(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) **1-0025153**

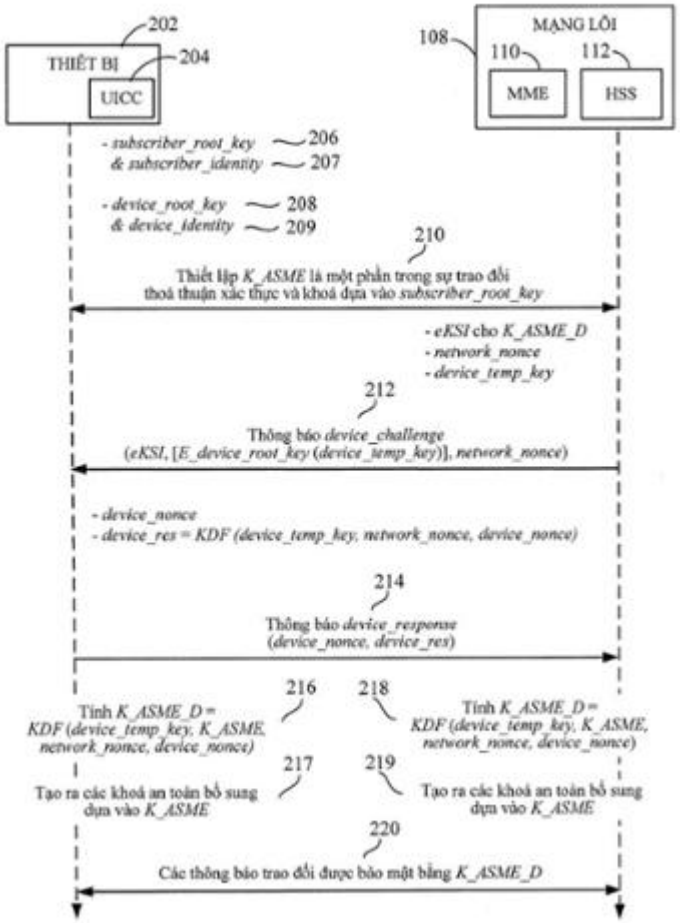
(51)[7] **H04W 12/04**; H04L 29/06

(13) **B**

(21) 1-2013-00152 (22) 16/06/2011
(86) PCT/US2011/040777 16/06/2011 (87) WO2011/159952 22/12/2011
(30) 61/355,423 16/06/2010 US; 13/161,336 15/06/2011 US
(45) 25/08/2020 389 (43) 25/04/2013 301A
(73) QUALCOMM INCORPORATED (US)
Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714, United States of America
(72) ESCOTT, Adrian Edward (GB); PALANIGOUNDER, Anand (IN).
(74) Công ty TNHH Quốc tế D & N (D&N INTERNATIONAL CO.,LTD.)

(54) PHƯƠNG PHÁP XÁC THỰC HOẠT ĐỘNG TRONG THIẾT BỊ VÀ THIẾT BỊ XÁC THỰC

(57) Sáng chế đề xuất phương pháp xác thực giữa thiết bị (ví dụ, thiết bị khách hoặc thiết bị đầu cuối truy nhập) và thực thể mạng. Thiết bị lưu trữ tháo lắp được có thể được kết nối với thiết bị và lưu trữ khoá dành cho thuê bao được dùng để xác thực thuê bao. Thiết bị lưu trữ an toàn có thể được kết nối với thiết bị và lưu trữ khoá dành cho thiết bị được dùng để xác thực thiết bị. Thủ tục xác thực thuê bao có thể được thực hiện giữa thiết bị và thực thể mạng. Thủ tục xác thực thiết bị cũng có thể được thực hiện giữa thiết bị và thực thể mạng. Khoá an toàn có thể được tạo ra để kết hợp xác thực thuê bao và xác thực thiết bị. Khoá an toàn này có thể được dùng để bảo mật thông tin truyền thông giữa thiết bị và mạng phục vụ.


202
THIẾT BỊ
204
UICC
MẠNG LÕI
108
110
MME
112
HSS
- subscriber_root_key
& subscriber_identity
206
207
- device_root_key
& device_identity
208
209
210
Thiết lập K_ASME là một phần trong sự trao đổi thoả thuận xác thực và khoá dựa vào subscriber_root_key
- eKSI cho K_ASME_D
- network_nonce
- device_temp_key
212
Thông báo device_challenge (eKSI, [E_device_root_key (device_temp_key)], network_nonce)
- device_nonce
- device_res = KDF (device_temp_key, network_nonce, device_nonce)
214
Thông báo device_response (device_nonce, device_res)
216
Tính K_ASME_D = KDF (device_temp_key, K_ASME, network_nonce, device_nonce)
217
Tạo ra các khoá an toàn bổ sung dựa vào K_ASME
218
Tính K_ASME_D = KDF (device_temp_key, K_ASME, network_nonce, device_nonce)
219
Tạo ra các khoá an toàn bổ sung dựa vào K_ASME
220
Các thông báo trao đổi được bảo mật bằng K_ASME_D

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống truyền thông và, cụ thể hơn là, phương pháp và thiết bị xác thực các thiết bị, như nút chuyển tiếp và thiết bị truyền thông giữa máy với máy, dùng trong hệ thống truyền thông nối dây và/hoặc không dây.

Tình trạng kỹ thuật của sáng chế

Mạng không dây hiện đại có thể có các nút chuyển tiếp và/hoặc các thiết bị đầu cuối truy nhập, dưới đây gọi chung là thiết bị. Để thực hiện đúng chức năng thì thiết bị này thường được cung cấp/tạo cấu hình có chứng nhận an toàn hoạt động và thuê bao trước khi thiết bị được đưa vào hoạt động. Chứng nhận an toàn thuê bao có thể được dùng để, ví dụ, xác thực thiết bị trước khi cho phép truy nhập hoặc cung cấp dịch vụ không dây và, trong một số trường hợp, chứng nhận an toàn thuê bao có thể được lưu trữ trong môđun kết nối không tháo lắp được với thiết bị chủ của nó. Có nguy cơ xảy ra trường hợp chứng nhận an toàn thuê bao có thể bị gỡ ra khỏi thiết bị đã được xác thực và lắp vào thiết bị không được phép. Đối với nút chuyển tiếp, cách làm này có thể tạo cho nút chuyển tiếp không được phép lén lút truyền yêu cầu truy nhập, ví dụ, giữa nút truy nhập và một hoặc nhiều thiết bị đầu cuối truy nhập và/hoặc truy nhập tự do vào các dịch vụ trên mạng. Nguy cơ hoặc điểm yếu này cũng xuất hiện ở các thiết bị truyền thông giữa máy với máy (*M2M: Machine-to-Machine*), trong đó chứng nhận thuê bao hợp lệ (ví dụ, các thông số giao thức thoả thuận xác thực và khoá (*AKA: Authentication and Key Agreement*) trong thẻ mạch tích hợp đa năng (*UICC: Universal Integrated Circuit Card*)) tháo lắp được ở thiết bị M2M có thể được chuyển sang thiết bị khác để có thể truy nhập tự do vào mạng. Điểm yếu liên quan ở đây là không cần phải truy nhập vật lý vào chính thiết bị M2M đó. Chỉ cần truy nhập dữ liệu (ví dụ, khoá an toàn thu được từ thủ tục xác thực) thông qua giao diện thiết bị M2M (ví dụ, giao diện thiết bị chủ với thẻ UICC) là có thể truy nhập khoá an toàn và lấy ra dữ liệu được bảo mật bằng khoá này.

Vấn đề tương tự xảy ra khi nhà điều hành muốn kiểm soát các thiết bị được phép truy nhập vào mạng của họ.

Do đó, cần có biện pháp an toàn bổ sung cho các thiết bị nhằm khắc phục những

điểm yếu và nguy cơ nêu trên và cả những điểm yếu và nguy cơ khác.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp và thiết bị bảo mật cho thiết bị bằng cách kết hợp xác thực thuê bao và xác thực thiết bị để tạo ra khoá an toàn.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp xác thực hoạt động trong thiết bị để kết hợp xác thực thuê bao và xác thực thiết bị. Thiết bị có thể bắt đầu bằng cách truyền yêu cầu kết nối đến thực thể mạng, yêu cầu kết nối này có thông tin chỉ báo về khả năng xác thực thiết bị của thiết bị. Thiết bị có thể thực hiện thủ tục xác thực thuê bao với thực thể mạng. Ví dụ, thủ tục xác thực thuê bao có thể dựa vào sự trao đổi thoả thuận xác thực và khoá giữa thiết bị và thực thể mạng. Thiết bị cũng có thể thực hiện thủ tục xác thực thiết bị với thực thể mạng. Ví dụ, thủ tục xác thực thiết bị có thể dựa vào sự trao đổi hỏi-đáp giữa thiết bị và thực thể mạng.

Khoá an toàn có thể được tạo ra để kết hợp xác thực thuê bao và xác thực thiết bị. Khoá an toàn có thể được tạo ra dưới dạng hàm số của ít nhất là khoá thứ nhất thu được từ thủ tục xác thực thuê bao và khoá thứ hai thu được từ thủ tục xác thực thiết bị. Ngoài ra, khoá an toàn cũng có thể là hàm số của số hiện tại (nonce) của mạng và số hiện tại của thiết bị. Sau đó, khoá an toàn này có thể được dùng để bảo mật thông tin truyền thông giữa thiết bị và mạng phục vụ. Lưu ý rằng, khoá an toàn có thể được tạo ra riêng biệt bằng thiết bị và thực thể mạng, vì vậy khoá an toàn không được truyền trên mạng vô tuyến.

Theo một phương án thực hiện, thủ tục xác thực thuê bao có thể được thực hiện bằng máy chủ xác thực thứ nhất là một phần của thực thể mạng, trong khi thủ tục xác thực thiết bị có thể được thực hiện bằng máy chủ xác thực thứ hai là một phần của thực thể mạng.

Theo một phương án làm ví dụ, thủ tục xác thực thiết bị có thể được thực hiện bằng cách sử dụng khoá bí mật dùng chung để mã hoá/giải mã một số thông tin trao đổi giữa thiết bị và thực thể mạng. Theo phương án khác làm ví dụ, thủ tục xác thực thiết bị có thể được thực hiện bằng cách: (a) thu dữ liệu từ thực thể mạng, dữ liệu này được mã hoá bằng khoá công cộng của thiết bị; (b) sử dụng khoá riêng tương ứng để giải mã dữ liệu đã mã hoá; và/hoặc (c) sau đó chứng minh cho thực thể mạng thấy là thiết bị đã biết

dữ liệu này.

Theo một khía cạnh, thủ tục xác thực thiết bị có thể được bảo mật bằng ít nhất một khoá được tạo ra khi xác thực thuê bao.

Theo các phương án thực hiện, thủ tục xác thực thuê bao và thủ tục xác thực thiết bị có thể được thực hiện đồng thời trong quá trình trao đổi thông báo kết hợp hoặc thủ tục xác thực thuê bao có thể được thực hiện trong quá trình trao đổi thông tin an toàn tách biệt và trước khi xác thực thiết bị.

Theo một phương án, khoá dành cho thuê bao có thể được tạo ra trên thiết bị như là một phần của thoả thuận dịch vụ, trong đó khoá dành cho thuê bao được dùng để xác thực thuê bao. Tương tự, khoá dành cho thiết bị có thể được tạo ra trên thiết bị trong quá trình sản xuất thiết bị, trong đó khoá dành cho thiết bị được dùng để xác thực thiết bị.

Theo một phương án thực hiện, thiết bị có thể là nút chuyển tiếp đóng vai trò là thiết bị đầu cuối truy nhập đối với thực thể mạng và đóng vai trò là thiết bị mạng đối với một hoặc nhiều thiết bị đầu cuối truy nhập. Theo phương án thực hiện khác, thiết bị có thể là thiết bị đầu cuối truy nhập.

Theo một phương án làm ví dụ, thiết bị có thể có giao diện truyền thông kết nối với mạch xử lý. Mạch xử lý có thể được làm thích ứng để: (a) thực hiện thủ tục xác thực thuê bao với thực thể mạng; (b) thực hiện thủ tục xác thực thiết bị cho thiết bị với thực thể mạng; (c) tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị; và/hoặc (d) sử dụng khoá an toàn này để bảo mật thông tin truyền thông giữa thiết bị và mạng phục vụ.

Theo phương án khác làm ví dụ, sáng chế đề xuất vật ghi đọc được bằng bộ xử lý để lưu trữ các lệnh hoạt động trên thiết bị. Khi được thi hành bằng bộ xử lý, các lệnh này có thể ra lệnh cho bộ xử lý: (a) thực hiện thủ tục xác thực thuê bao với thực thể mạng; (b) thực hiện thủ tục xác thực thiết bị cho thiết bị với thực thể mạng; (c) tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị; và/hoặc (d) sử dụng khoá an toàn này để bảo mật thông tin truyền thông giữa thiết bị và mạng phục vụ.

Theo khía cạnh khác, sáng chế đề xuất phương pháp xác thực hoạt động trong thực thể mạng. Thực thể mạng có thể thu yêu cầu kết nối từ thiết bị, yêu cầu kết nối này

có thông tin chỉ báo về khả năng xác thực thiết bị của thiết bị. Thực thể mạng có thể thực hiện thủ tục xác thực thuê bao với thiết bị. Tương tự, thực thể mạng có thể thực hiện thủ tục xác thực thiết bị cho thiết bị. Khoá an toàn có thể được tạo ra bằng thực thể mạng để kết hợp xác thực thuê bao và xác thực thiết bị. Sau đó, khoá an toàn này có thể được dùng để bảo mật thông tin truyền thông giữa thực thể mạng và thiết bị. Lưu ý rằng, để không phải truyền khoá an toàn trên mạng vô tuyến, thì khoá an toàn có thể được tạo ra riêng biệt bằng thiết bị và thực thể mạng.

Theo một phương án làm ví dụ, thủ tục xác thực thuê bao có thể dựa vào sự trao đổi thoả thuận xác thực và khoá giữa thực thể mạng và thiết bị. Thủ tục xác thực thiết bị có thể dựa vào sự trao đổi hỏi-đáp giữa thực thể mạng và thiết bị.

Theo một phương án thực hiện, thủ tục xác thực thiết bị có thể bao gồm các bước: (a) thu chứng nhận từ thiết bị; và (b) kiểm tra chứng nhận đi kèm với thiết bị chưa bị thu hồi.

Theo một phương án thực hiện, để tránh bị đánh cắp thông tin trong lúc xác thực thiết bị, thủ tục xác thực thiết bị có thể được bảo mật bằng ít nhất một khoá được tạo ra trong thủ tục xác thực thuê bao trước đó.

Theo các phương án làm ví dụ, thủ tục xác thực thuê bao và thủ tục xác thực thiết bị có thể được thực hiện đồng thời trong quá trình trao đổi thông báo kết hợp hoặc thủ tục xác thực thuê bao được thực hiện trong quá trình trao đổi thông tin an toàn tách biệt và trước khi xác thực thiết bị.

Theo phương án khác làm ví dụ, khoá an toàn có thể được tạo ra dưới dạng hàm số của ít nhất là khoá thứ nhất thu được từ thủ tục xác thực thuê bao và khoá thứ hai thu được từ thủ tục xác thực thiết bị.

Theo một phương án thực hiện, thực thể mạng có thể thu được khoá dành cho thuê bao như là một phần của thoả thuận dịch vụ, khoá dành cho thuê bao được dùng để xác thực thuê bao. Tương tự, thực thể mạng có thể thu được khoá dành cho thiết bị của thiết bị, khoá dành cho thiết bị được dùng để xác thực thiết bị.

Theo một phương án thực hiện, thực thể mạng có thể có giao diện truyền thông kết nối với mạch xử lý. Mạch xử lý có thể được làm thích ứng để: (a) thực hiện thủ tục

xác thực thuê bao với thiết bị; (b) thực hiện thủ tục xác thực thiết bị cho thiết bị; (c) tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị; và/hoặc (d) sử dụng khoá an toàn này để bảo mật thông tin truyền thông giữa thực thể mạng và thiết bị.

Theo một phương án thực hiện, sáng chế đề xuất vật ghi đọc được bằng bộ xử lý để lưu trữ các lệnh hoạt động trên thực thể mạng. Khi được thi hành bằng bộ xử lý, các lệnh này có thể ra lệnh cho bộ xử lý: (a) thực hiện thủ tục xác thực thuê bao với thiết bị; (b) thực hiện thủ tục xác thực thiết bị cho thiết bị; (c) tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị; và/hoặc (d) sử dụng khoá an toàn này để bảo mật thông tin truyền thông giữa thực thể mạng và thiết bị.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ khối thể hiện hệ thống truyền thông không dây trong đó nhiều loại thiết bị không dây khác nhau có thể được xác thực bằng mạng lõi để nhận được dịch vụ.

Fig.2 thể hiện giải pháp chung để kết hợp xác thực thiết bị và xác thực thuê bao.

Fig.3 (gồm Fig.3A và Fig.3B) thể hiện ví dụ về cách thức có thể sửa đổi cấu trúc phân cấp khoá dựa vào thủ tục xác thực thuê bao để bổ sung thủ tục xác thực thiết bị.

Fig.4 thể hiện cấu trúc giao thức làm ví dụ có thể được sử dụng trên thiết bị hoạt động trong mạng chuyển mạch gói.

Fig.5 là sơ đồ khối thể hiện hệ thống mạng trong đó có thể tạo ra khoá xác thực và/hoặc khoá an toàn thể hiện trên Fig.3 và Fig.4.

Fig.6 là sơ đồ khối thể hiện các bộ phận được chọn trong thiết bị không dây có thể được làm thích ứng để kết hợp xác thực thuê bao và xác thực thiết bị.

Fig.7 là lưu đồ thể hiện ví dụ về phương pháp xác thực hoạt động trong thiết bị không dây để tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị.

Fig.8 là sơ đồ khối thể hiện các bộ phận được chọn trong thực thể mạng có thể được làm thích ứng để kết hợp xác thực thuê bao và xác thực thiết bị.

Fig.9 là lưu đồ thể hiện ví dụ về phương pháp xác thực hoạt động trong thực thể mạng để tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị.

Fig.10 thể hiện phương pháp thứ nhất làm ví dụ để tạo ra khoá an toàn bằng cách

kết hợp xác thực thuê bao và xác thực thiết bị.

Fig.11 thể hiện phương pháp thứ hai làm ví dụ để tạo ra khoá an toàn bằng cách kết hợp xác thực thuê bao và xác thực thiết bị.

Fig.12 thể hiện phương pháp thứ ba làm ví dụ để tạo ra khoá an toàn bằng cách kết hợp xác thực thuê bao và xác thực thiết bị.

Mô tả chi tiết sáng chế

Trong phần mô tả dưới đây, những chi tiết cụ thể được đưa ra để giúp người đọc hiểu rõ các phương án thực hiện được mô tả trong sáng chế. Tuy nhiên, người có hiểu biết trung bình về lĩnh vực kỹ thuật này sẽ hiểu rằng có thể thực hiện nhiều phương án khác nhau mà không cần phải có những chi tiết cụ thể đó. Ví dụ, các mạch xử lý có thể được thể hiện dưới dạng sơ đồ khối để tránh làm rối sáng chế vì những chi tiết không cần thiết. Trong các trường hợp khác, mạch xử lý, cấu trúc và kỹ thuật đã biết có thể không được thể hiện chi tiết để tránh làm rối phương án thực hiện được mô tả trong sáng chế.

Cụm từ "làm ví dụ" được sử dụng trong bản mô tả này để chỉ việc "dùng làm mẫu, làm ví dụ, hoặc minh hoạ". Một phương án thực hiện hoặc phương án bất kỳ nêu trong bản mô tả này dưới dạng "làm ví dụ" thì không nhất thiết phương án thực hiện hoặc phương án đó phải được coi là sẽ được ưu tiên hoặc có ưu điểm hơn so với phương án thực hiện hoặc phương án khác. Tương tự, thuật ngữ "các phương án" không có nghĩa rằng tất cả các phương án đều phải có dấu hiệu, ưu điểm hoặc chế độ hoạt động như được mô tả.

Mô tả khái quát

Sáng chế đề xuất phương pháp xác thực giữa thiết bị (ví dụ, thiết bị khách hoặc thiết bị đầu cuối truy nhập) và thực thể mạng. Thiết bị lưu trữ tháo lắp được có thể được kết nối với thiết bị và lưu trữ khoá dành cho thuê bao được dùng để xác thực thuê bao. Thiết bị lưu trữ an toàn có thể được kết nối với thiết bị và lưu trữ khoá dành cho thiết bị được dùng để xác thực thiết bị. Thủ tục xác thực thuê bao có thể được thực hiện giữa thiết bị và thực thể mạng. Thủ tục xác thực thiết bị cũng có thể được thực hiện giữa thiết bị và thực thể mạng. Khoá an toàn có thể được tạo ra để kết hợp xác thực thuê bao và xác thực thiết bị. Có nghĩa là, khoá, dữ liệu và/hoặc thông tin từ thủ tục xác thực thuê bao và

khoá, dữ liệu và/hoặc thông tin từ thủ tục xác thực thiết bị có thể được kết hợp để tạo ra khoá an toàn (kết hợp). Khoá an toàn này có thể được dùng để bảo mật thông tin truyền thông giữa thiết bị và mạng phục vụ.

