(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) **1-0036152**

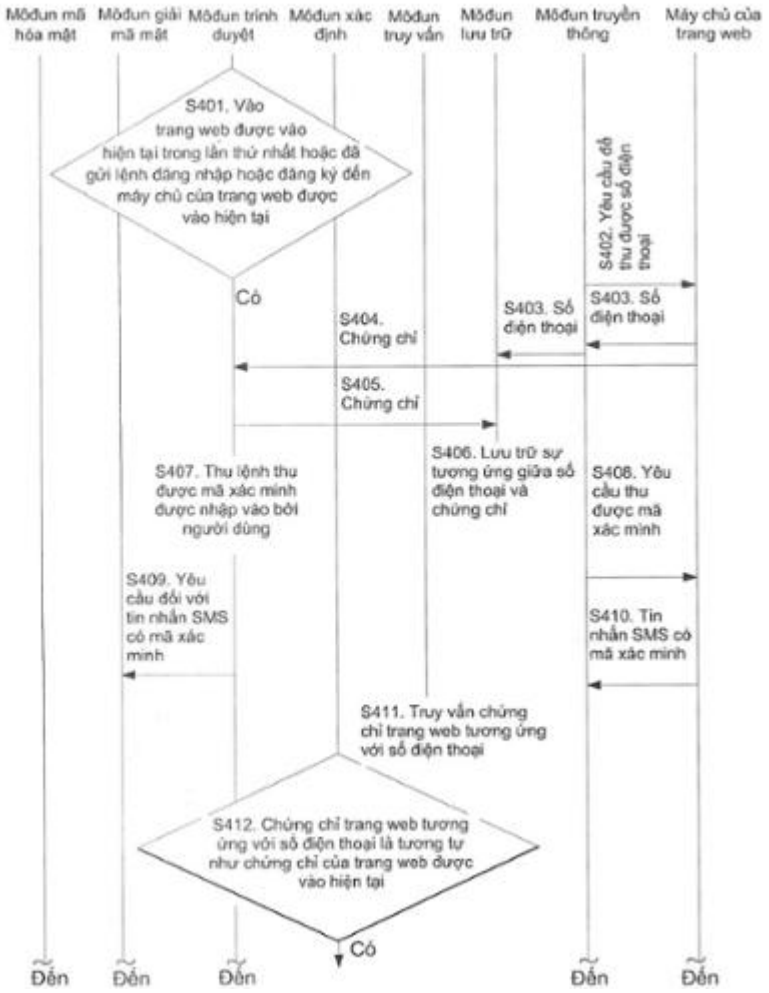
(51)[7] **H04L 29/06**

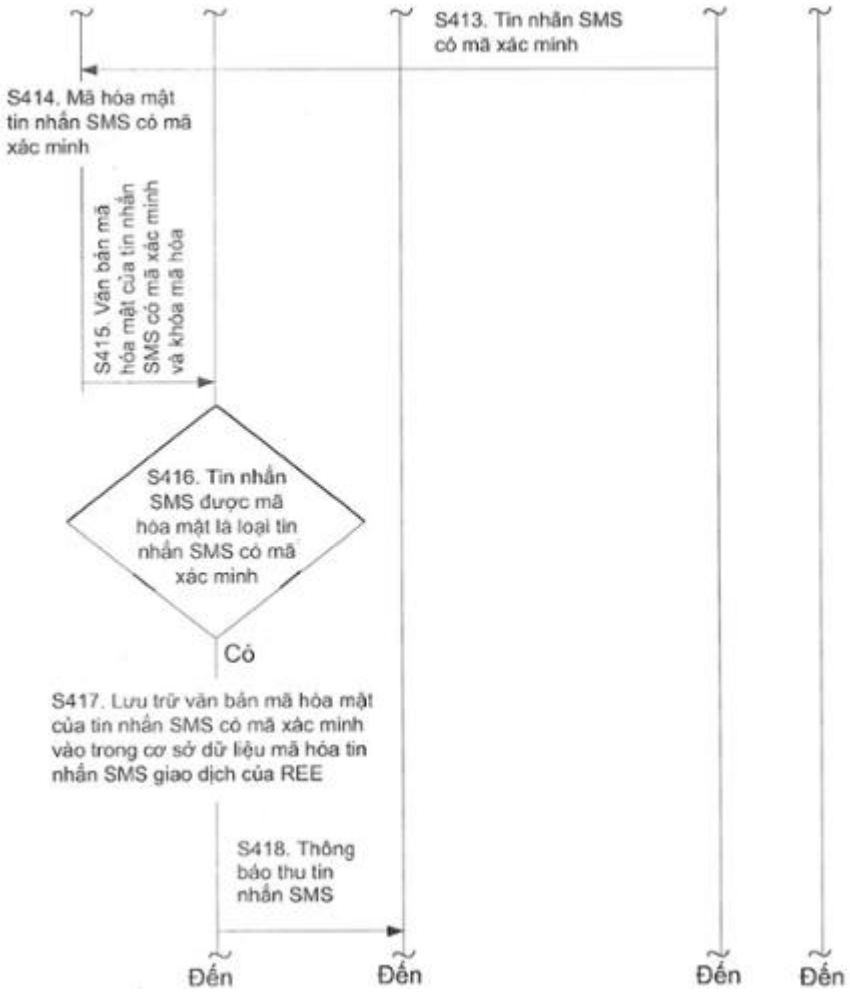
(13) **B**

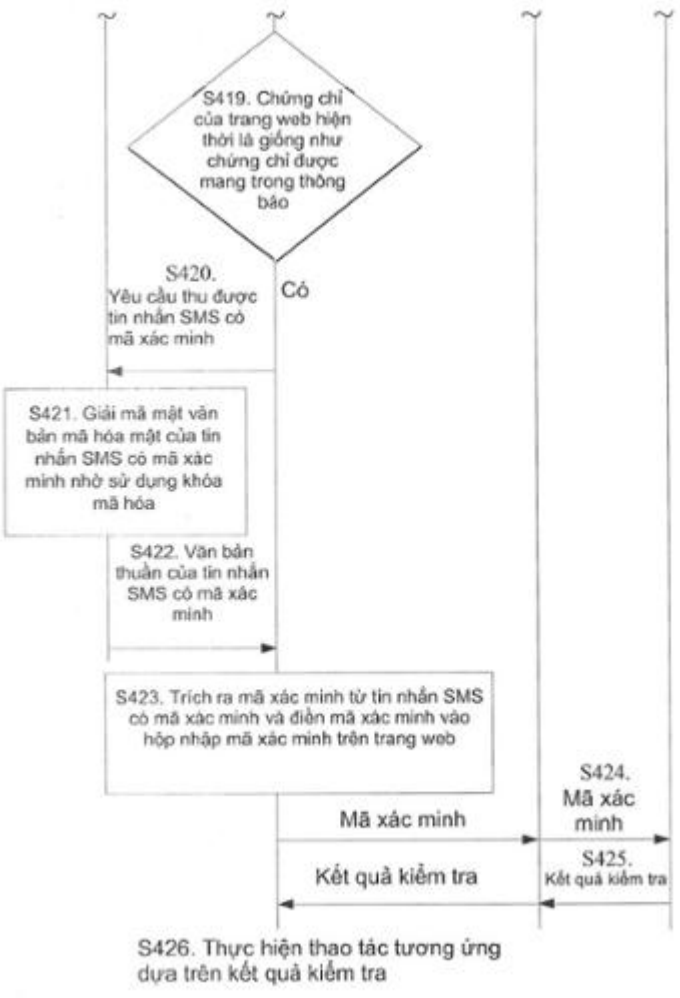
(21) 1-2019-00859
(22) 13/07/2017
(86) PCT/CN2017/092863 13/07/2017
(87) WO 2018/019134 01/02/2018
(30) 201610615989.6 29/07/2016 CN
(45) 26/06/2023 423
(43) 27/05/2019 374A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) LI, Ru (CN); PENG, Feng (CN); WANG, Zi (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP XỬ LÝ TIN NHẮN SMS (DỊCH VỤ TIN NHẮN NGẮN) CÓ MÃ XÁC MINH VÀ THIẾT BỊ ĐẦU CUỐI

(57) Sáng chế đề cập đến phương pháp xử lý tin nhắn SMS (dịch vụ tin nhắn ngắn - Short Message Service) có mã xác minh và thiết bị đầu cuối. Thiết bị đầu cuối thu tin nhắn SMS có mã xác minh mà bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; truy vấn, dựa trên sự tương ứng giữa thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; thu được văn bản mã hóa mật bằng cách mã hóa mật mật tin nhắn SMS có mã xác minh trong môi trường thực hiện tin cậy (TEE-Trusted execution environment) khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại; và thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong môi trường thực hiện đầy đủ (REE-Rich execution environment). Có thể được hiểu rằng, sau khi thu tin nhắn SMS có mã xác minh, thiết bị đầu cuối không trực tiếp phân tích mã xác minh từ tin nhắn SMS có mã xác minh, mà thu được mã xác minh chỉ khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng hiện đang vào. Ngoài ra, thiết bị đầu cuối thu được mã xác minh theo cách mã hóa mật tin nhắn SMS có mã xác minh trong TEE trước tiên và sau đó giải mã mật văn bản mã hóa mật trong REE. Theo cách này, độ bảo mật là cao hơn.


Môđun mã hóa mật
Môđun giải mã mật
Môđun trình duyệt
Môđun xác định
Môđun truy vấn
Môđun lưu trữ
Môđun truyền thông
Máy chủ của trang web
S401. Vào trang web được vào hiện tại trong lần thứ nhất hoặc đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang web được vào hiện tại
Có
S402. Yêu cầu để thu được số điện thoại
S403. Số điện thoại
S403. Số điện thoại
S404. Chứng chỉ
S405. Chứng chỉ
S406. Lưu trữ sự tương ứng giữa số điện thoại và chứng chỉ
S407. Thu lệnh thu được mã xác minh được nhập vào bởi người dùng
S408. Yêu cầu thu được mã xác minh
S409. Yêu cầu đối với tin nhắn SMS có mã xác minh
S410. Tin nhắn SMS có mã xác minh
S411. Truy vấn chứng chỉ trang web tương ứng với số điện thoại
S412. Chứng chỉ trang web tương ứng với số điện thoại là tương tự như chứng chỉ của trang web được vào hiện tại
Có
Đến
Đến
Đến
Đến
Đến


S413. Tin nhắn SMS có mã xác minh
S414. Mã hóa mật tin nhắn SMS có mã xác minh
S415. Văn bản mã hóa mật của tin nhắn SMS có mã xác minh và khóa mã hóa
S416. Tin nhắn SMS được mã hóa mật là loại tin nhắn SMS có mã xác minh
Có
S417. Lưu trữ văn bản mã hóa mật của tin nhắn SMS có mã xác minh vào trong cơ sở dữ liệu mã hóa tin nhắn SMS giao dịch của REE
S418. Thông báo thu tin nhắn SMS
Đến
Đến
Đến
Đến


S419. Chứng chỉ của trang web hiện thời là giống như chứng chỉ được mang trong thông báo
Có
S420. Yêu cầu thu được tin nhắn SMS có mã xác minh
S421. Giải mã mật văn bản mã hóa mật của tin nhắn SMS có mã xác minh nhờ sử dụng khóa mã hóa
S422. Văn bản thuần của tin nhắn SMS có mã xác minh
S423. Trích ra mã xác minh từ tin nhắn SMS có mã xác minh và điền mã xác minh vào hộp nhập mã xác minh trên trang web
Mã xác minh
S424. Mã xác minh
Kết quả kiểm tra
S425. Kết quả kiểm tra
S426. Thực hiện thao tác tương ứng dựa trên kết quả kiểm tra

**Lĩnh vực kỹ thuật được đề cập**

Sáng chế đề cập đến lĩnh vực truyền thông, và cụ thể, sáng chế đề cập đến phương pháp xử lý tin nhắn SMS (Dịch vụ tin nhắn ngắn-Short Message Service) có mã xác minh và thiết bị đầu cuối.

**Tình trạng kỹ thuật của sáng chế**

Với sự xuất hiện của công nghệ thanh toán di động, độ bảo mật của việc thanh toán di động đang thu hút sự quan tâm. Việc đăng nhập bằng mật mã thông thường không thể đáp ứng yêu cầu bảo mật khi thanh toán di động, và mã xác minh qua SMS trở thành cách thức thường được sử dụng để nâng cao độ bảo mật.

Hiện nay, để đạt được mục đích là trình duyệt tự động thu được mã xác minh, khi thiết bị đầu cuối nhận tin nhắn SMS có mã xác minh, trình duyệt tự động phân tích tin nhắn SMS có mã xác minh và thu được mã xác minh từ tin nhắn SMS có mã xác minh.

Tuy nhiên, cách tự động thu được mã xác minh từ tin nhắn SMS có mã xác minh có độ bảo mật thấp.

**Bản chất kỹ thuật của sáng chế**

Sáng chế đề xuất phương pháp xử lý tin nhắn SMS có mã xác minh và thiết bị đầu cuối để giải quyết vấn đề về độ bảo mật thấp của cách mà thiết bị đầu cuối tự động thu được mã xác minh.

Để đạt được mục đích nêu trên, sáng chế đề xuất giải pháp kỹ thuật dưới đây:

Khía cạnh thứ nhất của sáng chế đề xuất phương pháp xử lý tin nhắn SMS có mã xác minh bao gồm các bước: thu, bởi thiết bị đầu cuối, tin nhắn SMS có mã xác minh mà bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa

thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi tin nhắn SMS có mã xác minh; thu được, bởi thiết bị đầu cuối, văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong môi trường thực hiện tin cậy (TEE) khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng (web) hiện đang vào bởi thiết bị đầu cuối; và thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong môi trường thực hiện đầy đủ (REE). Có thể được hiểu rằng, so với kỹ thuật đã biết, sau khi thu tin nhắn SMS có mã xác minh, thiết bị đầu cuối không trực tiếp phân tích mã xác minh từ tin nhắn SMS có mã xác minh, mà thu được mã xác minh chỉ khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng hiện đang vào bởi thiết bị đầu cuối. Ngoài ra, trước hết thiết bị đầu cuối thu được mã xác minh theo cách mã hóa mật tin nhắn SMS có mã xác minh trong TEE và sau đó giải mã mật văn bản mã hóa mật trong REE. Theo cách này, độ bảo mật là cao hơn.

