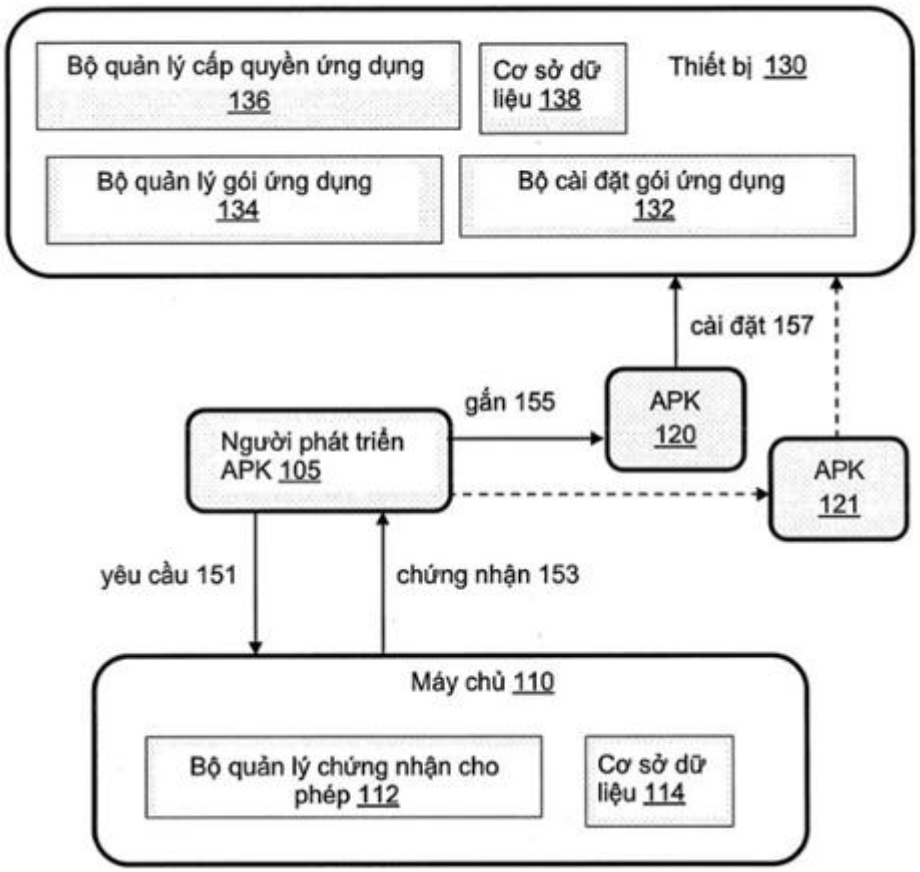
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0038542**
(51)[7] **G06F 21/51**; G06F 21/64; G06F 21/62
(13) **B**

(21) 1-2017-04161
(22) 03/11/2016
(86) PCT/SG2016/050539 03/11/2016
(87) WO/2017/078624 11/05/2017
(30) 10201509221Y 06/11/2015 SG
(45) 25/01/2024 430
(43) 25/07/2018 364A
(73) HUAWEI INTERNATIONAL PTE. LTD. (SG)
51, Changi Business Park Central 2, #07-08, The Signature, Singapore 486066
(72) WU, Yongzheng (CN); WEN, Xuejun (CN).
(74) Công ty TNHH T&T INVENMARK Sở hữu trí tuệ Quốc tế (T&T INVENMARK CO., LTD.)

(54) PHƯƠNG PHÁP QUẢN LÝ VIỆC CÀI ĐẶT GÓI ỨNG DỤNG VÀO THIẾT BỊ DI ĐỘNG VÀ THIẾT BỊ DI ĐỘNG

(57) Sáng chế đề cập đến phương pháp quản lý việc cài đặt gói ứng dụng Android (APK) vào thiết bị di động và thiết bị di động, nhờ đó APK yêu cầu thiết bị chấp thuận sự cho phép nguy cơ cao đặc trưng cho ứng dụng khi cài đặt.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống và phương pháp quản lý việc cài đặt gói ứng dụng Android (Android application package - APK) vào thiết bị di động và thiết bị di động trong đó APK yêu cầu thiết bị chấp thuận sự cho phép nguy cơ cao đặc trưng cho ứng dụng khi cài đặt.

Tình trạng kỹ thuật của sáng chế

Phần lớn nền tảng phần mềm hoặc hệ điều hành thường tạo ra các giao diện lập trình ứng dụng (application programming interface - API) mà mỗi giao diện thực hiện một chức năng cụ thể khi được gọi bởi các ứng dụng của nền tảng phần mềm hoặc hệ điều hành. Tuy nhiên, trước khi nền tảng phần mềm cho phép gọi ra API yêu cầu bởi ứng dụng, nền tảng phần mềm trước tiên sẽ xác định xem ứng dụng có cho phép gọi ra API hay không.

Hệ điều hành sử dụng cấu trúc cho phép hạn chế cái mà ứng dụng đã cài đặt có thể thực hiện khi chạy thực có thể là hệ điều hành Android. Trước khi ứng dụng được cài đặt trong thiết bị chạy hệ điều hành Android, danh mục cho phép yêu cầu bởi ứng dụng sẽ được liệt kê trong tệp kê khai ứng dụng. Trong quá trình cài đặt ứng dụng vào thiết bị, sự cho phép yêu cầu bởi ứng dụng được xác thực và chấp thuận bởi bộ cài đặt gói ứng dụng trong thiết bị. Bốn loại cho phép cơ bản mà có thể được chấp thuận bởi hệ điều hành Android là loại cho phép "bình thường", "nguy hại", "chữ ký", và "chữ ký/hệ thống".

Loại cho phép "bình thường" là sự cho phép nguy cơ thấp mà thường được chấp thuận theo mặc định với ứng dụng yêu cầu. Loại cho phép "nguy hại" là loại cho phép nguy cơ cao tiềm năng mà có thể cho phép ứng dụng yêu cầu truy cập dữ liệu riêng của thiết bị, ví dụ tin nhắn, ảnh, email, hoặc truy cập trực tiếp với thiết bị. Như vậy, bộ cài đặt gói ứng dụng của thiết bị sẽ thường yêu cầu người sử dụng thiết bị chấp nhận việc chấp thuận cho phép như vậy trước khi sự cho phép yêu cầu được chấp nhận với ứng dụng yêu cầu trong quá trình cài đặt. Loại cho phép "chữ ký" và "chữ ký/hệ thống" là sự cho phép nguy cơ cao mà yêu cầu ứng dụng phải có sự cho phép được ký bằng chữ ký của hệ thống Android. Những thứ của API mà có thể được gọi ra bởi loại cho phép

"bình thường" hoặc "nguy hại" bao gồm, không chỉ giới hạn ở, việc nhận và gửi tin nhắn dịch vụ tin nhắn ngắn (Short-Message-Service - SMS), tìm hệ tọa độ (Global Positioning System - GPS), đọc liên lạc, sử dụng camera, tìm ảnh v.v. trong khi những thứ của API mà chỉ có thể được gọi ra bởi loại cho phép "chữ ký" hoặc "chữ ký/hệ thống" bao gồm, nhưng không chỉ giới hạn ở, việc thiết lập lại các thiết lập của thiết bị với mặc định của hãng, hủy truyền thông, dỡ cài đặt các ứng dụng khác v.v..

Các ứng dụng mà được cho phép với loại cho phép "bình thường" hoặc "nguy hại" thường bao gồm các ứng dụng bên thứ ba trong khi các ứng dụng mà được chấp thuận thì loại cho phép "chữ ký" hoặc "chữ ký/hệ thống" thường bao gồm các hệ thống ứng dụng được phát triển bởi nhà sản xuất thiết bị. Như vậy, các ứng dụng mà được phân loại dưới dạng hệ thống các ứng dụng thường được chấp thuận với tất cả các loại cho phép "chữ ký" hoặc "chữ ký/hệ thống" của thiết bị.

Hiện nay, trong hệ điều hành Android, để ứng dụng bên thứ ba được làm phù hợp với sự cho phép nguy cơ cao, người phát triển ứng dụng bên thứ ba trước tiên sẽ đệ trình ứng dụng cần được ký lại bởi nhà sản xuất thiết bị trong hệ thống ứng dụng. Khi ứng dụng được ký lại, khóa phát triển gốc của ứng dụng trong ứng dụng đối tượng được loại bỏ và tiếp đó ứng dụng đối tượng được ký bằng khóa hệ thống Android. Sau khi ứng dụng bên thứ ba đã được ký lại dưới dạng hệ thống ứng dụng, tiếp đó ứng dụng bên thứ ba đã ký lại sẽ được làm phù hợp với tất cả sự cho phép nguy cơ cao. Trong quá trình cài đặt ứng dụng, hệ thống Android sẽ nhận biết ứng dụng đã ký lại dưới dạng ứng dụng hệ thống khi khóa mới ký của ứng dụng phù hợp với khóa chung của hệ điều hành Android. Nếu hai khóa này không giống nhau, thì khi đó ứng dụng sẽ được nhận biết dưới dạng ứng dụng bên thứ ba.

Khi ứng dụng bên thứ ba đã được ký lại dưới dạng hệ thống ứng dụng, điều này dẫn đến ứng dụng bên thứ ba không chỉ có sự cho phép nguy cơ cao yêu cầu mà còn có tất cả các sự cho phép loại chữ ký/hệ thống mà thường được ấn định cho hệ thống các ứng dụng. Đây là nhược điểm vì nó xâm phạm nguyên tắc đặc quyền tối thiểu. Như vậy, phương pháp này không đề cập đầy đủ đến trường hợp trong đó ứng dụng bên thứ ba chỉ yêu cầu sự cho phép đặc trưng để truy cập API.