Môi trường mạng làm ví dụ

Fig.1 là sơ đồ khối thể hiện hệ thống truyền thông không dây trong đó nhiều loại thiết bị không dây khác nhau có thể được xác thực bằng mạng lõi để nhận được dịch vụ. Hệ thống truyền thông không dây này có thể là, ví dụ, mạng tương thích hoặc mạng tuân theo tiêu chuẩn hệ thống viễn thông di động đa năng (*UMTS: Universal Mobile Telecommunications System*) hoặc mạng tương thích với hệ thống viễn thông di động toàn cầu (*GSM: Global System for Mobile communication*). Mặc dù một số ví dụ được mô tả trong sáng chế có thể đề cập đến mạng theo công nghệ phát triển dài hạn (*LTE: Long Term Evolution*), nhưng các dấu hiệu nêu trong sáng chế cũng có thể được áp dụng cho các mạng khác.

Hệ thống có thể có một hoặc nhiều thiết bị 101, như thiết bị đầu cuối truy nhập 103/104 và nút chuyển tiếp 102, các thiết bị này truyền thông với nút truy nhập 106. Nút chuyển tiếp 102 có thể tạo điều kiện thuận lợi để truyền tín hiệu không dây giữa mạng truyền thông không dây 106/108 và một hoặc nhiều thiết bị đầu cuối truy nhập 104. Hệ thống truyền thông không dây (ví dụ, mạng theo công nghệ phát triển dài hạn (LTE), mạng LTE-cải tiến, v.v.) có thể có mạng lõi 108 và một hoặc nhiều nút truy nhập 106. Nút truy nhập 106 có thể được kết nối với mạng lõi 108 thông qua liên kết hành trình ngược (ví dụ, liên kết nối dây). Mạng lõi 108 có thể bao gồm, ví dụ, thực thể quản lý di động (*MME: Mobile Management Entity*) 110, máy chủ thuê bao thường trú (*HSS: Home Subscriber Server*) 112 và/hoặc các thành phần khác.

Theo một phương án làm ví dụ, thực thể quản lý di động (MME) 110 có thể có nhiệm vụ kích hoạt/khử kích hoạt kênh vận chuyển cho thiết bị 101, nút chuyển tiếp 102, và/hoặc thiết bị đầu cuối truy nhập 103/104 (dưới đây gọi chung là "thiết bị") và hỗ trợ cho thủ tục xác thực bằng cách tương tác với máy chủ thuê bao thường trú (HSS) 112. Thực thể MME 110 cũng có thể tạo ra và/hoặc phân định ký hiệu nhận dạng tạm thời cho các thiết bị (ví dụ, thiết bị 101, nút chuyển tiếp 102, thiết bị đầu cuối truy nhập 103/104, v.v.). Thực thể này có thể kiểm tra quyền được phép lưu trú của thiết bị (ví dụ, thu nhận

dịch vụ từ, kết nối với, thiết lập liên kết truyền thông với) trong mạng công cộng mặt đất di động (*PLMN: Public Land Mobile Network*) của nhà cung cấp dịch vụ và có thể áp đặt các điều kiện hạn chế chuyển vùng đối với thiết bị. Thực thể MME 110 có thể là điểm kết thúc trong mạng để mã hoá/bảo vệ tính nguyên vẹn cho tín hiệu báo hiệu tầng không truy nhập (*NAS: Non Access Stratum*) và thực hiện chức năng quản lý khoá an toàn. Thực thể MME 110 cũng có thể thực hiện thủ tục giám sát và/hoặc nhắn tin (kể cả truyền lại) đối với các thiết bị kết nối với mạng lõi 108.

Máy chủ thuê bao thường trú (HSS) 112 là cơ sở dữ liệu thuê bao chính để hỗ trợ các thực thể mạng quản lý các thiết bị trên thực tế. Cơ sở dữ liệu này có thể chứa thông tin liên quan đến thuê bao (các profin thuê bao), hỗ trợ thực hiện thủ tục xác thực và cấp phép cho thuê bao, và có thể cung cấp thông tin về vị trí của thuê bao. Máy chủ thuê bao thường trú tương tự như bộ đăng ký vị trí thường trú (*HLR: Home Location Register*) trong hệ thống GSM và trung tâm xác thực (*AuC: Authentication Centre*). Bộ đăng ký vị trí thường trú (HLR) có thể là cơ sở dữ liệu chứa thông tin chi tiết của mỗi thuê bao được phép sử dụng mạng lõi. HLR có thể hỗ trợ AuC trong việc xác thực các thuê bao (tức là, sử dụng các thiết bị đầu cuối người dùng).

Nút chuyển tiếp 102 có thể được làm thích ứng để khuếch đại và/hoặc chuyển tiếp tín hiệu giữa thiết bị đầu cuối truy nhập 104 và nút truy nhập 106. Thông thường, nút chuyển tiếp 102 có thể đóng vai trò là nút truy nhập (*AN: Access Node*) đối với thiết bị đầu cuối truy nhập 104 và có thể đóng vai trò là thiết bị đầu cuối truy nhập (*AT: Access Terminal*) đối với nút truy nhập 106. Ví dụ, nút chuyển tiếp 102 có thể có giao diện thiết bị đầu cuối truy nhập 105 để truyền thông với nút truy nhập 106 và có thể còn có giao diện nút truy nhập 107 để truyền thông với thiết bị đầu cuối truy nhập 104. Có nghĩa là, giao diện thiết bị đầu cuối truy nhập 105 có thể làm cho nút chuyển tiếp trở thành thiết bị đầu cuối truy nhập đối với nút truy nhập 106. Tương tự, giao diện nút truy nhập 107 có thể làm cho nút chuyển tiếp 102 trở thành nút truy nhập đối với thiết bị đầu cuối truy nhập 104. Theo một số phương án thực hiện, nút chuyển tiếp 102 có thể chuyển đổi tín hiệu từ định dạng thứ nhất sang định dạng thứ hai giữa giao diện thiết bị đầu cuối truy nhập 105 và giao diện nút truy nhập 107. Nút chuyển tiếp 102 có thể được đặt ở gần biên của ô để cho thiết bị đầu cuối truy nhập 104 có thể truyền thông với nút chuyển tiếp 102 thay vì truyền thông trực tiếp với nút truy nhập 106.

Trong hệ thống truyền thông vô tuyến, ô là vùng địa lý phủ sóng thu phát. Các ô có thể chồng lấn lên nhau. Thường là có một nút truy nhập được liên hệ với mỗi ô. Phạm vi của ô được xác định bởi các yếu tố như dải tần số, mức công suất và các điều kiện kênh. Các nút chuyển tiếp, như nút chuyển tiếp 102, có thể được dùng để cải thiện vùng phủ sóng bên trong hoặc ở gần ô, hoặc mở rộng phạm vi phủ sóng của ô. Ngoài ra, việc sử dụng nút chuyển tiếp 102 có thể nâng cao năng suất truyền tín hiệu trong ô vì thiết bị đầu cuối truy nhập 104 có thể truy nhập nút chuyển tiếp 102 ở tốc độ dữ liệu cao hơn hoặc công suất truyền thấp hơn so với trường hợp thiết bị đầu cuối truy nhập 104 truyền thông trực tiếp với nút truy nhập 106 trong ô đó. Việc truyền tín hiệu ở tốc độ dữ liệu cao hơn tạo ra hiệu suất phổ cao hơn, và công suất truyền thấp hơn có lợi cho thiết bị đầu cuối truy nhập 104 vì, ví dụ, mức tiêu thụ năng lượng pin ít hơn.

Theo một số phương án làm ví dụ, nút chuyển tiếp 102 có thể được thực hiện dưới dạng là một trong ba loại nút chuyển tiếp sau đây: nút chuyển tiếp một tầng, nút chuyển tiếp hai tầng, và/hoặc nút chuyển tiếp ba tầng. Nút chuyển tiếp một tầng chủ yếu là bộ chuyển tiếp có thể truyền lại tín hiệu truyền mà không có thay đổi gì khác ngoài khuếch đại và có độ trễ nhỏ. Nút chuyển tiếp hai tầng có thể giải mã tín hiệu truyền mà nó thu nhận được, mã hoá lại tín hiệu đã được giải mã, và sau đó truyền dữ liệu đã được mã hoá lại. Nút chuyển tiếp ba tầng có thể có đầy đủ các khả năng điều khiển tài nguyên vô tuyến và do đó có thể thực hiện chức năng tương tự như nút truy nhập. Các giao thức điều khiển tài nguyên vô tuyến dùng cho nút chuyển tiếp có thể giống như các giao thức dùng cho nút truy nhập, và nút chuyển tiếp có thể có ký hiệu nhận dạng ô duy nhất thường dùng cho nút truy nhập. Nhằm mục đích của sáng chế, nút chuyển tiếp 102 được phân biệt với nút truy nhập 106 là vì nút chuyển tiếp 102 có thể dựa vào sự có mặt của ít nhất một nút truy nhập 106 (và ô liên quan đến nút truy nhập đó) hoặc nút chuyển tiếp khác để truy nhập vào các thành phần khác trong hệ thống viễn thông (ví dụ, mạng 108). Có nghĩa là, nút chuyển tiếp 102 có thể đóng vai trò là thiết bị thuê bao, thiết bị khách, hoặc thiết bị đầu cuối truy nhập đối với mạng, do đó nó kết nối với nút truy nhập để truyền thông trên mạng 108. Tuy nhiên, đối với thiết bị thuê bao, thiết bị người dùng, và/hoặc thiết bị đầu cuối truy nhập 104 khác, nút chuyển tiếp 102 có thể đóng vai trò là thiết bị mạng (ví dụ, nút truy nhập). Vì vậy, nút chuyển tiếp 102 có thể sử dụng một hoặc nhiều giao diện truyền thông để truyền thông với nút truy nhập và/hoặc một hay nhiều

thiết bị đầu cuối truy nhập/thuê bao/người dùng. Theo một phương án làm ví dụ, cùng một bộ truyền/thu (ví dụ, trên một hoặc nhiều kênh không dây) có thể được nút chuyển tiếp 102 sử dụng để truyền thông với nút truy nhập và/hoặc một hay nhiều thiết bị đầu cuối truy nhập của nó. Theo phương án khác làm ví dụ, nút chuyển tiếp 102 có thể sử dụng hai hay nhiều bộ truyền/thu khác nhau để truyền thông với nút truy nhập và/hoặc một hay nhiều thiết bị đầu cuối truy nhập.

Nhằm giảm bớt việc sử dụng trái phép thuê bao để truy nhập các dịch vụ mạng, thiết bị có thể kết hợp xác thực thiết bị với xác thực thuê bao. Thủ tục xác thực thiết bị có thể được thực hiện cùng với, ví dụ, thủ tục xác thực truy nhập AKA (thoả thuận xác thực và khoá) theo tiêu chuẩn 3GPP dựa vào chứng nhận (như khoá *subscriber_root_key* K) được lưu trữ trên thẻ mạch tích hợp đa năng (UICC) 109, 111, 113 và 116 hoặc môđun nhận dạng thuê bao đa năng (*USIM: Universal Subscriber Identification Module*) được kết nối tháo lắp được với thiết bị. Theo một số phương án, thủ tục xác thực thiết bị có thể được thực hiện trong các thông báo ở tầng không truy nhập (NAS) giống như các thông báo được dùng để xác thực AKA. Theo cách này, thiết bị (ví dụ, nút chuyển tiếp 102, thiết bị đầu cuối truy nhập 103/104, v.v.) có thể được kết hợp với thuê bao của nó (tức là, thuê bao dịch vụ với mạng lõi 108) để ngăn không cho người khác sử dụng chứng nhận thuê bao của nó (tức là, đối với dịch vụ thuê bao) trên thiết bị không được phép.

Một giải pháp đối phó với nguy cơ sử dụng trái phép chứng nhận thuê bao là để cho thiết bị (ví dụ, thiết bị 101, nút chuyển tiếp 102 hoặc thiết bị đầu cuối truy nhập 103/104) và thẻ UICC 109 xác thực lẫn nhau (ví dụ, sử dụng kênh an toàn giữa thiết bị chủ và thẻ UICC), nhưng có thể cần phải cung cấp trước cho thẻ UICC 109, 111, 113 và 116 và/hoặc thiết bị chủ (ví dụ, thiết bị 101, nút chuyển tiếp 102 hoặc thiết bị đầu cuối truy nhập 103/104) thông tin để thực hiện thủ tục xác nhận lẫn nhau.

Một giải pháp khác là có thể cần phải dùng khoá để truy nhập mạng (ví dụ, các khoá được dùng để bảo vệ dữ liệu lưu lượng giữa thiết bị và mạng) phụ thuộc vào cả chứng nhận được lưu trữ trên thẻ UICC 109, 111, 113 và 116 lẫn chứng nhận được lưu trữ trên thiết bị (ví dụ, thiết bị 101, nút chuyển tiếp 102 hoặc thiết bị đầu cuối truy nhập 103/104). Giải pháp này có thể được thực hiện bằng cách kết hợp khoá xác thực AKA với khoá xác thực thiết bị theo một cách nào đó. Giải pháp này cũng được sử dụng trong

trường hợp xác thực số nhận dạng thiết bị di động quốc tế (*IMEI: International Mobile Equipment Identity*) (ví dụ, số nhận dạng này có thể cho phép nhà điều hành ngăn chặn những thiết bị không được phép tấn công mạng của họ). Sở dĩ như vậy là vì, nhờ kết hợp (các) khoá thu được từ thủ tục xác thực AKA dùng để truy nhập mạng với khoá dùng để xác thực thiết bị, nên sẽ bảo đảm là tất cả các thông báo từ thiết bị đến mạng 108 thực sự phát đi từ thiết bị đã được xác thực. Giả sử là, các khoá kết hợp (và tất cả những khoá khác được tìm ra sau đó từ khoá kết hợp) được lưu trữ an toàn trên thiết bị (ví dụ, thiết bị 101, nút chuyển tiếp 102 hoặc thiết bị đầu cuối truy nhập 103/104), việc kết hợp khoá xác thực AKA với khoá xác thực thiết bị tạo ra độ an toàn cao hơn so với việc chỉ sử dụng mỗi cơ chế dựa vào hỏi/đáp để xác thực thiết bị. Việc chỉ sử dụng mỗi cơ chế hỏi/đáp để xác thực thiết bị chỉ chứng tỏ rằng thiết bị có mặt để tạo ra thông báo trả lời xác thực, nhưng không có nghĩa rằng nó vẫn có mặt ở thời điểm sau đó.

Fig.2 thể hiện giải pháp chung để kết hợp xác thực thiết bị và xác thực thuê bao. Thiết bị 202 (ví dụ, thiết bị 101, nút chuyển tiếp 102 hoặc thiết bị đầu cuối truy nhập 103/104) có thể được cung cấp *subscriber_root_key* 206 và/hoặc *subscriber_identity* 207 dùng để xác thực thuê bao với mạng lõi 108 và/hoặc tạo ra các khoá an toàn dùng để truy nhập dữ liệu lưu lượng mã hoá truyền đến thiết bị 202. Khoá *subscriber_root_key* 206 có thể được liên hệ duy nhất với *subscriber_identity* 207. Theo một phương án làm ví dụ, *subscriber_root_key* 206 và/hoặc *subscriber_identity* 207 có thể được lưu trữ trên thẻ UICC 204 và/hoặc thủ tục xác thực thuê bao có thể được xử lý bằng thẻ UICC 204. Tương tự, thiết bị 202 có thể được cung cấp (hoặc lưu trữ) *device_root_key* 208 và/hoặc *device_identity* 209 dùng để xác thực thiết bị với mạng lõi 108. Khoá *device_root_key* 208 có thể được liên hệ duy nhất với *device_identity* 209.

Theo một phương án làm ví dụ, *device_identity* 209 có thể là số nhận dạng thiết bị di động quốc tế (IMEI) của thiết bị 202 (ví dụ, thiết bị 101, nút chuyển tiếp 102 hoặc thiết bị đầu cuối truy nhập 103/104), tuy nhiên những dạng thức khác của số nhận dạng liên hệ với thiết bị (ví dụ, địa chỉ phần cứng theo tiêu chuẩn IEEE như EUI-48 hoặc EUI-64) cũng có thể được sử dụng.

Theo một số phương án thực hiện, *device_root_key* 208 có thể là khoá bí mật chỉ dùng chung cho thiết bị 202 và mạng lõi 108 nên không được truyền trên mạng vô tuyến.

Device_identity 209 có thể được thiết bị 202 truyền đến mạng lõi 108 để thu được *device_root_key* chính xác sẽ dùng để xác thực thiết bị. Theo cách khác, *device_root_key* 208 có thể là khoá công cộng trong cặp khoá công cộng/khoá riêng, trong đó chứng nhận được dùng để xác thực thiết bị. Ví dụ, thiết bị có thể thu một số dữ liệu từ mạng, trong đó dữ liệu này được mã hoá bằng khoá công cộng. Thiết bị có thể sử dụng khoá riêng của nó để giải mã dữ liệu đã mã hoá và sau đó chứng minh cho mạng thấy là thiết bị đã biết dữ liệu này. Chứng nhận (ví dụ, *device_credentials*) có thể được kiểm tra bằng mạng lõi 108. Khoá riêng đi kèm của thiết bị 202 có thể được lưu trữ an toàn trên thiết bị 202. *Device_credentials* có thể dùng để chỉ chứng nhận thiết bị hoặc con trỏ chỉ đến chứng nhận thiết bị. *Device_credentials* có thể cho phép thực thể mạng thích hợp tạo ra thông báo *device_challenge* và kiểm tra tình trạng thu hồi của thiết bị 202 (ví dụ, kiểm tra xem chứng nhận như khoá riêng hoặc khoá dùng chung đi kèm với thiết bị có bị xâm phạm hay không). Giả sử thêm là, phần an toàn của thiết bị (như môi trường tin cậy, viết tắt là TrE (*Trusted Environment*), như được xác định trong đặc tả kỹ thuật 3GPP Technical Specification 33.320) lưu trữ các khoá thiết bị nhạy cảm, như *device_root_key* và/hoặc khoá riêng liên quan đến chứng nhận. Ngoài ra, giả sử là, môi trường TrE thực hiện tất cả các thao tác mã hoá sử dụng các khoá này.

Ban đầu, thủ tục xác thực thuê bao có thể tiến hành giữa thiết bị 202 và mạng 108. Ví dụ, sự trao đổi thoả thuận xác nhận và khoá (AKA) 210 giữa thiết bị 202 và mạng 108 có thể dẫn đến việc thiết lập khoá *K_ASME*. Sự trao đổi AKA 210 có thể dựa vào, ví dụ, khoá *subscriber_root_key* 206 và/hoặc *subscriber_identity* 207 để xác thực thuê bao liên quan đến thiết bị 202. Ví dụ, thông tin thuê bao hoặc chứng nhận đó có thể được lưu trữ an toàn trên thẻ UICC 204 kết nối tháo lắp được với thiết bị chủ 202.

Mạng 108 cũng có thể thực hiện thủ tục xác thực thiết bị cho thiết bị 202. *Device_identity* 209 có thể được thiết bị 202 cung cấp cho mạng lõi 108 để mạng lõi 108 có thể tra cứu hoặc thu được *device_root_key* 208 tương ứng chính xác. Mạng 108 có thể tạo ra thông báo *device_challenge* 212 và truyền thông báo này đến thiết bị 202 (ví dụ, dưới dạng là một phần của thông báo NAS thích hợp). Để đáp lại, thiết bị 202 tính *device_response* 214 (ví dụ, dựa vào *device_challenge* và *device_root_key* 208 hoặc giá trị tìm được từ đó) và gửi thông báo này ngược trở lại mạng 108. Thiết bị 202 có thể sử dụng dữ liệu trong thông báo *device_challenge* và *device_response* để tính khoá an toàn

kết hợp *K_ASME_D* 216. Lưu ý rằng, đối với thiết bị 202, khoá an toàn kết hợp *K_ASME_D* 216 có thể được tạo ra trước hoặc sau khi thông báo *device_response* 214 được gửi đi. Theo một phương án làm ví dụ, khoá an toàn kết hợp *K_ASME_D* có thể là khoá tương đương với khoá an toàn *K_ASME* được xác định trong mạng truy nhập vô tuyến mặt đất đa năng cải tiến (*E-UTRAN: Evolved Universal Terrestrial Radio Access Network*) theo quy định trong đặc tả kỹ thuật 3GPP Technical Specification 33.401, ngoại trừ việc khoá *K_ASME_D* được kết hợp với *device_identity* 209 và với khoá thu được từ thủ tục xác thực AKA, như khoá *K_ASME*. Nếu mạng 108 thu được thông báo *device_response* hợp lệ, thì mạng 108 cũng tính khoá an toàn kết hợp *K_ASME_D* 218.

