



(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)



1-0026259

(51)⁷ H04L 9/32

(13) B

(21) 1-2016-04653

(22) 08/05/2014

(86) PCT/CN2014/077074 08/05/2014

(87) WO2015/168913 12/11/2015

(45) 25/11/2020 392

(43) 27/02/2017 347A

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)

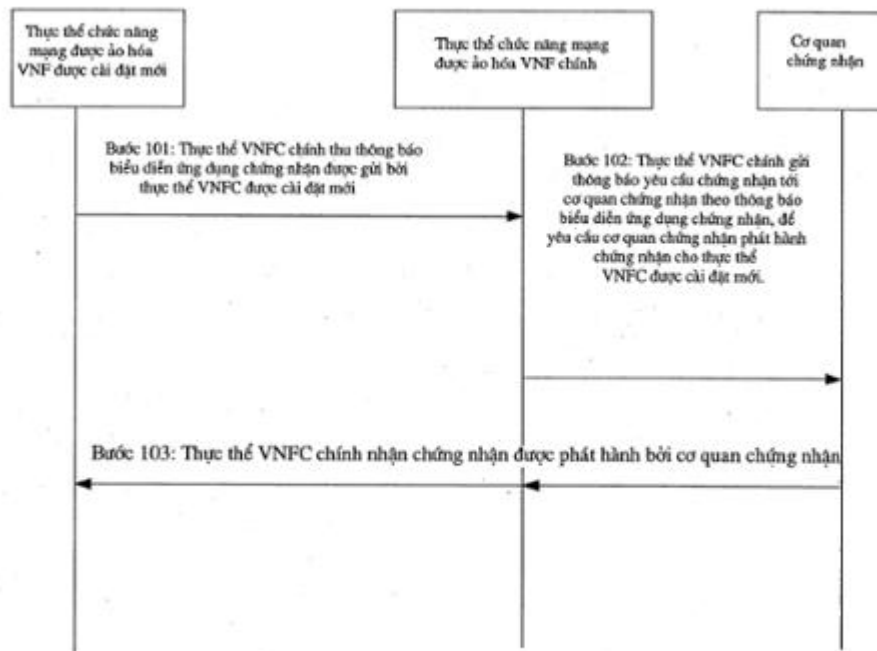
Huawei Administration Building, Bantian, Longgang, Shenzhen, Guangdong 518129, China

(72) FENG, Chengyan (CN); WANG, Jiangsheng (CN).

(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) THIẾT BỊ NHẬN CHỨNG NHẬN

(57) Sáng chế bộc lộ phương pháp và thiết bị nhận chứng nhận. Phương pháp này bao gồm các bước: thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể hợp phần chức năng mạng được ảo hóa (VNFC- Virtualized Network Function Component) được cài đặt mới; gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận; và nhận chứng nhận được phát hành bởi cơ quan chứng nhận. Theo cách này, thực thể VNFC được cài đặt mới không cần phải sử dụng cách thức hiện có để chức năng mạng được ảo hóa (VNF- Virtualized Network Function) nhận được chứng nhận, điều này tránh được một cách có hiệu quả vấn đề là phát sinh quy trình rắc rối và phức tạp hơn khi thực thể VNFC được cài đặt mới nhận chứng nhận; nhờ thực thể VNFC khác ở trên cùng một nền hạ tầng ảo hóa chức năng mạng và đã được nhận chứng nhận, mà kênh tin cậy, được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận bởi thực thể VNFC khác đó, được sử dụng để thay thế thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể được nhận một cách an toàn, mà quy trình này cũng được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống này được nâng cao.



Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến lĩnh vực triển khai mạng ảo, và cụ thể là, đến phương pháp và thiết bị nhận chứng nhận.

Tình trạng kỹ thuật của sáng chế

NFV (Network Function Virtualization, ảo hóa chức năng mạng) là tổ chức tiêu chuẩn được thành lập để "ảo hóa mạng thông thường", và tạo ra bộ tiêu chuẩn để triển khai mạng trong môi trường ảo hóa. Nhờ các tiêu chuẩn được tạo ra bởi tổ chức NFV mà các tính năng như ảo hóa mạng và triển khai linh hoạt có thể được thực hiện.

Do VNF (Virtualized Network Function, chức năng mạng được ảo hóa) được đưa vào trong công nghệ NFV, nên cấu trúc mạng CT thông thường và cấu trúc nút mạng đã có sự thay đổi tương đối lớn. Trong cấu trúc viễn thông mới, nút viễn thông vật lý thông thường tiến hóa thành nút ảo trong thiết bị ảo, và tồn tại dưới dạng máy ảo. Theo cách này, nhiều nút vật lý thông thường cùng được triển khai trong cùng máy chủ vật lý, để chia sẻ tài nguyên phần cứng, và thậm chí chia sẻ các tài nguyên với phần mềm ứng dụng của bên thứ ba khác, nhờ đó tăng được hiệu suất truyền thông giữa các máy ảo khác nhau trong cùng một thiết bị ảo.

Ví dụ, mạng IP (Internetworking Protocol, Giao thức Liên kết mạng) thông thường tiến hóa thành mạng ảo nhờ bộ chuyển đổi ảo và bộ thích ứng mạng ảo, và việc truyền thông được thực hiện giữa các máy ảo khác nhau nhờ mạng ảo này, sao cho đi vòng qua thiết bị mạng vật lý thông thường.

Mạng ảo giống như mạng thông thường, và cả việc truyền thông được thực hiện giữa các máy ảo bên trong mạng ảo và việc truyền thông được thực hiện giữa máy ảo và mạng bên ngoài đều gặp phải nguy cơ an ninh mạng. Ví dụ, các máy ảo tấn công lẫn nhau, hoặc ứng dụng của máy chủ thực hiện việc tấn công bằng cách sử dụng sự liên kết tới mạng máy ảo. Do đó, sự kết nối an toàn được thiết lập giữa các máy ảo trong mạng ảo bằng cách sử dụng công nghệ an ninh (ví dụ, công nghệ IPSec hoặc công nghệ TLS (Transport Layer Security, giao thức an toàn lớp truyền dẫn)). Trong công nghệ an ninh này, hai máy ảo truyền thông với nhau cần được tạo cấu hình với chứng nhận dựa trên X.509, để thực hiện việc xác thực lẫn nhau bởi đầu cuối ngang hàng truyền thông.

Trong tình huống được ảo hóa, VNF là nhóm phần mềm, và được tạo đối tượng khi cần. Việc tạo đối tượng VNF là quy trình xác định các tài nguyên ảo hóa cần thiết và phân phối các tài nguyên ảo hóa cần thiết này cho một phần mềm VNF và cài đặt phần mềm VNF này. VNF được tạo đối tượng không phải là phần tử phần cứng thông thường, và không luôn luôn tồn tại, mà được tạo ra dưới dạng phần mềm theo nhu cầu và tồn tại động, và vị trí vật lý mà ở đó VNF được tạo đối tượng được cài đặt là không cố định. Do đó, phương pháp tạo cấu hình chứng nhận phần tử thông thường không được áp dụng cho phần mềm ảo, ví dụ, VNF.

Để tạo cấu hình chứng nhận cho VNF theo đặc tính của VNF, cách thức tạo cấu hình chứng nhận được đề xuất, nghĩa là, trong quy trình tạo đối tượng VNF, người thao tác tạo cấu hình chứng nhận ban đầu cho VNF được tạo đối tượng, và cài đặt chứng nhận ban đầu này vào VNF được tạo đối tượng; VNF được tạo đối tượng sử dụng chứng nhận ban đầu để nhận chứng nhận từ cơ quan chứng nhận (CA, Certification Authority).

Trong ứng dụng thực tế, VNFC (Virtualized Network Function Component, hợp phần chức năng mạng được ảo hóa) được sử dụng dưới dạng hợp phần của VNF, và cách thức để VNFC nhận chứng nhận do CA phát hành cũng giống như cách thức để VNF nhận chứng nhận. Nghĩa là, khi VNF được tạo đối tượng, thì chứng nhận ban đầu được tạo cấu hình đối với mỗi VNFC, và chứng nhận ban đầu được cài đặt một cách thành công sau khi VNFC được tạo đối tượng; sau đó thực thể VNFC này sử dụng chứng nhận ban đầu để yêu cầu cấp chứng nhận chính thức từ CA. Sau khi chứng nhận ban đầu được đưa vào thì quy trình để VNF nhận được chứng nhận là tương đối phức tạp, và khóa riêng liên quan đến chứng nhận ban đầu gặp phải nguy cơ rò rỉ trong quy trình chuyển giao, điều này làm giảm tính an ninh đối với VNF để nhận chứng nhận.

Tuy nhiên, trong tình huống NFV, thì VNF có thể có nhiều phương án. Trong quy trình sử dụng, để nâng cao hiệu suất mạng, có thể cần phải bổ sung VNFC mới. Nếu VNFC mới được bổ sung này cần truyền thông với bên ngoài thì VNFC mới được bổ sung này cần nhận chứng nhận, nhưng nếu cách thức sử dụng chứng nhận ban đầu để nhận chứng nhận chính thức như nêu trên vẫn được sử dụng, thì quy trình sẽ công kênh và trở nên phức tạp hơn, và hơn nữa, hệ thống sẽ phản ứng chậm hơn và hoạt động kém hiệu quả hơn.

Bản chất kỹ thuật của sáng chế

Vì có vấn đề nêu trên, theo các phương án, sáng chế đề xuất phương pháp và thiết bị nhận chứng nhận, được sử dụng để giải quyết vấn đề về cách thức mà VNFC mới được bổ sung của VNF nhận chứng nhận nhằm nâng cao tốc độ phản ứng của hệ thống, và tăng hiệu quả hoạt động của hệ thống.

Theo khía cạnh thứ nhất của sáng chế, thiết bị nhận chứng nhận được đề xuất, thiết bị này bao gồm:

mô đun thu, được tạo cấu hình để thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể hợp phần chức năng mạng được ảo hóa VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận này chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

mô đun gửi, được tạo cấu hình để gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận thu được bởi mô đun thu, để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

mô đun nhận, được tạo cấu hình để nhận chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận được phát hành bởi cơ quan chứng nhận bằng cách sử dụng khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ nhất, thiết bị này còn bao gồm: mô đun xác thực, trong đó

mô đun thu còn được tạo cấu hình để trước khi mô đun nhận nhận được chứng nhận được phát hành bởi cơ quan chứng nhận, thì thu thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận; và

mô đun xác thực được tạo cấu hình để thực hiện việc xác thực đối với thông báo đáp chứng nhận thu được bởi mô đun thu.

Liên quan đến cách thức thực hiện khả thi thứ nhất theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ hai, thông báo đáp chứng nhận chứa chứng nhận được phát hành bởi cơ quan chứng nhận; và

mô đun nhận được tạo cấu hình cụ thể để khi mô đun xác thực xác định rằng thông

báo đáp chứng nhận đã được xác thực, thì nhận chứng nhận, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới và được chứa trong thông báo đáp chứng nhận, trong đó chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu ứng dụng chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ ba, thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Liên quan đến cách thức thực hiện khả thi thứ ba theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ tư, thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ năm, cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc

sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai vào thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư theo khía cạnh thứ

nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ sáu, mô đun gửi còn được tạo cấu hình để sau khi mô đun nhận nhận được chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, thì gửi, đến thực thể VNFC được cài đặt mới, qua mạng nội bộ, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm theo khía cạnh thứ nhất của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ sáu theo khía cạnh thứ nhất của sáng chế, theo cách thức thực hiện khả thi thứ bảy, thực thể VNFC chính và thực thể VNFC được cài đặt mới là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Theo khía cạnh thứ hai của sáng chế, thiết bị nhận chứng nhận được đề xuất, thiết bị này bao gồm:

mô đun thu, được tạo cấu hình để thu thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

mô đun phát hành chứng nhận, được tạo cấu hình để thực hiện việc xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của thực thể VNFC chính mà thu được bởi mô đun thu, và khi việc xác thực này thành công, thì đạt được chứng nhận cần phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

mô đun gửi, được tạo cấu hình để gửi, tới thực thể VNFC chính, chứng nhận cần được phát hành mà được phát hành bởi mô đun phát hành chứng nhận.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ hai của sáng chế, theo cách thức thực hiện khả thi thứ nhất, mô đun phát hành chứng nhận được tạo cấu hình cụ thể để thực hiện việc xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng

cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ hai của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất theo khía cạnh thứ hai của sáng chế, theo cách thức thực hiện khả thi thứ hai, thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Liên quan đến cách thức thực hiện khả thi thứ hai theo khía cạnh thứ hai của sáng chế, theo cách thức thực hiện khả thi thứ ba, mô đun phát hành chứng nhận còn được tạo cấu hình để thực hiện việc xác thực, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận, đối với thông tin POP được chứa trong thông báo yêu cầu chứng nhận.

Theo khía cạnh thứ ba của sáng chế, thiết bị nhận chứng nhận được đề xuất, thiết bị này bao gồm:

mô đun gửi, được tạo cấu hình để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể hợp phần chức năng mạng được ảo hóa VNFC chính, trong đó thông báo biểu thị ứng dụng chứng nhận này chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận này chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

mô đun thu, được tạo cấu hình để thu chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính, trong đó chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Liên quan đến cách thức thực hiện khả thi theo khía cạnh thứ ba của sáng chế, theo cách thức thực hiện khả thi thứ nhất, mô đun thu còn được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thu thông tin chứng nhận ứng dụng được gửi bởi NFVO hoặc VNFM, trong đó thông tin ứng dụng chứng nhận này chứa thông tin về thực thể VNFC chính được sử dụng dưới dạng chương

trình đại lý đối với ứng dụng chứng nhận.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ ba của sáng chế, theo cách thức thực hiện khả thi thứ hai, thiết bị này còn bao gồm:

mô đun thiết lập, được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thiết lập, theo thông tin ứng dụng chứng nhận thu được bởi mô đun thu, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận, trong đó kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ ba theo sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ ba của sáng chế, theo cách thức thực hiện khả thi thứ ba, mô đun thu được tạo cấu hình cụ thể để: trong khi cài đặt, thu thông tin ứng dụng chứng nhận được đưa vào bởi hạ tầng ảo hóa chức năng mạng NFVI.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ ba của sáng chế, theo cách thức thực hiện khả thi thứ tư, thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận chứa địa chỉ Giao thức Internet IP, bộ nhận dạng Điều Khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ ba của sáng chế, theo cách thức thực hiện khả thi thứ năm, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc

sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ ba của sáng chế,

hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ ba của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ ba của sáng chế, theo cách thức thực hiện khả thi thứ sáu, cách thức kích hoạt thực thể VNFC được cài đặt mới để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính bao gồm các bước:

kích hoạt bằng cách tạo đối tượng VNF; hoặc kích hoạt bằng cách phân tải ngoài VNF.