Vì các lý do nêu trên, người có hiểu biết trung bình về lĩnh vực này cố gắng đề xuất hệ thống và phương pháp quản lý việc cài đặt ứng dụng, thuộc người phát triển bên thứ ba, vào thiết bị trong đó ứng dụng cần được cài đặt yêu cầu loại cho phép nguy cơ cao như sự cho phép loại hệ thống và/hoặc chữ ký/hệ thống.

Bản chất kỹ thuật của sáng chế

Để giải quyết các vấn đề nêu trên, sáng chế đề xuất hệ thống và phương pháp quản lý việc cài đặt gói ứng dụng Android vào thiết bị.

Ưu điểm thứ nhất của các phương án về hệ thống và phương pháp theo sáng chế đó là chỉ các sự cho phép định trước đặc trưng được chấp thuận cho ứng dụng. Các sự cho phép ở mức hệ thống hoặc chữ ký/hệ thống khác mà không được yêu cầu sẽ không được chấp thuận một cách tự động cho ứng dụng.

Ưu điểm thứ hai của các phương án về hệ thống và phương pháp theo sáng chế đó là sự cho phép nguy cơ cao chỉ được chấp thuận cho một ứng dụng cụ thể vì chứng nhận cho phép đã cấp sẽ chỉ thực hiện với một ứng dụng cụ thể. Điều này đảm bảo rằng sự cho phép nguy cơ cao mà đã được chấp thuận không thể bị dùng sai hoặc khai thác bởi người phát triển ứng dụng.

Ưu điểm thứ ba của các phương án về hệ thống và phương pháp theo sáng chế đó là chứng nhận cho phép được cấp cho một ứng dụng có thể chứa các nhận dạng thiết bị nghĩa là chứng nhận cho phép có thể chấp thuận các sự cho phép nguy cơ cao chỉ cho một nhóm nhỏ thiết bị và không phải tất cả các thiết bị thuộc một nhà sản xuất cụ thể.

Ưu điểm thứ tư của các phương án về hệ thống và phương pháp theo sáng chế đó là chứng nhận cho phép có thể được gắn trong gói ứng dụng và được tìm trong quá trình cài đặt hoặc chứng nhận cho phép có thể được tải xuống từ máy chủ an toàn của nhà sản xuất thiết bị trong quá trình cài đặt gói ứng dụng.

Các ưu điểm nêu trên được tạo ra bởi hệ thống theo các phương án của sáng chế hoạt động theo cách sau.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp quản lý việc cài đặt gói ứng dụng Android (APK) vào thiết bị, trong đó phương pháp này bao gồm các bước: nhận, bởi thiết bị, yêu cầu cài đặt đối với APK; tìm, bởi thiết bị, chứng nhận cho phép đối với APK theo yêu cầu cài đặt, trong đó chứng nhận cho phép đối với APK bao gồm chữ ký theo mật mã; xác định, bởi thiết bị, tính hợp lệ của chứng nhận cho phép bằng cách xác thực chữ ký theo mật mã chứa trong chứng nhận cho phép bằng cách sử dụng khóa chung chứng nhận cho phép của nhà sản xuất thiết bị, trong đó khóa chung chứng nhận cho phép được lưu trữ trong thiết bị; và cho phép cài đặt APK vào thiết bị nếu chứng nhận cho phép được xác định là hợp lệ.

Đối với khía cạnh thứ nhất, theo cách thực hiện thứ nhất của khía cạnh thứ nhất, trong đó trước bước cho phép cài đặt APK vào thiết bị nếu chứng nhận cho phép được xác định là hợp lệ, phương pháp này còn bao gồm bước: xác định xem yêu cầu cho phép

chứa trong yêu cầu cài đặt tương ứng với sự cho phép được chấp thuận trong chứng nhận cho phép đối với APK hay không; và duyệt chứng nhận cho phép khi xác định rằng yêu cầu cho phép chứa trong yêu cầu cài đặt tương ứng với sự cho phép được chấp thuận trong chứng nhận cho phép.

Đối với khía cạnh thứ nhất hoặc cách thực hiện thứ nhất của khía cạnh thứ nhất, theo cách thực hiện thứ hai của khía cạnh thứ nhất, việc xác thực chữ ký theo mật mã chứa trong chứng nhận cho phép bao gồm: tính băm mật mã của APK bằng cách sử dụng hàm băm mật mã; và so sánh băm mật mã đã tính của APK với băm mật mã của APK lưu trữ trong chứng nhận cho phép.

Đối với khía cạnh thứ nhất, cách thực hiện thứ nhất của khía cạnh thứ nhất, hoặc cách thực hiện thứ hai của khía cạnh thứ nhất, theo cách thực hiện thứ ba của khía cạnh thứ nhất, chữ ký theo mật mã chứa trong chứng nhận cho phép được tạo ra ở máy chủ liên kết với nhà sản xuất thiết bị khi khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị được dùng để ký theo mật mã chứng nhận cho phép đối với APK.

Đối với cách thực hiện thứ ba của khía cạnh thứ nhất, theo cách thực hiện thứ tư của khía cạnh thứ nhất, chứng nhận cho phép đã ký theo mật mã đối với APK bao gồm khóa chung phát triển của APK, tên của APK; sự cho phép được chấp thuận với APK, và thời gian có hiệu lực của chứng nhận cho phép.

Đối với cách thực hiện thứ ba của khía cạnh thứ nhất hoặc cách thực hiện thứ tư của khía cạnh thứ nhất, theo cách thực hiện thứ năm của khía cạnh thứ nhất, chứng nhận cho phép đối với APK được ký theo mật mã sau khi máy chủ nhận APK phát hành trước chứa chứng nhận cho phép phát triển mà đã được ký theo mật mã bằng cách sử dụng khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị, và trong đó chứng nhận cho phép phát triển cho phép APK phát hành trước được cài đặt trong thiết bị phát triển định trước.

Đối với khía cạnh thứ nhất, hoặc cách thực hiện thứ nhất, thứ hai, thứ ba, thứ tư hoặc thứ năm của khía cạnh thứ nhất, theo cách thực hiện thứ sáu của khía cạnh thứ nhất, bước tìm chứng nhận cho phép đối với APK bao gồm bước tách chứng nhận cho phép ra khỏi APK.

Đối với khía cạnh thứ nhất, hoặc cách thực hiện thứ nhất, thứ hai, thứ ba, thứ tư hoặc thứ năm của khía cạnh thứ nhất, theo cách thực hiện thứ bảy của khía cạnh thứ nhất, bước tìm chứng nhận cho phép đối với APK bao gồm bước tải chứng nhận cho phép từ máy chủ ở xa vào thiết bị.

Mô tả vắn tắt các hình vẽ

Các ưu điểm và dấu hiệu nêu trên theo sáng chế được mô tả chi tiết dưới đây và được thể hiện trên các hình vẽ sau:

Fig.1 thể hiện sơ đồ khối của hệ thống quản lý việc cài đặt gói ứng dụng (APK) vào thiết bị theo một phương án của sáng chế;

Fig.2 thể hiện sơ đồ khối của hệ thống quản lý việc cài đặt gói ứng dụng (APK) vào thiết bị nhờ đó chứng nhận cho phép phát triển được cấp trước khi cấp chứng nhận cho phép theo một phương án của sáng chế;

Fig.3 thể hiện sơ đồ quy trình quản lý việc cài đặt gói ứng dụng (APK) vào thiết bị theo các phương án của sáng chế;

Fig.4 thể hiện sơ đồ quy trình để cấp chứng nhận cho phép cho một gói ứng dụng theo một phương án của sáng chế;

Fig.5 thể hiện sơ đồ quy trình để cấp chứng nhận cho phép phát triển tiếp theo là chứng nhận cho phép theo một phương án của sáng chế; và

Fig.6 thể hiện sơ đồ khối đại diện cho các hệ thống xử lý theo các phương án của sáng chế.

Mô tả chi tiết sáng chế

Sáng chế đề xuất hệ thống và phương pháp quản lý việc cài đặt gói ứng dụng Android (APK) vào thiết bị nhờ đó APK yêu cầu thiết bị chấp thuận sự cho phép nguy cơ cao đặc trưng cho ứng dụng khi cài đặt. Cụ thể hơn, sáng chế đề xuất hệ thống và phương pháp xác định xem APK, mà yêu cầu truy cập vào các giao diện lập trình (Programming Interface - API) ứng dụng đã bảo vệ, có thể được phép cài đặt trong thiết bị hay không. API đã bảo vệ đề cập đến API chỉ được gọi ra bởi các ứng dụng mà có sự cho phép nguy cơ cao yêu cầu.

Fig.1 thể hiện hệ thống quản lý việc cài đặt APK 120 hoặc APK 121 trong thiết bị 130 theo một phương án của sáng chế. Thiết bị 130 có thể bao gồm các thiết bị di động như, nhưng không chỉ giới hạn ở, điện thoại thông minh, máy tính bảng, máy tính xách tay và/hoặc hệ thống máy tính như vậy. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng các môđun phần mềm hoặc môđun chức năng thể hiện trên Fig.1, như các môđun trong thiết bị 130 và máy chủ 110, có thể được viết bằng cách sử dụng các mã phát triển đối với các hệ điều hành như vậy hoặc có thể được cải biến từ các loại hiện có hoặc các bộ phận được mã hóa đối với hệ điều hành như vậy để thực hiện các

quy trình yêu cầu bởi mỗi môđun như được mô tả dưới đây và rằng dữ liệu hoặc thông tin có thể được truyền giữa các môđun này khi cần.

