(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) **1-0052477**

(51)[2022.01] **H04W 12/00**

(13) **B**

(21) 1-2022-08640
(22) 24/05/2021
(86) PCT/CN2021/095434 24/05/2021
(87) WO 2021/244342 09/12/2021
(30) 202010480965.0 30/05/2020 CN
(45) 27/10/2025 451
(43) 25/04/2023 421A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) WU, Yizhuang (CN); LI, He (CN); HU, Li (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP XÁC ĐỊNH THÔNG TIN TĂNG CƯỜNG BẢO MẬT MẶT PHẲNG NGƯỜI DÙNG, THIẾT BỊ TRUYỀN THÔNG VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2022-08640

(57) Sáng chế đề cập đến phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính, để đảm bảo yêu cầu bảo mật của dữ liệu được truyền của thiết bị từ xa. Theo sáng chế này, phần tử mạng quản lý phiên có thể nhận yêu cầu thứ nhất, trong đó yêu cầu thứ nhất này yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, yêu cầu thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Sau đó, phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất; và sau đó gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập. Thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất được xác định bởi phần tử mạng quản lý phiên cũng có thể đáp ứng yêu cầu bảo mật của thiết bị từ xa, và đảm bảo độ bảo mật dữ liệu của thiết bị từ xa.

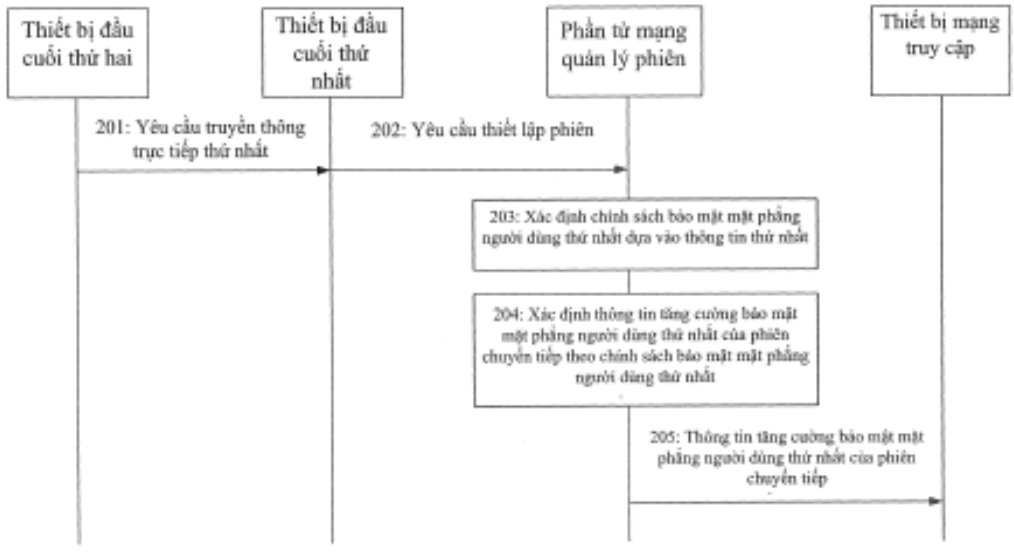

FIG. 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực các công nghệ truyền thông, và cụ thể là, phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính.

Tình trạng kỹ thuật của sáng chế

Hiện nay, truyền thông giữa thiết bị với thiết bị (device to device, D2D) cho phép truyền thông trực tiếp giữa các thiết bị người dùng (user equipment, UE).

Khi thiết bị từ xa (remote UE) nằm bên ngoài vùng phủ sóng của mạng truyền thông hoặc chất lượng truyền thông giữa thiết bị từ xa và thiết bị mạng truy cập trong mạng truyền thông kém, thì thiết bị từ xa có thể thiết lập truyền thông gián tiếp với mạng truyền thông bằng cách sử dụng thiết bị chuyển tiếp (UE chuyển tiếp) dựa vào truyền thông D2D. Thiết bị chuyển tiếp có thể thiết lập phiên của đơn vị dữ liệu giao thức (protocol data unit, PDU) để truyền dịch vụ giữa thiết bị từ xa và mạng dữ liệu, và truyền dữ liệu nhận được từ thiết bị từ xa đến mạng dữ liệu bằng cách sử dụng phiên PDU, hoặc gửi dữ liệu thu được từ mạng dữ liệu đến thiết bị từ xa bằng cách sử dụng phiên PDU.

Trong quy trình thiết lập phiên PDU, phần tử mạng quản lý phiên thu mã nhận dạng của thiết bị chuyển tiếp, và thu chính sách bảo mật mặt phẳng người dùng của phiên từ phần tử mạng quản lý dữ liệu hợp nhất hoặc cục bộ bằng cách sử dụng mã nhận dạng của thiết bị chuyển tiếp. Ngoài ra, phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng của phiên theo chính sách bảo mật mặt phẳng người dùng. Thông tin tăng cường bảo mật mặt phẳng người dùng được sử dụng bởi thiết bị mạng truy cập để tạo cấu hình trạng thái kích hoạt bảo mật giữa thiết bị chuyển tiếp và thiết bị mạng truy cập. Trong quy trình xác định chính sách bảo mật mặt phẳng người dùng của phiên PDU, phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng của phiên PDU đã thiết lập dựa vào thông tin thuê bao hoặc thông tin được tạo cấu hình trước của thiết bị chuyển tiếp. Vì phiên PDU đã thiết lập có thể là phiên PDU mà truyền dịch vụ giữa thiết bị từ xa và mạng dữ liệu, đây có thể là phương pháp để xác định việc bảo vệ bảo mật mặt phẳng người dùng chỉ bằng

cách sử dụng thông tin thuê bao hoặc thông tin được tạo cấu hình trước của thiết bị chuyển tiếp không thể đáp ứng yêu cầu bảo mật của dữ liệu đã truyền của thiết bị từ xa.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, thiết bị và hệ thống, để đảm bảo yêu cầu bảo mật của dữ liệu được truyền của thiết bị từ xa.

Theo khía cạnh thứ nhất, một phương án của sáng chế đề xuất phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng. Phương pháp này bao gồm các bước: Trước tiên, phần tử mạng quản lý phiên có thể nhận yêu cầu thứ nhất từ phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thứ nhất yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, yêu cầu thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Sau đó, phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất; và sau đó gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể thu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp bằng cách sử dụng thông tin thứ nhất. Sau đó, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất đã xác định cũng có thể đáp ứng yêu cầu bảo mật của thiết bị từ xa, và đảm bảo độ bảo mật dữ liệu của thiết bị từ xa.

Theo thiết kế khả thi, yêu cầu thứ nhất có thể bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ nhất. Trong trường hợp này, yêu cầu thứ nhất có thể là yêu cầu thiết lập phiên. Yêu cầu thứ nhất có thể theo cách khác bao gồm thông tin thứ nhất và vùng chứa N1 SM. Trong trường hợp này, yêu cầu thứ nhất bao gồm yêu cầu thiết lập phiên và thông tin thứ nhất. Vùng chứa N1 SM là từ thiết bị đầu cuối thứ nhất.

Theo phương pháp nêu trên, thiết bị đầu cuối thứ nhất có thể gửi, đến phần tử mạng quản lý phiên bằng cách sử dụng phần tử mạng quản lý truy cập và di động, vùng chứa N1 SM bao gồm thông tin thứ nhất. Thông tin thứ nhất có thể theo cách khác được gửi bởi phần tử mạng quản lý truy cập và di động đến phần tử mạng quản lý phiên.

Nghĩa là, có các dạnh thành phần của yêu cầu thứ nhất mà áp dụng được cho các kịch bản ứng dụng khác nhau.

Theo thiết kế khả thi, khi phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất, thì phần tử mạng quản lý phiên có thể trước tiên thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất; và sau đó có thể trực tiếp sử dụng chính sách bảo mật mặt phẳng người dùng thứ nhất làm thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên; hoặc có thể thực hiện thêm việc phân tích dựa vào thông tin xác định khác (ví dụ, yêu cầu chất lượng dịch vụ), và xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo phương pháp nêu trên, sau khi thu chính sách bảo mật mặt phẳng người dùng thứ nhất, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất theo nhiều cách.

Theo thiết kế khả thi, phần tử mạng quản lý phiên thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất bao gồm: Phần tử mạng quản lý phiên gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất có thể yêu cầu chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký biểu thị chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau đó, phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Phần tử mạng quản lý phiên xác định, dựa vào thông tin thứ nhất, chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và xác định chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất làm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo phương pháp nêu trên, sau khi thu, từ phần tử mạng quản lý dữ liệu hợp nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, phần tử mạng quản lý phiên có thể chọn, dựa vào thông tin thứ nhất, chính sách bảo mật

mặt phẳng người dùng thứ nhất từ chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, sao cho thông tin tăng cường bảo mật mặt phẳng người dùng áp dụng được cho phiên chuyển tiếp có thể được xác định cuối cùng.

Theo thiết kế khả thi, khi phần tử mạng quản lý phiên thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất,

phần tử mạng quản lý phiên có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm chỉ báo chuyển tiếp, chỉ báo chuyển tiếp yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và chỉ báo chuyển tiếp có thể là thông tin thứ nhất (trong đó đối với cách này, dựa vào nội dung nêu trên), hoặc chỉ báo chuyển tiếp có thể được xác định dựa vào thông tin thứ nhất; và sau đó, phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể thu, dựa vào chỉ báo chuyển tiếp từ phần tử mạng quản lý dữ liệu hợp nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Ví dụ, khi thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, chỉ báo chuyển tiếp có thể sử dụng theo cách chỉ báo rõ ràng, sao cho phần tử mạng quản lý dữ liệu hợp nhất không cần xác định mã nhận dạng của thiết bị đầu cuối thứ hai, và có thể xác định một cách nhanh chóng chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Theo thiết kế khả thi, khi thông tin thứ nhất biểu thị ngầm rằng kiểu của phiên là kiểu chuyển tiếp, ví dụ, thông tin thứ nhất có thể là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai, phần tử mạng quản lý phiên có thể trước tiên thu SUPI của thiết bị đầu cuối thứ hai dựa vào mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai khi thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào yêu cầu thứ nhất. Ví dụ, phần tử mạng quản lý phiên có thể thu SUPI của thiết bị đầu cuối thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất. Sau đó, phần tử mạng quản lý phiên có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm SUPI của thiết bị đầu cuối thứ hai. Sau đó, phần tử mạng quản lý phiên nhận phản

hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó thông tin được mang trong phản hồi thu thông tin thuê bao thứ nhất có thể là bất kỳ trong số sau:

1. Phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

2. Phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau đó, phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất theo chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

3. Phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký. Sau đó, phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể thu chính sách bảo mật mặt phẳng người dùng thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất theo cách khác nhau.

Theo thiết kế khả thi, khi phần tử mạng quản lý phiên thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào yêu cầu thứ nhất, thì phần tử mạng quản lý phiên có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất. Phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể trực tiếp thu chính sách bảo mật mặt phẳng người dùng thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất. Cách này đơn giản và hiệu quả hơn.

Theo thiết kế khả thi, có nhiều cách trong đó thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Ví dụ, thông tin thứ nhất sử dụng cách chỉ báo rõ ràng. Ví dụ, thông tin thứ nhất có thể là trường hoặc ký tự được thỏa thuận trước. Ví dụ khác, thông tin thứ nhất có thể theo cách khác sử dụng cách chỉ báo ngầm. Ví dụ, thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu

cuối thứ hai này bao gồm một phần hoặc tất cả các mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc mã nhận dạng cố định thuê bao (subscription permanent identifier, SUPI) của thiết bị đầu cuối thứ hai.

Theo phương pháp nêu trên, thông tin thứ nhất có thể biểu thị một cách linh hoạt, theo cách khác nhau, rằng kiểu của phiên là kiểu chuyển tiếp.

Theo thiết kế khả thi, chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được ưu tiên. Khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất, thì phần tử mạng quản lý phiên có thể còn đề cập đến tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất. Ví dụ, nếu phần tử mạng quản lý phiên xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, thì phần tử mạng quản lý phiên có thể xác định rằng việc bảo vệ tính toàn vẹn của phiên là không cần thiết, nghĩa là, việc bảo vệ tính toàn vẹn của phiên trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất là không cần thiết.

Theo phương pháp nêu trên, ngoài việc đảm bảo yêu cầu bảo mật của thiết bị đầu cuối thứ hai, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất được xác định bởi phần tử mạng quản lý phiên có thể còn đảm bảo rằng thiết bị đầu cuối thứ nhất có thể truyền một cách hiệu quả dữ liệu của thiết bị đầu cuối thứ hai bằng cách sử dụng phiên.

Theo thiết kế khả thi, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu, thì phần tử mạng quản lý phiên có thể gửi phản hồi từ chối thiết lập phiên đến thiết bị đầu cuối thứ nhất sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, trong đó phản hồi từ chối thiết lập phiên biểu thị việc từ chối thiết lập phiên.

Theo phương pháp nêu trên, sau khi xác định rằng thiết bị đầu cuối thứ nhất có thể hỗ trợ việc truyền dữ liệu của thiết bị đầu cuối thứ hai khi việc bảo vệ tính toàn vẹn được kích hoạt, phần tử mạng quản lý phiên có thể từ chối thiết lập phiên, sao cho độ bảo mật dữ liệu của thiết bị đầu cuối thứ hai có thể được đảm bảo.

Theo thiết kế khả thi, phần tử mạng quản lý phiên có thể còn nhận yêu cầu thứ

ba, trong đó yêu cầu thứ ba có thể biểu thị rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, yêu cầu thứ ba bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba, và yêu cầu thứ ba có thể là yêu cầu sửa đổi phiên, hoặc có thể là yêu cầu khác. Sau khi xác định, dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên, và gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể cập nhật thông tin tăng cường bảo mật mặt phẳng người dùng của phiên, cần áp dụng được cho yêu cầu bảo mật của thiết bị đầu cuối thứ ba.

Theo thiết kế khả thi, khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, thì phần tử mạng quản lý phiên có thể xác định chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba; và sau đó có thể trực tiếp sử dụng chính sách bảo mật mặt phẳng người dùng thứ hai làm thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên; hoặc có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào thông tin xác định khác (ví dụ, yêu cầu chất lượng dịch vụ).

Theo phương pháp nêu trên, sau khi thu chính sách bảo mật mặt phẳng người dùng thứ hai, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai theo nhiều cách.

Theo thiết kế khả thi, mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một phần hoặc tất cả các mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba hoặc SUPI của thiết bị đầu cuối thứ ba.

Theo phương pháp nêu trên, các mã nhận dạng khác nhau biểu thị thiết bị đầu cuối thứ ba, và áp dụng được cho nhiều kịch bản.

Theo thiết kế khả thi, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt

phẳng người dùng thứ hai theo cách bất kỳ trong số cách sau:

Cách 1: Phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên.

Cách 2: Phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất.

Cách 3: Phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chỉ theo chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai theo cách khác nhau mà áp dụng được cho các kịch bản ứng dụng khác nhau.

Theo thiết kế khả thi, phần tử mạng quản lý phiên thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba là tương tự để thu chính sách bảo mật mặt phẳng người dùng thứ nhất.

Ví dụ, phần tử mạng quản lý phiên gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai.

Ví dụ khác, phần tử mạng quản lý phiên có thể theo cách khác xác định, dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, chính sách bảo mật mặt phẳng người dùng thứ hai trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Ví dụ khác, phần tử mạng quản lý phiên gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Phần tử mạng

quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ hai theo chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

Ví dụ khác, phần tử mạng quản lý phiên gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ ba đăng ký. Phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ hai theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ ba đăng ký.

Theo phương pháp nêu trên, phần tử mạng quản lý phiên có thể thu một cách linh hoạt chính sách bảo mật mặt phẳng người dùng thứ hai, và kịch bản ứng dụng được mở rộng một cách hiệu quả.

Theo thiết kế khả thi, sau khi phần tử mạng quản lý phiên xác định rằng thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên, phần tử mạng quản lý phiên có thể gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập. Sau khi phần tử mạng quản lý phiên xác định rằng thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên giống với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên, phần tử mạng quản lý phiên có thể không gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập.

Theo phương pháp nêu trên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên được so sánh với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên, để xác định xem có gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên được xác định hay không, sao cho sự trao đổi thông tin giữa phần tử mạng quản lý phiên và thiết bị mạng truy cập có thể cũng được giảm bớt.

Theo thiết kế khả thi, chính sách bảo mật mặt phẳng người dùng thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn của phiên được ưu tiên. Phần tử mạng quản lý phiên có thể theo cách khác xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất. Ví dụ, sau khi xác định

rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, phần tử mạng quản lý phiên xác định để vô hiệu hóa việc bảo vệ tính toàn vẹn của phiên, nghĩa là, việc bảo vệ tính toàn vẹn của phiên trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai không cần thiết.

Theo phương pháp nêu trên, ngoài việc đảm bảo yêu cầu bảo mật của thiết bị đầu cuối thứ ba, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai được xác định bởi phần tử mạng quản lý phiên có thể còn đảm bảo rằng thiết bị đầu cuối thứ nhất có thể truyền một cách hiệu quả dữ liệu của thiết bị đầu cuối thứ ba bằng cách sử dụng phiên.

Theo khía cạnh thứ hai, một phương án của sáng chế đề xuất phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng. Phương pháp này bao gồm các bước: Trước tiên, thiết bị đầu cuối thứ nhất có thể gửi yêu cầu thứ hai đến phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thứ hai yêu cầu tạo ra phiên kiểu chuyển tiếp, yêu cầu thứ hai bao gồm thông tin thứ hai, và thông tin thứ hai này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Sau đó, thiết bị đầu cuối thứ nhất có thể nhận thông tin chỉ báo thứ nhất từ thiết bị mạng truy cập, trong đó thông tin chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập. Thiết bị đầu cuối thứ nhất tạo cấu hình trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin chỉ báo thứ nhất.

Theo phương pháp nêu trên, khi khởi tạo thủ tục tạo phiên, thiết bị đầu cuối thứ nhất có thể còn biểu thị kiểu phiên của phiên, sao cho phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng của phiên.

Theo thiết kế khả thi, thiết bị đầu cuối thứ nhất có thể nhận yêu cầu truyền thông trực tiếp thứ nhất được gửi bởi thiết bị đầu cuối thứ hai, trong đó yêu cầu truyền thông trực tiếp thứ nhất là để thiết lập truyền thông với thiết bị đầu cuối thứ nhất. Thiết bị đầu cuối thứ nhất có thể xác định rằng phiên kiểu chuyển tiếp cần được thiết lập, và gửi yêu cầu thứ hai. Thiết bị đầu cuối thứ nhất có thể tạo ra phiên kiểu chuyển tiếp trước. Nghĩa là, thiết bị đầu cuối thứ nhất có thể gửi yêu cầu thứ hai trước khi nhận nhận yêu cầu truyền thông trực tiếp thứ nhất của thiết bị đầu cuối thứ hai.

Theo phương pháp nêu trên, thiết bị đầu cuối thứ nhất có thể xác định, trong các kịch bản khác nhau, rằng phiên kiểu chuyển tiếp cần được tạo, và gửi yêu cầu thứ hai.

Theo thiết kế khả thi, yêu cầu thứ hai có thể bao gồm vùng chứa N1 SM, và vùng

chứa N1 SM này bao gồm thông tin thứ hai. Trong trường hợp này, yêu cầu thứ hai có thể là yêu cầu thiết lập phiên. Yêu cầu thứ hai có thể theo cách khác bao gồm thông tin thứ hai và vùng chứa N1 SM. Trong trường hợp này, yêu cầu thứ hai bao gồm yêu cầu thiết lập phiên (cụ thể là, vùng chứa N1 SM) và thông tin thứ hai.

Theo phương pháp nêu trên, có các dạng thành phần của yêu cầu thứ hai mà áp dụng được cho các kịch bản ứng dụng khác nhau.

Theo thiết kế khả thi, có nhiều cách trong đó thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Ví dụ, thông tin thứ hai sử dụng cách chỉ báo rõ ràng. Ví dụ, thông tin thứ hai có thể là trường hoặc ký tự được thỏa thuận trước. Ví dụ khác, thông tin thứ hai có thể theo cách khác sử dụng cách chỉ báo ngầm. Ví dụ, thông tin thứ hai là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu cuối thứ hai là một trong số sau: mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai, hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ hai. Trong trường hợp này, phiên là để truyền dữ liệu của thiết bị đầu cuối thứ hai.

Theo phương pháp nêu trên, thông tin thứ hai có thể biểu thị một cách linh hoạt, theo cách khác nhau, rằng kiểu của phiên là kiểu chuyển tiếp.

Theo thiết kế khả thi, thiết bị đầu cuối thứ nhất có thể còn nhận yêu cầu truyền thông trực tiếp thứ hai được gửi bởi thiết bị đầu cuối thứ ba, trong đó yêu cầu truyền thông trực tiếp thứ hai là để thiết lập truyền thông với thiết bị đầu cuối thứ nhất. Thiết bị đầu cuối thứ nhất xác định, dựa vào yêu cầu truyền thông trực tiếp thứ hai, rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, và sau đó gửi yêu cầu thứ ba, trong đó yêu cầu thứ ba biểu thị rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, và yêu cầu thứ ba bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Yêu cầu thứ ba có thể là yêu cầu sửa đổi phiên hoặc có thể là yêu cầu khác.

Theo phương pháp nêu trên, khi thiết bị đầu cuối thứ ba là để sử dụng lại phiên, thì thiết bị đầu cuối thứ nhất có thể thông báo, bằng cách gửi yêu cầu thứ ba, phần tử mạng quản lý phiên rằng thiết bị đầu cuối thứ ba là để sử dụng lại phiên, sao cho phần tử mạng quản lý phiên tái xác định thông tin tăng cường bảo mật mặt phẳng người dùng.

Theo thiết kế khả thi, mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một hoặc nhiều mã nhận dạng trong số sau: mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba hoặc SUPI của thiết bị đầu cuối thứ ba.

Theo phương pháp nêu trên, mã nhận dạng của thiết bị đầu cuối thứ ba có thể là các kiểu mã nhận dạng khác nhau mà áp dụng được cho các kịch bản ứng dụng khác nhau.

Theo thiết kế khả thi, sau khi nhận, từ thiết bị mạng truy cập, thông tin chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất, thiết bị đầu cuối thứ nhất có thể xác định trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất.

Theo phương pháp nêu trên, thiết bị đầu cuối thứ nhất có thể tạo cấu hình trạng thái kích hoạt bảo mật của giao diện PC5 (giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai), để đảm bảo độ bảo mật dữ liệu của thiết bị đầu cuối thứ hai.

Theo thiết kế khả thi, nếu việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất được yêu cầu, thiết bị đầu cuối thứ nhất có thể còn đề cập đến tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển Qos của thiết bị đầu cuối thứ hai khi tạo cấu hình trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất, nghĩa là, xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển QoS của thiết bị đầu cuối thứ hai, xem có kích hoạt việc bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai hay không.

Theo phương pháp nêu trên, ngoài việc đảm bảo độ bảo mật dữ liệu của thiết bị đầu cuối thứ hai, trạng thái kích hoạt bảo mật mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai có thể còn đảm bảo rằng thiết bị đầu cuối thứ hai có thể truyền một cách hiệu quả dữ liệu đến thiết bị đầu cuối thứ nhất.

Theo thiết kế khả thi, nếu việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất là không cần thiết, thì thiết bị đầu cuối thứ nhất gửi thông điệp từ chối truyền thông trực tiếp đến thiết bị đầu cuối thứ hai khi xác định rằng chính sách bảo mật mặt phẳng người dùng của thiết bị đầu cuối thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu (trong đó thông tin có thể được mang trong yêu cầu truyền thông trực tiếp thứ nhất).

Theo phương pháp nêu trên, khi xác định rằng thiết bị đầu cuối thứ hai có thể hỗ trợ việc truyền dữ liệu khi việc bảo vệ tính toàn vẹn được kích hoạt, thì thiết bị đầu cuối thứ nhất có thể từ chối thiết lập truyền thông trực tiếp, sao cho độ bảo mật dữ liệu của

thiết bị đầu cuối thứ hai có thể được đảm bảo.

Theo thiết kế khả thi, thiết bị đầu cuối thứ nhất có thể còn nhận thông tin chỉ báo thứ hai từ thiết bị mạng truy cập, trong đó thông tin chỉ báo thứ hai biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập; và sau đó cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin chỉ báo thứ hai, nghĩa là, cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất thành trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai dựa vào thông tin chỉ báo thứ hai.

Theo phương pháp nêu trên, thiết bị đầu cuối thứ nhất có thể cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập, để đảm bảo độ bảo mật dữ liệu của thiết bị đầu cuối thứ ba.

Theo thiết kế khả thi, sau khi nhận thông tin chỉ báo thứ hai được gửi bởi thiết bị mạng truy cập, thiết bị đầu cuối thứ nhất có thể còn cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai.

Theo phương pháp nêu trên, thiết bị đầu cuối thứ nhất có thể cập nhật trạng thái kích hoạt bảo mật của giao diện PC5 (giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ ba), để đảm bảo độ bảo mật dữ liệu của thiết bị đầu cuối thứ ba.

Theo thiết kế khả thi, việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai được yêu cầu. Khi cập nhật trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai, thiết bị đầu cuối thứ nhất có thể còn xem xét tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển Qos của thiết bị đầu cuối thứ ba, và xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển chất lượng dịch vụ (QoS) của thiết bị đầu cuối thứ ba, xem có kích hoạt việc bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai hay không.

Theo phương pháp nêu trên, ngoài việc đảm bảo độ bảo mật dữ liệu của thiết bị đầu cuối thứ ba, trạng thái kích hoạt bảo mật mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ ba có thể còn đảm bảo rằng thiết bị đầu cuối thứ ba có thể truyền một cách hiệu quả dữ liệu đến thiết bị đầu cuối thứ nhất.

Theo khía cạnh thứ ba, một phương án của sáng chế đề xuất phương pháp xác

định thông tin tăng cường bảo mật mặt phẳng người dùng. Phương pháp này bao gồm các bước: Trước tiên, phần tử mạng quản lý truy cập và di động nhận yêu cầu thứ hai được gửi bởi thiết bị đầu cuối thứ nhất, trong đó yêu cầu thứ hai bao gồm thông tin thứ hai, yêu cầu thứ hai yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Sau đó, phần tử mạng quản lý truy cập và di động gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên dựa vào yêu cầu thứ hai, trong đó yêu cầu thứ nhất bao gồm thông tin thứ nhất, thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp, và yêu cầu thứ nhất yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

Theo phương pháp nêu trên, sau khi nhận yêu cầu thứ hai bao gồm thông tin thứ hai, phần tử mạng quản lý truy cập và di động gửi, đến phần tử mạng quản lý phiên kịp thời, yêu cầu thứ nhất bao gồm thông tin thứ nhất, sao cho phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng của phiên dựa vào thông tin thứ nhất.

Theo thiết kế khả thi, thông tin thứ hai giống với thông tin thứ nhất, mỗi trong số yêu cầu thứ nhất và yêu cầu thứ hai bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ hai. Trong trường hợp này, yêu cầu thứ nhất và yêu cầu thứ hai có thể là yêu cầu thiết lập phiên. Nghĩa là, yêu cầu thứ nhất giống với yêu cầu thứ hai. Phần tử mạng quản lý truy cập và di động có thể truyền trực tiếp yêu cầu thứ nhất đến phần tử mạng quản lý phiên.

Theo thiết kế khả thi, yêu cầu thứ hai bao gồm thông tin thứ hai và vùng chứa N1 SM, và yêu cầu thứ nhất bao gồm thông tin thứ nhất và vùng chứa N1 SM.

Theo phương pháp nêu trên, vì thông tin thứ hai nằm bên ngoài vùng chứa N1 SM, nên phần tử mạng quản lý truy cập và di động có thể xác định thông tin thứ hai, và còn xác định thông tin thứ nhất mà cần được mang trong yêu cầu thứ nhất.

Theo thiết kế khả thi, khi gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên dựa vào thông tin thứ hai, phần tử mạng quản lý truy cập và di động có thể trước tiên xác định, dựa vào thông tin thứ hai, xem thiết bị đầu cuối thứ nhất có được ủy quyền để thiết lập phiên hay không. Nếu phần tử mạng quản lý truy cập và di động xác định rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên, phần tử mạng quản lý truy cập và di động gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên; nếu không thì, phần tử mạng quản lý truy cập và di động có thể trực tiếp từ chối thiết lập phiên.

Theo phương pháp nêu trên, phần tử mạng quản lý truy cập và di động có thể

thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ nhất dựa vào thông tin thứ hai trước, để đảm bảo rằng phiên có thể được thiết lập một cách hiệu quả sau đó.