Theo khía cạnh thứ tư của sáng chế, thiết bị nhận chứng nhận được đề xuất, thiết bị này bao gồm:

bộ thu tín hiệu, được tạo cấu hình để thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể chức năng mạng ảo VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

bộ phát tín hiệu, được tạo cấu hình để gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận, để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

bộ xử lý, được tạo cấu hình để nhận chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận được phát hành bởi cơ quan chứng nhận bằng cách sử dụng khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ nhất, bộ thu tín hiệu còn được tạo cấu hình để: trước khi nhận được chứng nhận được phát hành bởi cơ quan chứng nhận, thì thu thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận; và

bộ xử lý còn được tạo cấu hình để thực hiện việc xác thực đối với thông báo đáp chứng nhận đã thu được.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ hai, thông báo đáp chứng nhận chứa chứng

nhận được phát hành bởi cơ quan chứng nhận; và

bộ xử lý được tạo cấu hình cụ thể để: khi thông báo đáp chứng nhận đã được xác thực, thì nhận chứng nhận, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới và được chứa trong thông báo đáp chứng nhận, trong đó chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu ứng dụng chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ ba, thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ tư, thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ năm, cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc

sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ tư của sáng chế,

hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ sáu, bộ phát tín hiệu còn được tạo cấu hình để: sau khi nhận được chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, thì gửi, tới thực thể VNFC được cài đặt mới qua mạng nội bộ, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ tư của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ sáu của khía cạnh thứ tư của sáng chế, theo cách thức thực hiện khả thi thứ bảy, thực thể VNFC chính và thực thể VNFC được cài đặt mới là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Theo khía cạnh thứ năm của sáng chế, thiết bị nhận chứng nhận được đề xuất, thiết bị này bao gồm:

bộ thu tín hiệu, được tạo cấu hình để thu thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

bộ xử lý, được tạo cấu hình để thực hiện việc xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của thực thể VNFC chính, và khi việc xác thực này thành công, đạt được chứng nhận cần phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

bộ phát tín hiệu, được tạo cấu hình để gửi chứng nhận cần được phát hành tới thực thể VNFC chính.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ năm của sáng chế, theo cách thức thực hiện khả thi thứ nhất, bộ xử lý được tạo cấu hình cụ thể để thực hiện việc xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng cách sử dụng chứng

nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ năm của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ năm của sáng chế, theo cách thức thực hiện khả thi thứ hai, thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ năm của sáng chế, theo cách thức thực hiện khả thi thứ ba, bộ xử lý còn được tạo cấu hình để thực hiện việc xác thực đối với thông tin POP được chứa trong thông báo yêu cầu chứng nhận bởi cơ quan chứng nhận, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Theo khía cạnh thứ sáu của sáng chế, thiết bị nhận chứng nhận được đề xuất, thiết bị này bao gồm:

bộ phát tín hiệu, được tạo cấu hình để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể hợp phần chức năng mạng được ảo hóa VNFC chính, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

bộ thu tín hiệu, được tạo cấu hình để thu chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính, trong đó chứng nhận này đạt được bởi cơ quan chứng nhận bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ sáu của sáng chế, theo cách thức thực hiện khả thi thứ nhất, bộ thu tín hiệu còn được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thu thông tin chứng nhận ứng dụng được gửi bởi NFVO hoặc VNFM, trong đó thông tin ứng dụng chứng nhận này chứa thông tin về thực thể VNFC chính được sử dụng dưới dạng chương

trình đại lý đối với ứng dụng chứng nhận.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ sáu của sáng chế, theo cách thức thực hiện khả thi thứ hai, thiết bị này còn bao gồm: bộ xử lý, trong đó bộ xử lý này được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thiết lập, theo thông tin ứng dụng chứng nhận, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận, trong đó kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ sáu của sáng chế, theo cách thức thực hiện khả thi thứ ba, bộ thu tín hiệu được tạo cấu hình cụ thể để: trong khi cài đặt, thu thông tin ứng dụng chứng nhận được đưa vào bởi hạ tầng ảo hóa chức năng mạng NFVI.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ sáu của sáng chế, theo cách thức thực hiện khả thi thứ tư, thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận chứa địa chỉ Giao thức Internet IP, bộ nhận dạng Điều Khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ sáu của sáng chế, theo cách thức thực hiện khả thi thứ năm, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ sáu của sáng chế,

hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ sáu của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ sáu của sáng chế, theo cách thức thực hiện khả thi thứ sáu, cách thức kích hoạt thực thể VNFC được cài đặt mới để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính bao gồm các bước:

kích hoạt bằng cách tạo đối tượng VNF; hoặc

kích hoạt bằng cách phân tải ngoài VNF.

Theo khía cạnh thứ bảy của sáng chế, phương pháp nhận chứng nhận được đề xuất, phương pháp này bao gồm các bước:

thu, bởi thực thể hợp phần chức năng mạng được ảo hóa VNFC chính, thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

gửi, bởi thực thể VNFC chính, thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận, để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

nhận, bởi thực thể VNFC chính, chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận được phát hành bởi cơ quan chứng nhận bằng cách sử dụng khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ nhất, trước khi nhận, bởi thực thể VNFC chính, chứng nhận được phát hành bởi cơ quan chứng nhận, phương pháp này còn bao gồm bước:

thu, bởi thực thể VNFC chính, thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận, và thực hiện việc xác thực đối với thông báo đáp chứng nhận đã thu được.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ hai, thông báo đáp chứng nhận chứa chứng nhận được phát hành bởi cơ quan chứng nhận; và

việc nhận chứng nhận được phát hành bởi cơ quan chứng nhận bao gồm:

khi thông báo đáp chứng nhận đã được xác thực, thì nhận, bởi thực thể VNFC chính, chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới và được chứa trong thông báo đáp chứng nhận, trong đó chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu ứng dụng chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ ba, thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ tư, thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ năm, cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc

sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai vào thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ bảy của

sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ sáu, sau khi nhận, bởi thực thể VNFC chính, chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, phương pháp này còn bao gồm bước:

gửi, bởi thực thể VNFC chính, tới thực thể VNFC được cài đặt mới qua mạng nội bộ, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ bảy của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ sáu của khía cạnh thứ bảy của sáng chế, theo cách thức thực hiện khả thi thứ bảy, thực thể VNFC chính và thực thể VNFC được cài đặt mới là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Theo khía cạnh thứ tám của sáng chế, phương pháp nhận chứng nhận được đề xuất, phương pháp này bao gồm các bước:

thu, bởi cơ quan chứng nhận, thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

thực hiện, bởi cơ quan chứng nhận, xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của thực thể VNFC chính, và khi việc xác thực này thành công, đạt được chứng nhận cần được phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

gửi, bởi cơ quan chứng nhận, chứng nhận cần được phát hành tới thực thể VNFC chính.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tám của sáng chế, theo cách thức thực hiện khả thi thứ nhất, việc thực hiện, bởi cơ quan chứng nhận, xác thực

đối với thông báo yêu cầu chứng nhận theo chứng nhận của VNFC chính bao gồm:

thực hiện, bởi cơ quan chứng nhận, xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ tám của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ tám của sáng chế, theo cách thức thực hiện khả thi thứ hai, thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ tám của sáng chế, theo cách thức thực hiện khả thi thứ ba, việc thực hiện, bởi cơ quan chứng nhận, xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của VNFC chính còn bao gồm:

thực hiện, bởi cơ quan chứng nhận, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận, việc xác thực đối với thông tin POP được chứa trong thông báo yêu cầu chứng nhận.

Theo khía cạnh thứ chín của sáng chế, phương pháp nhận chứng nhận được đề xuất, phương pháp này bao gồm các bước:

gửi, bởi thực thể hợp phần chức năng mạng được ảo hóa VNFC được cài đặt mới, thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

thu, bởi thực thể VNFC được cài đặt mới, chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính, trong đó chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ chín của sáng chế, theo

cách thức thực hiện khả thi thứ nhất, trước khi gửi thông báo biểu thị ứng dụng chứng nhận tới VNFC chính, phương pháp này còn bao gồm bước:

thu, bởi thực thể VNFC được cài đặt mới, thông tin ứng dụng chứng nhận được gửi bởi NFVO hoặc VNFM, trong đó thông tin ứng dụng chứng nhận này chứa thông tin về thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ chín của sáng chế, theo cách thức thực hiện khả thi thứ hai, trước khi gửi, bởi thực thể VNFC được cài đặt mới, thông báo biểu thị ứng dụng chứng nhận tới VNFC chính, phương pháp này còn bao gồm bước:

thiết lập, bởi thực thể VNFC được cài đặt mới, theo thông tin ứng dụng chứng nhận, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận, trong đó kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ chín của sáng chế, theo cách thức thực hiện khả thi thứ ba, nhận, bởi thực thể VNFC được cài đặt mới, thông tin ứng dụng chứng nhận chứa:

trong khi cài đặt, thu, bởi thực thể VNFC được cài đặt mới, thông tin ứng dụng chứng nhận được đưa vào bởi hạ tầng ảo hóa chức năng mạng NFVI.

Liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ chín của sáng chế, theo cách thức thực hiện khả thi thứ tư, thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận chứa địa chỉ Giao thức Internet IP, bộ nhận dạng Điều Khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ chín

của sáng chế, theo cách thức thực hiện khả thi thứ năm, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai vào thực thể VNFC được cài đặt mới.

Liên quan đến cách thức thực hiện khả thi của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ nhất của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ hai của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ ba của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ tư của khía cạnh thứ chín của sáng chế, hoặc liên quan đến cách thức thực hiện khả thi thứ năm của khía cạnh thứ chín của sáng chế, theo cách thức thực hiện khả thi thứ sáu, cách thức kích hoạt thực thể VNFC được cài đặt mới để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính bao gồm các bước:

kích hoạt bằng cách tạo đối tượng VNF; hoặc

kích hoạt bằng cách phân tải ngoài VNF.

Theo các phương án của sáng chế, khi thực thể VNFC khác, mà thực thể này đã nhận chứng nhận, tồn tại trên nền NFVI, thì kênh tin cậy được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận, bởi thực thể VNFC khác đó, sẽ được sử dụng để thay thế thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể nhận được một cách an toàn, mà quy trình còn được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống được nâng cao.

Mô tả vắn tắt các hình vẽ

Để mô tả giải pháp kỹ thuật theo các phương án của sáng chế một cách rõ ràng hơn, phần dưới đây sẽ mô tả ngắn gọn các hình vẽ kèm theo vốn cần thiết để mô tả các phương án của sáng chế. Rõ ràng là, các hình vẽ kèm theo trong phần mô tả sau đây chỉ thể hiện một số phương án của sáng chế, và người có hiểu biết trung bình trong lĩnh vực kỹ thuật này vẫn có thể tạo ra các hình vẽ khác từ các hình vẽ kèm theo mà không cần đến nỗ lực sáng tạo.

FIG. 1 là lưu đồ của phương pháp nhận chứng nhận theo Phương án 1 của sáng chế;

FIG. 2 là lưu đồ của phương pháp nhận chứng nhận theo Phương án 2 của sáng chế;
 FIG. 3 là lưu đồ của phương pháp nhận chứng nhận theo Phương án 3 của sáng chế;
 FIG. 4A và FIG. 4B là các lưu đồ của phương pháp nhận chứng nhận theo Phương án 4 của sáng chế;

FIG. 5 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 6 của sáng chế;
 FIG. 6 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 7 của sáng chế;
 FIG. 7 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 8 của sáng chế;
 FIG. 8 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 9 của sáng chế;
 FIG. 9 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 10 của sáng chế; và

FIG. 10 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 11 của sáng chế.

Mô tả chi tiết các phương án thực hiện sáng chế

Nhằm đạt được mục đích của sáng chế, các phương án của sáng chế đề xuất phương pháp và thiết bị nhận chứng nhận. Thực thể VNFC chính thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận này chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và nhận chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Theo cách này, thực thể VNFC được cài đặt mới không cần phải sử dụng cách thức hiện có để VNF nhận được chứng nhận, nên tránh được một cách có hiệu quả vấn đề là quy trình rắc rối và phức tạp hơn vốn phát sinh khi thực thể VNFC được cài đặt mới nhận chứng nhận; nhờ vào thực thể VNFC khác vốn trên cùng một nền NFVI và đã nhận được chứng nhận, kênh tin cậy, được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận bởi thực thể VNFC khác đó, được sử dụng để thay thế thực thể VNFC được

cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể được nhận một cách an toàn, mà quy trình cũng được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống được nâng cao.

Cần lưu ý rằng, theo các phương án của sáng chế, thực thể VNFC được cài đặt mới bắt đầu được cài đặt khi thu được lệnh thao tác tạo đối tượng VNFC hoặc lệnh thao tác phân tải ngoài VNF; theo các phương án của sáng chế, khi thực thể VNFC được cài đặt mới cần yêu cầu cấp chứng nhận, thì thực thể VNFC khác trên cùng một nền NFVI và đã nhận được chứng nhận có thể được sử dụng dưới dạng chương trình đại lý để yêu cầu cấp chứng nhận.

Phần dưới đây mô tả chi tiết các phương án của sáng chế có dựa vào các hình vẽ kèm theo trong bản mô tả.

Phương án 1

Như được thể hiện trên FIG. 1, FIG. 1 là lưu đồ của phương pháp nhận chứng nhận theo Phương án 1 của sáng chế. Phương pháp này có thể được mô tả như sau: Phương án này của sáng chế có thể được thực hiện bởi thực thể VNFC đại lý cần yêu cầu cấp chứng nhận đối với thực thể VNFC được cài đặt mới, trong đó thực thể VNFC đại lý còn được gọi là thực thể VNFC chính; hoặc có thể là hợp phần VNF khác nằm trong thực thể VNFC liên quan đến thực thể VNFC được cài đặt mới và đã được nhận chứng nhận.

Bước 101: Thực thể VNFC chính thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể VNFC được cài đặt mới.

Thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ở bước 101, khi VNFM (VNF Manager, bộ quản lý VNF) thu được lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới, thì VNFM gửi thông tin yêu cầu xác thực lệnh thao tác tới NFVO.

Cần lưu ý rằng, lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới chứa lệnh thao tác tạo đối tượng VNFC, lệnh thao tác phân tải ngoài VNF, hoặc các lệnh tương tự.

Lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới có thể được kích hoạt thủ công hoặc tự động bằng cách sử dụng EMS (Element Management System, hệ thống quản lý phần tử), hoặc có thể đạt được bởi VNFM khi thu thập dữ liệu đo từ VNF và thấy

rằng cần thực hiện phân tải ngoài, nhưng không bị giới hạn ở đây.

Khi thu được thông tin yêu cầu xác thực lệnh thao tác, thì NFVO thực thi quyết định thao tác, kiểm tra sự khả dụng của tài nguyên, và gửi thông báo xác nhận lệnh thao tác tới VNFM.