Khía cạnh thứ hai của sáng chế đề xuất thiết bị đầu cuối bao gồm môđun truyền thông, môđun truy vấn, môđun mã hóa mật, và môđun thu được mã xác minh. Môđun truyền thông được tạo cấu hình để thu tin nhắn SMS có mã xác minh mà bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh. Môđun truy vấn được tạo cấu hình để truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh. Môđun mã hóa mật được tạo cấu hình để thu được văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong môi trường thực hiện tin cậy (TEE) khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối. Môđun thu được mã xác minh được tạo cấu hình để thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong môi trường thực hiện đầy đủ (REE). Thiết bị đầu cuối thu được mã xác minh chỉ khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ

của trang mạng được vào hiện tại bởi thiết bị đầu cuối. Ngoài ra, trước hết thiết bị đầu cuối thu được mã xác minh theo cách mã hóa mật tin nhắn SMS có mã xác minh trong TEE và sau đó giải mã mật văn bản mã hóa mật trong REE. Theo cách này, độ bảo mật là cao hơn.

Theo cách thức thực hiện, môđun truyền thông và môđun truy vấn được bố trí trong hệ thống truyền thông dải cơ sở. Hệ thống truyền thông dải cơ sở là hệ thống nền được sử dụng bởi thiết bị đầu cuối để truyền thông với thiết bị khác. Vì vậy, ưu điểm lưu trữ sự tương ứng và xác định liệu các chứng chỉ có được khớp với nhau trong hệ thống xử lý dải cơ sở hay không đó là ứng dụng lớp bên trên không cần tham gia vào việc truy vấn và xác định, nghĩa là, ứng dụng lớp bên trên không nhạy cảm. Theo cách này, xác suất can thiệp vào việc xác định nhờ sử dụng phần mềm ứng dụng có thể được giảm đi.

Theo cách thức thực hiện, môđun thu được mã xác minh bao gồm môđun giải mã mật và môđun trình duyệt. Môđun giải mã mật được tạo cấu hình để: khi loại văn bản mã hóa mật là tin nhắn SMS có mã xác minh, thu được tin nhắn SMS có mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE nhờ sử dụng khóa thu được từ TEE. Môđun trình duyệt được tạo cấu hình để thu được tin nhắn SMS có mã xác minh và thu được mã xác minh từ tin nhắn SMS có mã xác minh.

Theo cách thức thực hiện, cách thức thực hiện cụ thể trong đó môđun trình duyệt thu được tin nhắn SMS có mã xác minh là: thu được tin nhắn SMS có mã xác minh nhờ sử dụng giao diện bảo mật, để cải thiện độ bảo mật.

Theo cách thức thực hiện, môđun giải mã mật còn được tạo cấu hình để gửi thông báo cho môđun trình duyệt sau khi thu được tin nhắn SMS có mã xác minh, trong đó thông báo mang thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh. Cách thức thực hiện cụ thể trong đó môđun trình duyệt thu được mã xác minh từ tin nhắn SMS có mã xác minh là: thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ của trang mạng hiện đang vào khớp với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh. Sau khi môđun giải mã mật gửi thông báo đến môđun trình duyệt, môđun trình duyệt

thực hiện lại việc xác minh, sao cho môđun trình duyệt xác định lại xem liệu trang mạng được vào hiện tại là trang mạng mà cần được xác minh hay không, để cải thiện hơn nữa độ bảo mật.

Theo cách thức thực hiện, cách thức thực hiện cụ thể của bước thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE là: nếu được xác định rằng loại của văn bản mã hóa mật là tin nhắn SMS có mã xác minh, thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE bằng cách sử dụng khóa thu được từ TEE. Mục đích trước hết là xác định rằng loại của văn bản mã hóa mật là tin nhắn SMS có mã xác minh và sau đó giải mã mật văn bản mã hóa mật là để tránh quy trình giải mã mật không cần thiết và tiết kiệm tài nguyên.

Khía cạnh thứ ba của sáng chế đề xuất phương pháp xử lý tin nhắn SMS có mã xác minh, bao gồm các bước dưới đây: thu, bởi thiết bị đầu cuối, tin nhắn SMS có mã xác minh, trong đó tin nhắn SMS có mã xác minh bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; truy vấn, bởi thiết bị đầu cuối dựa trên sự tương ứng đã được lưu trữ giữa thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; và thu được, bởi thiết bị đầu cuối, mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối. So với kỹ thuật đã biết, sau khi thu tin nhắn SMS có mã xác minh, thiết bị đầu cuối không trực tiếp phân tích mã xác minh từ tin nhắn SMS có mã xác minh, mà thu được mã xác minh chỉ khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối. Theo cách này, độ bảo mật là cao hơn.

Khía cạnh thứ tư của sáng chế đề xuất thiết bị đầu cuối, bao gồm môđun truyền thông, môđun truy vấn, và môđun thu được mã xác minh. Môđun truyền thông được tạo cấu hình để thu tin nhắn SMS có mã xác minh, trong đó tin nhắn SMS có mã xác minh bao gồm thông tin nhận dạng người gửi của tin nhắn SMS

có mã xác minh. Môđun truy vấn được tạo cấu hình để truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh. Môđun thu được mã xác minh được tạo cấu hình để thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối.

Theo cách thức thực hiện, môđun thu được mã xác minh bao gồm môđun xác định và môđun trình duyệt. Môđun xác định được tạo cấu hình để xác định liệu chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối hay không. Môđun trình duyệt được tạo cấu hình để thu được tin nhắn SMS có mã xác minh và thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối.

Theo cách thức thực hiện, môđun xác định còn được tạo cấu hình để gửi thông báo đến môđun trình duyệt trước khi xác định liệu chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối hay không, trong đó thông báo mang chứng chỉ tương ứng với thông tin nhận dạng người gửi. Môđun trình duyệt còn được tạo cấu hình để gửi chứng chỉ của trang mạng hiện đang vào đến môđun xác định khi chứng chỉ tương ứng với thông tin nhận dạng người gửi khớp với chứng chỉ của trang mạng hiện đang vào.

Theo cách thức thực hiện, trước khi tin nhắn SMS có mã xác minh được thu, thiết bị đầu cuối còn bao gồm: gửi yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại khi được xác định rằng thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần thứ nhất hoặc đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại. Thiết bị đầu cuối thu thông tin nhận

dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào mà được gửi bởi máy chủ của trang mạng được vào hiện tại, và lưu trữ sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào. Vào trang mạng được vào hiện tại trong lần thứ nhất hoặc đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại chỉ báo rằng thiết bị đầu cuối có xác suất thu được mã xác minh. Yêu cầu thu được được gửi chỉ khi có xác suất thu được mã xác minh, để tiết kiệm tài nguyên.

**Mô tả vắn tắt các hình vẽ**

Để mô tả các giải pháp kỹ thuật theo các phương án của sáng chế hoặc theo kỹ thuật đã biết rõ ràng hơn, phần dưới đây mô tả vắn tắt các hình vẽ kèm theo đối với các phương án của kỹ thuật đã biết. Hiển nhiên là, các hình vẽ kèm theo trong phần mô tả dưới đây thể hiện một số phương án của sáng chế, và người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể vẫn suy ra các hình vẽ khác từ các hình vẽ này mà không cần các nỗ lực sáng tạo.

FIG.1 là hình vẽ dạng sơ đồ của thiết bị đầu cuối;

FIG.2A và FIG.2B là các lưu đồ về phương pháp xử lý tin nhắn SMS có mã xác minh theo phương án của sáng chế;

FIG.3 là hình vẽ dạng sơ đồ của thiết bị đầu cuối theo phương án của sáng chế;

FIG.4A, FIG.4B, và FIG.4C là các lưu đồ thực hiện quy trình xử lý tin nhắn SMS có mã xác minh bởi thiết bị đầu cuối theo phương án của sáng chế;

FIG.5 là sơ đồ thiết đặt API mở tin nhắn SMS có mã xác minh trong thiết bị đầu cuối theo phương án của sáng chế;

FIG.6A và FIG.6B là sơ đồ ví dụ về giao diện để thực hiện quy trình xử lý tin nhắn SMS có mã xác minh bởi thiết bị đầu cuối theo phương án của sáng chế;

FIG.7 là lưu đồ thể hiện phương pháp xử lý tin nhắn SMS có mã xác minh khác theo phương án của sáng chế;

FIG.8 là hình vẽ dạng sơ đồ thể hiện thiết bị đầu cuối khác theo phương án của sáng chế;

FIG.9A và FIG.9B là các lưu đồ khác thực hiện quy trình xử lý tin nhắn SMS có mã xác minh bởi thiết bị đầu cuối theo phương án của sáng chế; và

FIG.10 là hình vẽ dạng sơ đồ của thiết bị đầu cuối khác theo phương án của sáng chế.

**Mô tả chi tiết sáng chế**

FIG.1 thể hiện thiết bị đầu cuối. Để cải thiện độ bảo mật, hai môi trường được thiết đặt trên thiết bị đầu cuối: môi trường thực hiện đầy đủ (Môi trường thực hiện đầy đủ, REE) mà sự vận hành của môi trường này có khả năng xử lý mạnh và chức năng đa phương tiện, như môi trường Android, và môi trường thực hiện tin cậy (Trusted Executive Environment, TEE). Hệ điều hành có thể chạy trong môi trường Android, và tin nhắn SMS APK (Tiếng Anh: Android Package) chạy trong hệ điều hành.

TEE là môi trường đang chạy cùng tồn tại với REE trên thiết bị đầu cuối. Liên quan đến REE, TEE là vùng đảm bảo trong bộ xử lý chính và đảm bảo rằng dữ liệu nhạy được lưu trữ, được xử lý, và được bảo vệ trong môi trường tin cậy, để cung cấp dịch vụ bảo mật cho hệ điều hành REE. TEE có khoảng trống thực hiện của riêng nó và có mực độ bảo mật cao hơn so với hệ điều hành REE có. TEE không phải là chip bảo mật vật lý độc lập mà là kiến trúc bảo mật mà xếp chồng với kiến trúc phần cứng của bộ xử lý ứng dụng được sử dụng hiện thời. Các tài nguyên phần mềm và phần cứng mà có thể được truy cập bởi TEE tách biệt từ hệ điều hành REE, và phần cứng được hỗ trợ sự cách ly được bố trí. Chương trình ứng dụng tin cậy chạy trong TEE và tách biệt với hệ điều hành REE, để ngăn ngừa sự tấn công bằng phần mềm độc hại.

Trong quy trình vào trang mạng, thiết bị đầu cuối có thể cần được xác minh bởi máy chủ của trang mạng. Cụ thể, thiết bị đầu cuối thu tin nhắn SMS có mã xác minh được gửi bởi máy chủ của trang mạng, thu được mã xác minh từ tin nhắn SMS có mã xác minh, và gửi mã xác minh đến máy chủ của trang mạng,

và máy chủ của trang mạng xác minh mã xác minh.

Phương pháp xử lý tin nhắn SMS có mã xác minh được cung cấp trong ứng dụng này được áp dụng vào thiết bị đầu cuối được thể hiện trên FIG.1, để cải thiện độ bảo mật khi thiết bị đầu cuối thu được mã xác minh từ tin nhắn SMS có mã xác minh đã được thu.

FIG.2A và FIG.2B thể hiện thủ tục của phương pháp xử lý tin nhắn SMS có mã xác minh theo phương án của sáng chế. Phương pháp bao gồm các bước dưới đây:

S201. Thiết bị đầu cuối xác định liệu thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần thứ nhất hay liệu thiết bị đầu cuối đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại. Nếu có, thực hiện S202; nếu không, không thực hiện quy trình xử lý hoặc thực hiện đều đặn S201.

Bước vào trang mạng được vào hiện tại trong lần thứ nhất hoặc đã gửi lệnh truy cập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại nghĩa là thiết bị đầu cuối có xác suất thu được tin nhắn SMS có mã xác minh từ máy chủ của trang mạng được vào hiện tại. Nghĩa là, S201 là quy trình trong đó thiết bị đầu cuối xác định trước liệu thiết bị đầu cuối có xác suất thu được tin nhắn SMS có mã xác minh hay không.

Cần lưu ý rằng thiết bị đầu cuối xác định liệu thiết bị đầu cuối có xác suất thu được tin nhắn SMS có mã xác minh hay không chỉ là cách tùy ý để tiết kiệm tài nguyên và được nhằm mục đích để tiết kiệm tài nguyên. Theo cách khác, S201 có thể không được thực hiện và S202 được thực hiện trực tiếp.

S202. Thiết bị đầu cuối gửi yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại.

Cụ thể, thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có thể là số điện thoại được sử dụng để gửi tin nhắn SMS có mã xác minh, hoặc thông tin (bao gồm nhưng không bị giới hạn ở tên của công ty) về công ty liên

quan của trang mạng, hoặc số điện thoại được sử dụng để gửi tin nhắn SMS có mã xác minh và thông tin về công ty liên quan của trang mạng.

Ví dụ, đối với trang mạng chính thức của ngân hàng Trung Quốc, thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có thể là số điện thoại dịch vụ khách hàng 95566 của ngân hàng Trung Quốc và tên: Ngân hàng Trung Quốc.

S203. Thiết bị đầu cuối thu thông tin nhận dạng người gửi mà của tin nhắn SMS có mã xác minh và mà được gửi bởi máy chủ của trang mạng được vào hiện tại.

S204. Thiết bị đầu cuối thu được chứng chỉ của trang mạng được vào hiện tại.

S204 cũng có thể được thực hiện trước S201, S202, hoặc S203.

S205. Thiết bị đầu cuối lưu trữ sự tương ứng giữa chứng chỉ của trang mạng hiện đang vào và thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh.

Phần nêu trên là quy trình trong đó thiết bị đầu cuối đăng ký sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và trang chứng chỉ mạng (web). Sự tương ứng đã được lưu trữ được sử dụng làm cơ sở để xác định liệu có thu được mã xác minh từ tin nhắn SMS có mã xác minh hay không.

S206. Thiết bị đầu cuối gửi yêu cầu thu được mã xác minh đến máy chủ của trang mạng được vào hiện tại.

Cụ thể, thiết bị đầu cuối có thể gửi yêu cầu thu được mã xác minh đến máy chủ của trang mạng được vào hiện tại dựa trên thao tác của người dùng. Ví dụ, người dùng đăng ký trên trang mạng chính thức của ngân hàng Trung Quốc bằng cách sử dụng thiết bị đầu cuối, và nhấp chuột vào nút "thu được mã xác minh" dựa trên thông tin phản hồi trên trang mạng chính thức của ngân hàng Trung Quốc, kích hoạt thiết bị đầu cuối gửi yêu cầu thu được mã xác minh đến máy chủ của trang mạng chính thức của ngân hàng Trung Quốc.