Theo thiết kế khả thi, thông tin thứ hai là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai. Phần tử mạng quản lý truy cập và di động có thể xác định SUPI của thiết bị đầu cuối thứ hai dựa vào thông tin thứ hai, trong đó SUPI của thiết bị đầu cuối thứ hai có thể được sử dụng làm thông tin thứ nhất.

Theo phương pháp nêu trên, phần tử mạng quản lý truy cập và di động có thể xác định SUPI của thiết bị đầu cuối thứ hai, và thiết bị đầu cuối thứ nhất không cần truyền SUPI của thiết bị đầu cuối thứ hai, sao cho độ bảo mật SUPI của thiết bị đầu cuối thứ hai được đảm bảo.

Theo thiết kế khả thi, có nhiều cách trong đó thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Ví dụ, thông tin thứ hai sử dụng cách chỉ báo rõ ràng. Ví dụ, thông tin thứ hai có thể là trường hoặc ký tự được thỏa thuận trước. Ví dụ khác, thông tin thứ hai có thể theo cách khác sử dụng cách chỉ báo ngầm. Ví dụ, thông tin thứ hai là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu cuối thứ hai là một trong số sau: mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ hai.

Theo phương pháp nêu trên, thông tin thứ hai có thể biểu thị một cách linh hoạt, theo cách khác nhau, rằng kiểu của phiên là kiểu chuyển tiếp.

Theo thiết kế khả thi, có nhiều cách trong đó thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Ví dụ, thông tin thứ nhất sử dụng cách chỉ báo rõ ràng. Ví dụ, thông tin thứ nhất có thể là trường hoặc ký tự được thỏa thuận trước. Ví dụ khác, thông tin thứ nhất có thể theo cách khác sử dụng cách chỉ báo ngầm. Ví dụ, thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu cuối thứ hai bao gồm một phần hoặc tất cả các mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ hai.

Theo phương pháp nêu trên, thông tin thứ nhất có thể biểu thị một cách linh hoạt, theo cách khác nhau, rằng kiểu của phiên là kiểu chuyển tiếp.

Theo thiết kế khả thi, trước khi gửi yêu cầu thứ nhất đến phần tử mạng quản lý

phiên dựa vào yêu cầu thứ hai, phần tử mạng quản lý truy cập và di động có thể còn xác định, dựa vào thông tin thứ hai, rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên cho thiết bị đầu cuối thứ hai.

Theo phương pháp nêu trên, phần tử mạng quản lý truy cập và di động có thể thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ hai dựa vào thông tin thứ hai trước, để đảm bảo rằng thiết bị đầu cuối thứ nhất có thể truyền dữ liệu của thiết bị đầu cuối thứ hai.

Theo khía cạnh thứ tư, một phương án của sáng chế đề xuất phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng. Phương pháp này bao gồm: Phần tử mạng quản lý dữ liệu hợp nhất có thể cung cấp chính sách bảo mật mặt phẳng người dùng thứ nhất cho phần tử mạng quản lý phiên. Phần sau đề xuất hai cách:

Cách 1: Phần tử mạng quản lý dữ liệu hợp nhất có thể nhận yêu cầu thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu phiên là kiểu chuyển tiếp. Phần tử mạng quản lý dữ liệu hợp nhất xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất. Sau đó, phần tử mạng quản lý dữ liệu hợp nhất gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo cách nêu trên, phần tử mạng quản lý dữ liệu hợp nhất có thể trực tiếp xác định chính sách bảo mật mặt phẳng người dùng thứ nhất, và phản hồi lại chính sách bảo mật mặt phẳng người dùng thứ nhất cho phần tử mạng quản lý phiên.

Cách 2: Phần tử mạng quản lý dữ liệu hợp nhất nhận yêu cầu thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ nhất yêu cầu chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký biểu thị chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất. Phần tử mạng quản lý dữ liệu hợp nhất gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt

phẳng người dùng thứ nhất.

Theo cách nêu trên, phần tử mạng quản lý dữ liệu hợp nhất có thể chỉ cần phản hồi lại, cho phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và sau đó phần tử mạng quản lý phiên có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo thiết kế khả thi, khi phần tử mạng quản lý dữ liệu hợp nhất xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, thì phần tử mạng quản lý dữ liệu hợp nhất có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, trong đó chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký biểu thị các chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp và phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất.

Theo phương pháp nêu trên, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định, dựa vào thông tin thứ nhất, rằng phiên là phiên kiểu chuyển tiếp, và sau đó có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo thiết kế khả thi, thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai. Khi phần tử mạng quản lý dữ liệu hợp nhất xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất xác định, dựa vào mã nhận dạng của thiết bị đầu cuối thứ hai, chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

Theo phương pháp nêu trên, chính sách bảo mật mặt phẳng người dùng thứ nhất được xác định theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký có thể đảm bảo yêu cầu bảo mật của thiết bị đầu cuối thứ hai.

Theo thiết kế khả thi, phần tử mạng quản lý dữ liệu hợp nhất nhận yêu cầu thu thông tin thuê bao thứ hai từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Sau đó, phần tử mạng quản lý dữ liệu hợp nhất xác định chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba; và sau đó gửi phản hồi thu thông tin thuê bao thứ hai đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo phương pháp nêu trên, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định, dựa vào yêu cầu thu thông tin thuê bao thứ hai, rằng phiên là phiên kiểu chuyển tiếp, và sau đó có thể xác định chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo khía cạnh thứ năm, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong phần tử mạng quản lý phiên. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ nhất. Các chi tiết không được mô tả lại trong bản mô tả này. Thiết bị có chức năng thực hiện hành vi trong ví dụ về phương pháp theo khía cạnh thứ nhất. Chức năng có thể được thực hiện bằng cách sử dụng phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Theo thiết kế khả thi, cấu trúc của thiết bị bao gồm bộ phận nhận, bộ phận xử lý và bộ phận gửi. Các bộ phận này có thể thực hiện các chức năng tương ứng trong ví dụ về phương pháp theo khía cạnh thứ nhất. Để biết chi tiết, dựa vào các phần mô tả chi tiết trong ví dụ về phương pháp. Các chi tiết không được mô tả lại trong bản mô tả này.

Theo khía cạnh thứ sáu, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong thiết bị đầu cuối thứ nhất. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ hai. Các chi tiết không được mô tả lại trong bản mô tả này. Thiết bị có chức năng thực hiện hành vi trong ví dụ về phương pháp theo khía cạnh thứ hai. Chức năng có thể được thực hiện bằng cách sử dụng phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Theo thiết kế khả thi, cấu trúc của thiết bị bao gồm bộ phận nhận và bộ phận gửi, và một cách tùy chọn, còn bao gồm bộ phận xử lý. Các bộ phận này có thể thực hiện các chức năng tương ứng trong ví dụ về phương pháp theo khía cạnh thứ hai. Để biết chi tiết, dựa vào các phần mô tả chi tiết trong ví dụ về phương pháp. Các chi tiết không được mô tả lại trong bản mô tả này.

Theo khía cạnh thứ bảy, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong phần tử mạng quản lý truy cập và di động. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ ba. Các chi tiết không được mô tả lại trong bản mô tả này. Thiết bị có chức năng thực hiện hành vi trong ví dụ về phương pháp theo khía cạnh thứ ba. Chức năng có thể được thực hiện bằng cách sử dụng phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng

với chức năng nêu trên. Theo thiết kế khả thi, cấu trúc của thiết bị bao gồm bộ phận nhận và bộ phận gửi, và một cách tùy chọn, còn bao gồm bộ phận xử lý. Các bộ phận này có thể thực hiện các chức năng tương ứng trong ví dụ về phương pháp theo khía cạnh thứ ba. Để biết chi tiết, dựa vào các phần mô tả chi tiết trong ví dụ về phương pháp. Các chi tiết không được mô tả lại trong bản mô tả này.

Theo khía cạnh thứ tám, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong phần tử mạng quản lý dữ liệu hợp nhất. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ tư. Các chi tiết không được mô tả lại trong bản mô tả này. Thiết bị có chức năng thực hiện hành vi trong ví dụ về phương pháp theo khía cạnh thứ tư. Chức năng có thể được thực hiện bằng cách sử dụng phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Theo thiết kế khả thi, cấu trúc của thiết bị bao gồm bộ phận nhận và bộ phận gửi, và một cách tùy chọn, còn bao gồm bộ phận xử lý. Các bộ phận này có thể thực hiện các chức năng tương ứng trong ví dụ về phương pháp theo khía cạnh thứ tư. Để biết chi tiết, dựa vào các phần mô tả chi tiết trong ví dụ về phương pháp. Các chi tiết không được mô tả lại trong bản mô tả này.

Theo khía cạnh thứ chín, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong phần tử mạng quản lý phiên. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ nhất. Các chi tiết không được mô tả lại trong bản mô tả này. Cấu trúc của thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ. Bộ xử lý được tạo cấu hình để hỗ trợ phần tử mạng quản lý phiên trong khi thực hiện các chức năng tương ứng trong phương pháp theo khía cạnh thứ nhất. Bộ nhớ được ghép nối với bộ xử lý, và lưu trữ các lệnh chương trình và dữ liệu mà cần thiết cho thiết bị truyền thông. Cấu trúc của thiết bị truyền thông còn bao gồm giao diện truyền thông được tạo cấu hình để truyền thông với thiết bị khác.

Theo khía cạnh thứ mười, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong thiết bị đầu cuối thứ nhất. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ hai. Các chi tiết không được mô tả lại trong bản mô tả này. Cấu trúc của thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ. Bộ xử lý được tạo cấu hình để hỗ trợ thiết bị đầu cuối thứ nhất trong khi thực hiện các chức năng tương ứng trong phương pháp theo khía cạnh thứ hai. Bộ nhớ được ghép nối với bộ xử lý, và lưu trữ các lệnh chương trình và dữ liệu mà cần thiết cho thiết bị truyền thông. Cấu trúc của thiết bị truyền thông còn bao gồm bộ thu-phát được tạo

cấu hình để truyền thông với thiết bị khác.

Theo khía cạnh thứ mười một, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong phần tử mạng quản lý truy cập và di động. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ ba. Các chi tiết không được mô tả lại trong bản mô tả này. Cấu trúc của thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ. Bộ xử lý được tạo cấu hình để hỗ trợ phần tử mạng quản lý truy cập và di động trong khi thực hiện các chức năng tương ứng trong phương pháp theo khía cạnh thứ ba. Bộ nhớ được ghép nối với bộ xử lý, và lưu trữ các lệnh chương trình và dữ liệu mà cần thiết cho thiết bị truyền thông. Cấu trúc của thiết bị truyền thông còn bao gồm giao diện truyền thông được tạo cấu hình để truyền thông với thiết bị khác.

Theo khía cạnh thứ mười hai, một phương án của sáng chế còn đề xuất thiết bị truyền thông. Thiết bị truyền thông này được sử dụng trong phần tử mạng quản lý dữ liệu hợp nhất. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo khía cạnh thứ tư. Các chi tiết không được mô tả lại trong bản mô tả này. Cấu trúc của thiết bị truyền thông bao gồm bộ xử lý và bộ nhớ. Bộ xử lý được tạo cấu hình để hỗ trợ phần tử mạng quản lý dữ liệu hợp nhất trong khi thực hiện các chức năng tương ứng trong phương pháp theo khía cạnh thứ tư. Bộ nhớ được ghép nối với bộ xử lý, và lưu trữ các lệnh chương trình và dữ liệu mà cần thiết cho thiết bị truyền thông. Cấu trúc của thiết bị truyền thông còn bao gồm giao diện truyền thông được tạo cấu hình để truyền thông với thiết bị khác.

Theo khía cạnh thứ mười ba, một phương án của sáng chế còn đề xuất hệ thống truyền thông. Đối với các hiệu quả có lợi, dựa vào các phần mô tả theo các khía cạnh nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Hệ thống truyền thông bao gồm phần tử mạng quản lý phiên và phần tử mạng quản lý dữ liệu hợp nhất.

Phần tử mạng quản lý phiên được tạo cấu hình để gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm chỉ báo chuyển tiếp, và chỉ báo chuyển tiếp này yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

Phần tử mạng quản lý dữ liệu hợp nhất được tạo cấu hình để: nhận yêu cầu thu thông tin thuê bao thứ nhất; xác định, dựa vào thông tin thứ nhất, chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng mà

thiết bị đầu cuối thứ nhất đăng ký, trong đó chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất; và gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Phần tử mạng quản lý phiên còn được tạo cấu hình để nhận phản hồi thu thông tin thuê bao thứ nhất.

Theo thiết kế khả thi, hệ thống còn bao gồm phần tử mạng quản lý truy cập và di động.

Phần tử mạng quản lý truy cập và di động được tạo cấu hình để gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên, trong đó yêu cầu thứ nhất yêu cầu để thiết lập phiên kiểu chuyển tiếp cho thiết bị đầu cuối thứ nhất, yêu cầu thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp.

Phần tử mạng quản lý phiên được tạo cấu hình để nhận yêu cầu thứ nhất, trong đó chỉ báo chuyển tiếp là thông tin thứ nhất hoặc được xác định dựa vào thông tin thứ nhất.

Theo thiết kế khả thi, phiên là để truyền dữ liệu của thiết bị đầu cuối thứ hai, thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu cuối thứ hai bao gồm một phần hoặc tất cả các mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc SUPI của thiết bị đầu cuối thứ hai.

Theo thiết kế khả thi, hệ thống còn bao gồm thiết bị mạng truy cập.

Phần tử mạng quản lý phiên còn được tạo cấu hình để gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên đến thiết bị mạng truy cập sau khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất.

Thiết bị mạng truy cập được tạo cấu hình để nhận thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên, và kích hoạt trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập dựa vào thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên.

Theo thiết kế khả thi, hệ thống còn bao gồm thiết bị đầu cuối thứ nhất.

Thiết bị mạng truy cập còn được tạo cấu hình để gửi thông điệp chỉ báo thứ nhất đến thiết bị đầu cuối thứ nhất, trong đó thông điệp chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Thiết bị đầu cuối thứ nhất được tạo cấu hình để: nhận thông điệp chỉ báo thứ nhất, và kích hoạt trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập dựa vào thông tin chỉ báo thứ nhất; và tạo cấu hình trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất.

Theo thiết kế khả thi, thiết bị đầu cuối thứ nhất còn được tạo cấu hình để gửi yêu cầu thứ hai đến phần tử mạng quản lý phiên sau khi xác định rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, trong đó yêu cầu thứ hai yêu cầu để sửa đổi phiên, và yêu cầu thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba.

Phần tử mạng quản lý phiên còn được tạo cấu hình để thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, và gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập sau khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai.

Thiết bị mạng truy cập còn được tạo cấu hình để: nhận thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên, cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên, và cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất thành trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai.

Theo thiết kế khả thi, mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một phần hoặc tất cả các mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba hoặc SUPI của thiết bị đầu cuối thứ ba.

Theo thiết kế khả thi, thiết bị mạng truy cập còn được tạo cấu hình để gửi thông điệp chỉ báo thứ hai đến thiết bị đầu cuối thứ nhất, trong đó thông điệp chỉ báo thứ hai biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Thiết bị đầu cuối thứ nhất được tạo cấu hình để: nhận thông điệp chỉ báo thứ hai, cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin chỉ báo thứ hai, và cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất thành trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai; và cập nhật trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai.

Theo thiết kế khả thi, chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được ưu tiên. Khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất, phần tử mạng quản lý phiên được tạo cấu hình cụ thể để:

sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, xác định để vô hiệu hóa việc bảo vệ tính toàn vẹn của phiên.

Theo thiết kế khả thi, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu, phần tử mạng quản lý phiên còn được tạo cấu hình để: gửi phản hồi từ chối thiết lập phiên đến thiết bị đầu cuối thứ nhất sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, trong đó phản hồi từ chối thiết lập phiên biểu thị việc từ chối thiết lập phiên.

Theo thiết kế khả thi, khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai, phần tử mạng quản lý phiên được tạo cấu hình cụ thể để:

xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên; hoặc

xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo thiết kế khả thi, khi thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, phần tử mạng quản lý phiên được tạo cấu hình cụ thể để:

gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp

nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba.

Phần tử mạng quản lý dữ liệu hợp nhất được tạo cấu hình để: nhận yêu cầu thu thông tin thuê bao thứ hai, và xác định chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba; và gửi chính sách bảo mật mặt phẳng người dùng thứ hai đến phần tử mạng quản lý phiên.

Phần tử mạng quản lý phiên còn nhận chính sách bảo mật mặt phẳng người dùng thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất.

Theo thiết kế khả thi, trước khi gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập, phần tử mạng quản lý phiên còn được tạo cấu hình để:

xác định rằng thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên.

Theo thiết kế khả thi, chính sách bảo mật mặt phẳng người dùng thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn của phiên được ưu tiên. Khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai, phần tử mạng quản lý phiên được tạo cấu hình cụ thể để:

sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, xác định để vô hiệu hóa việc bảo vệ tính toàn vẹn của phiên.

Theo khía cạnh thứ mười bốn, sáng chế còn đề xuất phương tiện lưu trữ đọc được bằng máy tính. Phương tiện lưu trữ đọc được bằng máy tính lưu trữ các lệnh. Khi các lệnh chạy trên máy tính, thì máy tính này được cho phép thực hiện các phương pháp theo các khía cạnh nêu trên.

Theo khía cạnh thứ mười năm, sáng chế còn đề xuất sản phẩm chương trình máy tính bao gồm các lệnh. Khi sản phẩm chương trình máy tính này chạy trên máy tính, thì máy tính được cho phép thực hiện các phương pháp theo các khía cạnh nêu trên.

Theo khía cạnh thứ mười sáu, sáng chế còn đề xuất chip máy tính. Chip này được kết nối với bộ nhớ. Chip được tạo cấu hình để đọc và thực thi chương trình phần mềm được lưu trữ trong bộ nhớ, để thực hiện các phương pháp theo các khía cạnh nêu trên.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ kiến trúc của hệ thống theo một phương án của sáng chế;

Fig.2 là sơ đồ sơ lược phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế;

Fig.3 là sơ đồ sơ lược phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế;

Fig.4A và v4B là sơ đồ sơ lược phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế;

Fig.5A và Fig.5B là sơ đồ sơ lược phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế;

Fig.6A và Fig.6B là sơ đồ sơ lược phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế; và

Fig.7 đến Fig.13 mỗi hình vẽ này là sơ đồ sơ lược về cấu trúc của thiết bị truyền thông theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Fig.1 là sơ đồ sơ lược kiến trúc mạng cụ thể mà sáng chế có thể áp dụng. Kiến trúc mạng là kiến trúc mạng của hệ thống 5G. Phần tử mạng trong 5G kiến trúc bao gồm thiết bị đầu cuối (user equipment, UE). Kiến trúc mạng còn bao gồm mạng truy cập vô tuyến (radio access network, RAN), phần tử mạng chức năng quản lý truy cập và di động (access and mobility management function, AMF), phần tử mạng có chức năng quản lý phiên (session management function, SMF), phần tử mạng có chức năng mặt phẳng người dùng (user plane function, UPF), phần tử mạng quản lý dữ liệu hợp nhất (unified data management, UDM), phần tử mạng có chức năng ứng dụng (application function, AF), mạng dữ liệu (data network, DN) và dạng tương tự.

Thiết bị đầu cuối là thiết bị có chức năng thu-phát không dây, có thể được triển khai trên đất liền, và bao gồm thiết bị trong nhà hoặc ngoài nhà, thiết bị cầm tay, hoặc thiết bị gắn trên xe; có thể được triển khai dưới nước (ví dụ, trên tàu); hoặc có thể được triển khai trên không (ví dụ, trên máy bay, khinh khí cầu và vệ tinh). Thiết bị đầu cuối có thể là điện thoại di động (mobile phone), máy tính bảng (pad), máy tính có chức năng thu-phát không dây, thiết bị đầu cuối thực tế ảo (virtual reality, VR), thiết bị thực tế tăng cường (augmented reality, AR), thiết bị đầu cuối không dây trong điều khiển công nghiệp (industrial control), thiết bị đầu cuối không dây tự lái (self driving), thiết bị đầu cuối không dây trong y tế từ xa (remote medical), thiết bị đầu cuối không dây trong lưới

điện thông minh (smart grid), thiết bị đầu cuối không dây trong an toàn giao thông (transportation safety), thiết bị đầu cuối không dây trong thành phố thông minh (smart city), thiết bị đầu cuối không dây trong nhà thông minh (smart home) hoặc dạng tương tự. Theo các phương án của sáng chế, các thiết bị đầu cuối có thể được phân loại thành hai kiểu: UE từ xa (ví dụ, thiết bị đầu cuối thứ hai và thiết bị đầu cuối thứ ba) và UE chuyển tiếp (ví dụ, thiết bị đầu cuối thứ nhất). UE từ xa là UE mà cần để truyền thông với mạng dữ liệu bằng cách sử dụng UE chuyển tiếp, và UE chuyển tiếp là UE mà có thể trực tiếp truyền thông với mạng dữ liệu.

Theo các phương án của sáng chế, UE từ xa có thể gửi yêu cầu truyền thông trực tiếp (ví dụ, yêu cầu truyền thông trực tiếp thứ nhất và yêu cầu truyền thông trực tiếp thứ hai) đến UE chuyển tiếp, trong đó yêu cầu truyền thông trực tiếp là để thiết lập kết nối truyền thông giao diện PC5 với UE chuyển tiếp. UE chuyển tiếp có thể khởi tạo thủ tục thiết lập phiên đến phần tử mạng SMF, trong đó thủ tục thiết lập phiên là để thiết lập phiên để truyền dữ liệu giữa UE từ xa và DN (trong đó phiên về cơ bản là phiên được thiết lập bởi UE chuyển tiếp với mạng thông qua mạng truy cập, là để truyền dữ liệu được trao đổi giữa UE từ xa và mạng dữ liệu, và có thể còn được gọi là phiên chuyển tiếp). Khi khởi tạo thủ tục thiết lập phiên, UE chuyển tiếp có thể gửi trực tiếp, đến phần tử mạng SMF, mã nhận dạng của UE từ xa hoặc thông tin chỉ báo biểu thị rằng phiên được thiết lập là phiên chuyển tiếp. Khi khởi tạo thủ tục thiết lập phiên, UE chuyển tiếp có thể theo cách khác gửi mã nhận dạng của UE từ xa hoặc thông tin chỉ báo đến phần tử mạng SMF bằng cách sử dụng phần tử mạng AMF.

Chức năng chính của RAN là điều khiển thiết bị đầu cuối để truy cập mạng truyền thông di động theo cách không dây. RAN là một phần của hệ thống viễn thông di động. RAN thực hiện công nghệ truy cập vô tuyến. Về mặt khái niệm, RAN thường trú giữa thiết bị (ví dụ, điện thoại di động, máy tính, hoặc máy được điều khiển từ xa bất kỳ) và cung cấp kết nối đến mạng lõi của RAN.

Phần tử mạng AMF chịu trách nhiệm quản lý truy cập và quản lý di động của thiết bị đầu cuối. Trong quá trình ứng dụng thực tế, phần tử mạng AMF có chức năng quản lý di động của MME trong kiến trúc mạng LTE, và thêm chức năng quản lý truy cập.

Phần tử mạng SMF chịu trách nhiệm quản lý phiên chẳng hạn như thiết lập, sửa đổi hoặc xóa bỏ phiên người dùng. Theo các phương án của sáng chế, phần tử mạng SMF có thể xác định, dựa vào mã nhận dạng của UE từ xa hoặc thông tin chỉ báo, rằng

phiên được tạo ra bởi UE chuyển tiếp là phiên chuyển tiếp, thu chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp từ phần tử mạng UDM, và xác định, theo chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp, thông tin tăng cường bảo mật mặt phẳng người dùng mà là của phiên và được yêu cầu bởi RAN.

Phần tử mạng UPF là phần tử mạng chức năng mặt phẳng người dùng, và chịu trách nhiệm chính cho việc kết nối với mạng bên ngoài. Phần tử mạng UPF có các chức năng liên quan đến cổng phục vụ (serving gateway, SGW) và cổng mạng dữ liệu công cộng (public data network gateway, PDN-GW) trong LTE.

DN chịu trách nhiệm cho việc cung cấp dịch vụ cho thiết bị đầu cuối. Ví dụ, một số DN cung cấp chức năng truy cập mạng cho thiết bị đầu cuối, và một số DN khác cung cấp chức năng dịch vụ tin nhắn ngắn cho thiết bị đầu cuối.

Phần tử mạng UDM có thể lưu trữ thông tin thuê bao của người dùng, và việc thực hiện là tương tự với việc thực hiện của HSS trong 4G. Theo các phương án của sáng chế, phần tử mạng UDM có thể xác định mã nhận dạng cố định thuê bao (subscription permanent identifier, SUPI) của thiết bị đầu cuối dựa vào mã nhận dạng ẩn danh hoặc mã nhận dạng tạm thời của UE từ xa. Phần tử mạng UDM còn lưu trữ chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký. Chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp. Sau khi nhận yêu cầu thu thông tin thuê bao của phần tử mạng SMF, phần tử mạng UDM phản hồi chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp đến phần tử mạng SMF.

Phần tử mạng AF có thể là máy chủ ứng dụng bên thứ ba, hoặc có thể là thiết bị được triển khai bởi sóng mang, ví dụ, chức năng điều khiển phiên gọi proxy (proxy-call session control function, P-CSCF). Phần tử mạng AF có thể cung cấp các dịch vụ cho các máy chủ ứng dụng.

Mặc dù không được thể hiện, phần tử mạng lõi còn bao gồm phần tử mạng kho dữ liệu hợp nhất (unified data repository, UDR) và phần tử mạng chức năng giải mã mã nhận dạng thuê bao (subscription identifier de-concealing function, SIDF). Phần tử mạng UDR được tạo cấu hình chủ yếu để lưu trữ dữ liệu thuê bao liên quan đến người dùng, dữ liệu chính sách (ví dụ, chính sách bảo mật mặt phẳng người dùng mà UE đăng ký), dữ liệu có cấu trúc để tiếp xúc, và dữ liệu ứng dụng. Theo các phương án của sáng chế, phần tử mạng SIDF có thể phân tích cú pháp mã nhận dạng ẩn danh (SUCI) của UE để thu SUPI. Phần tử mạng SIDF có thể được triển khai một cách độc lập hoặc được

đồng triển khai với phần tử mạng còn lại. Ví dụ, phần tử mạng SIDF có thể được đồng triển khai với phần tử mạng UDM.

Theo các phương án của sáng chế, khi xác định rằng phiên chuyển tiếp cần được tạo ra, UE chuyển tiếp có thể khởi tạo thủ tục thiết lập phiên cho phần tử mạng quản lý phiên, trong đó thủ tục thiết lập phiên là để thiết lập phiên kiểu chuyển tiếp; và gửi, đến phần tử mạng quản lý phiên trong thủ tục thiết lập phiên, thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất, và gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên đến thiết bị mạng truy cập. Thiết bị mạng truy cập có thể xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất bằng cách sử dụng thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên. Trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn mặt phẳng người dùng và bảo vệ mã hóa giữa UE chuyển tiếp và thiết bị mạng truy cập được kích hoạt hoặc vô hiệu hóa. Theo các phương án của sáng chế, phần tử mạng quản lý phiên có thể thu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp bằng cách nhận thông tin thứ nhất, nhờ đó xác định thông tin tăng cường bảo mật mặt phẳng người dùng của phiên, sao cho trạng thái kích hoạt bảo mật được xác định bởi mạng truy cập dựa vào thông tin tăng cường bảo mật mặt phẳng người dùng của phiên có thể thỏa mãn yêu cầu bảo mật của UE từ xa.

Dựa vào các hình vẽ kèm theo, phần sau mô tả phương pháp xác định chính sách bảo mật mặt phẳng người dùng được đề xuất theo các phương án của sáng chế. Có hai cách của phương pháp xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng theo các phương án của sáng chế. Một cách như sau: Sự tham gia của phần tử mạng quản lý truy cập và di động là không cần thiết, và phần tử mạng quản lý phiên xác định độ bảo mật mặt phẳng người dùng của phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ hai hoặc thông tin chỉ báo. Cách còn lại như sau: Phần tử mạng quản lý truy cập và di động tham gia, phần tử mạng quản lý truy cập và di động cần thực hiện còn xử lý dựa vào thông tin được gửi bởi thiết bị đầu cuối thứ nhất, sau đó xác định, thu, hoặc tạo ra thông tin chỉ báo, và gửi thông tin chỉ báo đến phần tử mạng quản lý phiên, và sau đó phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng của phiên dựa vào thông tin. Phần sau mô tả riêng biệt hai cách.