Hệ thống thể hiện trên Fig.1 hoạt động theo cách sau. Người phát triển APK 105 bắt đầu quy trình chấp thuận chứng nhận cho phép bằng cách đệ trình trước tiên yêu cầu 151 với máy chủ 110. Máy chủ 110 có thể là máy chủ ở xa hoặc máy chủ nội vùng liên kết với, hoặc thuộc, nhà sản xuất thiết bị 130 và máy chủ 110 có thể được nối thông với người phát triển APK 105 qua kết nối có dây hoặc kết nối không dây. Yêu cầu 151 sẽ chứa thông tin như khóa chung phát triển của ứng dụng, tên của gói ứng dụng, và sự cho phép hoặc các sự cho phép yêu cầu bởi ứng dụng. Các sự cho phép chứa trong yêu cầu 151 có thể bao gồm sự cho phép loại bình thường, nguy hại, chữ ký và/hoặc chữ ký/hệ thống. Như nêu trên, sự cho phép nguy cơ cao đề cập đến sự cho phép loại chữ ký và/hoặc chữ ký/hệ thống mà thường chỉ được chấp thuận cho hệ thống các ứng dụng.

Khi nhận yêu cầu 151, máy chủ 110 sẽ phân tích các nội dung của yêu cầu 151 và trên cơ sở các nội dung của yêu cầu 151, xác định xem chứng nhận cho phép cần được cấp cho người phát triển APK 105 hay không. Nếu máy chủ 110 xác định rằng chứng nhận cho phép cần được cấp cho người phát triển APK 105, máy chủ 110 sử dụng bộ quản lý chứng nhận cho phép 112 để tạo ra chứng nhận cho phép dựa trên thông tin được đưa ra trong yêu cầu 151. Sau khi chứng nhận cho phép đã được tạo ra, khi đó bộ quản lý chứng nhận cho phép 112 tìm khóa riêng chứng nhận cho phép liên kết với nhà sản xuất thiết bị 130 từ cơ sở dữ liệu 114 và sử dụng khóa riêng này để ký theo mật mã chứng nhận cho phép để tạo ra chứng nhận 153. Tiếp đó, máy chủ 110 cung cấp chứng nhận 153 cho người phát triển APK 105. Ở giai đoạn này, cần lưu ý rằng chứng nhận 153 bao gồm khóa chung phát triển của ứng dụng, tên của gói ứng dụng, sự cho phép và các sự cho phép được yêu cầu bởi ứng dụng, thời gian có hiệu lực của chứng nhận cho phép và chữ ký theo mật mã.

Tiếp đó, người phát triển APK 105 có thể sử dụng chứng nhận 153 để phát triển thêm ứng dụng. Khi người phát triển APK 105 sẵn sàng công bố ứng dụng, người phát triển APK 105 có thể gắn chứng nhận 153 vào APK 120 ở bước gắn 155 hoặc người phát triển APK 105 có thể tải chứng nhận 153 lên máy chủ ở xa nhờ đó chứng nhận 153 có thể được tải xuống ở giai đoạn sau.

Theo phương án nhờ đó chứng nhận 153 được gắn vào APK 120 ở bước 155, tiếp đó APK 120 có chứng nhận cho phép gắn vào 153 được công bố bằng cách sử dụng các phương pháp thông thường, ví dụ qua các kho ứng dụng trực tuyến khác nhau. Để bắt

đầu cài đặt APK 120 vào thiết bị 130, thiết bị 130 trước tiên sẽ phải đệ trình yêu cầu để tải xuống APK 120 vào thiết bị 130. Khi điều này được thực hiện, quy trình cài đặt APK 120 trong thiết bị 130 có thể bắt đầu. Khi bộ cài đặt gói ứng dụng 132 nhận yêu cầu cài đặt APK 120 ở bước 157, bộ cài đặt gói ứng dụng 132 sẽ sử dụng bộ quản lý gói ứng dụng 134 để kiểm tra nếu APK 120 chứa các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 120 sẽ gọi ra API đã bảo vệ bất kỳ trong quá trình chạy thực trong thiết bị 130. Nếu không có sự cho phép nguy cơ cao được yêu cầu hoặc nếu không có API đã bảo vệ sẽ được gọi ra trong quá trình chạy thực, bộ quản lý gói ứng dụng 134 sẽ tiến hành chấp thuận các sự cho phép yêu cầu với APK 120 bằng cách sử dụng bộ phận chuẩn của hệ điều hành, như bộ phận phục vụ quản lý gói ứng dụng.

Nếu APK 120 bao gồm các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 120 có gọi ra API đã bảo vệ trong quá trình chạy thực, do vậy bộ quản lý gói ứng dụng 134 sẽ thông báo cho bộ quản lý cấp quyền ứng dụng 136. Tiếp đó bộ quản lý cấp quyền 136 sẽ thực hiện một số kiểm tra về nội dung của APK 120 để xác định xem ứng dụng cần được làm phù hợp với sự cho phép yêu cầu hay không. Theo các phương án của sáng chế, việc kiểm tra liên quan đến việc bộ quản lý cấp quyền 136 trước tiên tìm khóa chung chứng nhận cho phép thuộc thiết bị 130 từ cơ sở dữ liệu 138. Khóa chung chứng nhận cho phép đã tìm là khóa duy nhất thuộc nhà sản xuất thiết bị 130 và khóa duy nhất này cũng được lưu trữ an toàn trong cơ sở dữ liệu 138. Tiếp đó, bộ quản lý cấp quyền 136 sẽ xác thực chứng nhận cho phép 153 bằng cách sử dụng khóa chung chứng nhận cho phép đã tìm của thiết bị 130. Nếu chứng nhận cho phép 153 được xác định là hợp lệ, khi đó bộ quản lý cấp quyền 136 sẽ cho phép bộ quản lý gói ứng dụng 134 tiến hành chấp thuận sự cho phép nguy cơ cao yêu cầu với APK 120. Việc chấp thuận sự cho phép nguy cơ cao yêu cầu có thể được thực hiện bằng cách sử dụng bộ phận chuẩn của hệ điều hành, như bộ phận phục vụ quản lý gói ứng dụng. Khi điều này được thực hiện, tiếp đó bộ cài đặt gói ứng dụng 132 có thể tiến hành cài đặt APK 120 vào thiết bị 130 dưới dạng bình thường. Theo một phương án khác của sáng chế, bộ quản lý cấp quyền 136 thực hiện việc kiểm tra xác thực để xác định xem sự cho phép nguy cơ cao hoặc các sự cho phép nguy cơ cao yêu cầu bởi APK 120 được chứa trong chứng nhận cho phép 153 hay không. Nếu bộ quản lý cấp quyền 136 xác định rằng chứng nhận cho phép 153 chứa sự cho phép hoặc các sự cho phép yêu cầu, chỉ khi đó bộ cài đặt gói ứng dụng 132 có thể tiến hành cài đặt APK 120 vào thiết bị 130.

Theo một phương án khác của sáng chế, nhờ đó chứng nhận 153 không được gắn vào APK ở bước 155, một phiên bản của APK không có chứng nhận cho phép 153, tức

là APK 121, được công bố bằng cách sử dụng các phương pháp thông thường, ví dụ qua các kho ứng dụng trực tuyến khác nhau. Tương tự, để bắt đầu cài đặt APK 121 vào thiết bị 130, thiết bị 130 trước tiên sẽ phải đệ trình yêu cầu để tải APK 121 vào thiết bị 130. Khi việc này được thực hiện, quy trình cài đặt APK 121 vào thiết bị 130 có thể bắt đầu. Khi bộ cài đặt gói ứng dụng 132 nhận yêu cầu cài đặt APK 121 ở bước 157, bộ cài đặt gói ứng dụng 132 trước tiên sẽ sử dụng bộ quản lý gói ứng dụng 134 để kiểm tra nếu APK 121 chứa các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 121 sẽ gọi ra API đã bảo vệ bất kỳ trong quá trình chạy thực trong thiết bị 130. Tương tự, nếu không có sự cho phép nguy cơ cao được yêu cầu hoặc nếu không có API đã bảo vệ sẽ được gọi ra trong quá trình chạy thực, bộ quản lý gói ứng dụng 134 sẽ tiến hành chấp thuận sự cho phép yêu cầu với APK 121 bằng cách sử dụng cơ chế mặc định.

Trái lại, nếu APK 121 bao gồm các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 121 liên quan đến việc gọi ra API đã bảo vệ trong quá trình chạy thực, do vậy bộ quản lý gói ứng dụng 134 sẽ thông báo cho bộ quản lý cấp quyền ứng dụng 136. Trước khi bộ quản lý cấp quyền 136 tính chữ ký theo mật mã riêng của APK 121 bằng cách sử dụng khóa riêng chứng nhận cho phép đã tìm của thiết bị 130, bộ quản lý cấp quyền 136 trước tiên sẽ thiết lập kết nối đảm bảo với máy chủ mà chứa chứng nhận cho phép liên kết với APK 121, tức là chứng nhận 153. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng kết nối đảm bảo này có thể bao gồm kết nối có dây hoặc không dây và rằng dữ liệu truyền có thể được mã hóa bằng cách sử dụng các sơ đồ mã hóa khác nhau đã biết trong lĩnh vực kỹ thuật này. Khi kết nối đảm bảo đã được thiết lập, khi đó bộ quản lý cấp quyền 136 sẽ tải xuống và lưu trữ chứng nhận 153 trong cơ sở dữ liệu 138. Nếu việc tải xuống và lưu trữ chứng nhận 153 thành công, khi đó bộ quản lý cấp quyền 135 sẽ tiến hành thực hiện một số kiểm tra bằng cách sử dụng nội dung trong chứng nhận 153 để xác định xem ứng dụng cần được làm phù hợp với sự cho phép yêu cầu hay không. Các sự kiểm tra có thể được thực hiện là như được mô tả ở trên.

