị truyền thông, bao gồm bộ nhớ lưu trữ các lệnh chương trình, và bộ xử lý được ghép đôi với bộ nhớ và được tạo cấu hình để thực hiện các lệnh này để khiến thiết bị này thực hiện phương pháp theo điểm bất kỳ trong số các điểm 5 đến 7.

25. Thiết bị truyền thông, bao gồm bộ nhớ lưu trữ các lệnh chương trình, và bộ xử lý được ghép đôi với bộ nhớ và được tạo cấu hình để thực hiện các lệnh này để khiến thiết bị này thực hiện phương pháp theo điểm bất kỳ trong số các điểm 8 đến 10.

26. Thiết bị truyền thông theo điểm 25, trong đó thiết bị này là thiết bị người dùng (User Equipment - UE) hoặc con chip trong UE.

27. Hệ thống kích hoạt xác thực mạng, trong đó hệ thống này bao gồm thiết bị mạng thứ nhất, và thực thể chức năng bảo mật thứ nhất;

trong đó thiết bị mạng thứ nhất được tạo cấu hình để thu tin nhắn thứ nhất từ thiết bị đầu cuối, trong đó tin nhắn thứ nhất này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến, thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự

nhận dạng lâu dài của thiết bị đầu cuối dựa vào khóa công khai, và thông tin ký hiệu nhận dạng được sử dụng để chỉ báo cách thức mã hóa của thông tin nhận dạng thứ nhất; thông tin định tuyến bao gồm thông tin định tuyến thứ nhất và thông tin định tuyến thứ hai, thông tin định tuyến thứ nhất được sử dụng để xác định mạng gia đình của thiết bị đầu cuối, thông tin định tuyến thứ hai được sử dụng để xác định thực thể chức năng giải mã thông tin nhận dạng thứ nhất; và xác định thực thể chức năng bảo mật thứ nhất nằm trong mạng gia đình của thiết bị đầu cuối theo thông tin định tuyến thứ nhất; gửi tin nhắn thứ hai đến thực thể chức năng bảo mật thứ nhất, trong đó tin nhắn thứ hai này được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai này mang thông tin nhận dạng thứ nhất, thông tin ký hiệu nhận dạng và thông tin định tuyến thứ hai; và thu thông tin nhận dạng thứ hai từ thực thể chức năng bảo mật thứ nhất, trong đó thông tin nhận dạng thứ hai này được giải mã từ thông tin nhận dạng thứ nhất;

thực thể chức năng bảo mật thứ nhất được tạo cấu hình để thu tin nhắn thứ hai từ thiết bị mạng thứ nhất, xác định, theo thông tin định tuyến thứ hai được mang trong tin nhắn thứ hai thu được, thiết bị mạng thứ hai; gửi thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng đến thiết bị mạng thứ hai; và thu thông tin nhận dạng thứ hai và vectơ xác thực từ thiết bị mạng thứ hai; trong đó vectơ xác thực này được thu nhận theo thông tin nhận dạng thứ hai; và gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi việc xác thực cho thiết bị đầu cuối thành công.

28. Hệ thống theo điểm 27, trong đó hệ thống này còn bao gồm thiết bị mạng thứ hai, và

thiết bị mạng thứ hai này được tạo cấu hình để thu thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng từ thực thể chức năng bảo mật thứ nhất; giải mã thông tin nhận dạng thứ nhất dựa vào thông tin ký hiệu nhận dạng và khóa cá nhân được lưu trữ để thu nhận thông tin nhận dạng thứ hai, và thu nhận vectơ xác thực theo thông tin nhận dạng thứ hai; và gửi thông tin nhận dạng thứ hai và vectơ xác thực này đến thực thể chức năng bảo mật thứ nhất.

29. Hệ thống theo điểm 27 hoặc 28, trong đó thực thể chức năng bảo mật thứ nhất, được tạo cấu hình để gửi thông tin nhận dạng thứ hai đến thiết bị mạng thứ nhất khi việc xác thực cho thiết bị đầu cuối thành công, bao gồm:

thực thể chức năng bảo mật thứ nhất, được tạo cấu hình để thực hiện việc xác thực cho thiết bị đầu cuối dựa vào vectơ xác thực; gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất khi việc xác thực cho thiết bị đầu cuối thành công, trong đó tin nhắn thứ ba này mang thông tin nhận dạng thứ hai và tin nhắn thành công xác thực.

30. Hệ thống theo điểm 29, trong đó tin nhắn thành công xác thực là tin nhắn thành công EAP (Extensible Authentication Protocol - giao thức xác thực có thể mở rộng).

31. Phương tiện lưu trữ đọc được bởi máy tính, bao gồm lệnh, trong đó khi lệnh này được chạy trên máy tính, thì khiến máy tính đó thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4.

32. Phương tiện lưu trữ đọc được bởi máy tính, bao gồm lệnh, trong đó khi lệnh này được chạy trên máy tính, thì khiến máy tính đó thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 5 đến 7.

33. Phương tiện lưu trữ đọc được bởi máy tính, bao gồm lệnh, trong đó khi lệnh này được chạy trên máy tính, thì khiến máy tính đó thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 12.

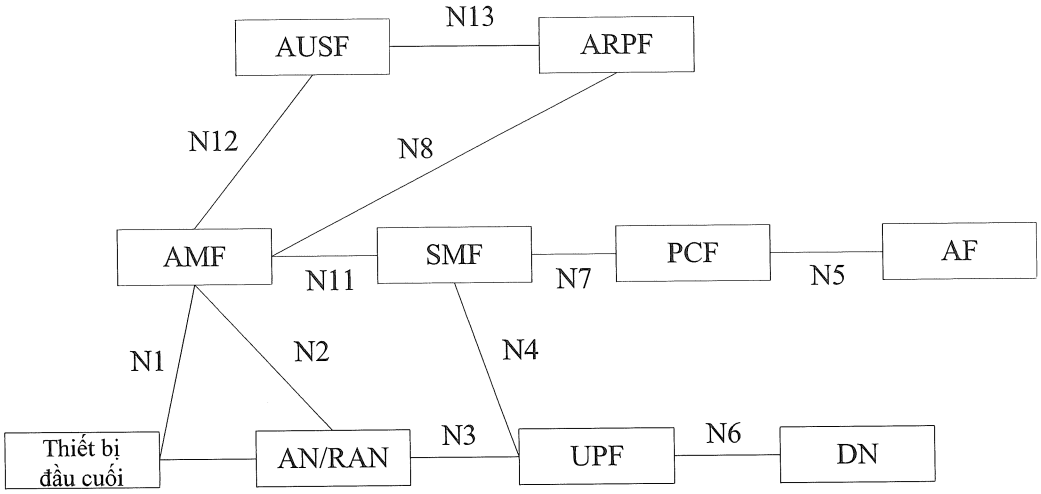
AUSF
N13
ARPF
N12
N8
AMF
N11
SMF
N7
PCF
N5
AF
N1
N2
N4
Thiết bị đầu cuối
AN/RAN
N3
UPF
N6
DN