S207. Thiết bị đầu cuối thu tin nhắn SMS có mã xác minh được gửi bởi máy chủ của trang mạng.

Thông thường, tin nhắn SMS có mã xác minh bao gồm mã xác minh, số điện thoại để gửi tin nhắn SMS có mã xác minh, và tên doanh nghiệp.

S208. Thiết bị đầu cuối truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi (số điện thoại và/hoặc tên doanh nghiệp) của tin nhắn SMS có mã xác minh được thu trong S207.

S209. Thiết bị đầu cuối xác định liệu chứng chỉ đã được tìm ra có khớp với chứng chỉ của trang mạng hiện đang vào hay không. Nếu khớp nhau, thực hiện S210; hoặc nếu không khớp nhau, xử lý tin nhắn SMS có mã xác minh dựa trên thủ tục xử lý tin nhắn SMS hiện có.

Điều cần được lưu ý là theo phương án này, "khớp nhau" nghĩa là trường hợp tương tự hoặc đặc biệt tương tự. Đặc biệt tương tự nghĩa là hai chứng chỉ thể hiện cùng trang mạng.

S210. Thiết bị đầu cuối thu được văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong TEE.

Cụ thể, ứng dụng được tin cậy (Trusted Application, TA) có thể được sử dụng trong TEE để mã hóa mật tin nhắn SMS có mã xác minh.

Bởi vì TEE có độ bảo mật cao hơn, tin nhắn SMS có mã xác minh văn bản mã hóa mật thu được trong TEE có độ bảo mật cao hơn.

S211. Thiết bị đầu cuối xác định, trong REE, liệu loại của văn bản mã hóa mật là tin nhắn SMS có mã xác minh hay không. Nếu có, thực hiện S212; hoặc nếu không, thực hiện quy trình xử lý dựa trên thủ tục xử lý tin nhắn SMS hiện có.

S212. Thiết bị đầu cuối thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE.

S213. Thiết bị đầu cuối gửi mã xác minh đến máy chủ của trang mạng để

xác minh.

Có thể được hiểu từ quy trình được thể hiện trên FIG.2A và FIG.2B rằng theo phương án này, thiết bị đầu cuối thu được mã xác minh từ tin nhắn SMS có mã xác minh chỉ khi chứng chỉ tương ứng với người gửi của mã xác minh khớp với chứng chỉ đã được đăng ký cục bộ. So với kỹ thuật đã biết rằng mã xác minh thu được một cách tự động đối với tin nhắn SMS có mã xác minh bất kỳ, sự tấn công được thực hiện bằng cách sử dụng tin nhắn SMS có mã xác minh (ví dụ, sau khi tin nhắn SMS có mã xác minh bị chặn, số điện thoại được thay đổi, và sau đó mã xác minh bị chặn) có thể được ngăn ngừa một cách hiệu quả, và độ bảo mật là cao hơn.

FIG.3 thể hiện cấu trúc cụ thể của thiết bị đầu cuối được thể hiện trên FIG.1. Thiết bị đầu cuối bao gồm môđun truyền thông, môđun truy vấn, môđun mã hóa mật, môđun giải mã mật, môđun trình duyệt, môđun xác định, và môđun lưu trữ. Cụ thể, môđun mã hóa mật có thể được bố trí trong TEE, và môđun truyền thông, môđun lưu trữ, môđun truy vấn, và môđun xác định có thể được bố trí trong hệ thống truyền thông dải cơ sở của thiết bị đầu cuối. Môđun trình duyệt và môđun giải mã mật có thể được bố trí trong REE. Môđun giải mã mật và môđun trình duyệt tạo nên theo cách liên kết môđun thu được mã xác minh.

FIG.4A, FIG.4B, và FIG.4C thể hiện thủ tục trong đó các môđun trong thiết bị đầu cuối được thể hiện trên FIG.3 phối hợp để thu được mã xác minh. Thu tục bao gồm các bước dưới đây:

S401. Môđun trình duyệt xác định liệu thiết bị đầu cuối có vào trang mạng được vào hiện tại trong lần thứ nhất hay không hoặc liệu thiết bị đầu cuối đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không. Nếu có, thực hiện S402; hoặc nếu không, không thực hiện quy trình xử lý hoặc thực hiện một cách đều đặn S401.

S402. Môđun truyền thông gửi yêu cầu để thu được số điện thoại (theo phương án này, rằng thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh là số điện thoại được sử dụng làm ví dụ) đến máy chủ của trang mạng.

S403. Môđun truyền thông thu số điện thoại mà có thể gửi tin nhắn SMS có mã xác minh và được truyền bởi máy chủ của trang mạng, và gửi số điện thoại đến môđun lưu trữ.

S404. Môđun trình duyệt thu được chứng chỉ của trang mạng được vào hiện tại.

S405. Môđun trình duyệt gửi chứng chỉ thu được đến môđun lưu trữ.

S406. Môđun lưu trữ lưu trữ sự tương ứng giữa số điện thoại và chứng chỉ.

Một cách tùy ý, hệ thống truyền thông dải cơ sở có thể lưu trữ danh sách trắng, và môđun lưu trữ lưu trữ sự tương ứng giữa số điện thoại và chứng chỉ vào trong danh sách trắng.

S401 đến S406 mô tả quy trình đăng ký của sự tương ứng giữa số điện thoại và chứng chỉ. So với quy trình được thể hiện trên FIG.2A và FIG.2B, theo phương án này, sự tương ứng giữa số điện thoại và chứng chỉ được lưu trữ trong hệ thống truyền thông dải cơ sở.

S407. Môđun trình duyệt thu mã xác minh thu được nhập theo lệnh bởi người dùng.

S408. Môđun truyền thông gửi yêu cầu thu được mã xác minh đến máy chủ của trang mạng được vào hiện tại.

S409. Môđun trình duyệt yêu cầu tin nhắn SMS có mã xác minh từ môđun giải mã mật.

S410. Môđun truyền thông thu tin nhắn SMS có mã xác minh được gửi bởi máy chủ của trang mạng.

S411. Môđun truy vấn truy vấn, dựa trên sự tương ứng giữa số điện thoại và chứng chỉ trang mạng, chứng chỉ trang mạng tương ứng với số điện thoại mà gửi tin nhắn SMS có mã xác minh và được bao gồm trong tin nhắn SMS có mã xác minh.

S412. Môđun xác định xác định liệu trang mạng chứng chỉ tương ứng với số điện thoại mà gửi tin nhắn SMS có mã xác minh là tương tự như chứng

chỉ của trang mạng được vào hiện tại bởi môđun trình duyệt hay không. Nếu có, thực hiện S413; hoặc nếu không, gửi tin nhắn SMS đến thiết bị liên quan trong môi trường REE, và thiết bị liên quan trong môi trường REE thực hiện quy trình xử lý dựa trên thủ tục xử lý tin nhắn SMS thông thường.

Hệ thống xử lý dải cơ sở là hệ thống nền được sử dụng bởi thiết bị đầu cuối để truyền thông với thiết bị khác. Vì vậy, ưu điểm lưu trữ sự tương ứng và xác định liệu các chứng chỉ có được khớp nhau hay không trong hệ thống xử lý dải cơ sở đó là ứng dụng lớp bên trên không cần tham gia vào việc truy vấn và xác định, nghĩa là, ứng dụng lớp bên trên là không nhạy cảm. Theo cách này, xác suất can thiệp vào việc xác định nhờ sử dụng phần mềm ứng dụng có thể được giảm đi.

S413. Môđun truyền thông gửi tin nhắn SMS có mã xác minh đến môđun mã hóa mật.

S414. Môđun mã hóa mật mã hóa mật tin nhắn SMS có mã xác minh. Cụ thể, môđun mã hóa mật có thể mã hóa mật tin nhắn SMS có mã xác minh nhờ sử dụng ứng dụng được tin cậy (Trusted Application, TA) trong TEE.

S415. Môđun mã hóa mật gửi văn bản mã hóa mật của tin nhắn SMS có mã xác minh và khóa mã hóa mật đến môđun giải mã mật.

Một cách tùy ý, khóa mã hóa mật là khóa dùng một lần, để cải thiện hơn nữa độ bảo mật của văn bản mã hóa mật của mã xác minh.

S416. Môđun giải mã mật giải mã mật văn bản mã hóa mật của tin nhắn SMS và phân tích văn bản, để xác định liệu tin nhắn SMS đã được mã hóa mật là của loại tin nhắn SMS có mã xác minh hay không. Nếu tin nhắn SMS đã được mã hóa mật là tin nhắn SMS có mã xác minh, thực hiện S417; nếu không phải (như tin nhắn SMS quảng cáo), thực hiện quy trình xử lý dựa trên thủ tục xử lý tin nhắn SMS hiện có.

S417. Môđun giải mã mật lưu trữ văn bản mã hóa mật của tin nhắn SMS có mã xác minh vào trong cơ sở dữ liệu mã hóa mật tin nhắn SMS giao dịch của REE.

S418. Môđun giải mã mật gửi thông báo đã thu tin nhắn SMS đến môđun trình duyệt, mà ở đó thông báo mang chứng chỉ tương ứng với số điện thoại mà gửi tin nhắn SMS xác minh.

S419. Môđun trình duyệt xác định liệu chứng chỉ của trang mạng hiện thời là tương tự như chứng chỉ được mang trong thông báo. Nếu đúng, thực hiện S420; hoặc nếu không đúng, không thực hiện phản hồi.

Điều cần lưu ý là S419 là bước tùy ý. Mục đích đó là khi môđun trình duyệt mở các trang mạng (các nhãn) ở cùng thời điểm, trang mạng được hiển thị hiện thời không phải trang mạng mà cần thu được mã xác minh, nó chỉ báo rằng người dùng có thể không thực hiện thao tác trên trang mạng tùy ý tạm thời. Môđun trình duyệt không phản hồi và ngăn không cho trang mạng hiện thời thu được mã xác minh, để cải thiện độ bảo mật và trải nghiệm người dùng.

S420. Môđun trình duyệt gửi tin nhắn SMS có yêu cầu thu được mã xác minh đến môđun giải mã mật nhờ sử dụng giao diện bảo mật.

S421. Môđun giải mã mật thu được văn bản mã hóa mật của tin nhắn SMS có mã xác minh từ cơ sở dữ liệu mã hóa mật tin nhắn SMS giao dịch và giải mã mật văn bản mã hóa mật của tin nhắn SMS có mã xác minh nhờ sử dụng khóa mã hóa mật.

S422. Môđun giải mã mật gửi văn bản thuần của tin nhắn SMS có mã xác minh đến môđun trình duyệt nhờ sử dụng giao diện bảo mật.

Theo phương án này, giao diện bảo mật là API mở tin nhắn SMS có mã xác minh được thể hiện trên được thể hiện trên FIG.5. Đặc trưng của giao diện bảo mật đó là giao diện bảo mật có độ bảo mật tương đối cao, và có thể thực hiện, nhờ sử dụng văn bản thuần, sự truyền dữ liệu với ứng dụng mà tính hiệu lực của nó được chứng thực, như môđun trình duyệt, và nhắc người dùng với tính hiệu lực của ứng dụng mà thực hiện sự truyền dữ liệu văn bản thuần với giao diện. Mục đích là để làm giảm xác suất của mã xác minh bị bộc lộ và bị trộm, và cải thiện trải nghiệm của người dùng về độ bảo mật.

S423. Môđun trình duyệt trích ra mã xác minh từ tin nhắn SMS có mã

xác minh và điền mã xác minh vào hộ nhập mã xác minh trên trang mạng.

S424. Môđun truyền thông gửi mã xác minh đến máy chủ của trang mạng.

Trình tự thực hiện bước S424 và S423 có thể được thay đổi.

S425. Máy chủ của trang mạng kiểm tra mã xác minh và đưa kết quả kiểm tra trở lại môđun thu.

S426. Môđun trình duyệt thực hiện thao tác tương ứng dựa trên kết quả kiểm tra.

Theo phương án này, chứng chỉ trang mạng và số tin nhắn SMS được ràng buộc và được lưu trữ. Hệ thống không phát rộng tin nhắn thu tin nhắn SMS có mã xác minh, mà thông báo định hướng môđun trình duyệt của thông báo thu tin nhắn SMS. Môđun trình duyệt xác định, dựa trên chứng chỉ, liệu trang hiện thời có hiệu lực hay không, và thu được một cách định hướng tin nhắn SMS có mã xác minh, sao cho trình duyệt có thể tự động thu được mã xác minh. So với cách đã biết trong đó sự cho phép đọc tin nhắn SMS là mở với môđun trình duyệt sao cho môđun trình duyệt có thể đọc tất cả các tin nhắn SMS, nguy cơ bộc lộc thông tin nhạy cảm có thể được giảm đi.

Ngoài ra, dựa trên TEE, độ bảo mật mã xác minh có thể được cải thiện hơn nữa, và nguy cơ bộc lộ và ăn trộm mã xác minh có thể được giảm đi.

Sơ đồ của giao diện để thực hiện sự trích mã xác minh tự động dựa trên thủ tục thể hiện trên FIG.4A, FIG.4B, và FIG.4C được thể hiện trên FIG.6A và FIG.6B.

FIG.7 thể hiện phương pháp khác xử lý tin nhắn SMS có mã xác minh theo phương án của sáng chế. Phương pháp bao gồm các bước dưới đây:

S701. Thiết bị đầu cuối xác định liệu thiết bị đầu cuối có vào trang mạng được vào hiện tại trong lần thứ nhất hay không hoặc liệu thiết bị đầu cuối đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không. Nếu có, thực hiện S702; hoặc nếu không, không thực hiện xử lý hoặc thực hiện đều đặn S701.

S702. Thiết bị đầu cuối gửi yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại.

S703. Thiết bị đầu cuối thu thông tin nhận dạng người gửi mà của tin nhắn SMS có mã xác minh và được gửi bởi máy chủ của trang mạng được vào hiện tại.

S704. Thiết bị đầu cuối thu được chứng chỉ của trang mạng được vào hiện tại.

S705. Thiết bị đầu cuối lưu trữ sự tương ứng giữa chứng chỉ của trang mạng hiện đang vào và thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh.

Phần nêu trên là quy trình trong đó thiết bị đầu cuối đăng ký sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ trang mạng. Sự tương ứng đã được lưu trữ được sử dụng làm cơ sở để xác định liệu có thu được mã xác minh từ tin nhắn SMS có mã xác minh hay không.