Fig.2 thể hiện sơ đồ khối của hệ thống quản lý việc cài đặt APK 120 hoặc APK 121 vào thiết bị 130 nhờ đó chứng nhận cho phép phát triển được cấp trước khi cấp chứng nhận cho phép theo một phương án khác của sáng chế.

Hệ thống thể hiện trên Fig.2 hoạt động theo cách sau. Người phát triển APK 105 bắt đầu quy trình chấp thuận chứng nhận cho phép bằng cách trước tiên đệ trình yêu cầu 251 với máy chủ 110. Yêu cầu 251 cũng sẽ chứa thông tin như khóa chung phát triển của ứng dụng, tên của gói ứng dụng, sự cho phép và các sự cho phép được yêu cầu bởi ứng dụng, và danh sách nhận dạng thiết bị. Các sự cho phép chứa trong yêu cầu 151 có

thể bao gồm sự cho phép loại bình thường, nguy hại, chữ ký và/hoặc chữ ký/hệ thống và danh sách nhận dạng thiết bị thiết lập các thiết bị mà chứng nhận cho phép có thể được sử dụng với chúng.

Khi nhận yêu cầu 251, máy chủ 110 sẽ phân tích các nội dung của yêu cầu 251 và dựa trên các nội dung của yêu cầu 251, xác định xem chứng nhận cho phép phát triển cần được cấp cho người phát triển APK 105 hay không. Nếu máy chủ 110 xác định rằng chứng nhận cho phép phát triển cần được cấp cho người phát triển APK 105, máy chủ 110 sử dụng bộ quản lý chứng nhận cho phép 112 để tạo ra chứng nhận cho phép phát triển dựa trên thông tin có trong yêu cầu 251. Sau khi chứng nhận cho phép phát triển đã được tạo ra, khi đó bộ quản lý chứng nhận cho phép 112 tìm khóa riêng chứng nhận cho phép liên kết với nhà sản xuất thiết bị 130 từ cơ sở dữ liệu 114 và sử dụng khóa riêng này để ký theo mật mã chứng nhận cho phép phát triển để tạo ra chứng nhận 252. Tiếp đó, máy chủ 110 cung cấp chứng nhận 252 cho người phát triển APK 105. Ở giai đoạn này, cần lưu ý rằng chứng nhận 252 bao gồm khóa chung phát triển của ứng dụng, tên của gói ứng dụng, sự cho phép và các sự cho phép được yêu cầu bởi ứng dụng, thời gian có hiệu lực của chứng nhận cho phép, danh sách nhận dạng thiết bị và chữ ký theo mật mã.

Tiếp đó, người phát triển APK 105 có thể sử dụng chứng nhận 252 để phát triển thêm ứng dụng. Trong quá trình phát triển ứng dụng, chứng nhận 252 có thể được gắn vào APK phát triển để tạo ra APK sửa lỗi 202. Tiếp đó, APK sửa lỗi 202 có thể được cài đặt trong thiết bị sửa lỗi 204. Thiết bị sửa lỗi 204 là công cụ phát triển mà được triển khai bởi người phát triển ứng dụng để thử nghiệm việc cài đặt APK sửa lỗi 202 và công cụ này có các chức năng giống như thiết bị 130. Trong quy trình cài đặt APK sửa lỗi 202 vào thiết bị sửa lỗi 204, thiết bị sửa lỗi 204 sẽ thực hiện một số bước xác nhận và kiểm tra để đảm bảo rằng chứng nhận 252 thực hiện chức năng như yêu cầu để chứng nhận 252 có thể được sử dụng một cách thích hợp cho việc xác nhận cài đặt APK. Cần lưu ý rằng APK sửa lỗi 202 có thể chỉ được cài đặt vào các thiết bị mà được thiết lập trong danh sách nhận dạng thiết bị nhờ đó danh sách nhận dạng thiết bị này được chứa trong chứng nhận 252. Nói cách khác, thiết bị sửa lỗi 204 phải được chứa trong danh sách nhận dạng thiết bị để APK sửa lỗi 202 có thể được cài đặt trong thiết bị sửa lỗi 204.

Sau khi người phát triển APK 105 đã hoàn tất sự phát triển ứng dụng, người phát triển APK 105 sẽ đệ trình APK sửa lỗi 202 với máy chủ 110 để kiểm tra. Máy chủ 110 sẽ kiểm tra APK sửa lỗi 202 đối với tác động có hại hoặc tác động không mong muốn

và nếu máy chủ 110 được đảm bảo rằng APK sửa lỗi là an toàn và phù hợp với yêu cầu của nhà sản xuất thiết bị 130, khi đó máy chủ 110 sẽ sử dụng bộ quản lý chứng nhận cho phép 112 để tạo ra chứng nhận cho phép phiên bản đối với APK sửa lỗi 202. Khi tạo ra chứng nhận cho phép phiên bản, bộ quản lý chứng nhận cho phép 112 sẽ tìm khóa riêng chứng nhận cho phép liên kết với nhà sản xuất thiết bị 130 từ cơ sở dữ liệu 114 và sau đó sẽ sử dụng khóa riêng này để ký theo mật mã chứng nhận cho phép phiên bản để tạo ra chứng nhận 260.

Theo các phương án của sáng chế, băm mật mã của một hoặc nhiều tệp trong APK sửa lỗi 202 được chứa trong chứng nhận 260. Ví dụ, băm mật mã của tệp "META-INF/MANIFEST.MF" trong APK sửa lỗi 202 được chứa trong chứng nhận 260. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng băm của các tệp khác cũng có thể được thực hiện mà không nằm ngoài phạm vi của sáng chế. Mục đích tạo ra băm của nội dung từ APK sửa lỗi 202 là đảm bảo rằng chứng nhận đã cấp được gắn chặt với APK sửa lỗi 202 và như vậy không thể được đưa theo cách có hại vào các gói ứng dụng khác.

Tiếp đó, máy chủ 110 cung cấp chứng nhận 260 đến người phát triển APK 105. Ở giai đoạn này, cần lưu ý rằng chứng nhận 260 bao gồm khóa chung phát triển của ứng dụng, tên của gói ứng dụng, sự cho phép và các sự cho phép được yêu cầu bởi ứng dụng, thời gian có hiệu lực của chứng nhận cho phép, băm mật mã của nội dung của gói ứng dụng và chữ ký theo mật mã.

Khi người phát triển APK 105 sẵn sàng công bố ứng dụng, người phát triển APK 105 có thể gắn chứng nhận 260 vào APK 120 ở bước gắn 265 hoặc người phát triển APK 105 có thể tải lên chứng nhận 260 vào máy chủ ở xa nhờ đó chứng nhận 260 có thể được tải xuống bởi thiết bị 130 ở giai đoạn sau.

Theo phương án nhờ đó chứng nhận 260 được gắn vào APK 120 ở bước 265, APK 120 với chứng nhận cho phép 260 đã gắn được công bố bằng cách sử dụng các phương pháp thông thường. Để bắt đầu cài đặt APK 120 vào thiết bị 130, thiết bị 130 trước tiên sẽ phải đệ trình yêu cầu tải APK 120 vào thiết bị 130. Khi việc này được thực hiện, quy trình cài đặt APK 120 trong thiết bị 130 có thể bắt đầu. Như đã mô tả ở trên, khi bộ cài đặt gói ứng dụng 132 nhận yêu cầu cài đặt APK 120 ở bước 157, bộ cài đặt gói ứng dụng 132 sẽ sử dụng bộ quản lý gói ứng dụng 134 để kiểm tra nếu APK 120 chứa các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 120 sẽ gọi ra API đã bảo vệ bất kỳ trong quá trình chạy thực trong thiết bị 130. Nếu APK 120 bao gồm các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 120 liên quan đến việc gọi ra

API đã bảo vệ trong quá trình chạy thực, do vậy bộ quản lý gói ứng dụng 134 sẽ thông báo cho bộ quản lý cấp quyền ứng dụng 136. Tiếp đó, bộ quản lý cấp quyền 135 sẽ thực hiện một số kiểm tra về nội dung của APK 120 để xác định xem ứng dụng cần được làm phù hợp với sự cho phép yêu cầu hay không.

Theo các phương án của sáng chế, việc kiểm tra liên quan đến việc bộ quản lý cấp quyền 136 trước tiên tìm khóa chung chứng nhận cho phép thuộc thiết bị 130 từ cơ sở dữ liệu 138. Tiếp đó, bộ quản lý cấp quyền 136 sẽ xác thực chứng nhận cho phép 260 bằng cách sử dụng khóa chung chứng nhận cho phép đã tìm của thiết bị 130. Nếu chứng nhận cho phép 260 được xác định là hợp lệ, khi đó bộ quản lý cấp quyền 136 sẽ cho phép bộ quản lý gói ứng dụng 134 tiến hành chấp thuận sự cho phép nguy cơ cao yêu cầu với APK 120. Theo một phương án khác của sáng chế, bộ quản lý cấp quyền 136 thực hiện việc kiểm tra xác thực để xác định xem sự cho phép nguy cơ cao hoặc các sự cho phép nguy cơ cao yêu cầu bởi APK 120 được chứa trong chứng nhận cho phép 260 hay không. Nếu bộ quản lý cấp quyền 136 xác định rằng chứng nhận cho phép 260 chứa sự cho phép hoặc các sự cho phép yêu cầu, chỉ khi đó bộ cài đặt gói ứng dụng 132 có thể tiến hành cài đặt APK 120 vào thiết bị 130.