FIG. 1

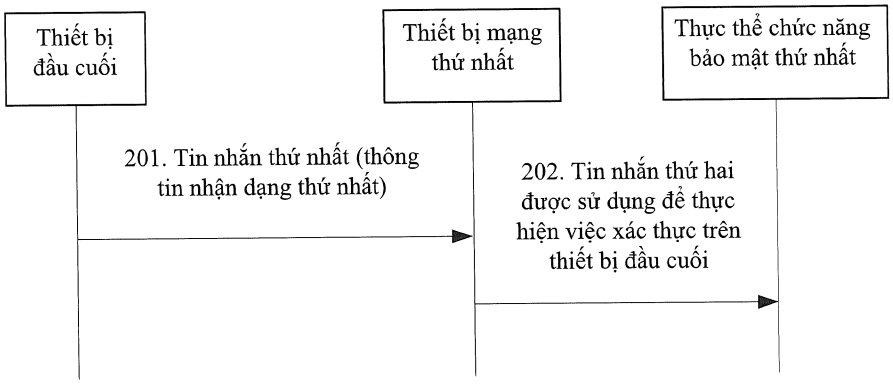
Thiết bị đầu cuối
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
201. Tin nhắn thứ nhất (thông tin nhận dạng thứ nhất)
202. Tin nhắn thứ hai được sử dụng để thực hiện việc xác thực trên thiết bị đầu cuối

FIG. 2

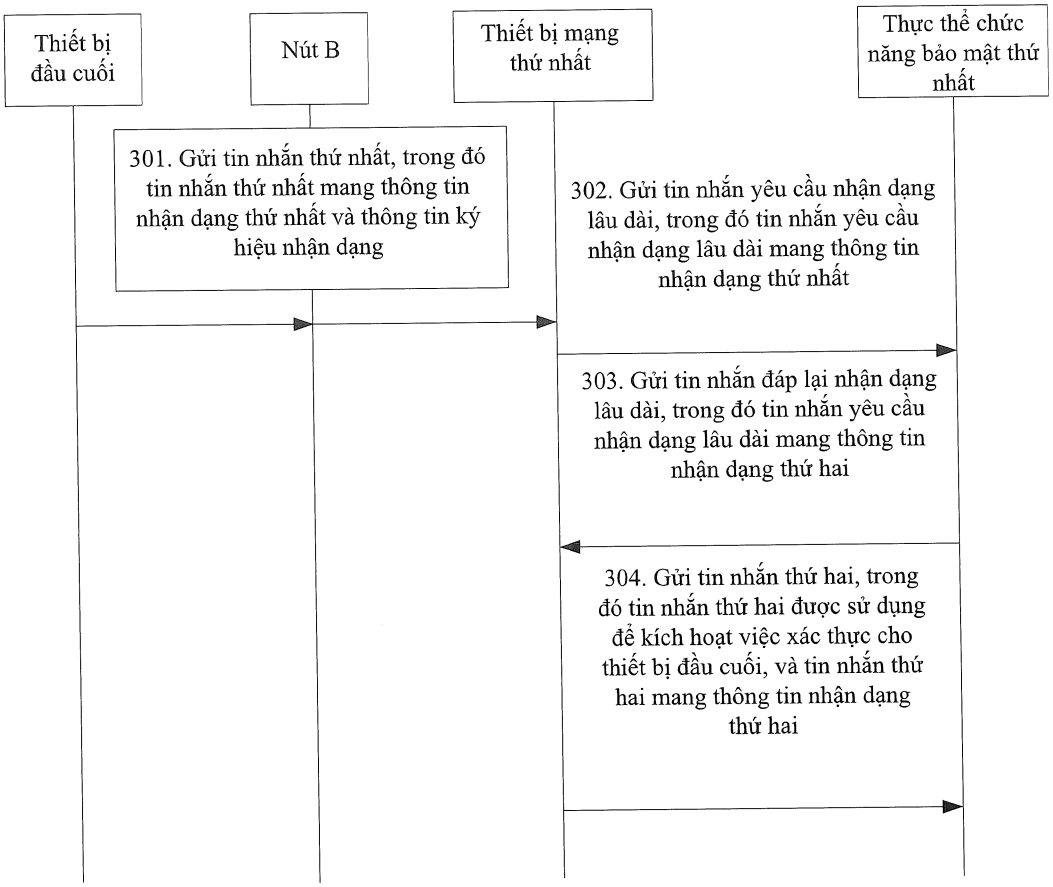
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
301. Gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng
302. Gửi tin nhắn yêu cầu nhận dạng lâu dài, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất
303. Gửi tin nhắn đáp lại nhận dạng lâu dài, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ hai
304. Gửi tin nhắn thứ hai, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ hai

