(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) **1-0020487**

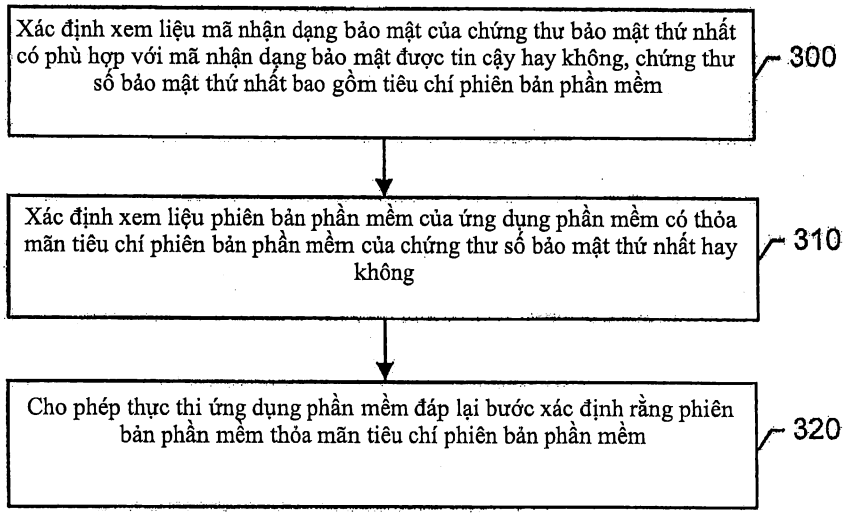
(51)[7] **G06F 21/00**

(13) **B**

(21) 1-2011-01556
(22) 13.11.2009
(86) PCT/IB2009/007447 13.11.2009
(87) WO2010/061261 03.06.2010
(30) 12/323,737 26.11.2008 US
(45) 25.02.2019 371
(43) 26.12.2011 285
(73) Nokia Technologies OY (FI)
Karaportti 3, FI-02610 Espoo, Finland
(72) Janne TAKALA (FI), Olli Pekka Juhani MUUKKA (FI), Rauno Juhani TAMMINEN (FI), Janne Johannes JARVINEN (FI)
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ QUẢN LÝ CÁC PHIÊN BẢN PHẦN MỀM

(57) Sáng chế đề cập tới thiết bị quản lý các phiên bản phần mềm có thể bao gồm bộ xử lý. Bộ xử lý có thể được tạo cấu hình để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không. Theo đó, chứng thư số bảo mật thứ nhất có thể bao gồm tiêu chí phiên bản phần mềm. Bộ xử lý cũng có thể được tạo cấu hình để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Bộ xử lý có thể được tạo cấu hình để ra quyết định đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy. Ngoài ra, bộ xử lý cũng có thể được tạo cấu hình để cho phép việc thực thi ứng dụng phần mềm, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm. Sáng chế cũng đề cập tới phương pháp quản lý các phiên bản phần mềm.



Lĩnh vực kỹ thuật được đề cập

Các phương án thực hiện theo sáng chế đề cập tới việc cài đặt phần mềm, và cụ thể hơn là đề cập tới phương pháp và thiết bị quản lý các phiên bản phần mềm.

Tình trạng kỹ thuật của sáng chế

Kỷ nguyên truyền thông hiện đại đã đem lại sự bùng nổ mạnh mẽ của các mạng có dây và không dây. Các loại công nghệ mạng khác nhau được phát triển tạo ra sự mở rộng chưa từng có của các mạng máy tính, mạng truyền hình, mạng điện thoại và các dạng tương tự và tiếp tục được kích thích bởi nhu cầu của người dùng. Các công nghệ mạng không dây và di động đã giải quyết các nhu cầu của người dùng, trong khi tạo ra độ linh hoạt và tính tức thời cao hơn cho việc truyền thông tin.

Các thiết bị được nối dây và/hoặc không dây để thực hiện các ứng dụng, truyền thông dữ liệu và lưu dữ liệu đã trở thành các công cụ quan trong trong cả môi trường kinh doanh và môi trường xã hội. Các cá nhân đều phụ thuộc vào các thiết bị này để thực hiện các công việc hàng ngày, đặc biệt là các công việc liên quan tới việc chia sẻ dữ liệu. Người sử dụng yêu cầu các khả năng truyền thông, do đó, các nhà cung cấp mạng khi thu phí cho các dịch vụ được cung cấp buộc phải thỏa mãn các nhu cầu của khách hàng.

Trong nhiều trường hợp, để tránh phải trả các khoản phí cho các truyền thông, các hacker cố gắng phát hiện các lỗ hổng an ninh trong phần mềm được thực hiện bởi sự truyền thông giữa các thiết bị. Ví dụ, các khiếm khuyết nguy hiểm trong phần mềm được thực hiện bởi thiết bị truyền thông, như điện thoại di động hoặc thiết bị đầu cuối di động khác, cũng có thể được nhận diện bởi các hacker. Sau đó, các hacker có thể phát hiện khiếm khuyết nguy hiểm liên quan tới việc thu phí truyền thông, sử dụng điện thoại di động trên các hệ thống truyền thông tế bào không được xác thực, hoặc phát hiện chức năng khác của điện thoại di động hoặc các hệ thống truyền thông hỗ trợ thiết bị.

Bản chất kỹ thuật của sáng chế

Phương pháp, thiết bị, và sản phẩm chương trình máy tính được mô tả cung cấp khả năng quản lý phần mềm theo cách có thể ngăn chặn sự suy giảm chất lượng của phần mềm hoặc sự lạc hậu hoặc các phiên bản cũ hơn. Các phương án thực hiện làm ví dụ theo

sáng chế có thể sử dụng các chứng thư số (ví dụ, các chứng thư số bảo mật) để xác nhận các phiên bản phần mềm phù hợp được cài trên thiết bị, như thiết bị tính toán hoặc thiết bị truyền thông. Theo nhiều phương án thực hiện làm ví dụ, chứng thư số có thể được kết hợp với thiết bị (ví dụ, các chứng thư số phần cứng) và một chứng thư số khác có thể được kết hợp với ứng dụng phần mềm của phiên bản cụ thể (ví dụ, các chứng thư số cấu hình chung). Các chứng thư số phần cứng có thể được xác thực với mã nhận dạng công khai của thiết bị. Nhờ việc xác thực các chứng thư số phần cứng, các chứng thư số cấu hình chung có thể được xác thực và phiên bản của các chứng thư số cấu hình chung có thể được xác thực chống lại tiêu chí phiên bản chứng thư số bảo mật của các chứng thư số phần cứng. Nếu các chứng thư số cấu hình chung được xác thực và phiên bản được xác thực, thì phiên bản của phần mềm được cài trên thiết bị có thể được xác thực và việc cho phép có thể được cấp để thực thi phần mềm. Cũng cần chú ý rằng mặc dù phần mô tả ở trên đề cập tới phương án thực hiện làm ví dụ sử dụng hai chứng thư số bảo mật, nhưng nhiều phương án thực hiện làm ví dụ có thể chỉ ứng dụng một chứng thư số bảo mật.

Theo một phương án thực hiện làm ví dụ, sáng chế đề xuất phương pháp quản lý các phiên bản phần mềm. Phương pháp làm ví dụ có thể bao gồm bước xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không. Theo đó, chứng thư số bảo mật thứ nhất có thể bao gồm tiêu chí phiên bản phần mềm. Phương pháp làm ví dụ cũng có thể bao gồm bước xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Quyết định này có thể được tạo ra đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy. Ngoài ra, phương pháp cũng có thể bao gồm bước cho phép thực thi ứng dụng phần mềm bởi bộ xử lý, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm.

Theo phương án thực hiện làm ví dụ khác, sáng chế đề xuất thiết bị quản lý các phiên bản phần mềm. Thiết bị có thể bao gồm bộ xử lý. Bộ xử lý có thể được tạo cấu hình để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không. Theo đó, chứng thư số bảo mật thứ nhất có thể bao gồm tiêu chí phiên bản phần mềm. Bộ xử lý cũng có thể được tạo

cấu hình để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Bộ xử lý có thể được tạo cấu hình để ra quyết định này đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy. Ngoài ra, bộ xử lý cũng có thể được tạo cấu hình để cho phép việc thực thi ứng dụng phần mềm, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm.

Theo phương án thực hiện làm ví dụ khác, sáng chế đề xuất sản phẩm chương trình máy tính quản lý các phiên bản phần mềm. Sản phẩm chương trình máy tính có thể bao gồm một hoặc nhiều vật ghi đọc được bằng máy tính có các lệnh mã chương trình có thể thực thi đọc được bởi máy tính được lưu ở đó. Các lệnh mã chương trình đọc được bởi máy tính có thể được tạo cấu hình để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không. Theo đó, chứng thư số bảo mật thứ nhất có thể bao gồm tiêu chí phiên bản phần mềm. Các lệnh mã chương trình đọc được bởi máy tính cũng có thể được tạo cấu hình để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm thỏa mãn có tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Các lệnh mã chương trình đọc được bởi máy tính có thể được tạo cấu hình để ra quyết định này đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy. Ngoài ra, các lệnh mã chương trình đọc được bởi máy tính cũng có thể được tạo cấu hình để cho phép việc thực thi ứng dụng, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm.