Thông báo xác nhận lệnh thao tác chứa ít nhất một hoặc nhiều thông tin trong số thông tin vị trí của thực thể VNFC mới được tạo ra hoặc thông tin cơ quan chứng nhận.

Thông tin vị trí của thực thể VNFC mới được tạo ra có thể là thông tin VIM liên quan đến NFVI mà trong đó thực thể VNFC được bố trí, ví dụ, thông tin bộ nhận dạng VIM hoặc thông tin địa chỉ VIM.

Thông tin cơ quan chứng nhận có thể chứa bộ nhận dạng của cơ quan chứng nhận trong miền của người thao tác, địa chỉ IP của cơ quan chứng nhận, hoặc thông tin tương tự.

Cơ quan chứng nhận có thể là phần tử mạng có chức năng phát hành chứng nhận, như cơ quan chứng nhận (CA, Certificate Authority), cơ quan đăng ký (RA, Registration Authority), hoặc hệ thống quản lý phần tử (EMS, Element Management System).

Trong trường hợp này, VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới theo thông tin vị trí của thực thể VNFC chính và thông tin vị trí của thực thể VNFC mới được tạo ra. Thông tin vị trí của thực thể VNFC mới được tạo ra được gửi bởi NFVO tới VNFM bằng cách sử dụng thông báo xác nhận lệnh thao tác.

Thông tin vị trí của thực thể VNFC mới được tạo ra có thể là thông tin VIM liên quan đến NFVI mà trong đó VNFC được bố trí, ví dụ, thông tin bộ nhận dạng VIM hoặc thông tin địa chỉ VIM.

Chính sách ứng dụng chứng nhận được sử dụng để xác định chương trình đại lý yêu cầu cấp chứng nhận cho thực thể VNFC được cài đặt mới.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Sau khi xác nhận rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI, thì VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới, và gửi thông tin ứng dụng chứng nhận tới thực thể VNFC được cài đặt mới.

Chính sách ứng dụng chứng nhận làm việc với cách thức mà được sử dụng để yêu cầu cấp chứng nhận cho thực thể VNFC mới được tạo ra, và với đối tượng được sử dụng dưới dạng chương trình đại lý nếu cơ chế chương trình đại lý được sử dụng.

Chính sách ứng dụng chứng nhận chứa thông tin ứng dụng chứng nhận, trong đó thông tin ứng dụng chứng nhận chứa một hoặc nhiều thông báo biểu thị ứng dụng chứng nhận hoặc chỉ báo cách thức ứng dụng chứng nhận.

Thông báo biểu thị ứng dụng chứng nhận chứa thông tin bộ nhận dạng của chương trình đại lý ứng dụng chứng nhận, ví dụ, địa chỉ IP (Internet Protocol, Giao thức Internet), bộ nhận dạng MAC (Media Access Control, Điều khiển Truy cập Môi trường), hoặc địa chỉ ảo NIC (Network Information Center, trung tâm thông tin mạng).

Chỉ báo cách thức ứng dụng chứng nhận có thể là sự chỉ báo rõ ràng hoặc sự chỉ báo ẩn. Sự chỉ báo rõ ràng là, ví dụ, cơ chế chương trình đại lý; và sự chỉ báo ẩn có thể được ngầm định bởi thông tin chương trình đại lý được định rõ, hoặc yếu tố tương tự.

Cần lưu ý rằng, chính sách ứng dụng chứng nhận chỉ báo thực thể VNFC đại lý, nghĩa là, thực thể VNFC chính yêu cầu cấp chứng nhận cho thực thể VNFC được cài đặt mới.

Ví dụ, đối với Đại lý VNFM hoặc VNFC Chính được xác định trong NFV, VNFC Chính có thể là VNFC đầu tiên được tạo ra trong quy trình tạo đối tượng VNF, và được tạo cấu hình để chịu trách nhiệm quản lý nội bộ của VNF; và trong quy trình phân tải ngoài VNF, thì VNFC Chính có thể được xác định là thực thể VNFC liên quan đến thực thể VNFC và được bố trí trên cùng một nền phần cứng hạ tầng ảo hóa chức năng mạng (NFVI, Network Function Virtualization Infrastructure).

VNFM gửi thông báo tạo VM tới VIM, để yêu cầu VIM này phân phối tài nguyên tới VNFC sẽ được cài đặt, trong đó thông báo tạo VM này chứa thông tin ứng dụng chứng nhận.

VIM ra lệnh cho NFVI tạo ra VM, và gửi thông tin ứng dụng chứng nhận tới NFVI, và NFVI tạo ra VM, và gửi thông báo xác nhận đã tạo ra tới VIM.

Sau khi VM được tạo ra, NFVI bắt đầu thực thể VNFC theo cách thức an toàn, chạy thực thể VNFC được cài đặt mới trên VM được tạo ra, và đưa thông tin ứng dụng chứng nhận vào thực thể VNFC được cài đặt mới.

Thực thể VNFC được cài đặt mới xác định, theo thông báo biểu thị ứng dụng chứng nhận được chứa trong thông tin ứng dụng chứng nhận, thực thể VNFC chính mà được sử dụng dưới dạng chương trình đại lý để thực hiện chứng nhận ứng dụng, và gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính.

Thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Cần lưu ý rằng, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận có thể được xác định theo cách thức sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc khi hạ tầng ảo hóa chức năng mạng NFVI tạo đối tượng thực thể VNFC được cài đặt mới, sinh ra cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Ngoài ra, thông báo biểu thị ứng dụng chứng nhận có thể còn chứa chỉ báo biểu thị chứng nhận, thông tin cơ quan chứng nhận, hoặc thông tin tương tự.

Bước 102: Thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận, để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới.

Thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ở bước 102, giả định rằng thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận của thực thể VNFC được cài đặt mới để thay thế thực thể VNFC được cài đặt mới để đăng ký chứng nhận với cơ quan chứng nhận.

Khi thu được thông báo biểu thị ứng dụng chứng nhận, thì thực thể VNFC chính sinh ra thông báo yêu cầu chứng nhận theo thông báo biểu thị ứng dụng chứng nhận này.

Thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ngoài ra, thực thể VNFC chính ký thông báo yêu cầu chứng nhận được tạo ra bằng

cách sử dụng khóa riêng tương ứng với chứng nhận cài đặt.

Thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận.

Trong trường hợp này, khi thu được thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, cơ quan chứng nhận thực hiện xác thực đối với chữ ký của thông báo yêu cầu chứng nhận thu được bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện xác thực đối với chứng nhận của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc hoặc chứng nhận trung gian.

Cần lưu ý rằng, khi giả định rằng việc xác thực được thực hiện đối với chứng nhận của thực thể VNFC chính bằng cách sử dụng chứng nhận trung gian, thì việc xác thực cũng cần được thực hiện đối với chứng nhận trung gian bằng cách sử dụng chứng nhận CA gốc.

Khi việc xác thực này thành công, thì cơ quan chứng nhận ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, và gửi thông báo đáp chứng nhận tới VNFC chính.

Thông báo đáp chứng nhận chứa chứng nhận được phát hành cho thực thể VNFC được cài đặt mới, và/hoặc chứng nhận CA gốc hoặc thông tin tương tự.

Bước 103: Thực thể VNFC chính nhận chứng nhận được phát hành bởi cơ quan chứng nhận.

Chứng nhận được phát hành bởi cơ quan chứng nhận theo khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ở bước 103, trước khi nhận được chứng nhận được phát hành bởi cơ quan chứng nhận, phương pháp này còn bao gồm bước:

thu thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận, và thực hiện việc xác thực đối với thông báo đáp chứng nhận đã thu được.

Cụ thể là, khi thu được thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận, thì thực thể VNFC chính thực hiện xác thực đối với chữ ký của thông báo đáp chứng nhận đã thu được bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện xác thực đối với chứng nhận CA bằng cách sử dụng chứng nhận CA gốc hoặc chứng nhận trung gian.

Cần lưu ý rằng, khi giả định rằng việc xác thực được thực hiện đối với chứng nhận của thực thể CA bằng cách sử dụng chứng nhận trung gian, thì việc xác thực cũng cần được thực hiện đối với chứng nhận trung gian bằng cách sử dụng chứng nhận CA gốc.

Khi việc xác thực này thành công, thì thực thể VNFC chính nhận được chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới và được chứa trong thông báo đáp chứng nhận.

Chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Theo cách thức thực hiện khác của sáng chế, thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng (POP, Proof of Possession).

Thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc khi hạ tầng ảo hóa chức năng mạng NFVI tạo đối tượng thực thể VNFC được cài đặt mới, sinh ra cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai vào thực thể VNFC được cài đặt mới.

Theo cách thức thực hiện khác của sáng chế, sau khi thực thể VNFC chính nhận chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, thì phương pháp này còn bao gồm bước:

gửi, tới hạ tầng ảo hóa chức năng mạng NFVI, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, sao cho NFVI gửi, tới thực thể VNFC được cài đặt mới để cài đặt, chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Sau khi cài đặt chứng nhận này, VNFC gửi báo nhận hoàn tất ứng dụng chứng nhận tới NFVI, NFVI gửi hoàn tất ứng dụng chứng nhận tới VIM, và VIM xác nhận hoàn tất phân phối tài nguyên tới VNFM.

VNFM tạo cấu hình thực thể VNFC được cài đặt mới, triển khai tham số cụ thể, và thông báo cho NFVO rằng thao tác đã hoàn tất. NFVO ánh xạ thực thể VNFC tới VIM

và bộ trữ tài nguyên; VNFM gửi thông báo xác nhận tới EMS; EMS bổ sung hoặc cập nhật thực thể VNFC tới thiết bị được quản lý, và EMS thực hiện cấu hình tham số cụ thể ứng dụng đối với thực thể VNFC được cài đặt mới.

Theo phương án này, nếu không có giao diện trực tiếp giữa thực thể VNFC chính và cơ quan chứng nhận, thông báo yêu cầu/đáp chứng nhận có thể được gửi bằng EMS.

Theo phương án này, chứng nhận mà thực thể VNFC được cài đặt mới yêu cầu cấp cũng có thể được phát hành bởi EMS; trong trường hợp này, thực thể VNFC chính thay thế thực thể VNFC được cài đặt mới để thực hiện đăng ký chứng nhận bằng EMS.

Theo giải pháp kỹ thuật theo Phương án 1 của sáng chế, sau khi nhận chứng nhận, thực thể VNFC chính có thể gửi thông báo ứng dụng chứng nhận tới thực thể VNFC được cài đặt mới, và thực thể VNFC được cài đặt mới không cần phải sử dụng cách thức hiện tại để VNF nhận được chứng nhận, điều này tránh được một cách có hiệu quả vấn đề là quy trình rắc rối và phức tạp hơn phát sinh khi thực thể VNFC được cài đặt mới nhận chứng nhận; nhờ thực thể VNFC khác trên cùng một nền NFVI và đã nhận được chứng nhận, kênh tin cậy được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận bởi thực thể VNFC khác đó được sử dụng để thay thế thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể được nhận một cách an toàn, mà quy trình cũng được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống được nâng cao.

Phương án 2

Như được thể hiện trên FIG. 2, FIG. 2 là lưu đồ của phương pháp nhận chứng nhận theo Phương án 2 của sáng chế. Phương pháp này có thể được mô tả như sau: Phương án này của sáng chế có thể được thực hiện bởi CA, hoặc có thể được thực hiện bởi thiết bị khác với chứng nhận được phát hành, ví dụ, RA hoặc EMS.

Bước 201: Cơ quan chứng nhận thu được thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính.

Thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ở bước 201, ngoài Đại lý VNFM hoặc VNFC Chính được xác định trong NFV ra, thì thực thể VNFC chính mà gửi thông báo yêu cầu chứng nhận còn có thể là hợp phần VNF khác nằm trong thực thể VNFC liên quan đến thực thể VNFC được cài đặt mới và

đã được nhận chứng nhận, nhưng không bị giới hạn ở đây.

Bước 202: Cơ quan chứng nhận thực hiện xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của VNFC chính, và khi việc xác thực này thành công, thì đạt được chứng nhận cần được phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ở bước 202, cơ quan chứng nhận thực hiện xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của VNFC chính chứa:

thực hiện, bởi cơ quan chứng nhận, xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

Cụ thể là, khi thu được thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, thì CA thực hiện xác thực đối với chữ ký của thông báo yêu cầu chứng nhận thu được bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện xác thực đối với chứng nhận của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc hoặc chứng nhận trung gian.

Cần lưu ý rằng, khi giả định rằng việc xác thực được thực hiện đối với chứng nhận của thực thể VNFC chính bằng cách sử dụng chứng nhận trung gian, thì việc xác thực cũng cần được thực hiện đối với chứng nhận trung gian bằng cách sử dụng chứng nhận CA gốc.

Khi việc xác thực này thành công, thì CA ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, và sinh ra thông báo đáp chứng nhận.

Thông báo đáp chứng nhận chứa chứng nhận được phát hành cho thực thể VNFC được cài đặt mới, chứng nhận CA gốc, hoặc thông tin tương tự.

Theo phương án khác của sáng chế, nếu thông báo yêu cầu chứng nhận còn chứa thông tin POP, thì cách thức để thực hiện việc xác thực đối với thông báo yêu cầu chứng nhận còn chứa:

thực hiện, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận, việc xác thực đối với thông tin POP được chứa trong thông báo yêu cầu chứng nhận.

Bước 203: Cơ quan chứng nhận gửi chứng nhận cần được phát hành tới thực thể

VNFC chính.

Ở bước 203, CA gửi thông báo đáp chứng nhận được tạo ra tới thực thể VNFC chính, trong đó thông báo đáp chứng nhận chứa chứng nhận được phát hành cho thực thể VNFC được cài đặt mới, và/hoặc chứng nhận CA gốc, hoặc thông tin tương tự.

Theo giải pháp kỹ thuật theo Phương án 2 của sáng chế, nhờ thực thể VNFC khác ở trên cùng một nền phân cứng NFVI và đã được nhận chứng nhận, mà kênh tin cậy, được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận bởi thực thể VNFC khác đó, được sử dụng để thay thế thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể được nhận một cách an toàn, mà quy trình cũng được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống được nâng cao.

Phương án 3

Như được thể hiện trên FIG. 3, FIG. 3 là lưu đồ của phương pháp nhận chứng nhận theo Phương án 3 của sáng chế. Phương pháp có thể được mô tả như sau: Phương án này của sáng chế được thực thi bởi thực thể VNFC được cài đặt mới.

Bước 301: Thực thể VNFC được cài đặt mới gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính.

Thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Ở bước 301, trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới thực thể VNFC chính, phương pháp này còn bao gồm bước:

thu, bởi thực thể VNFC được cài đặt mới, thông tin ứng dụng chứng nhận được gửi bởi NFVO hoặc VNFM.

Thông tin ứng dụng chứng nhận chứa thông tin về thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

Cụ thể là, trong quy trình cài đặt, thực thể VNFC được cài đặt mới thu thông báo

chính sách ứng dụng chứng nhận được đưa vào bởi NFVI.