Theo cách thứ nhất, Fig.2 thể hiện phương pháp xác định thông tin tăng cường

bảo mật mặt phẳng người dùng theo một phương án của sáng chế. Phương pháp này bao gồm các bước sau.

Bước 201: Thiết bị đầu cuối thứ hai gửi yêu cầu truyền thông trực tiếp thứ nhất đến thiết bị đầu cuối thứ nhất, trong đó yêu cầu truyền thông trực tiếp thứ nhất yêu cầu để thiết lập kết nối truyền thông với thiết bị đầu cuối thứ nhất, và yêu cầu truyền thông trực tiếp thứ nhất có thể bao gồm mã nhận dạng của thiết bị đầu cuối thứ hai.

Mã nhận dạng của thiết bị đầu cuối thứ hai bao gồm nhưng không bị giới hạn ở mã nhận dạng tạm thời, mã nhận dạng ẩn danh, và mã nhận dạng cố định thuê bao (subscription permanent identifier, SUPI) mà là của thiết bị đầu cuối thứ hai.

Mã nhận dạng tạm thời là mã nhận dạng được cấp phát trước cho thiết bị đầu cuối thứ hai. Mã nhận dạng ẩn danh có thể che giấu mã nhận dạng cố định của thiết bị đầu cuối, và chỉ phần tử mạng cụ thể có thể thu, bằng cách sử dụng mã nhận dạng ẩn danh, mã nhận dạng cố định mà là của thiết bị đầu cuối và được che giấu trong mã nhận dạng ẩn danh. Ví dụ, mã nhận dạng ẩn danh có thể là mã nhận dạng che giấu thuê bao (subscription concealed identifier, SUCI), và SUCI là mã nhận dạng bảo vệ riêng tư bao gồm SUPI.

Bước 202: Sau khi nhận yêu cầu truyền thông trực tiếp thứ nhất, thiết bị đầu cuối thứ nhất xác định rằng phiên để truyền dữ liệu của thiết bị đầu cuối thứ hai cần được tạo, nghĩa là, phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất cần được tạo. Thiết bị đầu cuối thứ nhất gửi yêu cầu thiết lập phiên đến phần tử mạng quản lý phiên, trong đó yêu cầu thiết lập phiên yêu cầu để tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và yêu cầu thiết lập phiên có thể bao gồm mã nhận dạng phiên. Phiên được tạo ra theo các phương án của sáng chế có thể là PDU phiên.

Cần lưu ý rằng, theo các phương án của sáng chế, phiên kiểu chuyển tiếp có thể còn được gọi là phiên chuyển tiếp. Phiên chuyển tiếp là phiên mà được thiết lập bởi thiết bị đầu cuối thứ nhất đóng vai trò làm UE chuyển tiếp và để hỗ trợ việc truyền dữ liệu giữa UE từ xa và mạng dữ liệu. Tương ứng, ngoài phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, có phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất. Theo các phương án của sáng chế, phiên kiểu không chuyển tiếp có thể còn được gọi là phiên không chuyển tiếp. Phiên không chuyển tiếp là phiên mà được thiết lập bởi thiết bị đầu cuối thứ nhất và để hỗ trợ việc truyền dữ liệu giữa thiết bị đầu cuối thứ nhất và mạng dữ liệu.

Để thông báo cho phần tử mạng quản lý phiên rằng phiên rằng thiết bị đầu cuối

thứ nhất yêu cầu tạo ra là phiên chuyển tiếp, thiết bị đầu cuối thứ nhất có thể bao gồm thông tin thứ nhất trong yêu cầu thiết lập phiên, trong đó thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp.

Cách trong đó thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp không bị giới hạn ở các phương án của sáng chế. Ví dụ, thông tin thứ nhất có thể sử dụng cách chỉ báo rõ ràng, và thông tin thứ nhất có thể là trường hoặc ký tự được thỏa thuận trước. Ví dụ khác, thông tin thứ nhất có thể sử dụng cách chỉ báo ngầm, và thông tin thứ nhất có thể là mã nhận dạng của thiết bị đầu cuối thứ hai.

Khi gửi yêu cầu thiết lập phiên đến phần tử mạng quản lý phiên, thiết bị đầu cuối thứ nhất có thể trước tiên gửi yêu cầu thiết lập phiên đến phần tử mạng quản lý truy cập và di động. Sau khi nhận yêu cầu thiết lập phiên, phần tử mạng quản lý truy cập và di động chuyển tiếp yêu cầu thiết lập phiên đến phần tử mạng quản lý phiên.

Ngoài ra, thiết bị đầu cuối thứ nhất gửi yêu cầu thiết lập phiên đến phần tử mạng quản lý truy cập và di động thông qua thông điệp NAS. Thông điệp NAS còn bao gồm tên mạng dữ liệu (data network name, DNN) và/hoặc một thông tin hỗ trợ lựa chọn lát mạng duy nhất (single-network slice selection assistance information, S-NSSAI). Theo cách khác, yêu cầu thiết lập phiên có trong vùng chứa N1 SM.

Bước 203: Sau khi nhận yêu cầu thiết lập phiên, phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất.

Bước 204: Sau khi thu chính sách bảo mật mặt phẳng người dùng thứ nhất, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp có thể xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Cần lưu ý rằng trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập về cơ bản là trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập. Để dễ mô tả hơn, giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập được gọi là giao diện thứ nhất.

Bước 205: Sau khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, phần tử mạng quản lý phiên có thể gửi thông tin tăng

cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp đến thiết bị mạng truy cập.

Cách trong đó phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất không bị giới hạn ở phương án này của sáng chế. Sau đây liệt kê bốn cách.

(1) Phần tử mạng quản lý phiên thu thông tin thuê bao của thiết bị đầu cuối thứ nhất, trong đó thông tin thuê bao của thiết bị đầu cuối thứ nhất bao gồm thông tin nhận dạng chuyển tiếp và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và thông tin nhận dạng chuyển tiếp biểu thị rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên kiểu chuyển tiếp, nghĩa là, xem thiết bị đầu cuối thứ nhất có được cho phép để đóng vai trò làm thiết bị chuyển tiếp hay không.

Chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp. Chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp bao gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất. Một cách tùy ý, chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp còn bao gồm chính sách bảo mật mặt phẳng người dùng mà là của phiên không chuyển tiếp và được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp, cụ thể là, chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp của thiết bị đầu cuối thứ nhất.

Một cách tùy ý, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký có thể còn bao gồm chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất không đóng vai trò làm thiết bị chuyển tiếp.

Cả hai chính sách bảo mật mặt phẳng người dùng mà là của phiên không chuyển tiếp và được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp và chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất không đóng vai trò làm thiết bị chuyển tiếp thuộc về chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp của thiết bị đầu cuối thứ nhất. Sự khác biệt nằm ở chỗ xem thiết bị đầu cuối thứ nhất có được cho phép để đóng vai trò làm thiết bị chuyển tiếp hay không.

Có nhiều cách trong đó chính sách bảo mật mặt phẳng người dùng mà thiết bị

đầu cuối thứ nhất đăng ký xác định chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp và chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất không được cho phép để đóng vai trò làm thiết bị chuyển tiếp. Ví dụ, các chính sách bảo mật mặt phẳng người dùng có thể được nhận dạng rõ ràng bằng cách sử dụng thông tin nhận dạng chuyển tiếp hoặc được nhận dạng bằng cách sử dụng phiên chuyển tiếp và phiên không chuyển tiếp. Theo cách trong đó các chính sách bảo mật mặt phẳng người dùng được nhận dạng bằng cách sử dụng phiên chuyển tiếp và phiên không chuyển tiếp, vì phiên chuyển tiếp và phiên không chuyển tiếp được phân biệt, điều này biểu thị rằng thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp.

Phần sau liệt kê một số chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Dựa vào bảng 1 và bảng 2.

Bảng 1

Thông tin thuê bao của thiết bị đầu cuối thứ nhất (chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký)	DNN của mạng dữ liệu 1 và S-NSSAI 1
	Thông tin nhận dạng chuyển tiếp
	Chính sách bảo mật mặt phẳng người dùng 1
	DNN của mạng dữ liệu 2 và S-NSSAI 2
	Chính sách bảo mật mặt phẳng người dùng 2

Chính sách bảo mật mặt phẳng người dùng 1 là chính sách bảo mật mặt phẳng người dùng được xác định bằng cách sử dụng thông tin nhận dạng chuyển tiếp, và là chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất đóng vai trò làm thiết bị chuyển tiếp. Chính sách bảo mật mặt phẳng người dùng 2 là chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất không đóng vai trò làm thiết bị chuyển tiếp. Chính sách bảo mật mặt phẳng người dùng 1 có thể được sử dụng làm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất, và chính sách bảo mật mặt phẳng người dùng 2 có thể được sử dụng làm chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp của thiết bị đầu cuối thứ nhất. Cần lưu ý ở đây rằng, vì phiên chuyển tiếp và phiên không chuyển tiếp không được phân biệt cho chính sách bảo mật mặt phẳng người dùng 1, mặt khác, khi mạng dữ liệu của phiên không chuyển tiếp của thiết bị đầu cuối

thứ nhất là mạng dữ liệu 1, chính sách bảo mật mặt phẳng người dùng 1 có thể còn được chọn làm chính sách bảo mật mặt phẳng người dùng.

Bảng 2

<table>
<tr><td rowspan="9">Thông tin thuê bao của thiết bị đầu cuối thứ nhất (chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký)</td><td colspan="2">DNN của mạng dữ liệu 1 và S-NSSAI 1</td></tr>
<tr><td colspan="2">Thông tin nhận dạng chuyển tiếp</td></tr>
<tr><td>Phiên chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 1</td></tr>
<tr><td>Phiên không chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 2</td></tr>
<tr><td colspan="2">DNN của mạng dữ liệu 2 và S-NSSAI 2</td></tr>
<tr><td>Phiên chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 3</td></tr>
<tr><td>Phiên không chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 4</td></tr>
<tr><td colspan="2">DNN của mạng dữ liệu 3 và S-NSSAI</td></tr>
<tr><td colspan="2">Chính sách bảo mật mặt phẳng người dùng 5</td></tr>
</table>

Chính sách bảo mật mặt phẳng người dùng 1 và chính sách bảo mật mặt phẳng người dùng 2 là các chính sách bảo mật mặt phẳng người dùng được xác định bằng cách sử dụng thông tin nhận dạng chuyển tiếp, và chính sách bảo mật mặt phẳng người dùng 5 là chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất không đóng vai trò làm thiết bị chuyển tiếp. Mặc dù chính sách bảo mật mặt phẳng người dùng 3 và chính sách bảo mật mặt phẳng người dùng 4 không mang thông tin nhận dạng chuyển tiếp, phiên chuyển tiếp và phiên không chuyển tiếp được phân biệt cho chính sách bảo mật mặt phẳng người dùng 3 và chính sách bảo mật mặt phẳng người dùng 4. Theo cách khác, thiết bị đầu cuối thứ nhất có thể đóng vai trò làm thiết bị chuyển tiếp, rằng thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm UE chuyển tiếp được biểu thị theo cách hiểm ngầm, và chính sách bảo mật mặt phẳng người dùng 3 về cơ bản là chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất đóng vai trò làm thiết bị chuyển tiếp.

Chính sách bảo mật mặt phẳng người dùng 1 và chính sách bảo mật mặt phẳng người dùng 3 là các chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất, và chính sách bảo mật mặt phẳng người dùng 2, chính

sách bảo mật mặt phẳng người dùng 4, và chính sách bảo mật mặt phẳng người dùng 5 là các chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp của thiết bị đầu cuối thứ nhất.

Cần lưu ý rằng, trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp và chính sách bảo mật mặt phẳng người dùng được sử dụng khi thiết bị đầu cuối thứ nhất không đóng vai trò làm thiết bị chuyển tiếp có thể được phân biệt theo cách khác. Chỉ thông tin nhận dạng chuyển tiếp được thêm vào thông tin thuê bao, và biểu thị rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên kiểu chuyển tiếp, nghĩa là, thiết bị đầu cuối thứ nhất có thể đóng vai trò làm thiết bị chuyển tiếp. Phần tử mạng quản lý phiên có thể chọn chính sách bảo mật mặt phẳng người dùng tương ứng dựa vào DNN và/hoặc S-NSSAI tương ứng với phiên.

(2) Phần tử mạng quản lý phiên thu thông tin thuê bao (bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký) của thiết bị đầu cuối thứ nhất, và phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký là chính sách bảo mật mặt phẳng người dùng được đăng ký được tạo cấu hình trước bởi mạng thuê bao cho thiết bị đầu cuối thứ nhất. Chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký có thể bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và có thể còn bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp.

Theo phương án này của sáng chế, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất và/hoặc chính sách bảo mật mặt phẳng người dùng thứ hai, và có thể còn bao gồm chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp.

Ví dụ, thông tin có trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký như được thể hiện trên bảng 3.

Bảng 3

<table>
<tr><td rowspan="8">Thông tin thuê bao của thiết bị đầu cuối thứ nhất (chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký)</td><td colspan="2">DNN của mạng dữ liệu 1 và S-NSSAI 1</td></tr>
<tr><td>Phiên chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 1</td></tr>
<tr><td>Phiên không chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 2</td></tr>
<tr><td colspan="2">DNN của mạng dữ liệu 2 và S-NSSAI 2</td></tr>
<tr><td>Phiên chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 3</td></tr>
<tr><td>Phiên không chuyển tiếp</td><td>Chính sách bảo mật mặt phẳng người dùng 4</td></tr>
<tr><td colspan="2">DNN của mạng dữ liệu 3 và S-NSSAI</td></tr>
<tr><td colspan="2">Chính sách bảo mật mặt phẳng người dùng</td></tr>
</table>

Một cách tùy ý, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký có thể còn bao gồm mã nhận dạng của thiết bị đầu cuối thứ hai. Mã nhận dạng của thiết bị đầu cuối thứ hai biểu thị thiết bị đầu cuối mà dữ liệu mà cần để được truyền bằng cách sử dụng phiên chuyển tiếp thuộc về.

Có thể biết được từ bảng 1 rằng chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm các chính sách bảo mật mặt phẳng người dùng mà được sử dụng khi các phiên được thiết lập với một hoặc nhiều các mạng dữ liệu là phiên chuyển tiếp hoặc phiên không chuyển tiếp và là của các phiên. Mạng dữ liệu có thể được biểu thị bằng cách sử dụng DNN của mạng dữ liệu. Một cách tùy ý, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký có thể còn bao gồm một thông tin hỗ trợ lựa chọn lát mạng duy nhất (single-network slice selection assistance information, S-NSSAI) để xác định hoặc biểu thị lát mạng.

Thông tin có trong chính sách bảo mật mặt phẳng người dùng được mô tả ở đây. Chính sách bảo mật mặt phẳng người dùng biểu thị xem có kích hoạt việc bảo vệ mã hóa và việc bảo vệ tính toàn vẹn hay không. Cụ thể, chính sách bảo mật mặt phẳng người dùng bao gồm chính sách bảo vệ mã hóa mặt phẳng người dùng (biểu thị xem có cho phép kích hoạt bảo vệ mã hóa hay không) và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng (biểu thị xem có kích hoạt việc bảo vệ tính toàn vẹn hay không). Có ba giá trị khả thi của chính sách bảo vệ mã hóa mặt phẳng người dùng:

không cần thiết (not needed), được ưu tiên (preferred), và được yêu cầu (required). Có ba giá trị khả thi của chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng: không cần thiết, được ưu tiên, và được yêu cầu. Không cần thiết biểu thị rằng chính sách không cần được kích hoạt, được ưu tiên biểu thị rằng chính sách có thể được kích hoạt hoặc có thể không bị vô hiệu hóa, và được yêu cầu biểu thị rằng chính sách cần được kích hoạt. Ba giá trị khả thi nêu trên, mỗi giá trị có thể được biểu thị bằng cách sử dụng hai bit (bit). Ví dụ, 00 biểu thị rằng chính sách không cần được kích hoạt, 01 biểu thị rằng chính sách có thể được kích hoạt hoặc có thể không được kích hoạt, và 11 biểu thị rằng chính sách cần được kích hoạt. Cách cụ thể trong đó ba giá trị khả thi được biểu thị cho chính sách bảo vệ mã hóa mặt phẳng người dùng và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng không bị giới hạn ở phương án này của sáng chế.

Bảo vệ mã hóa mặt phẳng người dùng là sự bảo vệ bí mật của dữ liệu trong quá trình truyền (do đó, bảo vệ mã hóa mặt phẳng người dùng có thể còn được gọi là bảo vệ bí mật mặt phẳng người dùng). Sự bí mật nghĩa là nội dung thực sự của dữ liệu đã truyền không thể được học trực tiếp. Việc bảo vệ tính toàn vẹn mặt phẳng người dùng là bảo vệ tính toàn vẹn của dữ liệu trong khi truyền trên mặt phẳng người dùng. Tính toàn vẹn có nghĩa là dữ liệu là bản gốc và chưa bị can thiệp.

Theo phương án này của sáng chế, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký có thể được lưu trữ cục bộ bởi phần tử mạng quản lý phiên, hoặc có thể thu được bởi phần tử mạng quản lý phiên từ phần tử mạng quản lý dữ liệu hợp nhất. Ví dụ, sau khi nhận yêu cầu thiết lập phiên, phần tử mạng quản lý phiên có thể thu, từ phần tử mạng quản lý dữ liệu hợp nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Ví dụ, phần tử mạng quản lý phiên có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất. Yêu cầu thu thông tin thuê bao thứ nhất có thể mang chỉ báo chuyển tiếp, và chỉ báo chuyển tiếp này yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Chỉ báo chuyển tiếp có thể là thông tin thứ nhất, hoặc có thể được xác định dựa vào thông tin thứ nhất.

Ví dụ, khi thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, chỉ báo chuyển tiếp có thể biểu thị, theo cách chỉ báo rõ ràng, rằng kiểu của phiên là kiểu chuyển tiếp, để yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau khi nhận yêu cầu thu thông tin thuê bao thứ nhất,

phần tử mạng quản lý dữ liệu hợp nhất xác định trực tiếp, dựa vào chỉ báo chuyển tiếp, rằng chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất cần được phản hồi.

Sau đó, phần tử mạng quản lý dữ liệu hợp nhất gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Phần tử mạng quản lý phiên nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất.

Phần tử mạng quản lý phiên chọn, là chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất được mang trong yêu cầu thiết lập phiên, chính sách bảo mật mặt phẳng người dùng tương ứng từ chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Nghĩa là, chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp được chọn làm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Khi thu, từ phần tử mạng quản lý dữ liệu hợp nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, thì phần tử mạng quản lý phiên có thể theo cách khác chỉ thu một phần của chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, ví dụ, chỉ thu chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất.

Phần tử mạng quản lý phiên đó có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất vẫn được sử dụng làm một ví dụ. Phần tử mạng quản lý phiên gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất yêu cầu chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất (trong đó yêu cầu thu thông tin thuê bao thứ nhất có thể theo cách khác bao gồm chỉ báo chuyển tiếp).

Sau khi nhận yêu cầu thu thông tin thuê bao thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định, dựa vào thông tin thứ nhất, chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Phần tử mạng quản lý dữ liệu hợp nhất gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị

đầu cuối thứ nhất.

Phần tử mạng quản lý phiên xác định, dựa vào thông tin thứ nhất được mang trong yêu cầu thiết lập phiên, xem phiên có phải là phiên chuyển tiếp hay không. Nếu phiên là phiên chuyển tiếp, thì phần tử mạng quản lý phiên có thể chọn, từ chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất, chính sách bảo mật mặt phẳng người dùng làm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Một cách tùy ý, phần tử mạng quản lý phiên có thể theo cách khác xác định, dựa vào thông tin thứ nhất được mang trong yêu cầu thiết lập phiên, xem phiên có phải là phiên chuyển tiếp hay không. Nếu phiên là phiên chuyển tiếp, thì phần tử mạng quản lý phiên có thể yêu cầu trực tiếp chính sách bảo mật mặt phẳng người dùng thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất. Theo cách khác, phần tử mạng quản lý phiên có thể gửi, đến phần tử mạng quản lý dữ liệu hợp nhất, thông điệp yêu cầu để yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên mà kiểu phiên là kiểu chuyển tiếp. Sau khi nhận thông điệp yêu cầu, phần tử mạng quản lý dữ liệu hợp nhất xác định chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp, và phản hồi chính sách bảo mật mặt phẳng người dùng thứ nhất đến phần tử mạng quản lý phiên.

Phần nêu trên minh họa một ví dụ trong đó phần tử mạng quản lý phiên thu, từ phần tử mạng quản lý dữ liệu hợp nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Thực tế là, phần tử mạng quản lý phiên có thể thu được theo cách khác, từ phần tử mạng quản lý dữ liệu hợp nhất bằng cách sử dụng thông tin thứ nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký. Cụ thể hơn là, sau khi phần tử mạng quản lý dữ liệu hợp nhất nhận yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất, nếu thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, thì phần tử mạng quản lý dữ liệu hợp nhất xác định, dựa vào thông tin thứ nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký, và bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký trong yêu cầu thu thông tin thuê bao thứ nhất. Phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ nhất theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

Theo một phương án thực hiện khả thi, phần tử mạng quản lý phiên có thể được lưu trữ cục bộ chính sách bảo mật mặt phẳng người dùng ở mức độ chi tiết DNN và/hoặc

mức độ chi tiết S-NSSAI. Chính sách bảo mật mặt phẳng người dùng ở mức độ chi tiết DNN và/hoặc chính sách bảo mật mặt phẳng người dùng ở mức độ chi tiết S-NSSAI bao gồm/gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp tương ứng với DNN và/hoặc S-NSSAI và/hoặc chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp tương ứng với DNN và/hoặc S-NSSAI. Phần tử mạng quản lý phiên có thể chọn chính sách bảo mật mặt phẳng người dùng tương ứng dựa vào DNN và/hoặc S-NSSAI tương ứng với phiên.

(3) Thông tin thứ nhất là mã nhận dạng ẩn danh hoặc mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai. Phần tử mạng quản lý phiên thứ nhất xác định mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, sau đó thu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, và sau đó xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất.

Phần tử mạng quản lý phiên có thể trước tiên thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất dựa vào thông tin thứ nhất.

Ví dụ, phần tử mạng quản lý phiên có thể gửi, đến phần tử mạng quản lý dữ liệu hợp nhất, thông điệp yêu cầu mang thông tin thứ nhất, trong đó thông điệp yêu cầu yêu cầu để thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai. Sau khi nhận thông điệp yêu cầu, phần tử mạng quản lý dữ liệu hợp nhất có thể thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai dựa vào thông điệp yêu cầu, và sau đó phản hồi lại, đến phần tử mạng quản lý phiên, thông điệp phản hồi mang mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai. Thông điệp yêu cầu có thể là thông báo được thêm vào mới, hoặc có thể là thông báo mà phần tử mạng quản lý phiên cần gửi đến phần tử mạng quản lý dữ liệu hợp nhất trong thủ tục tương tác hiện có.

Cách trong đó phần tử mạng quản lý dữ liệu hợp nhất thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai dựa vào thông báo thứ nhất không bị giới hạn ở phương án này của sáng chế. Ví dụ, phần tử mạng quản lý dữ liệu hợp nhất có thể lưu trữ sự tương ứng giữa mã nhận dạng tạm thời và mã nhận dạng cố định thuê bao mà là của thiết bị đầu cuối thứ hai hoặc sự tương ứng giữa mã nhận dạng ẩn danh và mã nhận dạng cố định thuê bao mà là của thiết bị đầu cuối thứ hai. Sau khi thu thông tin thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai dựa vào thông tin thứ nhất và sự tương ứng được lưu trữ.

Ví dụ khác, phần tử mạng quản lý dữ liệu hợp nhất có thể theo cách khác có khả năng phân tích mã nhận dạng, và có thể phân tích mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai thành mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai. Ví dụ khác, phần tử mạng quản lý dữ liệu hợp nhất có thể theo cách khác thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai bằng cách tương tác với phần tử mạng phân tích mã nhận dạng (ví dụ, phần tử mạng SIDF). Ví dụ, phần tử mạng quản lý dữ liệu hợp nhất gửi mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai đến phần tử mạng phân tích mã nhận dạng, và thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai từ phần tử mạng phân tích mã nhận dạng.

Sau khi thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, phần tử mạng quản lý phiên có thể thu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất dựa vào mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai.

Ví dụ, phần tử mạng quản lý phiên có thể gửi, đến phần tử mạng quản lý dữ liệu hợp nhất, yêu cầu thu thông tin thuê bao thứ nhất để mang mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, trong đó yêu cầu thu thông tin thuê bao thứ nhất yêu cầu để thu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Một cách tùy ý, yêu cầu thu thông tin thuê bao thứ nhất có thể còn bao gồm DNN và/hoặc S-NSSAI. Sau khi nhận yêu cầu thu thông tin thuê bao thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất xác định, dựa vào mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, rằng phiên là phiên chuyển tiếp, và sau đó xác định, trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau đó, phần tử mạng quản lý dữ liệu hợp nhất phản hồi, đến phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ nhất để mang chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Phần tử mạng quản lý phiên nhận chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất.

Theo một phương án thực hiện khả thi, sau khi nhận yêu cầu thu thông tin thuê bao thứ nhất để mang mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, phần tử mạng quản lý dữ liệu hợp nhất có thể theo cách khác xác định, dựa vào mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký, và sử dụng chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký làm chính sách bảo mật mặt phẳng người dùng

thứ nhất. Nếu chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký bao gồm các chính sách bảo mật mặt phẳng người dùng, phần tử mạng quản lý dữ liệu hợp nhất có thể chọn một trong số các chính sách bảo mật mặt phẳng người dùng làm chính sách bảo mật mặt phẳng người dùng thứ nhất. Ví dụ, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất trong các chính sách bảo mật mặt phẳng người dùng dựa vào DNN và/hoặc S-NSSAI, và sau đó phản hồi lại chính sách bảo mật mặt phẳng người dùng thứ nhất đến phần tử mạng quản lý phiên. Chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký là chính sách bảo mật mặt phẳng người dùng được đăng ký được tạo cấu hình trước bởi mạng thuê bao cho thiết bị đầu cuối thứ hai.

Cần lưu ý rằng thông tin được biểu thị bởi chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký có thể giống với thông tin được biểu thị bởi chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Theo cách khác, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký có thể biểu thị chính sách bảo mật mặt phẳng người dùng mà là của phiên chuyển tiếp và được sử dụng khi thiết bị đầu cuối thứ hai đóng vai trò làm UE từ xa để truy cập mạng bằng cách sử dụng UE chuyển tiếp, và có thể còn biểu thị chính sách bảo mật mặt phẳng người dùng mà là của phiên không chuyển tiếp và được sử dụng khi thiết bị đầu cuối thứ hai tạo ra phiên trực tiếp. Khi xác định chính sách bảo mật mặt phẳng người dùng thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất theo chính sách bảo mật mặt phẳng người dùng mà là của phiên chuyển tiếp và được sử dụng khi thiết bị đầu cuối thứ hai đóng vai trò làm UE từ xa để truy cập mạng bằng cách sử dụng UE chuyển tiếp.

(4) Phần tử mạng quản lý phiên trực tiếp thu chính sách bảo mật mặt phẳng người dùng thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất.

Phần tử mạng quản lý phiên có thể gửi trực tiếp, đến phần tử mạng quản lý dữ liệu hợp nhất, yêu cầu thu thông tin thuê bao thứ nhất mang thông tin thứ nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất yêu cầu thu chính sách bảo mật mặt phẳng người dùng thứ nhất. Một cách tùy ý, yêu cầu thu thông tin thuê bao thứ nhất có thể còn bao gồm DNN và/hoặc S-NSSAI, và được sử dụng bởi phần tử mạng quản lý dữ liệu hợp nhất để thu thông tin thuê bao tương ứng với DNN và/hoặc S-NSSAI, trong đó thông tin thuê bao bao gồm chính sách bảo mật mặt phẳng người dùng tương ứng.

Ở đây, yêu cầu thu thông tin thuê bao thứ nhất mang thông tin thứ nhất được sử

dụng làm một ví dụ. Trong quá trình ứng dụng thực tế, phần tử mạng quản lý phiên có thể theo cách khác xác định thông tin chỉ báo chuyển tiếp dựa vào thông tin thứ nhất. Thông tin chỉ báo chuyển tiếp có thể biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Theo cách khác, phần tử mạng quản lý phiên tạo ra chỉ báo chuyển tiếp dựa vào thông tin thứ nhất, và bao gồm chỉ báo chuyển tiếp trong yêu cầu thu thông tin thuê bao thứ nhất. Thông tin thứ nhất và chỉ báo chuyển tiếp có thể biểu thị, theo các cách khác nhau, rằng kiểu của phiên là kiểu chuyển tiếp. Theo một phương án thực hiện khả thi, chỉ báo chuyển tiếp có thể theo cách khác giống với thông tin thứ nhất. Nghĩa là, phần tử mạng quản lý phiên bao gồm thông tin thứ nhất trong yêu cầu thu thông tin thuê bao thứ nhất.

