(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) **1-0036546**

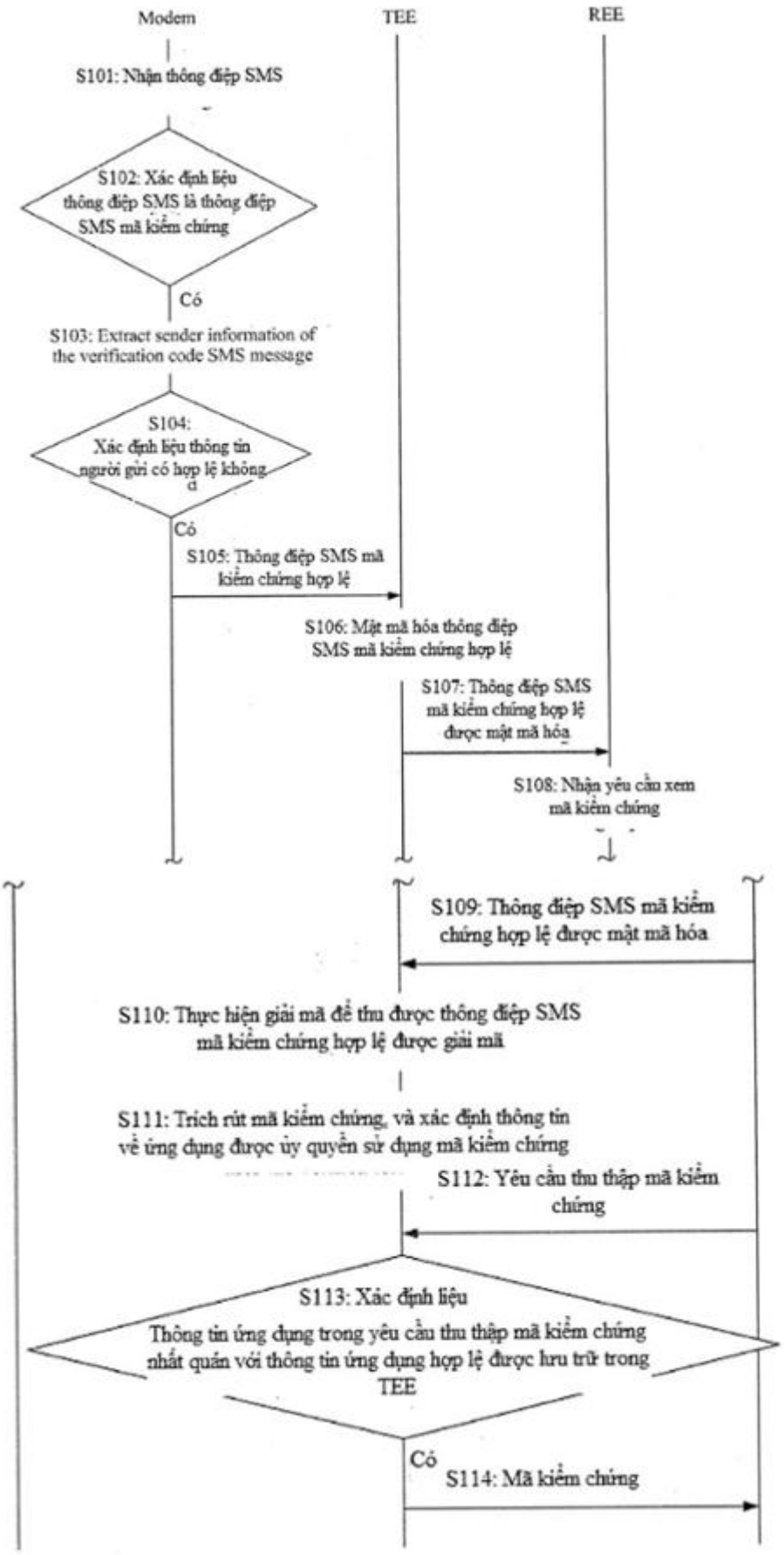
(51)[19] **H04L 29/06**

(13) **B**

(21) 1-2019-02328
(22) 12/10/2016
(86) PCT/CN2016/101899 12/10/2016
(87) WO2018/068228 19/04/2018
(45) 25/08/2023 425
(43) 25/07/2019 376A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building Bantian, Longgang District Shenzhen, Guangdong 518129, China
(72) HUANG, Jiejing (CN); PENG, Feng (CN).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP XỬ LÝ MÃ KIỂM CHỨNG VÀ THIẾT BỊ ĐẦU CUỐI DI ĐỘNG

(57) Sáng chế đề xuất phương pháp xử lý mã kiểm chứng và thiết bị đầu cuối di động. Phương pháp gồm: nhận, bởi môi trường thực thi tin cậy (trusted execution environment - TEE), yêu cầu thu thập mã kiểm chứng được gửi bởi môi trường thực thi phong phú (rich execution environment - REE), trong đó yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng; xác định, bởi TEE, liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và gửi mã kiểm chứng đến REE nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Có thể được biết rằng so với giải pháp kỹ thuật đã biết, sau khi nhận yêu cầu thu thập mã kiểm chứng, thiết bị đầu cuối không gửi trực tiếp mã kiểm chứng, và thay vào đó, gửi mã kiểm chứng đến REE chỉ nếu TEE xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng được gửi bởi REE và về ứng dụng để thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Do vậy, tính bảo mật cao hơn.


Modem
TEE
REE
S101: Nhận thông điệp SMS
S102: Xác định liệu thông điệp SMS là thông điệp SMS mã kiểm chứng
Có
S103: Extract sender information of the verification code SMS message
S104: Xác định liệu thông tin người gửi có hợp lệ không
d
Có
S105: Thông điệp SMS mã kiểm chứng hợp lệ
S106: Mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ
S107: Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa
S108: Nhận yêu cầu xem mã kiểm chứng
S109: Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa
S110: Thực hiện giải mã để thu được thông điệp SMS mã kiểm chứng hợp lệ được giải mã
S111: Trích rút mã kiểm chứng, và xác định thông tin về ứng dụng được ủy quyền sử dụng mã kiểm chứng
S112: Yêu cầu thu thập mã kiểm chứng
S113: Xác định liệu
Thông tin ứng dụng trong yêu cầu thu thập mã kiểm chứng nhất quán với thông tin ứng dụng hợp lệ được lưu trữ trong TEE
Có
S114: Mã kiểm chứng

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông, và cụ thể là, đến phương pháp xử lý mã kiểm chứng và thiết bị đầu cuối di động.

Tình trạng kỹ thuật của sáng chế

Với sự phổ biến của các thiết bị đầu cuối di động và sự phong phú của các chức năng của các thiết bị đầu cuối di động, các thiết bị đầu cuối di động ngày càng mở rộng. Một cách tương ứng, các vấn đề bảo mật thông tin của các thiết bị đầu cuối di động thu hút nhiều sự chú ý hơn. Chẳng hạn, cách thức hiện tại gửi mã kiểm chứng đến thiết bị đầu cuối di động để kiểm chứng sự cho phép của người dùng được áp dụng rộng rãi cho các kịch bản thanh toán di động và đăng nhập.

Tuy nhiên, theo giải pháp kỹ thuật đã biết, trong quá trình sử dụng mã kiểm chứng, hệ thống sao chép mã kiểm chứng, và sau đó gửi mã kiểm chứng mà không có xác định bất kỳ bất kể loại yêu cầu thu thập mã kiểm chứng nhận được (chẳng hạn, yêu cầu dán mã kiểm chứng). Trong trường hợp này, mã kiểm chứng về cơ bản là thông tin nhạy cảm có thể được gửi ngẫu nhiên, và mã kiểm chứng là không bảo mật. Kết quả là, mức độ bảo mật theo cách thức gửi mã kiểm chứng ngẫu nhiên theo giải pháp kỹ thuật đã biết là thấp.

Bản chất kỹ thuật của sáng chế

Do vậy, sáng chế đề xuất phương pháp xử lý mã kiểm chứng và thiết bị đầu cuối di động, để giải quyết vấn đề theo giải pháp kỹ thuật đã biết là bảo mật của cách thức gửi mã kiểm chứng ngẫu nhiên là thấp.

Để đạt được mục đích nêu trên, sáng chế đề xuất các giải pháp kỹ thuật sau.

Khía cạnh thứ nhất của sáng chế đề xuất phương pháp xử lý mã kiểm chứng, và phương pháp gồm các bước sau:

nhận, bởi môi trường thực thi tin cậy (trusted execution environment – TEE), yêu cầu thu thập mã kiểm chứng được gửi bởi môi trường thực thi phong phú (rich execution environment – REE), trong đó yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng; xác định, bởi TEE, liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và gửi mã kiểm chứng đến REE nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Có thể được biết rằng so với giải pháp kỹ thuật đã biết, sau khi nhận yêu cầu thu thập mã kiểm chứng, thiết bị đầu cuối không gửi trực tiếp mã kiểm chứng, và thay vào đó, gửi mã kiểm chứng đến REE chỉ nếu TEE xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng được gửi bởi REE và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Do vậy, bảo mật là cao hơn.

Theo triển khai, sau khi nhận, bởi TEE, yêu cầu thu thập mã kiểm chứng được gửi bởi REE, phương pháp còn gồm: nhận, bởi TEE, thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; và trích rút, bởi TEE, mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ. Modem là hệ thống cơ bản cho thiết bị đầu cuối để truyền thông với thiết bị khác. Thông điệp SMS mã kiểm chứng hợp lệ trước hết được xác định bằng cách sử dụng hệ thống cơ bản ở thiết bị đầu cuối, và sau đó được gửi đến TEE để xử lý. Do vậy, có thể được đảm bảo rằng thông điệp SMS mã kiểm chứng được nhận diện ngay lập tức, nhờ đó nhanh chóng nhập vào

thủ tục xử lý mã kiểm chứng.

Theo triển khai, quá trình thu thập mã kiểm chứng gồm: nhận, bởi TEE, thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; mật mã hóa và lưu trữ, bởi TEE, thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa gồm mã kiểm chứng được hiển thị ở dạng văn bản mật mã; thu thập, bởi TEE, chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó chỉ mục lưu trữ ghi nhận vị trí lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ; gửi, bởi TEE, chỉ mục lưu trữ đến REE; thu thập, bởi REE, thông điệp SMS mã kiểm chứng được mật mã hóa theo chỉ mục lưu trữ, và thêm thông điệp SMS mã kiểm chứng được mật mã hóa đến yêu cầu thu thập mã kiểm chứng; trích rút, bởi TEE, thông điệp SMS mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và giải mật mã, bởi TEE, thông điệp SMS mã kiểm chứng được mật mã hóa, và trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng được giải mật mã. TEE có thể bỏ chạy sau khi lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa và gửi chỉ mục lưu trữ đến REE, và có thể bắt đầu lại việc chạy sau khi nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE. Do vậy, thời gian chạy của TEE được giảm, và tiêu thụ tài nguyên trong khi chạy được giảm. Ngoài ra, so với REE, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa trong TEE, và sau đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được giải mã trong TEE. Do vậy, bảo mật là cao hơn.

Theo triển khai, trước khi nhận, bởi TEE, thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem, phương pháp còn gồm: nhận, bởi modem, thông điệp SMS mã kiểm chứng; trích rút, bởi modem, thông tin người gửi của thông điệp SMS mã kiểm chứng; xác định, bởi modem,

liệu thông tin người gửi là thông tin người gửi được ủy quyền; và nếu thông tin người gửi là thông tin người gửi được ủy quyền, xác định, bởi modem, rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ. Trước khi gửi thông điệp SMS mã kiểm chứng đến TEE, modem trước hết kiểm chứng liệu người gửi của thông điệp SMS mã kiểm chứng được ủy quyền, để còn cải thiện bảo mật.

Theo triển khai, việc xác định, bởi modem, liệu thông tin người gửi là thông tin người gửi được ủy quyền gồm: xác định, bởi modem, liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng. Do vậy, bảo mật của thông điệp SMS mã kiểm chứng được gửi đến TEE được đảm bảo.

Theo triển khai, việc xác định, bởi modem, liệu thông tin người gửi là thông tin người gửi được ủy quyền gồm: xác định, bởi modem, liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng. Do vậy, bảo mật của thông điệp SMS mã kiểm chứng được gửi đến TEE được đảm bảo.