Cách thức để xác định thông báo chính sách ứng dụng chứng nhận chứa, nhưng không bị giới hạn bởi, hai dạng dưới đây:

Dạng thứ nhất: NFVO quản lý luồng công việc NFV xác định thông tin chính sách ứng dụng chứng nhận theo thông tin vị trí của VNFC chính và thực thể VNFC mới được tạo ra.

Dạng thứ hai: VNFM xác định thông tin chính sách ứng dụng chứng nhận theo thông tin vị trí của VNFC chính và thực thể VNFC mới được tạo ra, trong đó thông tin vị trí của thực thể VNFC mới được tạo ra được gửi bởi NFVO tới VNFM.

Thông tin vị trí của VNFC chính và thực thể VNFC mới được tạo ra là: thông tin VIM liên quan đến NFVI mà trong đó VNFC chính và thực thể VNFC mới được tạo ra được bố trí, như thông tin bộ nhận dạng VIM hoặc thông tin địa chỉ VIM.

Ở dạng thứ nhất, NFVO quản lý luồng công việc NFV xác định chính sách ứng dụng chứng nhận theo thông tin vị trí của VNFC chính và thực thể VNFC mới được tạo ra bằng cách sử dụng cách thức cụ thể như sau:

khi NFVO thu được lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới, thì gửi, bởi NFVO, thông tin yêu cầu xác thực lệnh thao tác tới VNFM.

Cần lưu ý rằng, lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới chứa lệnh thao tác tạo đối tượng VNFC, lệnh thao tác phân tải ngoài VNF, hoặc lệnh tương tự.

Lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới có thể được kích hoạt thủ công hoặc tự động bằng cách sử dụng EMS (Element Management System, hệ thống quản lý phần tử), hoặc có thể đạt được bởi NFVO khi thu thập dữ liệu đo từ VNF và thấy rằng cần thực hiện phân tải ngoài, nhưng không bị giới hạn ở đây.

Khi thu được thông tin yêu cầu xác thực lệnh thao tác, VNFM gửi thông báo xác nhận lệnh thao tác tới NFVO.

Khi thu được thông báo xác nhận lệnh thao tác, NFVO thực thi quyết định thao tác, kiểm tra sự khả dụng của tài nguyên, và chọn bộ trữ tài nguyên và dự trữ tài nguyên.

NFVO xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, và gửi chính sách ứng dụng chứng nhận tới VNFM.

Cụ thể là, NFVO xác nhận, theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, rằng thực thể VNFC được cài đặt mới và thực thể VNFC

chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, NFVO xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Sau khi xác nhận rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI, NFVO xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới, và gửi thông tin ứng dụng chứng nhận tới thực thể VNFC được cài đặt mới.

Chính sách ứng dụng chứng nhận làm việc với cách thức mà được sử dụng để yêu cầu cấp chứng nhận cho thực thể VNFC mới được tạo ra, và với đối tượng được sử dụng dưới dạng chương trình đại lý nếu cơ chế chương trình đại lý được sử dụng.

Ở dạng thứ hai, VNFM xác định chính sách ứng dụng chứng nhận theo thông tin vị trí của VNFC chính và thực thể VNFC mới được tạo ra bằng cách sử dụng cách thức cụ thể như sau:

khi VNFM (VNF Manager, bộ quản lý VNF) thu được lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới, thì gửi, bởi VNFM, thông tin yêu cầu xác thực lệnh thao tác tới NFVO.

Cần lưu ý rằng, lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới chứa lệnh thao tác tạo đối tượng VNFC, lệnh thao tác phân tải ngoài VNF, hoặc lệnh tương tự.

Lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới có thể được kích hoạt thủ công hoặc tự động bằng cách sử dụng EMS (Element Management System, hệ thống quản lý phần tử), hoặc có thể đạt được bởi VNFM khi thu thập dữ liệu đo từ VNF và thấy rằng cần thực hiện phân tải ngoài, nhưng không bị giới hạn ở đây.

Khi thu được thông tin yêu cầu xác thực lệnh thao tác, NFVO thực thi quyết định thao tác, kiểm tra sự khả dụng của tài nguyên, chọn bộ trữ tài nguyên, dự trữ tài nguyên, và gửi thông báo xác nhận lệnh thao tác tới VNFM.

Thông báo xác nhận lệnh thao tác chứa thông tin vị trí của thực thể VNFC mới được tạo ra, và/hoặc thông tin vị trí của thực thể VNFC chính, và/hoặc thông tin cơ quan chứng nhận CA.

Thông tin cơ quan chứng nhận có thể chứa bộ nhận dạng của cơ quan chứng nhận

trong miền của người thao tác, địa chỉ IP của cơ quan chứng nhận, hoặc thông tin tương tự.

Cơ quan chứng nhận có thể là phần tử có chức năng phát hành chứng nhận, như CA, RA, hoặc EMS.

Trong trường hợp này, VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, trong đó thông tin vị trí của thực thể VNFC mới được tạo ra được gửi bởi NFVO tới VNFM bằng cách sử dụng thông báo xác nhận lệnh thao tác.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Sau khi xác nhận rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI, VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới, và gửi thông tin ứng dụng chứng nhận tới thực thể VNFC được cài đặt mới.

Chính sách ứng dụng chứng nhận làm việc với cách thức mà được sử dụng để yêu cầu cấp chứng nhận cho thực thể VNFC mới được tạo ra, và với đối tượng được sử dụng dưới dạng chương trình đại lý nếu cơ chế chương trình đại lý được sử dụng.

Do đó, như có thể thấy, sự khác biệt giữa cách thức thứ nhất để xác định chính sách ứng dụng chứng nhận và cách thức thứ hai để xác định chính sách ứng dụng chứng nhận là ở chỗ: Theo cách thức thứ nhất, chính sách ứng dụng chứng nhận được xác định bởi NFVO, và theo cách thức thứ hai, chính sách ứng dụng chứng nhận được xác định bởi VNFM.

Chính sách ứng dụng chứng nhận chứa thông tin ứng dụng chứng nhận, trong đó thông tin ứng dụng chứng nhận chứa một hoặc nhiều thông báo biểu thị ứng dụng chứng nhận hoặc chỉ báo cách thức ứng dụng chứng nhận.

Thông tin ứng dụng chứng nhận được gửi tới thực thể VNFC được cài đặt mới sau

khi NFVO hoặc VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới.

Cụ thể là, thông tin ứng dụng chứng nhận được tạo ra sau khi NFVO hoặc VNFM xác nhận rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, NFVO hoặc VNFM xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Thông báo biểu thị ứng dụng chứng nhận chứa thông tin bộ nhận dạng của chương trình đại lý ứng dụng chứng nhận, ví dụ, địa chỉ IP (Internet Protocol, Giao thức Internet), bộ nhận dạng MAC (Media access Control, Điều khiển Truy cập Môi trường), hoặc địa chỉ ảo NIC (Network Information Center, trung tâm thông tin mạng).

Chỉ báo cách thức ứng dụng chứng nhận có thể là sự chỉ báo rõ ràng hoặc sự chỉ báo ẩn. Sự chỉ báo rõ ràng là, ví dụ, cơ chế chương trình đại lý; và sự chỉ báo ẩn có thể được ngầm định bởi thông tin chương trình đại lý được định rõ, hoặc thông tin tương tự.

Cần lưu ý rằng, chính sách ứng dụng chứng nhận chỉ báo thực thể VNFC đại lý, nghĩa là, thực thể VNFC chính yêu cầu cấp chứng nhận cho thực thể VNFC được cài đặt mới.

Ví dụ, đối với Đại lý VNFM hoặc VNFC Chính được xác định trong NFV, thì VNFC Chính là VNFC đầu tiên được tạo ra trong quy trình tạo đối tượng VNF, và được tạo cấu hình để chịu trách nhiệm quản lý nội bộ của VNF; và trong quy trình phân tải ngoài VNF, thực thể VNFC chính có thể được xác định như VNFC liên quan đến thực thể VNFC và được bố trí trên cùng một nền phần cứng hạ tầng ảo hóa chức năng mạng (NFVI, Network Function Virtualization Infrastructure).

Tương tự, đối với cách thức thứ nhất để xác định chính sách ứng dụng chứng nhận, sau khi NFVO xác định chính sách ứng dụng chứng nhận, thì NFVO gửi thông báo tạo VM tới VIM, để yêu cầu VIM này phân phối tài nguyên tới VM cần được cài đặt, trong đó thông báo tạo VM chứa thông tin ứng dụng chứng nhận.

VIM ra lệnh cho NFVI tạo ra VM, và gửi thông tin ứng dụng chứng nhận tới NFVI, và NFVI tạo ra VM, và gửi thông báo xác nhận đã tạo ra tới VIM.

Sau khi VM được tạo ra, NFVI bắt đầu thực thể VNFC được cài đặt mới theo cách

thức an toàn, chạy thực thể VNFC được cài đặt mới trên VM được tạo ra, và đưa thông tin ứng dụng chứng nhận vào thực thể VNFC được cài đặt mới.

Đối với cách thức thứ hai để xác định chính sách ứng dụng chứng nhận, sau khi VNFM xác định chính sách ứng dụng chứng nhận, thì VNFM gửi thông báo tạo VM tới VIM, để yêu cầu VIM này phân phối tài nguyên tới VM cần được cài đặt, trong đó thông báo tạo VM chứa thông tin ứng dụng chứng nhận.

VIM ra lệnh cho NFVI tạo ra VM, và gửi thông tin ứng dụng chứng nhận tới NFVI, và NFVI tạo ra VM, và gửi thông báo xác nhận đã tạo ra tới VIM.

Sau khi VM được tạo ra, NFVI bắt đầu VNFC theo cách thức an toàn, chạy thực thể VNFC được cài đặt mới trên VM được tạo ra, và đưa thông tin ứng dụng chứng nhận vào thực thể VNFC được cài đặt mới.

Theo phương án khác của sáng chế, phương pháp này còn bao gồm bước: thiết lập, bởi thực thể VNFC được cài đặt mới theo thông tin ứng dụng chứng nhận, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

Kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền NFVI.

Thực thể VNFC được cài đặt mới xác định, theo thông báo biểu thị ứng dụng chứng nhận được chứa trong thông tin ứng dụng chứng nhận, thực thể VNFC chính mà được sử dụng dưới dạng chương trình đại lý để thực hiện chứng nhận ứng dụng, và gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính.

Cụ thể là, thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận chứa địa chỉ Giao thức Internet IP, bộ nhận dạng Điều Khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

Thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Cần lưu ý rằng, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận có thể được xác định theo cách thức sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc

khi hạ tầng ảo hóa chức năng mạng NFVI tạo đối tượng thực thể VNFC được cài đặt mới, thì sinh ra cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai vào thực thể VNFC được cài đặt mới.

Thông báo biểu thị ứng dụng chứng nhận còn chứa thông tin POP, trong đó thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Ngoài ra, thông báo biểu thị ứng dụng chứng nhận có thể còn chứa chỉ báo biểu thị chứng nhận, thông tin CA, hoặc thông tin tương tự.

Bước 302: Thực thể VNFC được cài đặt mới thu chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính.

Chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký, khi thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Cơ quan chứng nhận có thể là phần tử có chức năng phát hành chứng nhận, như CA, RA, hoặc EMS.

Cần lưu ý rằng, trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới thực thể VNFC chính, phương pháp này còn bao gồm bước:

xác định rằng sự cài đặt của thực thể VNFC được cài đặt mới được kích hoạt bởi việc tạo đối tượng VNF; hoặc

xác định rằng sự cài đặt của thực thể VNFC được cài đặt mới được kích hoạt bởi sự phân tải ngoài VNF.

Theo giải pháp của Phương án 3 của sáng chế, nhờ thực thể VNFC khác trên cùng một nền NFVI và đã nhận được chứng nhận, mà kênh tin cậy, được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận bởi thực thể VNFC khác đó, được sử dụng để thay thế thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể được nhận một cách an toàn, mà quy trình cũng được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống được nâng cao.

Phương án 4

Như được thể hiện trên FIG. 4A và FIG. 4B, FIG. 4A và FIG. 4B là lưu đồ của phương pháp nhận chứng nhận theo Phương án 4 của sáng chế. Phương pháp này có thể được mô tả như sau:

Bước 401: VNFM thu được lệnh thao tác được sử dụng để cài đặt thực thể VNFC

mới.

Cần lưu ý rằng, lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới chứa lệnh thao tác tạo đối tượng VNFC, lệnh thao tác phân tải ngoài VNF, hoặc lệnh tương tự.

Lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới có thể được kích hoạt thủ công hoặc tự động bằng cách sử dụng EMS (Element Management System, hệ thống quản lý phần tử), hoặc có thể đạt được bởi VNFM khi thu thập dữ liệu đo từ VNF và thấy rằng cần thực hiện phân tải ngoài, nhưng không bị giới hạn ở đây.

Bước 402: VNFM gửi thông tin yêu cầu xác thực lệnh thao tác tới NFVO.

Bước 403: Khi thu được thông tin yêu cầu xác thực lệnh thao tác, NFVO thực thi quyết định thao tác, và kiểm tra sự khả dụng của tài nguyên.

Bước 404: NFVO gửi thông báo xác nhận lệnh thao tác tới VNFM.

Thông báo xác nhận lệnh thao tác chứa thông tin vị trí của thực thể VNFC mới được tạo ra và/hoặc thông tin cơ quan chứng nhận.

Thông tin vị trí của thực thể VNFC mới được tạo ra là thông tin VIM liên quan đến NFVI mà trong đó thực thể VNFC mới được tạo ra được bố trí, ví dụ, thông tin bộ nhận dạng VIM hoặc thông tin địa chỉ VIM.

Thông tin cơ quan chứng nhận có thể chứa bộ nhận dạng của cơ quan chứng nhận trong miền của người thao tác, địa chỉ IP của cơ quan chứng nhận, hoặc thông tin tương tự. Cơ quan chứng nhận có thể là phần tử có chức năng phát hành chứng nhận, như CA, RA, hoặc EMS.

Bước 405: VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới theo thông tin vị trí của thực thể VNFC chính và thông tin vị trí của thực thể VNFC mới được tạo ra.

Chính sách ứng dụng chứng nhận được sử dụng để xác định chương trình đại lý yêu cầu cấp chứng nhận cho thực thể VNFC được cài đặt mới.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên

cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Sau khi xác nhận rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI, thì VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới, và gửi thông tin ứng dụng chứng nhận tới thực thể VNFC được cài đặt mới.

Chính sách ứng dụng chứng nhận làm việc với cách thức mà được sử dụng để yêu cầu cấp chứng nhận cho thực thể VNFC mới được tạo ra, và với đối tượng được sử dụng dưới dạng chương trình đại lý nếu cơ chế chương trình đại lý được sử dụng.