Việc tính *device_challenge* 212, *device_response* 214 và khoá an toàn kết hợp *K_ASME_D* có thể được thực hiện như sau. *Device_challenge* 212 có thể được tính theo công thức:

device_challenge = *eKSI*, [*E_device_root_key*(*device_temp_key*)], *network_nonce*

trong đó *eKSI* là ký hiệu nhận dạng tập hợp khoá cải tiến/mở rộng sẽ được liên hệ với khoá *K_ASME_D*, [..] là tham số tuỳ chọn, *E_k* (dữ liệu) có nghĩa là dữ liệu được mã hoá bằng khoá *k*, và *network_nonce* là số ngẫu nhiên có độ dài thích hợp (ví dụ, 128-bit) được chọn bằng mạng. Thuật toán mã hoá có thể là thuật toán không đối xứng (trong trường hợp *device_root_key* là khoá công cộng liên quan đến chứng nhận thiết bị) hoặc là thuật toán đối xứng (trong trường hợp *device_root_key* là khoá dùng chung). *Device_temp_key* có thể là khoá thu được hoặc được tạo ra như là một phần của thủ tục xác thực thiết bị. Theo một phương án làm ví dụ, *device_temp_key* có thể được chọn (ví dụ, ngẫu nhiên) bằng mạng 108, được truyền đến thiết bị 202 ở dạng mã hoá, và có độ dài thích hợp (ví dụ, giá trị 256-bit hoặc 128-bit).

Thiết bị 202 và mạng 108 đều có thể duy trì khoá *device_temp_key* giữa những lần truy nhập mạng vì mục đích tối ưu hoá. Nếu không phải như vậy, thì tham số thứ hai ([*E_device_root_key* (*device_temp_key*)]) trong *device_challenge* 212 không còn là tham số tuỳ chọn nữa.

Device_response 214 có thể được tính theo công thức:

device_response = *device_nonce*, *device_res*,

trong đó *device_nonce* là số ngẫu nhiên có độ dài thích hợp (ví dụ, 128-bit) được chọn bằng thiết bị, và

$$device\_res = KDF(device\_temp\_key, network\_nonce, device\_nonce)$$

trong đó *KDF* là hàm mã hoá phù hợp để tạo ra thông báo trả lời *device_res*.

Vì trước đó đã thu được khoá xác thực *K_ASME* (ví dụ, là một phần của sự trao đổi AKA 210), nên việc tính khoá an toàn kết hợp *K_ASME_D* 216 và 218 (tức là, kết hợp xác thực thiết bị và xác thực thuê bao), có thể được thực hiện như sau:

$$K\_ASME\_D = KDF(device\_temp\_key, K\_ASME, network\_nonce, device\_nonce)$$

trong đó *K_ASME* có thể là khoá hoặc giá trị thu được khi xác thực thuê bao giữa thiết bị và mạng (theo sự trao đổi xác thực AKA 210). Theo một phương án làm ví dụ, khoá *K_ASME* có thể là khoá đã được tạo ra trước đó và/hoặc được sử dụng giữa thiết bị 202 và mạng 108. Theo cách khác, nếu thủ tục xác thực thiết bị 212 và 214 đang được thực hiện bằng cách sử dụng các thông báo NAS giống như các thông báo NAS dùng cho thủ tục xác thực AKA 210, thì khoá *K_ASME* có thể được tạo mới hoặc được tạo ra đồng thời. Tương tự, *device_temp_key* có thể là khoá hoặc giá trị thu được khi xác thực thiết bị giữa thiết bị 202 và mạng 108.

Sau đó, khoá an toàn kết hợp có thể được sử dụng làm cơ sở và/hoặc làm gốc để tính các khoá an toàn bổ sung 217 và 219. Các khoá an toàn bổ sung này có thể dùng để bảo mật, ví dụ, cho thông tin truyền thông ở tầng NAS và/hoặc tầng AS.

Khoá an toàn kết hợp *K_ASME_D*, các tham số an toàn liên quan, và toàn bộ các khoá thu được từ *K_ASME_D* có thể được lưu trữ an toàn trên thiết bị 202 và không được lưu trữ trên thẻ UICC 204. Khoá an toàn kết hợp *K_ASME_D* có thể được dùng để bảo mật các thông báo trao đổi 220 giữa thiết bị 202 và mạng lõi 108.

Fig.3 (gồm Fig.3A và Fig.3B) thể hiện ví dụ về cách thức có thể sửa đổi cấu trúc phân cấp khoá dựa vào thủ tục xác thực thuê bao để bổ sung thủ tục xác thực thiết bị. Cấu trúc phân cấp khoá có thể được sử dụng để thiết lập các tham số an toàn (ví dụ, khoá an toàn) dùng để mã hoá/giải mã thông tin truyền thông giữa thiết bị và mạng. Trong ví dụ này, thủ tục xác thực thuê bao và thiết bị có thể được thực hiện giữa thiết bị 322 và thực thể mạng 324. Thiết bị 322 có thể là, ví dụ, thiết bị đầu cuối truy nhập (AT), thiết bị

người dùng (UE), máy điện thoại di động, và/hoặc nút chuyển tiếp. Thực thể mạng 324 có thể là một hoặc nhiều thiết bị mạng, như thực thể quản lý di động (MME) và/hoặc máy chủ thuê bao thường trú (HSS).

Ví dụ này thể hiện cách thức có thể sửa đổi cấu trúc phân cấp khoá thứ nhất 300 dựa vào xác thực thuê bao để thu được cấu trúc phân cấp khoá thứ hai 300' dựa vào cả xác thực thuê bao lẫn xác thực thiết bị.

Vì mục đích xác thực thuê bao như được thể hiện trong cấu trúc phân cấp khoá thứ nhất 300, nên thẻ mạch tích hợp đa năng (UICC trong thiết bị 322) và thực thể mạng 324 (ví dụ, thực thể MME 110, máy chủ HSS 112 trên Fig.1, hoặc thực thể mạng khác) có thể sử dụng khoá chính K 302 để tạo ra khoá mật mã (*CK: Cipher Key*) 304 và khoá nguyên vẹn (*IK: Integrity Key*) 306. Sau đó, khoá mật mã (CK) 304 và khoá nguyên vẹn (IK) 306 có thể được sử dụng cho thiết bị 322 và thực thể mạng 324 như là một phần của sự trao đổi thoả thuận xác thực và khoá (AKA) để tạo ra khoá thực thể quản lý an toàn truy nhập *K_ASME* 308 (dưới đây còn gọi là khoá xác thực thuê bao). Việc kích hoạt an toàn của thiết bị 202 có thể được thực hiện thông qua thủ tục thoả thuận xác thực và khoá (AKA), thủ tục cấu hình chế độ an toàn tầng không truy nhập (*NAS SMC: Non-Access Stratum Security Mode Configuration*) và thủ tục cấu hình chế độ an toàn tầng truy nhập (*AS SMC: Access Stratum Security Mode Configuration*).

Trong ví dụ này, thủ tục xác thực thuê bao có thể có sự trao đổi AKA 326 để tạo ra khoá *K_ASME* 308. Sự trao đổi AKA 326 có thể có thông báo yêu cầu xác thực thuê bao 340 và thông báo trả lời xác thực thuê bao 342. Trong ví dụ này, thủ tục xác thực thuê bao để tạo ra khoá *K_ASME* 308 cũng có thể tạo ra các khoá liên quan ở tầng NAS (ví dụ, K_NAS-enc 305 và K_NAS-int 311) và/hoặc các khoá ở tầng AS (ví dụ, K_UP-enc 315, K_RRC-enc 317 và K_RRC-int 319). Lưu ý rằng, theo một số phương án thực hiện, nếu những phiên bản này của các khoá ở tầng NAS và các khoá ở tầng AS không được sử dụng, thì việc tạo ra các khoá đó có thể được thực hiện từ trước trong lúc xác thực thuê bao.

Cấu trúc phân cấp khoá thứ hai 300' thể hiện cách thức có thể kết hợp xác thực thiết bị với xác thực thuê bao để tạo ra các khoá an toàn ở tầng NAS và tầng AS. Cùng lúc, trước hoặc sau thủ tục xác thực thuê bao (và tạo ra khoá *K_ASME* 308 tương ứng

của nó), thủ tục xác thực thiết bị 328 có thể được thực hiện dựa, ít nhất một phần, vào khoá gốc dành cho thiết bị. Thủ tục xác thực thiết bị 328 có thể có thông báo yêu cầu xác thực thiết bị 344 và thông báo trả lời xác thực thiết bị 346. Theo một phương án thực hiện, thủ tục xác thực thiết bị 307 có thể độc lập với thủ tục xác thực thuê bao; chỉ khi cả hai thủ tục xác thực thuê bao và thiết bị đều được đáp ứng thì khoá an toàn kết hợp *K_ASME_D* 309 mới được tạo ra. Theo phương án thực hiện khác, thủ tục xác thực thiết bị có thể được thực hiện trước thủ tục xác thực thuê bao.

Khoá an toàn kết hợp *K_ASME_D* 309 có thể được dùng làm khoá cơ sở để tính, ví dụ, các khoá NAS (tầng không truy nhập) 310 và 312 và các khoá AS (tầng truy nhập) 314, 316, 318 và 320. Có nghĩa là, thiết bị 322 và thực thể mạng 324 có thể sử dụng khoá *K_ASME_D* 309 để tạo ra một hoặc nhiều khoá an toàn.

Các mạng chuyển mạch gói có thể có cấu trúc gồm nhiều tầng giao thức phân cấp, trong đó các tầng giao thức dưới cung cấp dịch vụ cho các tầng giao thức trên và mỗi tầng có trách nhiệm thực hiện các nhiệm vụ khác nhau. Ví dụ, Fig.4 thể hiện cấu trúc giao thức làm ví dụ có thể được sử dụng trên thiết bị hoạt động trong mạng chuyển mạch gói. Trong ví dụ này, cấu trúc giao thức 402 bao gồm tầng vật lý (*PHY: Physical*) 404, tầng điều khiển truy nhập phương tiện (*MAC: Media Access Control*) 406, tầng điều khiển liên kết vô tuyến (*RLC: Radio Link Control*) 408, tầng giao thức hội tụ dữ liệu gói (*PDCP: Packet Data Convergence Protocol*) 410, tầng điều khiển tài nguyên vô tuyến (*RRC: Radio Resource Control*) 412, tầng không truy nhập (*NAS: Non-Access Stratum*) 414 và tầng ứng dụng (*APP: Application*) 416.

Các tầng ở phía dưới tầng NAS 414 thường được gọi là tầng truy nhập (*AS: Access Stratum*) 418. Tầng RLC 408 có thể có một hoặc nhiều kênh 420. Tầng RRC 412 có thể thực hiện các chế độ giám sát khác nhau đối với thiết bị đầu cuối truy nhập, kể cả trạng thái kết nối và trạng thái rỗi. Tầng không truy nhập (NAS) 414 có thể duy trì ngữ cảnh quản lý di động đối với thiết bị truyền thông, ngữ cảnh dữ liệu gói và/hoặc các địa chỉ IP của nó. Lưu ý rằng, các tầng khác có thể có mặt trong cấu trúc giao thức 402 (ví dụ, ở trên, ở dưới và/hoặc ở giữa các tầng được thể hiện trên hình vẽ), nhưng để cho dễ hiểu, trên hình vẽ không thể hiện các tầng đó.

Trên Fig.4, kênh vô tuyến/phiên 422 có thể được thiết lập, ví dụ ở tầng RRC 412

và/hoặc tầng NAS 414. Do đó, tầng NAS 414 có thể được thiết bị 202 và mạng lõi 108 sử dụng để tạo ra khoá an toàn K_NAS-enc 310 và K_NAS-int 312 thể hiện trên Fig.3. Tương tự, tầng RRC 412 có thể được thiết bị 202 và nút truy nhập 108 sử dụng để tạo ra khoá an toàn ở tầng truy nhập (AS) K_UP-enc 316, K_RRC-enc 318 và K_RRC-int 320. Mặc dù khoá an toàn K_UP-enc 316, K_RRC-enc 318 và K_RRC-int 320 có thể được tạo ra ở tầng RRC 312, nhưng các khoá này có thể được tầng PDCP 410 sử dụng để bảo mật cho tín hiệu báo hiệu và/hoặc thông tin truyền thông ở mặt phẳng người dùng/dữ liệu. Ví dụ, khoá K_UP-enc 316 có thể được tầng PDCP 410 sử dụng để bảo mật cho thông tin truyền thông ở mặt phẳng người dùng/dữ liệu (*UP: User Plane*), còn các khoá K_RRC-enc 318 và K_RRC-int 320 có thể được sử dụng để bảo mật cho tín hiệu báo hiệu (tức là, thông tin điều khiển) ở tầng PDCP 410.

Để tìm ra các khoá an toàn này, dùng trong các thuật toán mã hoá và bảo vệ tính nguyên vẹn, ở tầng AS (mặt phẳng người dùng và tầng RRC) và tầng NAS đều yêu cầu là số nhận dạng thuật toán riêng biệt phải được cung cấp dưới dạng là một trong số các giá trị đầu vào. Ở tầng AS, các thuật toán cần dùng được cung cấp theo lệnh cấu hình chế độ an toàn điều khiển tài nguyên vô tuyến (RRC).

Fig.5 là sơ đồ khối thể hiện hệ thống mạng trong đó có thể tạo ra khoá xác thực và/hoặc khoá an toàn thể hiện trên Fig.3 và Fig.4. Trong sáng chế, thiết bị 322 có thể sử dụng cấu trúc truyền thông có các tầng khác nhau (ví dụ, APP, NAS, RRC, RLC, MAC và PHY). Mạng truy nhập 504 (ví dụ, nút truy nhập 106 trên Fig.1) có thể cung cấp dịch vụ kết nối không dây cho thiết bị 322 để thiết bị có thể truyền thông với mạng 108. Máy chủ thuê bao thường trú 506 và thiết bị 322 có thể đều biết hoặc phải truy nhập khoá gốc (K) dùng để tạo ra hoặc thu được khoá mật mã (CK) và/hoặc khoá nguyên vẹn (IK). Sau đó, thiết bị 322 và/hoặc máy chủ HSS 506 có thể sử dụng khoá mật mã (CK) và/hoặc khoá nguyên vẹn (IK) để tạo ra khoá thực thể quản lý an toàn truy nhập *K_ASME*. Thủ tục xác thực thiết bị cũng có thể được thực hiện và kết hợp với hoặc dựa vào khoá *K_ASME* để tạo ra khoá an toàn kết hợp *K_ASME_D*, nhờ đó kết hợp xác thực thuê bao và xác thực thiết bị trong một khoá. Khi sử dụng khoá *K_ASME_D*, thiết bị 322 và thực thể quản lý di động (MME) 510 có thể tạo ra các khoá K_NAS-enc và K_NAS-int. Thiết bị 322 và thực thể MME 510 cũng có thể tạo ra khoá dành cho mạng truy nhập K_eNB/NH. Nhờ sử dụng khoá dành cho mạng truy nhập K_eNB/NH, thiết bị 322 và

mạng truy nhập 504 có thể tạo ra các khoá K_UP-enc và K_RRC-enc và K_RRC-int.

Việc tạo ra các khoá này được mô tả chi tiết trong tài liệu 3GPP STD-T63-33.401 "*System Architecture Evolution (SAE): Security Architecture*" (gọi là 3GPP TS 33.401) Release 8. Lưu ý rằng, mặc dù các hình vẽ từ Fig.3 đến Fig.5 thể hiện môi trường/ngữ cảnh cụ thể trong đó việc kết hợp xác thực thiết bị và xác thực thuê bao có thể được thực hiện, nhưng điều đó không có nghĩa rằng sáng chế bị giới hạn ở trường hợp này, sáng chế có thể được thực hiện trong nhiều loại mạng khác.

Thiết bị không dây làm ví dụ

Fig.6 là sơ đồ khối thể hiện các bộ phận được chọn trong thiết bị không dây 600 có thể được làm thích ứng để kết hợp xác thực thuê bao và xác thực thiết bị. Thiết bị không dây 600 thường có mạch xử lý 602 kết nối với một hoặc nhiều giao diện truyền thông không dây 604. Ví dụ, thiết bị không dây 600 có thể là nút chuyển tiếp và/hoặc thiết bị đầu cuối truy nhập.

Mạch xử lý 602 có thể được bố trí để thu được, xử lý và/hoặc truyền dữ liệu, điều khiển việc truy nhập và lưu trữ dữ liệu, đưa ra các lệnh, và điều khiển các thao tác cần thiết khác. Mạch xử lý 602 có thể là mạch có cấu hình để thực hiện chương trình cần thiết được cung cấp bởi phương tiện thích hợp theo ít nhất một phương án. Ví dụ, mạch xử lý 602 có thể được thực hiện dưới dạng một hoặc nhiều bộ xử lý, bộ điều khiển, nhiều bộ xử lý và/hoặc cấu trúc khác có cấu hình để thi hành các lệnh thi hành được bao gồm, ví dụ, các lệnh phần mềm và/hoặc phần sụn, và/hoặc mạch phần cứng. Theo các phương án, mạch xử lý 602 có thể là bộ xử lý đa năng, bộ xử lý tín hiệu số (*DSP: Digital Signal Processor*), mạch tích hợp chuyên dụng (*ASIC: Application Specific Integrated Circuit*), mảng cửa lập trình được bằng trường (*FPGA: Field Programmable Gate Array*) hoặc thiết bị logic lập trình được khác, mạch logic cửa hoặc tranzito rời rạc, các bộ phận phần cứng rời rạc, hoặc mọi dạng kết hợp của các loại này được chỉ định để thực hiện các chức năng được mô tả trong sáng chế. Bộ xử lý đa năng có thể là bộ vi xử lý, nhưng theo cách khác, bộ xử lý có thể là mọi bộ xử lý, bộ điều khiển, bộ vi điều khiển hoặc máy trạng thái thông thường. Bộ xử lý cũng có thể được thực hiện dưới dạng kết hợp giữa các thiết bị tính toán, như kết hợp giữa bộ xử lý DSP và một bộ vi xử lý, nhiều bộ vi xử lý, một hoặc nhiều bộ vi xử lý kết hợp với lõi DSP, hoặc mọi cấu hình phù hợp khác. Các ví

dụ nêu trên về mạch xử lý 602 chỉ nhằm mục đích minh hoạ và các cấu hình phù hợp khác vẫn được coi là nằm trong phạm vi của sáng chế.

Giao diện truyền thông không dây 604 có thể có cấu hình để tạo điều kiện truyền thông không dây cho thiết bị không dây 600. Ví dụ, giao diện truyền thông 604 có thể có cấu hình để truyền thông thông tin hai chiều với các thiết bị không dây khác, như thiết bị đầu cuối truy nhập, nút truy nhập, nút chuyển tiếp khác, v.v.. Giao diện truyền thông 604 có thể được kết nối với anten (không được thể hiện trên hình vẽ) và có thể có mạch thu phát không dây, gồm ít nhất một bộ truyền và/hoặc ít nhất một bộ thu (ví dụ, một hoặc nhiều mạch truyền/thu) để truyền thông không dây.

Mạch xử lý 602 có thể có môđun kết hợp xác thực thuê bao và xác thực thiết bị 610. Môđun kết hợp xác thực thuê bao và xác thực thiết bị 610 có thể là mạch và/hoặc chương trình được làm thích ứng để thực hiện các thủ tục xác thực thuê bao sử dụng chứng nhận an toàn thuê bao (ví dụ, khoá dành cho thuê bao 607 và/hoặc ký hiệu nhận dạng thuê bao 609 được lưu trữ trên thẻ mạch tích hợp đa năng 608), được làm thích ứng để thực hiện (trong môi trường tin cậy 606) các thủ tục xác thực thiết bị sử dụng chứng nhận dành cho thiết bị (ví dụ, khoá dành cho thiết bị 605 và/hoặc ký hiệu nhận dạng thiết bị 611), và kết hợp các thủ tục xác thực thuê bao và xác thực thiết bị với nhau. Việc "kết hợp" như vậy có thể là kết hợp một số kết quả thu được từ cả hai thủ tục xác thực thuê bao và xác thực thiết bị. Ví dụ, khoá an toàn thứ nhất thu được từ thủ tục xác thực thuê bao có thể được kết hợp với khoá an toàn thứ hai thu được từ thủ tục xác thực thiết bị để thu được khoá an toàn thứ ba (kết hợp).