Theo triển khai, trước khi trích rút, bởi TEE, mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ, phương pháp còn gồm: mật mã hóa, bởi TEE, thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ gồm văn bản mật mã hóa của mã kiểm chứng; lưu trữ, bởi TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE; sau khi REE tiếp nhận

yêu cầu xem mã kiểm chứng, gửi, bởi REE đến TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được lưu trữ trong không gian lưu trữ của REE; và giải mật mã, bởi TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, để thu thập thông điệp SMS mã kiểm chứng hợp lệ được giải mã. TEE có thể bỏ chạy sau khi lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ của REE, và có thể khởi động lại việc chạy sau khi nhận thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được gửi bởi REE. Do vậy, thời gian chạy của TEE được giảm, và tiêu thụ tài nguyên trong khi chạy được giảm. Ngoài ra, so với REE, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa trong TEE, và sau đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được giải mã trong TEE. Do vậy, bảo mật là cao hơn. Ngoài ra, TEE lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE, để tiết kiệm không gian lưu trữ của REE.

Theo triển khai, trước khi trích rút, bởi TEE, mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ, phương pháp còn gồm: lưu trữ, bởi TEE, thông điệp SMS mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE. TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Do vậy, thông điệp SMS mã kiểm chứng hợp lệ được lưu trữ trong không gian lưu trữ của TEE. Do vậy, bảo mật là cao hơn.

Theo triển khai, danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; và trước khi xác định, bởi TEE, liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, phương pháp còn gồm: xác định, bởi modem từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng

được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; và gửi thông tin về ứng dụng được ủy quyền đến TEE. TEE kiểm chứng, theo thông tin về ứng dụng được ủy quyền, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền. Do vậy, bảo mật là cao hơn.

Theo triển khai, trước khi xác định, bởi TEE, liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, phương pháp còn gồm: trích rút, bởi TEE, trường PDU của thông điệp SMS mã kiểm chứng hợp lệ; và xác định, bởi TEE từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Do vậy, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền được kiểm chứng theo thông tin về ứng dụng được ủy quyền. Do vậy, bảo mật là cao hơn.

Theo triển khai, trước khi xác định, bởi TEE, liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, phương pháp còn gồm: trích rút, bởi TEE, thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và xác định, bởi TEE theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ. Do vậy, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền được kiểm chứng theo thông tin về ứng dụng được ủy quyền. Do vậy, bảo mật là cao hơn.

Khía cạnh thứ hai của sáng chế đề xuất thiết bị đầu cuối di động, gồm:

môđun yêu cầu thu thập mã kiểm chứng nhận, được tạo cấu hình để nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE, trong đó yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng; môđun xác định thông tin, được tạo cấu hình để xác định liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và môđun gửi mã kiểm chứng, được tạo cấu hình để gửi mã kiểm chứng đến REE nếu môđun xác định thông tin xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Có thể được biết rằng so với giải pháp kỹ thuật đã biết, sau khi nhận yêu cầu thu thập mã kiểm chứng, thiết bị đầu cuối không gửi trực tiếp mã kiểm chứng, và thay vào đó, gửi mã kiểm chứng đến REE chỉ nếu TEE xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng được gửi bởi REE và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Do vậy, bảo mật là cao hơn.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun thu thập mã kiểm chứng thứ nhất, được tạo cấu hình để thu thập mã kiểm chứng, trong đó môđun thu thập mã kiểm chứng thứ nhất gồm: mô đun nhận thông điệp SMS mã kiểm chứng hợp lệ thứ nhất, được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; và môđun trích rút mã kiểm chứng, được tạo cấu hình để trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ. Modem là hệ thống cơ bản cho thiết bị đầu cuối để truyền thông với thiết bị khác. Thông điệp

SMS mã kiểm chứng hợp lệ trước hết được xác định bằng cách sử dụng hệ thống cơ bản ở thiết bị đầu cuối, và sau đó được gửi đến TEE để xử lý. Do vậy, có thể được đảm bảo rằng thông điệp SMS mã kiểm chứng được nhận diện ngay lập tức, nhờ đó nhanh chóng nhập vào thủ tục xử lý mã kiểm chứng.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun thu thập mã kiểm chứng thứ hai, được tạo cấu hình để thu thập mã kiểm chứng, trong đó môđun thu thập mã kiểm chứng thứ hai gồm: môđun nhận thông điệp SMS mã kiểm chứng hợp lệ thứ hai, được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; môđun lưu trữ và mật mã hóa, được tạo cấu hình để mật mã hóa và lưu trữ thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa gồm mã kiểm chứng được hiển thị ở dạng văn bản mật mã; môđun thu thập chỉ mục lưu trữ, được tạo cấu hình để thu thập chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó chỉ mục lưu trữ ghi nhận vị trí lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ; môđun gửi chỉ mục lưu trữ, được tạo cấu hình để gửi chỉ mục lưu trữ đến REE; môđun thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa theo chỉ mục lưu trữ; môđun thêm thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để thêm thông điệp SMS mã kiểm chứng được mật mã hóa vào yêu cầu thu thập mã kiểm chứng; môđun trích rút thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để trích rút thông điệp SMS mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và môđun giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa, để trích rút mã kiểm chứng

từ thông điệp SMS mã kiểm chứng được giải mật mã. TEE có thể bỏ chạy sau khi lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa và gửi chỉ mục lưu trữ đến REE, và có thể khởi động lại việc chạy sau khi nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE. Do vậy, thời gian chạy của TEE được giảm, và tiêu thụ tài nguyên trong khi chạy được giảm. Ngoài ra, so với REE, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa trong TEE, và sau đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được giải mã trong TEE. Do vậy, bảo mật là cao hơn.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun nhận thông điệp SMS mã kiểm chứng, được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng; môđun trích rút thông tin người gửi, được tạo cấu hình để trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng; môđun xác định thông tin người gửi, được tạo cấu hình để xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền; và môđun xác định thông điệp SMS mã kiểm chứng hợp lệ, được tạo cấu hình để: nếu môđun xác định thông tin người gửi xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, xác định rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ. Trước khi thông điệp SMS mã kiểm chứng được gửi đến TEE, liệu người gửi của thông điệp SMS mã kiểm chứng được ủy quyền trước hết được kiểm chứng, để còn cải thiện bảo mật.

Theo triển khai, môđun xác định thông tin người gửi gồm: môđun phụ xác định thông tin người gửi thứ nhất, được tạo cấu hình để xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng; và môđun xác định thông tin người gửi được ủy quyền thứ nhất, được tạo cấu hình để: nếu môđun phụ xác định thông tin người gửi thứ nhất xác định rằng thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng

gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng. Do vậy, bảo mật của thông điệp SMS mã kiểm chứng được gửi đến TEE được đảm bảo.

Theo triển khai, môđun xác định thông tin người gửi gồm: môđun phụ xác định thông tin người gửi thứ hai, được tạo cấu hình để xác định liệu thông tin người gửi được lưu trữ trong danh sách đen; và môđun xác định thông tin người gửi được ủy quyền xác định thứ hai, được tạo cấu hình để: nếu môđun phụ xác định thông tin người gửi thứ hai xác định rằng thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng. Do vậy, bảo mật của thông điệp SMS mã kiểm chứng được gửi đến TEE được đảm bảo.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun mật mã thứ nhất, được tạo cấu hình để mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ gồm văn bản mật mã hóa của mã kiểm chứng; môđun lưu trữ thứ nhất, được tạo cấu hình để lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE; môđun gửi thứ nhất, được tạo cấu hình để: sau khi yêu cầu xem mã kiểm chứng được nhận, gửi, đến TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được lưu trữ trong không gian lưu trữ của REE; và môđun giải mật mã thứ nhất, được tạo cấu hình để giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, để thu thập thông điệp SMS mã kiểm chứng hợp lệ được giải mã. TEE có thể bỏ chạy sau khi lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ của REE, và có thể khởi động lại việc chạy sau khi nhận thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được gửi bởi REE. Do vậy, thời gian

chạy của TEE được giảm, và tiêu thụ tài nguyên trong khi chạy được giảm. Ngoài ra, so với REE, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa trong TEE, và sau đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được giải mã trong TEE. Do vậy, bảo mật là cao hơn. Ngoài ra, TEE lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE, để tiết kiệm không gian lưu trữ của REE.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun lưu trữ thứ hai, được tạo cấu hình để lưu trữ thông điệp SMS mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE. TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Do vậy, thông điệp SMS mã kiểm chứng hợp lệ được lưu trữ trong không gian lưu trữ của TEE. Do vậy, bảo mật là cao hơn.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun xác định thông tin thứ nhất, được tạo cấu hình để xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ, trong đó danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; và môđun gửi thông tin thứ nhất, được tạo cấu hình để gửi thông tin về ứng dụng được ủy quyền đến TEE. TEE kiểm chứng, theo thông tin về ứng dụng được ủy quyền, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền. Do vậy, bảo mật là cao hơn.

Theo triển khai, thiết bị đầu cuối di động còn gồm: môđun trích rút trường PDU, được tạo cấu hình để trích rút trường PDU của thông điệp SMS mã kiểm chứng hợp lệ; và môđun xác định thông tin thứ hai, được tạo cấu hình để xác định, từ trường PDU, thông tin về ứng dụng được ủy

quyền mà sử dụng mã kiểm chứng. Do vậy, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền được kiểm chứng theo thông tin về ứng dụng được ủy quyền. Do vậy, bảo mật là cao hơn.

Theo triển khai, thiết bị đầu cuối di động còn gồm:

môđun trích rút thông tin người gửi được ủy quyền, được tạo cấu hình để trích rút thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và môđun xác định thông tin thứ ba, được tạo cấu hình để xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ. Do vậy, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền được kiểm chứng theo thông tin về ứng dụng được ủy quyền. Do vậy, bảo mật là cao hơn.

Khía cạnh thứ ba của sáng chế đề xuất thiết bị đầu cuối di động, gồm thành phần truyền thông, bộ nhớ, và bộ xử lý, trong đó bộ nhớ được tạo cấu hình để: lưu trữ mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, và lưu trữ chương trình ứng dụng và dữ liệu được tạo trong quá trình chạy chương trình ứng dụng; thành phần truyền thông được tạo cấu hình để: nhận yêu cầu thu thập mã kiểm chứng that mang ít nhất thông tin về ứng dụng để thu thập mã kiểm chứng, và gửi mã kiểm chứng nếu bộ xử lý xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và bộ xử lý được tạo cấu hình để xác định liệu thông tin được mang trong

yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Có thể được biết rằng so với giải pháp kỹ thuật đã biết, sau khi nhận yêu cầu thu thập mã kiểm chứng, thành phần truyền thông của thiết bị đầu cuối di động không gửi trực tiếp mã kiểm chứng, và thay vào đó, thành phần truyền thông gửi mã kiểm chứng đến REE sau khi bộ xử lý xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng được gửi bởi REE và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Do vậy, bảo mật là cao hơn.

Theo triển khai, thành phần truyền thông được tạo cấu hình cụ thể để: nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem, và trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ. Modem là hệ thống cơ bản cho thiết bị đầu cuối để truyền thông với thiết bị khác. Thông điệp SMS mã kiểm chứng hợp lệ trước hết được xác định bằng cách sử dụng hệ thống cơ bản ở thiết bị đầu cuối, và sau đó được gửi đến TEE để xử lý. Do vậy, có thể được đảm bảo rằng thông điệp SMS mã kiểm chứng được nhận diện ngay lập tức, nhờ đó nhanh chóng nhập vào thủ tục xử lý mã kiểm chứng.

Theo triển khai, thành phần truyền thông được tạo cấu hình cụ thể để nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; và bộ xử lý còn được tạo cấu hình để: mật mã hóa và lưu trữ thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa gồm mã kiểm chứng được hiển thị ở dạng văn bản mật mã; thu thập chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó chỉ mục lưu trữ ghi nhận vị trí lưu trữ của thông điệp SMS mã kiểm

chứng được mật mã hóa trong không gian lưu trữ; gửi chỉ mục lưu trữ đến REE; thu thập thông điệp SMS mã kiểm chứng được mật mã hóa theo chỉ mục lưu trữ, và thêm thông điệp SMS mã kiểm chứng được mật mã hóa vào yêu cầu thu thập mã kiểm chứng; trích rút thông điệp SMS mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và giải mã thông điệp SMS mã kiểm chứng được mật mã hóa, và trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng được giải mật mã. TEE có thể bỏ chạy sau khi lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa và gửi chỉ mục lưu trữ đến REE, và có thể khởi động lại việc chạy sau khi nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE. Do vậy, thời gian chạy của TEE được giảm, và tiêu thụ tài nguyên trong khi chạy được giảm. Ngoài ra, so với REE, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa trong TEE, và sau đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được giải mã trong TEE. Do vậy, bảo mật là cao hơn.

Theo triển khai, thành phần truyền thông còn được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng; và bộ xử lý còn được tạo cấu hình để: trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng; xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền; và nếu thông tin người gửi là thông tin người gửi được ủy quyền, xác định rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ. Trước khi gửi thông điệp SMS mã kiểm chứng đến TEE, modem trước hết kiểm chứng liệu người gửi của thông điệp SMS mã kiểm chứng được ủy quyền, để còn cải thiện bảo mật.