FIG. 3

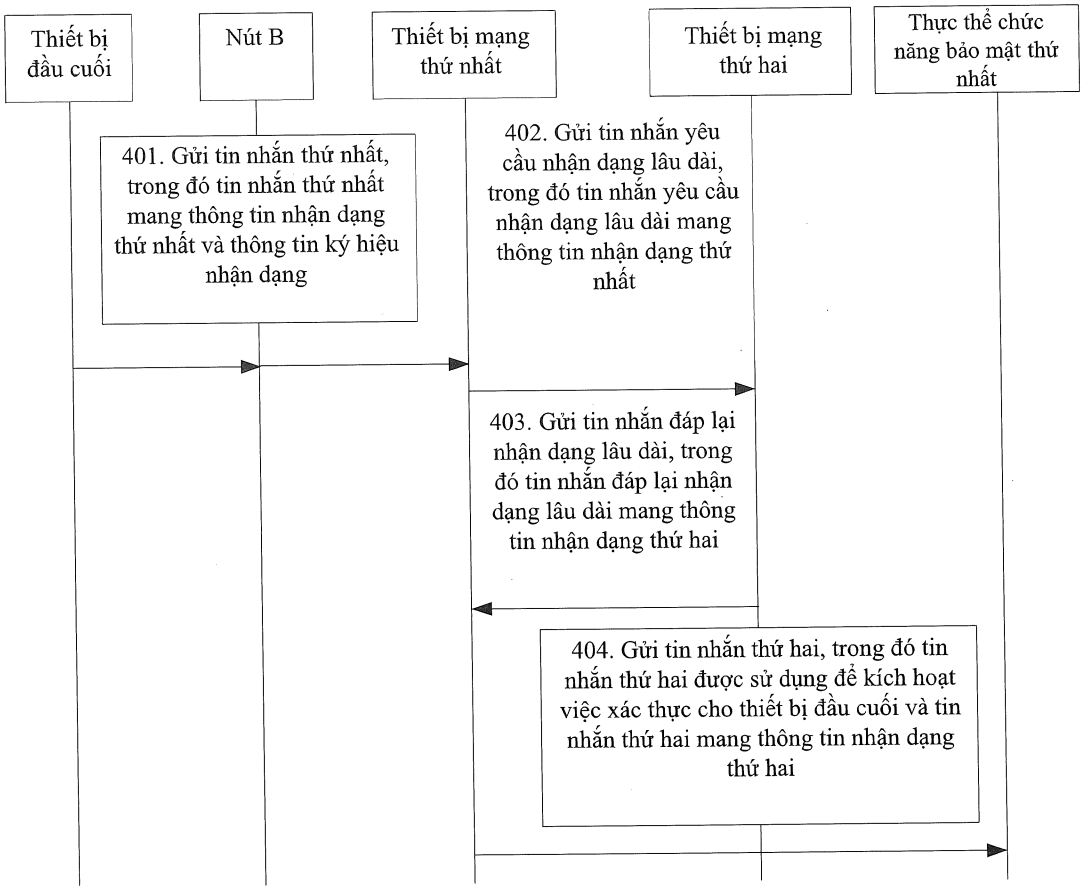
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thiết bị mạng thứ hai
Thực thể chức năng bảo mật thứ nhất
401. Gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng
402. Gửi tin nhắn yêu cầu nhận dạng lâu dài, trong đó tin nhắn yêu cầu nhận dạng lâu dài mang thông tin nhận dạng thứ nhất
403. Gửi tin nhắn đáp lại nhận dạng lâu dài, trong đó tin nhắn đáp lại nhận dạng lâu dài mang thông tin nhận dạng thứ hai
404. Gửi tin nhắn thứ hai, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối và tin nhắn thứ hai mang thông tin nhận dạng thứ hai

FIG. 4

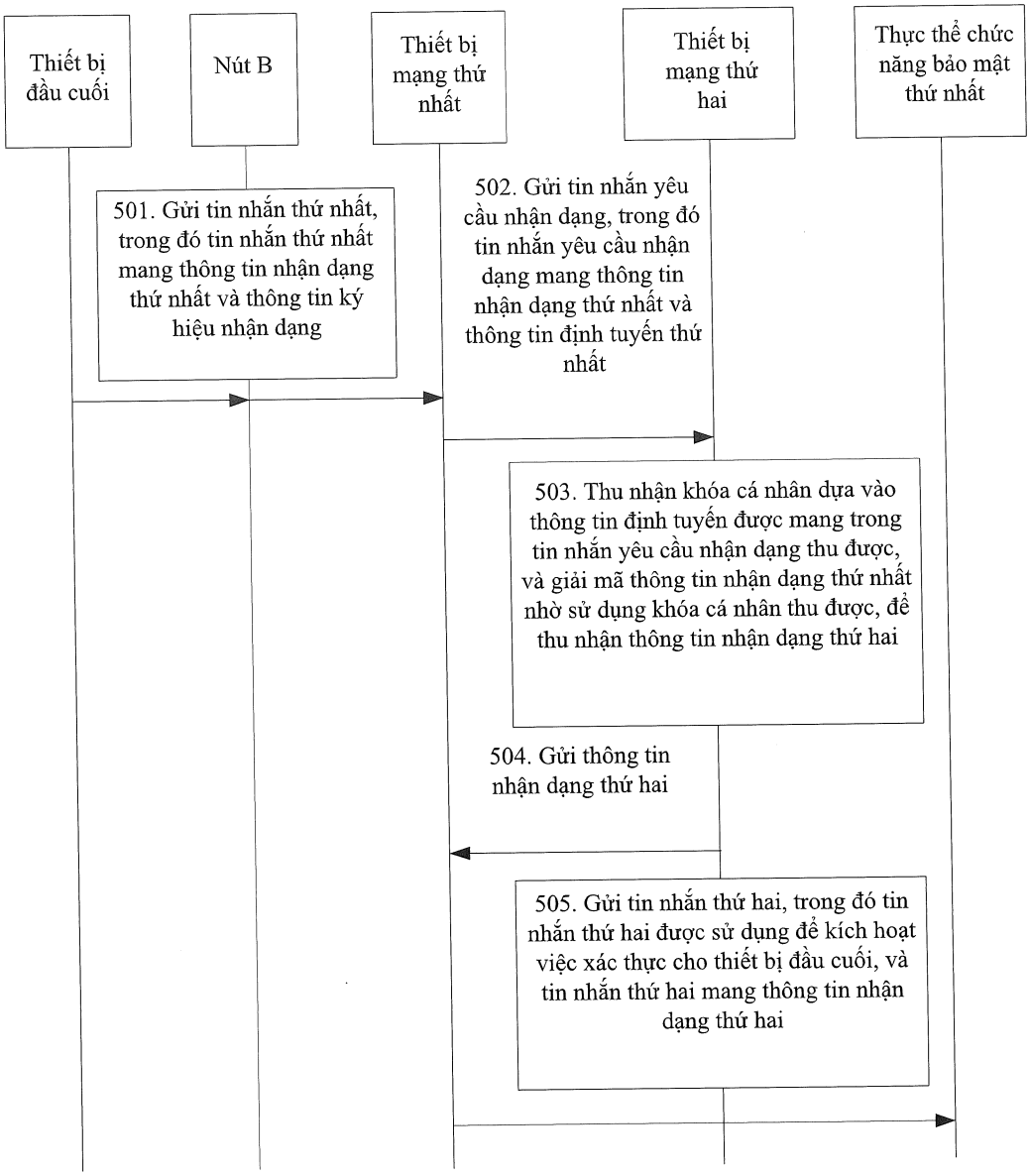
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thiết bị mạng thứ hai
Thực thể chức năng bảo mật thứ nhất
501. Gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất và thông tin ký hiệu nhận dạng
502. Gửi tin nhắn yêu cầu nhận dạng, trong đó tin nhắn yêu cầu nhận dạng mang thông tin nhận dạng thứ nhất và thông tin định tuyến thứ nhất
503. Thu nhận khóa cá nhân dựa vào thông tin định tuyến được mang trong tin nhắn yêu cầu nhận dạng thu được, và giải mã thông tin nhận dạng thứ nhất nhờ sử dụng khóa cá nhân thu được, để thu nhận thông tin nhận dạng thứ hai
504. Gửi thông tin nhận dạng thứ hai
505. Gửi tin nhắn thứ hai, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ hai