Sau khi phần tử mạng quản lý dữ liệu hợp nhất nhận yêu cầu thu thông tin thuê bao thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất có thể xác định, dựa vào thông tin thứ nhất, rằng thông tin thuê bao của phiên kiểu chuyển tiếp cần thu được, nghĩa là, xác định chính sách bảo mật mặt phẳng người dùng thứ nhất.

Khi xác định chính sách bảo mật mặt phẳng người dùng thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất có thể thu chính sách bảo mật mặt phẳng người dùng thứ nhất từ chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Nếu thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, thì phần tử mạng quản lý dữ liệu hợp nhất có thể theo cách khác cung cấp phần tử mạng quản lý phiên với chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký, và phần tử mạng quản lý phiên sử dụng chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký làm chính sách bảo mật mặt phẳng người dùng thứ nhất. Ngoài ra, nếu thông tin thuê bao của thiết bị đầu cuối thứ hai có thể bao gồm chính sách bảo mật mặt phẳng người dùng mà là của phiên chuyển tiếp và được sử dụng khi thiết bị đầu cuối thứ hai đóng vai trò làm UE từ xa để truy cập mạng bằng cách sử dụng UE chuyển tiếp, phần tử mạng quản lý dữ liệu hợp nhất có thể cung cấp phần tử mạng quản lý phiên cho chính sách bảo mật mặt phẳng người dùng làm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Ví dụ, thông tin thứ nhất là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai. Phần tử mạng quản lý dữ liệu hợp nhất có thể xác định mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai dựa vào mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai. Sau đó, phần tử mạng quản lý dữ liệu hợp nhất thu, dựa vào mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký, và

cung cấp phần tử mạng quản lý phiên cho chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký. Phần tử mạng quản lý phiên sử dụng, làm chính sách bảo mật mặt phẳng người dùng thứ nhất, chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

Sau khi xác định chính sách bảo mật mặt phẳng người dùng thứ nhất, phần tử mạng quản lý dữ liệu hợp nhất phản hồi, đến phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ nhất mà mang chính sách bảo mật mặt phẳng người dùng thứ nhất. Phần tử mạng quản lý phiên nhận chính sách bảo mật mặt phẳng người dùng thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất.

Cần lưu ý rằng, trong một vài phương án thực hiện khả thi nêu trên, thông tin được trao đổi giữa phần tử mạng quản lý phiên và phần tử mạng quản lý dữ liệu hợp nhất được đặt tên thống nhất là yêu cầu thu thông tin thuê bao thứ nhất và phản hồi thu thông tin thuê bao thứ nhất. Tuy nhiên, mỗi trong số yêu cầu thu thông tin thuê bao thứ nhất và phản hồi thu thông tin thuê bao thứ nhất có thể mang thông tin khác nhau trong các phương án thực hiện khác nhau.

Thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất mà là của phiên chuyển tiếp và để được xác định ở bước 204 tương tự với chính sách bảo mật mặt phẳng người dùng thứ nhất, và có thể biểu thị xem có cho phép kích hoạt bảo vệ mã hóa và bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập trong phiên chuyển tiếp hay không. Các giá trị bảo vệ mã hóa và việc bảo vệ tính toàn vẹn tương tự với các giá trị của chính sách bảo vệ mã hóa mặt phẳng người dùng và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng trong phần mô tả ở trên. Để biết chi tiết, dựa vào nội dung nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Khi bước thực hiện 204, phần tử mạng quản lý phiên có thể sử dụng trực tiếp chính sách bảo mật mặt phẳng người dùng thứ nhất làm thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp. Ví dụ, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng chính sách bảo vệ mã hóa mặt phẳng người dùng được yêu cầu và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng là không cần thiết, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp biểu thị rằng bảo vệ mã hóa của giao diện thứ nhất được yêu cầu và việc bảo vệ tính toàn vẹn của giao diện thứ nhất là không cần thiết. Theo cách khác, phần tử mạng quản lý phiên có thể phân tích thông tin về thiết bị đầu cuối thứ nhất. Thông tin về thiết bị đầu cuối thứ nhất bao gồm nhưng không bị giới hạn ở tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất và thông tin điều khiển chất lượng dịch vụ (quality of service, QoS)

(ví dụ, tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp của thiết bị đầu cuối thứ nhất) của thiết bị đầu cuối thứ nhất. Sau khi phân tích thông tin về thiết bị đầu cuối thứ nhất, phần tử mạng quản lý phiên xác định có sử dụng chính sách bảo mật mặt phẳng người dùng thứ nhất làm thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp. Phần tử mạng quản lý phiên có thể còn sửa đổi chính sách bảo mật mặt phẳng người dùng thứ nhất sau khi phân tích thông tin về thiết bị đầu cuối thứ nhất, để xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp.

Ví dụ, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng chính sách bảo vệ mã hóa mặt phẳng người dùng được ưu tiên, phần tử mạng quản lý phiên cần xác định thêm xem có kích hoạt việc bảo vệ mã hóa của giao diện thứ nhất hay không, và sau đó xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp.

Ví dụ khác, chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng cả hai chính sách bảo vệ mã hóa mặt phẳng người dùng và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng được ưu tiên, và phần tử mạng quản lý phiên cần phải xác định thêm xem có kích hoạt việc bảo vệ mã hóa và bảo vệ tính toàn vẹn của giao diện thứ nhất hay không.

Có nhiều cách trong đó phần tử mạng quản lý phiên còn xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp. Điều này không bị giới hạn ở phương án này của sáng chế. Ví dụ, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất.

Tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất biểu thị tốc độ truyền dữ liệu được hỗ trợ bởi thiết bị đầu cuối thứ nhất sau khi việc bảo vệ tính toàn vẹn được kích hoạt. Nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng được ưu tiên, phần tử mạng quản lý phiên xác định xem tốc độ truyền dữ liệu có được hỗ trợ bởi thiết bị đầu cuối thứ nhất hay không sau khi việc bảo vệ tính toàn vẹn được kích hoạt có thể thỏa mãn tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp. Tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp được xác định bởi phần tử mạng quản lý phiên dựa vào DNN và/hoặc S-NSSAI của phiên và/hoặc tham số khác để xác định tốc độ dữ liệu. Tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp có thể thu được bởi phần tử mạng quản lý

phiên từ phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng điều khiển chính sách (ví dụ, phần tử mạng PCF), hoặc có thể thu được dựa vào cấu hình cục bộ.

Nếu tốc độ truyền dữ liệu được hỗ trợ bởi thiết bị đầu cuối thứ nhất sau khi việc bảo vệ tính toàn vẹn được kích hoạt nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp, phần tử mạng quản lý phiên có thể xác định rằng việc bảo vệ tính toàn vẹn trong thông tin tăng cường bảo mật mặt phẳng người dùng là không cần thiết, nghĩa là, việc bảo vệ tính toàn vẹn của giao diện thứ nhất vô hiệu hóa.

Nếu tốc độ truyền dữ liệu được hỗ trợ bởi thiết bị đầu cuối thứ nhất sau khi việc bảo vệ tính toàn vẹn được kích hoạt không nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp, phần tử mạng quản lý phiên có thể xác định rằng việc bảo vệ tính toàn vẹn trong thông tin tăng cường bảo mật mặt phẳng người dùng được yêu cầu, nghĩa là, việc bảo vệ tính toàn vẹn của giao diện thứ nhất được kích hoạt.

Sau khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, phần tử mạng quản lý phiên có thể tạo ra phiên chuyển tiếp, và thực hiện bước 205.

Cần lưu ý rằng phần tử mạng quản lý phiên có thể bị từ chối theo cách khác, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất, thiết lập của phiên chuyển tiếp. Ví dụ, chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng được cho phép. Nếu tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp, mặt khác, sau khi việc bảo vệ tính toàn vẹn được kích hoạt, thiết bị đầu cuối thứ nhất không thể truyền dữ liệu dựa vào tốc độ dữ liệu được yêu cầu bởi phiên chuyển tiếp. Phần tử mạng quản lý phiên có thể từ chối thiết lập của phiên chuyển tiếp, và gửi phiên thiết lập phản hồi việc từ chối đến thiết bị đầu cuối thứ nhất.

Sau khi nhận thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, thiết bị mạng truy cập có thể tạo cấu hình trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất, trong đó trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất biểu thị xem bảo vệ mã hóa và việc bảo vệ tính toàn vẹn được kích hoạt giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập trong phiên chuyển tiếp; và gửi, đến thiết bị đầu cuối thứ nhất, thông tin chỉ báo biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất, để thông báo cho thiết bị đầu cuối thứ nhất xem việc bảo vệ mã hóa và việc bảo vệ tính toàn vẹn

có được kích hoạt trên giao diện thứ nhất hay không.

Cần lưu ý rằng bảo vệ mã hóa ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất chỉ có hai trạng thái: Một trạng thái được kích hoạt và trạng thái còn lại vô hiệu hóa. Việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất cũng chỉ có hai trạng thái: Một trạng thái được kích hoạt và trạng thái còn lại vô hiệu hóa. Trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất là cuối cùng được xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng của giao diện thứ nhất.

Sau khi nhận thông tin chỉ báo biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất, thiết bị đầu cuối thứ nhất có thể xác định trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất. Trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai biểu thị xem bảo vệ mã hóa và việc bảo vệ tính toàn vẹn được kích hoạt khi thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai thực hiện việc truyền dữ liệu.

Cần lưu ý rằng trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai về cơ bản là trạng thái kích hoạt bảo mật của giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai. Bảo vệ mã hóa ở trạng thái kích hoạt bảo mật chỉ có hai trạng thái: Một trạng thái được kích hoạt và trạng thái còn lại vô hiệu hóa. Việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật cũng chỉ có hai trạng thái: Một trạng thái được kích hoạt và trạng thái còn lại vô hiệu hóa. Trạng thái kích hoạt bảo mật là cuối cùng được xác định trạng thái kích hoạt bảo mật của giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai. Để dễ mô tả hơn, giao diện truyền thông giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai được gọi là giao diện thứ hai.

Ví dụ, thiết bị đầu cuối thứ nhất có thể thiết lập trạng thái kích hoạt bảo mật của giao diện thứ hai để phù hợp với trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất.

Ví dụ khác, thiết bị đầu cuối thứ nhất có thể xác định trạng thái kích hoạt bảo mật của giao diện thứ hai sau khi phân tích trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất. Nếu trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn của giao diện thứ nhất được kích hoạt, thiết bị đầu cuối thứ nhất có thể còn xác định xem việc

bảo vệ tính toàn vẹn có được kích hoạt trên giao diện thứ hai hay không.

Có nhiều cách trong đó thiết bị đầu cuối thứ nhất xác định trạng thái kích hoạt bảo mật của giao diện thứ hai. Điều này không bị giới hạn ở phương án này của sáng chế.

Ví dụ, thiết bị đầu cuối thứ nhất có thể xác định trạng thái kích hoạt bảo mật của giao diện thứ hai dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển chất lượng dịch vụ (quality of service, QoS) của thiết bị đầu cuối thứ hai. Tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển QoS của thiết bị đầu cuối thứ hai có thể được mang trong yêu cầu truyền thông trực tiếp thứ nhất.

Cách trong đó thiết bị đầu cuối thứ nhất có thể xác định trạng thái kích hoạt bảo mật của giao diện thứ hai dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ hai giống với cách trong đó phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất. Các chi tiết không được mô tả lại trong bản mô tả này.

Thông tin điều khiển QoS của thiết bị đầu cuối thứ hai biểu thị yêu cầu của thiết bị đầu cuối thứ hai trong khi truyền dữ liệu, ví dụ, băng thông yêu cầu, tốc độ truyền dữ liệu, độ trễ, hoặc tỷ lệ mất mát gói.

Thiết bị đầu cuối thứ nhất có thể xác định, dựa vào thông tin điều khiển QoS của thiết bị đầu cuối thứ hai, xem thiết bị đầu cuối thứ hai có hỗ trợ kích hoạt việc bảo vệ tính toàn vẹn hay không.

Ví dụ, thông tin điều khiển QoS của thiết bị đầu cuối thứ hai biểu thị rằng thiết bị đầu cuối thứ hai cần truyền dữ liệu, nhưng băng thông được yêu cầu bởi thiết bị đầu cuối thứ hai để truyền dữ liệu là 100 Mbp, và băng thông mà có thể được hỗ trợ sau khi việc bảo vệ tính toàn vẹn được kích hoạt là 50 Mbp. Thiết bị đầu cuối thứ nhất có thể xác định không kích hoạt việc bảo vệ tính toàn vẹn.

Thông qua các bước từ 201 đến 205, chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp được tạo ra bởi thiết bị đầu cuối thứ nhất được xác định dựa vào thông tin thứ nhất. Thiết bị đầu cuối thứ nhất có thể truyền dữ liệu của thiết bị đầu cuối thứ hai bằng cách sử dụng phiên chuyển tiếp, để đảm bảo độ bảo mật của dữ liệu đã truyền.

Trong quá trình ứng dụng thực tế, thiết bị đầu cuối thứ nhất có thể còn thiết lập

truyền thông với thiết bị đầu cuối khác, và thiết bị đầu cuối khác có thể trao đổi dữ liệu với mạng dữ liệu bằng cách sử dụng phiên của thiết bị đầu cuối thứ nhất. Theo cách khác, thiết bị đầu cuối thứ nhất có thể còn truyền dữ liệu của thiết bị đầu cuối khác bằng cách sử dụng được thiết lập phiên chuyển tiếp. Trong trường hợp này, phiên chuyển tiếp được sử dụng lại bởi thiết bị đầu cuối khác, và chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp có thể cần được xác định lại. Phần sau mô tả cách tái xác định chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp bằng cách sử dụng ví dụ trong đó thiết bị khác là thiết bị đầu cuối thứ ba.

Thiết bị đầu cuối thứ ba có thể gửi yêu cầu truyền thông trực tiếp thứ hai đến thiết bị đầu cuối thứ nhất, trong đó yêu cầu truyền thông trực tiếp thứ hai yêu cầu để thiết lập truyền thông với thiết bị đầu cuối thứ nhất, và yêu cầu truyền thông trực tiếp thứ hai có thể bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba.

Mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm nhưng không bị giới hạn ở mã nhận dạng tạm thời, mã nhận dạng ẩn danh, và SUPI mà là của thiết bị đầu cuối thứ ba.

Sau khi nhận yêu cầu truyền thông trực tiếp thứ hai, thiết bị đầu cuối thứ nhất xác định rằng phiên được thiết lập còn cần để truyền dữ liệu của thiết bị đầu cuối thứ ba, nghĩa là, thiết bị đầu cuối thứ ba cần sử dụng phiên chuyển tiếp. Thiết bị đầu cuối thứ nhất gửi yêu cầu sửa đổi phiên đến phần tử mạng quản lý phiên, trong đó yêu cầu sửa đổi phiên yêu cầu để sửa đổi phiên chuyển tiếp. Yêu cầu sửa đổi phiên có thể theo cách khác là thông điệp quản lý phiên khác hoặc thông điệp quản lý phiên được xác định mới.

Yêu cầu sửa đổi phiên có thể bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba, và có thể còn mang mã nhận dạng mà là của phiên chuyển tiếp và để biểu thị phiên chuyển tiếp mà cần được sửa đổi.

Sau khi nhận yêu cầu sửa đổi phiên, phần tử mạng quản lý phiên có thể xác định, dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, rằng thiết bị đầu cuối thứ ba là để sử dụng phiên chuyển tiếp. Phần tử mạng quản lý phiên có thể xác định chính sách bảo mật mặt phẳng người dùng thứ hai. Cách trong đó phần tử mạng quản lý phiên xác định chính sách bảo mật mặt phẳng người dùng thứ hai tương tự như ở bước 203. Để biết chi tiết, dựa vào nội dung nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Ngoài ra, phần tử mạng quản lý phiên xác định, theo chính sách bảo mật mặt phẳng người dùng thứ hai, xem có cập nhập hay không thông tin tăng cường bảo mật mặt phẳng người dùng của phiên chuyển tiếp.

Sau khi xác định chính sách bảo mật mặt phẳng người dùng thứ hai, phần tử mạng quản lý phiên có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai. Thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp có thể được sử dụng để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Có nhiều cách trong đó phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai. Phần sau liệt kê ba cách.

Cách 1: Phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp chỉ theo chính sách bảo mật mặt phẳng người dùng thứ hai. Cách này tương tự với cách ở bước 204. Để biết chi tiết, dựa vào nội dung nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này.

Phần tử mạng quản lý phiên có thể so sánh thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp. Nếu thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp phù hợp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, thì biểu thị rằng trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất có thể duy trì không thay đổi, và phần tử mạng quản lý phiên có thể không thông báo cho thiết bị mạng truy cập về thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai. Nếu thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp không phù hợp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, phần tử mạng quản lý phiên có thể cần thông báo cho thiết bị mạng truy cập của thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai, sao cho thiết bị mạng truy cập có thể tạo cấu hình trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất, và gửi, đến thiết bị đầu cuối thứ nhất, thông tin chỉ báo biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất, để thông báo cho thiết bị đầu cuối thứ nhất xem việc bảo vệ mã hóa và việc bảo vệ tính toàn vẹn có được kích hoạt trên giao diện thứ nhất hay không.

Sau khi nhận thông tin chỉ báo biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất, thiết bị đầu cuối thứ nhất có thể cập nhật trạng thái kích hoạt bảo mật của giao diện thứ hai dựa vào trạng thái kích hoạt bảo mật

mặt phẳng người dùng thứ hai của giao diện thứ nhất. Cách trong đó thiết bị đầu cuối thứ nhất cập nhật trạng thái kích hoạt bảo mật của giao diện thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất tương tự với cách trong đó thiết bị đầu cuối thứ nhất xác định trạng thái kích hoạt bảo mật của giao diện thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất. Để biết chi tiết, dựa vào phần mô tả ở trên. Các chi tiết không được mô tả lại trong bản mô tả này.

Cách 2: Phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất.

Phần tử mạng quản lý phiên xác định, theo chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất, xem có kích hoạt việc bảo vệ mã hóa và bảo vệ tính toàn vẹn của giao diện thứ nhất hay không.

Ví dụ, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng chính sách bảo vệ mã hóa mặt phẳng người dùng được ưu tiên và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng là không cần thiết, và chính sách bảo mật mặt phẳng người dùng thứ hai biểu thị rằng chính sách bảo vệ mã hóa mặt phẳng người dùng được yêu cầu và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng được yêu cầu, phần tử mạng quản lý phiên có thể xác định rằng việc bảo vệ mã hóa mặt phẳng người dùng của giao diện thứ nhất được yêu cầu và việc bảo vệ tính toàn vẹn mặt phẳng người dùng của giao diện thứ nhất được yêu cầu. Ví dụ khác, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng chính sách bảo vệ mã hóa mặt phẳng người dùng được yêu cầu và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng là không cần thiết, và chính sách bảo mật mặt phẳng người dùng thứ hai biểu thị rằng chính sách bảo vệ mã hóa mặt phẳng người dùng được yêu cầu và chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng được yêu cầu, phần tử mạng quản lý phiên có thể xác định rằng bảo vệ mã hóa mặt phẳng người dùng của giao diện thứ nhất được yêu cầu và việc bảo vệ tính toàn vẹn mặt phẳng người dùng của giao diện thứ nhất được yêu cầu.

Phần tử mạng quản lý phiên có thể giữa lại tính nhất quán của chính sách bảo vệ mã hóa mặt phẳng người dùng hoặc chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng trong chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất, và sử dụng chính sách bảo vệ mã hóa mặt phẳng người dùng hoặc chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng đã giữ lại dưới dạng

bảo vệ mã hóa hoặc bảo vệ tính toàn vẹn tương ứng trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất.

Đối với các chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng hoặc các chính sách bảo vệ mã hóa mặt phẳng người dùng không nhất quán, phần tử mạng quản lý phiên có thể chọn ưu tiên chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng hoặc chính sách bảo vệ mã hóa mặt phẳng người dùng mà có thể cải thiện độ bảo mật. Ví dụ, phần tử mạng quản lý phiên chọn chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng mà được yêu cầu và chính sách bảo vệ mã hóa mặt phẳng người dùng mà được yêu cầu, và sử dụng chính sách bảo vệ tính toàn vẹn mặt phẳng người dùng hoặc chính sách bảo vệ mã hóa mặt phẳng người dùng đã ưu tiên chọn làm bảo vệ tính toàn vẹn hoặc bảo vệ mã hóa tương ứng trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất.

Sau khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất, phần tử mạng quản lý phiên có thể so sánh thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp. Đối với hoạt động được thực hiện bởi phần tử mạng quản lý phiên sau khi so sánh và hoạt động được thực hiện bởi thiết bị đầu cuối thứ nhất, dựa vào các phần mô tả ở cách 1. Các chi tiết không được mô tả lại trong bản mô tả này.

Cách 3: Phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp.

Cách trong đó phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp tương tự với cách 2. Phần tử mạng quản lý phiên có thể giữa lại việc bảo vệ mã hóa hoặc bảo vệ tính toàn vẹn nhất quán trong chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, và sử dụng việc bảo vệ mã hóa hoặc bảo vệ tính toàn vẹn đã giữ lại làm bảo vệ mã hóa hoặc bảo vệ tính toàn vẹn tương ứng trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất.

Đối với việc bảo vệ tính toàn vẹn hoặc bảo vệ mã hóa không nhất quán, phần tử

mạng quản lý phiên có thể ưu tiên chọn bảo vệ tính toàn vẹn hoặc bảo vệ mã hóa mà có thể cải thiện độ an toàn, ví dụ, chọn bảo vệ mã hóa mà được kích hoạt và bảo vệ tính toàn vẹn mà được kích hoạt.

Sau khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất, phần tử mạng quản lý phiên có thể so sánh thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp. Đối với hoạt động được thực hiện bởi phần tử mạng quản lý phiên sau khi so sánh và hoạt động được thực hiện bởi thiết bị đầu cuối thứ nhất, dựa vào các phần mô tả ở cách 1.

Cần lưu ý rằng, khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai, phần tử mạng quản lý phiên có thể còn xem xét thông tin điều khiển QoS và/hoặc tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất. Cách trong đó phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp dựa vào thông tin điều khiển QoS và/hoặc tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất tương tự với cách trong đó phần tử mạng quản lý phiên xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp dựa vào thông tin điều khiển QoS và/hoặc tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất. Để biết chi tiết, dựa vào nội dung nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này.

Trong cách thứ hai, Fig.3 thể hiện phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng khác theo một phương án của sáng chế. Phương pháp này bao gồm các bước sau.

Bước 301 giống với bước 201. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 201. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 302: Sau khi nhận yêu cầu truyền thông trực tiếp thứ nhất, thiết bị đầu cuối thứ nhất xác định rằng phiên để truyền dữ liệu của thiết bị đầu cuối thứ hai cần được tạo, nghĩa là, phiên chuyển tiếp cần được tạo. Thiết bị đầu cuối thứ nhất gửi yêu cầu thiết lập phiên và thông tin thứ hai đến phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thiết lập phiên yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Cách trong đó thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp tương tự với cách trong đó thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp. Để biết chi

tiết, dựa vào phần mô tả ở trên. Các chi tiết không được mô tả lại trong bản mô tả này.

Thiết bị đầu cuối thứ nhất có thể gửi thông điệp N1 đến phần tử mạng quản lý truy cập và di động, trong đó thông điệp N1 bao gồm thông tin thứ hai và yêu cầu thiết lập phiên. Yêu cầu thiết lập phiên có trong vùng chứa N1 SM. Một cách tùy ý, yêu cầu thiết lập phiên có thể còn mang tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất.

Bước 303: Phần tử mạng quản lý truy cập và di động xác định thông tin thứ nhất dựa vào thông tin thứ hai.

Đối với thông tin thứ hai khác, thông tin thứ nhất được xác định bởi phần tử mạng quản lý truy cập và di động dựa vào thông tin thứ hai cũng khác nhau, mà được mô tả riêng biệt dưới đây.

1. Thông tin thứ hai là mã nhận dạng ẩn danh hoặc mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, và thông tin thứ nhất là mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai hoặc biểu thị, theo cách rõ ràng, rằng kiểu của phiên là kiểu chuyển tiếp.

Cách trong đó phần tử mạng quản lý truy cập và di động xác định mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai dựa vào mã nhận dạng ẩn danh hoặc mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai tương tự với cách trong đó phần tử mạng quản lý phiên xác định mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai dựa vào mã nhận dạng ẩn danh hoặc mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai theo phương án được thể hiện trên Fig.2. Phần tử mạng quản lý truy cập và di động có thể thu mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất dựa vào mã nhận dạng ẩn danh hoặc mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai. Để biết chi tiết, dựa vào nội dung nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này.

Một cách tùy ý, thông tin thứ hai có thể theo cách khác là mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai, và thông tin thứ nhất cũng là mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ hai hoặc biểu thị, theo cách rõ ràng, rằng kiểu của phiên là kiểu chuyển tiếp.

Phần tử mạng quản lý truy cập và di động có thể xác định, dựa vào thông tin thứ hai, rằng phiên được thiết lập là phiên chuyển tiếp, và thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ nhất để xác định xem thiết bị đầu cuối thứ nhất có quyền tạo

ra phiên chuyển tiếp hay không. Phần tử mạng quản lý truy cập và di động có thể thu thông tin thuê bao của thiết bị đầu cuối thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng còn lại (phần tử mạng mà hỗ trợ lưu trữ thông tin thuê bao), và xác định, dựa vào thông tin thuê bao, xem thiết bị đầu cuối thứ nhất có được ủy quyền để thiết lập phiên chuyển tiếp hay không. Thông tin thuê bao biểu thị xem thiết bị đầu cuối thứ nhất có được cho phép để đóng vai trò làm thiết bị chuyển tiếp hay không và/hoặc xem thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên chuyển tiếp tương ứng với DNN và/hoặc S-NSSAI được yêu cầu hay không (như được mô tả ở trên, rằng thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp có thể được biểu thị rõ ràng bằng cách sử dụng thông tin nhận dạng chuyển tiếp, hoặc rằng thiết bị đầu cuối thứ nhất được cho phép để đóng vai trò làm thiết bị chuyển tiếp có thể được biểu thị rõ ràng bằng cách phân biệt các chính sách bảo mật mặt phẳng người dùng bằng cách sử dụng phiên chuyển tiếp và phiên không chuyển tiếp. Xem thiết bị đầu cuối thứ nhất có được ủy quyền để thiết lập phiên chuyển tiếp tương ứng với DNN và/hoặc S-NSSAI được yêu cầu hay không có thể được xác định bằng cách xem chính sách bảo mật mặt phẳng người dùng có tương ứng với DNN và/hoặc chính sách bảo mật mặt phẳng người dùng có tương ứng với S-NSSAI mang/mang thông tin nhận dạng chuyển tiếp hoặc sử dụng/sử dụng phiên chuyển tiếp hoặc phiên không chuyển tiếp hay không). Phần tử mạng quản lý truy cập và di động có thể kiểm tra xem thiết bị đầu cuối thứ nhất có thể thiết lập phiên chuyển tiếp của kiểu cụ thể hay không, ví dụ, phiên chuyển tiếp tương ứng với DNN cụ thể và/hoặc S-NSSAI cụ thể.

Một cách tùy ý, phần tử mạng quản lý truy cập và di động có thể xác định, dựa vào thông tin thứ hai, để khởi tạo thủ tục kiểm tra ủy quyền cho phần tử mạng còn lại, sao cho việc kiểm tra ủy quyền phần tử mạng xác định xem thiết bị đầu cuối thứ nhất có được ủy quyền để tạo ra phiên chuyển tiếp hay không và/hoặc xác định xem thiết bị đầu cuối thứ nhất có thể đóng vai trò làm thiết bị chuyển tiếp của thiết bị đầu cuối thứ hai hay không. Phần tử mạng quản lý truy cập và di động xác định, dựa vào kết quả được gửi bởi phần tử mạng kiểm tra ủy quyền, xem thiết bị đầu cuối thứ nhất có được ủy quyền để thiết lập phiên chuyển tiếp hay không và/hoặc xác định xem thiết bị đầu cuối thứ nhất có thể đóng vai trò làm thiết bị chuyển tiếp của thiết bị đầu cuối thứ hai hay không.