Theo triển khai, bộ xử lý được tạo cấu hình cụ thể để:

xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó

danh sách trắng gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng. Do vậy, bảo mật của thông điệp SMS mã kiểm chứng được gửi đến TEE được đảm bảo.

Theo triển khai, bộ xử lý được tạo cấu hình cụ thể để:

xác định liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng. Do vậy, bảo mật của thông điệp SMS mã kiểm chứng được gửi đến TEE được đảm bảo.

Theo triển khai, bộ xử lý còn được tạo cấu hình để: mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ gồm văn bản mật mã hóa của mã kiểm chứng; và lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE; thành phần truyền thông còn được tạo cấu hình để: sau khi yêu cầu xem mã kiểm chứng được nhận, gửi, đến TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được lưu trữ trong không gian lưu trữ của REE; và bộ xử lý còn được tạo cấu hình để giải mã thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, để thu thập thông điệp SMS mã kiểm chứng hợp lệ được giải mã. TEE có thể bỏ chạy sau khi lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ của REE, và có thể khởi động lại việc chạy sau khi nhận thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được gửi bởi REE. Do vậy, thời gian chạy của TEE được giảm, và tiêu thụ tài nguyên trong khi chạy được giảm. Ngoài ra, so với REE, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa trong TEE, và sau đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được giải mã trong TEE.

Do vậy, bảo mật là cao hơn. Ngoài ra, TEE lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE, để tiết kiệm không gian lưu trữ của REE.

Theo triển khai, bộ xử lý còn được tạo cấu hình để lưu trữ thông điệp SMS mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE. TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Do vậy, thông điệp SMS mã kiểm chứng hợp lệ được lưu trữ trong không gian lưu trữ của TEE. Do vậy, bảo mật là cao hơn.

Theo triển khai, bộ xử lý còn được tạo cấu hình để xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ, trong đó danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; và thành phần truyền thông còn được tạo cấu hình để gửi thông tin về ứng dụng được ủy quyền đến TEE. TEE kiểm chứng, theo thông tin về ứng dụng được ủy quyền, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền. Do vậy, bảo mật là cao hơn.

Theo triển khai, bộ xử lý còn được tạo cấu hình để: trích rút trường PDU của thông điệp SMS mã kiểm chứng hợp lệ, và xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng. Do vậy, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền được kiểm chứng theo thông tin về ứng dụng được ủy quyền. Do vậy, bảo mật là cao hơn.

Theo triển khai, bộ xử lý còn được tạo cấu hình để: trích rút thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh

sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ. Do vậy, liệu ứng dụng mà gửi yêu cầu thu thập mã kiểm chứng được ủy quyền được kiểm chứng theo thông tin về ứng dụng được ủy quyền. Do vậy, bảo mật là cao hơn.

Mô tả vắn tắt các hình vẽ đi kèm

Để mô tả các giải pháp kỹ thuật theo các phương án thực hiện sáng chế hoặc theo giải pháp kỹ thuật đã biết rõ ràng hơn, phần sau mô tả vắn tắt các hình vẽ đi kèm được yêu cầu để mô tả các phương án thực hiện hoặc giải pháp kỹ thuật đã biết. Rõ ràng là, các hình vẽ đi kèm trong phần mô tả sau thể hiện chỉ một số phương án thực hiện sáng chế, và những người có kiến thức trung bình trong lĩnh vực có thể vẫn suy ra các hình vẽ khác từ các hình vẽ đi kèm này mà không cần nỗ lực sáng tạo.

Fig.1 là sơ đồ cấu trúc của thiết bị đầu cuối được bộc lộ giải pháp kỹ thuật đã biết;

Fig.2 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng chế;

Fig.3A và Fig.3B là lưu đồ báo hiệu của phương pháp xử lý mã kiểm chứng theo phương án thực hiện sáng chế;

Fig.4A và Fig.4B là lưu đồ báo hiệu của phương pháp xử lý mã kiểm chứng khác theo phương án thực hiện sáng chế;

Fig.5 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng chế; và

Fig.6 là sơ đồ cấu trúc của phần cứng của thiết bị đầu cuối theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Với sự phổ biến của các thiết bị đầu cuối di động và sự phong phú của các chức năng của các thiết bị đầu cuối di động, các thiết bị đầu cuối di động ngày càng mở rộng. Một cách tương ứng, các vấn đề bảo mật thông tin của các thiết bị đầu cuối di động thu hút nhiều sự chú ý hơn. Chẳng hạn, cách thức hiện tại gửi mã kiểm chứng đến thiết bị đầu cuối di động để kiểm chứng sự cho phép của người dùng được áp dụng rộng rãi vào các kịch bản đăng nhập và thanh toán di động. Các kịch bản đăng nhập và thanh toán di động liên quan đến tài sản cá nhân và dữ liệu riêng tư của các người dùng, và do vậy, cực kỳ quan trọng bảo vệ các mã kiểm chứng.

Fig.1 là sơ đồ cấu trúc của thiết bị đầu cuối được bộc lộ theo giải pháp kỹ thuật đã biết. Thiết bị đầu cuối gồm modem và REE. Theo giải pháp kỹ thuật đã biết, khi nhận thông điệp SMS mã kiểm chứng, thiết bị đầu cuối di động vận chuyển thông điệp SMS mã kiểm chứng đến modem để chuyển đổi tín hiệu, và sau đó vận chuyển mã kiểm chứng thu được sau khi chuyển đổi tín hiệu đến REE để xử lý. REE có khả năng xử lý dữ liệu mạnh, nhưng có độ bảo mật thấp. Sau khi yêu cầu sao chép mã kiểm chứng được nhận trong REE, tất cả nội dung được sao chép được lưu trữ trong bộ đệm của bộ nhớ tạm. Bất kể loại yêu cầu dán nhận được trong REE, mã kiểm chứng được trình diện mà không có xác định bất kỳ. Trong trường hợp này, mã kiểm chứng về cơ bản là thông tin nhạy cảm có thể được dán ngẫu nhiên, và mã kiểm chứng không an toàn. Do vậy, cách thức cải thiện bảo mật trong quá trình sao chép và dán mã kiểm chứng trở thành vấn đề khẩn cấp được giải quyết hiện tại.

Theo các phương án thực hiện sáng chế, tđể giải quyết vấn đề theo giải pháp kỹ thuật đã biết nêu trên, sơ đồ cấu trúc, được thể hiện trên Fig.2, của thiết bị đầu cuối được bộc lộ theo phương án thực hiện sáng chế được sử dụng, để thực hiện quá trình sao chép và dán mã kiểm chứng. Hệ điều hành được thể hiện ở thiết bị đầu cuối trên Fig.2 gồm modem,

TEE, và REE. TEE là môi trường chạy đồng tồn tại với REE trên thiết bị đầu cuối di động. Ngoài ra, TEE là môi trường chạy bảo mật mà chạy trong bộ xử lý chính. Kiểm chứng cần được thực hiện trong quá trình khởi động bảo mật của TEE, và quá trình khởi động bảo mật của TEE được tách khỏi quá trình của REE. Các chương trình ứng dụng được lưu trữ trong TEE độc lập với nhau, và không thể truy nhập lẫn nhau nếu không được phép, sao cho được đảm bảo rằng các chương trình ứng dụng quá trình xử lý dữ liệu và tài nguyên trong TEE được thực hiện trong môi trường đáng tin cậy, và dịch vụ bảo mật được cấp cho hệ điều hành REE. TEE có không gian thực thi cá nhân, và có mức bảo mật cao hơn mức của hệ điều hành REE. TEE không phải là vi mạch bảo mật vật lý độc lập, nhưng là kiến trúc bảo mật trùng lặp kiến trúc phần cứng của bộ xử lý ứng dụng hiện được sử dụng. Các tài nguyên phần cứng và phần mềm có thể được truy nhập bởi TEE được tách khỏi hệ điều hành REE, để hỗ trợ phần cứng cô lập. Do vậy, so với REE, TEE là môi trường thực thi có độ bảo mật cao hơn.

Phần sau mô tả rõ ràng và đầy đủ giải pháp kỹ thuật thực hiện sao chép và dán mã kiểm chứng trong TEE theo các phương án thực hiện sáng chế dựa vào các hình vẽ đi kèm theo các phương án thực hiện sáng chế.

Fig.3A và Fig.3B thể hiện quá trình cụ thể của phương pháp xử lý mã kiểm chứng theo phương án thực hiện sáng chế. Phương pháp gồm các bước sau.

S101: modem tiếp nhận thông điệp SMS.

S102: Modem xác định liệu thông điệp SMS có phải là thông điệp SMS mã kiểm chứng, và nếu thông điệp SMS là thông điệp SMS mã kiểm chứng, thực hiện S103, hoặc nếu thông điệp SMS không phải là thông điệp SMS mã kiểm chứng, gửi thông điệp SMS đến REE, trong đó thông điệp SMS được xử lý trong REE theo thủ tục xử lý thông điệp SMS

đã biết.

Nên lưu ý rằng thông điệp SMS được nhận bởi thiết bị đầu cuối di động trước hết cần được xử lý bởi modem. Cách thức xác định, bởi modem, liệu thông điệp SMS là thông điệp SMS mã kiểm chứng có thể đảm bảo rằng thông điệp SMS mã kiểm chứng được nhận diện ngay lập tức, nhờ đó nhanh chóng nhập vào thủ tục xử lý mã kiểm chứng. Nên lưu ý rằng theo phương án thực hiện sáng chế, bước xác định liệu thông điệp SMS là thông điệp SMS mã kiểm chứng có thể được thực hiện trong mô đun bất kỳ trong đó đặt thông điệp SMS trước thông điệp SMS được gửi đến REE để xử lý, để tránh gửi, khi thông điệp SMS mã kiểm chứng không thể được nhận diện đúng lúc, thông điệp SMS mã kiểm chứng đến REE để xử lý theo thủ tục xử lý thông điệp SMS đã biết.

Modem trích rút nội dung thông điệp SMS để xác định liệu nội dung thông điệp SMS gồm thông tin mã kiểm chứng, và nếu nội dung thông điệp SMS gồm thông tin mã kiểm chứng, xác định rằng thông điệp SMS là thông điệp SMS mã kiểm chứng. Cách thức xác định liệu nội dung thông điệp SMS gồm thông tin mã kiểm chứng có thể xác định liệu nội dung thông điệp SMS gồm từ khóa dấu hiệu nhận diện thông điệp SMS là thông điệp SMS mã kiểm chứng, chẳng hạn, “mã kiểm chứng là:” hoặc “mật khẩu động là”. Theo phương án thực hiện sáng chế, có thể còn được xác định liệu số trong nội dung thông điệp SMS có đặc tính mã kiểm chứng, chẳng hạn, liệu số lượng chữ số và đặc tính tổ hợp chữ số tuân theo đặc tính mã kiểm chứng định trước. Điều này không bị giới hạn cụ thể theo phương án thực hiện sáng chế.

Một cách tùy chọn, modem trích rút số người gửi của thông điệp SMS để xác định liệu số người gửi của thông điệp SMS có phải là số người gửi tương ứng với thông điệp SMS mã kiểm chứng, và nếu số người gửi của thông điệp SMS là số người gửi tương ứng với thông điệp SMS mã kiểm chứng, xác định rằng thông điệp SMS là thông điệp SMS mã kiểm chứng.

Phương án thực hiện sáng chế không bị giới hạn ở các cách thức xác định nêu trên.

S103: Modem trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng.

S104: Modem xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền, và nếu thông tin người gửi là thông tin người gửi được ủy quyền, thực hiện S105, hoặc nếu thông tin người gửi không phải là thông tin người gửi được ủy quyền, chặn thông điệp SMS mã kiểm chứng, hoặc gửi thông điệp SMS mã kiểm chứng đến REE, trong đó thông điệp SMS mã kiểm chứng được xử lý trong REE theo thủ tục xử lý thông điệp SMS đã biết, và người dùng được thông báo rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng không hợp lệ.

Một cách tùy chọn, danh sách trắng có thể được định trước trong modem. Danh sách trắng ghi nhận ít nhất thông tin về thông điệp SMS người gửi được ủy quyền. Theo phương án thực hiện sáng chế, thông điệp SMS được gửi bởi thông điệp SMS người gửi không được ủy quyền có thể được lọc ra bằng cách sử dụng danh sách trắng được định trước trong modem. Thông tin về thông điệp SMS người gửi được ủy quyền có thể là số điện thoại tương ứng với thông điệp SMS người gửi được ủy quyền (Chẳng hạn, thông điệp SMS người gửi được ủy quyền là China Unicom, và số điện thoại tương ứng với thông điệp SMS người gửi được ủy quyền là 10010, 10010022, hoặc tương tự), địa chỉ gửi tương ứng với thông điệp SMS người gửi được ủy quyền, hoặc tương tự. Điều này không bị giới hạn theo sáng chế. Tức là, modem xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng.