Theo một phương án thực hiện làm ví dụ khác nữa, sáng chế đề xuất thiết bị quản lý các phiên bản phần mềm. Thiết bị làm ví dụ có thể bao gồm các phương tiện để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không. Theo đó, chứng thư số bảo mật thứ nhất có thể bao gồm tiêu chí phiên bản phần mềm. Thiết bị làm ví dụ cũng có thể bao gồm các phương tiện để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Quyết định này có thể được tạo ra đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy. Ngoài ra, thiết bị cũng

có thể bao gồm các phương tiện để cho phép thực thi ứng dụng phần mềm, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm.

Mô tả vắn tắt các hình vẽ kèm theo

Như được mô tả, theo nghĩa chung nhất, sáng chế sẽ được đề cập cùng với việc tham khảo tới các hình vẽ kèm theo, chúng không nhất thiết là phải cùng một tỉ lệ, trong đó:

Các Fig.1a và 1b mô tả các giản đồ quan hệ bao gồm các chứng thư số bảo mật quản lý các phiên bản phần mềm theo các phương án thực hiện làm ví dụ theo sáng chế;

Fig.2 là giản đồ khối sơ lược của thiết bị quản lý các phiên bản phần mềm theo các phương án thực hiện làm ví dụ khác theo sáng chế; và

Fig.3 và Fig.4 là các lưu đồ của các phương pháp quản lý các phiên bản phần mềm theo các phương án thực hiện làm ví dụ khác theo sáng chế.

Mô tả chi tiết sáng chế

Các phương án thực hiện theo sáng chế sẽ được mô tả đầy đủ hơn ở đây với sự tham chiếu tới các hình vẽ kèm theo, trong đó một số, nhưng không phải là tất cả các phương án thực hiện theo sáng chế đều được bộc lộ. Thực sự là, sáng chế có thể được ứng dụng dưới nhiều dạng khác nhau và không nên bị hiểu nhầm là bị giới hạn vào các phương án thực hiện được nêu ra ở đây; ngoài ra, các phương án thực hiện này được tạo ra sao cho phần bộc lộ này sẽ thỏa mãn các yêu cầu pháp lý của đơn. Các số chỉ dẫn giống nhau đề cập tới các thành phần giống nhau. Khi được sử dụng ở đây, các thuật ngữ "dữ liệu", "nội dung", "thông tin" và các thuật ngữ tương tự có thể được sử dụng thay thế cho nhau để đề cập tới khả năng về dữ liệu được truyền, nhận, được thao tác và/hoặc được lưu theo các phương án thực hiện theo sáng chế. Khi được sử dụng ở đây, cụm từ phiên bản phần mềm có thể đề cập tới một phiên bản của toàn bộ ứng dụng phần mềm hoặc chỉ đơn thuần là một phần hoặc thành phần của ứng dụng phần mềm. Thuật ngữ "chứng thư số" khi được sử dụng ở đây có thể đề cập tới của dữ liệu bất kỳ được ký có thể được ký sử dụng mô hình đã biết bất kỳ, ví dụ như mô hình khóa riêng/công khai. Tuy nhiên, thuật ngữ "làm ví dụ" khi được sử dụng ở đây, không được tạo ra để đề cập tới vấn đề định tính, mà chỉ đơn thuần là cung cấp minh họa cho ví dụ.

Fig.1a mô tả giản đồ quan hệ bao gồm các chứng thư số bảo mật theo các phương án thực hiện làm ví dụ khác theo sáng chế. Theo đó, các chứng thư số phần cứng 105 và các chứng thư số cấu hình chung 125 (thường được đề cập tới như là các chứng thư số bảo mật) có thể được bao gồm trong mô hình quản lý các phiên bản phần mềm. Theo nhiều phương án thực hiện làm ví dụ, ứng dụng chứng thư số phần cứng 105 và chứng thư số cấu hình chung 125 cho phép cập nhật hoặc nâng cấp phiên bản phần mềm. Ngoài ra, theo nhiều phương án thực hiện làm ví dụ, ứng dụng của các chứng thư số phần cứng 105 và các chứng thư số cấu hình chung 125 cũng hạn chế thay đổi cho phiên bản phần mềm cũ hơn hoặc không mong muốn.

Các phương án thực hiện làm ví dụ sử dụng các chứng thư số phần cứng 105 và các chứng thư số cấu hình chung 125 được tạo ra để đảm bảo sự gắn kết giữa mã nhận dạng công khai duy nhất của thiết bị và phiên bản phần mềm cụ thể để đảm bảo rằng phiên bản phần mềm phù hợp được sử dụng bởi thiết bị. Theo đó, các chứng thư số phần cứng 105 có thể được kết hợp chặt chẽ hơn với thiết bị và các chứng thư số cấu hình chung 125 có thể được kết hợp chặt chẽ hơn với phiên bản phần mềm. Quan hệ giữa các chứng thư số phần cứng 105 và các chứng thư số cấu hình chung 125, có thể được xác thực một cách an toàn, có thể sử dụng việc cập nhật của phần mềm trên thiết bị trong khi cũng tạo ra các đặc điểm bảo mật.

Nói chung, theo nhiều phương án thực hiện làm ví dụ, các chứng thư số cấu hình chung 125 có thể được cập nhật trên thiết bị khi phiên bản phần mềm được cập nhật được đưa vào thiết bị. Tiêu chí của các chứng thư số phần cứng 105 có thể được sử dụng để xác thực rằng các chứng thư số cấu hình chung 125 là phù hợp và nhờ đó xác thực rằng phiên bản phần mềm là phù hợp cho thiết bị. Dựa vào việc xác định rằng phiên bản phần mềm phù hợp được cài trên thiết bị, phần mềm có thể được cho phép để thực hiện bởi thiết bị. Theo đó, phiên bản phần mềm có thể là phù hợp cho thiết bị không chỉ bởi phiên bản phần mềm là phiên bản được cập nhật, mà còn do phiên bản phần mềm phù hợp cho cấu hình cụ thể của thiết bị (ví dụ, biến thể của thiết bị).

Theo đó, cấu hình cụ thể của thiết bị có thể được nhận diện thông qua mã nhận dạng công khai duy nhất của thiết bị. Ví dụ, mã nhận dạng công khai có thể được yêu cầu trong cơ sở dữ liệu lưu thông tin cấu hình của các thiết bị. Tuy nhiên, ứng dụng của các chứng

thư số phần cứng 105 và các chứng thư số cấu hình chung 125 có thể hỗ trợ việc cập nhật phần mềm theo cách không yêu cầu rằng mã nhận dạng công khai của thiết bị phải được xác nhận cho mỗi cài đặt phần mềm mới. Ngoài ra, quy trình xác thực làm ví dụ giữa các chứng thư số phần cứng 105 và các chứng thư số cấu hình chung 125, sử dụng tiêu chí chung ngoài mã nhận dạng công khai duy nhất của thiết bị, có thể cập nhật các phiên bản phần mềm mà không kèm theo sự phức tạp liên quan đến mã nhận dạng công khai duy nhất trong mỗi cài đặt của phiên bản phần mềm mới trên thiết bị. Theo cách này, việc sản xuất các thiết bị có thể được đơn giản hóa, khi một phiên bản phần mềm mới được cài, do mỗi lần cài đặt không yêu cầu phải xác minh thông qua mã nhận dạng công khai duy nhất.

Đề cập tới Fig.1a, mã nhận dạng công khai 100 có thể là giá trị được mã hóa cứng hoặc giá trị không thể thay đổi được nằm trên thiết bị phần cứng có khả năng thực thi ứng dụng phần mềm. Mã nhận dạng công khai 100 có thể được lưu trên mạch tích hợp như thiết bị nhớ chỉ đọc. Theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng công khai 100 có thể được ký và/hoặc được kết hợp với khóa riêng. Ngoài ra, mã nhận dạng công khai 100 có thể là duy nhất cho thiết bị được kết hợp cụ thể. Do đó, mã nhận dạng công khai 100 có thể được sử dụng để nhận diện cấu hình cụ thể của thiết bị hoặc dạng biến đổi của thiết bị. Ví dụ, theo các phương án thực hiện, trong đó, thiết bị là điện thoại di động, cấu hình của thiết bị có thể bao gồm nhưng không chỉ ở cấu hình phần cứng của điện thoại di động, mà còn là nhà cung cấp mạng có thể được kết hợp với điện thoại di động. Theo đó, nhà cung cấp mạng có thể tạo ra các dịch vụ duy nhất yêu cầu phần mềm cụ thể để trợ giúp.

Ứng dụng phần mềm 145 có thể là ứng dụng phần mềm bất kỳ để thực hiện bởi thiết bị được kết hợp với mã nhận dạng công khai 100. Theo nhiều phương án thực hiện làm ví dụ, ứng dụng phần mềm 145 có thể là hệ điều hành cho thiết bị. Ứng dụng phần mềm 145 có thể có và/hoặc bao gồm phiên bản phần mềm 150, có thể là số, ngày, kích thước (ví dụ, kích thước theo kilobyte hoặc dạng tương tự), tổ hợp của chúng hoặc dạng tương tự. Phiên bản phần mềm 150 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn của ứng dụng phần mềm 145. Các chứng thư số phần cứng 105 có thể là duy nhất cho phần cứng thiết bị (tức là máy tính, thiết bị đầu cuối di động hoặc

dạng tương tự) và có thể được lưu trong bộ nhớ của thiết bị. Các chứng thư số phần cứng 105 có thể được kết hợp với hoặc bao gồm mã nhận dạng công khai 110, các mã nhận dạng chứng thư số cấu hình chung 115 và tiêu chí phiên bản chứng thư số cấu hình chung 120.