S706. Thiết bị đầu cuối gửi yêu cầu thu được mã xác minh đến máy chủ của trang mạng được vào hiện tại.

S707. Thiết bị đầu cuối thu tin nhắn SMS có mã xác minh được gửi bởi máy chủ của trang mạng.

S708. Thiết bị đầu cuối truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi (số điện thoại và/hoặc tên doanh nghiệp) của tin nhắn SMS có mã xác minh được thu trong S707.

S709. Thiết bị đầu cuối xác định liệu chứng chỉ đã được tìm ra khớp với chứng chỉ của trang mạng hiện đang vào hay không. Nếu có, thực hiện S710; hoặc nếu không, xử lý tin nhắn SMS có mã xác minh dựa trên thủ tục xử lý tin nhắn SMS hiện có.

S710. Thiết bị đầu cuối thu được mã xác minh từ tin nhắn SMS có mã xác minh.

S711. Thiết bị đầu cuối gửi mã xác minh đến máy chủ của trang mạng để xác minh.

FIG.8 thể hiện kết cấu của thiết bị đầu cuối khác theo phương án của sáng chế. Thiết bị đầu cuối bao gồm môđun truyền thông, môđun truy vấn, và môđun thu được mã xác minh, và một cách tùy ý, bao gồm môđun lưu trữ. Cụ thể, môđun thu được mã xác minh bao gồm môđun trình duyệt và môđun xác định.

Các môđun trong thiết bị đầu cuối được thể hiện trên FIG.9A và FIG.9B thực hiện việc thu được mã xác minh tự động nhờ sử dụng các bước dưới đây.

S901. Môđun trình duyệt xác định liệu thiết bị đầu cuối có vào trang mạng được vào hiện tại trong lần thứ nhất hay không hoặc liệu thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không. Nếu có, thực hiện S802; hoặc nếu không, không thực hiện xử lý hoặc thực hiện đều đặn S901.

S902. Môđun truyền thông thu số điện thoại mà có thể gửi tin nhắn SMS có mã xác minh và được gửi bởi máy chủ của trang mạng.

S903. Môđun trình duyệt gửi chứng chỉ của trang mạng được vào hiện tại đến môđun lưu trữ.

S904. Môđun lưu trữ kiểm tra liệu sự tương ứng giữa số điện thoại và chứng chỉ được lưu trữ hay không. Nếu không, lưu trữ sự tương ứng giữa số điện thoại và chứng chỉ; hoặc nếu có, thực hiện S905.

Một cách tùy ý, danh sách trắng có thể được thiết đặt trước trong thiết bị xử lý tin nhắn SMS có mã xác minh, và sự tương ứng giữa số điện thoại và chứng chỉ được lưu trữ trong danh sách trắng.

S901 đến S904 mô tả quy trình đăng ký sự tương ứng giữa số điện thoại và chứng chỉ trong thiết bị xử lý tin nhắn SMS có mã xác minh.

S905. Môđun trình duyệt thu lệnh thu được mã xác minh thu được.

Ví dụ, lệnh thu được mã xác minh là lệnh được gửi khi người dùng nhấp vào khóa "thu được mã xác minh" (có thể là khóa ảo) được hiển thị trên trang mạng.

S906. Môđun truyền thông gửi yêu cầu thu được mã xác minh đến máy chủ của trang mạng được vào hiện tại.

S907. Môđun truyền thông thu tin nhắn SMS có mã xác minh được gửi bởi máy chủ của trang mạng được vào hiện tại.

S908. Môđun truy vấn truy vấn chứng chỉ tương ứng với số điện thoại mà của người gửi và được bao gồm trong tin nhắn SMS có mã xác minh.

S909. Môđun xác định phát rộng thông báo thu tin nhắn SMS, trong đó thông báo mang chứng chỉ được tìm ra trong S908.

S910. Môđun trình duyệt xác định liệu chứng chỉ của trang mạng được hiển thị hiện thời là tương tự như chứng chỉ được mang trong thông báo hay không. Nếu có, thực hiện S911; hoặc nếu không, không phản hồi.

S910 là bước tùy ý. Mục đích đó là khi trình duyệt mở các trang mạng (các nhãn) đồng thời, nếu trang mạng được hiển thị hiện thời không phải trang mạng mà cần để thu được mã xác minh, nó chỉ báo rằng người dùng có thể không thực hiện thao tác trên trang mạng ban đầu một cách tạm thời. Môđun trình duyệt không tạo ra phản hồi và ngăn trang mạng hiện thời không thu được mã xác minh, để cải thiện độ bảo mật và trải nghiệm của người dùng.

S911. Môđun trình duyệt gửi chứng chỉ của trang mạng hiện đang vào đến thiết bị xác định.

S912. Môđun xác định xác định liệu chứng chỉ đã được thu là tương tự như chứng chỉ được tìm ra ở S908 hay không. Nếu có, thực hiện S913; hoặc nếu không, thực hiện S918.

S913. Môđun xác định gửi tin nhắn SMS có mã xác minh đến môđun trình duyệt.

S914. Môđun trình duyệt trích ra mã xác minh từ tin nhắn SMS có mã xác minh và điền mã xác minh vào trong hộp nhập mã xác minh trên trang

mạng.

S915. Môđun truyền thông gửi mã xác minh đến máy chủ của trang mạng được vào hiện tại.

S916. Máy chủ của trang mạng được vào hiện tại kiểm tra mã xác minh và đưa kết quả kiểm tra trở lại trình duyệt.

S917. Môđun trình duyệt thực hiện thao tác tương ứng dựa trên kết quả kiểm tra.

S918. Môđun xác định từ chối gửi tin nhắn SMS có mã xác minh đến môđun trình duyệt.

Điều có thể được hiểu từ quy trình được thể hiện trên FIG.9A và FIG.9B là, nếu người dùng nhấp vào khóa "thu được mã xác minh" trên trang mạng của trình duyệt, sau khi tin nhắn SMS có mã xác minh được gửi bởi máy chủ của trang mạng được thu, tin nhắn SMS có mã xác minh có thể được gửi đến môđun trình duyệt sau khi trang mạng được xác minh, và môđun trình duyệt có thể thu được mã xác minh từ tin nhắn SMS có mã xác minh. So với trình duyệt thông thường, theo phương án này, trình duyệt có thể thu được một cách tự động mã xác minh.

Cần nhấn mạnh rằng quy trình thu được mã xác minh tự động theo phương án này khác với cách theo kỹ thuật đã biết trong đó ứng dụng tự động thu được và điền mã xác minh. Theo kỹ thuật đã biết, ứng dụng thu được sự cho phép đọc tin nhắn SMS và có thể tự động trích ra mã xác minh sau khi thu tin nhắn SMS. Dựa trên cơ chế như vậy, ứng dụng thu được sự cho phép để đọc tin nhắn SMS bất kỳ một khi ứng dụng thu được sự cho phép đọc tin nhắn SMS. Vì vậy, nguy cơ bộc lộ thông tin nhạy cảm rõ ràng bị tăng lên. Ngoài ra, ứng dụng có thể đọc không chỉ tin nhắn SMS có mã xác minh thông thường mà còn các tin nhắn SMS khác được thu và được gửi khi người dùng thường sử dụng ứng dụng tin nhắn SMS, và dễ làm bộc lộ bí mật của người dùng.

Theo phương pháp theo phương án này, môđun trình duyệt có thể thu được tin nhắn SMS có mã xác minh chỉ khi chứng chỉ của trang mạng mà thu

được mã xác minh khớp với chứng chỉ của trang mạng mà thu được mã xác minh trong quá trình đăng ký, thay vì mở sự cho phép đọc tin nhắn SMS đến môđun trình duyệt để cho phép môđun trình duyệt đọc tất cả các tin nhắn SMS. Vì vậy, phương pháp theo phương án này thực hiện mục đích điền đầy tự động mã xác minh bởi trình duyệt trong khi độ bảo mật tương đối cao được đảm bảo.

FIG.10 thể hiện thiết bị đầu cuối khác theo phương án của sáng chế. Thiết bị đầu cuối bao gồm thành phần truyền thông, bộ nhớ, và bộ xử lý.

Bộ nhớ được tạo cấu hình để: lưu trữ sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ, và lưu trữ chương trình ứng dụng và dữ liệu được tạo ra trong quy trình chạy chương trình ứng dụng. Thành phần truyền thông được tạo cấu hình để thu tin nhắn SMS có mã xác minh mà bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh. Bộ xử lý được tạo cấu hình để: truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; thu được văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong môi trường thực hiện tin cậy (TEE) khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối; và thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong môi trường thực hiện đầy đủ (REE).

Cụ thể, việc thực hiện cụ thể trong đó bộ xử lý thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE có thể là: nếu được xác định rằng loại của văn bản mã hóa mật là tin nhắn SMS có mã xác minh, thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE bằng cách sử dụng khóa thu được từ TEE.

Ngoài ra, bộ xử lý còn được tạo cấu hình để xác định liệu thiết bị đầu cuối có vào trang mạng được vào hiện tại trong lần thứ nhất hay không hoặc liệu thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không. Thành phần truyền thông còn được tạo cấu hình để: nếu bộ xử lý xác định rằng thiết bị đầu cuối vào trang mạng được vào

hiện tại trong lần thứ nhất hoặc thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại, gửi yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại trước khi thu tin nhắn SMS có mã xác minh, và thu thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào mà được gửi bởi máy chủ của trang mạng được vào hiện tại. Bộ xử lý còn được tạo cấu hình để lưu trữ sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào.

Dựa vào FIG.2A và FIG.2B cho quy trình thực hiện cụ thể của các chức năng nêu trên.

Chức năng của thiết bị đầu cuối được thể hiện trên FIG.10 có thể được mô tả như sau: bộ xử lý được tạo cấu hình để: truy vấn, dựa trên sự tương ứng đã được lưu trữ giữa thông tin và chứng chỉ, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; và thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối. Chức năng của thành phần truyền thông được mô tả ở trên, và chi tiết không được mô tả ở đây. Dựa vào FIG.7 đối với quy trình thực hiện cụ thể của các chức năng.

Các phương án trong bản mô tả này đều được mô tả theo cách phát triển, đối với các phần giống nhau hoặc tương tự trong các phương án, có thể tham chiếu đến các phương án này, và mỗi phương án tập trung vào phần khác biệt giữa các phương án.

Các phương án được bộc lộ ở trên được mô tả để cho phép người có hiểu biết trung bình trong lĩnh vực kỹ thuật thực hiện hoặc sử dụng sáng chế. Các cải biến khác nhau của các phương án là hiển nhiên đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật, và các nguyên tắc chung được xác định trong bản mô tả này có thể được thực hiện trong các phương án khác mà không chệch khỏi phạm vi của sáng chế. Vì vậy, sáng chế không bị giới hạn ở các phương án được

thể hiện trong bản mô tả này, mà sáng chế sẽ được hiểu theo phạm vi rộng nhất phù hợp với các nguyên tắc và các dấu hiệu mới được bộc lộ trong bản mô tả này.

## YÊU CẦU BẢO HỘ

1. Phương pháp xử lý tin nhắn SMS (Dịch vụ tin nhắn ngắn - Short Message Service) có mã xác minh bao gồm các bước:

thu, bởi thiết bị đầu cuối và trong hệ thống truyền thông dải cơ sở, tin nhắn SMS có mã xác minh, trong đó tin nhắn SMS có mã xác minh bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

truy vấn trong hệ thống truyền thông dải cơ sở, bởi thiết bị đầu cuối dựa trên sự tương ứng giữa thông tin và chứng chỉ và được lưu trữ trong hệ thống truyền thông dải cơ sở, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

xác định, bởi thiết bị đầu cuối và trong hệ thống truyền thông dải cơ sở, rằng chứng chỉ mà tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có khớp với chứng chỉ của trang mạng đang được vào hay không;

thu được, bởi thiết bị đầu cuối, văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong môi trường thực hiện tin cậy (TEE) khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối; và

thu được, bởi thiết bị đầu cuối, mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong môi trường thực hiện đầy đủ (REE).

2. Phương pháp theo điểm 1, trong đó bước thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE bao gồm:

nếu được xác định rằng loại của văn bản mã hóa mật là tin nhắn SMS có mã xác minh, thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE bằng cách sử dụng khóa thu được từ TEE.

3. Phương pháp theo điểm 1 hoặc 2, trước khi thu tin nhắn SMS có mã xác minh, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, yêu cầu để thu được thông tin nhận dạng người

gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại khi xác định rằng thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần thứ nhất hoặc đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại;

thu, bởi thiết bị đầu cuối, thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào mà được gửi bởi máy chủ của trang mạng được vào hiện tại; và

lưu trữ, bởi thiết bị đầu cuối, sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào.

4. Phương pháp xử lý tin nhắn SMS (Dịch vụ tin nhắn ngắn - Short Message Service) có mã xác minh bao gồm các bước:

thu, bởi thiết bị đầu cuối và trong hệ thống truyền thông dải cơ sở, tin nhắn SMS có mã xác minh, trong đó tin nhắn SMS có mã xác minh bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

truy vấn trong hệ thống truyền thông dải cơ sở, bởi thiết bị đầu cuối dựa trên sự tương ứng giữa thông tin và chứng chỉ và được lưu trữ trong hệ thống truyền thông dải cơ sở, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

xác định, bởi thiết bị đầu cuối và trong hệ thống truyền thông dải cơ sở, rằng chứng chỉ mà tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có khớp với chứng chỉ của trang mạng đang được vào hay không; và

thu được, bởi thiết bị đầu cuối, mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối.

5. Phương pháp theo điểm 4, trước khi thu tin nhắn SMS có mã xác minh, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại khi xác định rằng thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần thứ nhất hoặc đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại;

thu, bởi thiết bị đầu cuối, thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào mà được gửi bởi máy chủ của trang mạng được vào hiện tại; và

lưu trữ sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào.