Theo phương án khác của sáng chế, bộ quản lý cấp quyền 136 sẽ tính băm mật mã của nội dung của APK 120 để tạo ra kết quả băm. Tiếp đó, kết quả băm như được tính bởi bộ quản lý cấp quyền 136 được so sánh với kết quả băm của APK 120 như được chứa trong chứng nhận cho phép 260. Nếu kết quả băm của APK 120 như được tính bởi bộ quản lý cấp quyền 136 phù hợp với kết quả băm của APK 120 như được chứa trong chứng nhận cho phép 260, điều này nghĩa là chứng nhận cho phép 260 được xác định là hợp lệ và tiếp đó bộ quản lý cấp quyền 136 sẽ cho phép bộ quản lý gói ứng dụng 134 tiến hành chấp thuận sự cho phép nguy cơ cao yêu cầu với APK 120. Khi các sự cho phép yêu cầu đã được chấp thuận, bộ cài đặt gói ứng dụng 132 có thể tiến hành cài đặt APK 120 vào thiết bị 130 dưới dạng bình thường.

Theo một phương án khác của sáng chế, nhờ đó chứng nhận 260 không được gắn vào APK ở bước 265, phiên bản của APK không có chứng nhận cho phép 260, tức là APK 121, được công bố bằng cách sử dụng các phương pháp thông thường. Tương tự, để bắt đầu cài đặt APK 121 vào thiết bị 130, trước tiên thiết bị 130 sẽ phải đệ trình yêu cầu tải APK 121 vào thiết bị 130. Khi việc này được thực hiện, quy trình cài đặt APK 121 vào thiết bị 130 có thể bắt đầu. Khi bộ cài đặt gói ứng dụng 132 nhận yêu cầu cài đặt APK 121 ở bước 157, bộ cài đặt gói ứng dụng 132 trước tiên sẽ sử dụng bộ quản lý gói ứng dụng 134 để kiểm tra nếu APK 121 chứa các yêu cầu đối với sự cho phép nguy

cơ cao hoặc nếu APK 121 sẽ gọi ra API đã bảo vệ bất kỳ trong quá trình chạy thực trong thiết bị 130.

Nếu APK 121 bao gồm các yêu cầu đối với sự cho phép nguy cơ cao hoặc nếu APK 121 liên quan đến việc gọi ra API đã bảo vệ trong quá trình chạy thực, do vậy bộ quản lý gói ứng dụng 134 sẽ thông báo cho bộ quản lý cấp quyền ứng dụng 136. Trước tiên bộ quản lý cấp quyền 136 sẽ thiết lập kết nối đảm bảo với máy chủ mà chứa chứng nhận cho phép liên kết với APK 121, tức là chứng nhận 260, để tải xuống và lưu trữ chứng nhận 260 trong cơ sở dữ liệu 138. Nếu việc tải xuống và lưu trữ chứng nhận 260 thành công, khi đó bộ quản lý cấp quyền 135 sẽ tiến hành thực hiện một số kiểm tra bằng cách sử dụng nội dung trong chứng nhận 260 để xác định xem ứng dụng cần được làm phù hợp với sự cho phép yêu cầu hay không.

Theo các phương án của sáng chế, việc kiểm tra liên quan đến việc bộ quản lý cấp quyền 136 trước tiên tìm khóa chung chứng nhận cho phép thuộc thiết bị 130 từ cơ sở dữ liệu 138. Tiếp đó, bộ quản lý cấp quyền 136 sẽ xác thực chứng nhận cho phép 260 bằng cách sử dụng khóa chung chứng nhận cho phép đã tìm của thiết bị 130. Nếu chứng nhận cho phép 260 được xác định là hợp lệ, khi đó bộ quản lý cấp quyền 136 sẽ cho phép bộ quản lý gói ứng dụng 134 tiến hành chấp thuận sự cho phép nguy cơ cao yêu cầu với APK 121. Việc chấp thuận sự cho phép nguy cơ cao yêu cầu có thể được tiến hành bằng cách sử dụng các cơ chế mặc định và khi đó bộ cài đặt gói ứng dụng 132 có thể tiến hành cài đặt APK 121 vào thiết bị 130.

Theo một phương án khác của sáng chế, bộ quản lý cấp quyền 136 sẽ tính băm của nội dung của APK 121 để tạo ra kết quả băm. Tiếp đó, kết quả băm như tính bởi bộ quản lý cấp quyền 136 được so sánh với kết quả băm của APK 121 như được chứa trong chứng nhận cho phép 260. Nếu kết quả băm của APK 121 như được tính bởi bộ quản lý cấp quyền 136 phù hợp với kết quả băm của APK 121 như được chứa trong chứng nhận cho phép 260, điều này nghĩa là chứng nhận cho phép 260 được xác định là hợp lệ và bộ quản lý cấp quyền 136 sẽ cho phép bộ quản lý gói ứng dụng 134 tiến hành chấp thuận sự cho phép nguy cơ cao yêu cầu với APK 121. Khi sự cho phép yêu cầu đã được chấp thuận, bộ cài đặt gói ứng dụng 132 có thể tiến hành cài đặt APK 121 vào thiết bị 130.

Theo một phương án của sáng chế, phương pháp quản lý việc cài đặt gói ứng dụng (APK) vào thiết bị trong đó APK gọi ra API đã bảo vệ trong quá trình chạy thực bao gồm bốn bước sau:

- nhận, bởi thiết bị, yêu cầu cài đặt đối với APK;

- tìm, bởi thiết bị, chứng nhận cho phép đối với APK theo yêu cầu cài đặt, trong đó chứng nhận cho phép đối với APK bao gồm chữ ký theo mật mã;

- xác định, bởi thiết bị, tính hợp lệ của chứng nhận cho phép bằng cách xác thực chữ ký theo mật mã chứa trong chứng nhận cho phép bằng cách sử dụng khóa chung chứng nhận cho phép của nhà sản xuất thiết bị, trong đó khóa chung chứng nhận cho phép được lưu trữ trong thiết bị; và

- cho phép cài đặt APK vào thiết bị nếu chứng nhận cho phép được xác định là hợp lệ.

Để tạo ra hệ thống hoặc phương pháp như vậy thì cần có quy trình quản lý việc cài đặt gói ứng dụng Android (APK) vào thiết bị nhờ đó APK yêu cầu sự cho phép nguy cơ cao cần được chấp thuận trong quy trình cài đặt. Phần mô tả dưới đây và các hình vẽ từ Fig.3 đến Fig.5 mô tả các phương án của các quy trình theo sáng chế.

Fig.3 thể hiện quy trình 300 được thực hiện bởi các môđun trong thiết bị để quản lý việc cài đặt gói ứng dụng Android (APK) vào thiết bị theo các phương án của sáng chế. Quy trình 300 bắt đầu ở bước 305 bằng cách tìm gói cài đặt từ APK. Tiếp đó, quy trình 300 tiến hành tìm chứng nhận cho phép đối với APK ở bước 310. Nếu chứng nhận cho phép được gắn trong APK, quy trình 300 sẽ được tách chứng nhận cho phép ra khỏi APK, nếu chứng nhận cho phép được lưu trữ trong máy chủ ở xa, quy trình 300 sẽ tải xuống chứng nhận cho phép từ máy chủ ở xa và lưu trữ chứng nhận cho phép đã tải vào thiết bị. Tiếp đó, quy trình 300 tiến hành kiểm tra tính hợp lệ của chứng nhận ở bước 315. Theo một phương án của sáng chế, quy trình 300 có thể kiểm tra tính hợp lệ của chứng nhận cho phép bằng cách xác thực chữ ký theo mật mã được lưu trữ trong chứng nhận cho phép bằng khóa chung chứng nhận cho phép của nhà sản xuất thiết bị. Theo một phương án khác của sáng chế, quy trình 300 có thể kiểm tra tính hợp lệ của chứng nhận cho phép bằng cách tính băm mật mã của APK và so khớp băm mật mã đã tính của APK với băm mật mã được lưu trữ trong chứng nhận cho phép. Trong cả hai phương án, nếu quy trình 300 xác định rằng có sự phù hợp, chứng nhận cho phép sẽ được xử lý bằng quy trình 300 dưới dạng hợp thức.

Nếu quy trình 300 xác định rằng chứng nhận là hợp thức, khi đó quy trình 300 tiến hành bước 320. Ở bước 320, quy trình 300 tiến hành chấp thuận sự cho phép nguy cơ cao yêu cầu với APK và tiếp đó tiến hành cài đặt APK vào thiết bị. Theo cách khác, nếu quy trình 300 xác định ở bước 315 rằng chứng nhận không hợp lệ, quy trình 300 chấm dứt quá trình cài đặt và kết thúc.