Mã nhận dạng công khai 110 của các chứng thư số phần cứng 105 có thể phù hợp với mã nhận dạng công khai 100 của thiết bị. Quan hệ giữa mã nhận dạng công khai 110 của các chứng thư số phần cứng 105 và mã nhận dạng công khai 100 của thiết bị có thể được sử dụng để xác thực các chứng thư số phần cứng 105. Theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng công khai 110 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn của các chứng thư số phần cứng 105. Sự thất bại khi xác thực các chứng thư số phần cứng thông qua mã nhận dạng công khai 110 có thể ngăn cản việc thực thi phần mềm trên thiết bị.

Mã nhận dạng chứng thư số cấu hình chung 115 có thể là giá trị có thể được sử dụng trong việc xác thực các chứng thư số cấu hình chung 125. Sự thất bại khi xác thực các chứng thư số cấu hình chung 125 thông qua các mã nhận dạng chứng thư số cấu hình chung 115 có thể ngăn cản việc thực thi phần mềm được kết hợp với các chứng thư số cấu hình chung này. Các mã nhận dạng chứng thư số cấu hình chung 115 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn của các chứng thư số cấu hình chung 125.

Tiêu chí phiên bản chứng thư số cấu hình chung 120 có thể là tiêu chí được sử dụng để xác định xem liệu các chứng thư số cấu hình chung 125 là của phiên bản có phù hợp hay không. Theo đó, tiêu chí phiên bản chứng thư số cấu hình chung 120 có thể được tạo cấu hình sao cho tiêu chí có thể quyết định xem liệu các chứng thư số cấu hình chung 125 được kết hợp với phần mềm là của phiên bản phù hợp và được tạo cấu hình cho dạng thay đổi thiết bị phù hợp. Thông qua việc sử dụng của tiêu chí phiên bản chứng thư số cấu hình chung 120, các chứng thư số cấu hình chung không thích hợp có thể được phát hiện và việc thực thi phần mềm được kết hợp với các chứng thư số cấu hình chung không thích hợp có thể được ngăn cản. Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản chứng thư số cấu hình chung 120 có thể bao gồm giá trị phiên bản ngưỡng cho các chứng thư số cấu hình chung 125. Theo đó, các chứng thư số cấu hình chung với

phiên bản giá trị cao hơn hoặc bằng với giá trị phiên bản ngưỡng có thể thỏa mãn ít nhất một khía cạnh của tiêu chí phiên bản chứng thư số cấu hình chung 120. Tiêu chí cấu hình phiên bản chung 120 có thể được ký và/hoặc được kết hợp với khóa riêng để hỗ trợ xác thực an toàn trước khi áp dụng tiêu chí. Các chứng thư số cấu hình chung 125 có thể được kết hợp với ứng dụng phần mềm 145. Theo nhiều phương án thực hiện làm ví dụ, các chứng thư số cấu hình chung có thể là chung cho tất cả các cài đặt của ứng dụng phần mềm cụ thể. Các chứng thư số cấu hình chung 125 có thể được lưu trong bộ nhớ của thiết bị. Các chứng thư số cấu hình chung 125 có thể bao gồm các mã nhận dạng chứng thư số cấu hình chung 130, phiên bản chứng thư số cấu hình chung 135, và tiêu chí phiên bản phần mềm 140.

Các mã nhận dạng chứng thư số cấu hình chung 130 có thể là giá trị có thể được sử dụng trong việc xác thực các chứng thư số cấu hình chung 125 với các chứng thư số phần cứng 105. Theo đó, theo nhiều phương án thực hiện làm ví dụ, nếu các mã nhận dạng chứng thư số cấu hình chung 115 của các chứng thư số phần cứng phù hợp với các mã nhận dạng chứng thư số cấu hình chung 130 của các chứng thư số cấu hình chung 125, thì các chứng thư số cấu hình chung 125 có thể được xác thực. Sự thất bại khi xác thực các chứng thư số cấu hình chung thông qua các mã nhận dạng chứng thư số cấu hình chung 130 có thể ngăn cản việc thực thi phần mềm được kết hợp với các chứng thư số cấu hình chung. Tương tự với các mã nhận dạng chứng thư số cấu hình chung 115, các mã nhận dạng chứng thư số cấu hình chung 130 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn của các chứng thư số cấu hình chung 125.

Như được mô tả ở trên, phiên bản chứng thư số cấu hình chung 135 có thể được áp dụng cho tiêu chí phiên bản chứng thư số cấu hình chung 120 của các chứng thư số phần cứng 105 để xác định xem liệu phiên bản chứng thư số cấu hình chung 135 có thỏa mãn tiêu chí phiên bản chứng thư số cấu hình chung 120. Sự thất bại của phiên bản chứng thư số cấu hình chung để thỏa mãn tiêu chí phiên bản chứng thư số cấu hình chung 120 có thể ngăn cản việc thực thi phần mềm được kết hợp với các chứng thư số cấu hình chung. Tương tự với các mã nhận dạng tiêu chỉ chứng thư số cấu hình chung 120, các chứng thư số cấu hình chung phiên bản 135 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn của phiên bản chứng thư số cấu hình chung 135.

Tiêu chí phiên bản phần mềm 140 có thể là tiêu chí được sử dụng để xác định xem liệu phiên bản phần mềm 150 là của phiên bản có phù hợp hay không với các chứng thư số cấu hình chung 125. Tiêu chí phiên bản phần mềm 140 có thể đóng góp nâng mức bổ sung cho tính an toàn để đảm bảo rằng các chứng thư số cấu hình chung 125 không được sử dụng cùng với phiên bản phần mềm không thích hợp. Do đó, thông qua việc sử dụng của tiêu chí phiên bản phần mềm 140, các ứng dụng phần mềm không thích hợp có thể được phát hiện và việc thực thi các ứng dụng phần mềm có thể được ngăn chặn. Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản phần mềm 140 có thể bao gồm giá trị phiên bản ngưỡng cho phiên bản phần mềm 150. Theo đó, các ứng dụng phần mềm có phiên bản giá trị cao hơn hoặc bằng với giá trị phiên bản ngưỡng có thể thỏa mãn tiêu chí phiên bản phần mềm 140. Tiêu chí phiên bản phần mềm 140 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn trước khi áp dụng tiêu chí cho phiên bản phần mềm 150.

Fig.1b mô tả giản đồ quan hệ cho phương án thực hiện khác quản lý các phiên bản phần mềm. Theo đó, mô hình làm ví dụ được kết hợp với Fig.1b sử dụng chứng thư số bảo mật đơn 155. Chứng thư số bảo mật 155 có thể là duy nhất cho phần cứng thiết bị (ví dụ máy tính, thiết bị đầu cuối di động hoặc dạng tương tự) và có thể được lưu trong bộ nhớ của thiết bị. Chứng thư số bảo mật 155 có thể được kết hợp với mã nhận dạng công khai 160 và tiêu chí phiên bản phần mềm 165. Mã nhận dạng công khai 160 của chứng thư số bảo mật 155 có thể phù hợp với mã nhận dạng công khai 100 của thiết bị như được mô tả ở trên. Quan hệ giữa mã nhận dạng công khai 160 của chứng thư số bảo mật 155 và mã nhận dạng công khai 100 của thiết bị có thể được sử dụng để xác thực chứng thư số bảo mật 155. Theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng công khai 160 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn của chứng thư số bảo mật 155. Thất bại để xác thực chứng thư số bảo mật 155 thông qua mã nhận dạng công khai 160 có thể ngăn cản việc thực thi phần mềm trên thiết bị.

Tiêu chí phiên bản phần mềm 165 có thể là tiêu chí được sử dụng để xác định xem liệu phiên bản phần mềm 150 là của phiên bản có phù hợp với việc thực hiện trên thiết bị. Mặc dù việc sử dụng của tiêu chí phiên bản phần mềm 165, các ứng dụng phần mềm không thích hợp có thể được phát hiện và việc thực thi các ứng dụng phần mềm có thể

được ngăn cản. Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản phần mềm 165 có thể bao gồm giá trị phiên bản ngưỡng cho phiên bản phần mềm 150. Theo đó, các ứng dụng phần mềm có phiên bản giá trị cao hơn hoặc bằng với giá trị phiên bản ngưỡng có thể thỏa mãn tiêu chí phiên bản phần mềm 165. Tiêu chí phiên bản phần mềm 165 có thể được ký và/hoặc được kết hợp với khóa riêng để thực hiện xác thực an toàn trước khi áp dụng tiêu chí cho phiên bản phần mềm 150.

Fig.2 minh họa thiết bị làm ví dụ 200 có thể được tạo ra để quản lý các phiên bản phần mềm như được mô tả ở đây. Theo nhiều phương án thực hiện làm ví dụ, thiết bị 200 có thể được ứng dụng làm, hoặc được bao gồm để làm thành phần của thiết bị tính toán và/hoặc thiết bị truyền thông với các khả năng truyền thông dùng dây hoặc không dây. Nhiều ví dụ của thiết bị 200 có thể bao gồm máy tính, máy chủ, thiết bị đầu cuối di động như điện thoại di động, thiết bị trợ giúp số di động (PDA), máy nhắn tin, ti vi di động, thiết bị chơi điện tử, máy tính di động, máy tính xách tay, máy ảnh, thiết bị ghi viđeo, thiết bị chơi nhạc/viđeo, rađiô, và/hoặc thiết bị hệ thống định vị toàn cầu (GPS), thực thể mạng như điểm truy cập như trạm cơ sở hoặc tổ hợp bất kỳ của các bộ phận nêu trên hoặc dạng tương tự. Ngoài ra, thiết bị 200 có thể được tạo cấu hình để áp dụng các khía cạnh khác theo sáng chế như được mô tả ở đây bao gồm, ví dụ các phương pháp làm ví dụ khác nhau theo sáng chế, trong đó, các phương pháp có thể được ứng dụng bởi các phương tiện của phần cứng hoặc phần mềm được tạo cấu hình bộ xử lý, vật ghi đọc được bởi máy tính hoặc dạng tương tự.