Theo một số phương án, thiết bị không dây 600 có thể có môi trường tin cậy (TrE) 606. Môi trường tin cậy 606 có thể được làm thích ứng để đáp ứng các đặc tả quy định cho môi trường tin cậy trong tài liệu 3GPP Specification Detail at TS 33.320. Môi trường tin cậy 606 có thể được cung cấp trước (hoặc được nhúng an toàn) ít nhất một số chứng nhận an toàn (ví dụ, khoá dành cho thiết bị 605 và/hoặc ký hiệu nhận dạng thiết bị 611). Ví dụ, môi trường tin cậy 606 có thể có chứng nhận liên quan đến việc xác thực thiết bị.

Theo một số phương án, thiết bị không dây 600 có thể có bước xử lý an toàn trong thẻ mạch tích hợp đa năng (UICC) 608. Thẻ UICC 608 có thể được kết nối tháo lắp được với thiết bị không dây 600. Thẻ UICC 608 có thể được cung cấp trước chứng nhận an

toàn thuê bao (ví dụ, khoá dành cho thuê bao 607 và/hoặc ký hiệu nhận dạng thuê bao 609), như chứng nhận thoả thuận xác thực và khoá (AKA) ban đầu. Theo cách khác, bước xử lý an toàn có thể được thực hiện trong môđun nhận dạng thuê bao đa năng (USIM).

Theo một hoặc nhiều dấu hiệu của thiết bị không dây 600, mạch xử lý 602 có thể được làm thích ứng để thực hiện mỗi một hoặc tất cả các quy trình, chức năng, bước và/hoặc thường trình liên quan được thể hiện trên các hình vẽ từ Fig.2 đến Fig.5, Fig.7, Fig.10, Fig.11 và Fig.12. Như được sử dụng trong sáng chế này, thuật ngữ "được làm thích ứng" đi kèm với mạch xử lý 602 có thể dùng để chỉ mạch xử lý 602 được tạo cấu hình, được sử dụng, ứng dụng và/hoặc lập trình để thực hiện quy trình, chức năng, bước và/hoặc thường trình theo các dấu hiệu được mô tả trong sáng chế.

Fig.7 là lưu đồ thể hiện ví dụ về phương pháp xác thực hoạt động trong thiết bị không dây để tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị. Thiết bị không dây có thể được cung cấp trước khoá dành cho thiết bị ở bước 702. Ví dụ, khoá dành cho thiết bị này có thể được nhúng vào chip hoặc được tạo cấu hình trong quá trình sản xuất thiết bị không dây. Thiết bị không dây cũng có thể có ký hiệu nhận dạng thiết bị đi kèm với khoá dành cho thiết bị. Ngoài ra, thiết bị không dây có thể được cung cấp trước khoá dành cho thuê bao ở bước 704. Ví dụ, khoá dành cho thuê bao này có thể là khoá gốc gán cho thuê bao và có thể được lưu trữ trong môđun gắn cố định hoặc tháo lắp được (ví dụ, UICC hoặc USIM) kết nối với thiết bị không dây. Thiết bị không dây cũng có thể có ký hiệu nhận dạng thuê bao đi kèm với khoá dành cho thuê bao. Thiết bị không dây có thể thực hiện thủ tục xác thực thuê bao với thực thể mạng (ví dụ, sử dụng khoá dành cho thuê bao) ở bước 706. Thiết bị không dây này có thể có, ví dụ, sự trao đổi thoả thuận xác thực và khoá với thực thể mạng. Thiết bị không dây cũng có thể thực hiện thủ tục xác thực thiết bị với thực thể mạng (ví dụ, sử dụng khoá dành cho thiết bị) ở bước 708. Thủ tục xác thực thuê bao và thủ tục xác thực thiết bị có thể được thực hiện ở cùng một thời điểm hoặc ở các thời điểm khác nhau và với cùng một thực thể mạng hoặc với các thực thể mạng khác nhau. Khoá an toàn (ví dụ, *K_ASME_D*, v.v.) có thể được tạo ra bằng thiết bị không dây, khoá an toàn đó kết hợp xác thực thuê bao và xác thực thiết bị ở bước 710. Ví dụ, theo một phương án làm ví dụ, dữ liệu (ví dụ, một hoặc nhiều khoá, chứng nhận, ký hiệu nhận dạng, v.v., thu được) từ thủ tục xác thực thiết bị và dữ liệu (ví

dụ, một hoặc nhiều khoá, chứng nhận, ký hiệu nhận dạng, v.v., thu được) từ thủ tục xác thực thuê bao có thể được kết hợp để tạo ra khoá an toàn. Ví dụ, trên Fig.1, khoá *K_ASME* thu được từ thủ tục xác thực thuê bao 210 và *device_temp_key* thu được từ thủ tục xác thực thiết bị trên Fig.1 có thể được kết hợp để tạo ra khoá an toàn *K_ASME_D*. Sau đó, khoá an toàn này có thể được dùng để bảo mật thông tin truyền thông không dây giữa thiết bị không dây và thực thể mạng ở bước 712. Ví dụ, khoá an toàn có thể được dùng để tạo ra các khoá và/hoặc chứng nhận khác (ví dụ, các khoá an toàn ở tầng NAS và/hoặc tầng AS) có thể dùng để mã hoá/giải mã thông tin truyền thông (ví dụ, dữ liệu và tín hiệu báo hiệu) giữa thiết bị không dây và mạng.

Thực thể mạng làm ví dụ

Fig.8 là sơ đồ khối thể hiện các bộ phận được chọn trong thực thể mạng 800 có thể được làm thích ứng để kết hợp xác thực thuê bao và xác thực thiết bị. Thực thể mạng 800 có thể có mạch xử lý 802 kết nối với giao diện truyền thông 804. Mạch xử lý 802 được bố trí để thu được, xử lý và/hoặc truyền dữ liệu, điều khiển việc truy nhập và lưu trữ dữ liệu, đưa ra các lệnh, và điều khiển các thao tác cần thiết khác. Mạch xử lý 802 có thể là mạch có cấu hình để thực hiện chương trình cần thiết được cung cấp bởi phương tiện thích hợp theo ít nhất một phương án. Ví dụ, mạch xử lý 802 có thể được thực hiện dưới dạng một hoặc nhiều bộ xử lý, bộ điều khiển, nhiều bộ xử lý và/hoặc cấu trúc khác có cấu hình để thi hành các lệnh thi hành được bao gồm, ví dụ, các lệnh phần mềm và/hoặc phần sụn, và/hoặc mạch phần cứng. Theo các phương án, mạch xử lý 802 có thể là bộ xử lý đa năng, bộ xử lý tín hiệu số (DSP), mạch tích hợp chuyên dụng (ASIC), mảng cửa lập trình được bằng trường (FPGA) hoặc thiết bị logic lập trình được khác, mạch logic cửa hoặc tranzito rời rạc, các bộ phận phần cứng rời rạc, hoặc mọi dạng kết hợp của các loại này được chỉ định để thực hiện các chức năng được mô tả trong sáng chế. Bộ xử lý đa năng có thể là bộ vi xử lý, nhưng theo cách khác, bộ xử lý có thể là mọi bộ xử lý, bộ điều khiển, bộ vi điều khiển hoặc máy trạng thái thông thường. Bộ xử lý cũng có thể được thực hiện dưới dạng kết hợp giữa các thiết bị tính toán, như kết hợp giữa bộ xử lý DSP và một bộ vi xử lý, nhiều bộ vi xử lý, một hoặc nhiều bộ vi xử lý kết hợp với lõi DSP, hoặc mọi cấu hình phù hợp khác. Các ví dụ nêu trên về mạch xử lý 802 chỉ nhằm mục đích minh hoạ và các cấu hình phù hợp khác vẫn được coi là nằm trong phạm vi của sáng chế.

Mạch xử lý 802 có môđun kết hợp xác thực thuê bao và xác thực thiết bị 806. Môđun kết hợp xác thực thuê bao và xác thực thiết bị 806 có thể là mạch và/hoặc chương trình được làm thích ứng để thực hiện các thủ tục xác thực thuê bao để xác thực thuê bao dựa vào chứng nhận an toàn thuê bao (ví dụ, khoá dành cho thuê bao và/hoặc ký hiệu nhận dạng thuê bao), thực hiện các thủ tục xác thực thiết bị để xác thực thiết bị dựa vào chứng nhận dành cho thiết bị (ví dụ, khoá dành cho thiết bị và/hoặc ký hiệu nhận dạng thiết bị), và kết hợp dữ liệu (ví dụ, các khoá, giá trị, chứng nhận, v.v.) từ các thủ tục xác thực thiết bị và xác thực thuê bao để tạo ra khoá an toàn.

Giao diện truyền thông 804 có cấu hình để tạo điều kiện cho thực thể mạng 800 truyền thông, trực tiếp hoặc gián tiếp (ví dụ, thông qua một hoặc nhiều thực thể mạng khác), với các thiết bị khác, như nút chuyển tiếp và thiết bị đầu cuối truy nhập.

Theo một hoặc nhiều dấu hiệu của thực thể mạng 800, mạch xử lý 802 có thể được làm thích ứng để thực hiện mỗi một hoặc tất cả các quy trình, chức năng, bước và/hoặc thường trình liên quan đến các thực thể mạng khác nhau, như thực thể quản lý di động (MME) 110 và máy chủ thuê bao thường trú (HSS) 112. Ngoài ra, thực thể mạng 800 có thể là một thực thể, hoặc kết hợp hai hay nhiều thực thể trong mạng. Ví dụ, nhưng không chỉ giới hạn ở đó, thực thể mạng 800 có thể là thực thể quản lý di động (MME), máy chủ thuê bao thường trú (HSS), máy chủ xác thực thiết bị, chưa kể đến những loại khác. Như được sử dụng trong sáng chế này, thuật ngữ "được làm thích ứng" đi kèm với mạch xử lý 802 có thể dùng để chỉ mạch xử lý 802 được tạo cấu hình, được sử dụng, ứng dụng hoặc lập trình để thực hiện quy trình, chức năng, bước và/hoặc thường trình theo các dấu hiệu được mô tả trong sáng chế.

Fig.9 là lưu đồ thể hiện ví dụ về phương pháp xác thực hoạt động trong thực thể mạng để tạo ra khoá an toàn kết hợp xác thực thuê bao và xác thực thiết bị. Thực thể mạng có thể thu được khoá dành cho thiết bị của thiết bị không dây ở bước 902. Ví dụ, khoá dành cho thiết bị này có thể được nhúng vào chip hoặc được tạo cấu hình trong quá trình sản xuất thiết bị không dây và thông tin này có thể được lưu trữ trong cơ sở dữ liệu mà thực thể mạng có thể truy nhập. Ký hiệu nhận dạng thiết bị có thể được liên hệ với khoá dành cho thiết bị và có thể được dùng để nhận dạng thiết bị và khoá của nó. Ngoài ra, thực thể mạng có thể thu được khoá dành cho thuê bao đi kèm với thuê bao của thiết

bị không dây ở bước 904. Ví dụ, khoá dành cho thuê bao này có thể là khoá gốc gán cho thuê bao và có thể được lưu trữ trong môđun gắn cố định hoặc tháo lắp được (ví dụ, UICC hoặc USIM) kết nối với thiết bị không dây. Thực thể mạng có thể thực hiện thủ tục xác thực thuê bao với thiết bị không dây (ví dụ, sử dụng khoá dành cho thuê bao) ở bước 906. Thực thể mạng này có thể có, ví dụ, sự trao đổi thoả thuận xác thực và khoá với thực thể mạng. Thực thể mạng cũng có thể thực hiện thủ tục xác thực thiết bị với thiết bị không dây (ví dụ, sử dụng khoá dành cho thiết bị) ở bước 908. Thủ tục xác thực thuê bao và thủ tục xác thực thiết bị có thể được thực hiện ở cùng một thời điểm hoặc ở các thời điểm khác nhau. Khoá an toàn (kết hợp) (ví dụ, *K_ASME_D*, v.v.) có thể được tạo ra bằng thực thể mạng, khoá an toàn đó kết hợp xác thực thuê bao và xác thực thiết bị ở bước 910. Ví dụ, theo một phương án làm ví dụ, dữ liệu (ví dụ, một hoặc nhiều khoá, chứng nhận, ký hiệu nhận dạng, v.v., thu được) từ thủ tục xác thực thiết bị và dữ liệu (ví dụ, *K_ASME*, v.v.) từ thủ tục xác thực thuê bao có thể được kết hợp để tạo ra khoá an toàn. Sau đó, khoá an toàn này có thể được dùng để bảo mật thông tin truyền thông không dây giữa thực thể mạng và thiết bị không dây ở bước 912. Ví dụ, khoá an toàn có thể được dùng để tạo ra các khoá và/hoặc chứng nhận khác có thể dùng để mã hoá/giải mã thông tin truyền thông giữa thiết bị không dây và mạng.

Phương pháp thứ nhất làm ví dụ để xác thực thuê bao-thiết bị

Fig.10 thể hiện phương pháp thứ nhất làm ví dụ để tạo ra khoá an toàn bằng cách kết hợp xác thực thuê bao và xác thực thiết bị. Trong ví dụ này, thiết bị 1002 có thể là nút chuyển tiếp hoặc thiết bị đầu cuối truy nhập. Ở giai đoạn kết nối, trong đó thiết bị 1002 có thể tìm cách kết nối với mạng không dây (ví dụ, có thực thể MME 1004 và máy chủ HSS 1006), việc để lộ số nhận dạng thiết bị hoặc thông tin liên quan khác của thiết bị trên mạng vô tuyến có thể làm ảnh hưởng đến sự an toàn (ví dụ, với thiết bị 1002). Do đó, trong phương pháp này, thiết bị 1002 không để lộ chứng nhận thiết bị của nó (ví dụ, ký hiệu nhận dạng dành cho thiết bị như số nhận dạng thiết bị di động quốc tế (IMEI), v.v.) trên mạng vô tuyến cho tới khi nhận được yêu cầu an toàn từ mạng để ngăn chặn sự tấn công thụ động đối với ký hiệu nhận dạng thiết bị.

Thiết bị có thể bắt đầu bằng cách truyền đến mạng yêu cầu kết nối 1010 có thông tin chỉ báo về khả năng xác thực thiết bị. Khi nhận được yêu cầu kết nối 1010, thực thể

quản lý di động (MME) 1004 có thể yêu cầu và thu nhận thông tin thuê bao và chứng nhận 1012 (ví dụ, liên quan đến tài khoản dựa vào thuê bao hoặc người dùng thiết bị 1002) từ máy chủ thuê bao thường trú (HSS) 1006. Sau đó, thực thể MME 1004 truyền yêu cầu xác thực 1014 có *AKA_challenge* để thực hiện thủ tục xác thực AKA. Khi nhận được yêu cầu xác thực AKA 1014, thiết bị 1002 truyền thông báo trả lời xác thực 1016 có *AKA_response*. Yêu cầu xác thực AKA 1014 và thông báo trả lời xác thực AKA 1016 dùng để thực hiện thủ tục xác thực thuê bao. Các thủ tục xác thực AKA như vậy có thể tìm được khoá xác thực thuê bao (ví dụ, *K_ASME*) được tạo ra bằng thiết bị 1002 và thực thể MME.

Thủ tục xác thực thiết bị có thể được thực hiện ở các giai đoạn khác nhau trong quá trình kích hoạt an toàn. Trong ví dụ này, thủ tục xác thực thiết bị có thể được cõng thêm trên các thông báo an toàn ở tầng NAS. Ví dụ, thực thể MME 1004 có thể truyền lệnh cấu hình chế độ an toàn NAS 1018 có yêu cầu ký hiệu nhận dạng thiết bị (ví dụ, yêu cầu phiên bản phần mềm IMEI (*IMEISV: IMEI Software Version*) và/hoặc yêu cầu *device_credentials*). Để đáp lại, thiết bị 1002 có thể cung cấp ký hiệu nhận dạng thiết bị hoặc chứng nhận, trong thông báo hoàn thành chế độ an toàn 1020, để thực hiện thủ tục xác thực thiết bị. Lưu ý rằng, để tránh bộc lộ ký hiệu nhận dạng thiết bị hoặc chứng nhận trên mạng vô tuyến khi truyền, ký hiệu nhận dạng thiết bị hoặc chứng nhận trong thông báo hoàn thành chế độ an toàn 1020 có thể được bảo mật bằng khoá xác thực thuê bao đã tính từ trước (ví dụ, *K_ASME*). Khi nhận được ký hiệu nhận dạng thiết bị hoặc chứng nhận, thực thể MME 1004 có thể truyền thông báo yêu cầu ký hiệu nhận dạng 1022, có ký hiệu nhận dạng tập hợp khoá cải tiến/mở rộng (*eKSI*) và *device_challenge*. Ký hiệu nhận dạng *eKSI* có thể được liên hệ với khoá *K_ASME_D* sẽ được tạo ra. Do đó, ký hiệu nhận dạng *eKSI* dùng trong thông báo yêu cầu ký hiệu nhận dạng 1022 có thể khác biệt với mọi *eKSI* khác đã từng sử dụng, ví dụ, để xác thực AKA (tức là, xác thực thuê bao). Khi nhận được thông báo yêu cầu ký hiệu nhận dạng 1022, thiết bị 1002 có thể tạo ra thông báo *device_response* dựa vào *device_challenge* và truyền thông báo này dưới dạng là một phần của thông báo trả lời ký hiệu nhận dạng 1024. Thông báo *device_response* có thể dựa vào *device_challenge* và ký hiệu nhận dạng thiết bị hoặc chứng nhận. Thiết bị 1002 có thể tính khoá an toàn (kết hợp) (*K_ASME_D*) 1025 dựa vào khoá xác thực (ví dụ, *K_ASME*) và thông tin xác thực thiết bị (ví dụ, *device_response*, v.v.). Thực thể

MME 1004 kiểm tra *device_response*, ví dụ, bằng cách sử dụng ký hiệu nhận dạng thiết bị hoặc chứng nhận của thiết bị 1002 và sử dụng *device_challenge*. Nếu thiết bị 1002 được xác thực thành công bằng thực thể MME 1004, thì thực thể MME 1004 cũng tạo ra khoá an toàn (*K_ASME_D*) 1027. Ở thời điểm này, thiết bị 1002 và thực thể MME 1004 dùng chung khoá an toàn (*K_ASME_D*) và ký hiệu nhận dạng *eKSI* liên quan của nó.

Sau đó, thực thể MME 1004 có thể truyền lệnh cấu hình chế độ an toàn 1026 có ký hiệu nhận dạng tập hợp khoá cải tiến/mở rộng *eKSI* đi kèm với khoá an toàn (*K_ASME_D*). Phương án này cho phép thiết bị 1002 tính một hoặc nhiều khoá an toàn dựa vào khoá an toàn (*K_ASME_D*). Thiết bị 1002 có thể truyền thông báo hoàn thành chế độ an toàn 1028 đến thực thể MME 1004, từ đó cho phép thực thể MME 1004 truyền thông báo hoàn thành kết nối 1030.

Phương pháp thứ hai làm ví dụ để xác thực thuê bao-thiết bị

Fig.11 thể hiện phương pháp thứ hai làm ví dụ để tạo ra khoá an toàn bằng cách kết hợp xác thực thuê bao và xác thực thiết bị. Trong ví dụ này, việc để lộ ký hiệu nhận dạng thiết bị hoặc chứng nhận (hoặc thông tin chứng nhận liên quan khác) trên mạng vô tuyến không làm ảnh hưởng đến sự an toàn. Khác với phương pháp trên Fig.10, trong trường hợp này, giả sử rằng việc để lộ ký hiệu nhận dạng thiết bị sẽ không gây ra bất kỳ vấn đề hoặc nguy cơ nào về bảo mật.

Thiết bị đã có ký hiệu nhận dạng thiết bị hoặc chứng nhận (ví dụ, IMEI) mà thực thể MME sẽ chấp nhận nhưng lại không có ngữ cảnh an toàn E-UTRAN để thực thể MME sẵn sàng sử dụng.

Thiết bị 1102 truyền yêu cầu kết nối 1108 có ký hiệu nhận dạng thiết bị hoặc chứng nhận của nó đến thực thể MME 1104. Thực thể MME 1104 có thể thu được thông tin thuê bao và chứng nhận 1110 từ máy chủ HSS 1106 và truyền yêu cầu xác thực 1112 có, ví dụ, *AKA_challenge* (để xác thực thuê bao) và/hoặc *device_challenge* (để xác thực thiết bị). Lưu ý rằng, thiết bị 1102 có thể đáp lại bằng cách truyền thông báo trả lời xác thực 1114 có thể có *AKA_response* và/hoặc *device_response*. *AKA_response* có thể dựa, ít nhất một phần, vào ký hiệu nhận dạng thuê bao. *Device_response* có thể dựa vào ký hiệu nhận dạng thiết bị và/hoặc chứng nhận và *device_challenge*. Sau đó, thiết bị 1104 có thể tạo ra khoá an toàn (kết hợp) *K_ASME_D* bằng cách kết hợp thông tin xác thực thuê

bao và thông tin xác thực thiết bị. Tương tự, khi việc kiểm tra *AKA_response* và *device_response* thành công, thực thể MME 1104 cũng có thể tạo ra khoá an toàn *K_ASME_D* bằng cách kết hợp thông tin xác thực thuê bao và thông tin xác thực thiết bị.