FIG. 5

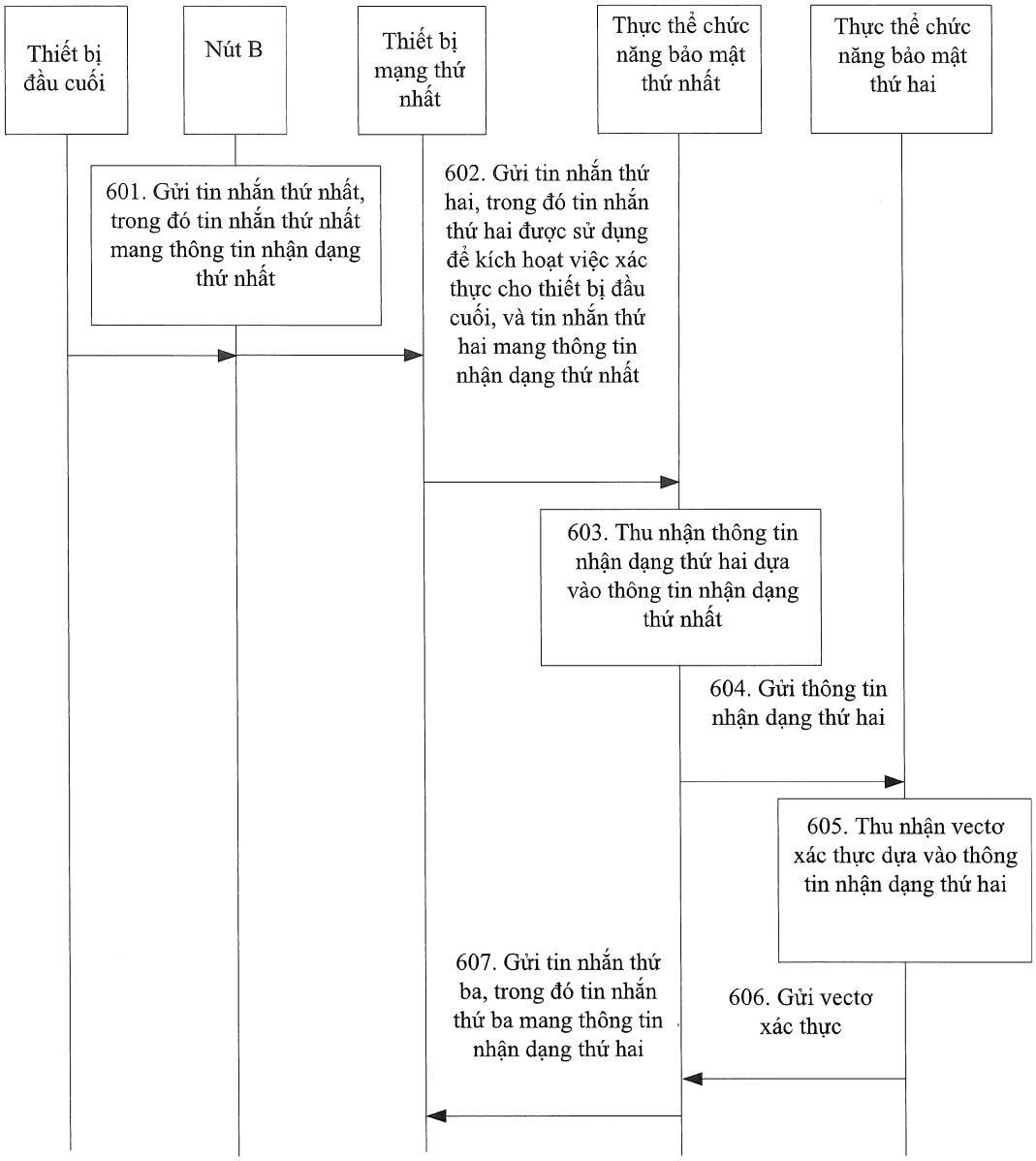
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
Thực thể chức năng bảo mật thứ hai
601. Gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất
602. Gửi tin nhắn thứ hai, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ nhất
603. Thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất
604. Gửi thông tin nhận dạng thứ hai
605. Thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai
606. Gửi vectơ xác thực
607. Gửi tin nhắn thứ ba, trong đó tin nhắn thứ ba mang thông tin nhận dạng thứ hai