Thiết bị 200 có thể bao gồm hoặc theo cách khác là liên kết với bộ xử lý 205 và thiết bị nhớ 210, nhưng có thể không nhất thiết bao gồm bộ nhớ chỉ đọc cho mã nhận dạng công khai 211. Theo đó, theo nhiều phương án thực hiện làm ví dụ, bộ nhớ cho mã nhận dạng công khai 211 là tách biệt khỏi thiết bị nhớ 210. Ngoài ra, theo nhiều phương án thực hiện, như các phương án thực hiện trong đó, thiết bị 200 là thiết bị đầu cuối di động, thiết bị 200 cũng có thể bao gồm giao diện truyền thông 215, và/hoặc giao diện người dùng 225. Bộ xử lý 205 có thể được ứng dụng làm các phương tiện khác nhau bao gồm, ví dụ, bộ vi xử lý, bộ đồng xử lý, bộ điều khiển, hoặc các thiết bị xử lý khác bao gồm các mạch tích hợp như, ví dụ, an ASIC (mạch tích hợp ứng dụng cụ thể), FPGA (mạng cổng trường lập trình được) hoặc bộ tăng tốc phần cứng. Theo phương án thực hiện làm ví dụ,

bộ xử lý 205 được tạo cấu hình để thực hiện các lệnh được lưu trong thiết bị nhớ 210 hoặc các lệnh mà theo cách khác có thể truy cập được bởi bộ xử lý 205. Bộ xử lý 205 cũng có thể được tạo cấu hình để thực hiện các truyền thông thông qua các giao diện truyền thông bởi, ví dụ, điều khiển phần cứng và/hoặc phần mềm được chứa trong giao diện truyền thông. Thiết bị nhớ 210 có thể được tạo cấu hình để lưu thông tin khác nhau được chứa trong các phương án thực hiện theo sáng chế như các chứng thư số bảo mật (ví dụ, các chứng thư số phần cứng và các chứng thư số cấu hình chung). Thiết bị nhớ 210 có thể là vật ghi đọc được bởi máy tính có thể bao gồm bộ nhớ xóa được và/hoặc bộ nhớ không xóa được. Ví dụ, thiết bị nhớ 210 có thể bao gồm bộ nhớ truy cập ngẫu nhiên (RAM) bao gồm RAM động và/hoặc RAM tĩnh, bộ nhớ đệm trên chip hoặc không trên chip và/hoặc dạng tương tự. Ngoài ra, thiết bị nhớ 210 có thể bao gồm bộ nhớ không xóa được, có thể được nhúng và/hoặc có thể loại bỏ được, và có thể bao gồm, ví dụ, bộ nhớ chỉ đọc, bộ nhớ tác động nhanh, các thiết bị lưu trữ từ (ví dụ, các đĩa cứng, các đĩa mềm, băng từ, v.v), các ổ đĩa quang và/hoặc môi trường nhớ, bộ nhớ truy cập ngẫu nhiên không xóa (NVRAM) và/hoặc dạng tương tự. Thiết bị nhớ 210 có thể bao gồm vùng đệm để lưu trữ tạm thời dữ liệu. Theo đó, một hoặc tất cả các thiết bị nhớ 210 có thể được bao gồm nằm trong bộ xử lý 205.

Ngoài ra, thiết bị nhớ 210 có thể được tạo cấu hình để lưu thông tin, dữ liệu, các ứng dụng, các lệnh mã chương trình đọc được bởi máy tính hoặc dạng tương tự để cho phép bộ xử lý 205 và thiết bị 200 thực hiện các chức năng khác theo các phương án thực hiện làm ví dụ theo sáng chế. Ví dụ, thiết bị nhớ 210 có thể được tạo cấu hình để đệm dữ liệu đầu vào để xử lý bởi bộ xử lý 205. Ngoài ra, hoặc theo cách khác, thiết bị nhớ 210 có thể được tạo cấu hình để lưu các lệnh để thực hiện bởi bộ xử lý 205. Giao diện người dùng 225 có thể truyền thông với bộ xử lý 205 để nhận đầu vào của người sử dụng tại giao diện người dùng 225 và/hoặc để cung cấp đầu ra cho người sử dụng như, ví dụ, các chỉ báo đầu ra nghe được, nhìn được, chỉ báo cơ học hoặc các chỉ báo đầu ra khác. Giao diện người dùng 225 có thể bao gồm, ví dụ, bàn phím, chuột, cần điều khiển, bộ phận hiển thị (ví dụ, bộ phận hiển thị màn hình chạm), micrô, loa hoặc các cơ chế đầu vào/ đầu ra khác.

Giao diện truyền thông 215 có thể là thiết bị hoặc các phương tiện khác được áp dụng trong cả phần cứng, phần mềm hoặc kết hợp của phần cứng và phần mềm mà được

tạo cấu hình để nhận và/hoặc truyền dữ liệu từ/tới mạng lưới và/hoặc thiết bị bất kỳ khác hoặc mô đun hoạt động với thiết bị 200. Theo đó, giao diện truyền thông 215 có thể bao gồm, ví dụ, ăng ten, máy phát, máy thu, máy thu phát và/hoặc phần cứng trợ giúp, bao gồm bộ xử lý hoặc phần mềm để cho phép các truyền thông với mạng lưới 220. Thông qua giao diện truyền thông 215 và mạng lưới 220, thiết bị 200 có thể truyền thông với các thực thể mạng khác. Giao diện truyền thông 215 có thể được tạo cấu hình để thực hiện truyền thông theo tiêu chuẩn truyền thông dùng dây hoặc không dây bất kỳ. Ví dụ, giao diện truyền thông 215 có thể được tạo cấu hình để thực hiện truyền thông theo các giao thức truyền thông không dây thế hệ hai 2G IS- 136 (truy cập đa chia thời (TDMA)), GSM (hệ thống toàn cầu cho truyền thông di động), IS-95 (truy cập đa chia mã (CDMA)), các giao thức truyền thông không dây thế hệ ba 3G, như Hệ thống truyền thông viễn thông di động toàn cầu (UMTS), CDMA2000, CDMA băng rộng (WCDMA) và CDMA đồng bộ chia thời (TD-SCDMA), các giao thức truyền thông không dây thế hệ 3,9 (3,9G), như mạng lưới truy cập rađiô vệ tinh toàn cầu cải tiến (E-UTRAN), với các giao thức truyền thông không dây thế hệ thứ tư 4G, các giao thức cải tiến truyền thông viễn thông di động quốc tế (IMT-Advanced), các giao thức cải tiến dài hạn (LTE) bao gồm LTE cải tiến hoặc dạng tương tự. Ngoài ra, giao diện truyền thông 215 có thể được tạo cấu hình để thực hiện truyền thông theo các kỹ thuật như, ví dụ, tần số rađiô (RF), hồng ngoại (IrDA) hoặc số bất kỳ trong các kỹ thuật mạng không dây khác nhau, bao gồm các kỹ thuật WLAN như IEEE 802.11 (ví dụ, 802.11a, 802.11b, 802.1 Ig, 802. Hn, v.v.), các giao thức mạng cục bộ không dây (WLAN), các kỹ thuật hoạt động liên thông toàn cầu cho truy cập vi sóng (WiMAX) như IEEE 802.16 và/hoặc các kỹ thuật mạng diện cá nhân không dây (WPAN) như IEEE 802.15, BlueTooth (BT), băng siêu rộng (UWB) và/hoặc dạng tương tự.

Bộ phận quản lý chứng thư số 240 và bộ phận quản lý ứng dụng 245 của thiết bị 200 có thể là các phương tiện hoặc thiết bị bất kỳ được lưu trong phần cứng, phần mềm hoặc kết hợp của phần cứng và phần mềm, như bộ xử lý 205 áp dụng các lệnh phần mềm hoặc phần cứng được tạo cấu hình bộ xử lý 205, được tạo cấu hình để thực hiện các chức năng của bộ phận quản lý chứng thư số 240 và/hoặc bộ phận quản lý ứng dụng 245 như được mô tả ở đây. Theo phương án thực hiện làm ví dụ, bộ xử lý 205 có thể bao gồm hoặc theo cách khác là điều khiển bộ phận quản lý chứng thư số 240 và/hoặc bộ phận quản lý ứng

dụng 245. Theo các phương án thực hiện làm ví dụ khác, bộ phận quản lý chứng thư số 240 và/hoặc bộ phận quản lý ứng dụng 245 có thể ở trên các thiết bị khác sao cho một số hoặc tất cả các chức năng của bộ phận quản lý chứng thư số 240 và/hoặc bộ phận quản lý ứng dụng 245 có thể được thực hiện bởi thiết bị thứ nhất và phần còn lại của chức năng của bộ phận quản lý chứng thư số 240 và/hoặc bộ phận quản lý ứng dụng 245 có thể được thực hiện bởi một hoặc nhiều thiết bị khác.

Theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý chứng thư số 240 có thể được tạo cấu hình để nhận ứng dụng phần mềm với chứng thư số bảo mật thứ nhất. Theo đó, chứng thư số bảo mật thứ nhất có thể được kết hợp với ứng dụng phần mềm. Bộ phận quản lý chứng thư số 240 cũng có thể được tạo cấu hình để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không. Theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng bảo mật là mã nhận dạng chứng thư số cấu hình chung của các chứng thư số cấu hình chung (ví dụ, mã nhận dạng chứng thư số cấu hình chung 135) và mã nhận dạng bảo mật được tin cậy là mã nhận dạng chứng thư số cấu hình chung của các chứng thư số phần cứng (ví dụ, các mã nhận dạng chứng thư số cấu hình chung 115). Theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng bảo mật là mã nhận dạng công khai của chứng thư số bảo mật (ví dụ, mã nhận dạng công khai 160) và mã nhận dạng bảo mật được tin cậy là mã nhận dạng công khai của thiết bị (ví dụ, mã nhận dạng công khai 100). Ngoài ra, theo nhiều phương án thực hiện làm ví dụ, xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không bao gồm việc sử dụng mã nhận dạng bảo mật được ký và/hoặc kết hợp với khóa riêng để xác thực mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất.

Bộ phận quản lý chứng thư số 240 cũng có thể được tạo cấu hình để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Theo đó, chứng thư số bảo mật thứ nhất có thể bao gồm tiêu chí phiên bản phần mềm. Theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý chứng thư số 240 được tạo cấu hình để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không, đáp lại bước xác định rằng mã nhận dạng bảo

mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy. Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản phần mềm có thể được thỏa mãn bởi các ứng dụng phần mềm có phiên bản phần mềm ngưỡng hoặc phiên bản phần mềm cao hơn phiên bản phần mềm ngưỡng. Theo các phương án thực hiện khác nhau, phiên bản cao hơn có thể bao gồm việc gia tăng hoặc các mức tăng liên tiếp theo thứ tự, trong đó, phiên bản cao hơn tiếp theo có thể được phát hành gần nhất. Theo nhiều phương án thực hiện làm ví dụ, các chỉ báo của các phiên bản cao hơn có thể được chỉ báo bởi việc tập hợp bất kỳ của các ký tự chữ cái - số.

Theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý chứng thư số 240 cũng được tạo cấu hình để xác thực mã nhận dạng bảo mật được tin cậy bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai phù hợp với mã nhận dạng thiết bị được tin cậy. Theo đó, theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng bảo mật được tin cậy (ví dụ, các mã nhận dạng chứng thư số cấu hình chung 115 của các chứng thư số phần cứng 105) có thể được xác thực bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai (ví dụ, mã nhận dạng công khai 110 của các chứng thư số phần cứng 105) phù hợp với mã nhận dạng thiết bị được tin cậy (ví dụ, mã nhận dạng công khai 100). Theo nhiều phương án thực hiện làm ví dụ, mã nhận dạng thiết bị được tin cậy là giá trị duy nhất, không thể thay đổi được, được kết hợp với thiết bị 200.

Ngoài ra, theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý chứng thư số 240 cũng được tạo cấu hình để xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai hay không. Theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý chứng thư số 240 cũng có thể được tạo cấu hình để xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất (ví dụ, phiên bản chứng thư số cấu hình chung 135) có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai (ví dụ, tiêu chí phiên bản chứng thư số cấu hình chung 120) hay không. Theo đó, chứng thư số bảo mật thứ hai có thể bao gồm tiêu chí phiên bản chứng thư số bảo mật. Tiêu chí phiên bản chứng thư số bảo mật có thể được thỏa mãn bởi giá trị được kết hợp với các biến thể thiết bị chấp nhận được, được xác định trước. Ngoài ra, bộ

phận quản lý chứng thư số 240 cũng có thể được tạo cấu hình để xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai hay không và xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không, đáp lại mã nhận dạng bảo mật được tin cậy được xác thực.

Bộ phận quản lý ứng dụng 245 có thể được tạo cấu hình để cho phép thực thi ứng dụng phần mềm, đáp lại bước xác định rằng phiên bản phần mềm được kết hợp với ứng dụng phần mềm thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất. Theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý ứng dụng 245 được tạo cấu hình để cho phép việc thực thi ứng dụng đáp lại các chứng thư số phần cứng (ví dụ, các chứng thư số phần cứng 105) và các chứng thư số cấu hình chung (ví dụ, các chứng thư số cấu hình chung 125) được xác thực như được mô tả ở đây. Ngoài ra, theo nhiều phương án thực hiện làm ví dụ, bộ phận quản lý ứng dụng 245 được tạo cấu hình để cho phép việc thực thi ứng dụng đáp lại chứng thư số bảo mật đơn được xác thực (ví dụ, chứng thư số bảo mật 155).

Các Fig.3 và Fig.4 minh họa các lưu đồ của hệ thống, phương pháp và sản phẩm chương trình máy tính theo các phương án thực hiện làm ví dụ theo sáng chế. Cần hiểu rằng mỗi khối, bước hoặc công đoạn của các lưu đồ và/hoặc các tổ hợp của các khối, các bước, hoặc các công đoạn trong các lưu đồ, có thể được ứng dụng bởi các phương tiện khác nhau. Các phương tiện để ứng dụng các khối, các bước hoặc các công đoạn của các lưu đồ và/hoặc các tổ hợp của các khối, các bước hoặc các công đoạn trong các lưu đồ có thể bao gồm phần cứng, phần sụn và/hoặc phần mềm bao gồm một hoặc nhiều máy tính các lệnh mã chương trình, các lệnh chương trình hoặc các lệnh mã chương trình có thể thực hiện được đọc được bởi máy tính. Theo một phương án thực hiện làm ví dụ, một hoặc nhiều của các quy trình được mô tả ở đây có thể được ứng dụng bởi các lệnh mã chương trình. Theo đó, các lệnh mã chương trình áp dụng các quy trình được mô tả ở đây có thể được lưu bởi hoặc trên thiết bị nhớ như thiết bị nhớ 210, của thiết bị như thiết bị 200 và được thực hiện bởi bộ xử lý như bộ xử lý 205. Như có thể được xem xét, các lệnh mã chương trình bất kỳ này có thể được tải lên trên máy tính hoặc thiết bị có thể lập trình

được khác (ví dụ, bộ xử lý 205, thiết bị nhớ 210) để tạo ra máy, mà các lệnh khi thực hiện trên máy tính hoặc thiết bị khác có thể lập trình được tạo ra các phương tiện để áp dụng các chức năng được chỉ ra trong các khối (các khối), bước (các bước) hoặc công đoạn (các công đoạn) của lưu đồ. Các lệnh mã chương trình cũng có thể được lưu trong vật ghi đọc được bằng máy tính có thể ra lệnh cho máy tính, bộ xử lý hoặc thiết bị có thể lập trình được khác để thực hiện chức năng theo cách cụ thể, như các lệnh được lưu trong vật ghi đọc được bằng máy tính tạo ra vật phẩm được sản xuất bao gồm các phương tiện hướng dẫn ứng dụng chức năng được chỉ ra trong khối (các khối), bước (các bước) hoặc công đoạn (các công đoạn) của lưu đồ. Các lệnh mã chương trình cũng có thể được tải lên trên máy tính, bộ xử lý hoặc thiết bị có thể lập trình được khác để thực hiện các chuỗi, các bước của công đoạn để được thực hiện trên hoặc bởi máy tính, bộ xử lý hoặc thiết bị có thể lập trình được khác để tạo ra quy trình được ứng dụng bởi máy tính sao cho các lệnh khi thực hiện trên máy tính, bộ xử lý hoặc thiết bị có thể lập trình được khác tạo ra các bước để áp dụng các chức năng được chỉ ra trong khối (các khối), bước (các bước) hoặc công đoạn (các công đoạn) của các lưu đồ. Theo đó, các khối, các bước hoặc các công đoạn của các lưu đồ trợ giúp các tổ hợp của các phương tiện để thực hiện các chức năng cụ thể, các tổ hợp của các bước để thực hiện các chức năng cụ thể và lệnh mã chương trình các phương tiện để thực hiện các chức năng cụ thể. Cũng cần hiểu rằng một hoặc nhiều các khối, các bước hoặc các công đoạn của các lưu đồ và các tổ hợp của các khối, các bước hoặc các công đoạn trong lưu đồ, có thể được ứng dụng bởi các hệ thống máy tính dựa trên phần cứng có mục đích đặc biệt để thực hiện các chức năng hoặc các bước cụ thể, hoặc các tổ hợp của phần cứng có mục đích đặc biệt và các lệnh mã chương trình.