Thực thể MME truyền thông báo lệnh cấu hình chế độ an toàn 1116 để bắt đầu sử dụng ngữ cảnh an toàn dựa vào khoá an toàn *K_ASME_D*. Thiết bị 1102 đáp lại bằng thông báo hoàn thành chế độ an toàn 1118. Có nghĩa là, thiết bị 1102 và thực thể MME 1104 có thể tạo ra một hoặc nhiều khoá an toàn bổ sung (hoặc thông tin truyền thông an toàn khác giữa thiết bị 1102 và thực thể MME 1104) sử dụng khoá an toàn *K_ASME_D*. Sau đó, thực thể MME 1104 có thể truyền thông báo hoàn thành kết nối 1120 đến thiết bị 1102.

Ở đây nhận thấy rằng, nếu ký hiệu nhận dạng thiết bị và/hoặc chứng nhận (hoặc các khoá thiết bị được tạo ra/thu được từ trước) đã được lưu trữ trong máy chủ HSS 1106 hoặc máy chủ khác trên mạng có ký hiệu nhận dạng thuê bao, thì thiết bị 1102 có thể sử dụng lưu đồ này để thực hiện việc kết nối. Để làm được điều đó, thiết bị 1102 có thể chỉ báo (ví dụ, trong yêu cầu kết nối 1108) cho biết là ký hiệu nhận dạng thiết bị và/hoặc chứng nhận của nó có thể thu được từ máy chủ HSS 1106 hoặc máy chủ khác trên mạng. Theo cách khác, thực thể MME 1104 có thể chỉ báo cho thiết bị 1102 biết là *device_challenge* được liên hệ với một ký hiệu nhận dạng thiết bị cụ thể (ví dụ, bằng cách kết hợp ký hiệu nhận dạng thiết bị, như IMEI, với *device_challenge* theo một dạng thức nào đó). Bằng cách này, thiết bị 1102 có thể biết là *device_challenge* (trong yêu cầu xác thực 1112) được liên hệ với ký hiệu nhận dạng thiết bị của nó.

Phương pháp thứ ba làm ví dụ để xác thực thuê bao-thiết bị

Fig.12 thể hiện phương pháp thứ ba làm ví dụ để tạo ra khoá an toàn bằng cách kết hợp xác thực thuê bao và xác thực thiết bị. Trong ví dụ này, thủ tục xác thực thuê bao đã được thực hiện từ trước cho nên ngữ cảnh an toàn thuê bao 1206 (ví dụ, *K_ASME*) đã có sẵn. Thủ tục xác thực thuê bao và thiết bị kết hợp có thể được khởi động bằng mạng để thay thế ngữ cảnh an toàn hiện có. Phương án này có thể có lợi cho các thiết bị có thể cần phải thiết lập ngữ cảnh an toàn dựa vào AKA ban đầu để thu được chứng nhận hợp thức hoàn toàn hoặc chứng nhận hoạt động từ nhà điều hành.

Giải pháp này coi rằng thực thể MME đã biết ký hiệu nhận dạng thiết bị (ví dụ,

IMEI) và/hoặc *device_credentials*.

Thực thể MME 1204 truyền yêu cầu xác thực 1208 có *device_challenge* đến thiết bị 1202. Để đáp lại, thiết bị 1202 truyền thông báo trả lời xác thực 1210 có *device_response* đến thực thể MME 1204. *Device_response* có thể dựa vào *device_challenge* và ký hiệu nhận dạng thiết bị và/hoặc chứng nhận. Ở thời điểm này, thiết bị 1202 và thực thể MME 1204 đều có thể có đủ thông tin để tính khoá an toàn (kết hợp) *K_ASME_D* (ví dụ, dựa vào ngữ cảnh an toàn dựa vào AKA và thông tin xác thực thiết bị).

Thực thể MME 1204 có thể truyền lệnh cấu hình chế độ an toàn NAS 1212 đến thiết bị 1202 để thay thế ngữ cảnh an toàn hiện có 1206 bằng ngữ cảnh an toàn mới dựa vào khoá an toàn *K_ASME_D* (ví dụ, khoá an toàn này kết hợp xác thực thuê bao và xác thực thiết bị). Để đáp lại, thiết bị 1202 có thể tạo ra ngữ cảnh an toàn mới dựa vào khoá an toàn *K_ASME_D* và có thể truyền thông báo hoàn thành chế độ an toàn NAS 1214.

Lưu ý rằng, các ví dụ trên đây thể hiện hai thủ tục xác thực thuê bao và xác thực thiết bị có thể được thực hiện thông qua thực thể MME, tuy nhiên các thực thể mạng khác có thể thực hiện một số chức năng cùng với, hoặc thay cho, thực thể MME.

Một hoặc nhiều bộ phận, bước, dấu hiệu và/hoặc chức năng được thể hiện trên Fig.1, Fig.2, Fig.3, Fig.4, Fig.5, Fig.6, Fig.7, Fig.8, Fig.9, Fig.10, Fig.11 và/hoặc Fig.12 có thể được sắp xếp lại và/hoặc được kết hợp thành một bộ phận, bước, dấu hiệu và/hoặc chức năng hoặc được thực hiện trong một số bộ phận, bước, dấu hiệu và/hoặc chức năng. Các bộ phận, bước, dấu hiệu và/hoặc chức năng khác cũng có thể được đưa thêm vào mà không bị coi là vượt ra ngoài phạm vi của sáng chế. Thiết bị, cơ cấu, và/hoặc bộ phận cấu thành được thể hiện trên Fig.1, Fig.5, Fig.6 và/hoặc Fig.8 có thể có cấu hình để thực hiện một hoặc nhiều phương pháp, dấu hiệu hoặc bước được thể hiện trên Fig.2, Fig.3, Fig.4, Fig.7 và/hoặc từ Fig.9 đến Fig.12. Các thuật toán mới nêu trong sáng chế cũng có thể được áp dụng có hiệu quả ở dạng phần mềm và/hoặc được nhúng vào phần cứng.

Ngoài ra, cần lưu ý rằng ít nhất một số phương án thực hiện đã được mô tả ở dạng quy trình được thể hiện dưới dạng lưu đồ, sơ đồ cấu trúc hoặc sơ đồ khối. Mặc dù lưu đồ có thể thể hiện các thao tác theo một quy trình tuần tự, nhưng nhiều thao tác có thể được thực hiện song song hoặc đồng thời. Hơn nữa, thứ tự của các thao tác có thể được sắp

xếp lại. Quy trình sẽ kết thúc khi các thao tác trong quy trình đã hoàn thành. Quy trình có thể tương ứng với phương pháp, hàm, thủ tục, thường trình con, chương trình con, v.v.. Khi quy trình tương ứng với hàm, sự kết thúc quy trình tương ứng với sự quay trở lại hàm gọi hoặc hàm chính.

Ngoài ra, các phương án có thể được thực hiện bằng phần cứng, phần mềm, phần sụn, phần trung, vi mã, hoặc mọi dạng kết hợp của các loại này. Khi được thực hiện bằng phần mềm, phần sụn, phần trung hoặc vi mã, mã chương trình hoặc đoạn mã để thực hiện các tác vụ cần thiết có thể được lưu trữ trong vật ghi đọc được bằng máy tính như phương tiện nhớ hoặc (các) thiết bị lưu trữ khác. Bộ xử lý có thể thực hiện tác vụ cần thiết. Đoạn mã có thể là thủ tục, hàm, chương trình con, chương trình, thường trình, thường trình con, môđun, gói chương trình phần mềm, lớp, hoặc mọi dạng kết hợp của các lệnh, cấu trúc dữ liệu, hoặc các câu lệnh chương trình. Một đoạn mã có thể được kết nối với đoạn mã khác hoặc mạch phần cứng bằng cách chuyển tiếp và/hoặc thu thông tin, dữ liệu, đối số, tham số, hoặc nội dung trong bộ nhớ. Thông tin, đối số, tham số, dữ liệu, v.v., có thể được chuyển qua, chuyển tiếp hoặc truyền bằng cách mọi cách thức phù hợp, như dùng chung bộ nhớ, gửi thông báo, chuyển mã thông báo, truyền qua mạng, v.v..

Các thuật ngữ "vật ghi đọc được bằng máy", "vật ghi đọc được bằng máy tính" và/hoặc "vật ghi đọc được bằng bộ xử lý" có thể là thiết bị lưu trữ cầm tay hoặc cố định, thiết bị lưu trữ quang, và nhiều phương tiện không khả biến khác có khả năng lưu trữ, chứa hoặc mang (các) lệnh và/hoặc dữ liệu, nhưng không chỉ giới hạn ở đó. Vì vậy, các phương pháp được mô tả trong sáng chế có thể được thực hiện toàn bộ hoặc một phần bằng các lệnh và/hoặc dữ liệu có thể được lưu trữ trong "vật ghi đọc được bằng máy", "vật ghi đọc được bằng máy tính" và/hoặc "vật ghi đọc được bằng bộ xử lý" và được thi hành bằng một hoặc nhiều bộ xử lý, máy và/hoặc thiết bị.

Các phương pháp hoặc thuật toán được mô tả liên quan đến các ví dụ nêu trong sáng chế có thể được thực hiện trực tiếp bằng phần cứng, môđun phần mềm thi hành được bằng bộ xử lý, hoặc kết hợp hai loại này, dưới dạng bộ xử lý, các lệnh thực hiện chương trình, hoặc các lệnh khác, và có thể được lưu trữ trong một thiết bị hoặc được lưu trữ phân tán trên nhiều thiết bị. Môđun phần mềm có thể nằm trong bộ nhớ truy nhập ngẫu nhiên (*RAM: Random Access Memory*), bộ nhớ tác động nhanh, bộ nhớ chỉ đọc

(*ROM: Read Only Memory*), bộ nhớ chỉ đọc lập trình được bằng điện (*EPROM: Electrically Programmable Read Only Memory*), bộ nhớ chỉ đọc lập trình được xoá được bằng điện (*EEPROM: Electrically Erasable Programmable Read Only Memory*), thanh ghi, đĩa cứng, đĩa tháo lắp được, đĩa compac-bộ nhớ chỉ đọc (*CD-ROM: Compact Disc-Read Only Memory*) hoặc mọi dạng phương tiện lưu trữ không khả biến khác đã được biết đến trong lĩnh vực kỹ thuật này. Phương tiện lưu trữ có thể được kết nối với bộ xử lý sao cho bộ xử lý có thể đọc được thông tin từ phương tiện lưu trữ, và ghi thông tin lên đó. Theo cách khác, phương tiện lưu trữ có thể liền khối với bộ xử lý.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật này cần phải hiểu thêm rằng các khối logic, môđun, mạch và các bước thực hiện thuật toán làm ví dụ được mô tả liên quan đến các phương án nêu trong sáng chế có thể được thực hiện dưới dạng phần cứng điện tử, phần mềm máy tính, hoặc kết hợp hai loại này. Để thể hiện rõ khả năng có thể hoán đổi giữa phần cứng và phần mềm này, các bộ phận, khối, môđun, mạch và các bước thực hiện làm ví dụ được mô tả trên đây thường dựa theo chức năng của chúng. Chức năng được thực hiện dưới dạng phần cứng hay phần mềm là tuỳ thuộc vào ứng dụng cụ thể và các quy định ràng buộc về thiết kế áp đặt cho toàn bộ hệ thống.

Các dấu hiệu của sáng chế được mô tả ở đây có thể được áp dụng trong các hệ thống khác nhau mà không bị coi là vượt ra ngoài phạm vi của sáng chế. Cần lưu ý rằng, các phương án nêu trên chỉ là ví dụ và không được coi là để giới hạn phạm vi của sáng chế. Phần mô tả các phương án của sáng chế chỉ nhằm mục đích minh hoạ, và không nhằm mục đích giới hạn phạm vi của sáng chế. Vì vậy, các giải pháp theo sáng chế có thể được áp dụng dễ dàng cho các loại thiết bị khác và nhiều dạng thay đổi, cải biến và sửa đổi sẽ trở nên rõ ràng đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này.

YÊU CẦU BẢO HỘ

1. Phương pháp xác thực hoạt động trong thiết bị, phương pháp này bao gồm các bước:

thực hiện xác thực thuê bao với thực thể mạng dựa vào khóa xác thực thuê bao;

thực hiện xác thực thiết bị cho thiết bị với thực thể mạng để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi do thiết bị nhận được và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại (nonce-number used once/number once) của mạng và số hiện tại của thiết bị;

tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

sử dụng khóa an toàn để bảo mật sự truyền thông giữa thiết bị và mạng cung cấp.

2. Phương pháp theo điểm 1, trong đó việc xác thực thuê bao được thực hiện bởi máy chủ xác thực thứ nhất là một phần của thực thể mạng, và việc xác thực thiết bị được thực hiện bởi máy chủ xác thực thứ hai là một phần của thực thể mạng.

3. Phương pháp theo điểm 1, trong đó việc xác thực thiết bị được thực hiện bằng cách:

nhận dữ liệu từ thực thể mạng được mã hóa bằng khóa công cộng của thiết bị;

sử dụng khóa riêng tương ứng để giải mã dữ liệu đã mã hóa; và

sau đó chứng minh cho thực thể mạng thấy là thiết bị đã biết dữ liệu này.

4. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước:

truyền yêu cầu kết nối từ thiết bị đến thực thể mạng, yêu cầu kết nối này có thông tin chỉ báo về khả năng xác thực thiết bị của thiết bị.

5. Phương pháp theo điểm 1, trong đó việc xác thực thiết bị được bảo mật bằng ít nhất một khóa được tạo ra khi xác thực thuê bao.

6. Phương pháp theo điểm 1, trong đó việc xác thực thuê bao và xác thực thiết bị được thực hiện đồng thời trong các quá trình trao đổi thông báo trong đó việc xác thực thuê bao và xác thực thiết bị được kết hợp.

7. Phương pháp theo điểm 1, trong đó việc xác thực thuê bao được thực hiện trong quá trình trao đổi thông tin an toàn tách biệt và trước khi xác thực thiết bị.

8. Phương pháp theo điểm 1, trong đó khóa an toàn được tạo ra dưới dạng hàm số của ít nhất khóa thứ nhất thu được từ việc xác thực thuê bao và khóa thứ hai thu được từ việc xác thực thiết bị.

9. Phương pháp theo điểm 1, trong đó thiết bị là nút chuyển tiếp đóng vai trò là thiết bị đầu cuối truy nhập đối với thực thể mạng và đóng vai trò là thiết bị mạng đối với một hoặc nhiều thiết bị đầu cuối truy nhập.

10. Phương pháp theo điểm 1, trong đó khóa an toàn được tạo ra tách biệt bằng thiết bị và thực thể mạng.

11. Phương pháp theo điểm 1, phương pháp này còn bao gồm các bước:

tạo ra khóa dành riêng cho thuê bao là một phần của hợp đồng dịch vụ, trong đó khóa dành riêng cho thuê bao được dùng để xác thực thuê bao; và

tạo ra khóa dành riêng cho thiết bị trong quá trình sản xuất thiết bị, trong đó khóa dành riêng cho thiết bị được dùng để xác thực thiết bị.

12. Phương pháp theo điểm 1, trong đó việc xác thực thiết bị được thực hiện sau hoặc đồng thời với việc xác thực thuê bao.

13. Phương pháp theo điểm 1, trong đó thông tin hỏi bao gồm ký hiệu nhận dạng và phương pháp này còn bao gồm các bước:

nhận lệnh từ thực thể mạng chứa ký hiệu nhận dạng; và

tạo khóa an toàn bổ sung dựa vào khóa an toàn và ký hiệu nhận dạng.

14. Phương pháp theo điểm 1, trong đó việc xác thực thiết bị được thực hiện sau việc xác thực thuê bao.

15. Phương pháp theo điểm 1, trong đó việc xác thực thuê bao được thực hiện dựa vào khóa xác thực thuê bao thu được bằng cách sử dụng nhận dạng thuê bao hoặc khóa được lưu trữ bằng thiết bị.

16. Thiết bị xác thực, bao gồm:

giao diện truyền thông; và

mạch xử lý kết nối với giao diện truyền thông, mạch xử lý này được làm thích ứng để:

thực hiện xác thực thuê bao với thực thể mạng dựa vào khóa xác thực thuê bao;

thực hiện xác thực thiết bị cho thiết bị với thực thể mạng để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi do thiết bị nhận được và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

sử dụng khóa an toàn để bảo mật sự truyền thông giữa thiết bị và mạng cung cấp.

17. Thiết bị theo điểm 16, trong đó việc xác thực thiết bị dựa vào sự trao đổi hỏi-đáp giữa thiết bị và thực thể mạng.

18. Thiết bị theo điểm 16, trong đó việc xác thực thiết bị được thực hiện bằng cách:

nhận dữ liệu từ thực thể mạng được mã hóa bằng khóa công cộng của thiết bị;

sử dụng khóa riêng tương ứng để giải mã dữ liệu đã mã hóa; và

sau đó chứng minh cho thực thể mạng thấy là thiết bị đã biết dữ liệu này.

19. Thiết bị theo điểm 16, trong đó thiết bị này còn bao gồm:

truyền yêu cầu kết nối từ thiết bị đến thực thể mạng, yêu cầu kết nối này có thông tin chỉ báo về khả năng xác thực thiết bị của thiết bị.

20. Thiết bị theo điểm 16, trong đó thiết bị xác thực được bảo mật bằng ít nhất một khóa được tạo ra khi xác thực thuê bao.

21. Thiết bị theo điểm 16, trong đó việc xác thực thuê bao và xác thực thiết bị được thực hiện đồng thời trong các quá trình trao đổi thông báo kết hợp, trong đó việc xác thực thuê bao và xác thực thiết bị được kết hợp.

22. Thiết bị theo điểm 16, trong đó việc xác thực thuê bao được thực hiện trong quá trình trao đổi thông tin an toàn tách biệt và trước khi xác thực thiết bị.

23. Thiết bị theo điểm 16, trong đó khóa an toàn được tạo ra dưới dạng hàm số của ít nhất khóa thứ nhất thu được từ việc xác thực thuê bao và khóa thứ hai thu được từ việc xác thực thiết bị.

24. Thiết bị theo điểm 16, trong đó thiết bị này là nút chuyển tiếp đóng vai trò là thiết bị đầu cuối truy nhập đối với thực thể mạng và đóng vai trò là thiết bị mạng đối với một hoặc nhiều thiết bị đầu cuối truy nhập.

25. Thiết bị theo điểm 16, trong đó thiết bị này còn bao gồm:

thiết bị lưu trữ tháo lắp được kết nối với mạch xử lý và lưu trữ khóa dành riêng cho thuê bao được dùng để xác thực thuê bao; và

thiết bị lưu trữ an toàn kết nối với mạch xử lý và lưu trữ khóa dành riêng cho thiết bị được dùng để xác thực thiết bị.

26. Thiết bị xác thực, bao gồm:

phương tiện để thực hiện xác thực thuê bao với thực thể mạng dựa vào khóa xác thực thuê bao;

phương tiện để thực hiện xác thực thiết bị cho thiết bị với thực thể mạng để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi do thiết bị nhận được và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

phương tiện để tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

phương tiện để sử dụng khóa an toàn để bảo mật sự truyền thông giữa thiết bị và mạng cung cấp.

27. Thiết bị theo điểm 26, trong đó thiết bị này còn bao gồm:

phương tiện để lưu trữ khóa dành riêng cho thuê bao được dùng để xác thực thuê bao; và

phương tiện để lưu trữ khóa dành riêng cho thiết bị được dùng để xác thực thiết bị.

28. Phương tiện bất biến đọc được bằng bộ xử lý chứa các lệnh hoạt động trên thiết bị, khi được thực thi bằng bộ xử lý, khiến cho bộ xử lý:

thực hiện xác thực thuê bao với thực thể mạng dựa vào khóa xác thực thuê bao;

thực hiện xác thực thiết bị cho thiết bị với thực thể mạng để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi do thiết bị nhận được và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

sử dụng khóa an toàn để bảo mật sự truyền thông giữa thiết bị và mạng cung cấp.

29. Phương pháp xác thực hoạt động trong thực thể mạng, phương pháp này bao gồm các bước:

thực hiện xác thực thuê bao với thiết bị dựa vào khóa xác thực thuê bao;

thực hiện xác thực thiết bị cho thiết bị để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi được truyền đến thiết bị và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

sử dụng khóa an toàn để bảo mật sự truyền thông giữa thực thể mạng và thiết bị.