6. Thiết bị đầu cuối bao gồm:

môđun truyền thông được bố trí trong hệ thống truyền thông dải cơ sở, trong đó môđun truyền thông được tạo cấu hình để thu tin nhắn SMS có mã xác minh, và tin nhắn SMS có mã xác minh bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

môđun truy vấn được bố trí trong hệ thống truyền thông dải cơ sở, trong đó môđun truy vấn được tạo cấu hình để truy vấn, dựa trên sự tương ứng giữa thông tin và chứng chỉ và được lưu trữ trong hệ thống truyền thông dải cơ sở, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

môđun xác định được bố trí trong hệ thống truyền thông dải cơ sở, được tạo cấu hình để xác định rằng chứng chỉ mà tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có khớp với chứng chỉ của trang mạng đang được vào bởi thiết bị đầu cuối hay không; và

môđun mã hóa mật, được tạo cấu hình để thu được văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong môi trường thực hiện tin cậy (TEE-Trusted execution environment) khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối; và

môđun thu được mã xác minh, được tạo cấu hình để thu được mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong môi trường thực hiện đầy đủ (REE- Rich execution environment).

7. Thiết bị đầu cuối theo điểm 6, trong đó môđun thu được mã xác minh bao gồm:

môđun giải mã mật, được tạo cấu hình để: khi loại của văn bản mã hóa mật là tin nhắn SMS có mã xác minh, thu được tin nhắn SMS có mã xác minh bằng cách giải mã mật văn bản mã hóa mật trong REE bằng cách sử dụng khóa thu được từ TEE; và

môđun trình duyệt, được tạo cấu hình để thu được tin nhắn SMS có mã xác minh và thu được mã xác minh từ tin nhắn SMS có mã xác minh.

8. Thiết bị đầu cuối theo điểm 7, trong đó môđun trình duyệt được tạo cấu hình để thu được tin nhắn SMS có mã xác minh bao gồm:

môđun trình duyệt được tạo cấu hình cụ thể để thu được tin nhắn SMS có mã xác minh nhờ sử dụng giao diện bảo mật.

9. Thiết bị đầu cuối theo điểm 7 hoặc 8, trong đó môđun giải mã mật còn được tạo cấu hình để:

gửi thông báo đến môđun trình duyệt sau khi thu được tin nhắn SMS có mã xác minh, trong đó thông báo mang thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh; và

môđun trình duyệt được tạo cấu hình để thu được mã xác minh từ tin nhắn SMS có mã xác minh bao gồm:

môđun trình duyệt được tạo cấu hình cụ thể để thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ của trang mạng hiện đang vào khớp với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh.

10. Thiết bị đầu cuối theo điểm 7, trong đó thiết bị đầu cuối còn bao gồm môđun lưu trữ;

môđun trình duyệt còn được tạo cấu hình để:

xác định liệu thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần

thứ nhất hay không hoặc liệu thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không;

môđun truyền thông còn được tạo cấu hình để:

khi môđun trình duyệt xác định rằng thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần thứ nhất hoặc liệu thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không, gửi yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh đến máy chủ của trang mạng được vào hiện tại, và thu thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào mà được gửi bởi máy chủ của trang mạng được vào hiện tại; và

môđun lưu trữ được tạo cấu hình để lưu trữ sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào.

11. Thiết bị đầu cuối bao gồm:

môđun truyền thông được bố trí trong hệ thống truyền thông dải cơ sở, trong đó môđun truyền thông được tạo cấu hình để thu tin nhắn SMS có mã xác minh, và tin nhắn SMS có mã xác minh bao gồm thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

môđun truy vấn được bố trí trong hệ thống truyền thông dải cơ sở, trong đó môđun truy vấn được tạo cấu hình để truy vấn, dựa trên sự tương ứng giữa thông tin và chứng chỉ và được lưu trữ trong hệ thống truyền thông dải cơ sở, chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh;

môđun xác định được bố trí trong hệ thống truyền thông dải cơ sở, được tạo cấu hình để xác định rằng chứng chỉ mà tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh có khớp với chứng chỉ của trang mạng đang được vào bởi thiết bị đầu cuối hay không; và môđun thu được mã xác minh, được tạo cấu hình để thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin

nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối.

12. Thiết bị đầu cuối theo điểm 11, trong đó môđun thu được mã xác minh bao gồm:

môđun trình duyệt, được tạo cấu hình để thu được tin nhắn SMS có mã xác minh và thu được mã xác minh từ tin nhắn SMS có mã xác minh khi chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối.

13. Thiết bị đầu cuối theo điểm 12, trong đó môđun xác định còn được tạo cấu hình để:

gửi thông báo đến môđun trình duyệt trước khi xác định liệu chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh khớp với chứng chỉ của trang mạng được vào hiện tại bởi thiết bị đầu cuối hay không, trong đó thông báo mang chứng chỉ tương ứng với thông tin nhận dạng người gửi; và

môđun trình duyệt còn được tạo cấu hình để gửi chứng chỉ của trang mạng hiện đang vào đến môđun xác định khi chứng chỉ tương ứng với thông tin nhận dạng người gửi khớp với chứng chỉ của trang mạng hiện đang vào.

14. Thiết bị đầu cuối theo điểm 12, trong đó thiết bị đầu cuối còn bao gồm môđun lưu trữ;

môđun trình duyệt còn được tạo cấu hình để:

xác định liệu thiết bị đầu cuối có vào trang mạng được vào hiện tại trong lần thứ nhất hay không hoặc liệu thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại hay không;

môđun truyền thông còn được tạo cấu hình để:

khi môđun trình duyệt xác định rằng thiết bị đầu cuối vào trang mạng được vào hiện tại trong lần thứ nhất hoặc liệu thiết bị đầu cuối đã gửi thông tin đăng nhập hoặc đăng ký đến máy chủ của trang mạng được vào hiện tại, gửi yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh

đến máy chủ của trang mạng được vào hiện tại, và thu thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào mà được gửi bởi máy chủ của trang mạng được vào hiện tại; và

môđun lưu trữ được tạo cấu hình để lưu trữ sự tương ứng giữa thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh và chứng chỉ của trang mạng hiện đang vào.

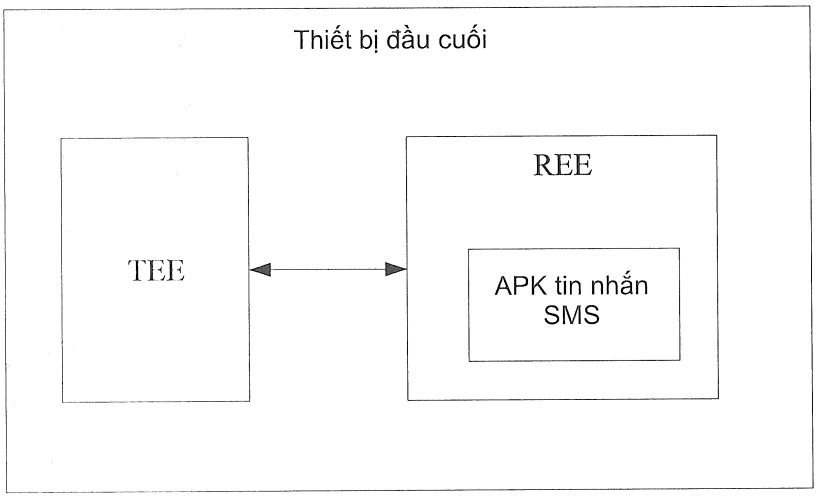



FIG. 1

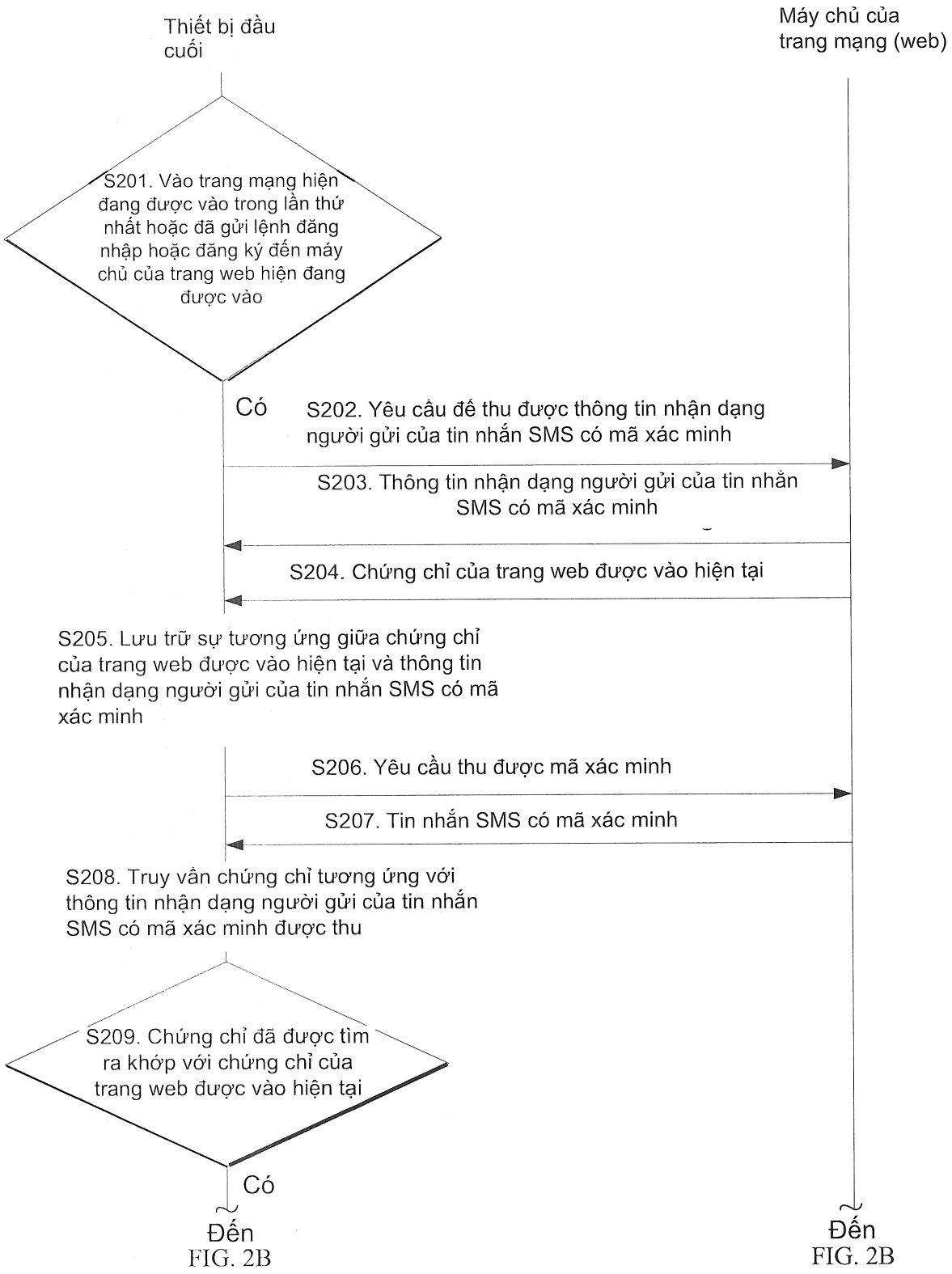

Thiết bị đầu cuối
Máy chủ của trang mạng (web)
S201. Vào trang mạng hiện đang được vào trong lần thứ nhất hoặc đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang web hiện đang được vào
Có
S202. Yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh
S203. Thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh
S204. Chứng chỉ của trang web được vào hiện tại
S205. Lưu trữ sự tương ứng giữa chứng chỉ của trang web được vào hiện tại và thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh
S206. Yêu cầu thu được mã xác minh
S207. Tin nhắn SMS có mã xác minh
S208. Truy vấn chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh được thu
S209. Chứng chỉ đã được tìm ra khớp với chứng chỉ của trang web được vào hiện tại
Có
Đến FIG. 2B
Đến FIG. 2B

FIG. 2A

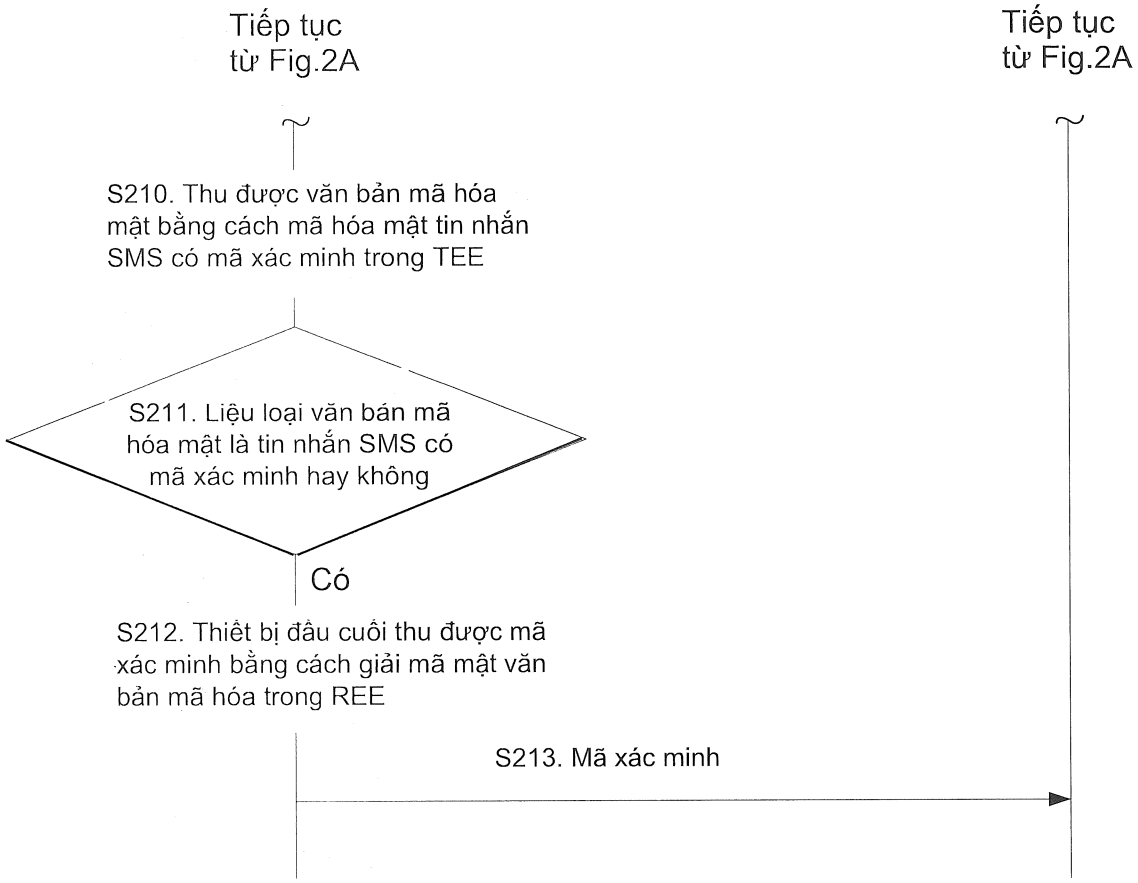

Tiếp tục
từ Fig.2A
Tiếp tục
từ Fig.2A
S210. Thu được văn bản mã hóa mật bằng cách mã hóa mật tin nhắn SMS có mã xác minh trong TEE
S211. Liệu loại văn bản mã hóa mật là tin nhắn SMS có mã xác minh hay không
Có
S212. Thiết bị đầu cuối thu được mã xác minh bằng cách giải mã mật văn bản mã hóa trong REE
S213. Mã xác minh