Chính sách ứng dụng chứng nhận chứa thông tin ứng dụng chứng nhận, trong đó thông tin ứng dụng chứng nhận chứa một hoặc nhiều thông báo biểu thị ứng dụng chứng nhận hoặc chỉ báo cách thức ứng dụng chứng nhận.

Thông tin ứng dụng chứng nhận được gửi tới thực thể VNFC được cài đặt mới sau khi VNFM xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới.

Cụ thể là, thông tin ứng dụng chứng nhận được tạo ra sau khi VNFM xác nhận rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, VNFM xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Thông báo biểu thị ứng dụng chứng nhận chứa thông tin bộ nhận dạng của chương trình đại lý ứng dụng chứng nhận, ví dụ, địa chỉ IP (Internet Protocol, Giao thức Internet), bộ nhận dạng MAC (Media access Control, Điều khiển Truy cập Môi trường), hoặc địa chỉ ảo NIC (Network Information Center, trung tâm thông tin mạng).

Chỉ báo cách thức ứng dụng chứng nhận có thể là sự chỉ báo rõ ràng hoặc sự chỉ báo ẩn. Sự chỉ báo rõ ràng là, ví dụ, cơ chế chương trình đại lý; và sự chỉ báo ẩn có thể được ngầm định bởi thông tin chương trình đại lý được định rõ, hoặc thông tin tương tự.

Cần lưu ý rằng, chính sách ứng dụng chứng nhận chỉ báo thực thể VNFC đại lý, nghĩa là, thực thể VNFC chính yêu cầu cấp chứng nhận cho thực thể VNFC được cài đặt mới.

Ví dụ, đối với Đại lý VNFM hoặc VNFC Chính được xác định trong NFV, thì VNFC Chính là VNFC đầu tiên được tạo ra trong quy trình tạo đối tượng VNF, và được tạo cấu hình để chịu trách nhiệm quản lý nội bộ của VNF; và trong quy trình phân tải ngoài VNF, VNFC chính có thể được xác định là thực thể VNFC liên quan đến thực thể VNFC và được bố trí trên cùng một nền phần cứng hạ tầng ảo hóa chức năng mạng (NFVI, Network Function Virtualization Infrastructure).

Bước 406: VNFM gửi thông báo tạo VM tới VIM, để yêu cầu VIM này phân phối tài nguyên tới VM cần được cài đặt.

Thông báo tạo VM này chứa thông tin ứng dụng chứng nhận.

Bước 407: VIM ra lệnh cho NFVI để tạo ra VM, và gửi thông tin ứng dụng chứng nhận tới NFVI.

Bước 408: NFVI tạo ra VM, và gửi thông báo xác nhận đã tạo ra tới VIM.

Bước 409: Sau khi VM được tạo ra, NFVI bắt đầu thực thể VNFC được cài đặt mới theo cách thức an toàn, chạy thực thể VNFC được cài đặt mới trên VM được tạo ra, và đưa thông tin ứng dụng chứng nhận vào thực thể VNFC được cài đặt mới.

Bước 410: Thực thể VNFC được cài đặt mới xác định, theo thông tin ứng dụng chứng nhận, thực thể VNFC chính mà được sử dụng dưới dạng chương trình đại lý để thực hiện chứng nhận ứng dụng, và thiết lập kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

Kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền NFVI.

Bước 411: Thực thể VNFC được cài đặt mới gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính.

Thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Cần lưu ý rằng, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận có thể được xác định theo cách thức sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc

khi hạ tầng ảo hóa chức năng mạng NFVI tạo đối tượng thực thể VNFC được cài đặt mới, thì sinh ra cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Thông báo biểu thị ứng dụng chứng nhận còn chứa thông tin POP, trong đó thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong

cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng POP.

Ngoài ra, thông báo biểu thị ứng dụng chứng nhận có thể còn chứa chỉ báo biểu thị chứng nhận, thông tin CA, hoặc thông tin tương tự.

Bước 412: Thực thể VNFC chính trao đổi thông tin với cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận, và nhận chứng nhận được phát hành bởi CA tới thực thể VNFC được cài đặt mới.

Cách thức thực hiện cụ thể của bước 412 cũng giống như cách thức mà trong đó thực thể VNFC chính thay thế thực thể VNFC được cài đặt mới để nhận chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới theo Phương án 1 của sáng chế, Phương án 2 của sáng chế, và Phương án 3 của sáng chế, và không được mô tả chi tiết ở đây.

Bước 413: Thực thể VNFC chính gửi, tới thực thể VNFC được cài đặt mới qua kết nối mạng nội bộ, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Bước 414: Thực thể VNFC được cài đặt mới cài đặt chứng nhận.

Bước 415: Sau khi cài đặt chứng nhận này, VNFC gửi báo nhận hoàn tất ứng dụng chứng nhận tới NFVI.

Bước 416: NFVI gửi hoàn tất ứng dụng chứng nhận tới VIM.

Bước 417: VIM xác nhận hoàn tất phân phối tài nguyên tới VNFM.

Bước 418: VNFM tạo cấu hình thực thể VNFC được cài đặt mới, triển khai tham số cụ thể, và thông báo cho NFVO rằng thao tác đã hoàn tất.

Ngoài ra, NFVO ánh xạ thực thể VNFC tới VIM và bộ trữ tài nguyên; VNFM gửi thông báo xác nhận tới EMS; EMS bổ sung hoặc cập nhật thực thể VNFC tới thiết bị được quản lý, và EMS thực hiện cấu hình tham số cụ thể ứng dụng đối với thực thể VNFC được cài đặt mới.

Theo phương án này, nếu không có giao diện trực tiếp giữa thực thể VNFC chính và cơ quan chứng nhận CA, thì thông báo yêu cầu/đáp chứng nhận có thể được gửi bằng EMS.

Theo phương án này, chứng nhận mà thực thể VNFC được cài đặt mới yêu cầu cấp cũng có thể được phát hành bởi EMS; trong trường hợp này, thực thể VNFC chính thay thế thực thể VNFC được cài đặt mới để thực hiện đăng ký chứng nhận với EMS.

Theo giải pháp kỹ thuật của Phương án 4 của sáng chế, nhờ thực thể VNFC khác

trên cùng một nền NFVI và đã nhận được chứng nhận, kênh tin cậy được thiết lập giữa thực thể VNFC khác đó và cơ quan chứng nhận bởi thực thể VNFC khác đó được sử dụng để thay thế thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, sao cho không chỉ chứng nhận có thể được nhận một cách an toàn, mà quy trình cũng được đơn giản hóa một cách có hiệu quả, tốc độ phản ứng của hệ thống được tăng lên, và hiệu quả hoạt động của hệ thống được nâng cao.

Phương án 5

Phương án 5 của sáng chế liên quan đến phương pháp nhận chứng nhận. Phương pháp nhận chứng nhận theo Phương án 5 của sáng chế và phương pháp nhận chứng nhận theo Phương án 4 về cơ bản là giống nhau, và cũng có sự khác biệt. Sự khác biệt lớn nhất là ở các cách thức khác nhau để xác định chính sách ứng dụng chứng nhận.

Cụ thể là, khi NFVO thu được lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới, thì NFVO gửi thông tin yêu cầu xác thực lệnh thao tác tới VNFM.

Cần lưu ý rằng, lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới chứa lệnh thao tác tạo đối tượng VNFC, lệnh thao tác phân tải ngoài VNF, hoặc lệnh tương tự.

Lệnh thao tác được sử dụng để cài đặt thực thể VNFC mới có thể được kích hoạt thủ công hoặc tự động bằng cách sử dụng EMS (Element Management System, hệ thống quản lý phần tử), hoặc có thể đạt được bởi NFVO khi thu thập dữ liệu đo từ VNF và thấy rằng cần thực hiện phân tải ngoài, nhưng không bị giới hạn ở đây.

Khi thu được thông tin yêu cầu xác thực lệnh thao tác, VNFM gửi thông báo xác nhận lệnh thao tác tới NFVO.

Khi thu thông báo xác nhận lệnh thao tác, NFVO thực thi quyết định thao tác, kiểm tra sự khả dụng của tài nguyên, và chọn bộ trữ tài nguyên và dự trữ tài nguyên. NFVO xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới theo thông tin vị trí của thực thể VNFC chính và thực thể VNFC mới được tạo ra, và gửi chính sách ứng dụng chứng nhận này tới VNFM.

Chính sách ứng dụng chứng nhận này chứa thông tin ứng dụng chứng nhận.

Thông tin ứng dụng chứng nhận được gửi tới thực thể VNFC được cài đặt mới sau khi NFVO xác định chính sách ứng dụng chứng nhận của thực thể VNFC được cài đặt mới.

Cụ thể là, thông tin ứng dụng chứng nhận được tạo ra sau khi NFVO xác nhận rằng

thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, NFVO xác nhận, theo thông tin vị trí của thực thể VNFC được cài đặt mới và thực thể VNFC chính và/hoặc thông tin bộ nhận dạng VNF, rằng thực thể VNFC được cài đặt mới và thực thể VNFC chính là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Phương án 6

Như được thể hiện trên FIG. 5, FIG. 5 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 6 của sáng chế. Thiết bị này bao gồm: mô đun thu 51, mô đun gửi 52, và mô đun nhận 53.

Mô đun thu 51 được tạo cấu hình để thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể chức năng mạng ảo VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Mô đun gửi 52 được tạo cấu hình để gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận thu được bởi mô đun thu 51, và yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Mô đun nhận 53 được tạo cấu hình để nhận chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận được phát hành bởi cơ quan chứng nhận bằng cách sử dụng khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Theo tùy chọn, thiết bị này còn bao gồm: mô đun xác thực 54.

Mô đun thu 51 còn được tạo cấu hình để: trước khi mô đun nhận nhận được chứng nhận được phát hành bởi cơ quan chứng nhận, thì thu thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận.

Mô đun xác thực 54 được tạo cấu hình để thực hiện việc xác thực đối với thông báo đáp chứng nhận thu được bởi mô đun thu 51.

Cụ thể là, thông báo đáp chứng nhận chứa chứng nhận được phát hành bởi cơ quan

chứng nhận.

Mô đun nhận 53 được tạo cấu hình cụ thể để: khi mô đun xác thực xác định rằng thông báo đáp chứng nhận đã được xác thực, thì nhận chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới và được chứa trong thông báo đáp chứng nhận, trong đó chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu ứng dụng chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Theo tùy chọn, thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Theo tùy chọn, thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Theo tùy chọn, cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Mô đun gửi 52 còn được tạo cấu hình để: sau khi mô đun nhận nhận được chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, thì gửi, tới thực thể VNFC được cài đặt mới qua mạng nội bộ, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Thực thể VNFC chính và thực thể VNFC được cài đặt mới là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cần lưu ý rằng, thiết bị theo phương án này của sáng chế có thể là hợp phần khác mà thuộc về, cùng với thực thể VNFC được cài đặt mới, cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI, ví dụ, thực thể VNFC chính. Cách thức thực hiện có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm.

Phương án 7

Như được thể hiện trên FIG. 6, FIG. 6 là sơ đồ kết cấu của thiết bị nhận chứng nhận

theo Phương án 7 của sáng chế. Thiết bị này bao gồm: mô đun thu 61, mô đun phát hành chứng nhận 62, và mô đun gửi 63.

Mô đun thu 61 được tạo cấu hình để thu thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Mô đun phát hành chứng nhận 62 được tạo cấu hình để thực hiện việc xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của thực thể VNFC chính mà thu được bởi mô đun thu, và khi việc xác thực này thành công, thì đạt được chứng nhận cần phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Mô đun gửi 63 được tạo cấu hình để gửi, tới thực thể VNFC chính, chứng nhận cần được phát hành mà được phát hành bởi mô đun phát hành chứng nhận.

Cụ thể là, mô đun phát hành chứng nhận 62 được tạo cấu hình cụ thể để thực hiện việc xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

Theo tùy chọn, thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Mô đun phát hành chứng nhận 62 còn được tạo cấu hình để thực hiện việc xác thực, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận, đối với thông tin POP được chứa trong thông báo yêu cầu chứng nhận.

Cần lưu ý rằng, thiết bị theo phương án này của sáng chế có thể là cơ quan chứng nhận, ví dụ, thiết bị phần tử mạng có chức năng phát hành chứng nhận, như CA, ESA, hoặc RA. Cách thức thực hiện có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm.

Phương án 8

Như được thể hiện trên FIG. 7, FIG. 7 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 8 của sáng chế. Thiết bị này bao gồm: mô đun gửi 71 và mô đun thu 72.

Mô đun gửi 71 được tạo cấu hình để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể hợp phần chức năng mạng được ảo hóa VNFC chính, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Mô đun thu 72 được tạo cấu hình để thu chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính, trong đó chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Theo tùy chọn, mô đun thu 71 còn được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thu thông tin chứng nhận ứng dụng được gửi bởi NFVO hoặc VNFM, trong đó thông tin ứng dụng chứng nhận này chứa thông tin về thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

Theo tùy chọn, thiết bị này còn bao gồm: mô đun thiết lập 73.

Mô đun thiết lập 73 được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thiết lập, theo thông tin ứng dụng chứng nhận thu được bởi mô đun thu, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận, trong đó kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, mô đun thu 72 được tạo cấu hình cụ thể để: trong khi cài đặt, thu thông tin ứng dụng chứng nhận được đưa vào bởi hạ tầng ảo hóa chức năng mạng NFVI.

Theo tùy chọn, thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận chứa địa chỉ Giao thức Internet IP, bộ nhận dạng Điều Khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

Theo tùy chọn, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai vào thực thể VNFC được cài đặt mới.

Theo tùy chọn, cách thức kích hoạt thực thể VNFC được cài đặt mới để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính chứa bước:

kích hoạt bằng cách tạo đối tượng VNF; hoặc kích hoạt bằng cách phân tải ngoài VNF.

Cần lưu ý rằng, thiết bị theo phương án này của sáng chế có thể là thực thể VNFC được cài đặt mới cần yêu cầu cấp chứng nhận, hoặc có thể là phần tử mạng điều khiển được tích hợp trên thực thể VNFC được cài đặt mới cần yêu cầu cấp chứng nhận. Cách thức thực hiện có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm, nhưng không bị giới hạn ở đây.

Phương án 9

Như được thể hiện trên FIG. 8, FIG. 8 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 9 của sáng chế. Thiết bị này bao gồm: bộ thu tín hiệu 81, bộ phát tín hiệu 82, và bộ xử lý 83, trong đó bộ thu tín hiệu 81, bộ phát tín hiệu 82, và bộ xử lý 83 được kết nối bằng cách sử dụng buýt truyền thông 84.