Fig.3 mô tả lưu đồ mô tả phương pháp làm ví dụ quản lý các phiên bản phần mềm. Tại bước 300, phương pháp làm ví dụ bao gồm bước xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất (ví dụ, mã nhận dạng công khai của các chứng thư số phần cứng) có phù hợp với mã nhận dạng bảo mật được tin cậy (ví dụ, mã nhận dạng công khai của thiết bị) hay không. Tại bước 310, phương pháp làm ví dụ còn bao gồm bước xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất. Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản phần mềm có thể được thỏa mãn bởi ứng dụng

phần mềm có phiên bản bằng với giá trị phiên bản ngưỡng hoặc vượt quá giá trị ngưỡng. Theo nhiều phương án thực hiện làm ví dụ, các ngưỡng thời gian của phiên bản và/hoặc các ngưỡng kích thước phần mềm (ví dụ, kích thước theo kilobyte) cũng có thể được sử dụng làm tiêu chí. Ngoài ra, theo nhiều phương án thực hiện làm ví dụ, bước xác định được thực hiện tại bước 310 có thể được thực hiện đáp lại việc xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy ở bước 300. Phương pháp làm ví dụ cũng có thể bao gồm bước cho phép thực thi ứng dụng bởi bộ xử lý tại bước 320. Việc thực thi ứng dụng có thể được cho phép đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm tại bước 310. Ngoài ra, việc thực thi ứng dụng có thể được cho phép đáp lại bước xác định rằng một hoặc nhiều các chứng thư số bảo mật được xác thực.

Fig.4 mô tả lưu đồ của phương pháp khác quản lý các phiên bản phần mềm theo các phương án thực hiện làm ví dụ theo sáng chế. Tại bước 400, phương pháp làm ví dụ có thể bao gồm bước nhận ứng dụng phần mềm và/hoặc có thể tùy chọn để nhận chứng thư số bảo mật thứ nhất được kết hợp (ví dụ, các chứng thư số cấu hình chung). Chứng thư số bảo mật thứ nhất có thể được nhận với ứng dụng phần mềm hoặc tách biệt từ ứng dụng phần mềm, có thể tại thời điểm khác. Theo nhiều phương án thực hiện làm ví dụ, ứng dụng phần mềm và chứng thư số bảo mật thứ nhất được kết hợp có thể được nhận trên thiết bị nhớ như thiết bị nhớ 210.

Phương pháp làm ví dụ cũng có thể bao gồm, ở bước 410, bước xác thực mã nhận dạng bảo mật được tin cậy (ví dụ, các mã nhận dạng chứng thư số cấu hình chung của các chứng thư số phần cứng) bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai (ví dụ, mã nhận dạng công khai của các chứng thư số phần cứng) phù hợp với mã nhận dạng thiết bị được tin cậy (ví dụ, mã nhận dạng công khai của thiết bị). Theo đó, chứng thư số bảo mật thứ hai cũng có thể bao gồm tiêu chí phiên bản chứng thư số bảo mật (ví dụ, tiêu chí phiên bản chứng thư số cấu hình chung). Ngoài ra, mã nhận dạng thiết bị được tin cậy có thể là duy nhất, giá trị không thể biến đổi được. Tại bước 420, phương pháp làm ví dụ có thể bao gồm bước xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất (ví dụ, phiên bản chứng thư số cấu hình chung) có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật

thứ hai hay không. Bước xác định được thực hiện tại bước 420 có thể được thực hiện đáp lại mã nhận dạng bảo mật được tin cậy được xác thực tại bước 410. Ngoài ra, phương pháp làm ví dụ cũng có thể bao gồm, tại bước 430, bước xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất (ví dụ, các mã nhận dạng chứng thư số cấu hình chung của các chứng thư số cấu hình chung) có phù hợp với mã nhận dạng bảo mật được tin cậy hay không (ví dụ, các mã nhận dạng chứng thư số cấu hình chung của các chứng thư số phần cứng). Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản chứng thư số bảo mật có thể được thỏa mãn bởi giá trị được kết hợp với các biến thể thiết bị chấp nhận được, được xác định trước. Ngoài ra, theo nhiều phương án thực hiện làm ví dụ, bước xác định được thực hiện tại bước 430 có thể xuất hiện đáp lại mã nhận dạng bảo mật được tin cậy được xác thực tại bước 410.

Ở bước 440, phương pháp làm ví dụ còn có thể bao gồm bước xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không. Theo nhiều phương án thực hiện làm ví dụ, tiêu chí phiên bản phần mềm có thể được thỏa mãn bởi ứng dụng phần mềm có phiên bản bằng với giá trị phiên bản ngưỡng hoặc vượt quá giá trị ngưỡng. Theo nhiều phương án thực hiện làm ví dụ, các ngưỡng thời gian của phiên bản và/hoặc các ngưỡng kích thước phần mềm (ví dụ, kích thước theo kilobyte) cũng có thể được sử dụng làm tiêu chí. Theo nhiều phương án thực hiện làm ví dụ, bước xác định được thực hiện ở bước 440 có thể được thực hiện đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy ở bước 430.

Phương pháp làm ví dụ cũng có thể bao gồm bước cho phép thực thi ứng dụng bởi bộ xử lý ở bước 450. Việc thực thi ứng dụng có thể được cho phép đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm ở bước 440.

Hiệu quả của nhiều phương án thực hiện làm ví dụ theo sáng chế là để ngăn cản các phiên bản phần mềm không được xác thực được thực thi bởi các thiết bị. Sáng chế có ưu điểm là ngăn cản việc lỗi thời hoặc theo cách khác là phần mềm không mong muốn bị cài đặt và được sử dụng trên các thiết bị, như các thiết bị tính toán và/hoặc các thiết bị truyền thông khác. Ngoài ra, nhiều phương án thực hiện làm ví dụ theo sáng chế cho phép phần mềm mới và/hoặc phần mềm được cải tiến được cài đặt trên các thiết bị trong khi sản

xuất hoặc trước khi vận chuyển tới người tiêu dùng và nhờ đó ngăn chặn việc cài lại phần mềm trên các thiết bị này về các bản cũ hoặc các phiên bản không mong muốn sau khi các thiết bị được sử dụng bởi người tiêu dùng.

Nhiều biến thể và các phương án thực hiện khác theo sáng chế được nêu ở đây sẽ là hiển nhiên đối với người có hiểu biết trung bình trong lĩnh vực liên quan nhờ phần bộc lộ của phần mô tả nêu trên và các hình vẽ kèm theo. Do đó, cần hiểu rằng các sáng chế không bị hạn chế vào các phương án thực hiện cụ thể được bộc lộ và các biến thể và các phương án thực hiện khác được nhằm mục đích được chứa trong phạm vi của các yêu cầu bảo hộ kèm theo. Tuy nhiên, mặc dù các phần mô tả nêu trên và các hình vẽ kèm theo mô tả các phương án thực hiện làm ví dụ trong ngữ cảnh của các tổ hợp làm ví dụ cụ thể của các thành phần và/hoặc các chức năng, cần hiểu rằng các tổ hợp khác nhau của các thành phần và/hoặc các chức năng có thể được tạo ra bởi các phương án thực hiện thay thế mà không tách khỏi phạm vi của các điểm yêu cầu bảo hộ kèm theo. Theo đó, ví dụ, các tổ hợp khác nhau của các thành phần và/hoặc các chức năng khác với các tổ hợp đã được mô tả rõ ràng ở trên cũng được coi là có thể được bao hàm trong các điểm yêu cầu bảo hộ kèm theo. Mặc dù các thuật ngữ cụ thể được nêu ra ở đây, nhưng chúng được sử dụng chỉ theo nghĩa chung và nghĩa mô tả và không nhằm mục đích làm hạn chế sáng chế.

Yêu cầu bảo hộ

1. Phương pháp quản lý các phiên bản phần mềm bao gồm các bước:

xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không, chứng thư số bảo mật thứ nhất bao gồm tiêu chí phiên bản phần mềm;

xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không, đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy; và

cho phép thực thi ứng dụng phần mềm nhờ bộ xử lý, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm;

xác thực mã nhận dạng bảo mật được tin cậy bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai phù hợp với mã nhận dạng thiết bị được tin cậy, chứng thư số bảo mật thứ hai bao gồm tiêu chí phiên bản chứng thư số bảo mật; và

xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai hay không, đáp lại mã nhận dạng bảo mật được tin cậy được xác thực; và

trong đó bước xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không bao gồm việc xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không, đáp lại mã nhận dạng bảo mật được tin cậy được xác thực.

2. Phương pháp theo điểm 1, trong đó bước xác thực mã nhận dạng bảo mật được tin cậy bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai phù hợp với mã nhận dạng thiết bị được tin cậy bao gồm mã nhận dạng thiết bị được tin cậy là giá trị duy nhất, không thể biến đổi được.

3. Phương pháp theo điểm 1, trong đó bước xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thỏa mãn tiêu chí phiên bản chứng thư số

bảo mật của chứng thư số bảo mật thứ hai hay không bao gồm tiêu chí phiên bản chứng thư số bảo mật được thỏa mãn bởi giá trị được kết hợp với các biến thể thiết bị được xác định trước.

4. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm bước nhận ứng dụng phần mềm với chứng thư số bảo mật thứ nhất, chứng thư số bảo mật thứ nhất được kết hợp với ứng dụng phần mềm.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó bước xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không bao gồm tiêu chí phiên bản phần mềm được thỏa mãn bởi các ứng dụng phần mềm có phiên bản phần mềm ngưỡng hoặc phiên bản phần mềm cao hơn phiên bản phần mềm ngưỡng.