FIG. 2B

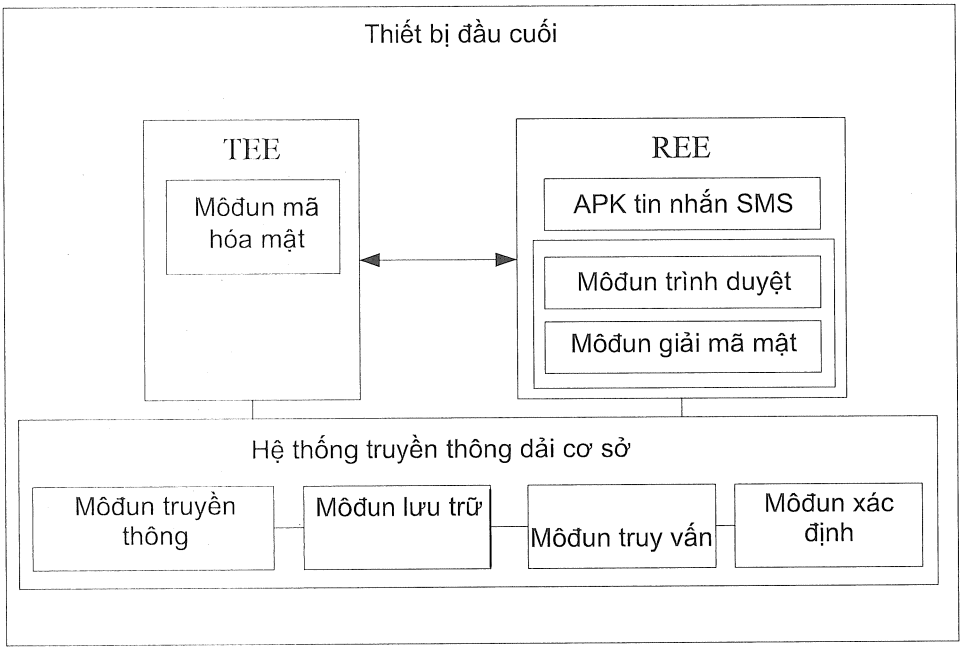

Thiết bị đầu cuối
TEE
Môđun mã hóa mật
REE
APK tin nhắn SMS
Môđun trình duyệt
Môđun giải mã mật
Hệ thống truyền thông dải cơ sở
Môđun truyền thông
Môđun lưu trữ
Môđun truy vấn
Môđun xác định

FIG. 3

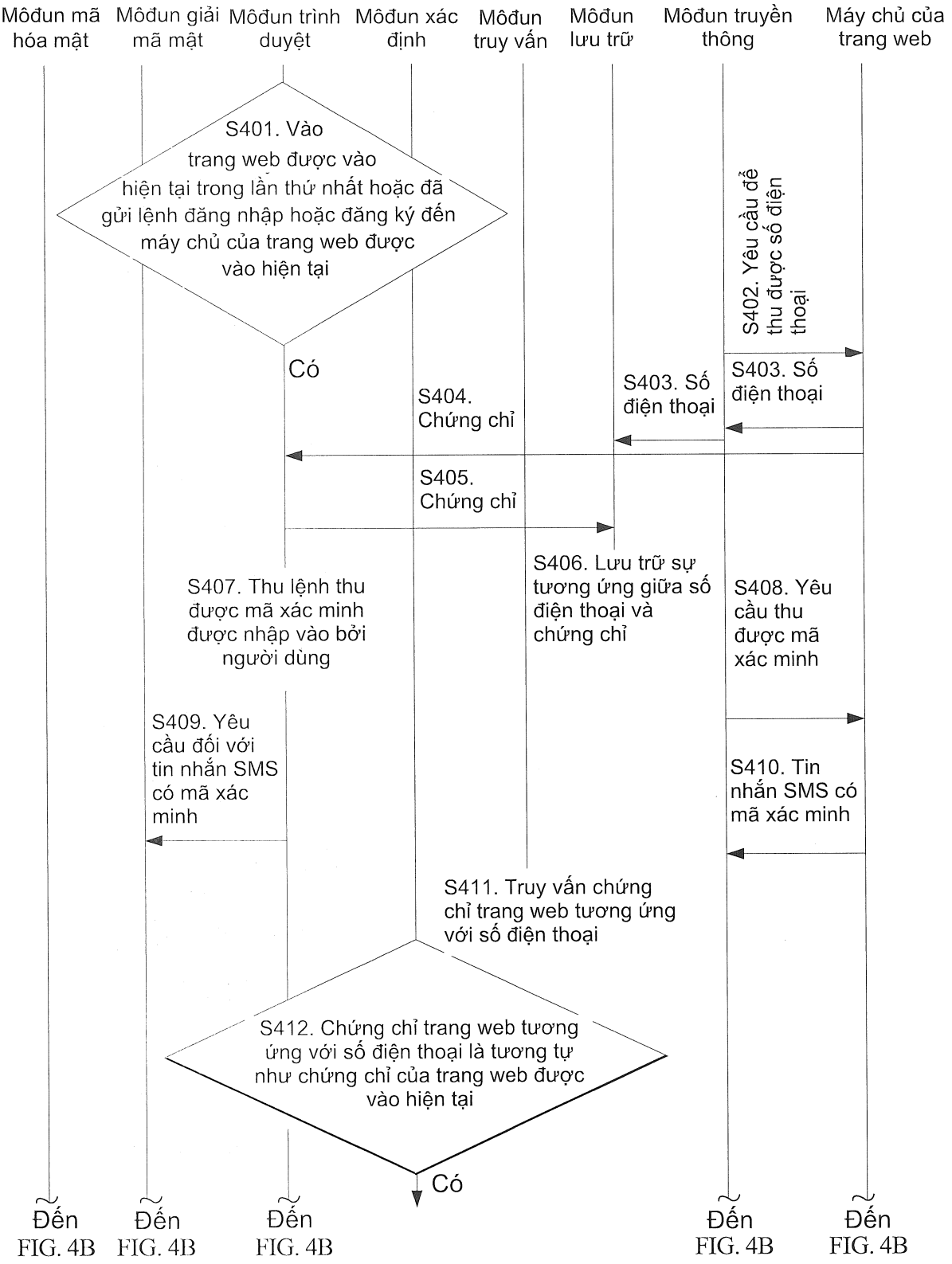

Môđun mã hóa mật
Môđun giải mã mật
Môđun trình duyệt
Môđun xác định
Môđun truy vấn
Môđun lưu trữ
Môđun truyền thông
Máy chủ của trang web
S401. Vào trang web được vào hiện tại trong lần thứ nhất hoặc đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang web được vào hiện tại
Có
S402. Yêu cầu để thu được số điện thoại
S403. Số điện thoại
S403. Số điện thoại
S404. Chứng chỉ
S405. Chứng chỉ
S406. Lưu trữ sự tương ứng giữa số điện thoại và chứng chỉ
S407. Thu lệnh thu được mã xác minh được nhập vào bởi người dùng
S408. Yêu cầu thu được mã xác minh
S409. Yêu cầu đối với tin nhắn SMS có mã xác minh
S410. Tin nhắn SMS có mã xác minh
S411. Truy vấn chứng chỉ trang web tương ứng với số điện thoại
S412. Chứng chỉ trang web tương ứng với số điện thoại là tương tự như chứng chỉ của trang web được vào hiện tại
Có
Đến FIG. 4B
Đến FIG. 4B
Đến FIG. 4B
Đến FIG. 4B
Đến FIG. 4B

FIG. 4A

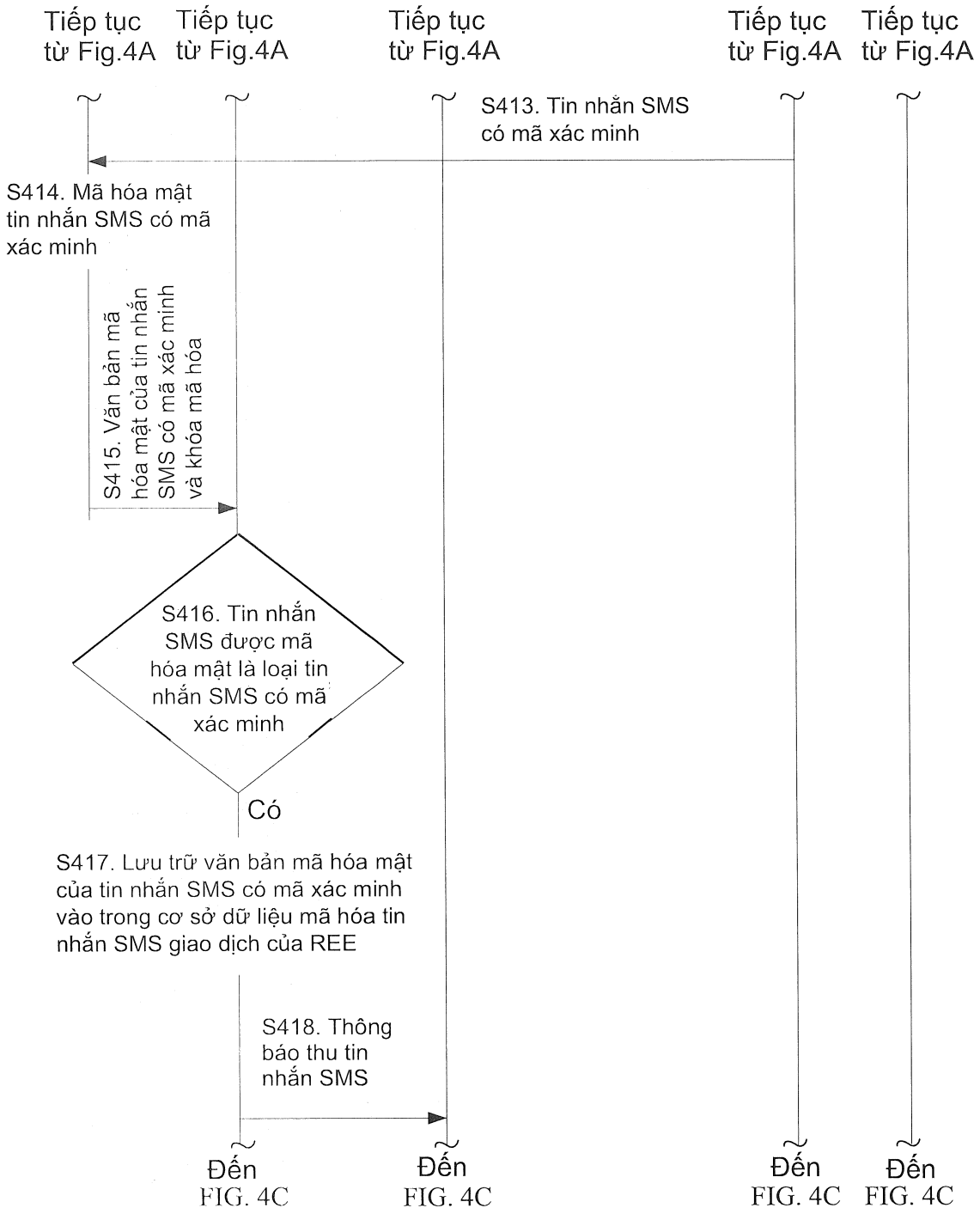

Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
S413. Tin nhắn SMS có mã xác minh
S414. Mã hóa mật tin nhắn SMS có mã xác minh
S415. Văn bản mã hóa mật của tin nhắn SMS có mã xác minh và khóa mã hóa
S416. Tin nhắn SMS được mã hóa mật là loại tin nhắn SMS có mã xác minh
Có
S417. Lưu trữ văn bản mã hóa mật của tin nhắn SMS có mã xác minh vào trong cơ sở dữ liệu mã hóa tin nhắn SMS giao dịch của REE
S418. Thông báo thu tin nhắn SMS
Đến FIG. 4C
Đến FIG. 4C
Đến FIG. 4C
Đến FIG. 4C