FIG. 6a

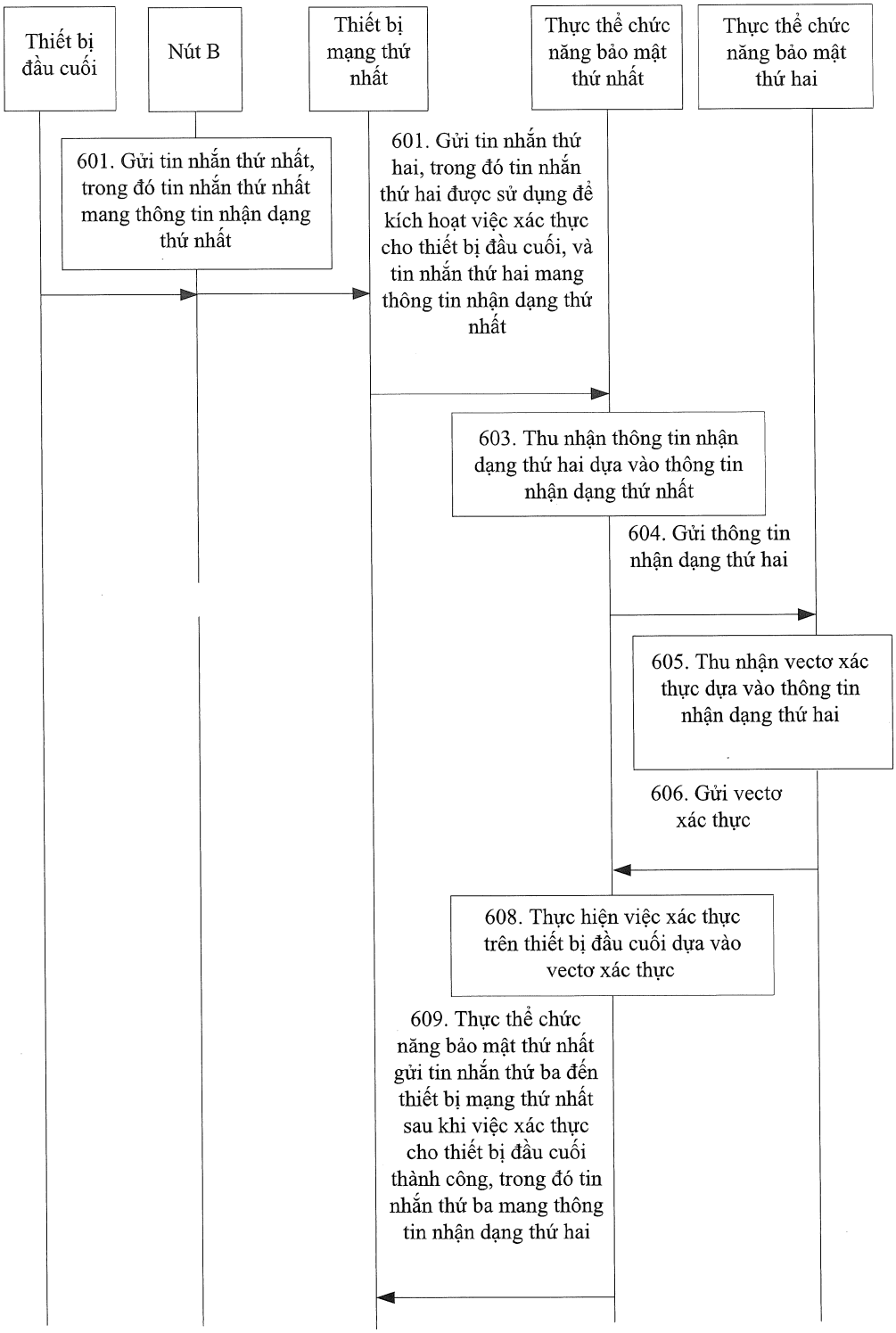
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
Thực thể chức năng bảo mật thứ hai
601. Gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất
601. Gửi tin nhắn thứ hai, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ nhất
603. Thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất
604. Gửi thông tin nhận dạng thứ hai
605. Thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai
606. Gửi vectơ xác thực
608. Thực hiện việc xác thực trên thiết bị đầu cuối dựa vào vectơ xác thực
609. Thực thể chức năng bảo mật thứ nhất gửi tin nhắn thứ ba đến thiết bị mạng thứ nhất sau khi việc xác thực cho thiết bị đầu cuối thành công, trong đó tin nhắn thứ ba mang thông tin nhận dạng thứ hai

FIG. 6b

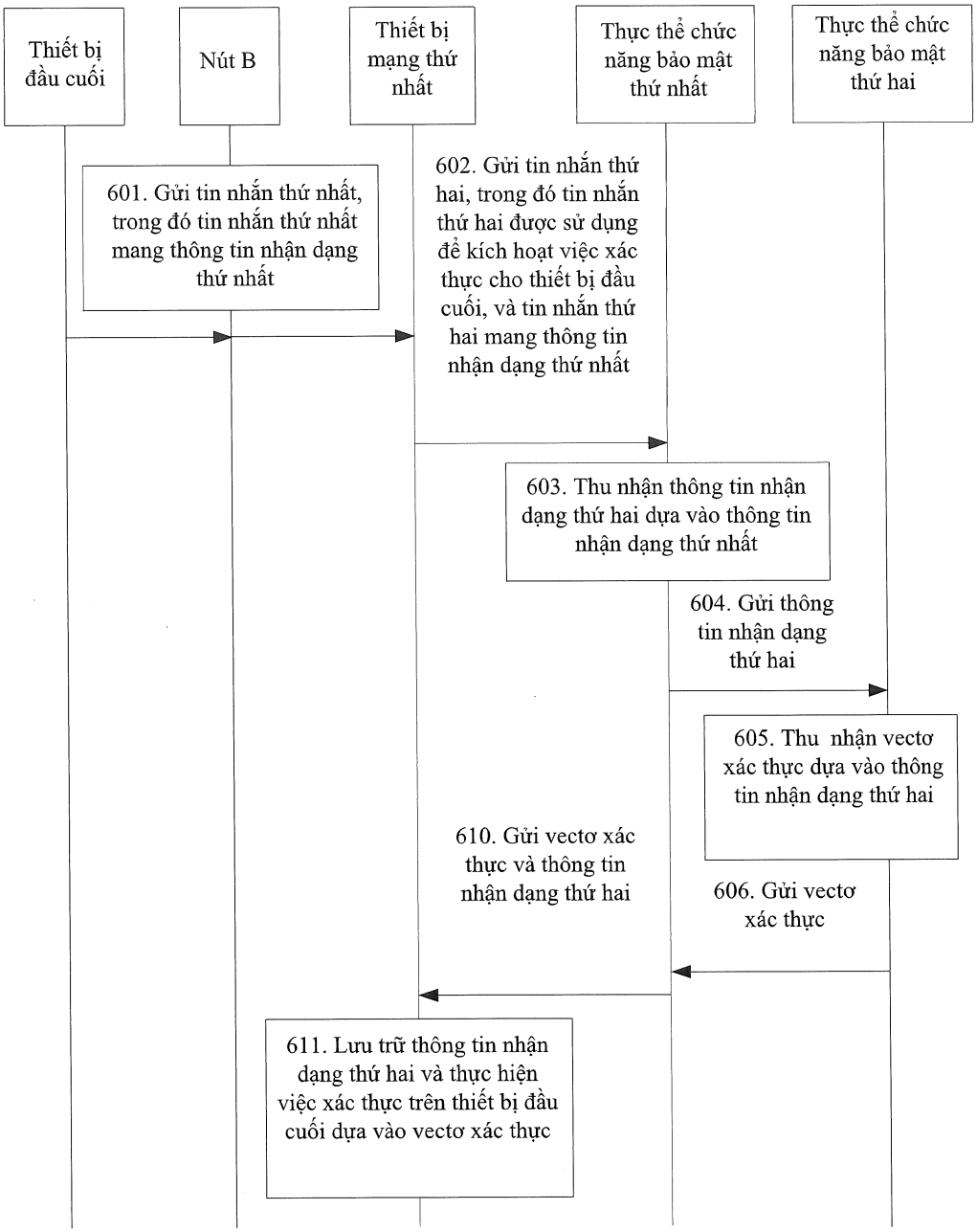
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
Thực thể chức năng bảo mật thứ hai
601. Gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất
602. Gửi tin nhắn thứ hai, trong đó tin nhắn thứ hai được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ nhất
603. Thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất
604. Gửi thông tin nhận dạng thứ hai
605. Thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai
610. Gửi vectơ xác thực và thông tin nhận dạng thứ hai
606. Gửi vectơ xác thực
611. Lưu trữ thông tin nhận dạng thứ hai và thực hiện việc xác thực trên thiết bị đầu cuối dựa vào vectơ xác thực