Fig.4 thể hiện quy trình 400 được thực hiện bởi các môđun trong máy chủ liên kết với hệ thống máy tính của nhà sản xuất thiết bị để cấp chứng nhận cho phép đối với APK. Quy trình 400 bắt đầu ở bước 405 khi máy chủ nhận yêu cầu từ người phát triển APK đối với việc cấp chứng nhận cho phép. Được chứa trong yêu cầu sẽ là khóa chung phát triển của ứng dụng, tên gói ứng dụng và các sự cho phép mà yêu cầu bởi ứng dụng. Tiếp đó, quy trình 400 sẽ đánh giá yêu cầu đã nhận và sẽ xác định ở bước 410 xem chứng nhận cho phép cần được cấp hay không. Nếu quy trình 400 xác định rằng yêu cầu cần được từ chối và chứng nhận cho phép cần không được cấp, quy trình 400 tiến hành bước 425 nhờ đó yêu cầu được từ chối và quy trình 400 kết thúc. Theo cách khác, nếu quy trình 400 xác định ở bước 410 rằng chứng nhận cho phép cần được cấp, quy trình 400 tiến hành bước 415. Ở bước 415, chứng nhận cho phép sẽ được ký theo mật mã bằng cách sử dụng khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị. Chứng nhận cho phép đã ký theo mật mã mà chứa khóa chung phát triển của ứng dụng, tên gói ứng dụng, các sự cho phép mà được yêu cầu bởi ứng dụng và chữ ký theo mật mã khi đó sẽ được cấp bởi quy trình 400 ở bước 420. Khi đó, quy trình 400 kết thúc.

Fig.5 thể hiện quy trình 500 được thực hiện bởi các môđun trong máy chủ liên kết với hệ thống máy tính của nhà sản xuất thiết bị để cấp chứng nhận cho phép đối với APK nhờ đó chứng nhận cho phép phát triển được cấp bởi quy trình 500 trước khi cấp chứng nhận cho phép phiên bản. Quy trình 500 bắt đầu ở bước 505 khi máy chủ nhận yêu cầu từ người phát triển APK để cấp chứng nhận cho phép phát triển. Được chứa trong yêu cầu sẽ là khóa chung phát triển của ứng dụng, tên gói ứng dụng, danh sách nhận dạng thiết bị sử dụng trong giai đoạn phát triển và các sự cho phép mà được yêu cầu bởi ứng dụng. Tiếp đó, quy trình 500 sẽ đánh giá yêu cầu đã nhận và sẽ xác định ở bước 510 xem chứng nhận cho phép phát triển cần được cấp hay không. Nếu quy trình 500 xác định rằng yêu cầu cần được từ chối và chứng nhận cho phép phát triển không cần được cấp, quy trình 500 tiến hành bước 545 nhờ đó yêu cầu được từ chối và quy trình 500 kết thúc.

Theo cách khác, nếu quy trình 500 xác định ở bước 510 rằng chứng nhận cho phép phát triển cần được cấp, quy trình 500 tiến hành bước 515. Ở bước 515, chứng nhận cho phép phát triển sẽ được ký theo mật mã bằng cách sử dụng khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị. Giờ đây chứng nhận cho phép đã ký theo mật mã phát triển chứa khóa chung phát triển của ứng dụng, tên gói ứng dụng, các sự cho phép mà được yêu cầu bởi ứng dụng, danh sách nhận dạng thiết bị mà sẽ được sử dụng

để phát triển ứng dụng và tiếp đó chữ ký theo mật mã sẽ được cấp bởi quy trình 500 ở bước 520. Tiếp đó, quy trình 500 nhận APK phát hành trước cùng với yêu cầu đối với chứng nhận cho phép, hoặc chứng nhận cho phép thông thường ở bước 525. APK phát hành trước là APK cuối mà được tạo ra bởi người phát triển ứng dụng sau khi người phát triển APK đã hoàn tất thử nghiệm và sửa lỗi APK bằng cách sử dụng chứng nhận cho phép phát triển.

Tiếp đó, quy trình 500 sẽ đánh giá yêu cầu đã nhận và kiểm tra APK phát hành trước ở bước 530. Nếu quy trình 500 xác định ở bước 530 rằng yêu cầu cần được từ chối và chứng nhận cho phép không cần được cấp, quy trình 500 tiến hành bước 550 nhờ đó yêu cầu được từ chối và quy trình 500 kết thúc. Theo cách khác, nếu quy trình 500 xác định ở bước 530 rằng chứng nhận cho phép cần được cấp, quy trình 500 tiến hành bước 535. Ở bước 535, chứng nhận cho phép đã cấp sẽ được ký theo mật mã bằng cách sử dụng khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị. Giờ đây chứng nhận cho phép đã ký theo mật mã chứa khóa chung phát triển của ứng dụng, tên gói ứng dụng, các sự cho phép mà được yêu cầu bởi ứng dụng, băm mật mã của nội dung của APK và tiếp đó chữ ký theo mật mã sẽ được cấp bởi quy trình 500 ở bước 540. Tiếp đó, quy trình 500 kết thúc.

Các quy trình thực hiện bởi các lệnh được lưu trữ trong phương tiện có thể đọc bằng máy tính chuyển tiếp được thực hiện bởi bộ phận xử lý trong hệ thống máy tính. Để tránh phức tạp, phương tiện có thể đọc bằng máy tính chuyển tiếp cần được xem là bao gồm tất cả các phương tiện đọc được bằng máy tính ngoại trừ tín hiệu truyền tạm thời. Hệ thống máy tính có thể được bố trí trong một hoặc nhiều thiết bị di động và/hoặc máy chủ máy tính để thực hiện sáng chế. Các lệnh có thể được lưu trữ dưới dạng phần sụn, phần cứng hoặc phần mềm. Fig.6 thể hiện một ví dụ về hệ thống xử lý như vậy. Hệ thống xử lý 600 có thể là hệ thống xử lý trong thiết bị di động mà thực thi các lệnh để thực hiện các quy trình để tạo ra phương pháp và/hoặc hệ thống theo các phương án của sáng chế. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng cấu hình chính xác của mỗi hệ thống xử lý có thể là khác nhau và cấu hình chính xác của hệ thống xử lý trong mỗi thiết bị di động có thể thay đổi và Fig.6 được đưa ra chỉ để làm ví dụ.

Hệ thống xử lý 600 bao gồm bộ xử lý trung tâm (CPU) 605. CPU 605 là bộ xử lý, bộ vi xử lý, hoặc tổ hợp bất kỳ của các bộ xử lý và các bộ vi xử lý mà thực thi các lệnh để thực hiện các quy trình theo sáng chế. CPU 605 nối với buýt bộ nhớ 610 và buýt

nhập/xuất (I/O) 615. Buýt bộ nhớ 610 nối CPU 605 với các bộ nhớ 620 và 625 để truyền dữ liệu và các lệnh giữa các bộ nhớ 620, 625 và CPU 605. Buýt I/O 615 nối CPU 1105 với các thiết bị ngoại vi để truyền dữ liệu giữa CPU 605 và các thiết bị ngoại vi. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng buýt I/O 615 và buýt bộ nhớ 610 có thể được kết hợp thành một buýt hoặc được chia thành nhiều buýt khác và cấu hình chính xác được tạo ra bởi người có hiểu biết trung bình về lĩnh vực này.

Bộ nhớ không khả biến 620, như bộ nhớ chỉ đọc (Read Only Memory - ROM), được nối với buýt bộ nhớ 610. Bộ nhớ không khả biến 620 lưu trữ các lệnh và dữ liệu cần thiết để vận hành các hệ con khác nhau của hệ thống xử lý 600 và để khởi động hệ thống khi bắt đầu. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng số loại bộ nhớ bất kỳ có thể được sử dụng để thực hiện chức năng này.

Bộ nhớ khả biến 625, như bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM), cũng được nối với buýt bộ nhớ 610. Bộ nhớ khả biến 625 lưu trữ các lệnh và dữ liệu cần thiết bởi CPU 605 để thực hiện các lệnh phần mềm cho các quy trình như các quy trình cần thiết để tạo ra hệ thống theo các phương án của sáng chế. Người có hiểu biết trung bình về lĩnh vực này sẽ nhận thấy rằng số loại bộ nhớ bất kỳ có thể được sử dụng làm bộ nhớ khả biến và loại chính xác được lựa chọn bởi người có hiểu biết trung bình về lĩnh vực này.

Thiết bị I/O 630, bàn phím 635, màn hình 640, bộ nhớ 645, thiết bị mạng 650 và số lượng bất kỳ các thiết bị ngoại vi khác nối với buýt I/O 615 để trao đổi dữ liệu với CPU 605 để sử dụng trong các ứng dụng đang được thực hiện bởi CPU 605. Thiết bị I/O 630 là thiết bị bất kỳ mà truyền và/hoặc nhận dữ liệu từ CPU 605. Bàn phím 635 là loại I/O đặc trưng mà nhận dữ liệu vào của người sử dụng và truyền dữ liệu vào đến CPU 605. Màn hình 640 nhận dữ liệu màn hình từ CPU 605 và hình ảnh hiển thị trên màn hình để người sử dụng nhìn thấy. Bộ nhớ 645 là thiết bị mà truyền và nhận dữ liệu đến và ra khỏi CPU 605 để lưu trữ dữ liệu vào phương tiện. Thiết bị mạng 650 nối CPU 605 với mạng lưới để truyền dữ liệu đến và ra khỏi các hệ thống xử lý khác.