FIG. 4B

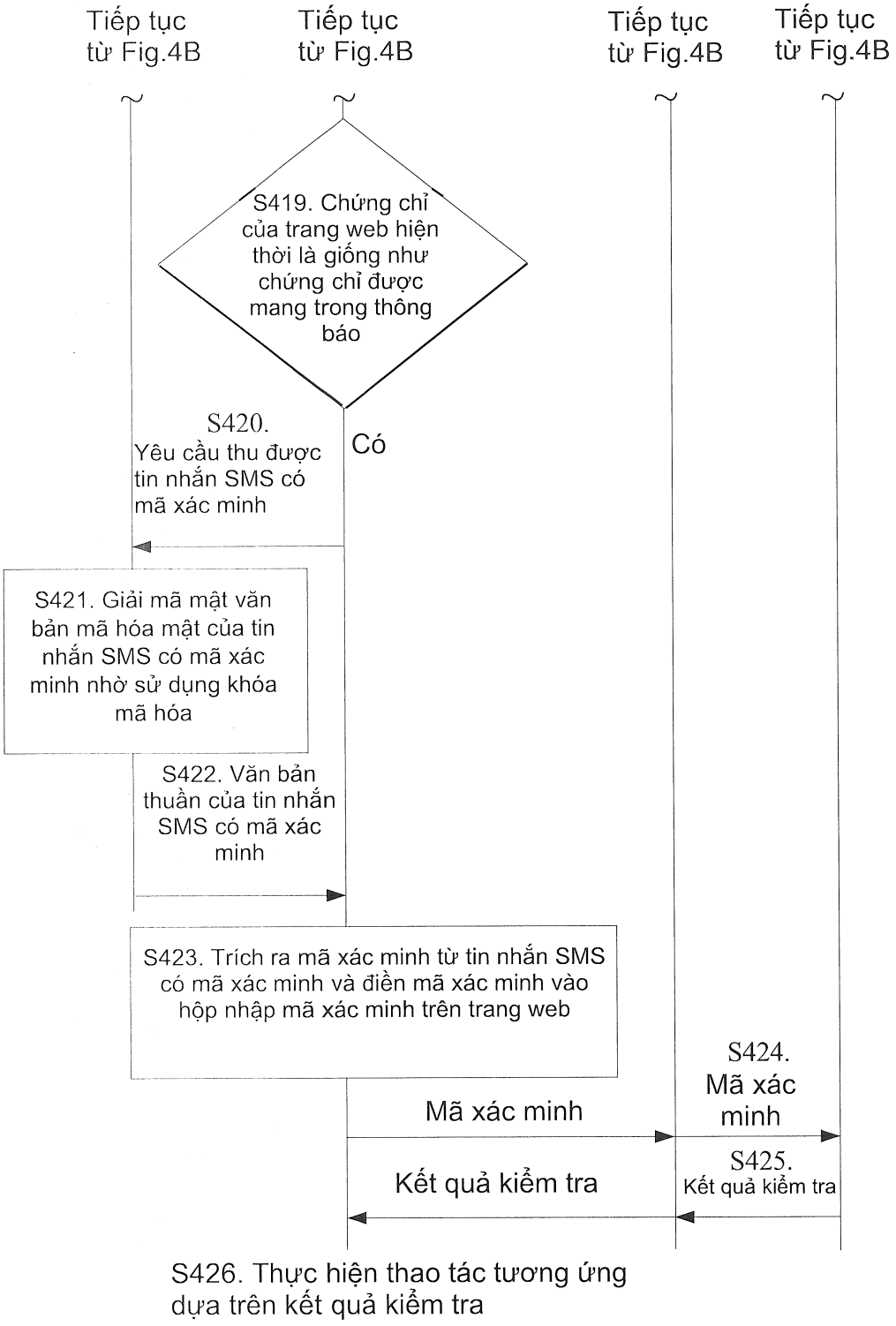

Tiếp tục từ Fig.4B
Tiếp tục từ Fig.4B
Tiếp tục từ Fig.4B
Tiếp tục từ Fig.4B
S419. Chứng chỉ của trang web hiện thời là giống như chứng chỉ được mang trong thông báo
Có
S420. Yêu cầu thu được tin nhắn SMS có mã xác minh
S421. Giải mã mật văn bản mã hóa mật của tin nhắn SMS có mã xác minh nhờ sử dụng khóa mã hóa
S422. Văn bản thuần của tin nhắn SMS có mã xác minh
S423. Trích ra mã xác minh từ tin nhắn SMS có mã xác minh và điền mã xác minh vào hộp nhập mã xác minh trên trang web
S424. Mã xác minh
Mã xác minh
S425. Kết quả kiểm tra
Kết quả kiểm tra
S426. Thực hiện thao tác tương ứng dựa trên kết quả kiểm tra

FIG. 4C

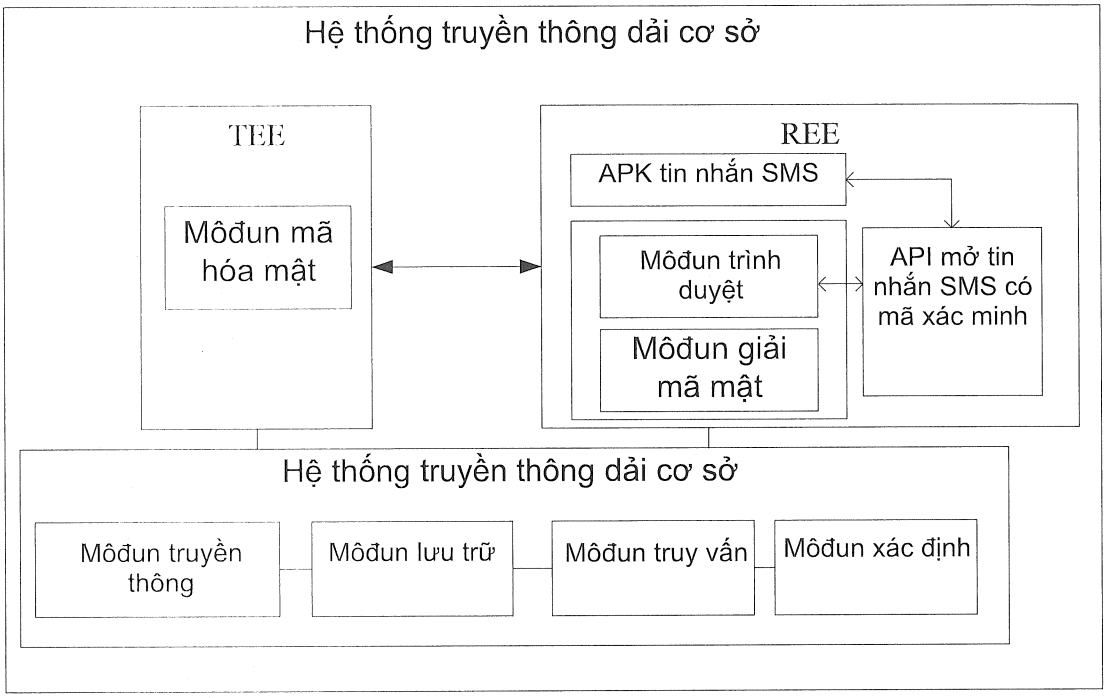

Hệ thống truyền thông dải cơ sở
TEE
Môđun mã hóa mật
REE
APK tin nhắn SMS
Môđun trình duyệt
Môđun giải mã mật
API mở tin nhắn SMS có mã xác minh
Hệ thống truyền thông dải cơ sở
Môđun truyền thông
Môđun lưu trữ
Môđun truy vấn
Môđun xác định

FIG. 5

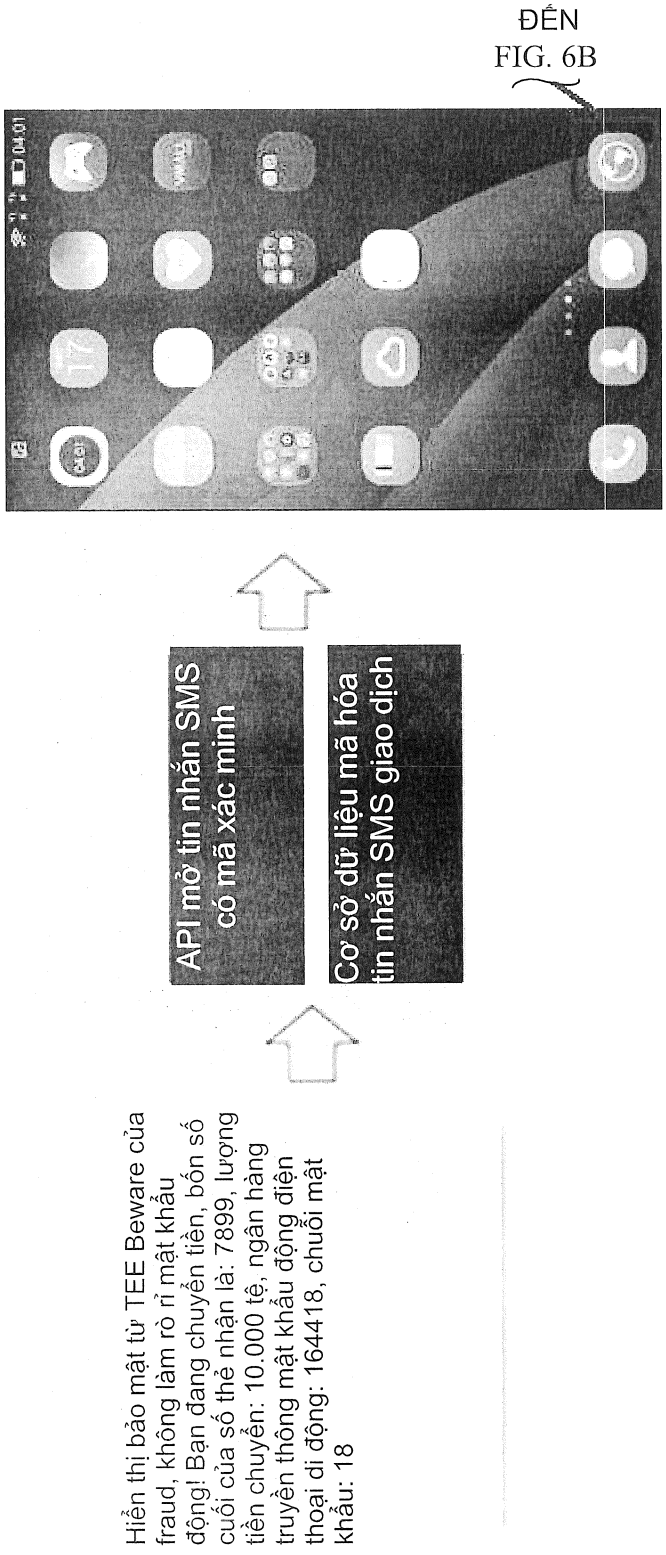

ĐẾN
FIG. 6B
API mở tin nhắn SMS có mã xác minh
Cơ sở dữ liệu mã hóa tin nhắn SMS giao dịch
Hiển thị bảo mật từ TEE Beware của fraud, không làm rò rỉ mật khẩu động! Bạn đang chuyển tiền, bốn số cuối của số thẻ nhận là: 7899, lượng tiền chuyển: 10.000 tệ, ngân hàng truyền thông mật khẩu động điện thoại di động: 164418, chuỗi mật khẩu: 18

FIG. 6A

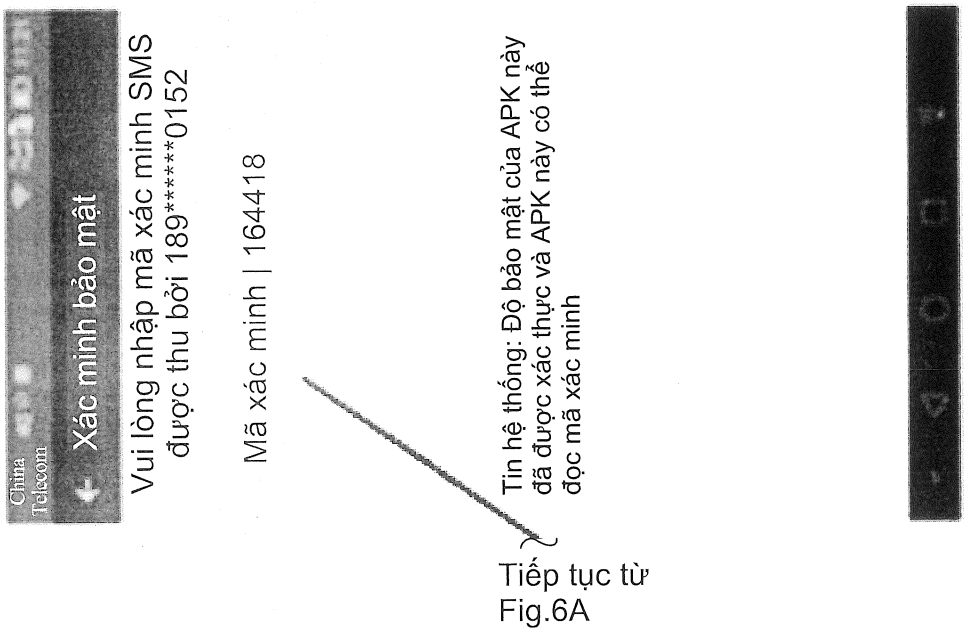

China Telecom
Xác minh bảo mật
Vui lòng nhập mã xác minh SMS được thu bởi 189******0152
Mã xác minh | 164418
Tin hệ thống: Độ bảo mật của APK này đã được xác thực và APK này có thể đọc mã xác minh
Tiếp tục từ Fig.6A

FIG. 6B

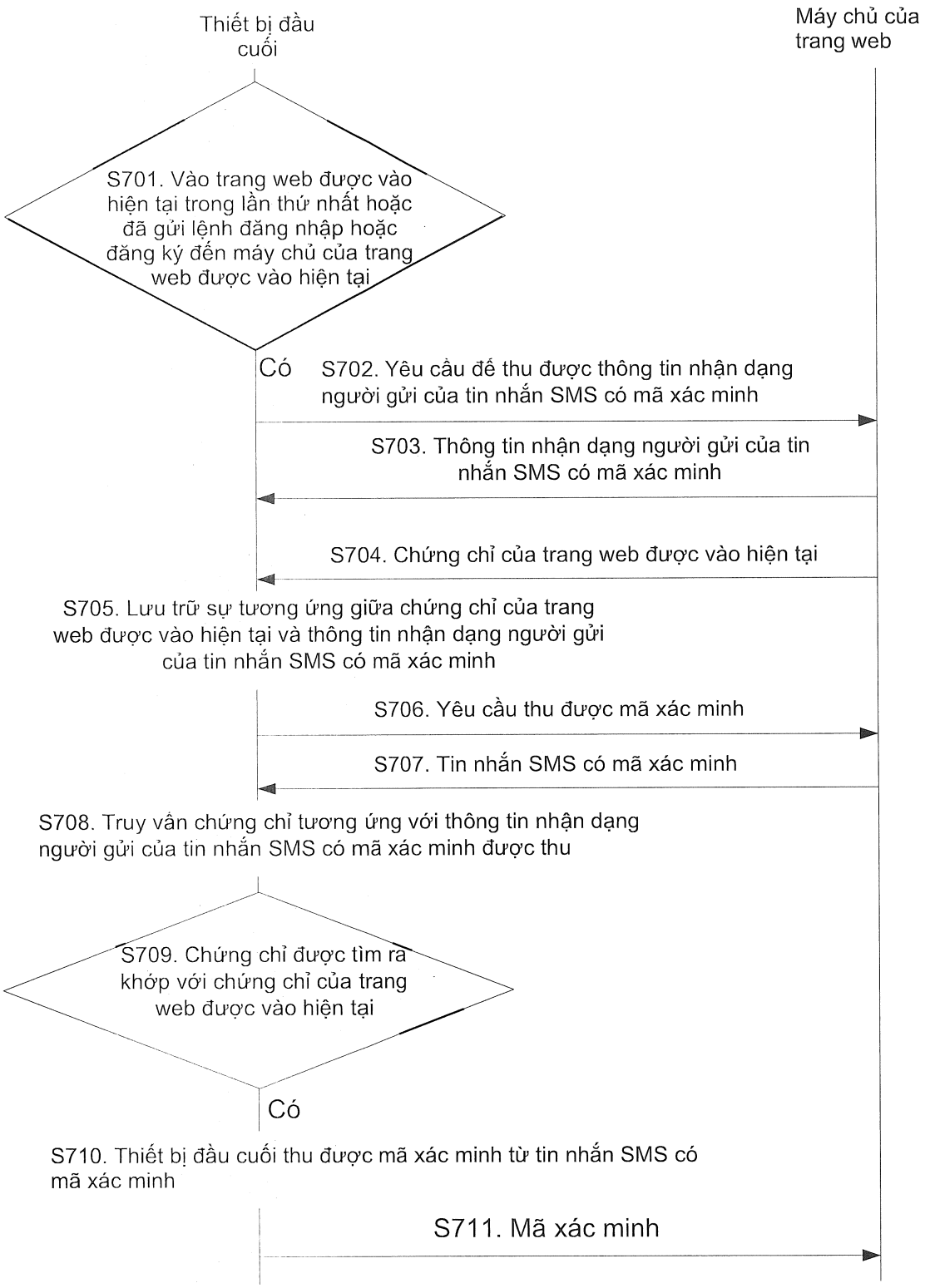

Thiết bị đầu cuối
Máy chủ của trang web
S701. Vào trang web được vào hiện tại trong lần thứ nhất hoặc đã gửi lệnh đăng nhập hoặc đăng ký đến máy chủ của trang web được vào hiện tại
Có
S702. Yêu cầu để thu được thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh
S703. Thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh
S704. Chứng chỉ của trang web được vào hiện tại
S705. Lưu trữ sự tương ứng giữa chứng chỉ của trang web được vào hiện tại và thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh
S706. Yêu cầu thu được mã xác minh
S707. Tin nhắn SMS có mã xác minh
S708. Truy vấn chứng chỉ tương ứng với thông tin nhận dạng người gửi của tin nhắn SMS có mã xác minh được thu
S709. Chứng chỉ được tìm ra khớp với chứng chỉ của trang web được vào hiện tại
Có
S710. Thiết bị đầu cuối thu được mã xác minh từ tin nhắn SMS có mã xác minh
S711. Mã xác minh