FIG. 6c

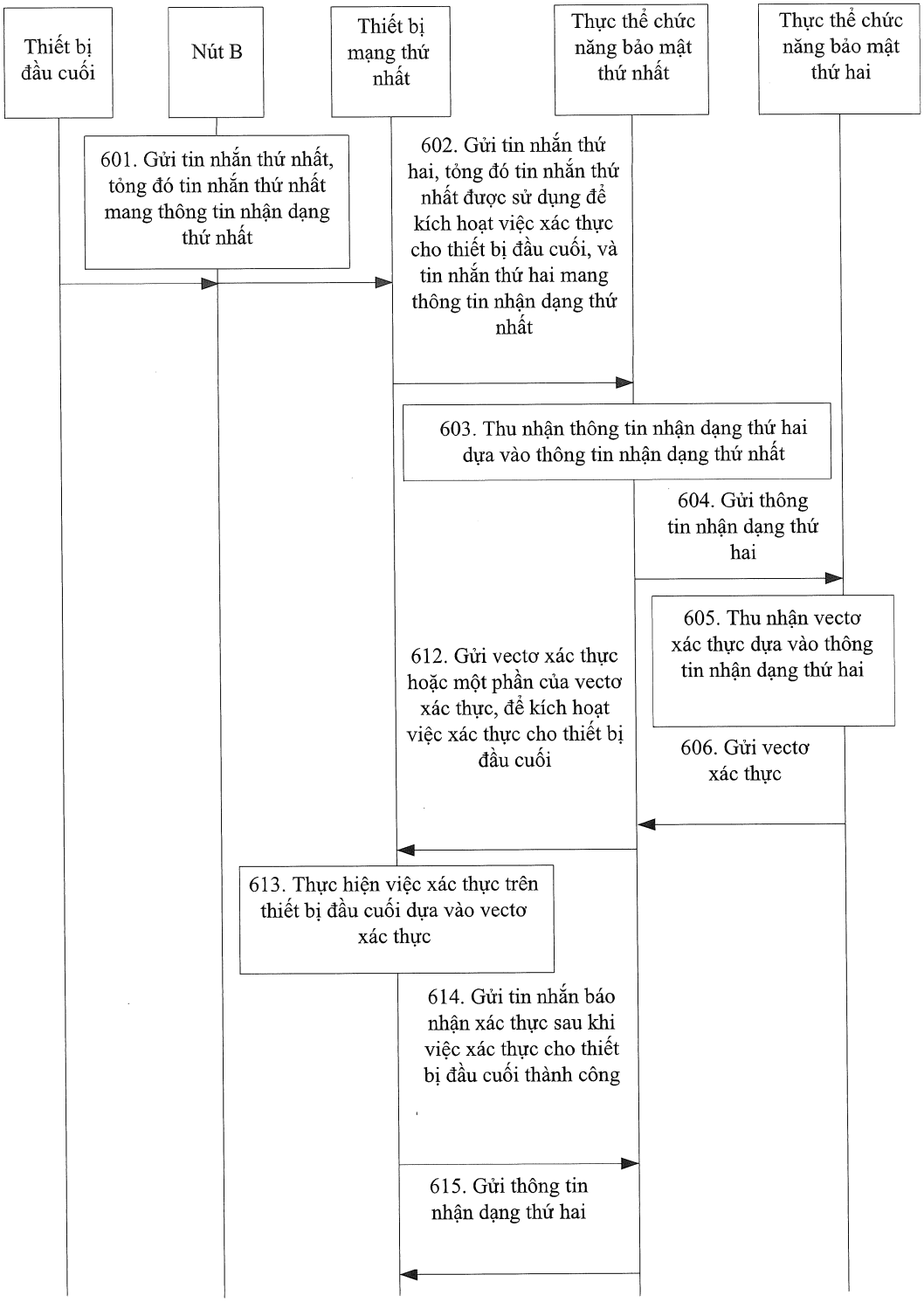
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
Thực thể chức năng bảo mật thứ hai
601. Gửi tin nhắn thứ nhất, tổng đó tin nhắn thứ nhất mang thông tin nhận dạng thứ nhất
602. Gửi tin nhắn thứ hai, tổng đó tin nhắn thứ nhất được sử dụng để kích hoạt việc xác thực cho thiết bị đầu cuối, và tin nhắn thứ hai mang thông tin nhận dạng thứ nhất
603. Thu nhận thông tin nhận dạng thứ hai dựa vào thông tin nhận dạng thứ nhất
604. Gửi thông tin nhận dạng thứ hai
605. Thu nhận vectơ xác thực dựa vào thông tin nhận dạng thứ hai
612. Gửi vectơ xác thực hoặc một phần của vectơ xác thực, để kích hoạt việc xác thực cho thiết bị đầu cuối
606. Gửi vectơ xác thực
613. Thực hiện việc xác thực trên thiết bị đầu cuối dựa vào vectơ xác thực
614. Gửi tin nhắn báo nhận xác thực sau khi việc xác thực cho thiết bị đầu cuối thành công
615. Gửi thông tin nhận dạng thứ hai