Một cách tùy chọn, danh sách đen có thể được định trước trong

modem. Danh sách đen ghi nhận ít nhất thông tin về thông điệp SMS người gửi không được ủy quyền. Theo phương án thực hiện sáng chế, thông điệp SMS mã kiểm chứng được gửi bởi thông điệp SMS người gửi không được ủy quyền có thể được lọc ra bằng cách sử dụng danh sách đen được định trước trong modem. Thông tin về thông điệp SMS người gửi không được ủy quyền có thể là số điện thoại tương ứng với thông điệp SMS người gửi không được ủy quyền, địa chỉ gửi tương ứng với thông điệp SMS người gửi không được ủy quyền, hoặc tương tự. Điều này không bị giới hạn theo phương án thực hiện sáng chế. Tức là, modem xác định liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng.

S105: Modem xác định rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ, và gửi thông điệp SMS mã kiểm chứng hợp lệ đến TEE.

S106: TEE mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ gồm văn bản mật mã hóa của mã kiểm chứng.

S107: Gửi thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ đến REE, và lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE.

S108: REE tiếp nhận yêu cầu xem mã kiểm chứng.

S109: REE gửi, đến TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được lưu trữ trong không gian lưu trữ của REE.

S110: TEE giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, để thu thập thông điệp SMS mã kiểm chứng hợp lệ được giải

mã.

Nên lưu ý rằng sau khi thông điệp SMS mã kiểm chứng được giải mật mã hợp lệ thu được, phương pháp còn gồm: hiển thị thông điệp SMS mã kiểm chứng được giải mật mã hợp lệ. Thông điệp SMS mã kiểm chứng được giải mật mã hợp lệ có thể được hiển thị theo cách thức văn bản thường hoặc cách thức văn bản mã hóa. Điều này không bị giới hạn cụ thể theo phương án thực hiện sáng chế.

Một cách tùy chọn, TEE lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ của TEE, để cải tiến bảo mật của thông điệp SMS mã kiểm chứng.

S111: TEE trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng được giải mật mã hợp lệ, xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, và lưu trữ thông tin.

Thông tin về ứng dụng được ủy quyền là thông tin ứng dụng của ứng dụng không độc hại sẽ sử dụng mã kiểm chứng, và thông tin ứng dụng là thông tin có thể sử dụng duy nhất ứng dụng không độc hại mà sẽ sử dụng mã kiểm chứng. thông tin ứng dụng có thể là thông tin tên miền của ứng dụng được ủy quyền, tên gói của ứng dụng được ủy quyền, thông tin chữ ký của gói của ứng dụng được ủy quyền, ủy nhiệm cài đặt của ứng dụng được ủy quyền, giá trị băm của ứng dụng được ủy quyền, hoặc tương tự. Điều này không bị giới hạn theo sáng chế.

Một cách tùy chọn, TEE lưu trữ, trong không gian lưu trữ của TEE, mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, để đảm bảo bảo mật của mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Một cách tùy chọn, cách thức trong đó TEE xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng như sau:

Modem xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng

được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ, và gửi thông tin về ứng dụng được ủy quyền đến TEE, trong đó danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; hoặc

TEE trích rút trường khối dữ liệu giao thức (Protocol Data Unit – PDU) của thông điệp SMS mã kiểm chứng hợp lệ, và TEE xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; hoặc

TEE trích rút thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và TEE xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về an ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ.

S112: TEE tiếp nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE, trong đó yêu cầu thu thập mã kiểm chứng mang thông tin về ứng dụng để thu thập mã kiểm chứng.

S113: TEE xác định liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và thực hiện S114 nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, hoặc nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu

thập mã kiểm chứng không nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, từ chối yêu cầu thu thập mã kiểm chứng được gửi bởi REE.

S114: TEE gửi mã kiểm chứng đến REE.

Một cách tùy chọn, theo phương án thực hiện sáng chế, TEE gửi mã kiểm chứng đến REE theo cách thức văn bản thường hoặc cách thức văn bản mã hóa.

Fig.4A và Fig.4B thể hiện quá trình cụ thể của phương pháp xử lý khác mã kiểm chứng theo phương án thực hiện sáng chế. Phương pháp gồm các bước sau.

S201: Modem tiếp nhận thông điệp SMS.

S202: Modem xác định liệu thông điệp SMS có phải là thông điệp SMS mã kiểm chứng, và nếu thông điệp SMS là thông điệp SMS mã kiểm chứng, thực hiện S203, hoặc nếu thông điệp SMS không phải là thông điệp SMS mã kiểm chứng, gửi thông điệp SMS đến REE, trong đó thông điệp SMS được xử lý trong REE theo thủ tục xử lý thông điệp SMS đã biết.

S203: Modem trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng.

S204: Modem xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền, và nếu thông tin người gửi là thông tin người gửi được ủy quyền, thực hiện S205, hoặc nếu thông tin người gửi không phải là thông tin người gửi được ủy quyền, chặn thông điệp SMS mã kiểm chứng, hoặc gửi thông điệp SMS mã kiểm chứng đến REE, trong đó thông điệp SMS mã kiểm chứng được xử lý trong REE theo thủ tục xử lý thông điệp SMS đã biết, và người dùng được thông báo rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng không hợp lệ.

Nên lưu ý rằng, việc modem xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền gồm:

modem xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng; hoặc

modem xác định liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng.

S205: Modem xác định rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ, và gửi thông điệp SMS mã kiểm chứng hợp lệ đến TEE.

S206: TEE mật mã hóa và lưu trữ thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa gồm mã kiểm chứng được hiển thị ở dạng văn bản mật mã.

Theo phương án thực hiện sáng chế, TEE lưu trữ thông điệp SMS mã kiểm chứng trong không gian lưu trữ của REE hoặc không gian lưu trữ của TEE. Điều này không bị giới hạn cụ thể theo phương án thực hiện sáng chế.

S207: TEE thu thập chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó chỉ mục lưu trữ ghi nhận vị trí lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ.

S208: TEE gửi chỉ mục lưu trữ đến REE.

Nên lưu ý rằng TEE có thể bỏ chạy sau khi gửi chỉ mục lưu trữ đến REE, và có thể khởi động lại việc chạy sau khi nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE. Thông tin về ứng dụng được ủy quyền mà

sử dụng mã kiểm chứng được xác định theo thông điệp SMS mã kiểm chứng được mật mã hóa trong yêu cầu thu thập mã kiểm chứng, để giảm thời gian chạy của TEE.

S209: REE tiếp nhận yêu cầu xem mã kiểm chứng.

S210: REE thu thập thông điệp SMS mã kiểm chứng được mật mã hóa từ không gian lưu trữ theo chỉ mục lưu trữ thu được từ TEE, và tạo yêu cầu thu thập mã kiểm chứng theo thông điệp SMS mã kiểm chứng được mật mã hóa và thông tin về ứng dụng để thu thập mã kiểm chứng.

S211: REE gửi yêu cầu thu thập mã kiểm chứng đến TEE.

Yêu cầu thu thập mã kiểm chứng mang ít nhất thông điệp SMS mã kiểm chứng được mật mã hóa và thông tin về ứng dụng để thu thập mã kiểm chứng.

S212: TEE trích rút thông điệp SMS mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng, giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa, và trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng được giải mật mã.

S213: TEE xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, và lưu trữ thông tin.

Cách thức trong đó TEE xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng như sau:

Modem xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ, và gửi thông tin về ứng dụng được ủy quyền đến TEE, trong đó danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; hoặc

TEE trích rút trường PDU của thông điệp SMS mã kiểm chứng hợp lệ, và TEE xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền

mà sử dụng mã kiểm chứng; hoặc

TEE trích rút thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và TEE xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ.

S214: TEE xác định liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và thực hiện S215 nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, hoặc nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng không nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, TEE từ chối yêu cầu thu thập mã kiểm chứng được gửi bởi REE.

S215: Gửi mã kiểm chứng đến REE.

Một cách tùy chọn, theo phương án thực hiện sáng chế, TEE gửi mã kiểm chứng đến REE theo cách thức văn bản thường hoặc cách thức văn bản mã hóa.

Một cách tùy chọn, thiết bị xử lý mã kiểm chứng lưu trữ, trong không gian lưu trữ của TEE, mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, để đảm bảo bảo mật của mã kiểm chứng and thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm

chứng.

Một cách tùy chọn, thông tin về ứng dụng được ủy quyền của mã kiểm chứng gồm thông tin tên miền của ứng dụng được ủy quyền, tên gói của ứng dụng được ủy quyền, thông tin chữ ký của gói của ứng dụng được ủy quyền, ủy nhiệm cài đặt của ứng dụng được ủy quyền, giá trị băm, và tương tự. Điều này không bị giới hạn theo sáng chế.

Fig.5 thể hiện thiết bị đầu cuối di động theo phương án thực hiện sáng chế. Thiết bị đầu cuối di động gồm môđun yêu cầu thu thập mã kiểm chứng nhận, môđun xác định thông tin, và môđun gửi mã kiểm chứng. Cụ thể là, môđun xác định thông tin có thể được đặt trong TEE, và môđun yêu cầu thu thập mã kiểm chứng nhận và môđun gửi mã kiểm chứng có thể được đặt trong hệ thống truyền thông băng gốc của thiết bị đầu cuối.

Môđun yêu cầu thu thập mã kiểm chứng nhận được tạo cấu hình để nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE, trong đó yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng.

Môđun xác định thông tin được tạo cấu hình để xác định liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Môđun gửi mã kiểm chứng được tạo cấu hình để gửi mã kiểm chứng đến REE nếu môđun xác định thông tin xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Thiết bị đầu cuối di động còn gồm: môđun thu thập mã kiểm chứng thứ nhất, được tạo cấu hình để thu thập mã kiểm chứng, trong đó:

môđun thu thập mã kiểm chứng thứ nhất gồm:

mô đun nhận thông điệp SMS mã kiểm chứng hợp lệ thứ nhất, được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; và

môđun trích rút mã kiểm chứng, được tạo cấu hình để trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ.

Thiết bị đầu cuối di động còn gồm: môđun thu thập mã kiểm chứng thứ hai, được tạo cấu hình để thu thập mã kiểm chứng, trong đó:

môđun thu thập mã kiểm chứng thứ hai gồm:

môđun nhận thông điệp SMS mã kiểm chứng hợp lệ thứ hai, được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem;

môđun lưu trữ và mật mã hóa, được tạo cấu hình để mật mã hóa và lưu trữ thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa gồm mã kiểm chứng được hiển thị ở dạng văn bản mật mã;

môđun thu thập chỉ mục lưu trữ, được tạo cấu hình để thu thập chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó chỉ mục lưu trữ ghi nhận vị trí lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ;

môđun gửi chỉ mục lưu trữ, được tạo cấu hình để gửi chỉ mục lưu trữ đến REE;

môđun thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa theo chỉ mục lưu trữ;

môđun thêm thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để thêm thông điệp SMS mã kiểm chứng được mật mã hóa đến yêu cầu thu thập mã kiểm chứng;

môđun trích rút thông điệp SMS mã kiểm chứng được mật mã hóa,

được tạo cấu hình để trích rút thông điệp SMS mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và

môđun giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa, được tạo cấu hình để giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa, để trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng được giải mật mã.

Thiết bị đầu cuối di động còn gồm:

môđun nhận thông điệp SMS mã kiểm chứng, được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng;

môđun trích rút thông tin người gửi, được tạo cấu hình để trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng;

môđun xác định thông tin người gửi, được tạo cấu hình để xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền; và

môđun xác định thông điệp SMS mã kiểm chứng hợp lệ, được tạo cấu hình để: nếu môđun xác định thông tin người gửi xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, xác định rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ.

Môđun xác định thông tin người gửi gồm:

môđun phụ xác định thông tin người gửi thứ nhất, được tạo cấu hình để xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng; và

môđun xác định thông tin người gửi được ủy quyền thứ nhất, được tạo cấu hình để: nếu môđun phụ xác định thông tin người gửi thứ nhất xác định rằng thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng.

Môđun xác định thông tin người gửi gồm:

môđun phụ xác định thông tin người gửi thứ hai, được tạo cấu hình để

xác định liệu thông tin người gửi được lưu trữ trong danh sách đen; và

môđun xác định thông tin người gửi được ủy quyền xác định thứ hai, được tạo cấu hình để: nếu môđun phụ xác định thông tin người gửi thứ hai xác định rằng thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng.