Một cách tùy ý, phần tử mạng quản lý truy cập và di động có thể theo cách khác xác định, dựa vào thông tin thứ hai, xem thiết bị đầu cuối thứ nhất có thể đóng vai trò làm thiết bị chuyển tiếp của thiết bị đầu cuối thứ hai hay không.

Một cách tùy ý, phần tử mạng quản lý truy cập và di động có thể theo cách khác thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ hai dựa vào thông tin thứ hai, để xác định xem thiết bị đầu cuối thứ hai có thể thực hiện việc truyền dữ liệu bằng cách sử dụng UE chuyển tiếp hay không. Phần tử mạng quản lý truy cập và di động có thể thu thông tin thuê bao của thiết bị đầu cuối thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng khác, và xác định, dựa vào thông tin thuê bao, xem thiết bị đầu cuối thứ hai có được ủy quyền để sử dụng phiên chuyển tiếp hay không. Thông tin thuê bao biểu thị xem thiết bị đầu cuối thứ hai có thể thực hiện việc truyền dữ liệu bằng cách sử dụng UE chuyển tiếp hay không.

Sau khi việc kiểm tra ủy quyền được thực hiện bởi phần tử mạng quản lý truy cập và di động trên thiết bị đầu cuối thứ nhất thành công, phần tử mạng quản lý truy cập và di động có thể gửi thông tin thứ nhất đến phần tử mạng quản lý phiên. Nếu không thì, phần tử mạng quản lý truy cập và di động có thể từ chối yêu cầu thiết lập phiên của thiết bị đầu cuối thứ nhất.

2. Thông tin thứ nhất biểu thị, theo cách rõ ràng, rằng kiểu của phiên là kiểu chuyển tiếp.

Sau khi nhận thông tin thứ hai, phần tử mạng quản lý truy cập và di động có thể xác định rằng phiên rằng thiết bị đầu cuối thứ nhất cần tạo ra phiên chuyển tiếp, nghĩa là, phiên sau đó cần truyền dữ liệu của thiết bị đầu cuối thứ hai.

Phần tử mạng quản lý truy cập và di động có thể thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ nhất dựa vào thông tin thứ hai, để xác định xem thiết bị đầu cuối thứ nhất có quyền tạo ra phiên chuyển tiếp hay không. Phần tử mạng quản lý truy cập và di động có thể thu thông tin thuê bao của thiết bị đầu cuối thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng khác (phần tử mạng mà hỗ trợ lưu trữ thông tin thuê bao), và xác định, dựa vào thông tin thuê bao, xem thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên chuyển tiếp hay không. Thông tin thuê bao biểu thị xem thiết bị đầu cuối thứ nhất có được ủy quyền để đóng vai trò làm UE chuyển tiếp hay không và/hoặc xem thiết bị đầu cuối thứ nhất có được ủy quyền để thiết lập phiên chuyển tiếp tương ứng với DNN và/hoặc S-NSSAI được yêu cầu hay không. Phần tử mạng quản lý truy cập và di động có thể kiểm tra xem thiết bị đầu cuối thứ nhất có thể thiết lập phiên chuyển tiếp của kiểu cụ thể hay không, ví dụ, phiên chuyển tiếp tương ứng với DNN cụ thể và/hoặc S-NSSAI cụ thể.

Một cách tùy ý, phần tử mạng quản lý truy cập và di động có thể xác định, dựa

vào thông tin thứ hai, để khởi tạo thủ tục kiểm tra ủy quyền cho phần tử mạng còn lại, sao cho việc kiểm tra ủy quyền phần tử mạng xác định xem thiết bị đầu cuối thứ nhất có được ủy quyền để tạo ra phiên chuyển tiếp hay không.

Một cách tùy ý, phần tử mạng quản lý truy cập và di động có thể theo cách khác thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ hai dựa vào thông tin thứ hai, để xác định xem thiết bị đầu cuối thứ hai có thể thực hiện việc truyền dữ liệu bằng cách sử dụng UE chuyển tiếp hay không. Phần tử mạng quản lý truy cập và di động có thể thu thông tin thuê bao của thiết bị đầu cuối thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng khác, và xác định, dựa vào thông tin thuê bao, xem thiết bị đầu cuối thứ hai có được ủy quyền để sử dụng phiên chuyển tiếp hay không. Thông tin thuê bao biểu thị xem thiết bị đầu cuối thứ hai có thể thực hiện việc truyền dữ liệu bằng cách sử dụng UE chuyển tiếp hay không.

Sau khi việc kiểm tra ủy quyền được thực hiện bởi phần tử mạng quản lý truy cập và di động trên thiết bị đầu cuối thứ nhất thành công, phần tử mạng quản lý truy cập và di động có thể gửi thông tin thứ nhất đến phần tử mạng quản lý phiên. Nếu không thì, phần tử mạng quản lý truy cập và di động có thể từ chối yêu cầu thiết lập phiên của thiết bị đầu cuối thứ nhất.

3. Thông tin thứ nhất giống với thông tin thứ hai.

Điều này tương tự với trường hợp trước đó. Phần tử mạng quản lý truy cập và di động có thể thực hiện việc kiểm tra ủy quyền trên thiết bị đầu cuối thứ nhất dựa vào thông tin thứ hai. Nếu việc kiểm tra ủy quyền được thực hiện bởi phần tử mạng quản lý truy cập và di động trên thiết bị đầu cuối thứ nhất thành công, phần tử mạng quản lý truy cập và di động có thể gửi thông tin thứ nhất đến phần tử mạng quản lý phiên. Nghĩa là, thông tin thứ nhất được gửi bởi phần tử mạng quản lý truy cập và di động đến phần tử mạng quản lý phiên giống với thông tin thứ hai được gửi bởi thiết bị đầu cuối thứ nhất đến phần tử mạng quản lý truy cập và di động. Nếu không thì, phần tử mạng quản lý truy cập và di động có thể từ chối yêu cầu thiết lập phiên của thiết bị đầu cuối thứ nhất.

Bước 304: Phần tử mạng quản lý truy cập và di động gửi yêu cầu thiết lập phiên và thông tin thứ nhất đến phần tử mạng quản lý phiên.

Bước 305 giống với bước 203. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 203. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 306 giống với bước 204. Để biết chi tiết, dựa vào các phần mô tả liên quan

ở bước 204. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 307 giống với bước 205. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 205. Các chi tiết không được mô tả lại trong bản mô tả này.

Thông qua các bước từ 301 đến 307, chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp được tạo ra bởi thiết bị đầu cuối thứ nhất được xác định dựa vào thông tin thứ nhất. Thiết bị đầu cuối thứ nhất có thể truyền dữ liệu của thiết bị đầu cuối thứ hai bằng cách sử dụng phiên chuyển tiếp, để đảm bảo độ bảo mật của dữ liệu đã truyền.

Trong quá trình ứng dụng thực tế, thiết bị đầu cuối thứ nhất có thể còn thiết lập truyền thông với thiết bị đầu cuối khác, và thiết bị đầu cuối khác có thể trao đổi dữ liệu với mạng dữ liệu bằng cách sử dụng phiên của thiết bị đầu cuối thứ nhất. Theo cách khác, thiết bị đầu cuối thứ nhất có thể còn truyền dữ liệu của thiết bị đầu cuối khác bằng cách sử dụng phiên chuyển tiếp đã thiết lập. Trong trường hợp này, phiên chuyển tiếp được sử dụng lại bởi thiết bị đầu cuối khác, và chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp có thể cần được xác định lại. Đối với cách trong đó thiết bị đầu cuối thứ ba sử dụng lại phiên chuyển tiếp và xác định lại chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp, dựa vào các phần mô tả liên quan trên Fig.2. Các chi tiết không được mô tả lại trong bản mô tả này.

Cần lưu ý rằng, khi thiết bị đầu cuối thứ ba sử dụng lại phiên chuyển tiếp, thiết bị đầu cuối thứ nhất có thể còn gửi mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba đến phần tử mạng quản lý truy cập và di động theo cách được thể hiện trên Fig.3. Phần tử mạng quản lý truy cập và di động có thể còn xác định mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ ba theo cách tương tự, và sau đó gửi yêu cầu sửa đổi phiên (trong đó yêu cầu sửa đổi phiên không mang mã nhận dạng của thiết bị đầu cuối thứ ba) và mã nhận dạng cố định thuê bao của thiết bị đầu cuối thứ ba đến phần tử mạng quản lý phiên.

Cần lưu ý rằng, theo các phương án được thể hiện trên Fig.2 và Fig.3, ví dụ trong đó thiết bị đầu cuối thứ nhất yêu cầu việc tạo phiên chuyển tiếp sau khi thiết bị đầu cuối thứ hai khởi tạo yêu cầu truyền thông trực tiếp thứ nhất được sử dụng. Trong quá trình ứng dụng thực tế, thiết bị đầu cuối thứ nhất có thể theo cách khác thiết lập phiên chuyển tiếp trước khi thiết bị đầu cuối thứ hai bắt đầu yêu cầu truyền thông trực tiếp thứ nhất, nghĩa là, gửi yêu cầu thiết lập phiên đến phần tử mạng quản lý phiên. Trong trường hợp này, thông tin thứ nhất có thể biểu thị trực tiếp, theo cách chỉ báo rõ ràng, rằng kiểu của

phiên là kiểu chuyển tiếp.

Dựa vào kiến trúc mạng được thể hiện trên Fig.1, phần sau còn mô tả, bằng cách sử dụng một ví dụ trong đó phần tử mạng quản lý dữ liệu hợp nhất là phần tử mạng UDM, phần tử mạng quản lý phiên là phần tử mạng SMF, phần tử mạng quản lý truy cập và di động là phần tử mạng AMF, thiết bị đầu cuối thứ nhất là UE chuyển tiếp, và thiết bị đầu cuối thứ hai là UE từ xa, phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng được thể hiện trên Fig.2. Fig.4A và Fig.4B thể hiện phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế. Phương pháp này bao gồm các bước sau.

Bước 401: Chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký được tạo cấu hình trong phần tử mạng UDM, trong đó chính sách bảo mật mặt phẳng người dùng bao gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp. Chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký có thể được thể hiện trên bảng 1 đến bảng 3. Bảng chỉ là cách biểu diễn dữ liệu. Cách biểu diễn của chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký không bị giới hạn ở phương án này của sáng chế. Ví dụ, chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký có thể theo cách khác được biểu diễn theo cách ánh xạ dữ liệu.

Bước 402: UE chuyển tiếp gửi yêu cầu thiết lập phiên đến phần tử mạng SMF, trong đó yêu cầu thiết lập phiên yêu cầu tạo ra phiên kiểu chuyển tiếp của UE chuyển tiếp, yêu cầu thiết lập phiên bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp.

Bước 403: Phần tử mạng SMF gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng UDM, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất, yêu cầu thu thông tin thuê bao thứ nhất yêu cầu thu thông tin thuê bao của thiết bị đầu cuối thứ nhất, và thông tin thuê bao bao gồm chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký.

Bước 404: Sau khi nhận yêu cầu thu thông tin thuê bao thứ nhất, phần tử mạng UDM xác định chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký.

Bước 405: Phần tử mạng UDM gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng SMF, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký.

Cần lưu ý rằng yêu cầu thu thông tin thuê bao thứ nhất được gửi bởi phần tử mạng SMF đến phần tử mạng UDM có thể yêu cầu tất cả thông tin thuê bao của thiết bị đầu cuối thứ nhất, bao gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất (trong đó chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất và chính sách bảo mật mặt phẳng người dùng khác của phiên chuyển tiếp) và chính sách bảo mật mặt phẳng người dùng của phiên không chuyển tiếp. Phản hồi thu thông tin thuê bao thứ nhất được gửi bởi phần tử mạng UDM đến phần tử mạng SMF bao gồm tất cả thông tin thuê bao của thiết bị đầu cuối thứ nhất. Phần tử mạng SMF có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất trong tất cả thông tin thuê bao của thiết bị đầu cuối thứ nhất. Ngoài ra, yêu cầu thu thông tin thuê bao thứ nhất được gửi bởi phần tử mạng SMF đến phần tử mạng UDM có thể yêu cầu tất cả thông tin thuê bao tương ứng với DNN/S-NSSAI của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất. Ngoài ra, phần tử mạng SMF xác định chính sách bảo mật mặt phẳng người dùng thứ nhất trong tất cả thông tin thuê bao.

Theo một phương án thực hiện khả thi khác, yêu cầu thu thông tin thuê bao thứ nhất được gửi bởi phần tử mạng SMF đến phần tử mạng UDM có thể theo cách khác yêu cầu một số thông tin thuê bao của thiết bị đầu cuối thứ nhất, ví dụ, thông tin thuê bao của thiết bị đầu cuối thứ nhất đóng vai trò làm UE chuyển tiếp. Thông tin thuê bao của thiết bị đầu cuối thứ nhất đóng vai trò làm UE chuyển tiếp bao gồm chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất (trong đó chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất và chính sách bảo mật mặt phẳng người dùng khác của phiên chuyển tiếp). Phản hồi thu thông tin thuê bao thứ nhất được gửi bởi phần tử mạng UDM đến phần tử mạng SMF có thể bao gồm tất cả thông tin thuê bao của thiết bị đầu cuối thứ nhất đóng vai trò làm UE chuyển tiếp, ví dụ, chính sách bảo mật mặt phẳng người dùng thứ nhất và chính sách bảo mật mặt phẳng người dùng khác của phiên chuyển tiếp; hoặc có thể bao gồm chỉ một số thông tin thuê bao của thiết bị đầu cuối thứ nhất đóng vai trò làm UE chuyển tiếp, ví dụ, bao gồm chỉ chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất. Khi nhận chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất, phần tử mạng SMF xác định chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng của phiên chuyển tiếp của thiết bị đầu cuối thứ nhất.

Bước 406: Phần tử mạng SMF xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất, và giao diện thứ nhất có thể còn được gọi là giao diện Uu.

Bước 407: Phần tử mạng SMF gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp đến RAN, và RAN tạo cấu hình trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất dựa vào thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp, và kích hoạt trạng thái kích hoạt bảo mật mặt phẳng người dùng của phiên chuyển tiếp.

Bước 408: RAN gửi thông tin chỉ báo thứ nhất đến UE chuyển tiếp, trong đó thông tin chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất.

Bước 409: UE từ xa gửi yêu cầu truyền thông trực tiếp thứ nhất đến UE chuyển tiếp, trong đó yêu cầu truyền thông trực tiếp thứ nhất bao gồm mã nhận dạng của UE từ xa, và một cách tùy ý, có thể còn bao gồm tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của UE từ xa.

Bước 410: Sau khi nhận yêu cầu truyền thông trực tiếp thứ nhất, UE chuyển tiếp xác định rằng phiên chuyển tiếp được tạo ra cần để truyền dữ liệu của thiết bị đầu cuối thứ hai, và xác định trạng thái kích hoạt bảo mật thông tin của giao diện PC5 dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất, trong đó giao diện PC5 là giao diện truyền thông giữa UE chuyển tiếp và UE từ xa.

Ví dụ, UE chuyển tiếp có thể thiết lập trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của giao diện thứ nhất thành trạng thái kích hoạt bảo mật của giao diện PC5. Ví dụ, nếu bảo vệ mã hóa của giao diện thứ nhất được yêu cầu, và bảo vệ tính toàn vẹn của giao diện thứ nhất là không cần thiết, bảo vệ mã hóa của giao diện PC5 cũng được kích hoạt, và việc bảo vệ tính toàn vẹn của giao diện PC5 vô hiệu hóa.

Ví dụ khác, nếu việc bảo vệ tính toàn vẹn của giao diện thứ nhất được kích hoạt, UE chuyển tiếp có thể xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn và/hoặc thông tin điều khiển Qos của UE từ xa, xem có kích hoạt việc bảo vệ tính toàn vẹn hay không.

Bước 411: UE chuyển tiếp gửi lệnh chế độ bảo mật trực tiếp thứ nhất đến UE từ

xa, trong đó lệnh chế độ bảo mật trực tiếp thứ nhất bao gồm chỉ báo bảo vệ mã hóa và chỉ báo bảo vệ tính toàn vẹn mà lần lượt biểu thị xem có kích hoạt việc bảo vệ mã hóa hay không và xem có kích hoạt việc bảo vệ tính toàn vẹn hay không.

Bước 412: Sau khi nhận lệnh chế độ bảo mật trực tiếp thứ nhất, UE từ xa tạo cấu hình bảo vệ mã hóa và bảo vệ tính toàn vẹn của giao diện PC5 theo lệnh chế độ bảo mật trực tiếp thứ nhất, và gửi thông điệp hoàn thành chế độ bảo mật trực tiếp thứ nhất đến UE chuyển tiếp.

Bước 413: UE chuyển tiếp gửi phản hồi truyền thông trực tiếp thứ nhất đến UE từ xa.

Cần lưu ý rằng, trong các phần mô tả nêu trên, thủ tục tạo phiên chuyển tiếp (bước 402 đến bước 408) được thực hiện trước khi thiết bị đầu cuối thứ hai bắt đầu khởi tạo thủ tục truyền thông trực tiếp (bước 409). Trong quá trình ứng dụng thực tế, thủ tục tạo phiên chuyển tiếp có thể theo cách khác được thực hiện sau bước 409. Nói cách khác, sau khi UE chuyển tiếp nhận yêu cầu truyền thông trực tiếp thứ nhất của UE từ xa, khi phiên chuyển tiếp không được thiết lập hoặc phiên chuyển tiếp đã thiết lập không thể sử dụng lại, UE chuyển tiếp có thể khởi tạo thủ tục tạo phiên chuyển tiếp. Trong trường hợp này, mã nhận dạng của UE từ xa có thể được sử dụng làm thông tin thứ nhất trong yêu cầu thiết lập phiên.

Dựa vào kiến trúc mạng được thể hiện trên Fig.1, phần sau còn mô tả, bằng cách sử dụng một ví dụ trong đó phần tử mạng quản lý dữ liệu hợp nhất là phần tử mạng UDM, phần tử mạng quản lý phiên là phần tử mạng SMF, phần tử mạng quản lý truy cập và di động là phần tử mạng AMF, thiết bị đầu cuối thứ nhất là UE chuyển tiếp, và thiết bị đầu cuối thứ hai là UE từ xa, phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng được thể hiện trên Fig.3. Fig.5A và Fig.5B thể hiện phương pháp xác định chính sách bảo mật mặt phẳng người dùng theo một phương án của sáng chế. Phương pháp này bao gồm các bước sau.

Bước 501 giống với bước 409. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 409. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 502: Sau khi nhận yêu cầu truyền thông trực tiếp thứ nhất, UE chuyển tiếp xác định rằng phiên chuyển tiếp cần được thiết lập, và UE chuyển tiếp gửi thông điệp N1 thứ nhất đến phần tử mạng AMF, trong đó thông điệp N1 thứ nhất bao gồm mã nhận dạng của UE từ xa và vật chứa N1 SM thứ nhất, vật chứa N1 SM thứ nhất bao gồm yêu cầu thiết lập phiên, và vật chứa N1 SM thứ nhất bao gồm tốc độ dữ liệu tối đa bảo vệ

tính toàn vẹn của UE chuyển tiếp.

Bước 503: Sau khi phần tử mạng AMF nhận thông điệp N1 thứ nhất, phần tử mạng AMF có thể xác định, dựa vào mã nhận dạng của UE từ xa, rằng phiên mà UE chuyển tiếp cần tạo ra là phiên chuyển tiếp, và phần tử mạng AMF thực hiện việc kiểm tra ủy quyền trên UE chuyển tiếp, để xác định rằng UE chuyển tiếp có quyền tạo ra phiên chuyển tiếp.

Một cách tùy ý, nếu mã nhận dạng của UE từ xa là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh, phần tử mạng AMF có thể thu SUPI của UE từ xa từ phần tử mạng UDM dựa vào mã nhận dạng của UE từ xa. Phần tử mạng AMF thực hiện việc kiểm tra ủy quyền trên UE từ xa dựa vào SUPI của UE từ xa, để xác định rằng UE từ xa có thể truyền dữ liệu bằng cách sử dụng UE chuyển tiếp.

Bước 504: Sau khi việc kiểm tra ủy quyền được thực hiện bởi phần tử mạng AMF trên UE chuyển tiếp thành công, phần tử mạng AMF gửi thông điệp dịch vụ Nsmf thứ nhất đến phần tử mạng SMF, trong đó thông điệp dịch vụ Nsmf thứ nhất bao gồm SUPI của UE từ xa và vật chứa N1 SM thứ nhất.

Bước 505: Sau khi nhận thông điệp dịch vụ phần tử mạng NSMF thứ nhất, phần tử mạng SMF gửi, đến phần tử mạng UDM, yêu cầu thu thông tin thuê bao thứ nhất mà mang SUPI của UE từ xa, trong đó yêu cầu thu thông tin thuê bao thứ nhất còn bao gồm DNN và S-NSSAI mà là của phiên chuyển tiếp.

Bước 506: Phần tử mạng UDM xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào SUPI của UE từ xa và chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký, và sau đó gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng SMF, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Bước 507 giống với bước 406. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 406. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 508 giống với bước 407. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 407. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 509 giống với bước 408. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 408. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 510 giống với bước 410. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 410. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 511 giống với bước 411. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 411. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 512 giống với bước 412. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 412. Các chi tiết không được mô tả lại trong bản mô tả này.

Bước 513 giống với bước 413. Để biết chi tiết, dựa vào các phần mô tả liên quan ở bước 413. Các chi tiết không được mô tả lại trong bản mô tả này.

Dựa vào kiến trúc mạng được thể hiện trên Fig.1, phần sau còn mô tả, bằng cách sử dụng ví dụ trong đó phần tử mạng quản lý dữ liệu hợp nhất là phần tử mạng UDM, phần tử mạng quản lý phiên là phần tử mạng SMF, phần tử mạng quản lý truy cập và di động là phần tử mạng AMF, thiết bị đầu cuối thứ nhất là UE chuyển tiếp, thiết bị đầu cuối thứ hai là UE từ xa 1, và thiết bị đầu cuối thứ ba là UE từ xa 2, phương pháp xác định thông tin tăng cường bảo mật các mặt phẳng người dùng được thể hiện trên Fig.2 và Fig.3. Fig.6A và Fig.6B thể hiện phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng theo một phương án của sáng chế. Phương pháp bao gồm các bước sau.

Bước 601: UE chuyển tiếp truyền dữ liệu của UE từ xa 1 bằng cách sử dụng phiên chuyển tiếp. Đối với cách thiết lập phiên chuyển tiếp, dựa vào các phương án được thể hiện trên các hình vẽ từ Fig.2 đến Fig.5B.

Bước 602: UE từ xa 2 gửi yêu cầu truyền thông trực tiếp thứ hai đến UE chuyển tiếp, trong đó yêu cầu truyền thông trực tiếp thứ hai mang tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của UE từ xa 2.

Bước 603: Sau khi nhận yêu cầu truyền thông trực tiếp thứ hai, UE chuyển tiếp xác định rằng UE từ xa 2 là để sử dụng lại phiên chuyển tiếp đã thiết lập.

Bước 604: UE chuyển tiếp gửi thông điệp N1 thứ hai đến phần tử mạng AMF, trong đó thông điệp N1 thứ hai bao gồm mã nhận dạng của UE từ xa 2 và vật chứa N1 SM thứ hai, và vật chứa N1 SM thứ hai bao gồm yêu cầu sửa đổi phiên.

Cần lưu ý rằng, nếu bảo vệ mã hóa của phiên chuyển tiếp được kích hoạt, và bảo vệ tính toàn vẹn của phiên chuyển tiếp được kích hoạt, thì thủ tục sửa đổi phiên có thể không được khởi tạo, nghĩa là, bước 604 và các bước tiếp theo không cần được thực hiện.

Bước 605: Sau khi nhận thông điệp N1 thứ hai, phần tử mạng AMF có thể gửi thông điệp dịch vụ Nsmf thứ hai đến phần tử mạng SMF, trong đó thông điệp dịch vụ

Nsmf thứ hai bao gồm mã nhận dạng của UE từ xa 2 và vật chứa N1 SM thứ hai.

Bước 606: Sau khi phần tử mạng SMF nhận thông điệp dịch vụ phần tử mạng NSMF thứ hai, nếu mã nhận dạng của UE từ xa 2 là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh, thì phần tử mạng SMF có thể trước tiên thu SUPI của UE từ xa 2 từ phần tử mạng UDM dựa vào mã nhận dạng của UE từ xa 2.

Bước 607: Phần tử mạng SMF gửi, đến phần tử mạng UDM, yêu cầu thu thông tin thuê bao thứ hai mà mang SUPI của UE từ xa 2, trong đó yêu cầu thu thông tin thuê bao thứ hai còn bao gồm DNN và S-NSSAI mà là của phiên chuyển tiếp.

Bước 608: Phần tử mạng UDM gửi phản hồi thu thông tin thuê bao thứ hai đến phần tử mạng SMF, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai.

Bước 609: Phần tử mạng SMF xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai.

Ví dụ, phần tử mạng SMF xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất và chính sách bảo mật mặt phẳng người dùng thứ hai. Sau đó, phần tử mạng SMF so sánh thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp, và thực hiện bước 609 nếu thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp.

Nếu chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn của phiên chuyển tiếp được kích hoạt hoặc được ưu tiên kích hoạt, phần tử mạng SMF có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của UE chuyển tiếp.

Ví dụ khác, phần tử mạng SMF xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất. Sau đó, phần tử mạng SMF so sánh thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ

hai của phiên chuyển tiếp, và thực hiện bước 609 nếu thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp.

Nếu chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được kích hoạt hoặc được ưu tiên kích hoạt, thì phần tử mạng SMF có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của UE chuyển tiếp.

Ví dụ khác, phần tử mạng SMF xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai. Sau đó, phần tử mạng SMF so sánh thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp, và thực hiện bước 609 nếu thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp.

Bước 610: Phần tử mạng SMF gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp đến RAN, và RAN tạo cấu hình trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất dựa vào thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp, và kích hoạt trạng thái kích hoạt bảo mật mặt phẳng người dùng của phiên chuyển tiếp.

Bước 611: RAN gửi thông tin chỉ báo thứ hai đến UE chuyển tiếp, trong đó thông tin chỉ báo thứ hai biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất.

Bước 612: UE chuyển tiếp cập nhật trạng thái kích hoạt bảo mật của giao diện PC5 dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của giao diện thứ nhất.

Bước 613: UE chuyển tiếp gửi lệnh chế độ bảo mật trực tiếp thứ hai đến UE từ xa 2, trong đó lệnh chế độ bảo mật trực tiếp thứ hai bao gồm chỉ báo bảo vệ mã hóa và chỉ báo bảo vệ tính toàn vẹn mà lần lượt biểu thị xem có kích hoạt việc bảo vệ mã hóa hay không và xem có kích hoạt việc bảo vệ tính toàn vẹn hay không.

Bước 614: Sau khi nhận lệnh chế độ bảo mật trực tiếp thứ hai, UE từ xa 2 tạo cấu hình bảo vệ mã hóa và bảo vệ tính toàn vẹn của giao diện PC5 theo lệnh chế độ bảo mật

trực tiếp thứ hai, và gửi thông điệp hoàn thành chế độ bảo mật trực tiếp thứ hai đến UE chuyển tiếp.

Bước 615: UE chuyển tiếp gửi phản hồi truyền thông trực tiếp thứ hai đến UE từ xa 2.

Dựa vào cùng khái niệm sáng tạo với các phương án về phương pháp, một phương án của sáng chế còn đề xuất thiết bị truyền thông, được tạo cấu hình để thực hiện các phương pháp được thực hiện bởi phần tử mạng quản lý phiên hoặc phần tử mạng SMF theo các phương án về phương pháp nêu trên. Đối với các dấu hiệu liên quan, dựa vào các phương án về phương pháp nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Như được thể hiện trên Fig.7, thiết bị bao gồm bộ phận nhận 701, bộ phận xử lý 702 và bộ phận gửi 703.

Bộ phận nhận 701 được tạo cấu hình để nhận yêu cầu thứ nhất, trong đó yêu cầu thứ nhất này yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, yêu cầu thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp.

Bộ phận xử lý 702 được tạo cấu hình để xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất.

Bộ phận gửi 703 được tạo cấu hình để gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Theo một phương án thực hiện khả thi, yêu cầu thứ nhất bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ nhất. Yêu cầu thứ nhất bao gồm thông tin thứ nhất và vùng chứa N1 SM.