6. Thiết bị quản lý các phiên bản phần mềm bao gồm:

phương tiện để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không, chứng thư số bảo mật thứ nhất bao gồm tiêu chí phiên bản phần mềm;

phương tiện để xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không, đáp lại bước xác định rằng mã nhận dạng bảo mật của chứng thư số thứ nhất phù hợp với mã nhận dạng bảo mật được tin cậy; và

phương tiện để cho phép thực thi ứng dụng phần mềm, đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm,

phương tiện để xác thực mã nhận dạng bảo mật được tin cậy bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai phù hợp với mã nhận dạng thiết bị được tin cậy, chứng thư số bảo mật thứ hai bao gồm tiêu chí phiên bản chứng thư số bảo mật; và

phương tiện để xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai hay không, đáp lại mã nhận dạng bảo mật được tin cậy được xác thực; và

trong đó phương tiện để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không bao gồm phương tiện để xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không, đáp lại mã nhận dạng bảo mật được tin cậy được xác thực.

7. Thiết bị theo điểm 6, trong đó mã nhận dạng thiết bị được tin cậy là giá trị duy nhất, không thể biến đổi được.

8. Thiết bị theo điểm 6, trong đó bước xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thỏa mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai hay không bao gồm tiêu chí phiên bản chứng thư số bảo mật được thỏa mãn bởi giá trị được kết hợp với các biến thể thiết bị được xác định trước.

9. Thiết bị theo điểm 6, trong đó thiết bị này còn bao gồm phương tiện để nhận ứng dụng phần mềm với chứng thư số bảo mật thứ nhất, chứng thư số bảo mật thứ nhất được kết hợp với ứng dụng phần mềm.

10. Thiết bị theo điểm 6, trong đó thiết bị này còn bao gồm phương tiện để lưu chứng thư số bảo mật thứ hai.

11. Thiết bị theo điểm 6, trong đó bước xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không bao gồm tiêu chí phiên bản phần mềm được thỏa mãn bởi các ứng dụng phần mềm có phiên bản phần mềm ngưỡng hoặc phiên bản phần mềm cao hơn phiên bản phần mềm ngưỡng.

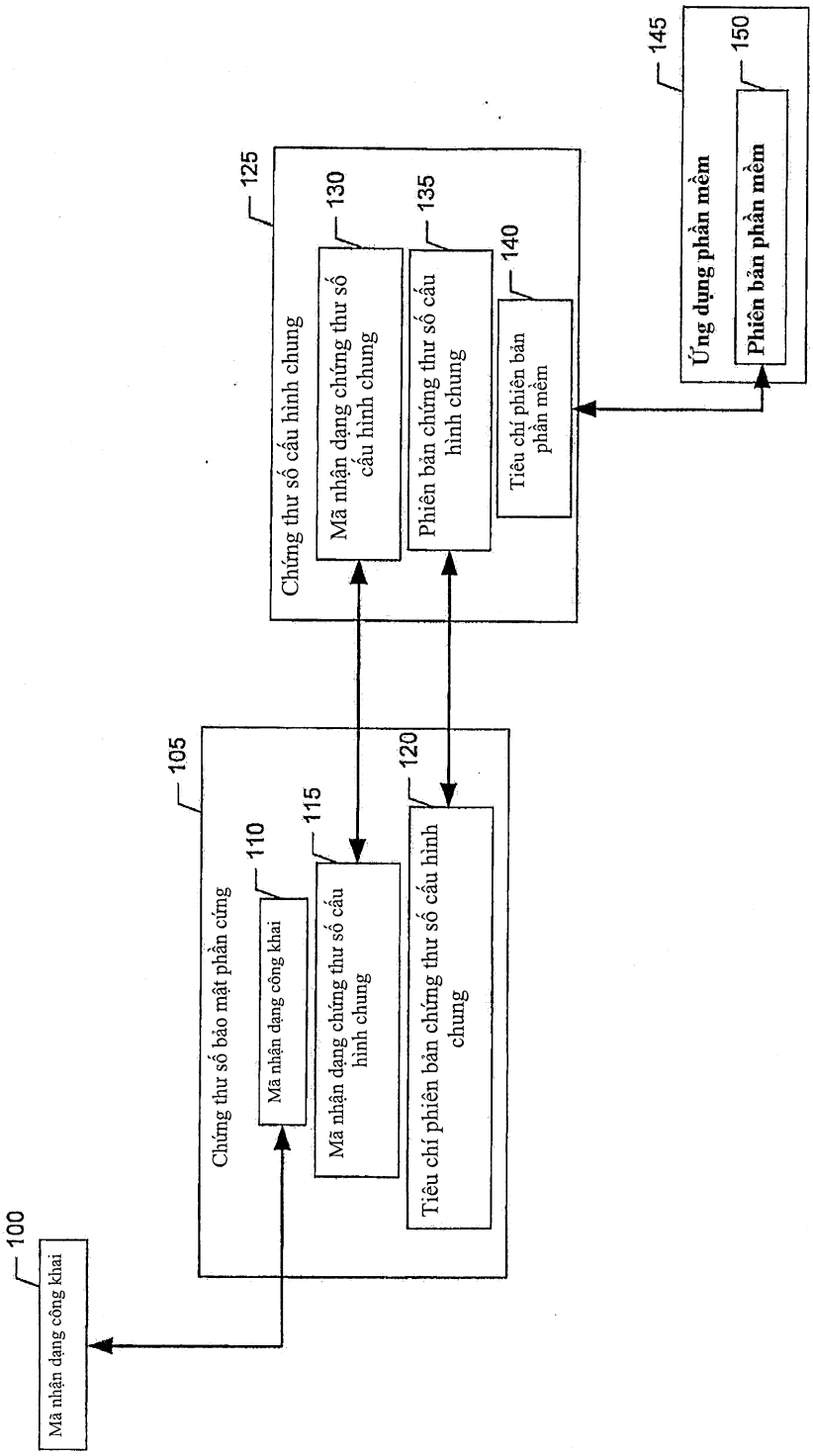

100
Mã nhận dạng công khai
105
Chứng thư số bảo mật phần cứng
110
Mã nhận dạng công khai
115
Mã nhận dạng chứng thư số cấu hình chung
120
Tiêu chí phiên bản chứng thư số cấu hình chung
125
Chứng thư số cấu hình chung
130
Mã nhận dạng chứng thư số cấu hình chung
135
Phiên bản chứng thư số cấu hình chung
140
Tiêu chí phiên bản phần mềm
145
Ứng dụng phần mềm
150
Phiên bản phần mềm

FIG. 1a

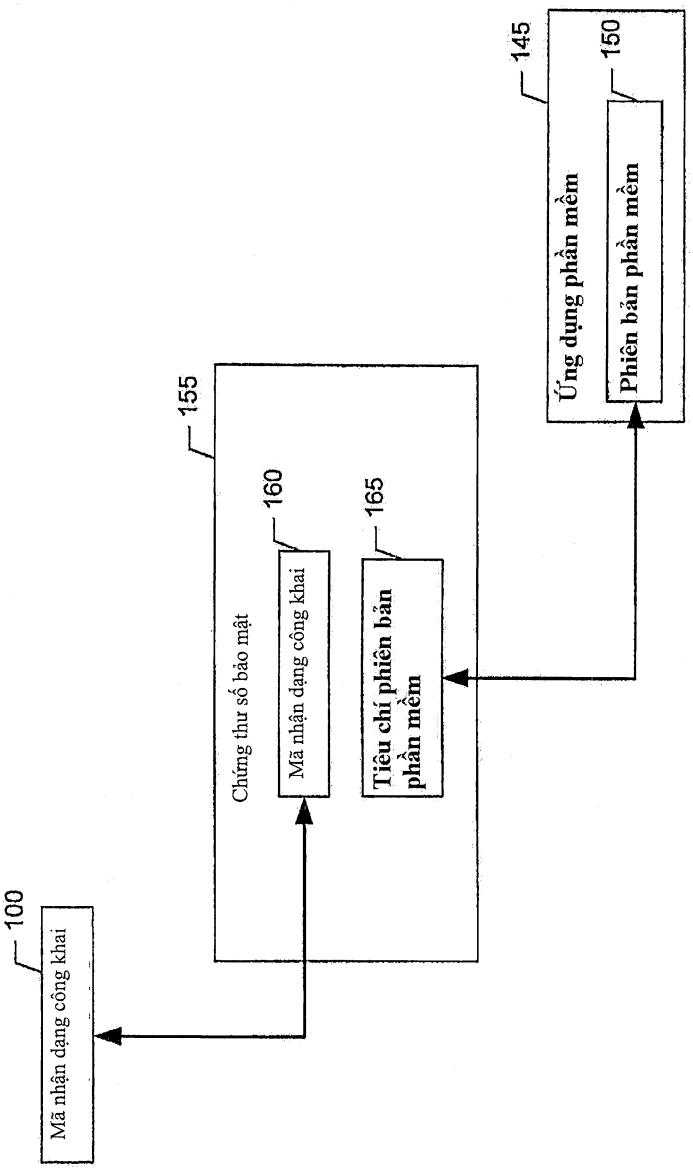

100
Mã nhận dạng công khai
155
Chứng thư số bảo mật
160
Mã nhận dạng công khai
165
Tiêu chí phiên bản phần mềm
145
Ứng dụng phần mềm
150
Phiên bản phần mềm