Thiết bị đầu cuối di động còn gồm:

môđun mật mã thứ nhất, được tạo cấu hình để mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ gồm văn bản mật mã hóa của mã kiểm chứng;

môđun lưu trữ thứ nhất, được tạo cấu hình để lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE;

môđun gửi thứ nhất, được tạo cấu hình để: sau khi yêu cầu xem mã kiểm chứng được nhận, gửi, đến TEE, thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ được lưu trữ trong không gian lưu trữ của REE; và

môđun giải mật mã thứ nhất, được tạo cấu hình để giải mật mã thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, để thu thập thông điệp SMS mã kiểm chứng hợp lệ được giải mã.

Thiết bị đầu cuối di động còn gồm:

môđun lưu trữ thứ hai, được tạo cấu hình để lưu trữ thông điệp SMS mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE.

Thiết bị đầu cuối di động còn gồm:

môđun xác định thông tin thứ nhất, được tạo cấu hình để xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử

dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ, trong đó danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; và

môđun gửi thông tin thứ nhất, được tạo cấu hình để gửi thông tin về ứng dụng được ủy quyền đến TEE.

Thiết bị đầu cuối di động còn gồm:

môđun trích rút trường PDU, được tạo cấu hình để trích rút trường PDU của thông điệp SMS mã kiểm chứng hợp lệ; và

môđun xác định thông tin thứ hai, được tạo cấu hình để xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Thiết bị đầu cuối di động còn gồm:

môđun trích rút thông tin người gửi được ủy quyền, được tạo cấu hình để trích rút thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và

môđun xác định thông tin thứ ba, được tạo cấu hình để xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ.

Fig.6 thể hiện thiết bị đầu cuối di động theo phương án thực hiện sáng chế. Thiết bị đầu cuối di động gồm thành phần truyền thông, bộ nhớ, và bộ xử lý.

Bộ nhớ được tạo cấu hình để: lưu trữ mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, và lưu trữ chương trình ứng dụng và dữ liệu được tạo trong quá trình chạy chương trình ứng

dụng.

Thành phần truyền thông được tạo cấu hình để: nhận yêu cầu thu thập mã kiểm chứng mà mang ít nhất thông tin về ứng dụng để thu thập mã kiểm chứng, và gửi mã kiểm chứng nếu bộ xử lý xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Bộ xử lý được tạo cấu hình để xác định liệu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng mà thu thập mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Cụ thể là, thành phần truyền thông được tạo cấu hình để: nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem, và trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng hợp lệ.

Cụ thể là, thành phần truyền thông được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng hợp lệ được gửi bởi modem; và bộ xử lý còn được tạo cấu hình để: mật mã hóa và lưu trữ thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa gồm mã kiểm chứng được hiển thị ở dạng văn bản mật mã; thu thập chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa, trong đó chỉ mục lưu trữ ghi nhận vị trí lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa trong không gian lưu trữ; gửi chỉ mục lưu trữ đến REE; thu thập thông điệp SMS mã kiểm chứng được mật mã hóa theo chỉ mục lưu trữ, và thêm thông điệp SMS mã kiểm chứng được mật mã hóa vào yêu cầu thu thập mã kiểm chứng; trích rút thông điệp SMS mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi

REE; và giải mã thông điệp SMS mã kiểm chứng được mật mã hóa, và trích rút mã kiểm chứng từ thông điệp SMS mã kiểm chứng được giải mật mã.

Ngoài ra, thành phần truyền thông còn được tạo cấu hình để nhận thông điệp SMS mã kiểm chứng; và bộ xử lý còn được tạo cấu hình để: trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng; xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền; và nếu thông tin người gửi là thông tin người gửi được ủy quyền, xác định rằng thông điệp SMS mã kiểm chứng là thông điệp SMS mã kiểm chứng hợp lệ.

Cụ thể là, bộ xử lý được tạo cấu hình để:

xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng.

Cụ thể là, bộ xử lý được tạo cấu hình để:

xác định liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen gồm ít nhất thông tin người gửi không được ủy quyền của thông điệp SMS mã kiểm chứng.

Ngoài ra, bộ xử lý còn được tạo cấu hình để: mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ, để thu thập thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, trong đó thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ gồm văn bản mật mã hóa của mã kiểm chứng; và lưu trữ thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ trong không gian lưu trữ của REE; thành phần truyền thông còn được tạo cấu hình để: sau khi yêu cầu xem mã kiểm chứng được nhận, gửi, đến TEE, thông điệp

SMS mã kiểm chứng được mật mã hóa hợp lệ được lưu trữ trong không gian lưu trữ của REE; và bộ xử lý còn được tạo cấu hình để giải mã thông điệp SMS mã kiểm chứng được mật mã hóa hợp lệ, để thu thập thông điệp SMS mã kiểm chứng hợp lệ được giải mã.

Ngoài ra, bộ xử lý còn được tạo cấu hình để lưu trữ thông điệp SMS mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE.

Ngoài ra, bộ xử lý còn được tạo cấu hình để xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ, trong đó danh sách trắng còn gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ; và thành phần truyền thông còn được tạo cấu hình để gửi thông tin về ứng dụng được ủy quyền đến TEE.

Ngoài ra, bộ xử lý còn được tạo cấu hình để: trích rút trường PDU của thông điệp SMS mã kiểm chứng hợp lệ, và xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

Ngoài ra, bộ xử lý còn được tạo cấu hình để: trích rút thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng hợp lệ; và xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của ứng dụng được ủy quyền và được định trước trong TEE gồm ít nhất thông tin người gửi được ủy quyền của thông điệp SMS mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong thông điệp SMS mã kiểm chứng hợp lệ.

Đối với quá trình triển khai cụ thể của các chức năng nêu trên, tham khảo Fig.3A và Fig.3B, và Fig.4A và Fig.4B.

Các phương án thực hiện sáng chế đều được mô tả theo cách lũy tiến,

đối với các phần tương tự hoặc giống nhau theo theo các phương án thực hiện, tham khảo các phương án thực hiện này, và mỗi phương án thực hiện tập trung vào khác biệt với các phương án thực hiện khác.

Các phương án thực hiện nêu trên được mô tả để cho phép chuyên gia trong lĩnh vực thực hiện hoặc sử dụng sáng chế. Các biến thể khác nhau với các phương án thực hiện là rõ ràng với các chuyên gia trong lĩnh vực, và các nguyên lý tổng quát được định nghĩa theo sáng chế có thể được thực hiện theo các phương án thực hiện khác mà không xa rời phạm vi của sáng chế. Do vậy, sáng chế không được nhằm bị giới hạn ở các phương án thực hiện này được minh họa theo sáng chế, nhưng sẽ được hiểu theo nghĩa rộng nhất tuân theo các nguyên lý và các dấu hiệu được bộc lộ theo sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xử lý mã kiểm chứng bao gồm các bước:

nhận, bằng môi trường thực thi đáng tin cậy (trusted execution environment, TEE), yêu cầu thu thập mã kiểm chứng được gửi bởi môi trường thực thi phong phú (rich execution environment REE), trong đó yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng, và TEE bao gồm mã kiểm chứng;

nhận, bởi TEE, tin nhắn của dịch vụ tin nhắn ngắn (Short Message Services, SMS) chứa mã kiểm chứng hợp lệ được gửi bằng modem;

mật mã hóa, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng được mật mã hóa hợp lệ bao gồm bản mã của mã kiểm chứng;

gửi, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa đến REE;

lưu trữ, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa trong không gian lưu trữ của REE;

nhận, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa được gửi bởi REE và được lưu trữ trong không gian lưu trữ của REE;

giải mã, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã;

trích xuất, bởi TEE, mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã;

xác định, bởi TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ, và lưu trữ thông tin;

xác định, bởi TEE, liệu thông tin có được mang trong yêu cầu thu

thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và

gửi mã kiểm chứng đến REE nếu thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

2. Phương pháp theo điểm 1, trong đó sau khi nhận, bởi TEE, yêu cầu thu thập mã kiểm chứng được gửi bởi REE, phương pháp còn bao gồm các bước:

nhận, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem; và

trích xuất, bởi TEE, mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ.

3. Phương pháp theo điểm 1, trong đó quá trình thu thập mã kiểm chứng bao gồm:

nhận, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem;

mật mã hóa và lưu trữ, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng được mật mã hóa bao gồm mã kiểm chứng được hiển thị ở dạng bản mã;

thu được, bởi TEE, chỉ số lưu trữ của tin nhắn SMS có mã kiểm chứng được mật mã hóa, trong đó chỉ số lưu trữ ghi nhận vị trí lưu trữ của tin nhắn SMS có mã kiểm chứng được mật mã hóa trong không gian lưu trữ;

gửi, bởi TEE, chỉ số lưu trữ đến REE;

thu được, bởi REE, tin nhắn SMS có mã kiểm chứng được mật mã hóa theo chỉ số lưu trữ, và bổ sung tin nhắn SMS có mã kiểm chứng được mật mã hóa vào yêu cầu thu thập mã kiểm chứng;

trích xuất, bởi TEE, tin nhắn SMS có mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và

giải mã, bởi TEE, tin nhắn SMS có mã kiểm chứng được mật mã hóa, và trích xuất mã kiểm chứng từ thông điệp SMS có mã kiểm chứng được giải mã.

4. Phương pháp theo điểm 2 hoặc 3, trong đó trước khi nhận, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem, phương pháp còn bao gồm các bước:

nhận, bằng modem, tin nhắn SMS có mã kiểm chứng;

trích xuất, bằng modem, thông tin người gửi của tin nhắn SMS có mã kiểm chứng;

xác định, bằng modem, liệu thông tin người gửi có phải là thông tin người gửi được ủy quyền; và

nếu thông tin người gửi là thông tin người gửi được ủy quyền, xác định, bằng modem, rằng tin nhắn SMS có mã kiểm chứng là tin nhắn SMS có mã kiểm chứng hợp lệ.

5. Phương pháp theo điểm 4, trong đó việc xác định, bằng modem, liệu thông tin người gửi là thông tin người gửi được ủy quyền bao gồm bước:

xác định, bằng modem, liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng bao gồm ít nhất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng.

6. Phương pháp theo điểm 4, trong đó việc xác định, bằng modem, liệu thông tin người gửi là thông tin người gửi được ủy quyền bao gồm bước:

xác định, bằng modem, liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen bao gồm ít nhất thông tin người gửi không được ủy quyền của tin nhắn SMS có mã kiểm chứng.

7. Phương pháp theo điểm 2, trong đó trước khi trích xuất, bởi TEE, mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ, phương pháp còn bao gồm các bước:

mật mã hóa, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa bao gồm bản mã của mã kiểm chứng;

lưu trữ, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa trong không gian lưu trữ của REE;

sau khi REE nhận yêu cầu xem mã kiểm chứng, gửi, bởi REE đến TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa được lưu trữ trong không gian lưu trữ của REE; và

giải mã, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã.

8. Phương pháp theo điểm 2, trong đó trước khi trích xuất, bởi TEE, mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ, phương pháp còn bao gồm bước:

lưu trữ, bởi TEE, tin nhắn SMS có mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE.

9. Phương pháp theo điểm 5, trong đó danh sách trắng còn bao gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng in tin nhắn SMS có mã kiểm chứng hợp lệ; và

trước khi xác định, bởi TEE, liệu thông tin có được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, phương pháp còn bao gồm:

xác định, bằng modem từ danh sách trắng theo thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ; và

gửi thông tin về thông tin được ủy quyền đến TEE.

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó trước khi xác định, bởi TEE, liệu thông tin có được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, phương pháp còn bao gồm các bước:

trích xuất, bởi TEE, trường đơn vị dữ liệu giao thức (protocol data unit, PDU) của tin nhắn SMS có mã kiểm chứng hợp lệ; và

xác định, bởi TEE từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó trước khi xác định, bởi TEE, liệu thông tin có được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong TEE và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, phương pháp còn bao gồm các bước:

trích xuất, bởi TEE, thông tin người gửi được ủy quyền của tin nhắn

SMS có mã kiểm chứng hợp lệ; và

xác định, bởi TEE theo thông tin người gửi được ủy quyền và từ danh sách thông tin của thông tin được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của thông tin được ủy quyền và được định trước trong TEE bao gồm ít nhất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ.