Theo một phương án thực hiện khả thi, khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất, bộ phận xử lý 702 có thể thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất; và sau đó có thể trực tiếp sử dụng chính sách bảo mật mặt phẳng người dùng thứ nhất làm thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên; hoặc có thể phân tích chính sách bảo mật mặt phẳng người dùng thứ nhất, và xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách

bảo mật mặt phẳng người dùng thứ nhất.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, bộ phận gửi 703 có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký biểu thị chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau đó bộ phận nhận 701 nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký. Sau đó, bộ phận xử lý 702 xác định chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất dưới dạng chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, bộ phận gửi 703 có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm chỉ báo chuyển tiếp, và chỉ báo chuyển tiếp này yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau đó, bộ phận nhận 701 nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký (trong đó chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất). Sau đó, bộ phận xử lý 702 xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Theo một phương án thực hiện khả thi, thông tin thứ nhất là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai. Khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, bộ phận xử lý 702 có thể thu SUPI của thiết bị đầu cuối thứ hai dựa vào mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai. Sau đó, bộ phận gửi 703 có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm SUPI của thiết bị đầu

cuối thứ hai. Bộ phận nhận 701 có thể nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó thông tin được mang trong phản hồi thu thông tin thuê bao thứ nhất có thể là bất kỳ trong số sau:

1. Phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

2. Phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Sau đó, bộ phận xử lý 702 xác định chính sách bảo mật mặt phẳng người dùng thứ nhất theo chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

3. Phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký. Sau đó, bộ phận xử lý 702 xác định chính sách bảo mật mặt phẳng người dùng thứ nhất theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, bộ phận gửi 703 có thể gửi yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất. Sau đó, bộ phận nhận 701 nhận phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo một phương án thực hiện khả thi, thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu cuối thứ hai bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai, hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ hai.

Theo một phương án thực hiện khả thi, chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được ưu tiên. Khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất, bộ phận xử lý 702 có thể xác định, sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc

độ dữ liệu được yêu cầu bởi phiên, rằng việc bảo vệ tính toàn vẹn của phiên là không cần thiết.

Theo một phương án thực hiện khả thi, nếu chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu, bộ phận xử lý 702 có thể xác định xem tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất có nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên hay không. Sau khi bộ phận xử lý 702 xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, bộ phận gửi 703 gửi phản hồi từ chối thiết lập phiên đến thiết bị đầu cuối thứ nhất, trong đó phản hồi từ chối thiết lập phiên biểu thị việc từ chối thiết lập phiên.

Theo một phương án thực hiện khả thi, bộ phận nhận 701 có thể còn nhận yêu cầu thứ ba, trong đó yêu cầu thứ ba biểu thị rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, và yêu cầu thứ ba bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Bộ phận xử lý 702 có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba. Bộ phận gửi 703 có thể gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Theo một phương án thực hiện khả thi, khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, bộ phận xử lý 702 có thể xác định chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba; và sau đó xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo một phương án thực hiện khả thi, mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba, hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ ba.

Theo một phương án thực hiện khả thi, khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai, bộ phận xử lý 702 có thể xác định thông tin tăng cường bảo mật mặt phẳng

người dùng thứ hai của phiên dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên; có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất; hoặc có thể xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chỉ theo chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, bộ phận gửi 703 có thể gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Bộ phận nhận 701 có thể nhận phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, bộ phận xử lý 702 có thể xác định chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, bộ phận gửi 703 gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Bộ phận nhận 701 nhận phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất. Bộ phận xử lý 702 xác định chính sách bảo mật mặt phẳng người dùng thứ hai theo chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

Theo một phương án thực hiện khả thi, khi bộ phận xử lý 702 thu chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, bộ phận gửi 703 gửi yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng

của thiết bị đầu cuối thứ ba. Bộ phận nhận 701 nhận phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ ba đăng ký. Bộ phận xử lý 702 xác định chính sách bảo mật mặt phẳng người dùng thứ hai theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ ba đăng ký.

Theo một phương án thực hiện khả thi, trước khi bộ phận gửi 703 gửi thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập, bộ phận xử lý 702 có thể xác định rằng thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên.

Theo một phương án thực hiện khả thi, chính sách bảo mật mặt phẳng người dùng thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn của phiên được ưu tiên. Khi xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai, bộ phận xử lý 702 xác định, sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, để vô hiệu hóa việc bảo vệ tính toàn vẹn của phiên.

Dựa vào cùng các khái niệm sáng tạo với các phương án về phương pháp, một phương án của sáng chế còn đề xuất thiết bị truyền thông, được tạo cấu hình để thực hiện các phương pháp được thực hiện bởi thiết bị đầu cuối thứ nhất hoặc UE chuyển tiếp theo các phương án về phương pháp nêu trên. Đối với các dấu hiệu liên quan, dựa vào các phương án về phương pháp nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Như được thể hiện trên Fig.8, thiết bị bao gồm bộ phận gửi 801 và bộ phận nhận 802.

Bộ phận gửi 801 được tạo cấu hình để gửi yêu cầu thứ hai đến phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thứ hai yêu cầu tạo ra phiên kiểu chuyển tiếp, yêu cầu thứ hai bao gồm thông tin thứ hai, và thông tin thứ hai này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp.

Bộ phận nhận 802 được tạo cấu hình để nhận thông tin chỉ báo thứ nhất được gửi bởi thiết bị mạng truy cập, trong đó thông tin chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Theo một phương án thực hiện khả thi, trước khi bộ phận gửi 801 gửi yêu cầu thứ hai, bộ phận nhận 802 có thể nhận yêu cầu truyền thông trực tiếp thứ nhất được gửi

bởi thiết bị đầu cuối thứ hai, trong đó yêu cầu truyền thông trực tiếp thứ nhất là để thiết lập truyền thông với thiết bị đầu cuối thứ nhất.

Theo một phương án thực hiện khả thi, yêu cầu thứ hai bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ hai; hoặc yêu cầu thứ hai bao gồm thông tin thứ hai và vùng chứa N1 SM.

Theo một phương án thực hiện khả thi, phiên là để truyền dữ liệu của thiết bị đầu cuối thứ hai. Thông tin thứ hai bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc SUPI của thiết bị đầu cuối thứ hai.

Theo một phương án thực hiện khả thi, thiết bị còn bao gồm bộ phận xử lý 803.

Bộ phận nhận 802 có thể nhận yêu cầu truyền thông trực tiếp thứ hai được gửi bởi thiết bị đầu cuối thứ ba, trong đó yêu cầu truyền thông trực tiếp thứ hai là để thiết lập truyền thông với thiết bị đầu cuối thứ nhất. Sau đó, bộ phận xử lý 803 có thể xác định, dựa vào yêu cầu truyền thông trực tiếp thứ hai, rằng thiết bị đầu cuối thứ ba là để sử dụng phiên. Bộ phận gửi 801 có thể gửi yêu cầu thứ ba đến phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thứ ba biểu thị rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, và yêu cầu thứ ba bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba.

Theo một phương án thực hiện khả thi, mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba hoặc SUPI của thiết bị đầu cuối thứ ba.

Theo một phương án thực hiện khả thi, sau khi bộ phận nhận 802 nhận, từ thiết bị mạng truy cập, thông tin chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất, bộ phận xử lý 803 có thể xác định trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Theo một phương án thực hiện khả thi, nếu việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất được yêu cầu, khi tạo cấu hình trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất, bộ phận xử lý 803 có thể xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển

Qos của thiết bị đầu cuối thứ hai, xem có kích hoạt việc bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai hay không.

Theo một phương án thực hiện khả thi, nếu việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất là không cần thiết, bộ phận gửi 801 có thể gửi thông điệp từ chối truyền thông trực tiếp đến thiết bị đầu cuối thứ hai khi chính sách bảo mật mặt phẳng người dùng của thiết bị đầu cuối thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu.

Theo một phương án thực hiện khả thi, bộ phận nhận 802 có thể còn nhận thông tin chỉ báo thứ hai từ thiết bị mạng truy cập, trong đó thông tin chỉ báo thứ hai biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

Bộ phận xử lý 803 có thể cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất thành trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai dựa vào thông tin chỉ báo thứ hai.

Theo một phương án thực hiện khả thi, sau khi bộ phận nhận 802 nhận thông tin chỉ báo thứ hai từ thiết bị mạng truy cập, bộ phận xử lý 803 có thể cập nhật trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai.

Theo một phương án thực hiện khả thi, việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai được yêu cầu. Khi cập nhật trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai, bộ phận xử lý 803 có thể xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển Qos của thiết bị đầu cuối thứ ba, xem có kích hoạt việc bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai hay không.

Dựa vào cùng khái niệm sáng tạo với các phương án về phương pháp, một phương án của sáng chế còn đề xuất thiết bị truyền thông, được tạo cấu hình để thực hiện các phương pháp được thực hiện bởi phần tử mạng quản lý truy cập và di động hoặc phần tử mạng AMF theo các phương án về phương pháp nêu trên. Đối với các dấu hiệu liên quan, dựa vào các phương án về phương pháp nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Như được thể hiện trên Fig.9, thiết bị bao gồm bộ phận nhận 901 và bộ phận gửi 902.

Bộ phận nhận 901 được tạo cấu hình để nhận yêu cầu thứ hai được gửi bởi thiết bị đầu cuối thứ nhất, trong đó yêu cầu thứ hai bao gồm thông tin thứ hai, yêu cầu thứ hai yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp.

Bộ phận gửi 902 được tạo cấu hình để gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên dựa vào yêu cầu thứ hai, trong đó yêu cầu thứ nhất bao gồm thông tin thứ nhất, thông tin thứ nhất biểu thị rằng kiểu của phiên là kiểu chuyển tiếp, và yêu cầu thứ nhất yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

Theo một phương án thực hiện khả thi, thông tin thứ hai giống với thông tin thứ nhất, mỗi trong số yêu cầu thứ nhất và yêu cầu thứ hai bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ hai.

Theo một phương án thực hiện khả thi, yêu cầu thứ hai bao gồm thông tin thứ hai và vùng chứa N1 SM, và yêu cầu thứ nhất bao gồm thông tin thứ nhất và vùng chứa N1 SM.

Theo một phương án thực hiện khả thi, thiết bị bao gồm bộ phận xử lý 903. Bộ phận xử lý 903 có thể xác định, dựa vào thông tin thứ hai, rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên. Sau khi bộ phận xử lý 903 xác định, dựa vào thông tin thứ hai, rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên, bộ phận gửi 902 gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên.

Theo một phương án thực hiện khả thi, thông tin thứ hai là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai, và thông tin thứ nhất là SUPI của thiết bị đầu cuối thứ hai.

Theo một phương án thực hiện khả thi, thông tin thứ hai bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc SUPI của thiết bị đầu cuối thứ hai.

Theo một phương án thực hiện khả thi, trước khi bộ phận gửi 902 gửi yêu cầu thứ nhất đến phần tử mạng quản lý phiên dựa vào yêu cầu thứ hai, bộ phận xử lý 903 có thể xác định, dựa vào thông tin thứ hai, rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên cho thiết bị đầu cuối thứ hai.

Dựa vào cùng khái niệm sáng tạo với các phương án về phương pháp, một phương án của sáng chế còn đề xuất thiết bị truyền thông, được tạo cấu hình để thực

hiện các phương pháp được thực hiện bởi phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng UDM theo các phương án về phương pháp nêu trên. Đối với các dấu hiệu liên quan, dựa vào các phương án về phương pháp nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Như được thể hiện trên Fig.10, thiết bị bao gồm bộ phận nhận 1001, bộ phận xử lý 1002, và bộ phận gửi 1003.

Bộ phận nhận 1001 được tạo cấu hình để nhận yêu cầu thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ nhất yêu cầu chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu phiên là kiểu chuyển tiếp.

Bộ phận xử lý 1002 được tạo cấu hình để xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất.

Bộ phận gửi 1003 được tạo cấu hình để gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

Theo một phương án thực hiện khả thi, khi xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, bộ phận xử lý 1002 có thể xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, trong đó chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký biểu thị các chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp và phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất.

Theo một phương án thực hiện khả thi, thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai. Khi bộ phận xử lý 1002 xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất, bộ phận xử lý 1002 xác định, dựa vào mã nhận dạng của thiết bị đầu cuối thứ hai, chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

Theo một phương án thực hiện khả thi, bộ phận nhận 1001 có thể nhận yêu cầu thu thông tin thuê bao thứ hai từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba.

Bộ phận xử lý 1002 có thể xác định chính sách bảo mật mặt phẳng người dùng

thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba.

Bộ phận gửi 1003 có thể gửi phản hồi thu thông tin thuê bao thứ hai đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai.

Theo một phương án thực hiện khả thi, mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba, hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ ba.

Dựa vào cùng khái niệm sáng tạo với các phương án về phương pháp, một phương án của sáng chế còn đề xuất thiết bị truyền thông, được tạo cấu hình để thực hiện các phương pháp được thực hiện bởi phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng UDM theo các phương án về phương pháp nêu trên. Đối với các dấu hiệu liên quan, dựa vào các phương án về phương pháp nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này. Như được thể hiện trên Fig.11, thiết bị bao gồm bộ phận nhận 1101 hoặc bộ phận gửi 1102.

Bộ phận nhận 1101 được tạo cấu hình để nhận yêu cầu thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ nhất yêu cầu chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký biểu thị chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất.

Bộ phận gửi 1102 được tạo cấu hình để gửi phản hồi thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

Theo một phương án thực hiện khả thi, thiết bị còn bao gồm bộ phận xử lý 1103.

Bộ phận nhận 1101 có thể nhận yêu cầu thu thông tin thuê bao thứ hai từ phần tử mạng quản lý phiên, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba. Bộ phận xử lý 1103 có thể xác định chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba.

Bộ phận gửi 1102 có thể gửi phản hồi thu thông tin thuê bao thứ hai đến phần tử mạng quản lý phiên, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai.

Sự phân chia thành các bộ phận theo các phương án của sáng chế là một ví dụ và chỉ là sự phân chia chức năng logic, và có thể có cách phân chia khác trong quá trình thực hiện thực tế. Ngoài ra, các bộ phận chức năng theo các phương án của sáng chế có thể được tích hợp vào một bộ xử lý, mỗi trong số các bộ phận này có thể tồn tại độc lập về mặt vật lý, hoặc hai hoặc nhiều hơn hai bộ phận được tích hợp vào một môđun. Bộ phận đã tích hợp có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng môđun chức năng phần mềm.

Khi bộ phận đã tích hợp được thực hiện dưới dạng bộ phận chức năng phần mềm và được bán hoặc sử dụng dưới dạng sản phẩm độc lập, bộ phận đã tích hợp có thể được lưu trữ trong phương tiện lưu trữ đọc được bằng máy tính. Dựa vào việc hiểu này, các giải pháp kỹ thuật của sáng chế về cơ bản hoặc một phần đóng góp vào tình trạng kỹ thuật, hoặc tất cả hoặc một phần của các giải pháp kỹ thuật có thể được thể hiện dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm máy tính được lưu trữ trong phương tiện lưu trữ, và bao gồm một số lệnh để lệnh cho thiết bị đầu cuối (mà có thể là máy tính cá nhân, điện thoại di động, thiết bị mạng hoặc dạng tương tự) hoặc bộ xử lý (processor) để thực hiện tất cả hoặc một số bước của các phương pháp theo các phương án của sáng chế. Phương tiện lưu trữ nêu trên bao gồm phương tiện bất kỳ mà có thể lưu trữ mã chương trình, chẳng hạn như ổ đĩa chớp USB, đĩa cứng tháo rời được, bộ nhớ chỉ đọc (read-only memory, ROM), bộ nhớ truy cập ngẫu nhiên (random access memory, RAM), đĩa từ hoặc đĩa quang.

Theo các phương án của sáng chế, mỗi trong số phần tử mạng quản lý dữ liệu hợp nhất, phần tử mạng quản lý phiên, phần tử mạng quản lý truy cập và di động, và thiết bị đầu cuối thứ nhất có thể được biểu diễn dưới dạng các môđun chức năng thu được thông qua việc phân chia theo cách được tích hợp. "Môđun" trong bản mô tả này có thể là ASIC cụ thể, mạch, bộ xử lý và bộ nhớ mà thực thi một hoặc nhiều chương trình phần mềm hoặc phần sụn, mạch logic tích hợp và/hoặc thành phần khác mà có thể tạo ra các chức năng nêu trên.

Theo một phương án đơn giản, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể chỉ ra rằng phần tử mạng quản lý dữ liệu hợp nhất, phần tử mạng quản lý phiên, và mỗi trong số phần tử mạng quản lý truy cập và di động có thể ở dạng được thể

hiện trên Fig.12.

Thiết bị truyền thông 1200 được thể hiện trên Fig.12 bao gồm ít nhất một bộ xử lý 1201 và bộ nhớ 1202, và một cách tùy chọn, có thể còn bao gồm giao diện truyền thông 1203.

Bộ nhớ 1202 có thể là bộ nhớ khả biến chẳng hạn như bộ nhớ truy cập ngẫu nhiên. Theo cách khác, bộ nhớ có thể là bộ nhớ không khả biến, ví dụ, bộ nhớ chỉ đọc, bộ nhớ chớp, ổ đĩa cứng (hard disk drive, HDD) hoặc ổ đĩa thể rắn (solid-state drive, SSD). Theo cách khác, bộ nhớ 1202 là phương tiện khác bất kỳ mà có thể thực hiện hoặc lưu trữ mã chương trình được dự kiến dưới dạng các lệnh hoặc cấu trúc dữ liệu và có thể được truy cập bởi máy tính. Tuy nhiên, điều này không bị giới hạn ở đó. Bộ nhớ 1202 có thể là sự kết hợp của các bộ nhớ nêu trên.

Theo các phương án này của sáng chế, phương tiện kết nối cụ thể giữa bộ xử lý 1201 và bộ nhớ 1202 không bị giới hạn. Theo các phương án này của sáng chế, bộ nhớ 1202 được kết nối với bộ xử lý 1201 thông qua bus 1204 trên hình vẽ. Bus 1204 được biểu thị bởi đường đậm trên hình vẽ. Chế độ kết nối giữa các thành phần khác được mô tả sơ lược, và không bị giới hạn ở đó. Bus 1204 có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển và dạng tương tự. Để dễ biểu diễn, chỉ một đường đậm là để biểu diễn bus trên Fig.12, nhưng không có nghĩa là chỉ có một bus hoặc chỉ một kiểu bus.

Bộ xử lý 1201 có thể có chức năng gửi/nhận dữ liệu, và có thể truyền thông với thiết bị khác. Trong thiết bị được thể hiện trên Fig.12, môđun thu-phát dữ liệu độc lập, ví dụ, giao diện truyền thông 1203, có thể còn được bố trí và được tạo cấu hình để gửi/nhận dữ liệu. Khi truyền thông với thiết bị khác, bộ xử lý 1201 có thể thực hiện việc truyền dữ liệu thông qua giao diện truyền thông 1203.

Khi phần tử mạng quản lý phiên là ở dạng được thể hiện trên Fig.12, bộ xử lý 1201 trên Fig.12 có thể gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202, sao cho phần tử mạng quản lý phiên có thể thực hiện phương pháp được thực hiện bởi phần tử mạng quản lý phiên hoặc phần tử mạng SMF theo phương án bất kỳ trong số các phương án về phương pháp nêu trên.

Cụ thể, tất cả các chức năng/quy trình thực hiện của bộ phận gửi, bộ phận nhận, và bộ phận xử lý trên Fig.7 có thể được thực hiện bởi bộ xử lý 1201 trên Fig.12 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202. Theo cách khác, chức năng/quy trình thực hiện của bộ phận xử lý trên Fig.7 có thể được thực

hiện bởi bộ xử lý 1201 trên Fig.12 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202, và các chức năng/quy trình thực hiện của bộ phận gửi và bộ phận nhận trên Fig.7 có thể được thực hiện bởi giao diện truyền thông 1203 trên Fig.12.

Khi phần tử mạng quản lý truy cập và di động là ở dạng được thể hiện trên Fig.12, bộ xử lý 1201 trên Fig.12 có thể gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202, sao cho phần tử mạng quản lý truy cập và di động có thể thực hiện phương pháp được thực hiện bởi phần tử mạng quản lý truy cập và di động hoặc phần tử mạng AMF theo phương án bất kỳ trong số các phương án về phương pháp nêu trên.

Cụ thể, tất cả các chức năng/tquy trình hực hiện của bộ phận nhận, bộ phận gửi, và bộ phận xử lý trên Fig.9 có thể được thực hiện bởi bộ xử lý 1201 trên Fig.12 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202. Theo cách khác, chức năng/quy trình thực hiện của bộ phận xử lý trên Fig.9 có thể được thực hiện bởi bộ xử lý 1201 trên Fig.12 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202, và các chức năng/quy trình thực hiện của bộ phận nhận và bộ phận gửi trên Fig.9 có thể được thực hiện bởi giao diện truyền thông 1203 trên Fig.12.

Khi phần tử mạng quản lý dữ liệu hợp nhất là ở dạng được thể hiện trên Fig.12, bộ xử lý 1201 trên Fig.12 có thể gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202, sao cho phần tử mạng quản lý dữ liệu hợp nhất có thể thực hiện phương pháp được thực hiện bởi phần tử mạng quản lý dữ liệu hợp nhất hoặc phần tử mạng UDM theo phương án bất kỳ trong số các phương án về phương pháp nêu trên.

Cụ thể, tất cả các chức năng/quy trình thực hiện của bộ phận gửi, bộ phận nhận, và bộ phận xử lý trên Fig.10 hoặc Fig.11 có thể được thực hiện bởi bộ xử lý 1201 trên Fig.12 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202. Theo cách khác, chức năng/quy trình thực hiện của bộ phận xử lý trên Fig.10 hoặc Fig.11 có thể được thực hiện bởi bộ xử lý 1201 trên Fig.12 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1202, và các chức năng/quy trình thực hiện của bộ phận gửi và bộ phận nhận trên Fig.10 hoặc Fig.11 có thể được thực hiện bởi giao diện truyền thông 1203 trên Fig.12.

Theo một phương án đơn giản, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể chỉ ra rằng thiết bị đầu cuối thứ nhất có thể là ở dạng được thể hiện trên

Fig.13.

Thiết bị truyền thông 1300 được thể hiện trên Fig.13 bao gồm ít nhất một bộ xử lý 1301 và bộ nhớ 1302, và một cách tùy chọn, có thể còn bao gồm bộ thu-phát 1303.

Bộ xử lý 1301 và bộ nhớ 1302 tương tự với bộ xử lý 1201 và bộ nhớ 1202. Để biết chi tiết, dựa vào nội dung nêu trên. Các chi tiết không được mô tả lại trong bản mô tả này.

Theo các phương án này của sáng chế, phương tiện kết nối cụ thể giữa bộ xử lý 1301 và bộ nhớ 1302 không bị giới hạn. Theo các phương án này của sáng chế, bộ nhớ 1302 được kết nối với bộ xử lý 1301 thông qua bus 1304 trên hình vẽ. Bus 1304 được biểu thị bởi đường đậm trên hình vẽ. Chế độ kết nối giữa các thành phần khác được mô tả sơ lược, và không bị giới hạn ở đó. Bus 1304 có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển và dạng tương tự. Để dễ thể hiện, chỉ một đường đậm là để biểu diễn bus trên Fig.13, nhưng không có nghĩa là chỉ có một bus hoặc chỉ một kiểu bus.

Bộ xử lý 1301 có thể có chức năng gửi/nhận dữ liệu, và có thể truyền thông với thiết bị khác. Trong thiết bị được thể hiện trên Fig.13, môđun thu-phát dữ liệu độc lập, ví dụ, bộ thu-phát 1303, có thể còn được bố trí và được tạo cấu hình để gửi/nhận dữ liệu. Khi truyền thông với thiết bị khác, bộ xử lý 1301 có thể thực hiện việc truyền dữ liệu thông qua bộ thu-phát 1303.

Khi thiết bị đầu cuối thứ nhất là ở dạng được thể hiện trên Fig.13, bộ xử lý 1301 trên Fig.13 có thể gọi ra lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1302, sao cho thiết bị đầu cuối thứ nhất có thể thực hiện phương pháp được thực hiện bởi thiết bị đầu cuối thứ nhất hoặc UE chuyển tiếp theo phương án bất kỳ trong số các phương án về phương pháp nêu trên.

Cụ thể, tất cả các chức năng/quy trình thực hiện của bộ phận gửi, bộ phận nhận, và bộ phận xử lý trên Fig.8 có thể được thực hiện bởi bộ xử lý 1301 trên Fig.13 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1302. Theo cách khác, chức năng/quy trình thực hiện của bộ phận xử lý trên Fig.8 có thể được thực hiện bởi bộ xử lý 1301 trên Fig.13 bằng cách gọi ra các lệnh thực thi được bằng máy tính được lưu trữ trong bộ nhớ 1302, và các chức năng/quy trình thực hiện của bộ phận gửi và bộ phận nhận trên Fig.8 có thể được thực hiện bởi bộ thu-phát 1303 trên Fig.13.

Trong phương pháp, người có hiểu biết trung bình trong lĩnh vực kỹ thuật cần

hiểu rằng các phương án của sáng chế có thể được đề xuất dưới dạng phương pháp, hệ thống hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng các phương án chỉ phần cứng, các phương án chỉ phần mềm hoặc các phương án với sự kết hợp của phần mềm và phần cứng. Ngoài ra, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính mà được thực hiện một hoặc nhiều phương tiện lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa, CD-ROM, bộ nhớ qaung và dạng tương tự) mà bao gồm mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả dựa vào các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống) và sản phẩm chương trình máy tính theo sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi quy trình và/hoặc mỗi khối trên các lưu đồ và/hoặc các sơ đồ khối và sự kết hợp của quy trình và/hoặc khối trên các lưu đồ và/hoặc các sơ đồ khối. Máy tính các lệnh chương trình có thể được tạo ra cho máy tính dùng cho mục đích chung, máy tính được dành riêng, bộ xử lý nhúng hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra máy, sao cho các lệnh được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác tạo ra thiết bị được tạo cấu hình để thực hiện chức năng được chỉ định trong một hoặc nhiều bộ xử lý trên các lưu đồ và/hoặc trong một hoặc nhiều khối trên các sơ đồ khối.

Các lệnh chương trình máy tính có thể theo cách khác được lưu trữ trong bộ nhớ đọc được bằng máy tính mà có thể hướng dẫn máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác hoạt động theo cách cụ thể, sao cho các lệnh được lưu trữ trong bộ nhớ đọc được bằng máy tính tạo ra thành phần lạ mà bao gồm thiết bị lệnh. Thiết bị lệnh thực hiện chức năng được chỉ định trong một hoặc nhiều bộ xử lý trên các lưu đồ và/hoặc trong một hoặc nhiều khối trên các sơ đồ khối.

Các lệnh chương trình máy tính có thể theo cách khác được tải lên trên máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho một loạt các hoạt động và bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác để tạo ra quá trình xử lý được thực hiện bằng máy tính. Do đó, các lệnh được thực thi trên máy tính hoặc thiết bị lập trình được khác tạo ra các bước để thực hiện chức năng được chỉ định trong một hoặc nhiều bộ xử lý trên các lưu đồ và/hoặc trong một hoặc nhiều khối trên các sơ đồ khối.

Rõ ràng, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể thực hiện các cải biến và thay đổi khác nhau đối với sáng chế mà không lệch khỏi phạm vi của

sáng chế. Sáng chế nhằm bao gồm các cải biến và thay đổi này của sáng chế được đề xuất mà chúng sẽ nằm trong phạm vi của các điểm yêu cầu bảo hộ của sáng chế và các công nghệ tương đương của chúng.

YÊU CẦU BẢO HỘ

1. Phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, phương pháp này bao gồm các bước:

nhận (202), bởi phần tử mạng quản lý phiên, yêu cầu thứ nhất, trong đó yêu cầu thứ nhất này yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, thiết bị đầu cuối thứ nhất là thiết bị chuyển tiếp, yêu cầu thứ nhất bao gồm thông tin thứ nhất, và thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp;

xác định (203, 204), bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất; và

gửi (205), bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập, trong đó trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn và bảo vệ mã hóa mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập được kích hoạt hoặc vô hiệu hóa.

2. Phương pháp theo điểm 1, trong đó yêu cầu thứ nhất bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ nhất; hoặc

yêu cầu thứ nhất bao gồm thông tin thứ nhất và vùng chứa N1 SM.

3. Phương pháp theo điểm 1 hoặc điểm 2, trong đó bước xác định (203, 204), bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông tin thứ nhất bao gồm các bước:

thu (203), bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất; và

xác định (204), bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất.

4. Phương pháp theo điểm 3, trong đó bước thu (203), bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất bao gồm các bước:

gửi, bởi phần tử mạng quản lý phiên, yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất;

nhận, bởi phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký này bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng của phiên kiểu không chuyển tiếp của thiết bị đầu cuối thứ nhất; và

xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất dưới dạng chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất.