Trên đây là phần mô tả các phương án về hệ thống và quy trình theo sáng chế như nêu trong yêu cầu bảo hộ dưới đây. Các cải biến và thay đổi khác có thể được thực hiện với các phương án này và chúng đều nằm trong phạm vi của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp quản lý việc cài đặt gói ứng dụng Android (APK) vào thiết bị di động bao gồm các bước sau đây:

nhận, bởi thiết bị, yêu cầu cài đặt để cài đặt gói ứng dụng Android (APK) trong thiết bị;

tìm, bởi thiết bị, chứng nhận cho phép đối với gói ứng dụng Android (APK) theo yêu cầu cài đặt, trong đó chứng nhận cho phép đối với gói ứng dụng Android (APK) bao gồm chữ ký theo mật mã;

xác thực, bởi thiết bị, chữ ký theo mật mã sử dụng khóa chung chứng nhận cho phép của nhà sản xuất thiết bị để xác định tính hợp lệ của giấy chứng nhận cho phép, trong đó khóa chung chứng nhận cho phép được lưu trữ trong thiết bị và trong đó chứng nhận cho phép hợp lệ chỉ ra rằng nhà sản xuất thiết bị cho phép cài đặt gói ứng dụng Android (APK) trong thiết bị này; và

cho phép cài đặt gói ứng dụng Android (APK) vào thiết bị khi chứng nhận cho phép được xác định là hợp lệ,

trong đó bước xác thực chữ ký theo mật mã để xác định tính hợp lệ của giấy chứng nhận cho phép bao gồm các bước nhỏ:

tính toán băm mật mã của gói ứng dụng Android (APK) bằng cách sử dụng hàm băm mật mã; và

so sánh băm mật mã đã tính toán của gói ứng dụng Android (APK) với băm mật mã của gói ứng dụng Android (APK) được lưu trữ trong chứng nhận cho phép.

2. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm bước:

trước khi cho phép cài đặt gói ứng dụng Android (APK) trong thiết bị khi giấy chứng nhận cho phép được xác định là hợp lệ, xác định, bằng thiết bị, xem yêu cầu cho phép chứa trong yêu cầu cài đặt tương ứng với sự cho phép được chấp thuận trong chứng nhận cho phép đối với gói ứng dụng Android (APK) hay không; và

duyệt, bởi thiết bị, chứng nhận cho phép khi xác định rằng yêu cầu cho phép chứa trong yêu cầu cài đặt tương ứng với sự cho phép được chấp thuận trong chứng nhận cho phép.

3. Phương pháp theo điểm 1, trong đó chữ ký theo mật mã được tạo ra ở máy chủ liên kết với nhà sản xuất thiết bị khi khóa riêng chứng nhận cho phép của nhà sản xuất thiết

bị được sử dụng để ký theo mật mã chứng nhận cho phép đối với gói ứng dụng Android (APK).

4. Phương pháp theo điểm 3, trong đó chứng nhận cho phép đã ký theo mật mã đối với gói ứng dụng Android (APK) bao gồm khóa chung phát triển của gói ứng dụng Android (APK), tên của gói ứng dụng Android (APK); một lần cho phép hoặc các lần cho phép được chấp thuận với gói ứng dụng Android (APK), và thời gian có hiệu lực của chứng nhận cho phép.

5. Phương pháp theo điểm 3, trong đó chứng nhận cho phép đối với gói ứng dụng Android (APK) được ký theo mật mã sau khi máy chủ nhận gói ứng dụng Android (APK) phát hành trước chứa chứng nhận cho phép phát triển mà đã được ký theo mật mã bằng cách sử dụng khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị, và

trong đó chứng nhận cho phép phát triển cho phép gói ứng dụng Android (APK) phát hành trước được cài đặt vào thiết bị phát triển định trước.

6. Phương pháp theo điểm 1, trong đó bước tìm chứng nhận cho phép đối với gói ứng dụng Android (APK) bao gồm bước tách chứng nhận cho phép ra khỏi gói ứng dụng Android (APK).

7. Phương pháp theo điểm 1, trong đó bước tìm chứng nhận cho phép đối với gói ứng dụng Android (APK) bao gồm bước tải chứng nhận cho phép từ máy chủ vào thiết bị.

8. Phương pháp theo điểm 1, trong đó gói ứng dụng Android (APK) là gói ứng dụng Android™.

9. Thiết bị di động bao gồm:

bộ phận xử lý; và

môi trường chuyển tiếp lưu trữ các lệnh đọc được bởi bộ phận xử lý, trong đó các lệnh này khi được thực thi bởi bộ phận xử lý làm cho thiết bị:

nhận yêu cầu cài đặt để cài đặt gói ứng dụng Android (APK) trong thiết bị;

tìm chứng nhận cho phép đối với gói ứng dụng Android (APK) theo yêu cầu cài đặt, trong đó chứng nhận cho phép đối với gói ứng dụng Android (APK) bao gồm chữ ký theo mật mã;

xác thực chữ ký theo mật mã sử dụng khóa chung chứng nhận cho phép của nhà sản xuất thiết bị để xác định tính hợp lệ của giấy chứng nhận cho phép, trong đó khóa

chung chứng nhận cho phép được lưu trữ trong thiết bị và trong đó chứng nhận cho phép hợp lệ chỉ ra rằng nhà sản xuất thiết bị cho phép cài đặt gói ứng dụng Android (APK) trong thiết bị này; và

cho phép cài đặt gói ứng dụng Android (APK) vào thiết bị khi chứng nhận cho phép được xác định là hợp lệ,

trong đó trong bước xác thực chữ ký theo mật mã để xác định tính hợp lệ của giấy chứng nhận cho phép, các lệnh làm cho thiết bị:

tính toán băm mật mã của gói ứng dụng Android (APK) bằng cách sử dụng hàm băm mật mã; và

so sánh băm mật mã đã tính toán của gói ứng dụng Android (APK) với băm mật mã của gói ứng dụng Android (APK) được lưu trữ trong chứng nhận cho phép.

10. Thiết bị theo điểm 9, trong đó khi được thực thi bởi bộ xử lý, còn làm cho thiết bị:

trước khi cho phép cài đặt gói ứng dụng Android (APK) trong thiết bị khi giấy chứng nhận cho phép được xác định là hợp lệ, xác định, bằng thiết bị, xem yêu cầu cho phép chứa trong yêu cầu cài đặt tương ứng với sự cho phép được chấp thuận trong chứng nhận cho phép đối với gói ứng dụng Android (APK) hay không; và

duyệt, bởi thiết bị, chứng nhận cho phép khi xác định rằng yêu cầu cho phép chứa trong yêu cầu cài đặt tương ứng với sự cho phép được chấp thuận trong chứng nhận cho phép.

11. Thiết bị theo điểm 9, trong đó chữ ký theo mật mã chứa trong chứng nhận cho phép được tạo ra ở máy chủ liên kết với nhà sản xuất thiết bị khi khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị được sử dụng để ký theo mật mã chứng nhận cho phép đối với gói ứng dụng Android (APK).

12. Thiết bị theo điểm 11, trong đó chứng nhận cho phép đã ký theo mật mã đối với gói ứng dụng Android (APK) bao gồm khóa chung phát triển của gói ứng dụng Android (APK), tên của gói ứng dụng Android (APK); một lần cho phép hoặc các lần cho phép được chấp thuận với gói ứng dụng Android (APK), và thời gian có hiệu lực của chứng nhận cho phép.

13. Thiết bị theo điểm 11, trong đó chứng nhận cho phép đối với gói ứng dụng Android (APK) được ký theo mật mã sau khi máy chủ nhận gói ứng dụng Android (APK) phát

hành trước chứa chứng nhận cho phép phát triển mà đã được ký theo mật mã bằng cách sử dụng khóa riêng chứng nhận cho phép của nhà sản xuất thiết bị, và

trong đó chứng nhận cho phép phát triển cho phép gói ứng dụng Android (APK) phát hành trước được cài đặt vào thiết bị phát triển định trước.

14. Thiết bị theo điểm 9, trong đó các lệnh để tìm chứng nhận cho phép đối với gói ứng dụng Android (APK) bao gồm các lệnh để tách chứng nhận cho phép ra khỏi gói ứng dụng Android (APK).

15. Thiết bị theo điểm 9, trong đó các lệnh để tìm chứng nhận cho phép đối với gói ứng dụng Android (APK) bao gồm bước tải chứng nhận cho phép từ máy chủ vào thiết bị.