12. Thiết bị đầu cuối di động bao gồm:

môđun nhận yêu cầu thu thập mã kiểm chứng, được tạo cấu hình để nhận yêu cầu thu thập mã kiểm chứng được gửi bởi REE, trong đó yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng;

môđun nhận mã kiểm chứng thứ ba, được tạo cấu hình để thu được mã kiểm chứng, trong đó môđun nhận mã kiểm chứng thứ ba bao gồm:

môđun phụ nhận tin nhắn SMS có mã kiểm chứng hợp lệ, được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem;

môđun phụ mật mã hóa và lưu trữ, được tạo cấu hình để mật mã hóa tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, tin nhắn SMS có mã kiểm chứng được mật mã hóa hợp lệ bao gồm bản mã của mã kiểm chứng, gửi tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa đến REE, và lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa trong không gian lưu trữ của REE;

môđun phụ nhận tin nhắn SMS có mã kiểm chứng được mật mã hóa, được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng hợp lệ được

mật mã hóa được gửi bởi REE và được lưu trữ trong không gian lưu trữ của REE;

môđun phụ giải mã tin nhắn SMS có mã kiểm chứng được mật mã hóa, được tạo cấu hình để giải mã tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã;

môđun phụ trích xuất tin nhắn SMS có mã kiểm chứng, được tạo cấu hình để trích xuất mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã, xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ, và lưu trữ thông tin;

môđun xác định thông tin, được tạo cấu hình để xác định liệu thông tin có được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và

môđun gửi mã kiểm chứng, được tạo cấu hình để gửi mã kiểm chứng đến REE nếu môđun xác định thông tin xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

13. Thiết bị đầu cuối di động theo điểm 12, trong đó thiết bị còn bao gồm: môđun nhận mã kiểm chứng thứ nhất, được tạo cấu hình để thu được mã kiểm chứng, trong đó:

môđun nhận mã kiểm chứng thứ nhất bao gồm:

môđun nhận tin nhắn SMS có mã kiểm chứng hợp lệ thứ nhất, được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng hợp lệ được gửi

bởi modem; và

môđun trích xuất mã kiểm chứng, được tạo cấu hình để trích xuất mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ.

14. Thiết bị đầu cuối di động theo điểm 12, trong đó thiết bị còn bao gồm: môđun nhận mã kiểm chứng thứ hai, được tạo cấu hình để thu được mã kiểm chứng, trong đó:

môđun nhận mã kiểm chứng thứ hai bao gồm:

môđun nhận tin nhắn SMS có mã kiểm chứng hợp lệ thứ hai, được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem;

môđun mật mã hóa và lưu trữ, được tạo cấu hình để mật mã hóa và lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng được mật mã hóa bao gồm mã kiểm chứng được hiển thị ở dạng bản mã;

môđun nhận chỉ số lưu trữ, được tạo cấu hình để thu được chỉ số lưu trữ của tin nhắn SMS có mã kiểm chứng được mật mã hóa, trong đó chỉ số lưu trữ ghi nhận vị trí lưu trữ của tin nhắn SMS có mã kiểm chứng được mật mã hóa trong không gian lưu trữ;

môđun gửi chỉ số lưu trữ, được tạo cấu hình để gửi chỉ số lưu trữ đến REE;

môđun nhận tin nhắn SMS có mã kiểm chứng được mật mã hóa, được tạo cấu hình để thu được tin nhắn SMS có mã kiểm chứng được mật mã hóa theo chỉ số lưu trữ;

môđun bổ sung tin nhắn SMS có mã kiểm chứng được mật mã hóa, được tạo cấu hình để bổ sung tin nhắn SMS có mã kiểm chứng được mật mã hóa vào yêu cầu thu thập mã kiểm chứng;

môđun trích xuất tin nhắn SMS có mã kiểm chứng được mật mã hóa,

được tạo cấu hình để trích xuất tin nhắn SMS có mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và

môđun giải mã tin nhắn SMS có mã kiểm chứng được mật mã hóa, được tạo cấu hình để giải mã tin nhắn SMS có mã kiểm chứng được mật mã hóa, để trích xuất mã kiểm chứng từ thông điệp SMS có mã kiểm chứng được giải mã.

15. Thiết bị đầu cuối di động theo điểm 13 hoặc 14, trong đó thiết bị còn bao gồm:

môđun nhận tin nhắn SMS có mã kiểm chứng, được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng;

môđun trích xuất thông tin người gửi, được tạo cấu hình để trích xuất thông tin người gửi của tin nhắn SMS có mã kiểm chứng;

môđun xác định thông tin người gửi, được tạo cấu hình để xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền; và

môđun xác định tin nhắn SMS có mã kiểm chứng hợp lệ, được tạo cấu hình để: nếu môđun xác định thông tin người gửi xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, xác định rằng tin nhắn SMS có mã kiểm chứng là tin nhắn SMS có mã kiểm chứng hợp lệ.

16. Thiết bị đầu cuối di động theo điểm 15, trong đó môđun xác định thông tin người gửi bao gồm:

môđun phụ xác định thông tin người gửi thứ nhất, được tạo cấu hình để xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng; và

môđun phụ xác định thông tin người gửi được ủy quyền thứ nhất, được tạo cấu hình để: nếu môđun phụ xác định thông tin người gửi thứ nhất xác định rằng thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền,

trong đó danh sách trắng bao gồm ít nhất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng.

17. Thiết bị đầu cuối di động theo điểm 15, trong đó môđun xác định thông tin người gửi bao gồm:

môđun phụ xác định thông tin người gửi thứ hai, được tạo cấu hình để xác định liệu thông tin người gửi được lưu trữ trong danh sách đen; và

môđun phụ xác định thông tin người gửi được ủy quyền thứ hai, được tạo cấu hình để: nếu môđun phụ xác định thông tin người gửi thứ hai xác định rằng thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen bao gồm ít nhất thông tin người gửi không được ủy quyền của tin nhắn SMS có mã kiểm chứng.

18. Thiết bị đầu cuối di động theo điểm 13, trong đó thiết bị còn bao gồm:

môđun mật mã hóa thứ nhất, được tạo cấu hình để mật mã hóa tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa bao gồm bản mã của mã kiểm chứng;

môđun lưu trữ thứ nhất, được tạo cấu hình để lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa trong không gian lưu trữ của REE;

môđun gửi thứ nhất, được tạo cấu hình để: sau khi yêu cầu xem mã kiểm chứng được nhận, gửi, đến TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa được lưu trữ trong không gian lưu trữ của REE; và

môđun giải mã thứ nhất, được tạo cấu hình để giải mã tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã.

19. Thiết bị đầu cuối di động theo điểm 13, trong đó thiết bị còn bao gồm:

môđun lưu trữ thứ hai, được tạo cấu hình để lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE.

20. Thiết bị đầu cuối di động theo điểm 16, trong đó thiết bị còn bao gồm:

môđun xác định thông tin thứ nhất, được tạo cấu hình để xác định, from danh sách trắng theo thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ, trong đó danh sách trắng còn bao gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng in tin nhắn SMS có mã kiểm chứng hợp lệ; và

môđun gửi thông tin thứ nhất, được tạo cấu hình để gửi thông tin về thông tin được ủy quyền đến TEE.

21. Thiết bị đầu cuối di động theo điểm bất kỳ trong số các điểm từ 12 đến 14, trong đó thiết bị còn bao gồm:

môđun trích xuất trường PDU, được tạo cấu hình để trích xuất trường PDU của tin nhắn SMS có mã kiểm chứng hợp lệ; và

môđun xác định thông tin thứ hai, được tạo cấu hình để xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

22. Thiết bị đầu cuối di động theo điểm bất kỳ trong số các điểm từ 12 đến 14, trong đó thiết bị còn bao gồm:

mô đun trích xuất thông tin người gửi được ủy quyền, được tạo cấu hình để trích xuất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng hợp lệ; và

môđun xác định thông tin thứ ba, được tạo cấu hình để xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của thông tin được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của thông tin được ủy quyền và được định trước trong TEE bao gồm ít nhất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ.

23. Thiết bị đầu cuối di động bao gồm thành phần truyền thông, bộ nhớ, và bộ xử lý, trong đó:

bộ nhớ được tạo cấu hình để: lưu trữ mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, và lưu trữ chương trình ứng dụng và dữ liệu được tạo trong quá trình chạy chương trình ứng dụng;

thành phần truyền thông được tạo cấu hình để: nhận yêu cầu thu thập mã kiểm chứng mang ít nhất thông tin về ứng dụng thu thập mã kiểm chứng, và gửi mã kiểm chứng nếu bộ xử lý xác định rằng thông tin được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng; và

bộ xử lý được tạo cấu hình để xác định liệu thông tin có được mang trong yêu cầu thu thập mã kiểm chứng và về ứng dụng để thu được mã kiểm chứng nhất quán với thông tin được lưu trữ trong bộ nhớ của thiết bị đầu cuối di động và về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng;

thành phần truyền thông còn được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem;

bộ xử lý còn được tạo cấu hình để:

mật mã hóa tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng được mật mã hóa hợp lệ bao gồm bản mã của mã kiểm chứng;

gửi tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa đến REE;

lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa trong không gian lưu trữ của REE;

nhận tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa được gửi bởi REE và được lưu trữ trong không gian lưu trữ của REE;

giải mã tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã;

trích xuất mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã;

xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng in tin nhắn SMS có mã kiểm chứng hợp lệ, và lưu trữ thông tin.

24. Thiết bị đầu cuối di động theo điểm 23, trong đó thành phần truyền thông được tạo cấu hình cụ thể để: nhận tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem, và trích xuất mã kiểm chứng từ tin nhắn SMS có mã kiểm chứng hợp lệ.

25. Thiết bị đầu cuối di động theo điểm 23, trong đó thành phần truyền thông được tạo cấu hình cụ thể để nhận tin nhắn SMS có mã kiểm chứng hợp lệ được gửi bởi modem; và bộ xử lý còn được tạo cấu hình để: mật mã hóa và lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng được mật mã hóa bao gồm mã kiểm chứng được

hiển thị ở dạng bản mã; thu được chỉ số lưu trữ của tin nhắn SMS có mã kiểm chứng được mật mã hóa, trong đó chỉ số lưu trữ ghi nhận vị trí lưu trữ của tin nhắn SMS có mã kiểm chứng được mật mã hóa trong không gian lưu trữ; gửi chỉ số lưu trữ đến REE; thu được tin nhắn SMS có mã kiểm chứng được mật mã hóa theo chỉ số lưu trữ, và bổ sung tin nhắn SMS có mã kiểm chứng được mật mã hóa vào yêu cầu thu thập mã kiểm chứng; trích xuất tin nhắn SMS có mã kiểm chứng được mật mã hóa từ yêu cầu thu thập mã kiểm chứng được gửi bởi REE; và giải mã tin nhắn SMS có mã kiểm chứng được mật mã hóa, và trích xuất mã kiểm chứng từ thông điệp SMS có mã kiểm chứng được giải mã.

26. Thiết bị đầu cuối di động theo điểm 24 hoặc 25, trong đó thành phần truyền thông còn được tạo cấu hình để nhận tin nhắn SMS có mã kiểm chứng; và bộ xử lý còn được tạo cấu hình để: trích xuất thông tin người gửi của tin nhắn SMS có mã kiểm chứng; xác định liệu thông tin người gửi là thông tin người gửi được ủy quyền; và nếu thông tin người gửi là thông tin người gửi được ủy quyền, xác định rằng tin nhắn SMS có mã kiểm chứng là tin nhắn SMS có mã kiểm chứng hợp lệ.

27. Thiết bị đầu cuối di động theo điểm 26, trong đó bộ xử lý được tạo cấu hình cụ thể để:

xác định liệu thông tin người gửi được lưu trữ trong danh sách trắng, và nếu thông tin người gửi được lưu trữ trong danh sách trắng, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách trắng bao gồm ít nhất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng.

28. Thiết bị đầu cuối di động theo điểm 26, trong đó bộ xử lý được tạo cấu hình cụ thể để:

xác định liệu thông tin người gửi được lưu trữ trong danh sách đen, và nếu thông tin người gửi không được lưu trữ trong danh sách đen, xác định rằng thông tin người gửi là thông tin người gửi được ủy quyền, trong đó danh sách đen bao gồm ít nhất thông tin người gửi không được ủy quyền của tin nhắn SMS có mã kiểm chứng.

29. Thiết bị đầu cuối di động theo điểm 24, trong đó:

bộ xử lý còn được tạo cấu hình để: mật mã hóa tin nhắn SMS có mã kiểm chứng hợp lệ, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, trong đó tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa bao gồm bản mã của mã kiểm chứng; và lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa trong không gian lưu trữ của REE; thành phần truyền thông còn được tạo cấu hình để: sau khi yêu cầu xem mã kiểm chứng được nhận, gửi, đến TEE, tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa được lưu trữ trong không gian lưu trữ của REE; và bộ xử lý còn được tạo cấu hình để giải mã tin nhắn SMS có mã kiểm chứng hợp lệ được mật mã hóa, để thu được tin nhắn SMS có mã kiểm chứng hợp lệ được giải mã.