FIG. 6d

9/13

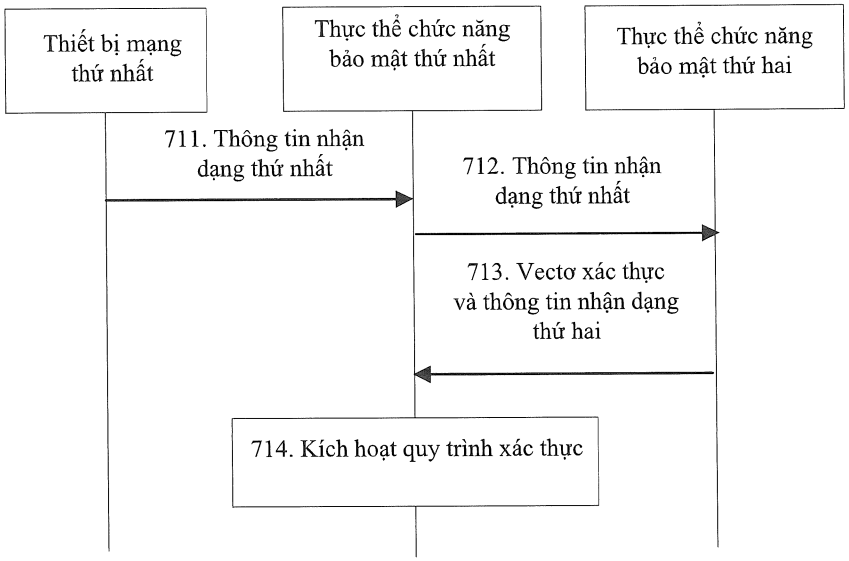
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
Thực thể chức năng bảo mật thứ hai
711. Thông tin nhận dạng thứ nhất
712. Thông tin nhận dạng thứ nhất
713. Vectơ xác thực và thông tin nhận dạng thứ hai
714. Kích hoạt quy trình xác thực

FIG. 7a

10/13

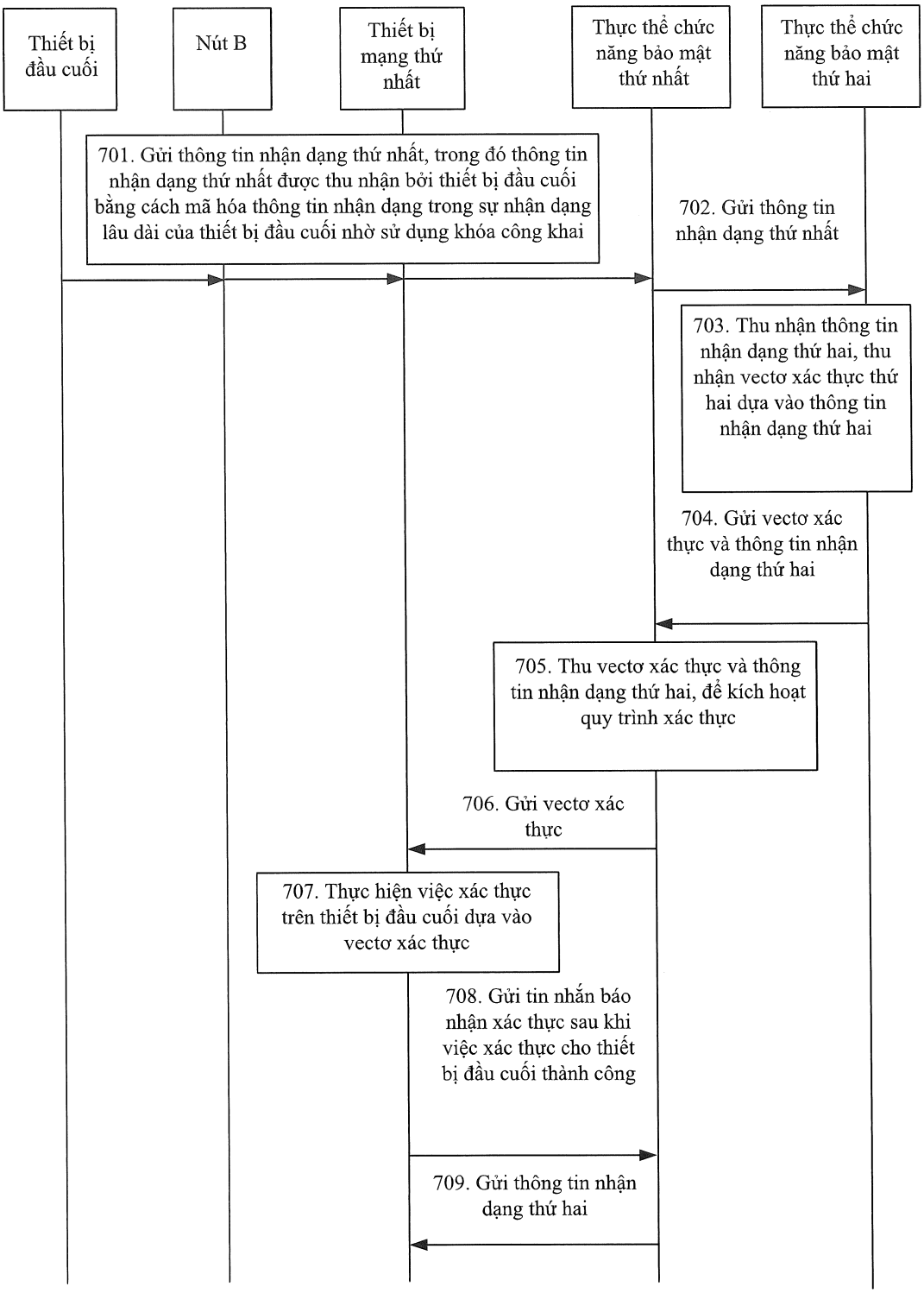
Thiết bị đầu cuối
Nút B
Thiết bị mạng thứ nhất
Thực thể chức năng bảo mật thứ nhất
Thực thể chức năng bảo mật thứ hai
701. Gửi thông tin nhận dạng thứ nhất, trong đó thông tin nhận dạng thứ nhất được thu nhận bởi thiết bị đầu cuối bằng cách mã hóa thông tin nhận dạng trong sự nhận dạng lâu dài của thiết bị đầu cuối nhờ sử dụng khóa công khai
702. Gửi thông tin nhận dạng thứ nhất
703. Thu nhận thông tin nhận dạng thứ hai, thu nhận vectơ xác thực thứ hai dựa vào thông tin nhận dạng thứ hai
704. Gửi vectơ xác thực và thông tin nhận dạng thứ hai
705. Thu vectơ xác thực và thông tin nhận dạng thứ hai, để kích hoạt quy trình xác thực
706. Gửi vectơ xác thực
707. Thực hiện việc xác thực trên thiết bị đầu cuối dựa vào vectơ xác thực
708. Gửi tin nhắn báo nhận xác thực sau khi việc xác thực cho thiết bị đầu cuối thành công
709. Gửi thông tin nhận dạng thứ hai