30. Phương pháp theo điểm 29, trong đó việc xác thực thiết bị bao gồm các bước:

thu chứng nhận từ thiết bị;

kiểm tra chứng nhận đi kèm với thiết bị chưa bị thu hồi.

31. Phương pháp theo điểm 29, phương pháp này còn bao gồm bước:

nhận yêu cầu kết nối từ thiết bị, yêu cầu kết nối này có thông tin chỉ báo về khả năng xác thực thiết bị của thiết bị.

32. Phương pháp theo điểm 29, trong đó việc xác thực thiết bị được bảo mật bằng ít nhất một khóa được tạo ra khi xác thực thuê bao.

33. Phương pháp theo điểm 29, trong đó việc xác thực thuê bao và xác thực thiết bị được thực hiện đồng thời trong các quá trình trao đổi thông báo kết hợp, trong đó việc xác thực thuê bao và xác thực thiết bị được kết hợp.

34. Phương pháp theo điểm 29, trong đó việc xác thực thuê bao được thực hiện trong quá trình trao đổi thông tin an toàn tách biệt và trước khi xác thực thiết bị.

35. Phương pháp theo điểm 29, trong đó khóa an toàn được tạo ra dưới dạng hàm số của ít nhất khóa thứ nhất thu được từ việc xác thực thuê bao và khóa thứ hai thu được từ việc xác thực thiết bị.

36. Phương pháp theo điểm 29, trong đó khóa an toàn được tạo ra tách biệt bằng thiết bị và thực thể mạng.

37. Phương pháp theo điểm 29, phương pháp này còn bao gồm các bước:

thu được khóa dành riêng cho thuê bao là một phần của hợp đồng dịch vụ, khóa dành riêng cho thuê bao này được dùng để xác thực thuê bao; và

thu được khóa dành riêng cho thiết bị dùng cho thiết bị, khóa dành riêng cho thiết bị này được dùng để xác thực thiết bị.

38. Phương pháp theo điểm 29, trong đó việc xác thực thiết bị được thực hiện sau hoặc đồng thời với việc xác thực thuê bao.

39. Phương pháp theo điểm 29, trong đó thông tin hỏi bao gồm ký hiệu nhận dạng và phương pháp này còn bao gồm các bước:

truyền lệnh đến thiết bị chứa ký hiệu nhận dạng; và

nhận các khóa an toàn bổ sung được tạo ra bằng thiết bị dựa vào khóa an toàn và ký hiệu nhận dạng.

40. Phương pháp theo điểm 29, trong đó việc xác thực thuê bao được thực hiện dựa vào khóa xác thực thuê bao thu được bằng cách sử dụng nhận dạng thuê bao hoặc khóa được lưu trữ bằng thiết bị.

41. Thực thể mạng, bao gồm:

giao diện truyền thông; và

mạch xử lý kết nối với giao diện truyền thông, mạch xử lý này được làm thích ứng để:

thực hiện xác thực thuê bao với thiết bị dựa vào khóa xác thực thuê bao;

thực hiện xác thực thiết bị cho thiết bị để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi được truyền đến thiết bị và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

sử dụng khóa an toàn để bảo mật sự truyền thông giữa thực thể mạng và thiết bị.

42. Thực thể mạng theo điểm 41, trong đó mạch xử lý còn được làm thích ứng để:

nhận yêu cầu kết nối từ thiết bị, yêu cầu kết nối này có thông tin chỉ báo về khả năng xác thực thiết bị của thiết bị.

43. Thực thể mạng theo điểm 41, trong đó thiết bị xác thực được bảo mật bằng ít nhất một khóa được tạo ra khi xác thực thuê bao.

44. Thực thể mạng theo điểm 41, trong đó việc xác thực thuê bao và xác thực thiết bị được thực hiện đồng thời trong các quá trình trao đổi thông báo kết hợp, trong đó việc xác thực thuê bao và xác thực thiết bị được kết hợp.

45. Thực thể mạng theo điểm 41, trong đó việc xác thực thuê bao được thực hiện trong quá trình trao đổi thông tin an toàn tách biệt và trước khi xác thực thiết bị.

46. Thực thể mạng theo điểm 41, trong đó khóa an toàn được tạo ra dưới dạng hàm số của ít nhất khóa thứ nhất thu được từ việc xác thực thuê bao và khóa thứ hai thu được từ việc xác thực thiết bị.

47. Thực thể mạng theo điểm 41, trong đó thực thể này còn bao gồm:

thu được khóa dành riêng cho thuê bao là một phần của hợp đồng dịch vụ, khóa dành riêng cho thuê bao này được dùng để xác thực thuê bao; và

thu được khóa dành riêng cho thiết bị dùng cho thiết bị, khóa dành riêng cho thiết bị này được dùng để xác thực thiết bị.

48. Thực thể mạng, bao gồm:

phương tiện để thực hiện xác thực thuê bao với thiết bị dựa vào khóa xác thực thuê bao;

phương tiện để thực hiện xác thực thiết bị cho thiết bị để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi được truyền đến thiết bị và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

phương tiện dành cho khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và xác thực thiết bị; và

phương tiện để sử dụng khóa an toàn để bảo mật sự truyền thông giữa thực thể mạng và thiết bị.

49. Phương tiện bất biến đọc được bằng bộ xử lý chứa các lệnh hoạt động trên thực thể mạng, khi được thực thi bằng bộ xử lý, khiến cho bộ xử lý:

thực hiện xác thực thuê bao với thiết bị dựa vào khóa xác thực thuê bao;

thực hiện xác thực thiết bị cho thiết bị để thu được dữ liệu xác thực thiết bị, trong đó dữ liệu xác thực thiết bị thu được dựa vào thông tin hỏi được truyền đến thiết bị và nhận dạng hoặc chứng nhận thiết bị, dữ liệu xác thực thiết bị kết hợp ít nhất một phần của thông tin hỏi và trong đó dữ liệu xác thực thiết bị bao gồm tham số mã hóa thu được từ khóa tạm thời của thiết bị, số hiện tại của mạng và số hiện tại của thiết bị;

tạo ra khóa an toàn dựa vào khóa xác thực thuê bao và ít nhất một phần của dữ liệu xác thực thiết bị để ràng buộc việc xác thực thuê bao và việc xác thực thiết bị; và

sử dụng khóa an toàn để bảo mật sự truyền thông giữa thực thể mạng và thiết bị.

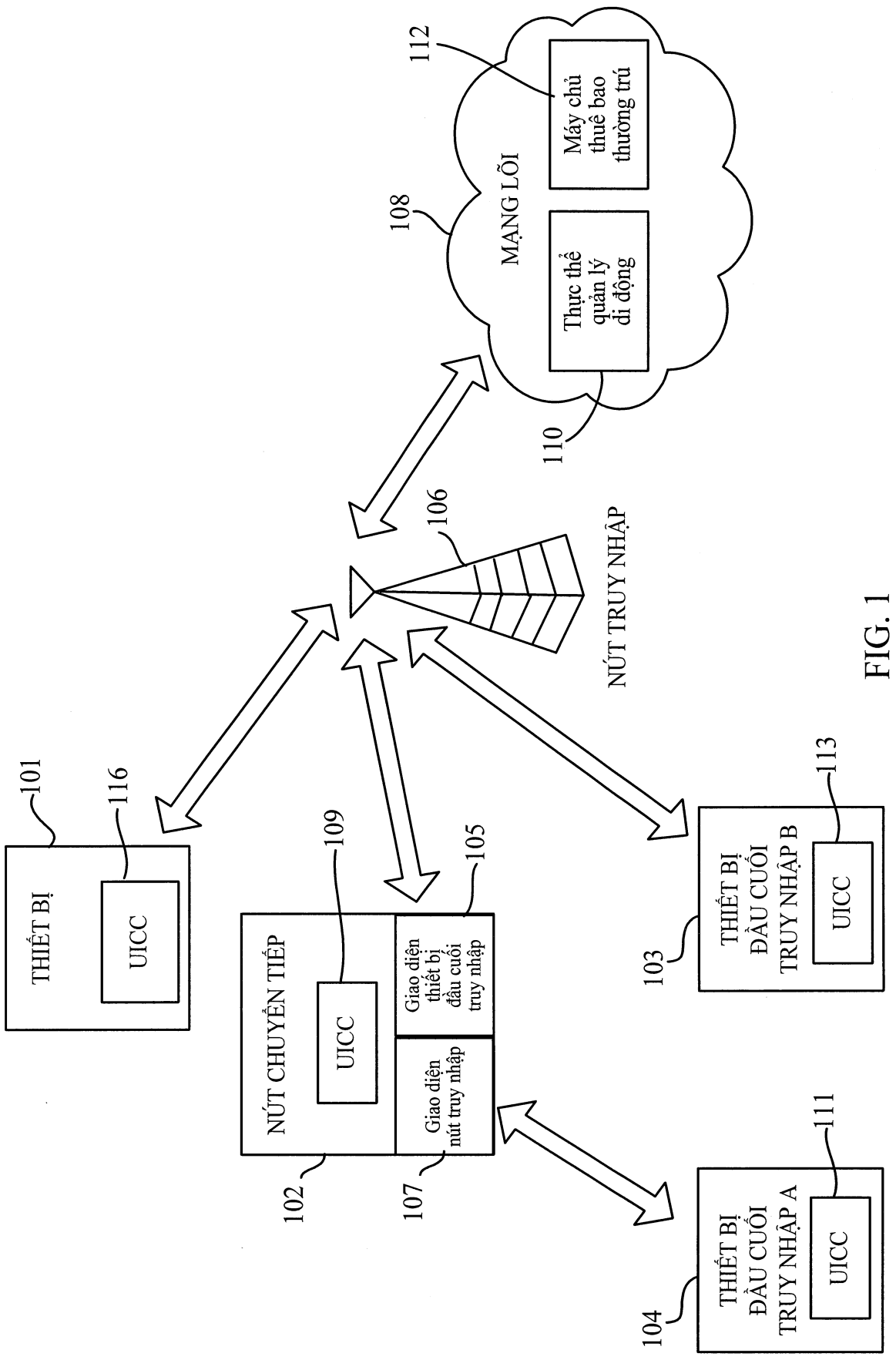

112
Máy chủ thuê bao thường trú
108
MẠNG LÕI
Thực thể quản lý di động
110
106
NÚT TRUY NHẬP
101
116
THIẾT BỊ
UICC
109
105
NÚT CHUYỂN TIẾP
UICC
Giao diện thiết bị đầu cuối truy nhập
Giao diện nút truy nhập
102
107
103
THIẾT BỊ ĐẦU CUỐI TRUY NHẬP B
UICC
113
104
THIẾT BỊ ĐẦU CUỐI TRUY NHẬP A
UICC
111

FIG. 1

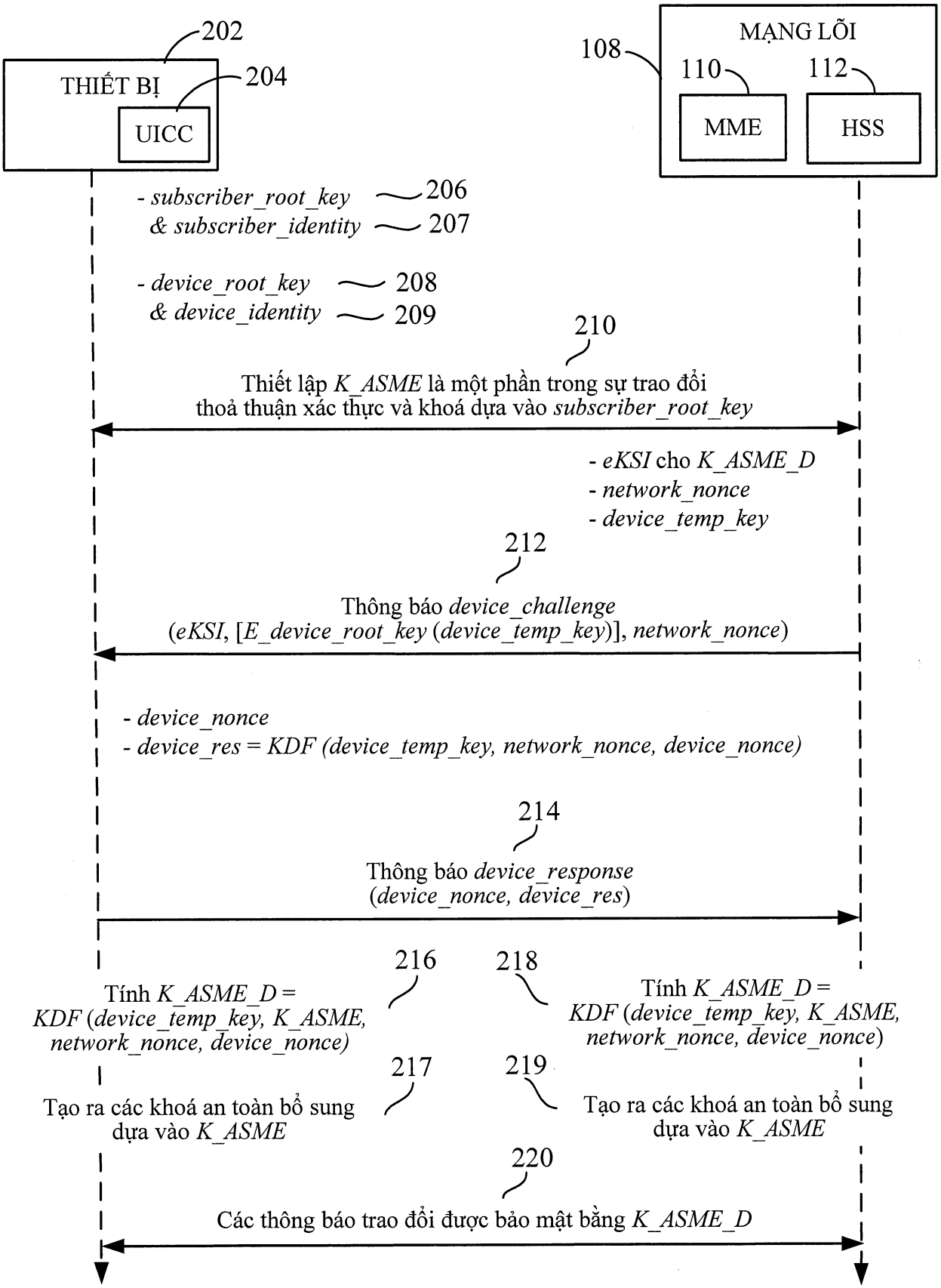

202
THIẾT BỊ
204
UICC
MẠNG LÕI
108
110
112
MME
HSS
- subscriber_root_key
& subscriber_identity
206
207
- device_root_key
& device_identity
208
209
210
Thiết lập K_ASME là một phần trong sự trao đổi thoả thuận xác thực và khoá dựa vào subscriber_root_key
- eKSI cho K_ASME_D
- network_nonce
- device_temp_key
212
Thông báo device_challenge (eKSI, [E_device_root_key (device_temp_key)], network_nonce)
- device_nonce
- device_res = KDF (device_temp_key, network_nonce, device_nonce)
214
Thông báo device_response (device_nonce, device_res)
216
218
Tính K_ASME_D = KDF (device_temp_key, K_ASME, network_nonce, device_nonce)
Tính K_ASME_D = KDF (device_temp_key, K_ASME, network_nonce, device_nonce)
217
219
Tạo ra các khoá an toàn bổ sung dựa vào K_ASME
Tạo ra các khoá an toàn bổ sung dựa vào K_ASME
220
Các thông báo trao đổi được bảo mật bằng K_ASME_D

FIG. 2

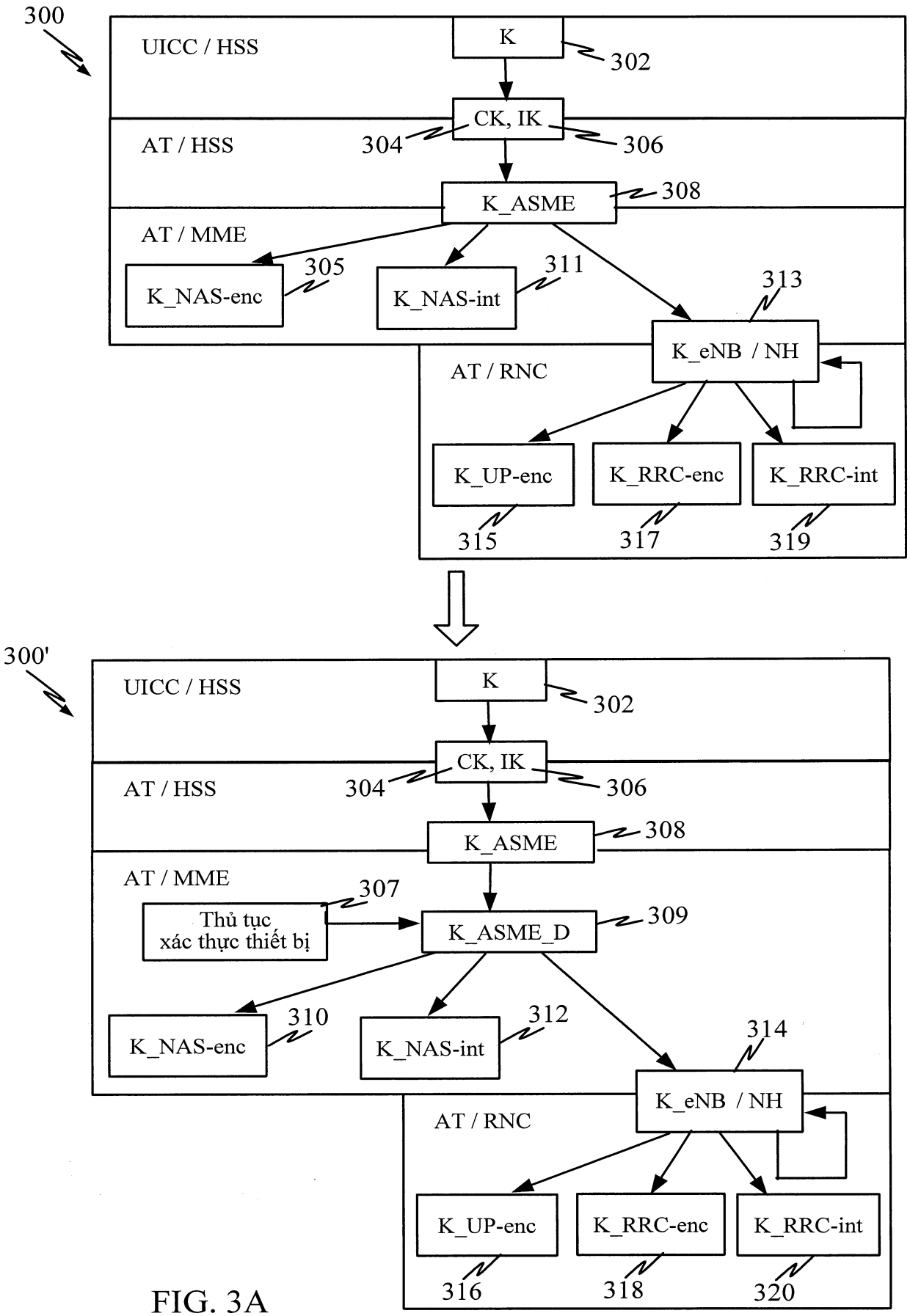

300
UICC / HSS
K
302
AT / HSS
CK, IK
304
306
K_ASME
308
AT / MME
K_NAS-enc
305
K_NAS-int
311
313
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
315
317
319
300'
UICC / HSS
K
302
AT / HSS
CK, IK
304
306
K_ASME
308
AT / MME
307
Thủ tục xác thực thiết bị
K_ASME_D
309
K_NAS-enc
310
K_NAS-int
312
314
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
316
318
320