5. Phương pháp theo điểm 3, trong đó bước thu, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất bao gồm các bước:

gửi, bởi phần tử mạng quản lý phiên, yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm chỉ báo chuyển tiếp, và chỉ báo chuyển tiếp này yêu cầu chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất; và

nhận, bởi phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký, và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

6. Phương pháp theo điểm 4 hoặc điểm 5, trong đó thông tin thứ nhất có thể là mã nhận dạng tạm thời hoặc mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai, và phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bất kỳ trong số các chính sách sau:

chính sách bảo mật mặt phẳng người dùng thứ nhất, chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất và chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ hai đăng ký.

7. Phương pháp theo điểm 3, trong đó bước xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên dựa vào thông

tin thứ nhất bao gồm các bước:

gửi, bởi phần tử mạng quản lý phiên, yêu cầu thu thông tin thuê bao thứ nhất đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ nhất bao gồm thông tin thứ nhất; và

nhận, bởi phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ nhất từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ nhất bao gồm chính sách bảo mật mặt phẳng người dùng thứ nhất.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó thông tin thứ nhất là mã nhận dạng của thiết bị đầu cuối thứ hai, và mã nhận dạng của thiết bị đầu cuối thứ hai bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai, hoặc mã nhận dạng cố định thuê bao (subscription permanent identifier, SUPI) của thiết bị đầu cuối thứ hai.

9. Phương pháp theo điểm bất kỳ trong số các điểm từ 3 đến 8, trong đó chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được ưu tiên, và bước xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất bao gồm bước:

sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, thì xác định, bởi phần tử mạng quản lý phiên, rằng việc bảo vệ tính toàn vẹn của phiên trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất là không cần thiết.

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 3 đến 8, trong đó chính sách bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu, và bước xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên theo chính sách bảo mật mặt phẳng người dùng thứ nhất bao gồm bước:

gửi, bởi phần tử mạng quản lý phiên, phản hồi từ chối thiết lập phiên đến thiết bị đầu cuối thứ nhất sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, trong đó phản hồi từ chối thiết lập phiên biểu thị việc từ chối thiết lập phiên.

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 10, trong đó phương pháp

này còn bao gồm các bước:

nhận, bởi phần tử mạng quản lý phiên, yêu cầu thứ ba, trong đó yêu cầu thứ ba biểu thị rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, và yêu cầu thứ ba này bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba;

xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba; và

gửi, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập, trong đó thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên là để xác định trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập.

12. Phương pháp theo điểm 11, trong đó bước xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm các bước:

xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba; và

xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai.

13. Phương pháp theo điểm 11 hoặc điểm 12, trong đó trước khi gửi, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên đến thiết bị mạng truy cập, phương pháp này còn bao gồm bước:

xác định, bởi phần tử mạng quản lý phiên, rằng thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên khác với thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên.

14. Phương pháp theo điểm bất kỳ trong số các điểm từ 11 đến 13, trong đó mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một phần hoặc tất cả các mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba hoặc SUPI của thiết bị đầu cuối thứ ba.

15. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 14, trong đó bước xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai bao gồm các bước:

xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên dựa vào chính sách bảo mật mặt phẳng người dùng thứ hai và thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên;

xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai và chính sách bảo mật mặt phẳng người dùng thứ nhất; hoặc

xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai.

16. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 15, trong đó bước xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm các bước:

gửi, bởi phần tử mạng quản lý phiên, yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba; và nhận, bởi phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng thứ hai; hoặc

xác định, bởi phần tử mạng quản lý phiên dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba, chính sách bảo mật mặt phẳng người dùng thứ hai từ chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ nhất đăng ký.

17. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 15, trong đó bước xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm các bước:

gửi, bởi phần tử mạng quản lý phiên, yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba;

nhận, bởi phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ hai từ

phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất; và

xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ hai theo chính sách bảo mật mặt phẳng người dùng của phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

18. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 15, trong đó bước xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ hai dựa vào mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm các bước:

gửi, bởi phần tử mạng quản lý phiên, yêu cầu thu thông tin thuê bao thứ hai đến phần tử mạng quản lý dữ liệu hợp nhất, trong đó yêu cầu thu thông tin thuê bao thứ hai bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba;

nhận, bởi phần tử mạng quản lý phiên, phản hồi thu thông tin thuê bao thứ hai từ phần tử mạng quản lý dữ liệu hợp nhất, trong đó phản hồi thu thông tin thuê bao thứ hai bao gồm chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ ba đăng ký; và

xác định, bởi phần tử mạng quản lý phiên, chính sách bảo mật mặt phẳng người dùng thứ hai theo chính sách bảo mật mặt phẳng người dùng mà thiết bị đầu cuối thứ ba đăng ký.

19. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 18, trong đó chính sách bảo mật mặt phẳng người dùng thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn của phiên được ưu tiên, và bước xác định, bởi phần tử mạng quản lý phiên, thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên theo chính sách bảo mật mặt phẳng người dùng thứ hai bao gồm bước:

sau khi xác định rằng tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn của thiết bị đầu cuối thứ nhất nhỏ hơn tốc độ dữ liệu được yêu cầu bởi phiên, thì xác định, bởi phần tử mạng quản lý phiên, rằng việc bảo vệ tính toàn vẹn của phiên trong thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai là không cần thiết.

20. Phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, phương pháp này bao gồm các bước:

gửi (302) yêu cầu thứ hai đến phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thứ hai yêu cầu tạo ra phiên kiểu chuyển tiếp, yêu cầu thứ hai bao gồm thông

tin thứ hai, và thông tin thứ hai này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp; và

nhận thông tin chỉ báo thứ nhất từ thiết bị mạng truy cập, trong đó thông tin chỉ báo thứ nhất biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập, trong đó thiết bị đầu cuối thứ nhất là thiết bị chuyển tiếp và trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất biểu thị rằng việc bảo vệ tính toàn vẹn và bảo vệ mã hóa giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập được kích hoạt hoặc vô hiệu hóa.

21. Phương pháp theo điểm 20, trong đó trước khi gửi (302) yêu cầu thứ hai đến phần tử mạng quản lý truy cập và di động, phương pháp này còn bao gồm bước:

nhận (301) yêu cầu truyền thông trực tiếp thứ nhất được gửi bởi thiết bị đầu cuối thứ hai, trong đó yêu cầu truyền thông trực tiếp thứ nhất này là để thiết lập truyền thông với thiết bị đầu cuối thứ nhất.

22. Phương pháp theo điểm 20 hoặc điểm 21, trong đó yêu cầu thứ hai bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ hai; hoặc yêu cầu thứ hai bao gồm thông tin thứ hai và vùng chứa N1 SM.

23. Phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 22, trong đó phiên là để truyền dữ liệu của thiết bị đầu cuối thứ hai, và thông tin thứ hai bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ hai.

24. Phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 23, trong đó phương pháp này bao gồm các bước:

nhận yêu cầu truyền thông trực tiếp thứ hai được gửi bởi thiết bị đầu cuối thứ ba, trong đó yêu cầu truyền thông trực tiếp thứ hai này là để thiết lập truyền thông với thiết bị đầu cuối thứ nhất;

xác định, dựa vào yêu cầu truyền thông trực tiếp thứ hai, rằng thiết bị đầu cuối thứ ba là để sử dụng phiên; và

gửi yêu cầu thứ ba đến phần tử mạng quản lý truy cập và di động, trong đó yêu cầu thứ ba biểu thị rằng thiết bị đầu cuối thứ ba là để sử dụng phiên, và yêu cầu thứ ba bao gồm mã nhận dạng của thiết bị đầu cuối thứ ba.

25. Phương pháp theo điểm 24, trong đó mã nhận dạng của thiết bị đầu cuối thứ ba bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ ba, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ ba hoặc mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ ba.

26. Phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 25, trong đó sau khi nhận thông tin chỉ báo thứ nhất từ thiết bị mạng truy cập, phương pháp này còn bao gồm bước:

xác định trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất.

27. Phương pháp theo điểm 26, trong đó việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất được yêu cầu, và bước xác định trạng thái kích hoạt bảo mật giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất bao gồm bước:

xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển Qos của thiết bị đầu cuối thứ hai, xem có kích hoạt việc bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai hay không.

28. Phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 27, trong đó việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất là không cần thiết, và phương pháp này còn bao gồm bước:

gửi thông điệp từ chối truyền thông trực tiếp đến thiết bị đầu cuối thứ hai khi xác định rằng chính sách bảo mật mặt phẳng người dùng của thiết bị đầu cuối thứ hai biểu thị rằng việc bảo vệ tính toàn vẹn được yêu cầu.

29. Phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 28, trong đó phương pháp này còn bao gồm các bước:

nhận thông tin chỉ báo thứ hai được gửi bởi thiết bị mạng truy cập, trong đó thông tin chỉ báo thứ hai này biểu thị trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai của phiên giữa thiết bị đầu cuối thứ nhất và thiết bị mạng truy cập; và

cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ nhất thành trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai dựa vào thông tin chỉ báo thứ hai.

30. Phương pháp theo điểm 29, trong đó sau khi nhận thông tin chỉ báo thứ hai được gửi bởi thiết bị mạng truy cập, phương pháp này còn bao gồm bước:

cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai.

31. Phương pháp theo điểm 29 hoặc điểm 30, trong đó việc bảo vệ tính toàn vẹn ở trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai được yêu cầu, và bước cập nhật trạng thái kích hoạt bảo mật mặt phẳng người dùng giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai dựa vào trạng thái kích hoạt bảo mật mặt phẳng người dùng thứ hai bao gồm bước:

xác định, dựa vào tốc độ dữ liệu tối đa bảo vệ tính toàn vẹn hoặc thông tin điều khiển chất lượng dịch vụ (quality of service, QoS) của thiết bị đầu cuối thứ ba, xem có kích hoạt việc bảo vệ tính toàn vẹn giữa thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai hay không.

32. Phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, phương pháp này bao gồm các bước:

nhận (302), bởi phần tử mạng quản lý truy cập và di động, yêu cầu thứ hai được gửi bởi thiết bị đầu cuối thứ nhất, trong đó thiết bị đầu cuối thứ nhất là thiết bị chuyển tiếp, yêu cầu thứ hai bao gồm thông tin thứ hai, yêu cầu thứ hai này yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất, và thông tin thứ hai biểu thị rằng kiểu của phiên là kiểu chuyển tiếp; và

gửi (304), bởi phần tử mạng quản lý truy cập và di động, yêu cầu thứ nhất đến phần tử mạng quản lý phiên dựa vào yêu cầu thứ hai, trong đó yêu cầu thứ nhất bao gồm thông tin thứ nhất, thông tin thứ nhất này biểu thị rằng kiểu của phiên là kiểu chuyển tiếp, và yêu cầu thứ nhất yêu cầu tạo ra phiên kiểu chuyển tiếp của thiết bị đầu cuối thứ nhất.

33. Phương pháp theo điểm 32, trong đó thông tin thứ hai giống với thông tin thứ nhất, mỗi trong số yêu cầu thứ nhất và yêu cầu thứ hai bao gồm vùng chứa N1 SM, và vùng chứa N1 SM này bao gồm thông tin thứ hai.

34. Phương pháp theo điểm 32, trong đó yêu cầu thứ hai bao gồm thông tin thứ hai và vùng chứa N1 SM, và yêu cầu thứ nhất bao gồm thông tin thứ nhất và vùng chứa N1 SM.

35. Phương pháp theo điểm bất kỳ trong số các điểm từ 32 đến 34, trong đó bước gửi (304), bởi phần tử mạng quản lý truy cập và di động, yêu cầu thứ nhất đến phần tử mạng

quản lý phiên dựa vào thông tin thứ hai bao gồm bước:

gửi, bởi phần tử mạng quản lý truy cập và di động, yêu cầu thứ nhất đến phần tử mạng quản lý phiên sau khi xác định, dựa vào thông tin thứ hai, rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên.

36. Phương pháp theo điểm bất kỳ trong số các điểm từ 32 đến 35, trong đó thông tin thứ hai bao gồm một hoặc nhiều mã nhận dạng trong số sau:

mã nhận dạng tạm thời của thiết bị đầu cuối thứ hai, mã nhận dạng ẩn danh của thiết bị đầu cuối thứ hai và mã nhận dạng cố định thuê bao (SUPI) của thiết bị đầu cuối thứ hai.

37. Phương pháp theo điểm bất kỳ trong số các điểm từ 32 đến 36, trong đó trước khi gửi (304), bởi phần tử mạng quản lý truy cập và di động, yêu cầu thứ nhất đến phần tử mạng quản lý phiên dựa vào yêu cầu thứ hai, phương pháp này còn bao gồm bước:

xác định, bởi phần tử mạng quản lý truy cập và di động dựa vào thông tin thứ hai, rằng thiết bị đầu cuối thứ nhất được ủy quyền để thiết lập phiên cho thiết bị đầu cuối thứ hai.

38. Thiết bị truyền thông, bao gồm phương tiện để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 19 (1200, 1300).

39. Thiết bị truyền thông, bao gồm phương tiện để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 31 (1200, 1300).

40. Thiết bị truyền thông, bao gồm phương tiện để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 32 đến 37 (1200, 1300).

41. Phương tiện lưu trữ đọc được bằng máy tính, trong đó phương tiện lưu trữ đọc được bằng máy tính này lưu trữ các lệnh; và khi các lệnh chạy trên máy tính, thì máy tính này được cho phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 19.

42. Phương tiện lưu trữ đọc được bằng máy tính, trong đó phương tiện lưu trữ đọc được bằng máy tính này lưu trữ các lệnh; và khi các lệnh chạy trên máy tính, thì máy tính này được cho phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 20 đến 31.

43. Phương tiện lưu trữ đọc được bằng máy tính, trong đó phương tiện lưu trữ đọc được bằng máy tính này lưu trữ các lệnh; và khi các lệnh chạy trên máy tính, thì máy tính này được cho phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 32 đến 37.

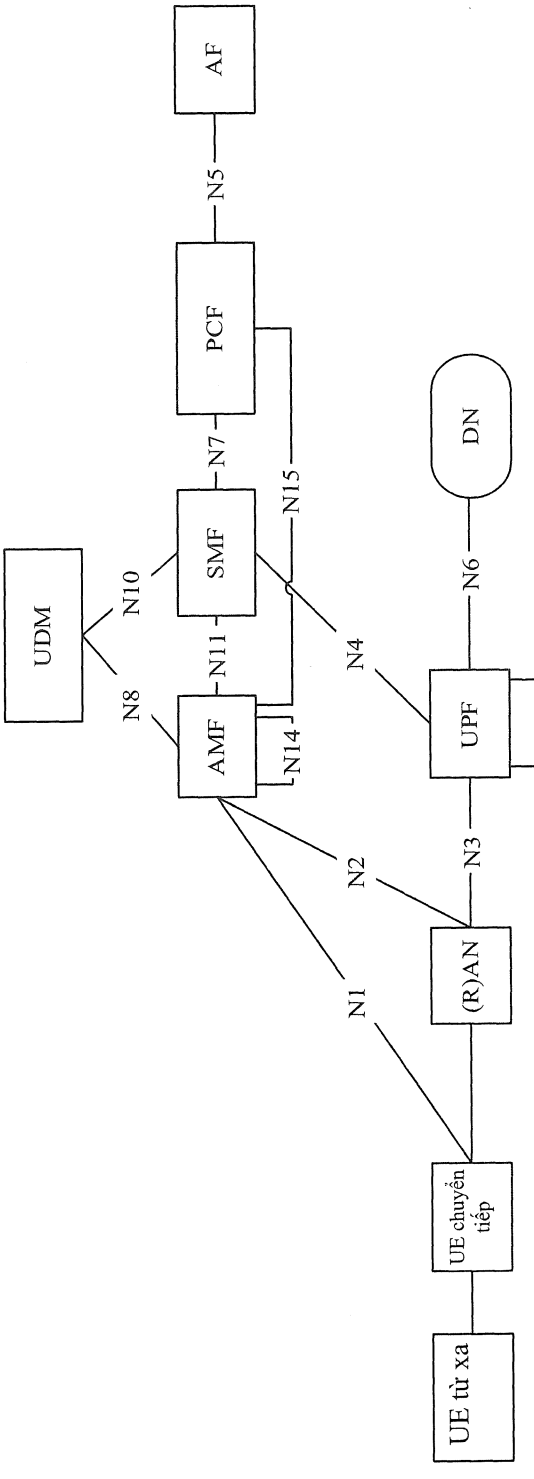
AF
N5
PCF
N7
N15
SMF
N10
UDM
N11
N8
AMF
N14
N4
UPF
N9
DN
N6
N2
N3
(R)AN
N1
UE chuyển tiếp
UE từ xa

FIG. 1

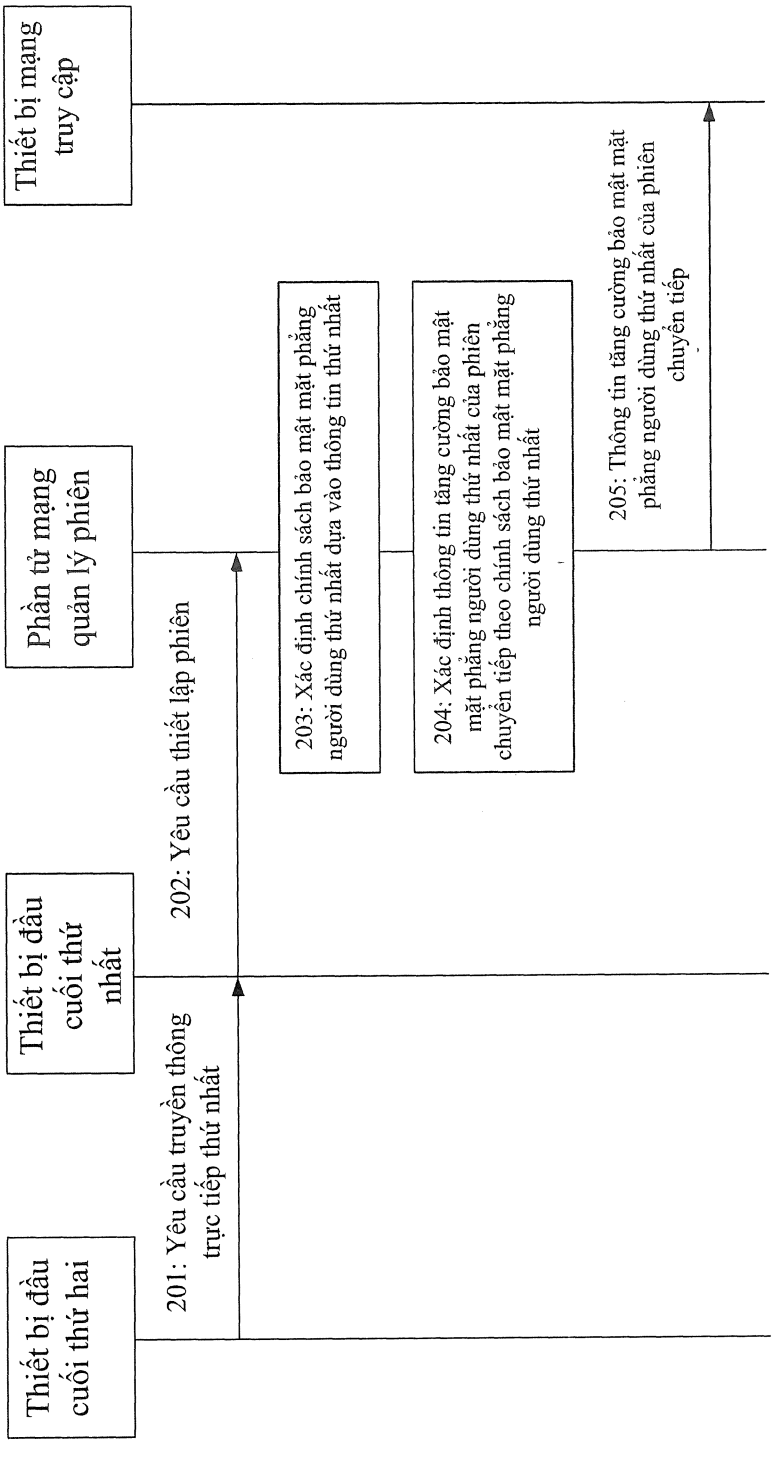
Thiết bị đầu cuối thứ hai
Thiết bị đầu cuối thứ nhất
Phần tử mạng quản lý phiên
Thiết bị mạng truy cập
201: Yêu cầu truyền thông trực tiếp thứ nhất
202: Yêu cầu thiết lập phiên
203: Xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất
204: Xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất
205: Thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp

FIG. 2

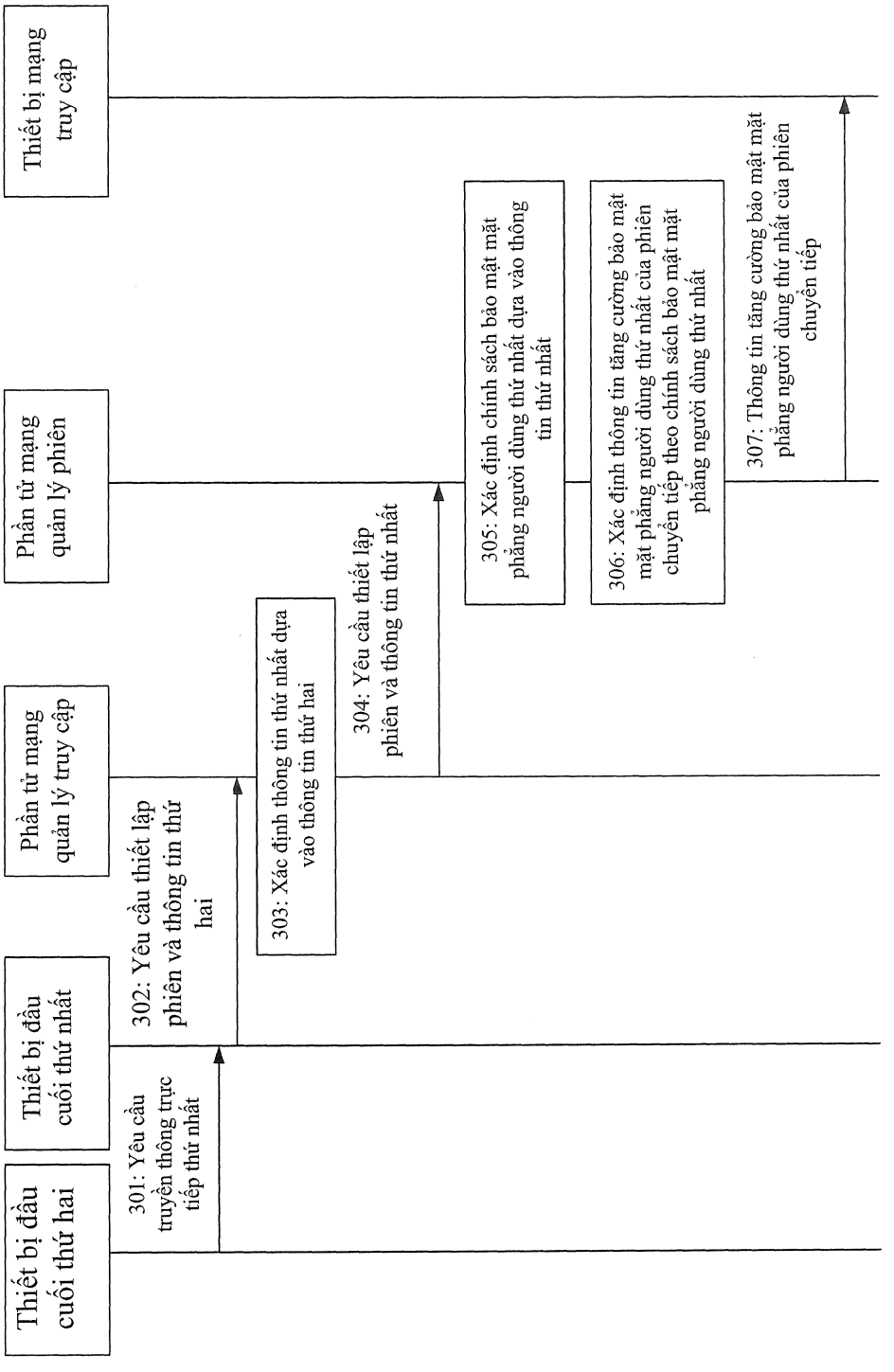
Thiết bị đầu cuối thứ hai
Thiết bị đầu cuối thứ nhất
Phần tử mạng quản lý truy cập
Phần tử mạng quản lý phiên
Thiết bị mạng truy cập
301: Yêu cầu truyền thông trực tiếp thứ nhất
302: Yêu cầu thiết lập phiên và thông tin thứ hai
303: Xác định thông tin thứ nhất dựa vào thông tin thứ hai
304: Yêu cầu thiết lập phiên và thông tin thứ nhất
305: Xác định chính sách bảo mật mặt phẳng người dùng thứ nhất dựa vào thông tin thứ nhất
306: Xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất
307: Thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp

FIG. 3

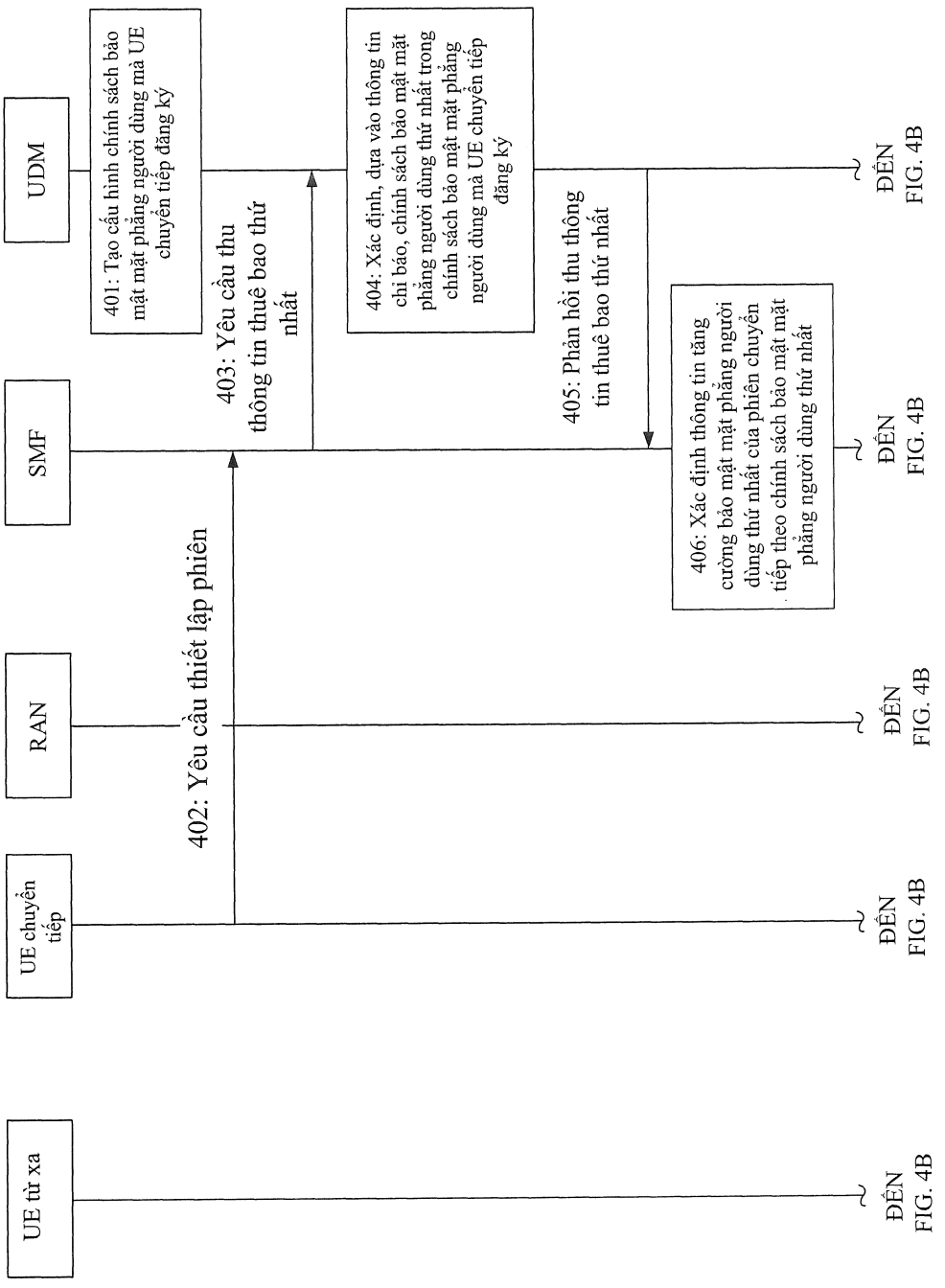
UE từ xa
UE chuyển tiếp
RAN
SMF
UDM
401: Tạo cấu hình chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký
402: Yêu cầu thiết lập phiên
403: Yêu cầu thu thông tin thuê bao thứ nhất
404: Xác định, dựa vào thông tin chỉ báo, chính sách bảo mật mặt phẳng người dùng thứ nhất trong chính sách bảo mật mặt phẳng người dùng mà UE chuyển tiếp đăng ký
405: Phản hồi thu thông tin thuê bao thứ nhất
406: Xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất
ĐẾN FIG. 4B
ĐẾN FIG. 4B
ĐẾN FIG. 4B
ĐẾN FIG. 4B
ĐẾN FIG. 4B