Bộ thu tín hiệu 81 được tạo cấu hình để thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể chức năng mạng ảo VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Bộ phát tín hiệu 82 được tạo cấu hình để gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận, để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Bộ xử lý 83 được tạo cấu hình để nhận chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận được phát hành bởi cơ quan chứng nhận bằng cách sử dụng khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Theo tùy chọn, bộ thu tín hiệu 81 còn được tạo cấu hình để: trước khi nhận được

chứng nhận được phát hành bởi cơ quan chứng nhận, thì thu thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận.

Bộ xử lý 83 còn được tạo cấu hình để thực hiện việc xác thực đối với thông báo đáp chứng nhận đã thu được.

Cụ thể là, thông báo đáp chứng nhận chứa chứng nhận được phát hành bởi cơ quan chứng nhận.

Bộ xử lý 83 được tạo cấu hình cụ thể để: khi thông báo đáp chứng nhận đã được xác thực, thì nhận chứng nhận được chứa trong thông báo đáp chứng nhận và được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, trong đó chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu ứng dụng chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Theo tùy chọn, thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Theo tùy chọn, thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

Theo tùy chọn, cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

Theo tùy chọn, bộ phát tín hiệu 82 còn được tạo cấu hình để: sau khi nhận được chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới, thì gửi, tới thực thể VNFC được cài đặt mới qua mạng nội bộ, chứng nhận đã nhận được, được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới.

Thực thể VNFC chính và thực thể VNFC được cài đặt mới là các hợp phần khác nhau của cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Bộ xử lý 83 có thể là bộ xử lý trung tâm đa năng (CPU), bộ vi xử lý, mạch tích hợp chuyên dụng (application-specific intergrated circuit, ASIC), hoặc một hoặc nhiều mạch

tích hợp được tạo cấu hình để điều khiển chương trình cần được thực thi theo giải pháp của sáng chế.

Buýt truyền thông 84 có thể chứa kênh, và truyền thông tin giữa các hợp phần nêu trên.

Cần lưu ý rằng, thiết bị theo phương án này của sáng chế có thể là hợp phần khác thuộc về, cùng với thực thể VNFC được cài đặt mới, cùng một VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI, ví dụ, thực thể VNFC chính. Cách thức thực hiện có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm.

Phương án 10

Như được thể hiện trên FIG. 9, FIG. 9 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 10 của sáng chế. Thiết bị này bao gồm: bộ thu tín hiệu 91, bộ xử lý 92, và bộ phát tín hiệu 93, trong đó bộ thu tín hiệu 91, bộ xử lý 92, và bộ phát tín hiệu 93 được kết nối bằng cách sử dụng buýt truyền thông 94.

Bộ thu tín hiệu 91 được tạo cấu hình để thu thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, trong đó thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Bộ xử lý 92 được tạo cấu hình để thực hiện việc xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của thực thể VNFC chính, và khi việc xác thực này thành công, đạt được chứng nhận cần phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Bộ phát tín hiệu 93 được tạo cấu hình để gửi chứng nhận cần được phát hành tới thực thể VNFC chính.

Cụ thể là, bộ xử lý 92 được tạo cấu hình cụ thể để thực hiện việc xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

Theo tùy chọn, thông báo yêu cầu chứng nhận còn chứa thông tin bằng chứng sở hữu khóa riêng POP.

Bộ xử lý 92 còn được tạo cấu hình để thực hiện việc xác thực đối với thông tin POP

được chứa trong thông báo yêu cầu chứng nhận bởi cơ quan chứng nhận, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được chứa trong thông báo yêu cầu chứng nhận.

Bộ xử lý 92 có thể là bộ xử lý trung tâm đa năng (CPU), bộ vi xử lý, mạch tích hợp chuyên dụng (application-specific integrated circuit, ASIC), hoặc một hoặc nhiều mạch tích hợp được tạo cấu hình để điều khiển chương trình cần được thực thi theo giải pháp của sáng chế.

Buýt truyền thông 94 có thể chứa kênh, và truyền thông tin giữa các hợp phần nêu trên.

Cần lưu ý rằng, thiết bị theo phương án này của sáng chế có thể là cơ quan chứng nhận, ví dụ, thiết bị phần tử mạng có chức năng phát hành chứng nhận, như CA, ESA, hoặc RA. Cách thức thực hiện có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm.

Phương án 11

Như được thể hiện trên FIG. 10, FIG. 10 là sơ đồ kết cấu của thiết bị nhận chứng nhận theo Phương án 10 của sáng chế. Thiết bị này bao gồm: bộ phát tín hiệu 1001 và bộ thu tín hiệu 1002, trong đó bộ phát tín hiệu 1001 và bộ thu tín hiệu 1002 được kết nối bằng cách sử dụng buýt truyền thông 1003.

Bộ phát tín hiệu 1001 được tạo cấu hình để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể hợp phần chức năng mạng được ảo hóa VNFC chính, trong đó thông báo biểu thị ứng dụng chứng nhận chứa khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận chứa chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Bộ thu tín hiệu 1002 được tạo cấu hình để nhận chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính, trong đó chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

Theo tùy chọn, bộ thu tín hiệu 1002 còn được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thu thông tin chứng nhận ứng dụng được gửi bởi NFVO hoặc VNFM, trong đó thông tin ứng dụng chứng nhận này chứa thông tin về thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

Theo tùy chọn, thiết bị này còn bao gồm: bộ xử lý 1004.

Bộ xử lý 1004 được tạo cấu hình để: trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thiết lập, theo thông tin ứng dụng chứng nhận, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận, trong đó kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

Cụ thể là, bộ thu tín hiệu 1002 được tạo cấu hình cụ thể để: trong khi cài đặt, thu thông tin ứng dụng chứng nhận được đưa vào bởi hạ tầng ảo hóa chức năng mạng NFVI.

Theo tùy chọn, thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận chứa địa chỉ Giao thức Internet IP, bộ nhận dạng Điều Khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

Theo tùy chọn, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận đạt được theo cách sau đây:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khoá công khai; hoặc
sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khoá công khai và đưa cặp khóa riêng-khoá công khai này vào thực thể VNFC được cài đặt mới.

Theo tùy chọn, cách thức kích hoạt thực thể VNFC được cài đặt mới để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể VNFC chính bao gồm việc:

kích hoạt bằng cách tạo đối tượng VNF; hoặc
kích hoạt bằng cách phân tải ngoài VNF.

Bộ xử lý 1004 có thể là bộ xử lý trung tâm đa năng (CPU), bộ vi xử lý, mạch tích hợp chuyên dụng (application-specific integrated circuit, ASIC), hoặc một hoặc nhiều mạch tích hợp được tạo cấu hình để điều khiển chương trình cần được thực thi theo giải pháp của sáng chế.

Buýt truyền thông 1003 có thể chứa kênh, và truyền thông tin giữa các hợp phần nêu trên.

Cần lưu ý rằng, thiết bị theo phương án này của sáng chế có thể là thực thể VNFC được cài đặt mới cần yêu cầu cấp chứng nhận, hoặc có thể là phần tử mạng điều khiển được tích hợp trên thực thể VNFC được cài đặt mới cần yêu cầu cấp chứng nhận. Cách thức thực hiện có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm, nhưng không bị giới hạn ở đây.

Người có hiểu biết trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án của sáng chế có thể được tạo ra dưới dạng phương pháp, thiết bị (cơ cấu), hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể có các phương án chỉ phần cứng, các phương án chỉ phần mềm, hoặc các phương án kết hợp phần mềm và phần cứng. Hơn nữa, sáng chế có thể được thực hiện dưới dạng sản phẩm chương trình máy tính được thực hiện trên một hoặc nhiều môi trường lưu trữ đọc được bằng máy tính (bao gồm nhưng không bị giới hạn bởi bộ nhớ đĩa, CD-ROM, bộ nhớ quang, và các thiết bị tương tự) có chứa mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả có dựa vào các lưu đồ và sơ đồ khối của phương pháp, thiết bị (cơ cấu), và sản phẩm chương trình máy tính theo các phương án của sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện từng quy trình và/hoặc từng khối trong các lưu đồ và/hoặc các sơ đồ khối và sự kết hợp của quy trình và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được cấp cho máy tính đa năng, máy tính chuyên dụng, bộ xử lý nhúng, hoặc bộ xử lý của bất kỳ thiết bị xử lý dữ liệu có thể lập trình nào khác để tạo ra cỗ máy, sao cho các lệnh được thực thi bởi máy tính hoặc bộ xử lý của bất kỳ thiết bị xử lý dữ liệu có thể lập trình nào khác tạo ra được thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được cấp cho máy tính đa năng, máy tính chuyên dụng, bộ xử lý nhúng, hoặc bộ xử lý của bất kỳ thiết bị xử lý dữ liệu có thể lập trình nào khác để tạo ra cỗ máy, sao cho các lệnh được thực thi bởi máy tính hoặc bộ xử lý của bất kỳ thiết bị xử lý dữ liệu có thể lập trình nào khác tạo ra được thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính cũng có thể được nạp vào máy tính hoặc thiết bị xử lý dữ liệu có thể lập trình khác, sao cho các chuỗi thao tác và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo ra quy trình xử lý bằng máy

tính. Do đó, các lệnh được thực thi trên máy tính hoặc thiết bị lập trình được khác tạo ra các bước để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Mặc dầu một số phương án ưu tiên của sáng chế đã được mô tả, nhưng người có hiểu biết trong lĩnh vực này có thể thay đổi và cải biến các phương án này một khi họ nắm được ý đồ sáng tạo cơ bản. Do đó, các điểm yêu cầu bảo hộ dưới đây cần được giải thích là bao gồm các phương án được ưu tiên và tất cả các thay đổi và cải biến đó đều nằm trong phạm vi của sáng chế.

Hiển nhiên là, người có hiểu biết trong lĩnh vực này có thể tạo ra các cải biến và biến đổi khác nhau đối với sáng chế mà không ra khỏi và phạm vi của sáng chế. Sáng chế cũng nhằm bao gồm các cải biến và biến đổi này chừng nào mà chúng còn nằm trong phạm vi của các điểm yêu cầu bảo hộ của sáng chế và các công nghệ tương đương với chúng.

YÊU CẦU BẢO HỘ

1. Thiết bị nhận chứng nhận bao gồm:

mô đun thu (51), được tạo cấu hình để thu thông báo biểu thị ứng dụng chứng nhận được gửi bởi thực thể hợp phần chức năng mạng được ảo hóa VNFC được cài đặt mới, trong đó thông báo biểu thị ứng dụng chứng nhận bao gồm khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

mô đun gửi (52), được tạo cấu hình để gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận theo thông báo biểu thị ứng dụng chứng nhận thu được bởi mô đun thu (51), để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, trong đó thông báo yêu cầu chứng nhận bao gồm chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

mô đun nhận (53), được tạo cấu hình để nhận chứng nhận được phát hành bởi cơ quan chứng nhận, trong đó chứng nhận được phát hành bởi cơ quan chứng nhận bằng cách sử dụng khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

2. Thiết bị theo điểm 1, trong đó thiết bị này còn bao gồm: mô đun xác thực, trong đó:

mô đun thu còn được tạo cấu hình để trước khi mô đun nhận nhận được chứng nhận được phát hành bởi cơ quan chứng nhận, thì thu thông báo đáp chứng nhận được gửi bởi cơ quan chứng nhận; và

mô đun xác thực được tạo cấu hình để thực hiện việc xác thực đối với thông báo đáp chứng nhận thu được bởi mô đun thu.

3. Thiết bị theo điểm 2, trong đó thông báo đáp chứng nhận bao gồm chứng nhận được phát hành bởi cơ quan chứng nhận; và

mô đun nhận được tạo cấu hình cụ thể để khi mô đun xác thực xác định rằng thông báo đáp chứng nhận đã được xác thực, thì nhận chứng nhận được phát hành bởi cơ quan chứng nhận cho thực thể VNFC được cài đặt mới và được bao gồm trong thông báo đáp chứng nhận, trong đó chứng nhận của thực thể VNFC được cài đặt mới đạt được bởi cơ quan chứng nhận bằng cách ký, sau khi thông báo yêu cầu ứng dụng chứng nhận được gửi bởi VNFC chính đã được xác thực theo chứng nhận của thực thể VNFC chính, khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận

và được bao gồm trong thông báo yêu cầu chứng nhận.

4. Thiết bị theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó thông báo biểu thị ứng dụng chứng nhận và thông báo yêu cầu chứng nhận còn bao gồm thông tin bằng chứng sở hữu khóa riêng POP.

5. Thiết bị theo điểm 4, trong đó thông tin POP đạt được bởi thực thể VNFC được cài đặt mới bằng cách sử dụng khóa riêng trong cặp khóa riêng-khóa công khai để ký trường khóa ký bằng chứng sở hữu khóa riêng.

6. Thiết bị theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó cặp khóa riêng-khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới đạt được theo cách sau:

sinh ra, bởi thực thể VNFC được cài đặt mới, cặp khóa riêng-khóa công khai; hoặc sinh ra, bởi hạ tầng ảo hóa chức năng mạng NFVI, cặp khóa riêng-khóa công khai và đưa cặp khóa riêng-khóa công khai này vào thực thể VNFC được cài đặt mới.

7. Thiết bị nhận chứng nhận bao gồm: 2

mô đun thu (61), được tạo cấu hình để thu thông báo yêu cầu chứng nhận được gửi bởi thực thể VNFC chính, trong đó thông báo yêu cầu chứng nhận bao gồm chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận;

mô đun phát hành chứng nhận (62), được tạo cấu hình để thực hiện việc xác thực đối với thông báo yêu cầu chứng nhận theo chứng nhận của thực thể VNFC chính mà thu được bởi mô đun thu (61), và khi việc xác thực này thành công, thì đạt được chứng nhận cần phát hành bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

mô đun gửi (63), được tạo cấu hình để gửi, tới thực thể VNFC chính, chứng nhận cần được phát hành mà được phát hành bởi mô đun phát hành chứng nhận (62).

8. Thiết bị theo điểm 7, trong đó:

mô đun phát hành chứng nhận được tạo cấu hình cụ thể để thực hiện việc xác thực đối với chữ ký của thông báo yêu cầu chứng nhận bằng cách sử dụng chứng nhận của thực thể VNFC chính, và thực hiện việc xác thực đối với chứng nhận thu được của thực thể VNFC chính bằng cách sử dụng chứng nhận CA gốc đã được phát hành hoặc chứng nhận trung gian đã được phát hành.

9. Thiết bị theo điểm 7 hoặc 8, trong đó thông báo yêu cầu chứng nhận còn bao gồm thông tin bằng chứng sở hữu khóa riêng POP.

10. Thiết bị theo điểm 9, trong đó

mô đun phát hành chứng nhận còn được tạo cấu hình để thực hiện việc xác thực, bằng cách sử dụng khóa công khai mà được sử dụng để yêu cầu cấp chứng nhận và được bao gồm trong thông báo yêu cầu chứng nhận, đối với thông tin POP được bao gồm trong thông báo yêu cầu chứng nhận.