FIG. 1b

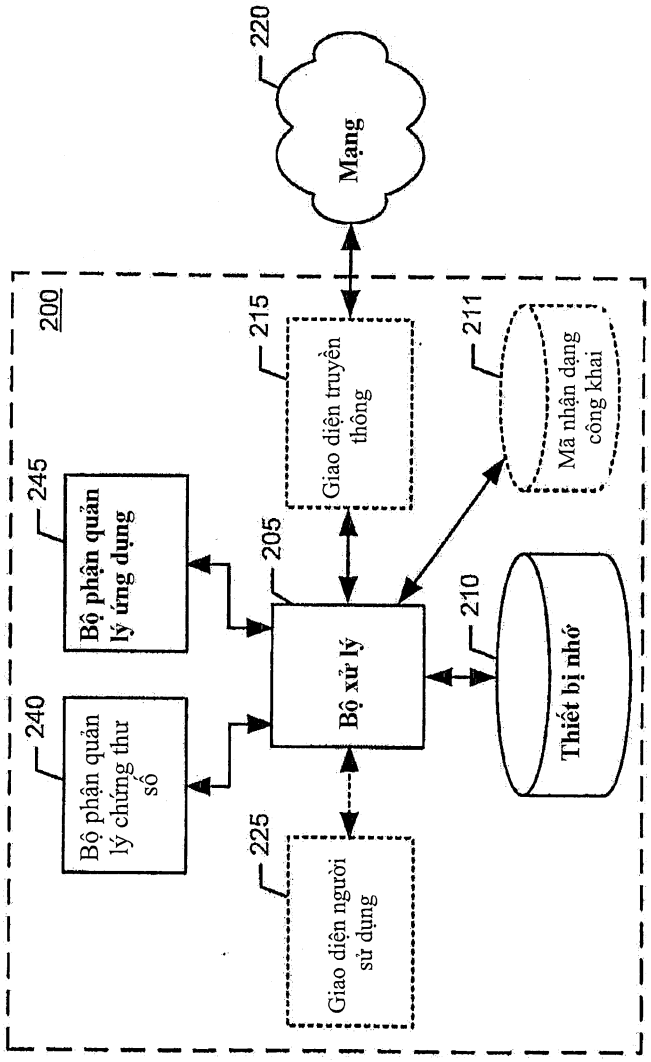

220
Mạng
200
215
Giao diện truyền thông
211
Mã nhận dạng công khai
245
Bộ phận quản lý ứng dụng
205
Bộ xử lý
210
Thiết bị nhớ
240
Bộ phận quản lý chứng thư số
225
Giao diện người sử dụng

FIG. 2

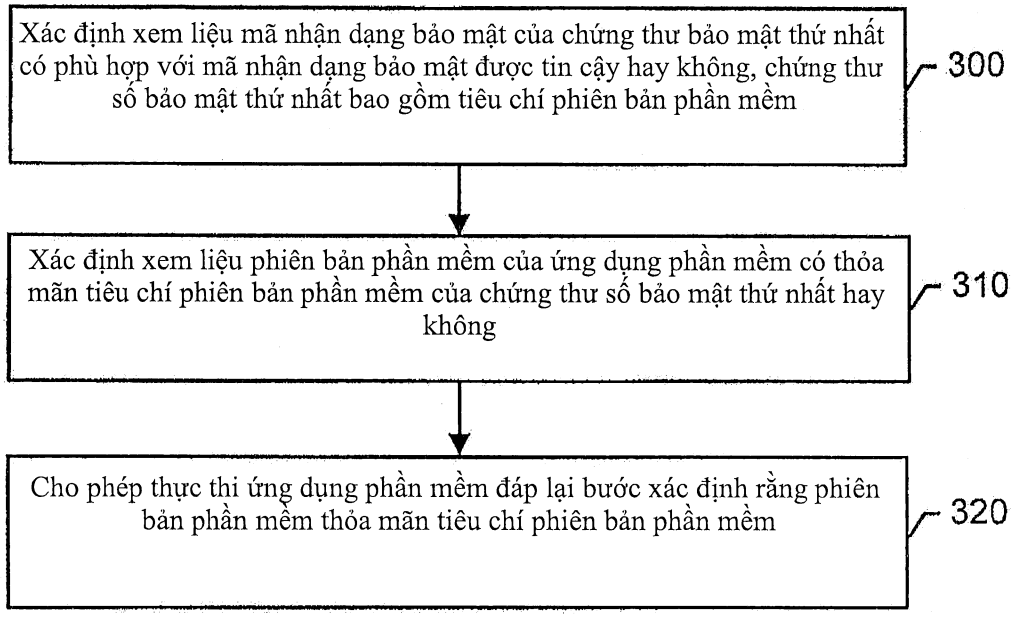

Xác định xem liệu mã nhận dạng bảo mật của chứng thư bảo mật thứ nhất có phù hợp với mã nhận dạng bảo mật được tin cậy hay không, chứng thư số bảo mật thứ nhất bao gồm tiêu chí phiên bản phần mềm
300
Xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mãn tiêu chí phiên bản phần mềm của chứng thư số bảo mật thứ nhất hay không
310
Cho phép thực thi ứng dụng phần mềm đáp lại bước xác định rằng phiên bản phần mềm thỏa mãn tiêu chí phiên bản phần mềm
320

FIG. 3

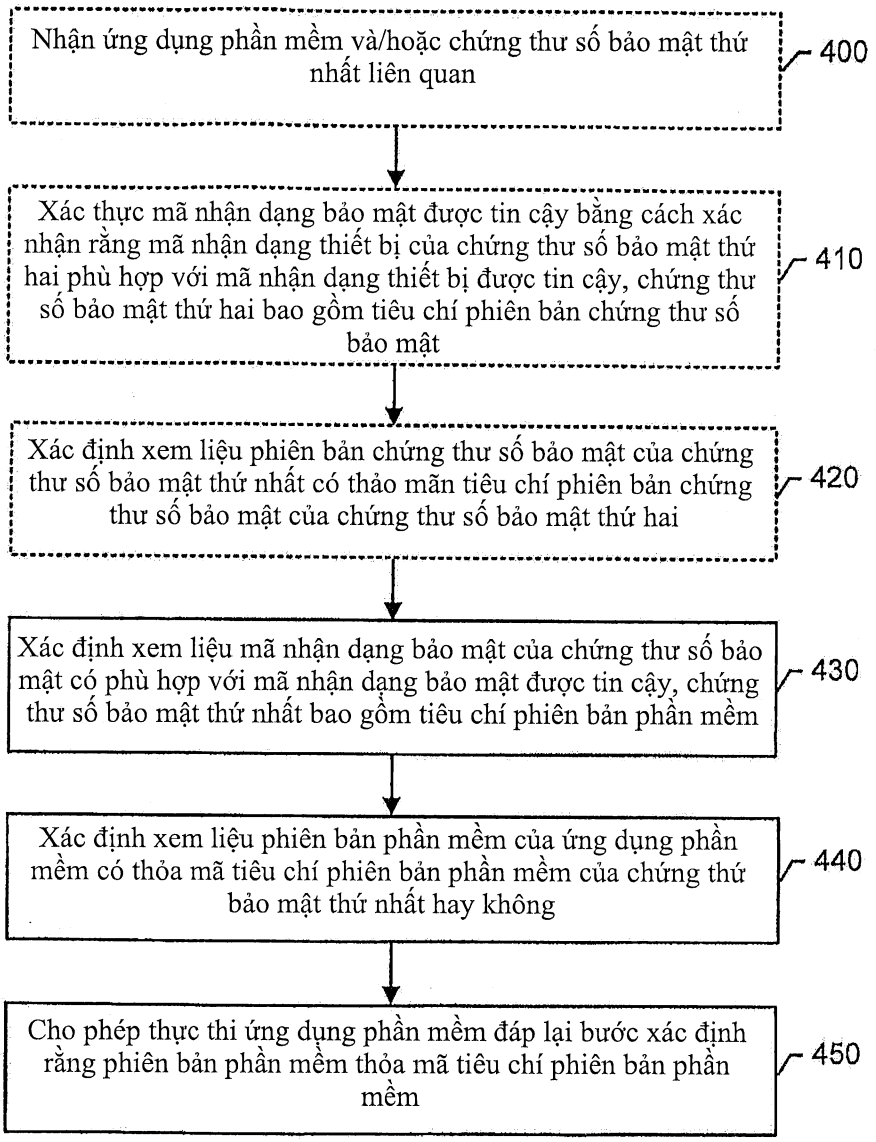

Nhận ứng dụng phần mềm và/hoặc chứng thư số bảo mật thứ nhất liên quan
400
Xác thực mã nhận dạng bảo mật được tin cậy bằng cách xác nhận rằng mã nhận dạng thiết bị của chứng thư số bảo mật thứ hai phù hợp với mã nhận dạng thiết bị được tin cậy, chứng thư số bảo mật thứ hai bao gồm tiêu chí phiên bản chứng thư số bảo mật
410
Xác định xem liệu phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ nhất có thảo mãn tiêu chí phiên bản chứng thư số bảo mật của chứng thư số bảo mật thứ hai
420
Xác định xem liệu mã nhận dạng bảo mật của chứng thư số bảo mật có phù hợp với mã nhận dạng bảo mật được tin cậy, chứng thư số bảo mật thứ nhất bao gồm tiêu chí phiên bản phần mềm
430
Xác định xem liệu phiên bản phần mềm của ứng dụng phần mềm có thỏa mã tiêu chí phiên bản phần mềm của chứng thứ bảo mật thứ nhất hay không
440
Cho phép thực thi ứng dụng phần mềm đáp lại bước xác định rằng phiên bản phần mềm thỏa mã tiêu chí phiên bản phần mềm
450

FIG. 4