FIG. 4A

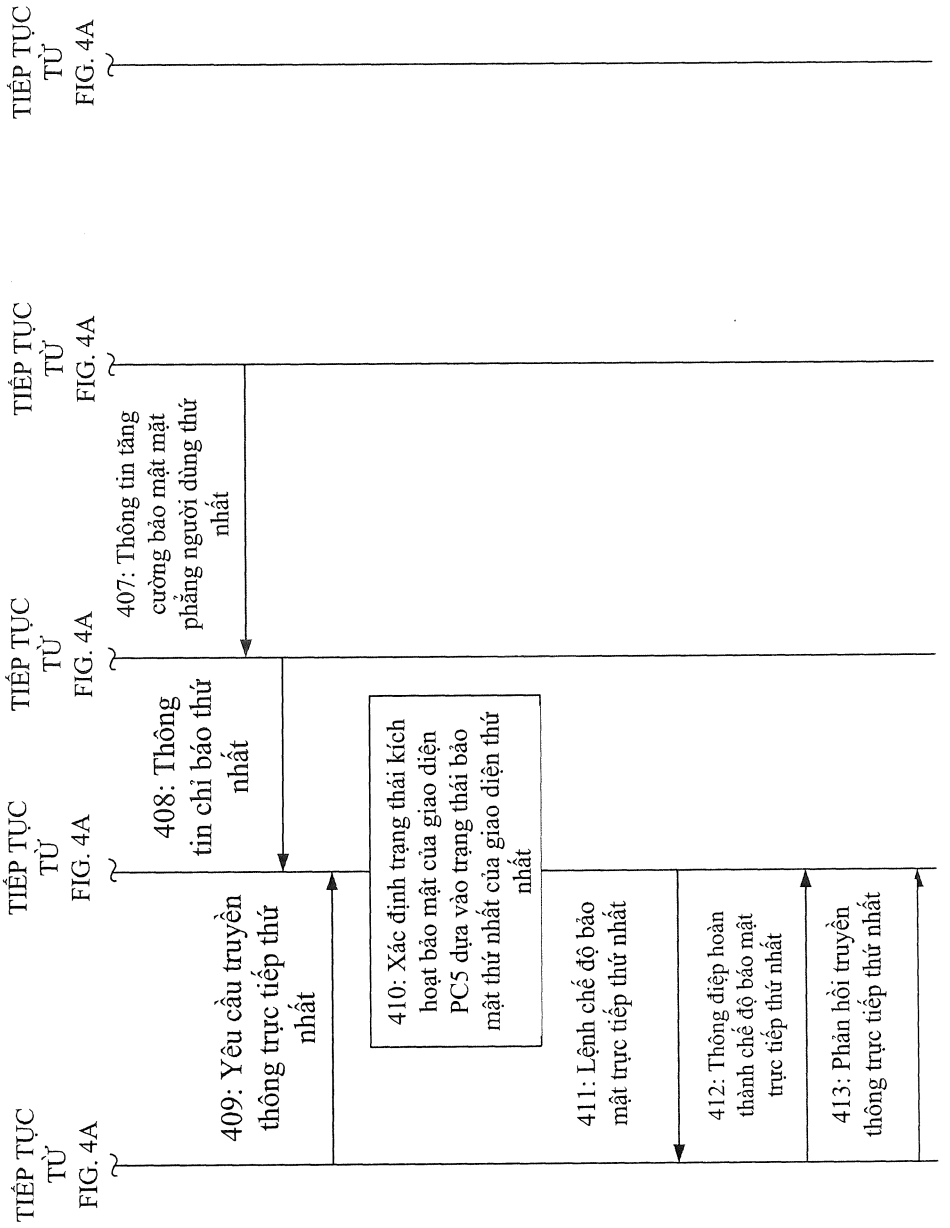
TIẾP TỤC TỪ FIG. 4A
TIẾP TỤC TỪ FIG. 4A
407: Thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất
TIẾP TỤC TỪ FIG. 4A
408: Thông tin chỉ báo thứ nhất
TIẾP TỤC TỪ FIG. 4A
409: Yêu cầu truyền thông trực tiếp thứ nhất
410: Xác định trạng thái kích hoạt bảo mật của giao diện PC5 dựa vào trạng thái bảo mật thứ nhất của giao diện thứ nhất
411: Lệnh chế độ bảo mật trực tiếp thứ nhất
412: Thông điệp hoàn thành chế độ bảo mật trực tiếp thứ nhất
413: Phản hồi truyền thông trực tiếp thứ nhất

FIG. 4B

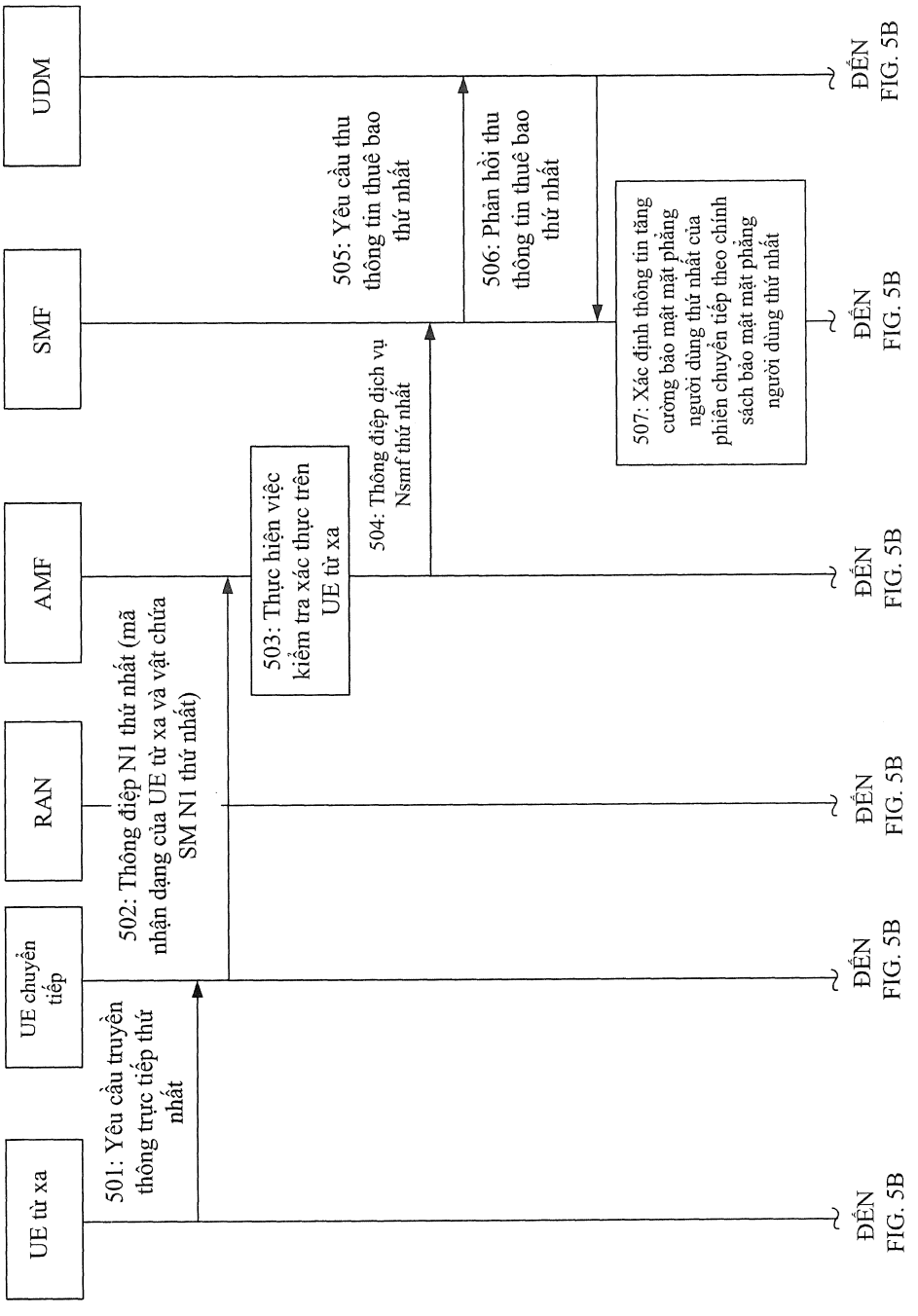
UE từ xa
UE chuyển tiếp
RAN
AMF
SMF
UDM
501: Yêu cầu truyền thông trực tiếp thứ nhất
502: Thông điệp N1 thứ nhất (mã nhận dạng của UE từ xa và vật chứa SM N1 thứ nhất)
503: Thực hiện việc kiểm tra xác thực trên UE từ xa
504: Thông điệp dịch vụ Nsmf thứ nhất
505: Yêu cầu thu thông tin thuê bao thứ nhất
506: Phản hồi thu thông tin thuê bao thứ nhất
507: Xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ nhất
ĐẾN FIG. 5B

FIG. 5A

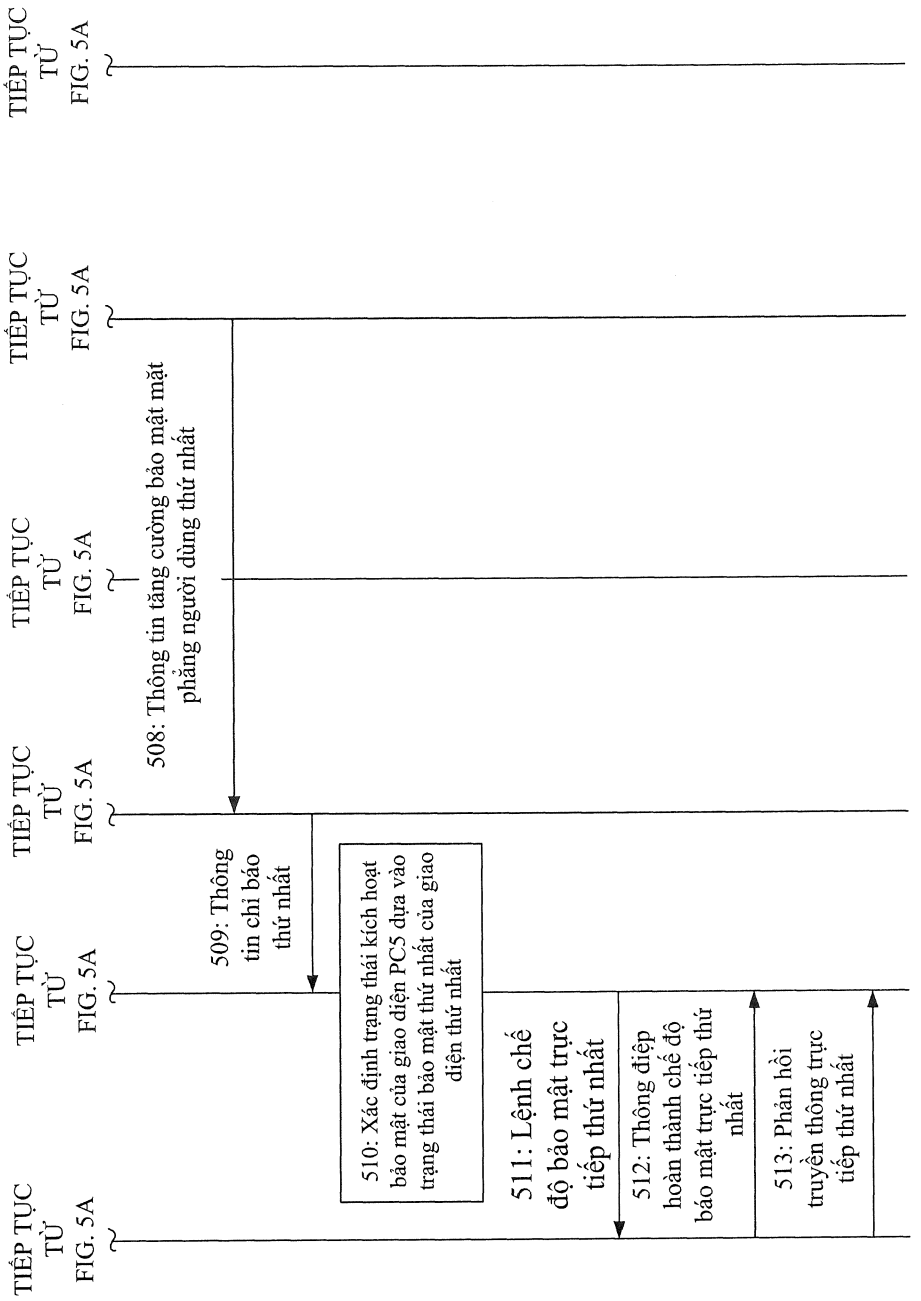
TIẾP TỤC TỪ FIG. 5A
TIẾP TỤC TỪ FIG. 5A
508: Thông tin tăng cường bảo mật mặt phẳng người dùng thứ nhất
TIẾP TỤC TỪ FIG. 5A
TIẾP TỤC TỪ FIG. 5A
509: Thông tin chỉ báo thứ nhất
510: Xác định trạng thái kích hoạt bảo mật của giao diện PC5 dựa vào trạng thái bảo mật thứ nhất của giao diện thứ nhất
511: Lệnh chế độ bảo mật trực tiếp thứ nhất
512: Thông điệp hoàn thành chế độ bảo mật trực tiếp thứ nhất
513: Phản hồi truyền thông trực tiếp thứ nhất
TIẾP TỤC TỪ FIG. 5A

FIG. 5B

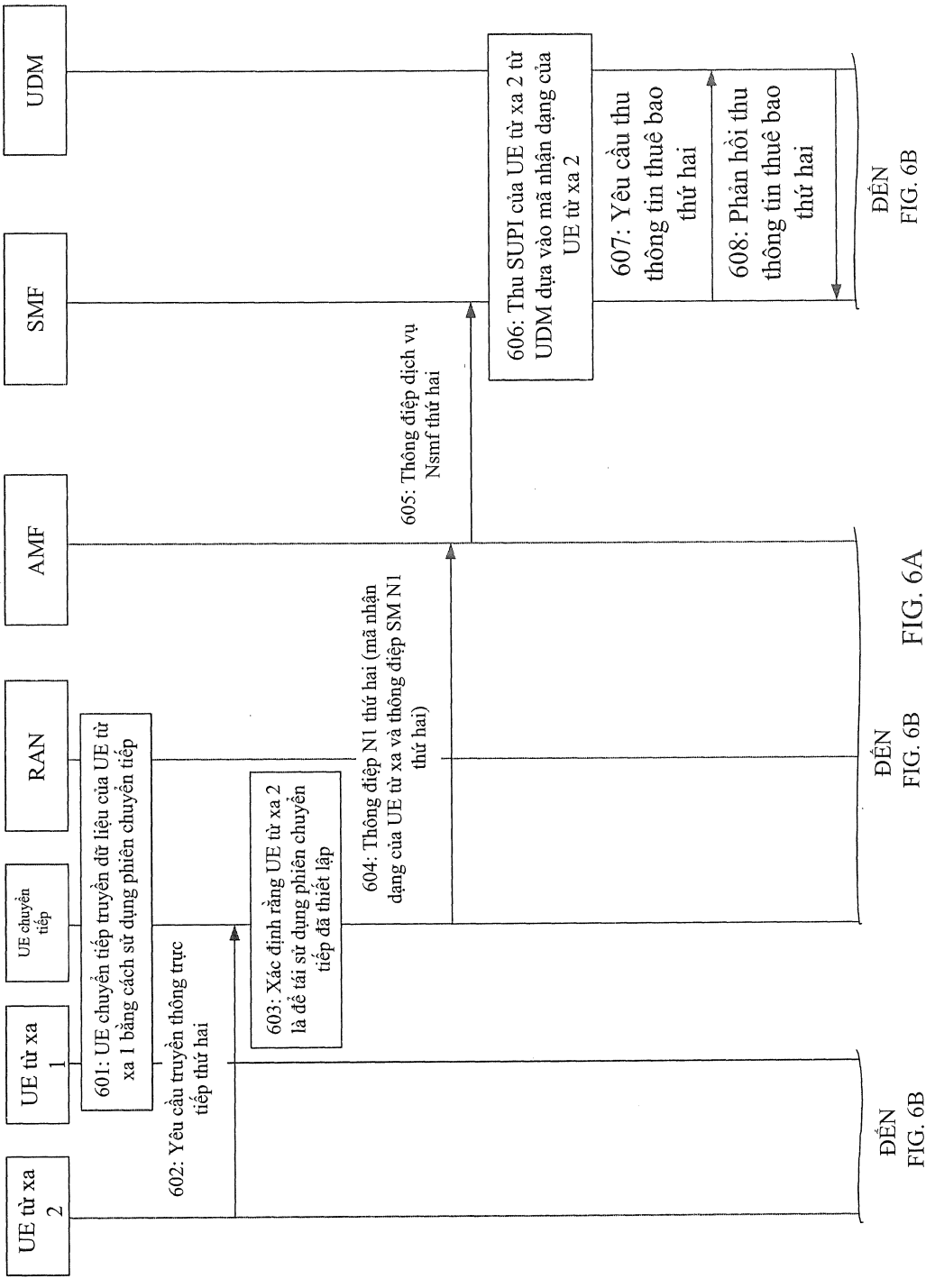
UE từ xa 2
UE từ xa 1
UE chuyển tiếp
RAN
AMF
SMF
UDM
601: UE chuyển tiếp truyền dữ liệu của UE từ xa 1 bằng cách sử dụng phiên chuyển tiếp
602: Yêu cầu truyền thông trực tiếp thứ hai
603: Xác định rằng UE từ xa 2 là để tái sử dụng phiên chuyển tiếp đã thiết lập
604: Thông điệp N1 thứ hai (mã nhận dạng của UE từ xa và thông điệp SM N1 thứ hai)
605: Thông điệp dịch vụ Nsmf thứ hai
606: Thu SUPI của UE từ xa 2 từ UDM dựa vào mã nhận dạng của UE từ xa 2
607: Yêu cầu thu thông tin thuê bao thứ hai
608: Phản hồi thu thông tin thuê bao thứ hai
ĐẾN FIG. 6B
ĐẾN FIG. 6B
ĐẾN FIG. 6B

FIG. 6A

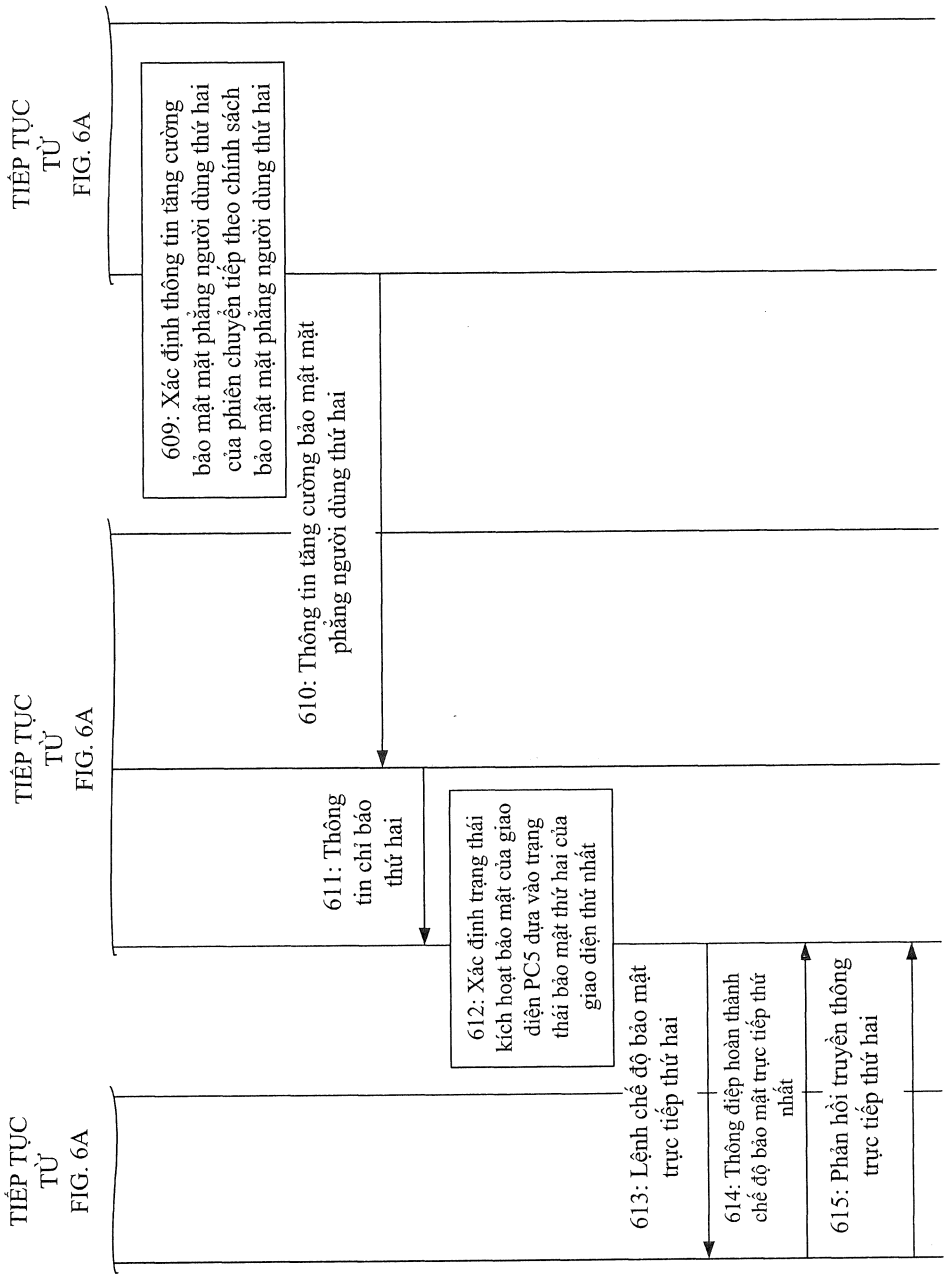
TIẾP TỤC TỪ FIG. 6A
609: Xác định thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai của phiên chuyển tiếp theo chính sách bảo mật mặt phẳng người dùng thứ hai
610: Thông tin tăng cường bảo mật mặt phẳng người dùng thứ hai
TIẾP TỤC TỪ FIG. 6A
611: Thông tin chỉ báo thứ hai
612: Xác định trạng thái kích hoạt bảo mật của giao diện PC5 dựa vào trạng thái bảo mật thứ hai của giao diện thứ nhất
TIẾP TỤC TỪ FIG. 6A
613: Lệnh chế độ bảo mật trực tiếp thứ hai
614: Thông điệp hoàn thành chế độ bảo mật trực tiếp thứ nhất
615: Phản hồi truyền thông trực tiếp thứ hai

FIG. 6B

10/11

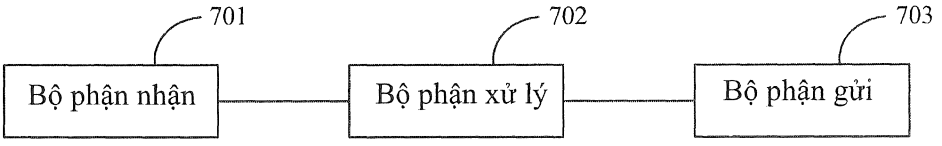

FIG. 7

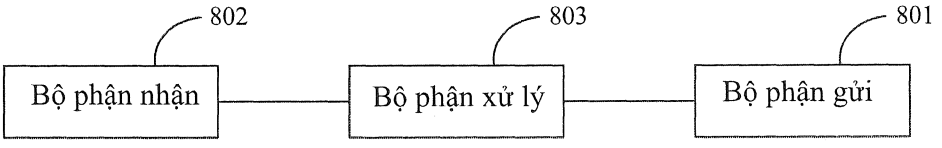

FIG. 8

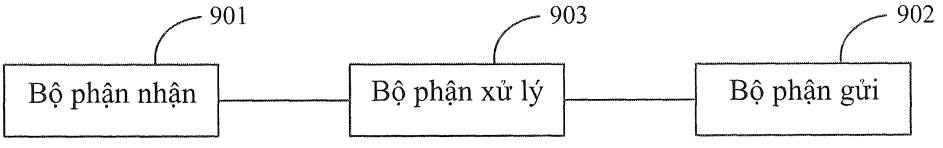

FIG. 9

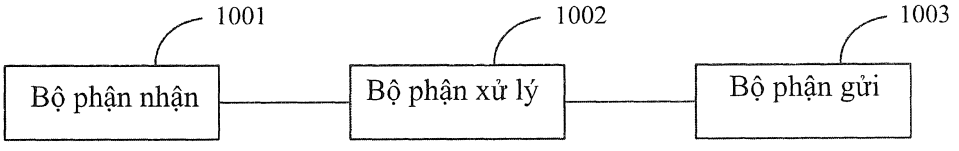

FIG. 10

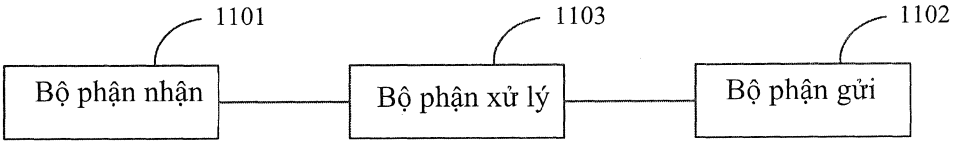

FIG. 11

11/11

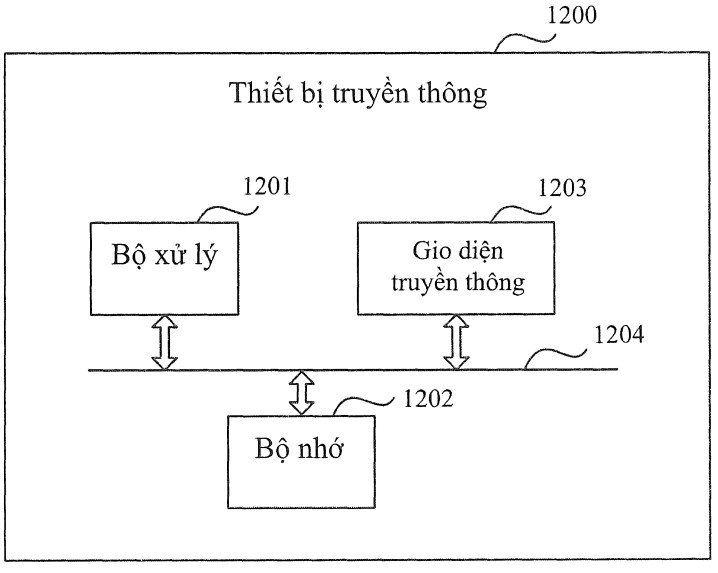

FIG. 12

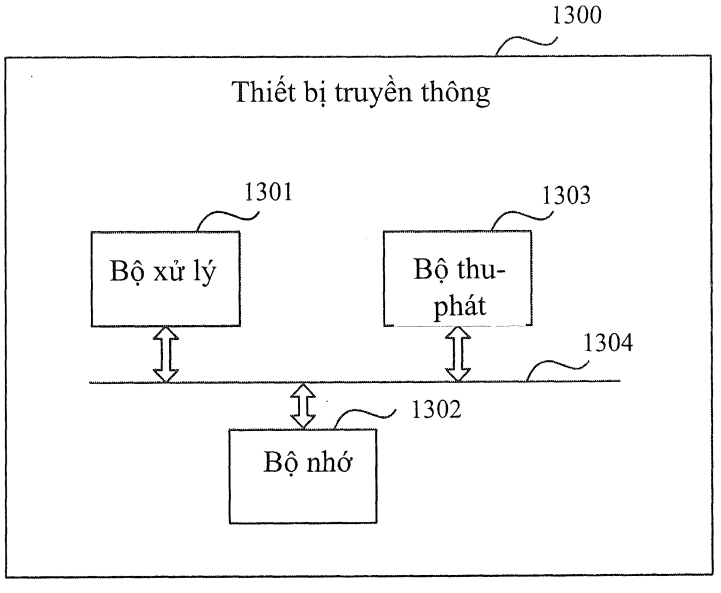

FIG. 13