30. Thiết bị đầu cuối di động theo điểm 24, trong đó bộ xử lý còn được tạo cấu hình để lưu trữ tin nhắn SMS có mã kiểm chứng hợp lệ trong không gian lưu trữ của TEE.

31. Thiết bị đầu cuối di động theo điểm 27, trong đó:

bộ xử lý còn được tạo cấu hình để xác định, từ danh sách trắng theo thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng hợp lệ, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ, trong đó danh sách trắng còn bao gồm thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm

chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ; và thành phần truyền thông còn được tạo cấu hình để gửi thông tin về thông tin được ủy quyền đến TEE.

32. Thiết bị đầu cuối di động theo điểm bất kỳ trong số các điểm từ 23 đến 25, trong đó:

bộ xử lý còn được tạo cấu hình để: trích xuất trường PDU của tin nhắn SMS có mã kiểm chứng hợp lệ, và xác định, từ trường PDU, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng.

33. Thiết bị đầu cuối di động theo điểm bất kỳ trong số các điểm từ 23 đến 25, trong đó:

bộ xử lý còn được tạo cấu hình để: trích xuất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng hợp lệ; và xác định, theo thông tin người gửi được ủy quyền và từ danh sách thông tin của thông tin được ủy quyền và được định trước trong TEE, thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng, trong đó danh sách thông tin của thông tin được ủy quyền và được định trước trong TEE bao gồm ít nhất thông tin người gửi được ủy quyền của tin nhắn SMS có mã kiểm chứng và thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng trong tin nhắn SMS có mã kiểm chứng hợp lệ.

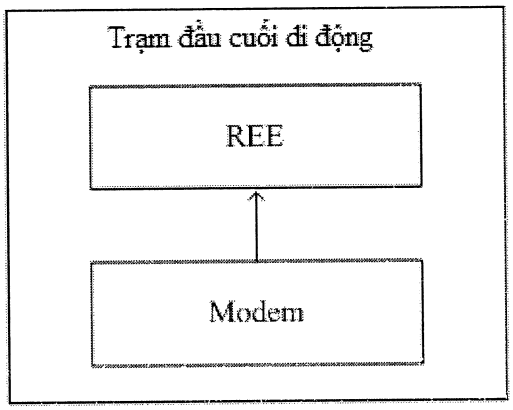

Trạm đầu cuối di động
REE
Modem

Fig.1

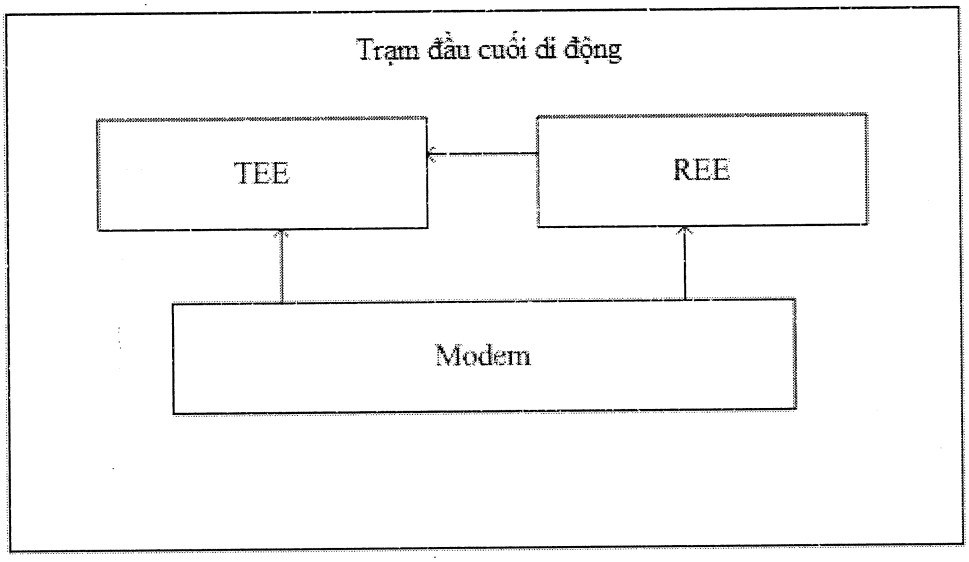

Trạm đầu cuối di động
TEE
REE
Modem

Fig.2

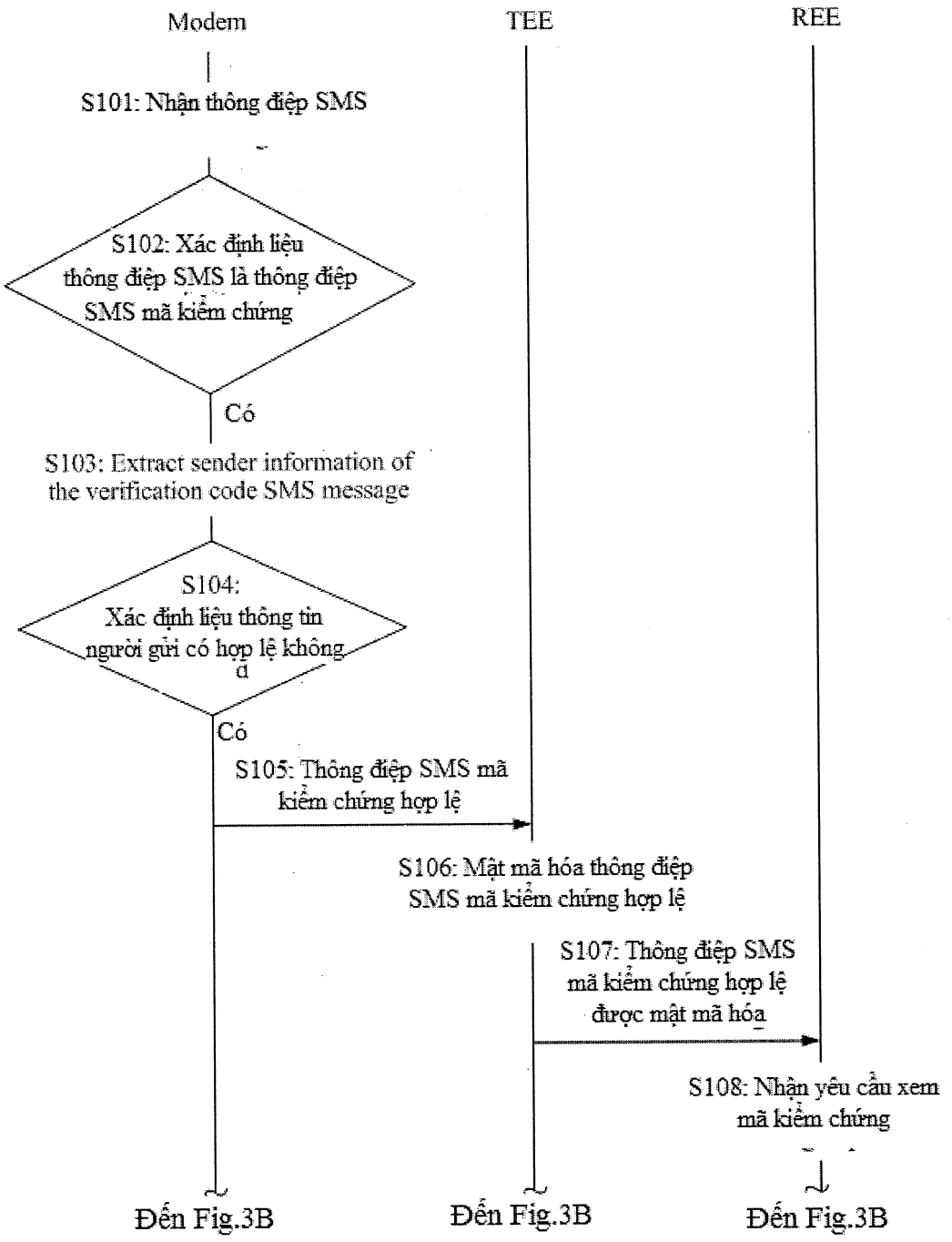

Modem
TEE
REE
S101: Nhận thông điệp SMS
S102: Xác định liệu thông điệp SMS là thông điệp SMS mã kiểm chứng
Có
S103: Extract sender information of the verification code SMS message
S104: Xác định liệu thông tin người gửi có hợp lệ không
Có
S105: Thông điệp SMS mã kiểm chứng hợp lệ
S106: Mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ
S107: Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa
S108: Nhận yêu cầu xem mã kiểm chứng
Đến Fig.3B
Đến Fig.3B
Đến Fig.3B

Fig.3A

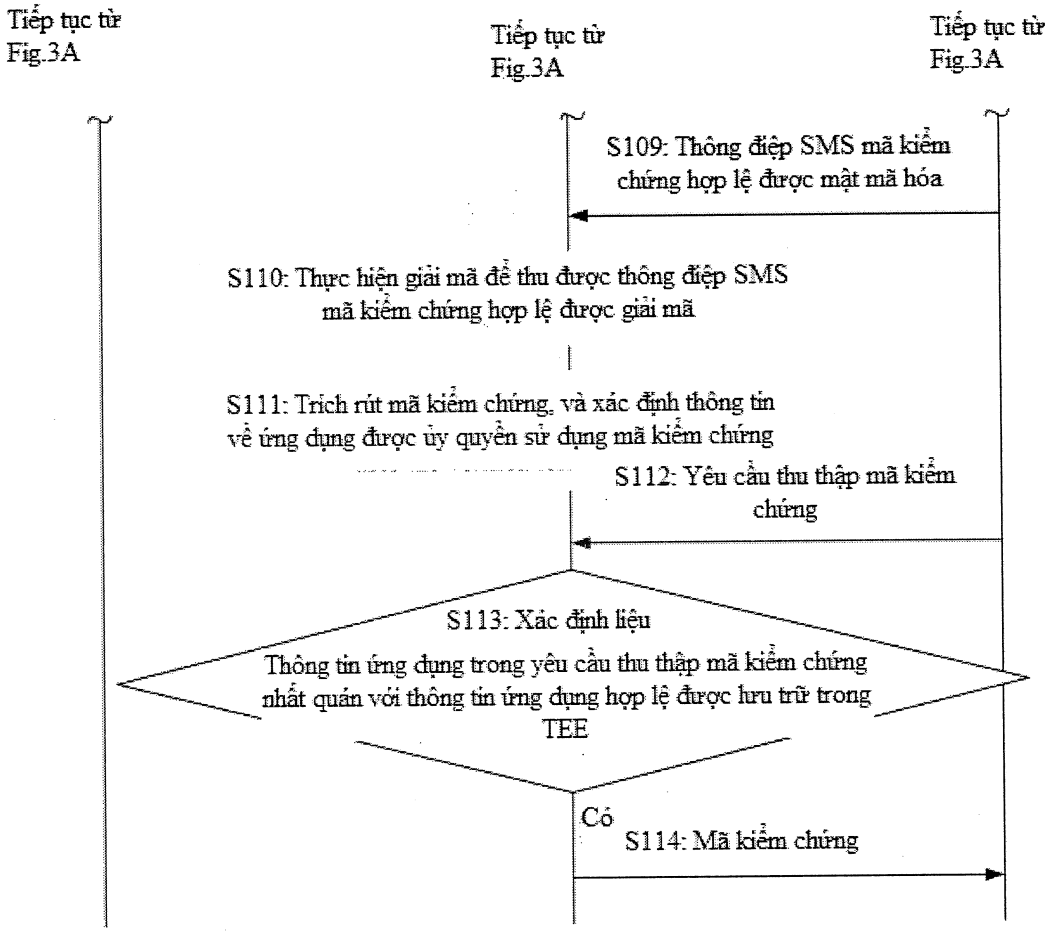

Tiếp tục từ
Fig.3A
Tiếp tục từ
Fig.3A
Tiếp tục từ
Fig.3A
S109: Thông điệp SMS mã kiểm chứng hợp lệ được mật mã hóa
S110: Thực hiện giải mã để thu được thông điệp SMS mã kiểm chứng hợp lệ được giải mã
S111: Trích rút mã kiểm chứng, và xác định thông tin về ứng dụng được ủy quyền sử dụng mã kiểm chứng
S112: Yêu cầu thu thập mã kiểm chứng
S113: Xác định liệu
Thông tin ứng dụng trong yêu cầu thu thập mã kiểm chứng nhất quán với thông tin ứng dụng hợp lệ được lưu trữ trong TEE
Có
S114: Mã kiểm chứng