FIG. 3A

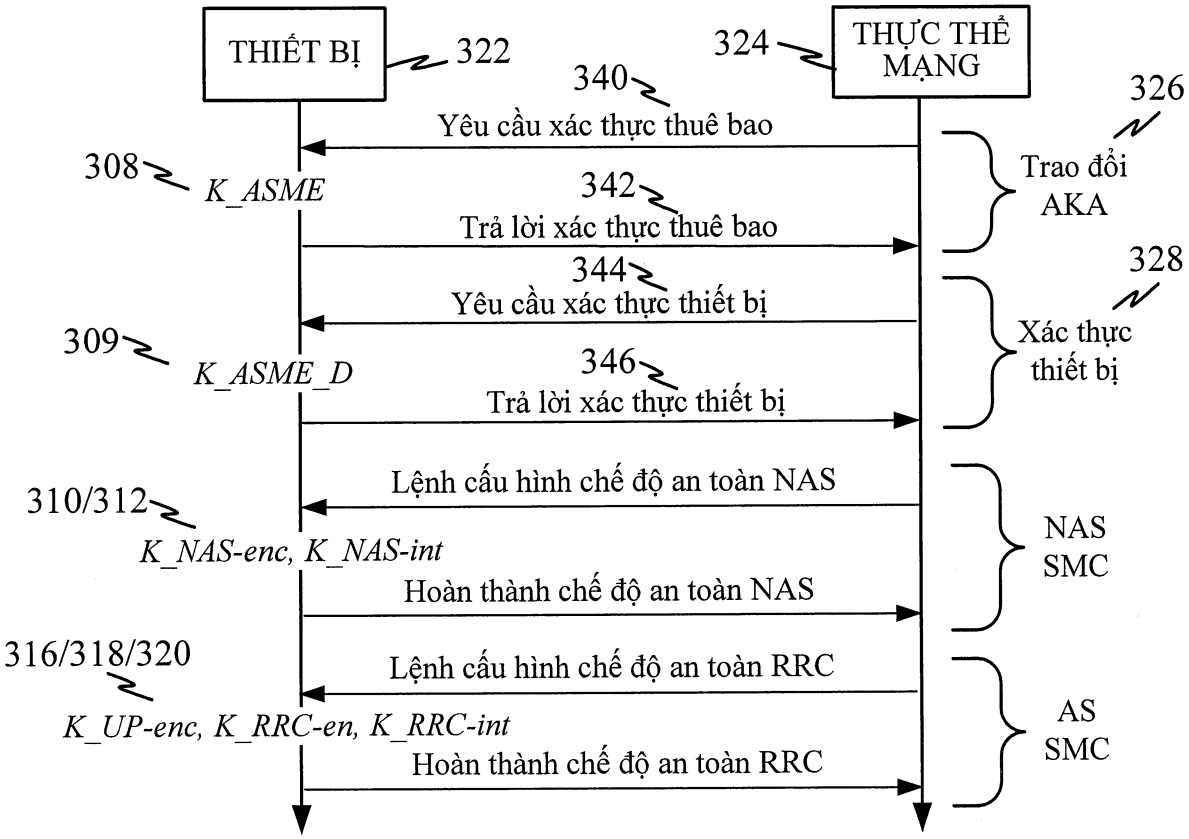

THIẾT BỊ
322
324
THỰC THỂ MẠNG
340
Yêu cầu xác thực thuê bao
326
Trao đổi AKA
308
K_ASME
342
Trả lời xác thực thuê bao
344
Yêu cầu xác thực thiết bị
328
Xác thực thiết bị
309
K_ASME_D
346
Trả lời xác thực thiết bị
Lệnh cấu hình chế độ an toàn NAS
310/312
K_NAS-enc, K_NAS-int
NAS SMC
Hoàn thành chế độ an toàn NAS
316/318/320
Lệnh cấu hình chế độ an toàn RRC
K_UP-enc, K_RRC-en, K_RRC-int
AS SMC
Hoàn thành chế độ an toàn RRC

FIG. 3B

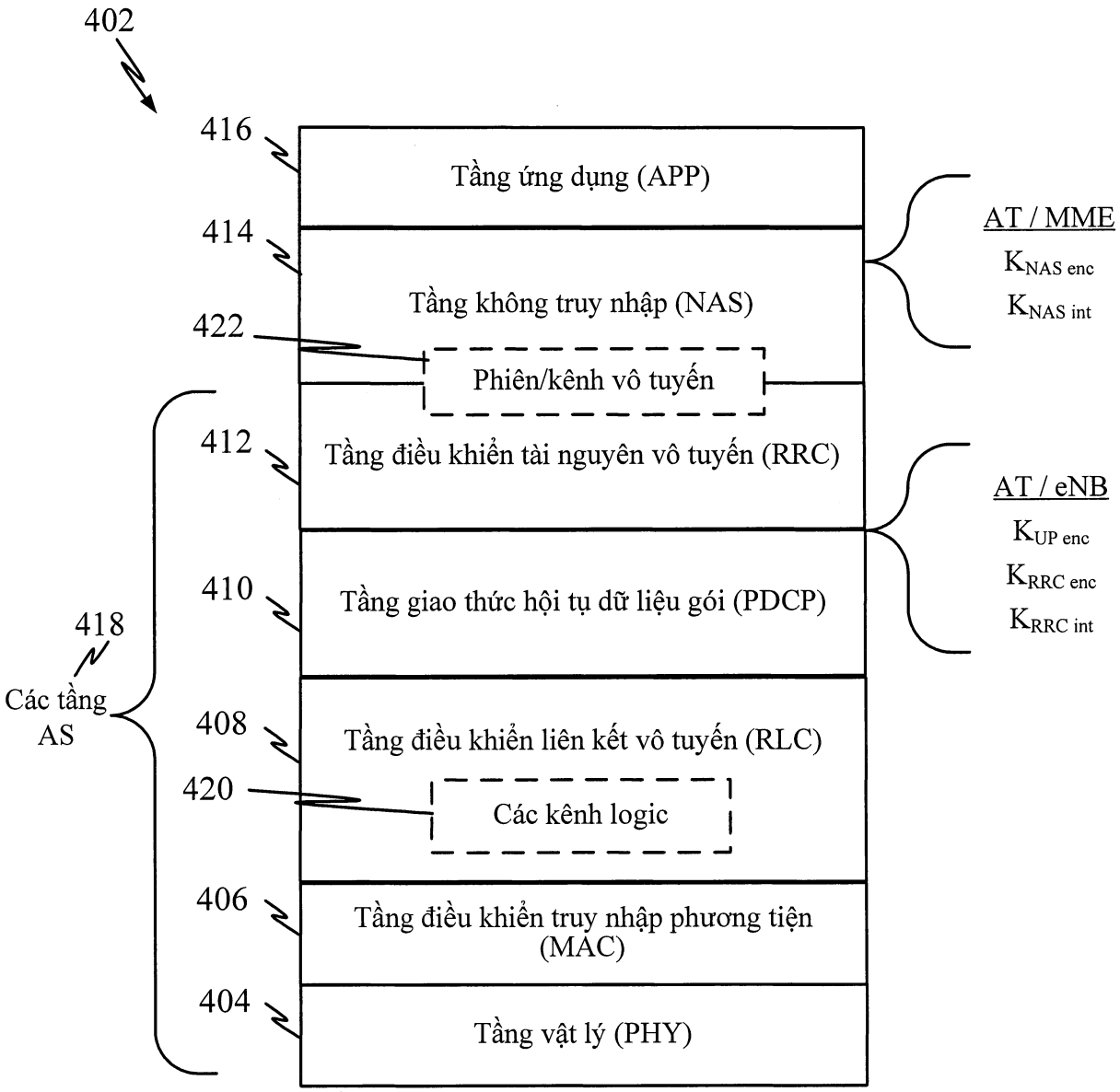

402
416
Tầng ứng dụng (APP)
414
Tầng không truy nhập (NAS)
422
Phiên/kênh vô tuyến
412
Tầng điều khiển tài nguyên vô tuyến (RRC)
410
Tầng giao thức hội tụ dữ liệu gói (PDCP)
408
Tầng điều khiển liên kết vô tuyến (RLC)
420
Các kênh logic
406
Tầng điều khiển truy nhập phương tiện (MAC)
404
Tầng vật lý (PHY)
418
Các tầng AS
AT / MME
$K_{NAS\ enc}$
$K_{NAS\ int}$
AT / eNB
$K_{UP\ enc}$
$K_{RRC\ enc}$
$K_{RRC\ int}$

FIG. 4

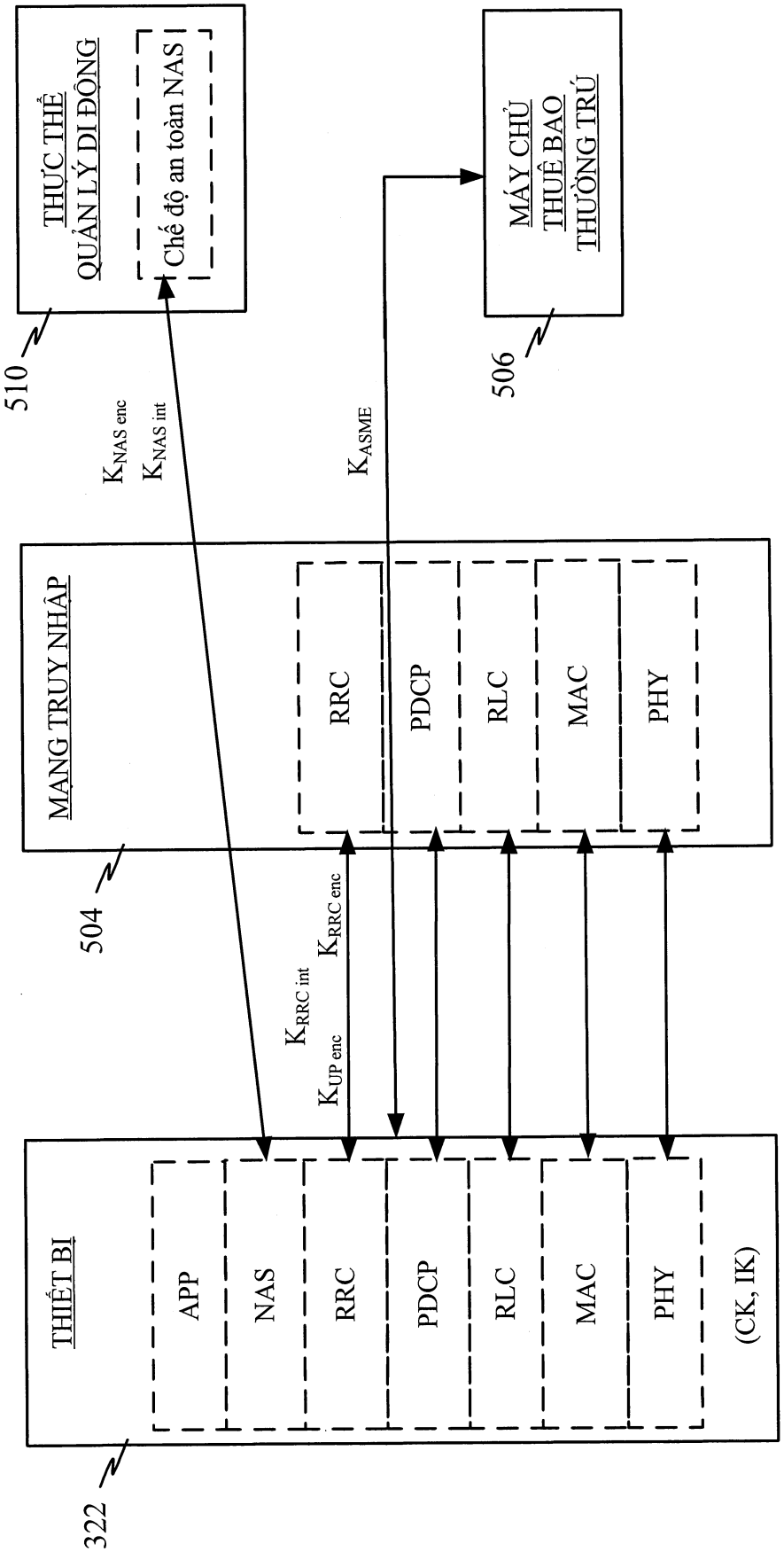

THỰC THỂ QUẢN LÝ DI ĐỘNG
Chế độ an toàn NAS
510
MÁY CHỦ THUÊ BAO THƯỜNG TRÚ
506
$K_{NAS\ enc}$
$K_{NAS\ int}$
K_{ASME}
MẠNG TRUY NHẬP
RRC
PDCP
RLC
MAC
PHY
504
$K_{RRC\ int}$
$K_{RRC\ enc}$
$K_{UP\ enc}$
THIẾT BỊ
APP
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
322

FIG. 5

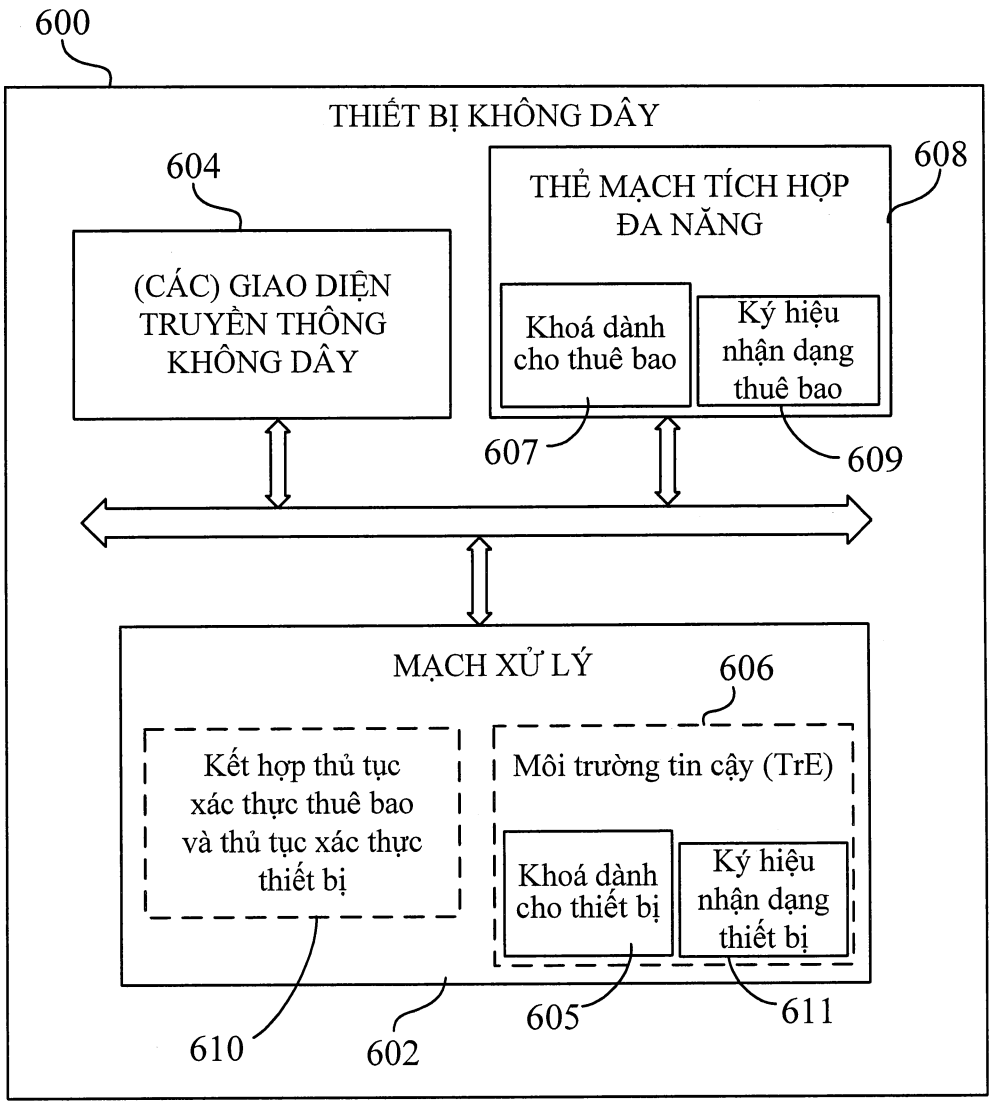

600
THIẾT BỊ KHÔNG DÂY
604
(CÁC) GIAO DIỆN TRUYỀN THÔNG KHÔNG DÂY
608
THẺ MẠCH TÍCH HỢP ĐA NĂNG
Khoá dành cho thuê bao
Ký hiệu nhận dạng thuê bao
607
609
MẠCH XỬ LÝ
606
Kết hợp thủ tục xác thực thuê bao và thủ tục xác thực thiết bị
Môi trường tin cậy (TrE)
Khoá dành cho thiết bị
Ký hiệu nhận dạng thiết bị
610
602
605
611

FIG. 6

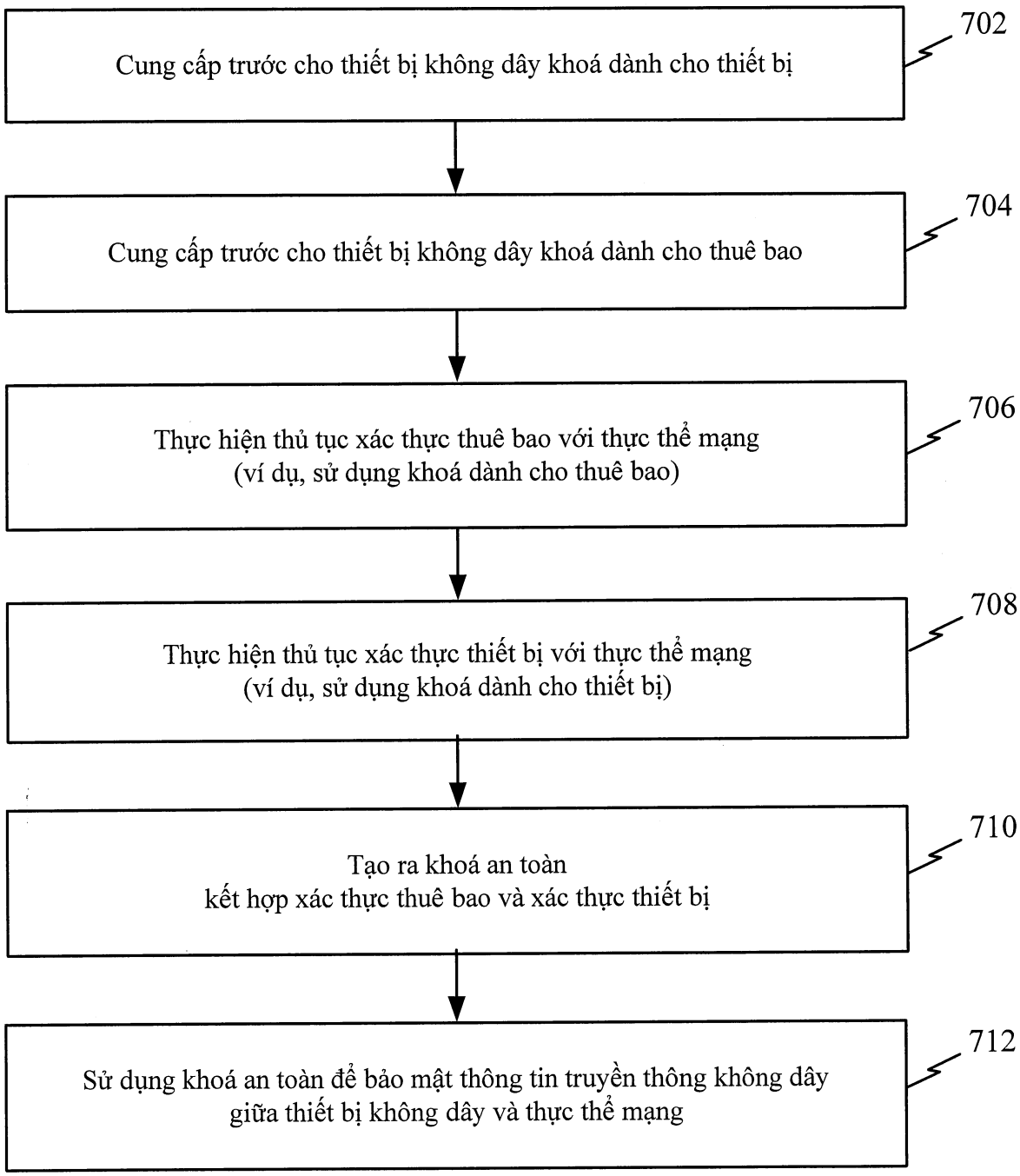

Cung cấp trước cho thiết bị không dây khoá dành cho thiết bị
702
Cung cấp trước cho thiết bị không dây khoá dành cho thuê bao
704
Thực hiện thủ tục xác thực thuê bao với thực thể mạng
(ví dụ, sử dụng khoá dành cho thuê bao)
706
Thực hiện thủ tục xác thực thiết bị với thực thể mạng
(ví dụ, sử dụng khoá dành cho thiết bị)
708
Tạo ra khoá an toàn
kết hợp xác thực thuê bao và xác thực thiết bị
710
Sử dụng khoá an toàn để bảo mật thông tin truyền thông không dây
giữa thiết bị không dây và thực thể mạng
712