FIG. 7

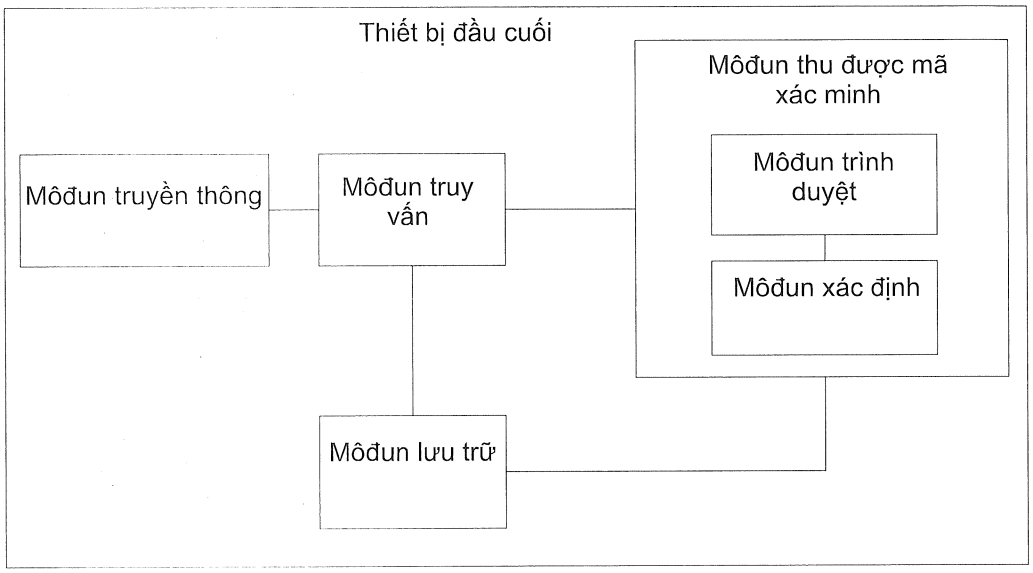

Thiết bị đầu cuối
Môđun thu được mã xác minh
Môđun trình duyệt
Môđun xác định
Môđun truyền thông
Môđun truy vấn
Môđun lưu trữ

FIG. 8

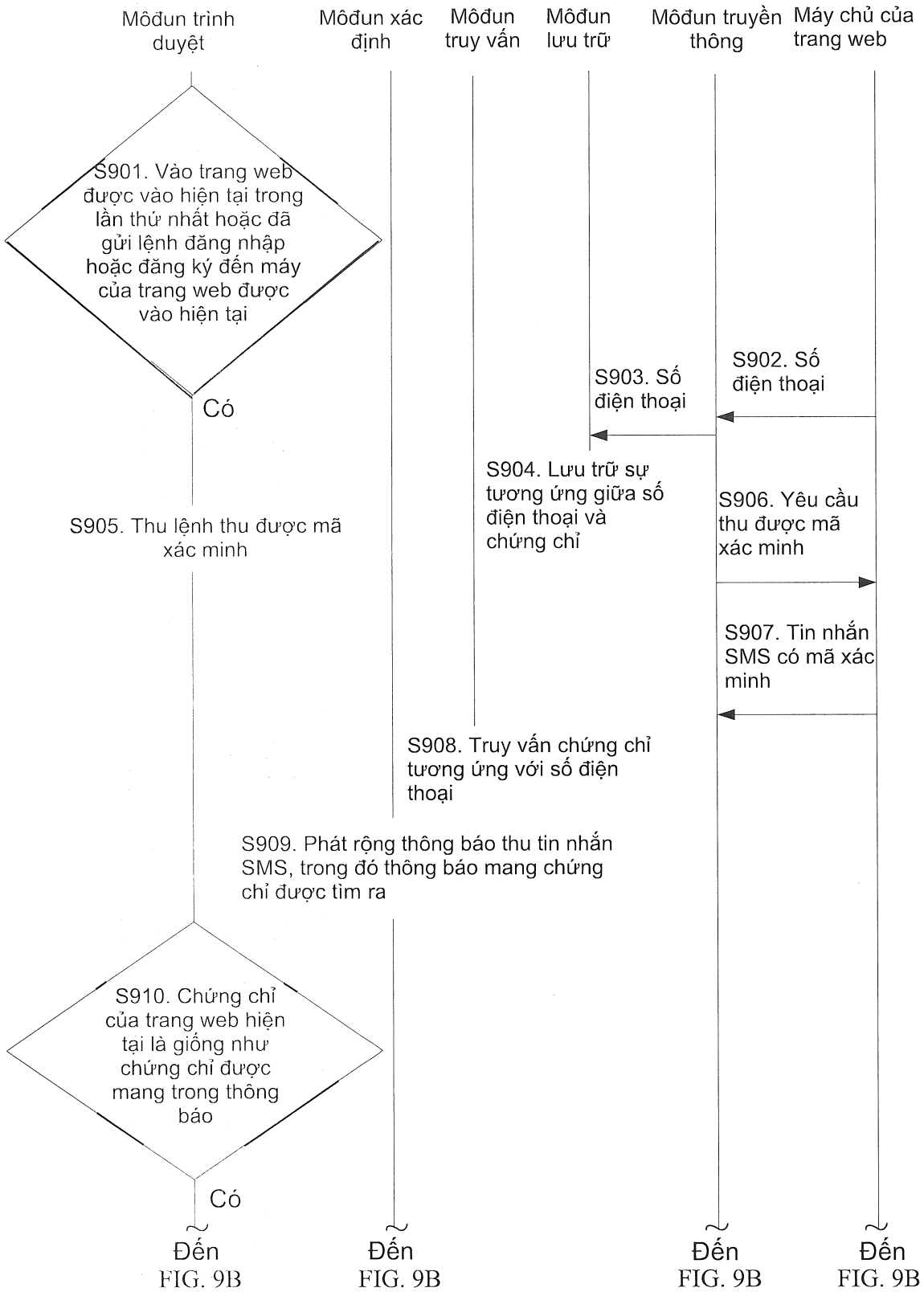

Môđun trình duyệt
Môđun xác định
Môđun truy vấn
Môđun lưu trữ
Môđun truyền thông
Máy chủ của trang web
S901. Vào trang web được vào hiện tại trong lần thứ nhất hoặc đã gửi lệnh đăng nhập hoặc đăng ký đến máy của trang web được vào hiện tại
Có
S902. Số điện thoại
S903. Số điện thoại
S904. Lưu trữ sự tương ứng giữa số điện thoại và chứng chỉ
S905. Thu lệnh thu được mã xác minh
S906. Yêu cầu thu được mã xác minh
S907. Tin nhắn SMS có mã xác minh
S908. Truy vấn chứng chỉ tương ứng với số điện thoại
S909. Phát rộng thông báo thu tin nhắn SMS, trong đó thông báo mang chứng chỉ được tìm ra
S910. Chứng chỉ của trang web hiện tại là giống như chứng chỉ được mang trong thông báo
Có
Đến FIG. 9B
Đến FIG. 9B
Đến FIG. 9B
Đến FIG. 9B

FIG. 9A

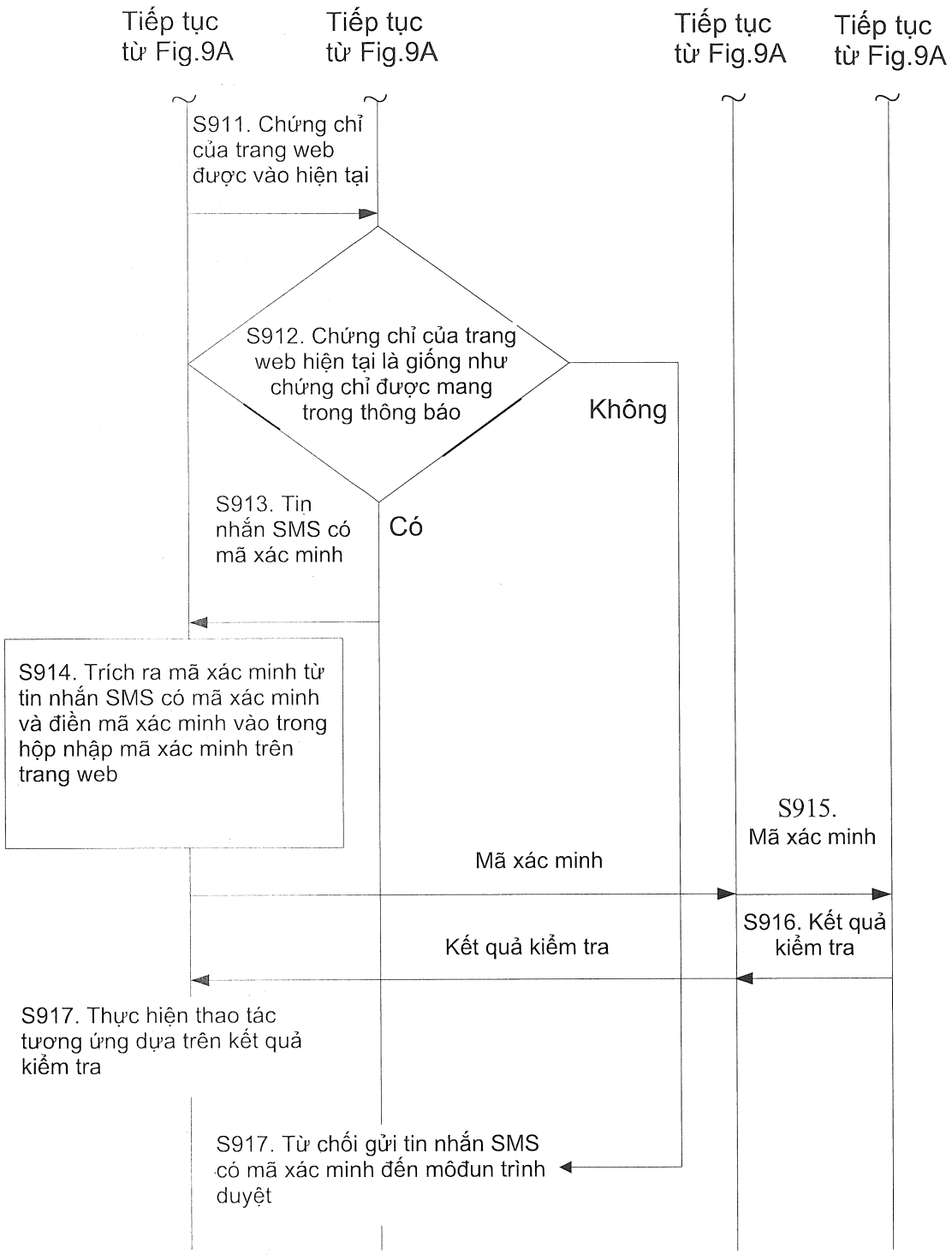

Tiếp tục từ Fig.9A
Tiếp tục từ Fig.9A
Tiếp tục từ Fig.9A
Tiếp tục từ Fig.9A
S911. Chứng chỉ của trang web được vào hiện tại
S912. Chứng chỉ của trang web hiện tại là giống như chứng chỉ được mang trong thông báo
Không
Có
S913. Tin nhắn SMS có mã xác minh
S914. Trích ra mã xác minh từ tin nhắn SMS có mã xác minh và điền mã xác minh vào trong hộp nhập mã xác minh trên trang web
S915. Mã xác minh
Mã xác minh
S916. Kết quả kiểm tra
Kết quả kiểm tra
S917. Thực hiện thao tác tương ứng dựa trên kết quả kiểm tra
S917. Từ chối gửi tin nhắn SMS có mã xác minh đến môđun trình duyệt

FIG. 9B

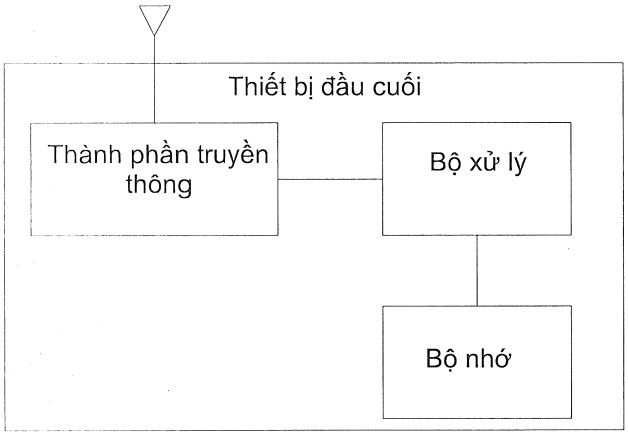



FIG. 10