FIG. 7b

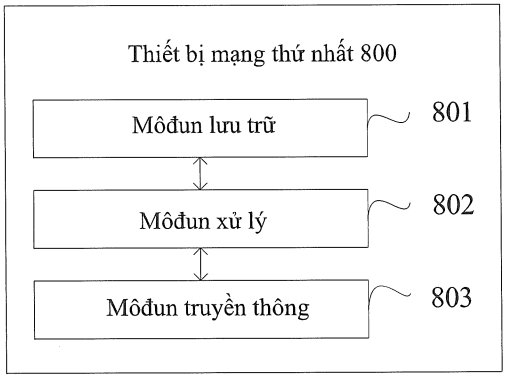
Thiết bị mạng thứ nhất 800
Môđun lưu trữ
801
Môđun xử lý
802
Môđun truyền thông
803

FIG. 8a

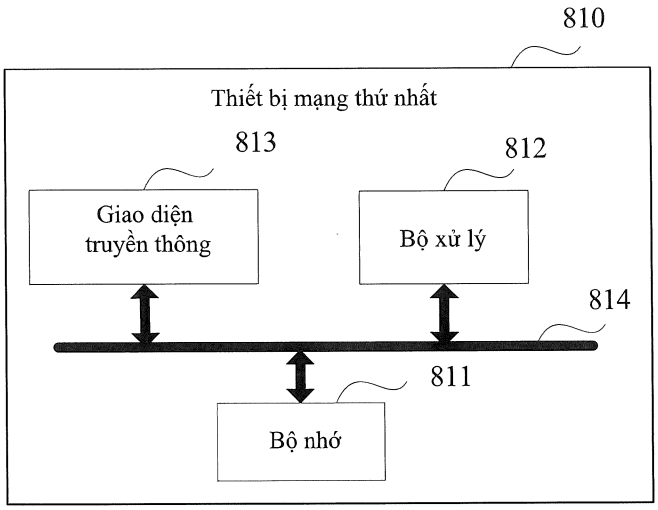
810
Thiết bị mạng thứ nhất
813
812
Giao diện truyền thông
Bộ xử lý
814
811
Bộ nhớ

FIG. 8b

12/13

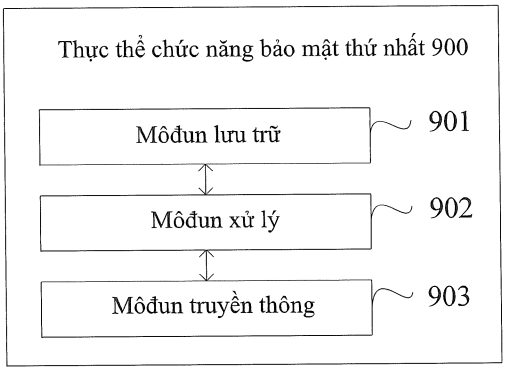

FIG. 9a

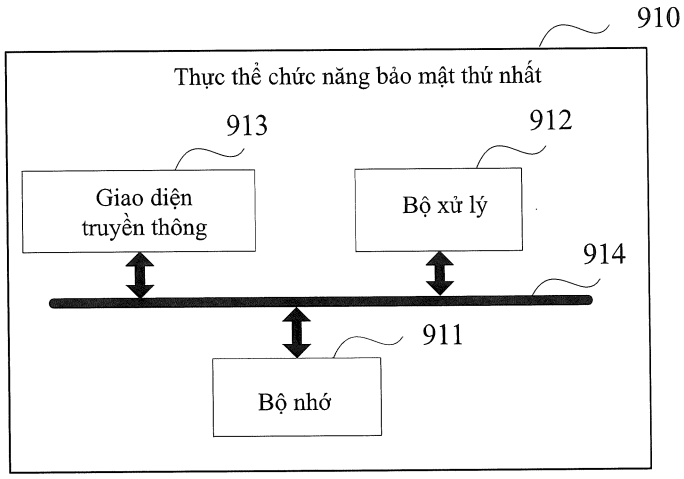

FIG. 9b

13/13

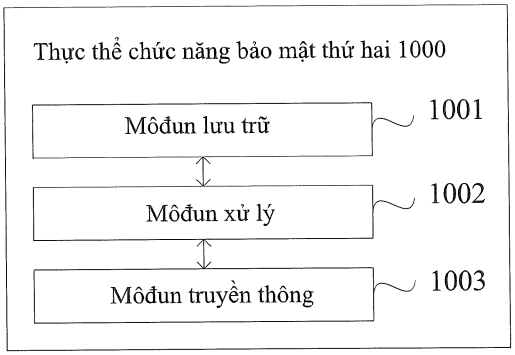

FIG. 10a

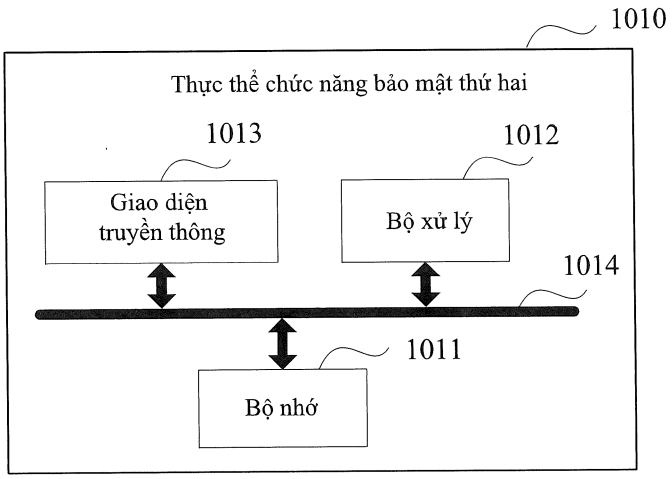

FIG. 10b