11. Thiết bị nhận chứng nhận bao gồm:

mô đun gửi (71), được tạo cấu hình để gửi thông báo biểu thị ứng dụng chứng nhận tới thực thể hợp phần chức năng mạng được ảo hóa VNFC chính, trong đó thông báo biểu thị ứng dụng chứng nhận bao gồm khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận, thông báo biểu thị ứng dụng chứng nhận được sử dụng để yêu cầu thực thể VNFC chính gửi thông báo yêu cầu chứng nhận tới cơ quan chứng nhận, thông báo yêu cầu chứng nhận được sử dụng để yêu cầu cơ quan chứng nhận phát hành chứng nhận cho thực thể VNFC được cài đặt mới, và thông báo yêu cầu chứng nhận bao gồm chứng nhận của thực thể VNFC chính và khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận; và

mô đun thu (72), được tạo cấu hình để thu chứng nhận được phát hành bởi cơ quan chứng nhận và được gửi bởi thực thể VNFC chính, trong đó chứng nhận đạt được bởi cơ quan chứng nhận bằng cách ký khóa công khai được sử dụng bởi thực thể VNFC được cài đặt mới để yêu cầu cấp chứng nhận.

12. Thiết bị theo điểm 11, trong đó

mô đun thu còn được tạo cấu hình để trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thu thông tin ứng dụng chứng nhận được gửi bởi NFVO hoặc VNFM, trong đó thông tin chứng nhận ứng dụng bao gồm thông tin về thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận.

13. Thiết bị theo điểm 12, trong đó thiết bị này còn bao gồm:

mô đun thiết lập, được tạo cấu hình để trước khi thông báo biểu thị ứng dụng chứng nhận được gửi tới VNFC chính, thì thiết lập, theo thông tin ứng dụng chứng nhận thu được bởi mô đun thu, kết nối mạng tới thực thể VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận, trong đó kết nối mạng này là kết nối mạng bên trong VNF trên cùng một nền hạ tầng ảo hóa chức năng mạng NFVI.

14. Thiết bị theo điểm 12 hoặc 13, trong đó:

mô đun thu được tạo cấu hình cụ thể để trong khi cài đặt, thu thông tin ứng dụng chứng nhận được đưa vào bởi hạ tầng ảo hóa chức năng mạng, NFVI.

15. Thiết bị theo điểm bất kỳ trong số các điểm từ 12 đến 14, trong đó thông tin về VNFC chính được sử dụng dưới dạng chương trình đại lý đối với ứng dụng chứng nhận bao gồm địa chỉ Giao thức Internet IP, bộ nhận dạng Điều khiển Truy cập Môi trường MAC, và địa chỉ trung tâm thông tin mạng ảo NIC, của thực thể VNFC chính.