Fig.3B

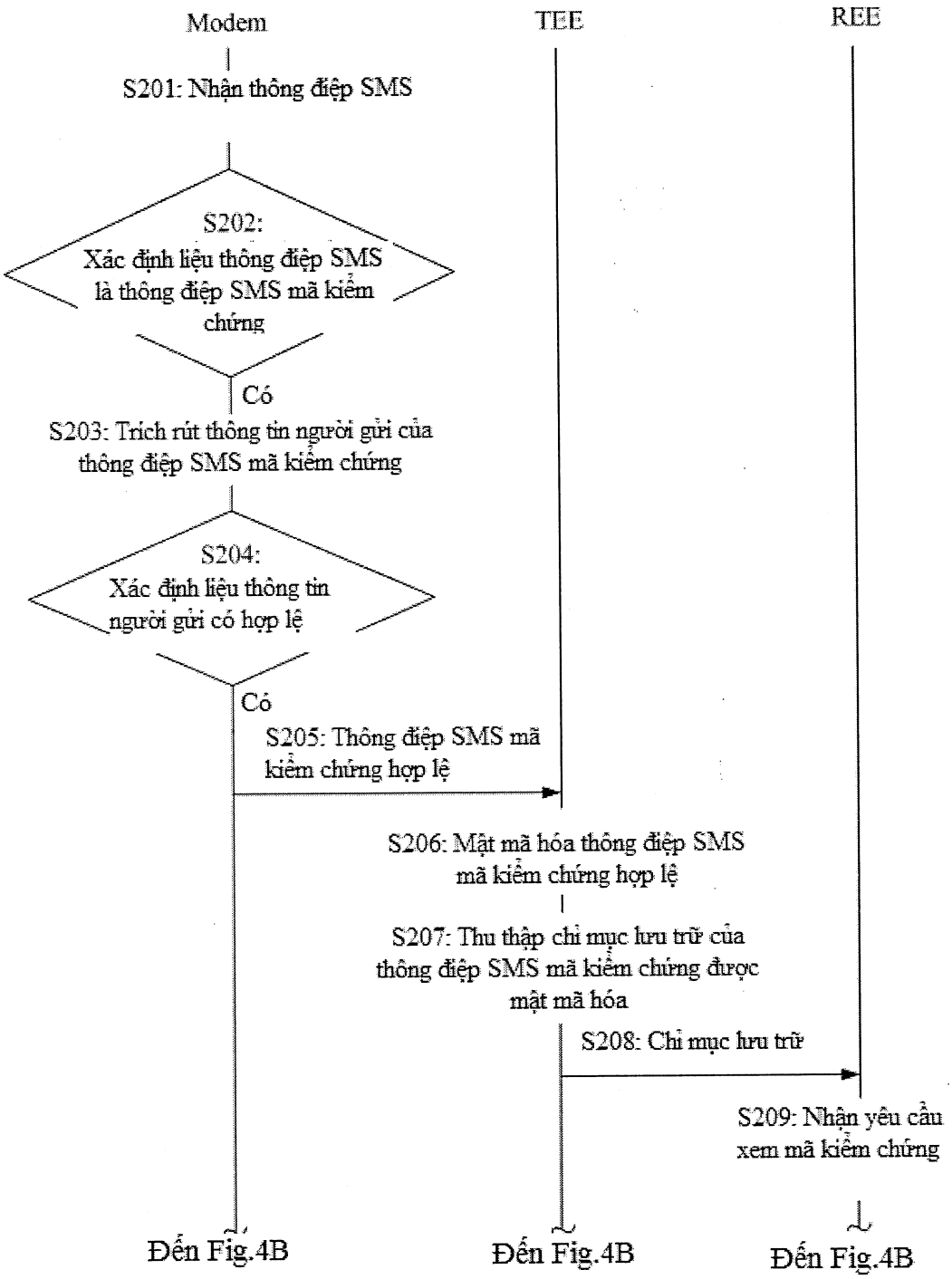

Modem
TEE
REE
S201: Nhận thông điệp SMS
S202: Xác định liệu thông điệp SMS là thông điệp SMS mã kiểm chứng
Có
S203: Trích rút thông tin người gửi của thông điệp SMS mã kiểm chứng
S204: Xác định liệu thông tin người gửi có hợp lệ
Có
S205: Thông điệp SMS mã kiểm chứng hợp lệ
S206: Mật mã hóa thông điệp SMS mã kiểm chứng hợp lệ
S207: Thu thập chỉ mục lưu trữ của thông điệp SMS mã kiểm chứng được mật mã hóa
S208: Chỉ mục lưu trữ
S209: Nhận yêu cầu xem mã kiểm chứng
Đến Fig.4B
Đến Fig.4B
Đến Fig.4B

Fig.4A

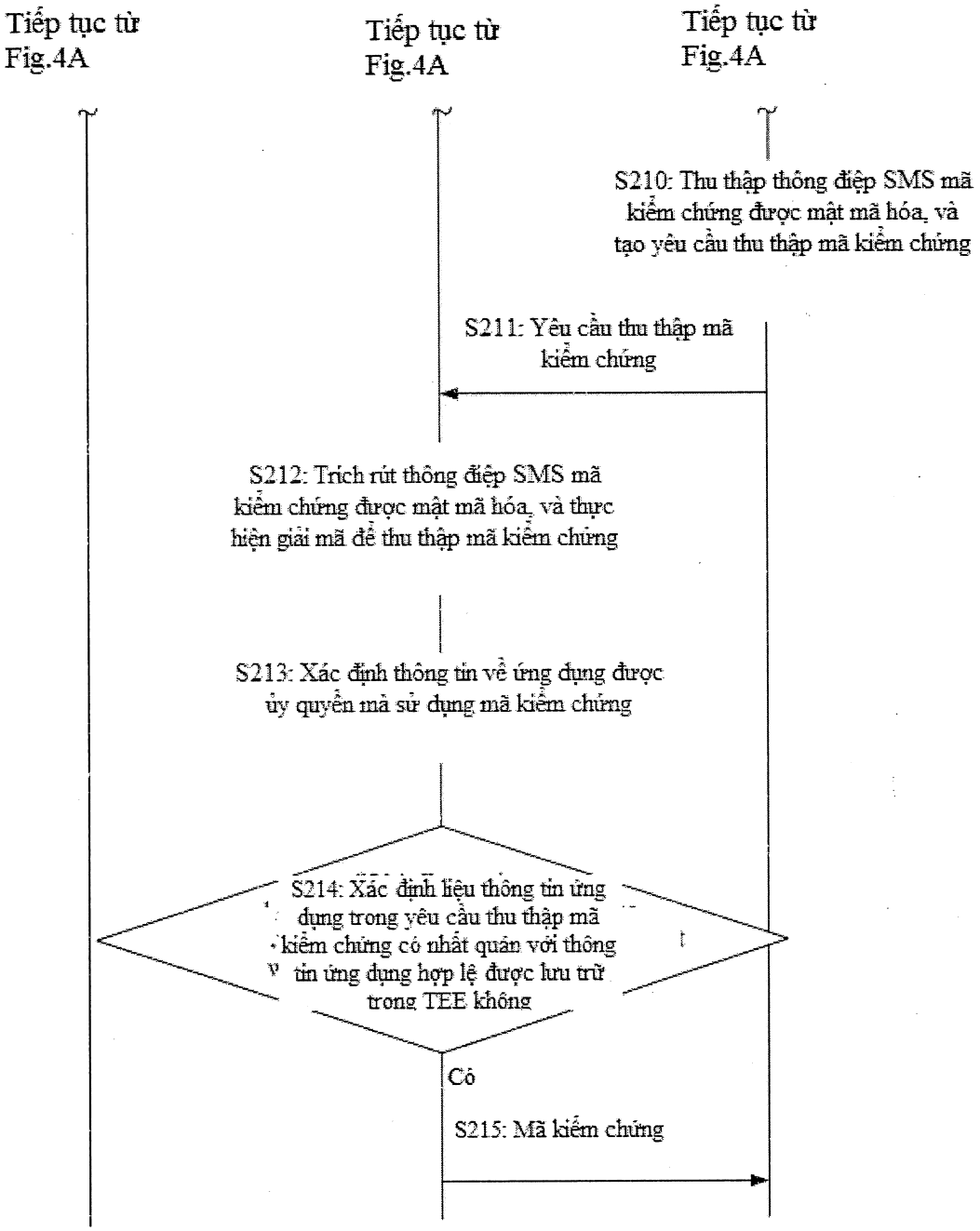

Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
S210: Thu thập thông điệp SMS mã kiểm chứng được mật mã hóa, và tạo yêu cầu thu thập mã kiểm chứng
S211: Yêu cầu thu thập mã kiểm chứng
S212: Trích rút thông điệp SMS mã kiểm chứng được mật mã hóa, và thực hiện giải mã để thu thập mã kiểm chứng
S213: Xác định thông tin về ứng dụng được ủy quyền mà sử dụng mã kiểm chứng
S214: Xác định liệu thông tin ứng dụng trong yêu cầu thu thập mã kiểm chứng có nhất quán với thông tin ứng dụng hợp lệ được lưu trữ trong TEE không
Có
S215: Mã kiểm chứng

Fig.4B

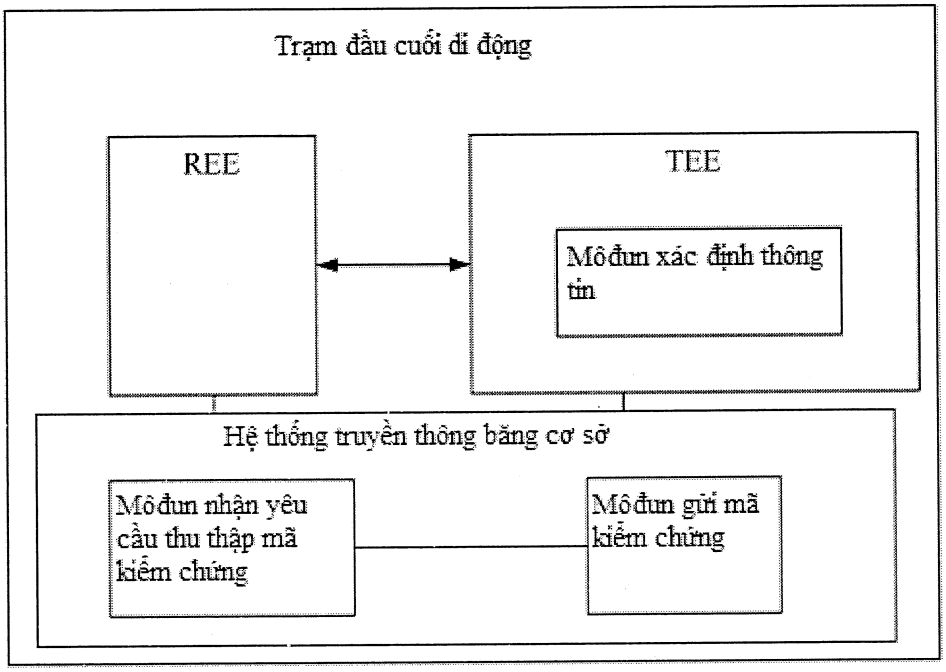

Trạm đầu cuối di động
REE
TEE
Môđun xác định thông tin
Hệ thống truyền thông băng cơ sở
Môđun nhận yêu cầu thu thập mã kiểm chứng
Môđun gửi mã kiểm chứng

Fig.5

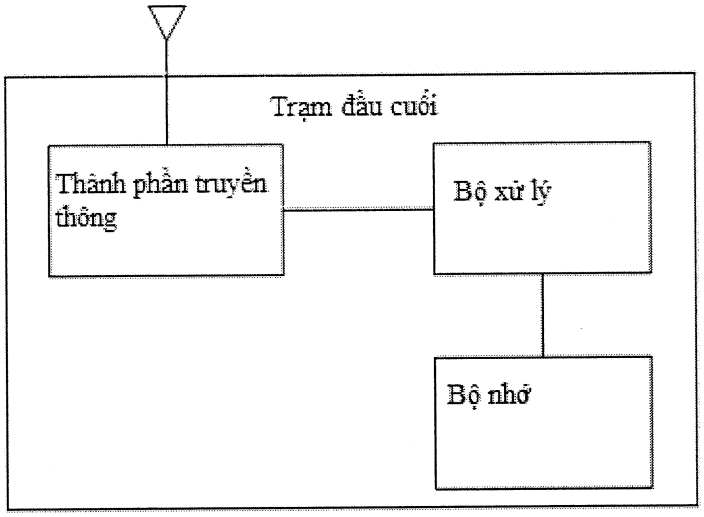

Trạm đầu cuối
Thành phần truyền thông
Bộ xử lý
Bộ nhớ

Fig.6