FIG. 7

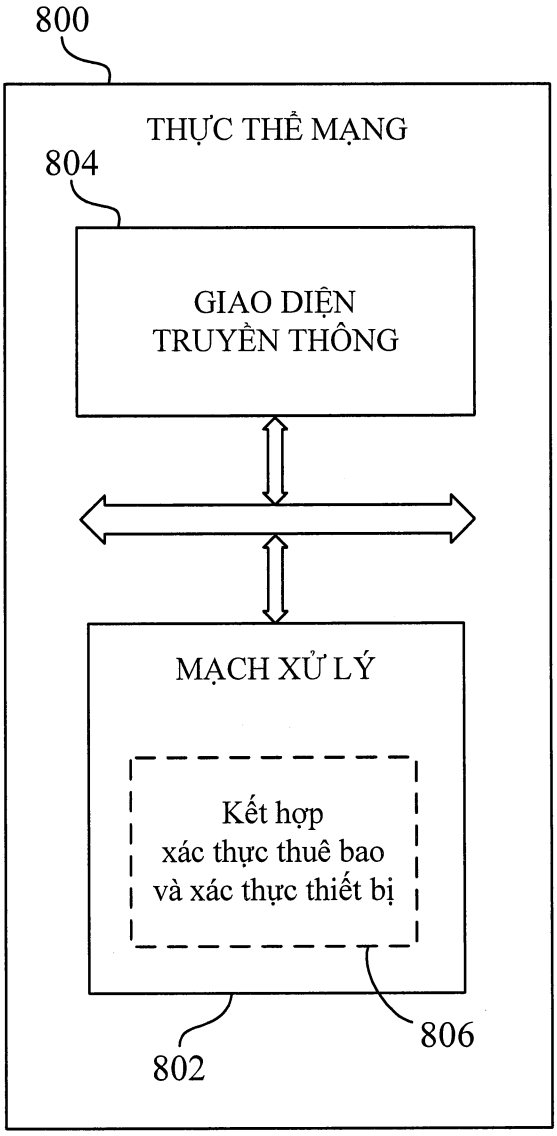

800
THỰC THỂ MẠNG
804
GIAO DIỆN
TRUYỀN THÔNG
MẠCH XỬ LÝ
Kết hợp
xác thực thuê bao
và xác thực thiết bị
802
806

FIG. 8

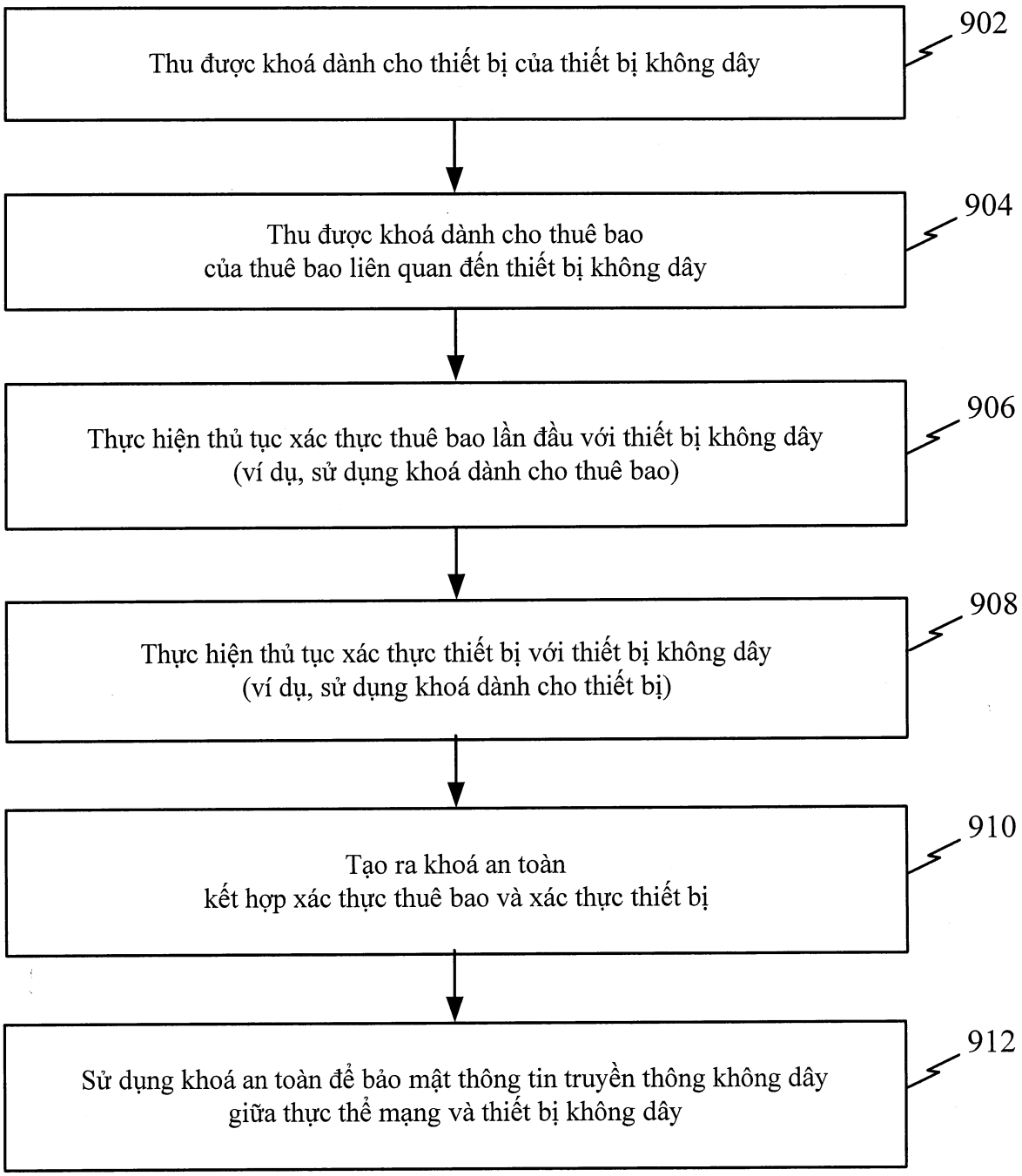

Thu được khoá dành cho thiết bị của thiết bị không dây
902
Thu được khoá dành cho thuê bao
của thuê bao liên quan đến thiết bị không dây
904
Thực hiện thủ tục xác thực thuê bao lần đầu với thiết bị không dây
(ví dụ, sử dụng khoá dành cho thuê bao)
906
Thực hiện thủ tục xác thực thiết bị với thiết bị không dây
(ví dụ, sử dụng khoá dành cho thiết bị)
908
Tạo ra khoá an toàn
kết hợp xác thực thuê bao và xác thực thiết bị
910
Sử dụng khoá an toàn để bảo mật thông tin truyền thông không dây
giữa thực thể mạng và thiết bị không dây
912

FIG. 9

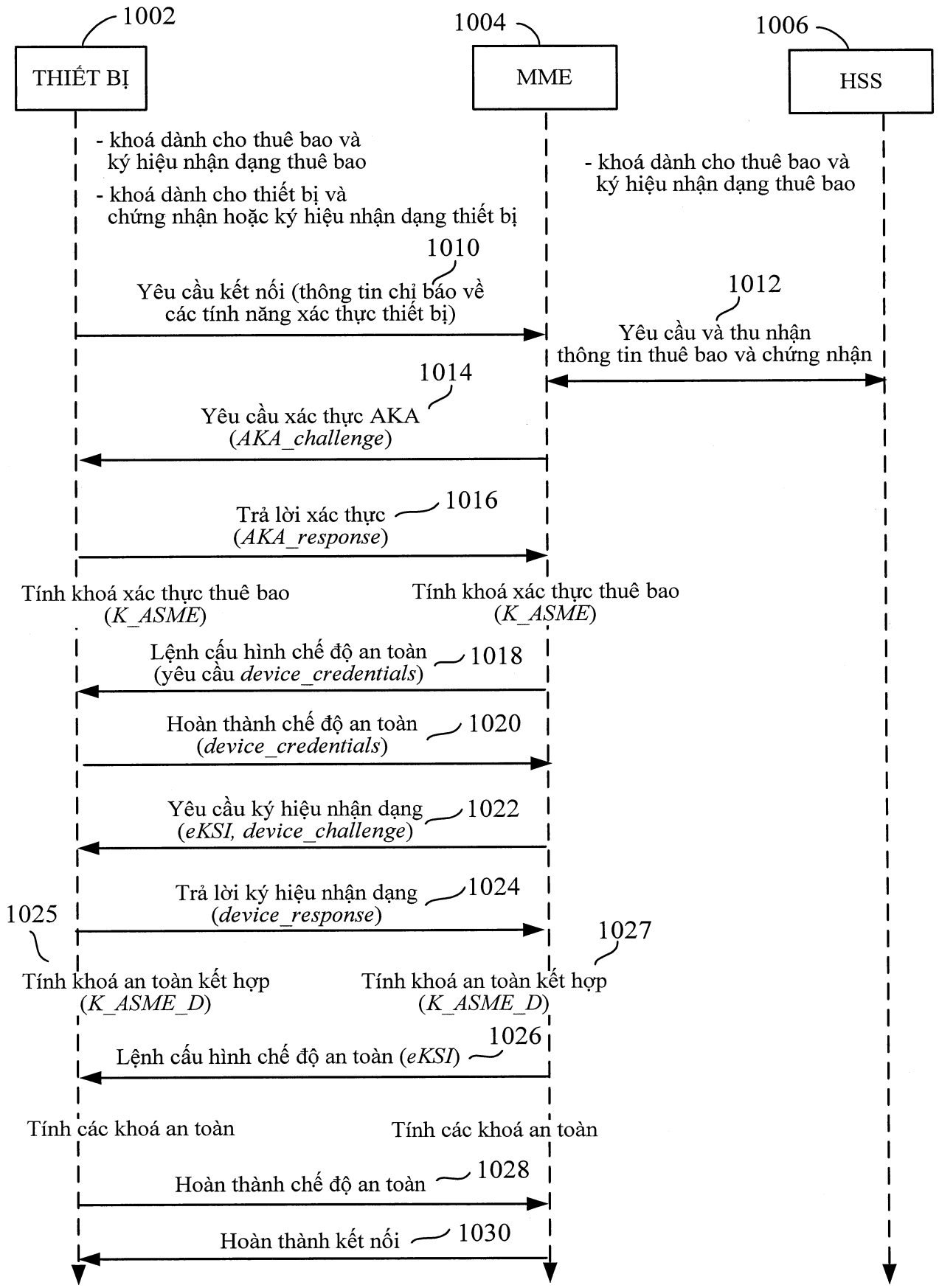

1002
THIẾT BỊ
1004
MME
1006
HSS
- khoá dành cho thuê bao và ký hiệu nhận dạng thuê bao
- khoá dành cho thiết bị và chứng nhận hoặc ký hiệu nhận dạng thiết bị
- khoá dành cho thuê bao và ký hiệu nhận dạng thuê bao
1010
Yêu cầu kết nối (thông tin chỉ báo về các tính năng xác thực thiết bị)
1012
Yêu cầu và thu nhận thông tin thuê bao và chứng nhận
1014
Yêu cầu xác thực AKA (AKA_challenge)
1016
Trả lời xác thực (AKA_response)
Tính khoá xác thực thuê bao (K_ASME)
Tính khoá xác thực thuê bao (K_ASME)
Lệnh cấu hình chế độ an toàn (yêu cầu device_credentials)
1018
Hoàn thành chế độ an toàn (device_credentials)
1020
Yêu cầu ký hiệu nhận dạng (eKSI, device_challenge)
1022
Trả lời ký hiệu nhận dạng (device_response)
1024
1025
1027
Tính khoá an toàn kết hợp (K_ASME_D)
Tính khoá an toàn kết hợp (K_ASME_D)
1026
Lệnh cấu hình chế độ an toàn (eKSI)
Tính các khoá an toàn
Tính các khoá an toàn
Hoàn thành chế độ an toàn
1028
Hoàn thành kết nối
1030

FIG. 10

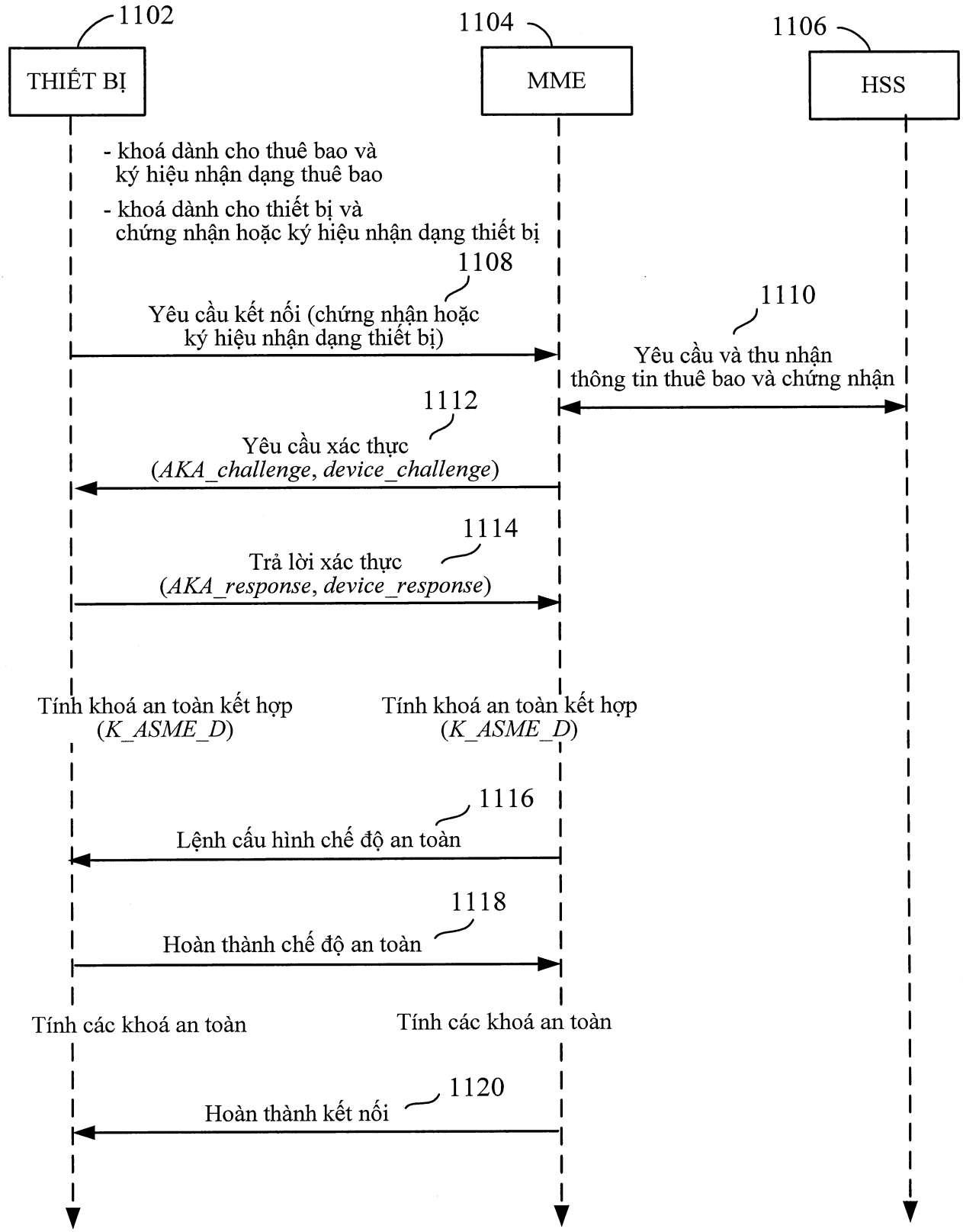

1102
THIẾT BỊ
1104
MME
1106
HSS
- khoá dành cho thuê bao và ký hiệu nhận dạng thuê bao
- khoá dành cho thiết bị và chứng nhận hoặc ký hiệu nhận dạng thiết bị
1108
Yêu cầu kết nối (chứng nhận hoặc ký hiệu nhận dạng thiết bị)
1110
Yêu cầu và thu nhận thông tin thuê bao và chứng nhận
1112
Yêu cầu xác thực (AKA_challenge, device_challenge)
1114
Trả lời xác thực (AKA_response, device_response)
Tính khoá an toàn kết hợp (K_ASME_D)
Tính khoá an toàn kết hợp (K_ASME_D)
1116
Lệnh cấu hình chế độ an toàn
1118
Hoàn thành chế độ an toàn
Tính các khoá an toàn
Tính các khoá an toàn
1120
Hoàn thành kết nối

FIG. 11

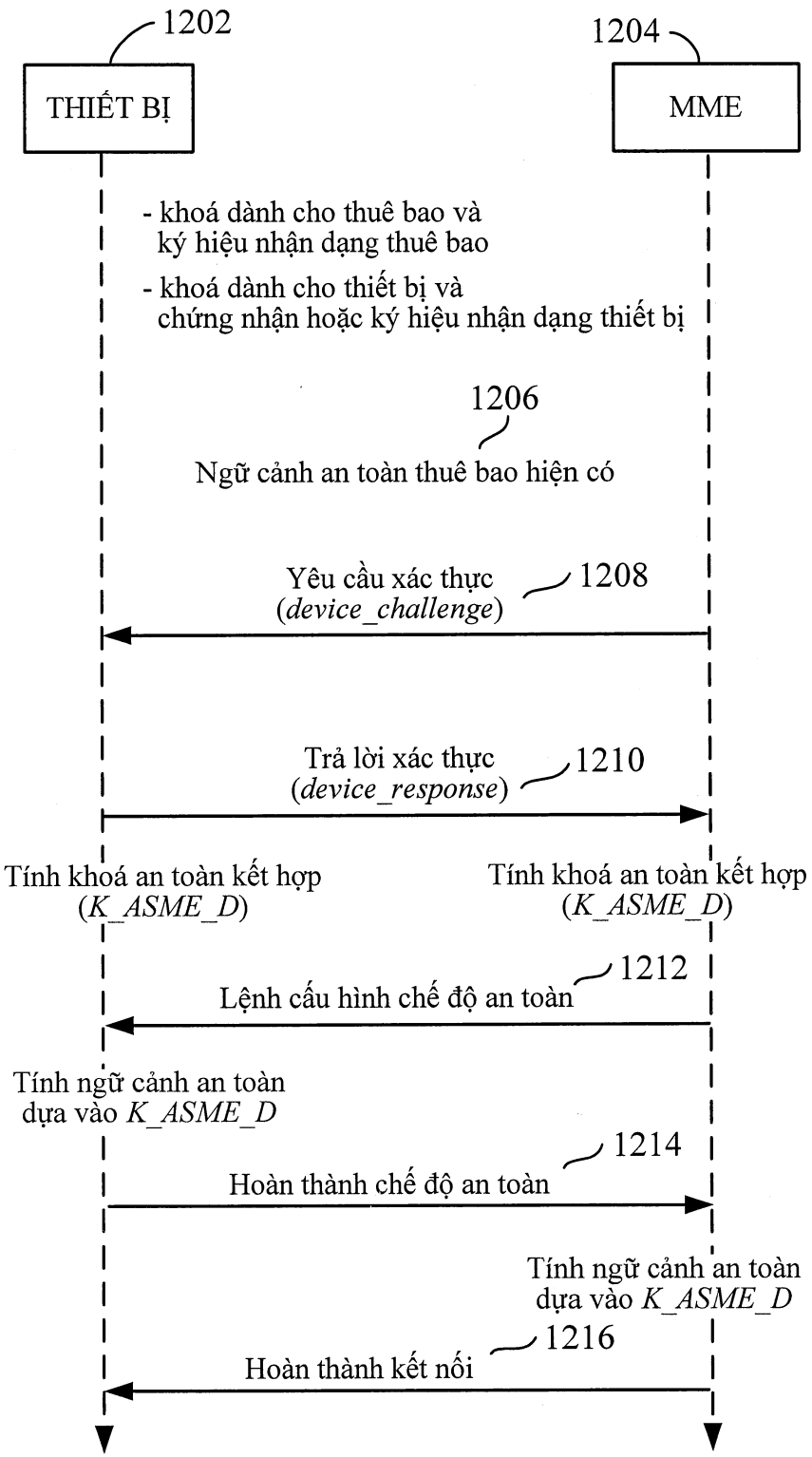

1202
THIẾT BỊ
1204
MME
- khoá dành cho thuê bao và
ký hiệu nhận dạng thuê bao
- khoá dành cho thiết bị và
chứng nhận hoặc ký hiệu nhận dạng thiết bị
1206
Ngữ cảnh an toàn thuê bao hiện có
Yêu cầu xác thực
(device_challenge)
1208
Trả lời xác thực
(device_response)
1210
Tính khoá an toàn kết hợp
(K_ASME_D)
Tính khoá an toàn kết hợp
(K_ASME_D)
1212
Lệnh cấu hình chế độ an toàn
Tính ngữ cảnh an toàn
dựa vào K_ASME_D
1214
Hoàn thành chế độ an toàn
Tính ngữ cảnh an toàn
dựa vào K_ASME_D
1216
Hoàn thành kết nối

FIG. 12