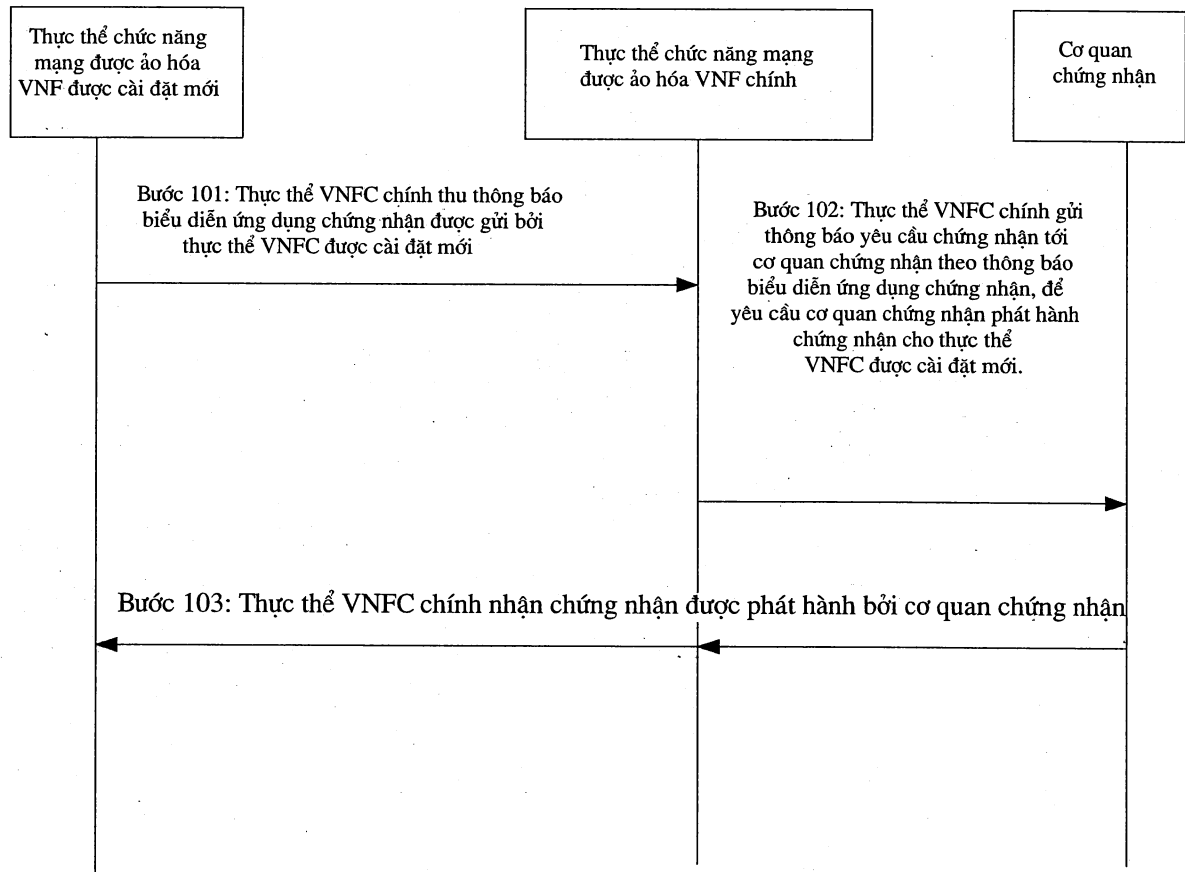


FIG. 1

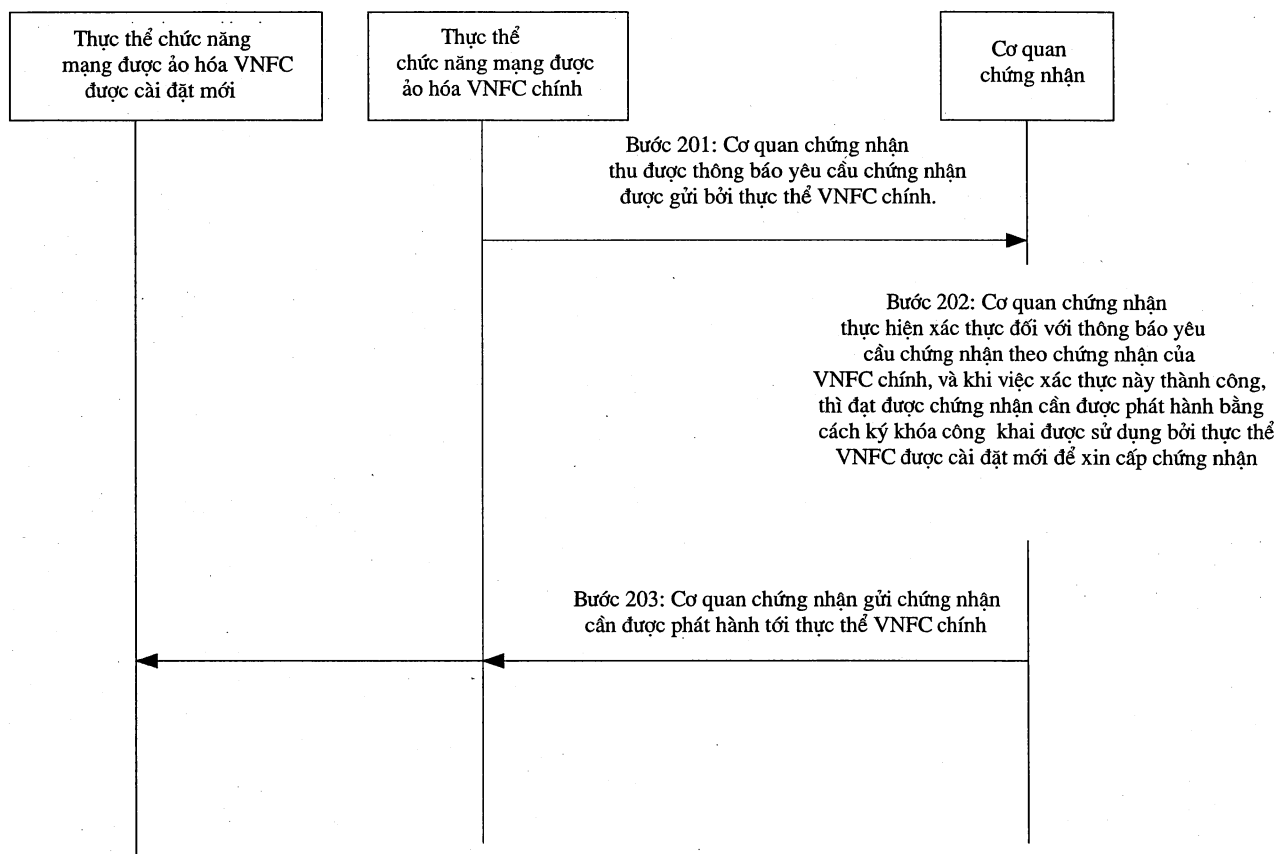


FIG. 2

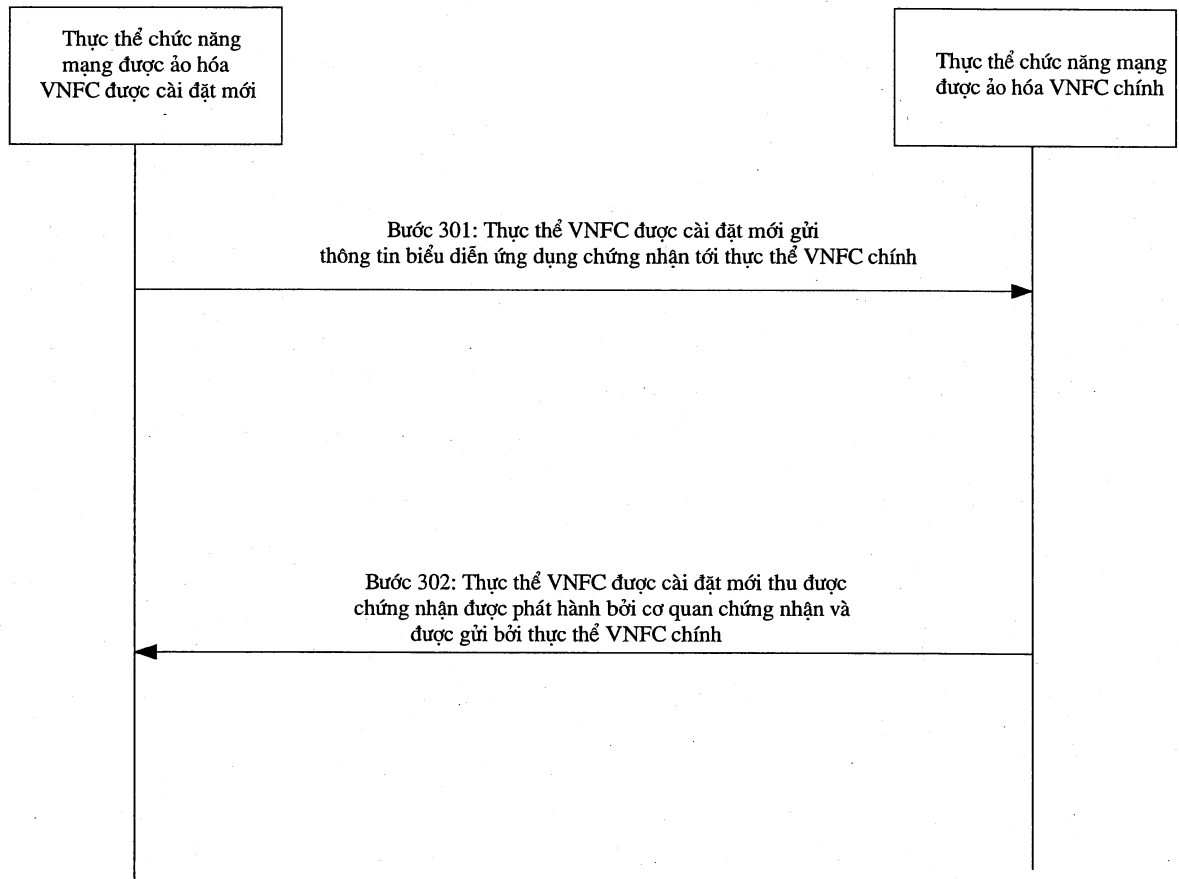


FIG. 3

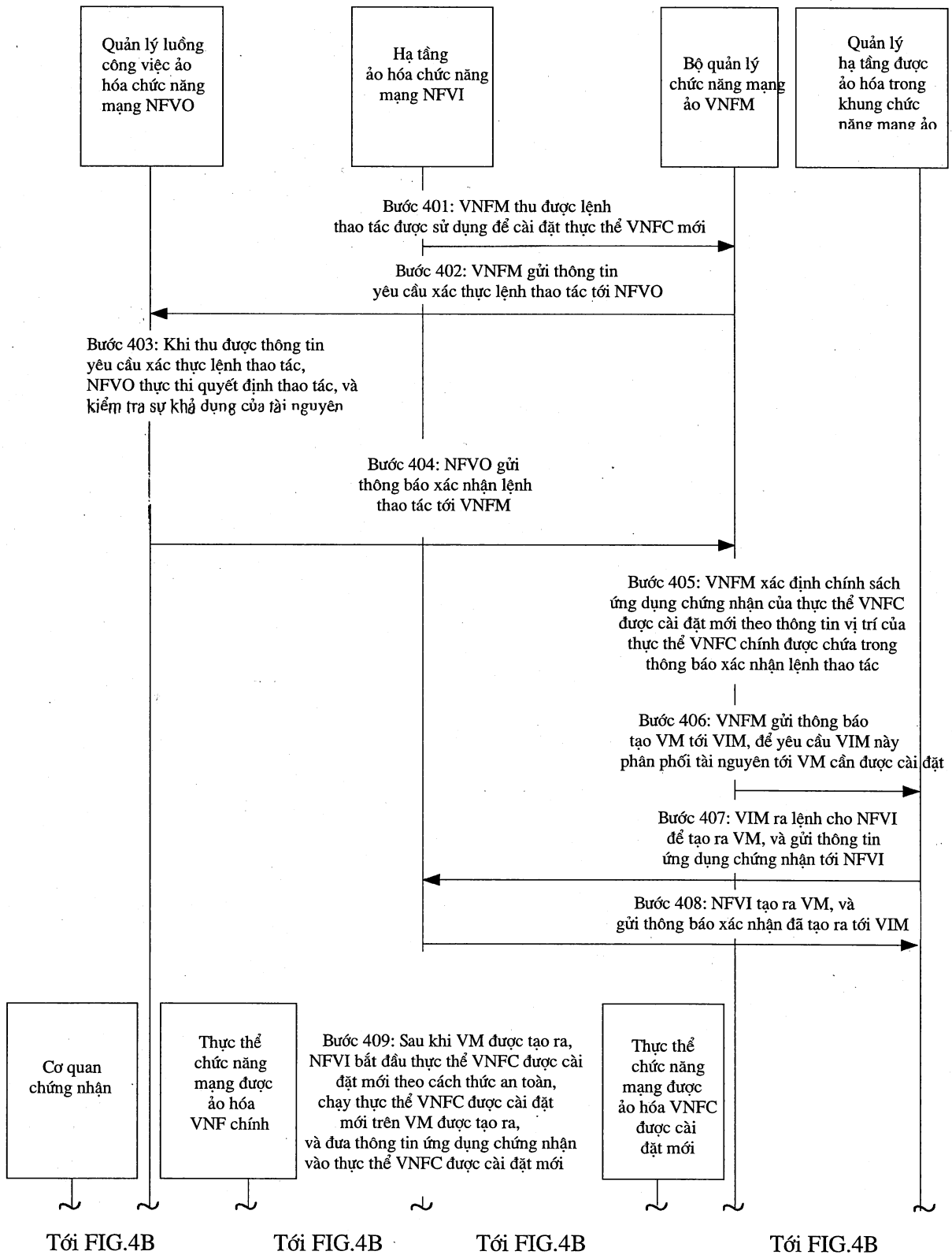


FIG. 4A

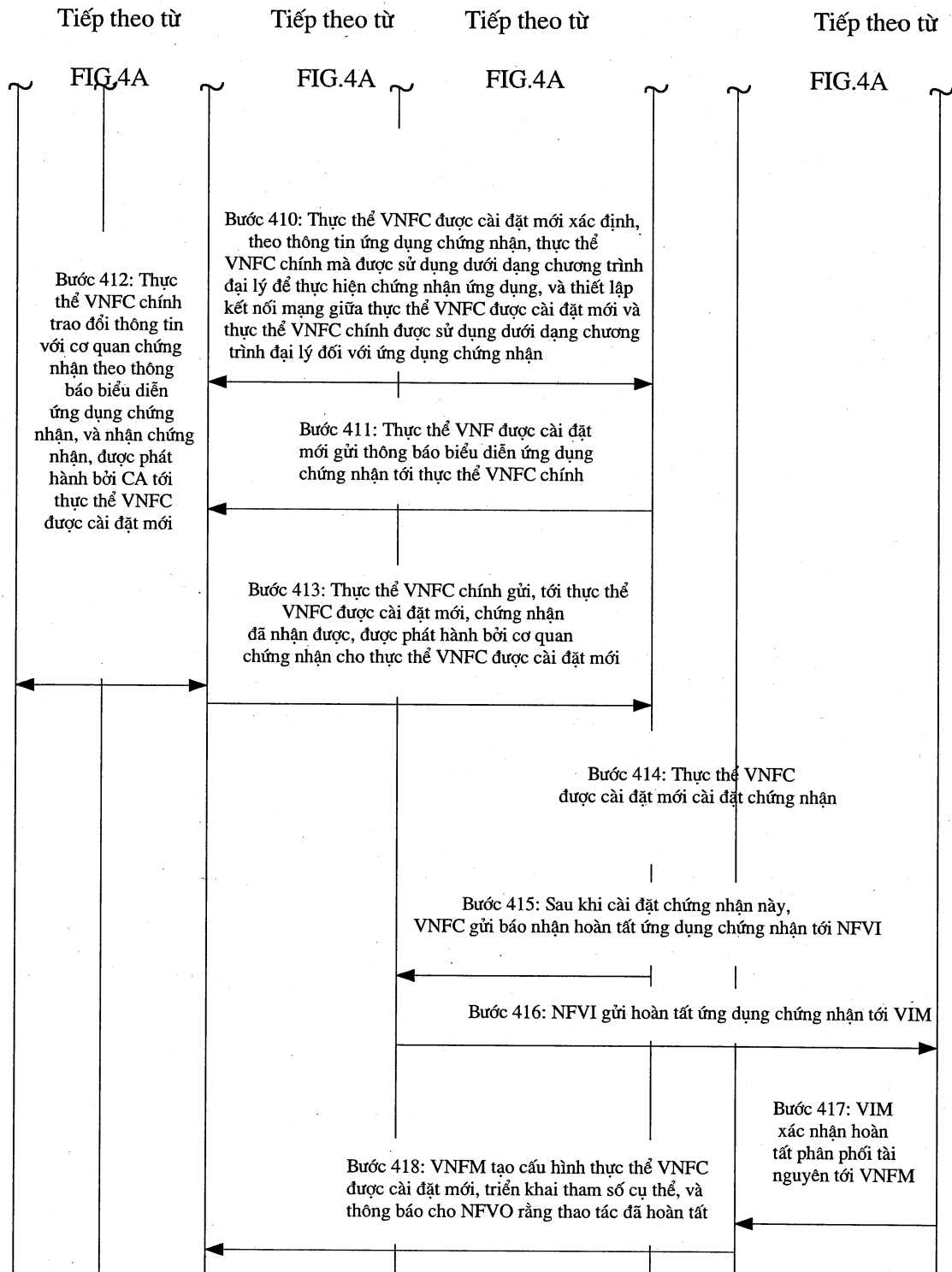


FIG. 4B

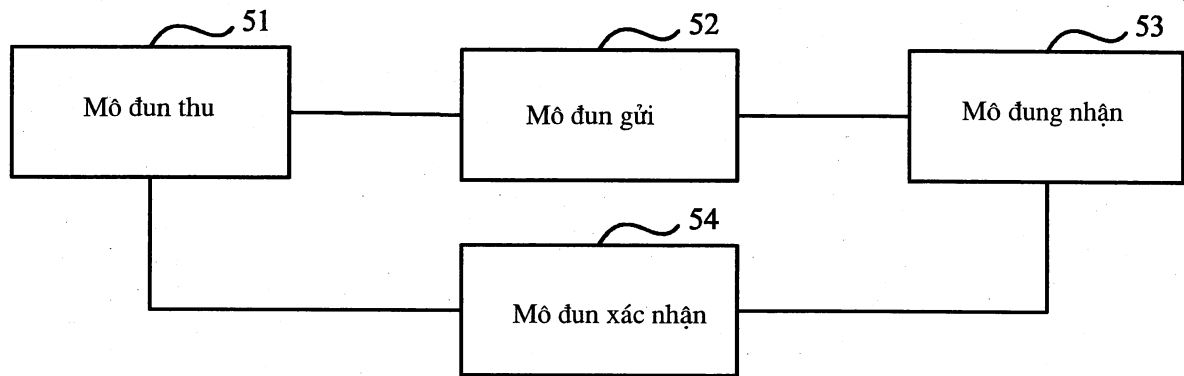


FIG. 5

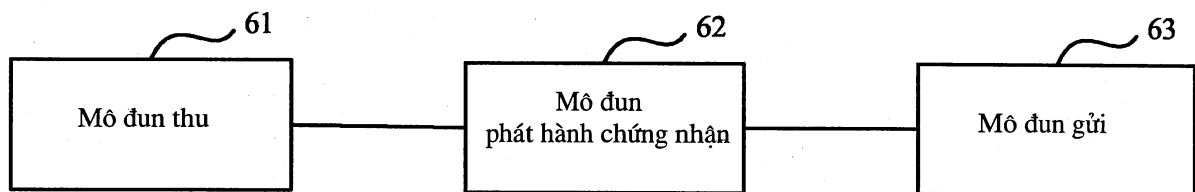


FIG. 6

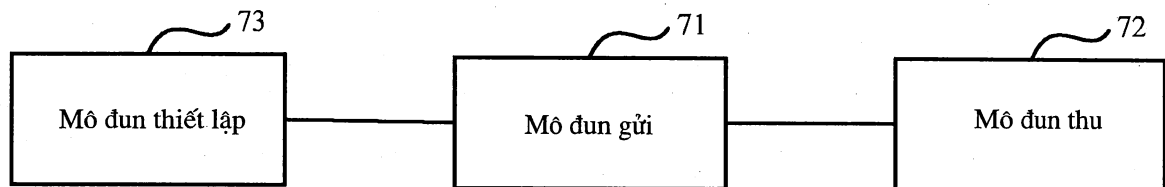


FIG. 7

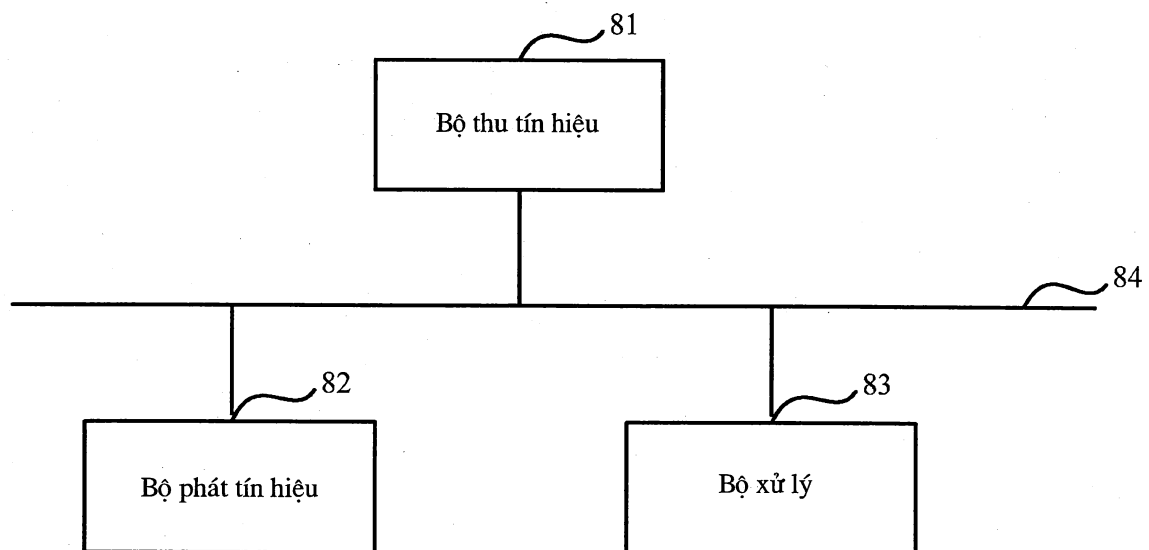


FIG. 8

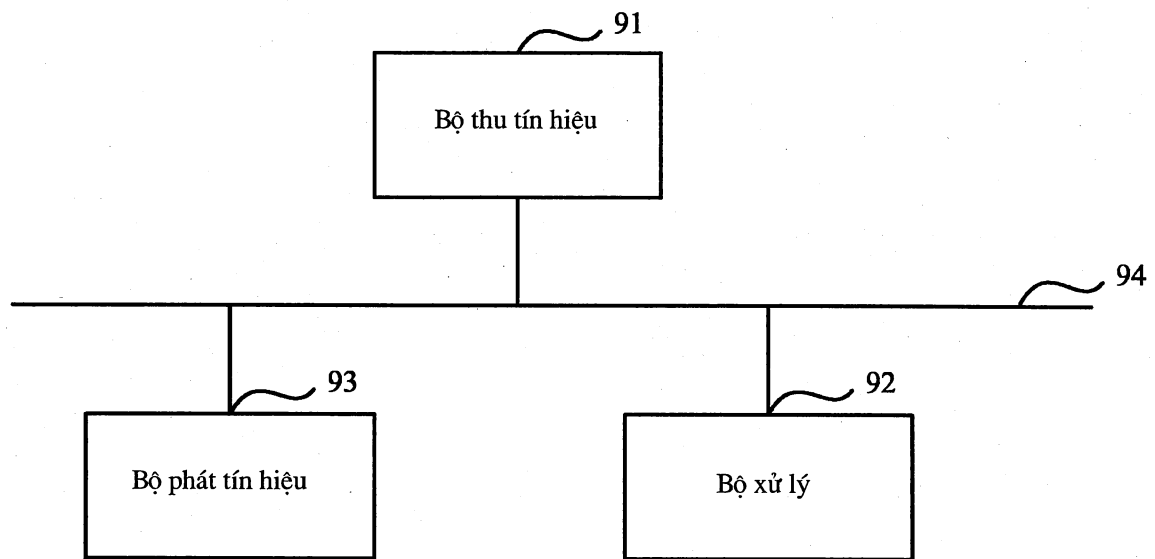


FIG. 9

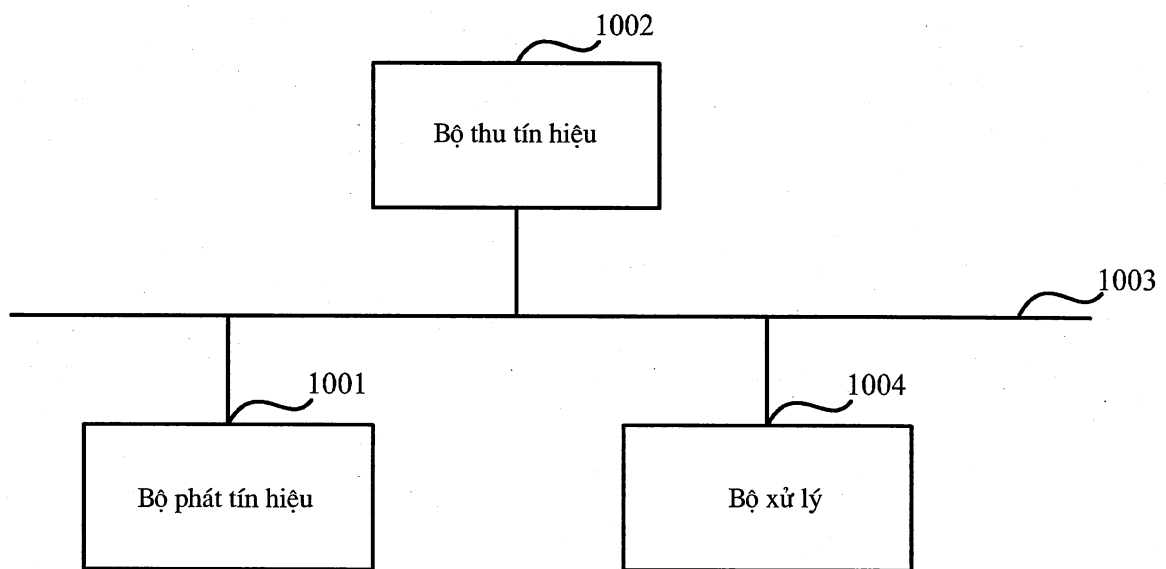


FIG. 10