16. Thiết bị theo điểm 9, trong đó gói ứng dụng Android (APK) là gói ứng dụng Android™.

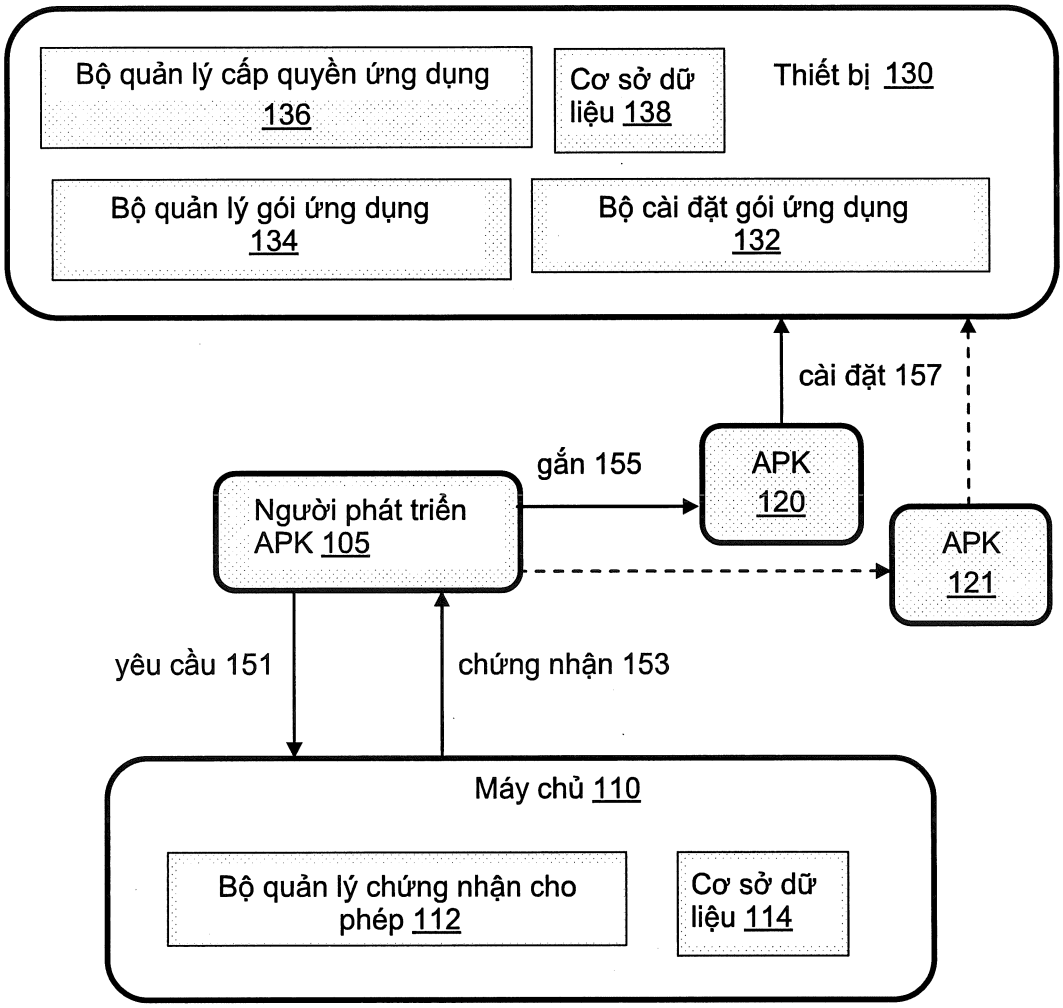

Bộ quản lý cấp quyền ứng dụng 136
Cơ sở dữ liệu 138
Thiết bị 130
Bộ quản lý gói ứng dụng 134
Bộ cài đặt gói ứng dụng 132
cài đặt 157
gắn 155
APK 120
Người phát triển APK 105
APK 121
yêu cầu 151
chứng nhận 153
Máy chủ 110
Bộ quản lý chứng nhận cho phép 112
Cơ sở dữ liệu 114

Fig.1

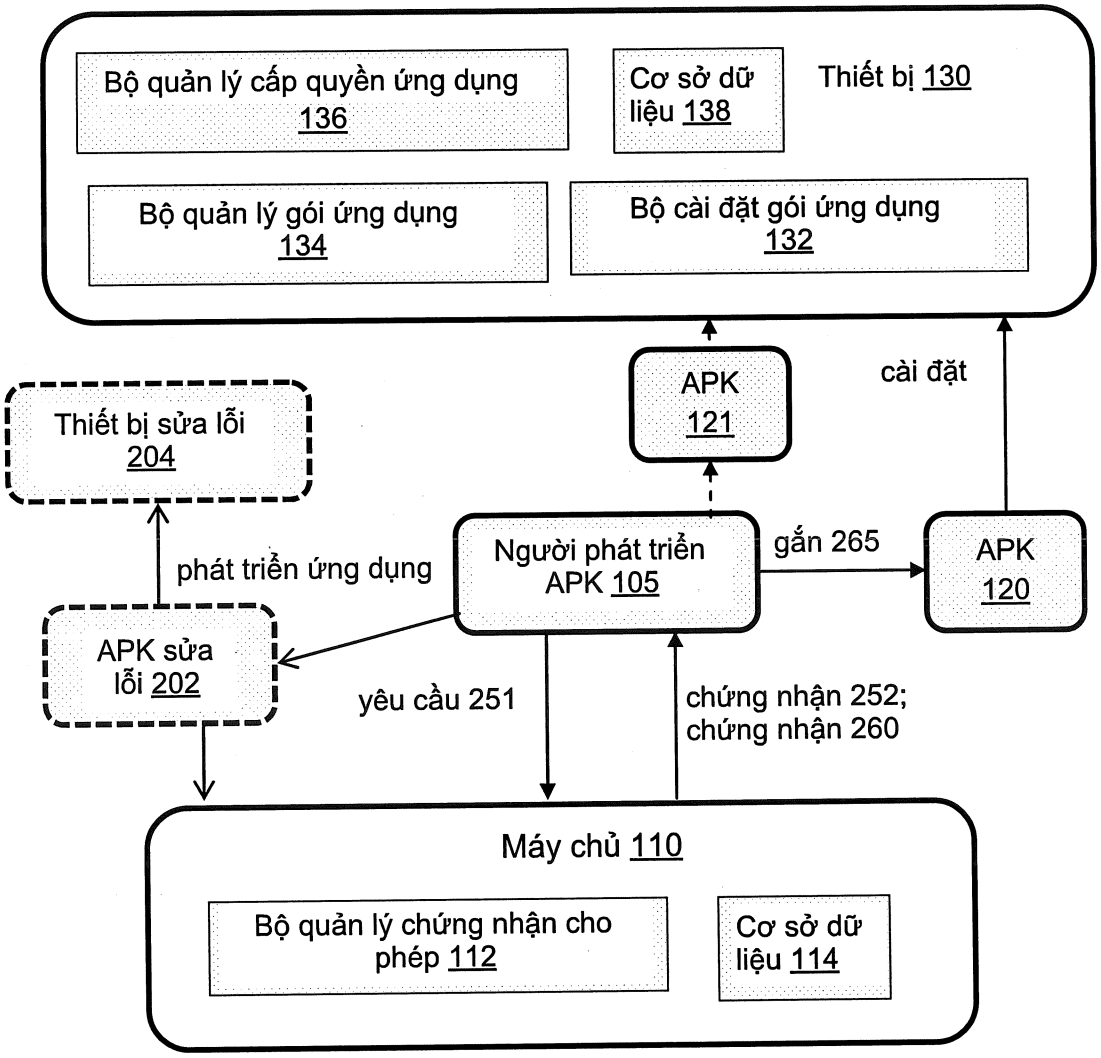

Bộ quản lý cấp quyền ứng dụng 136
Cơ sở dữ liệu 138
Thiết bị 130
Bộ quản lý gói ứng dụng 134
Bộ cài đặt gói ứng dụng 132
APK 121
cài đặt
Thiết bị sửa lỗi 204
phát triển ứng dụng
Người phát triển APK 105
gắn 265
APK 120
APK sửa lỗi 202
yêu cầu 251
chứng nhận 252; chứng nhận 260
Máy chủ 110
Bộ quản lý chứng nhận cho phép 112
Cơ sở dữ liệu 114

Fig.2

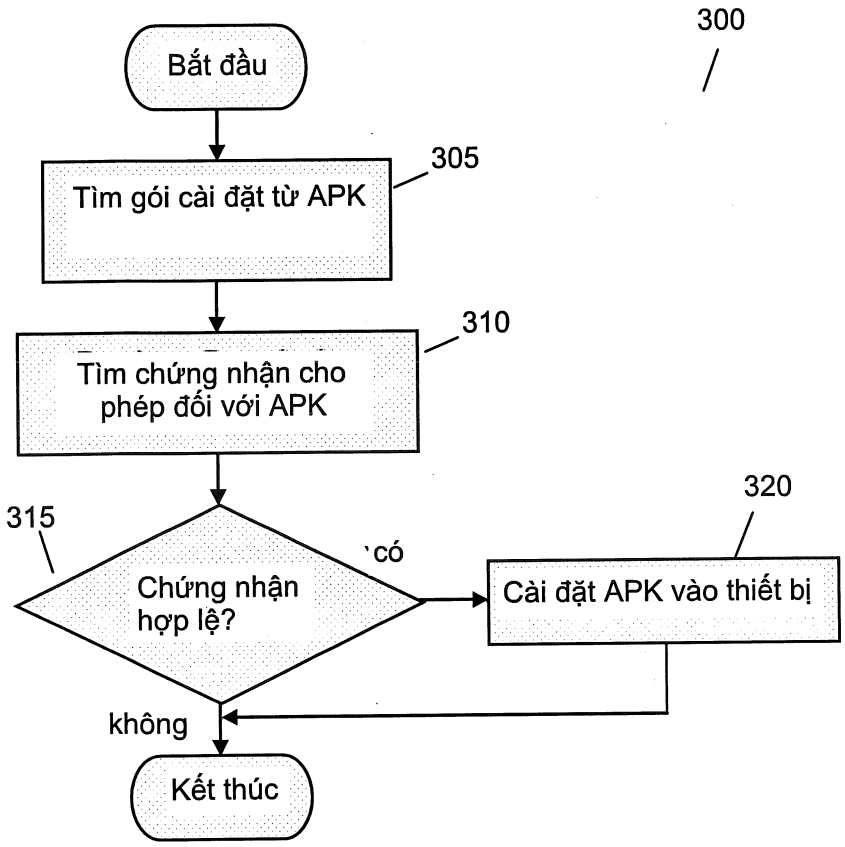

300
Bắt đầu
305
Tìm gói cài đặt từ APK
310
Tìm chứng nhận cho phép đối với APK
315
Chứng nhận hợp lệ?
có
320
Cài đặt APK vào thiết bị
không
Kết thúc

Fig.3

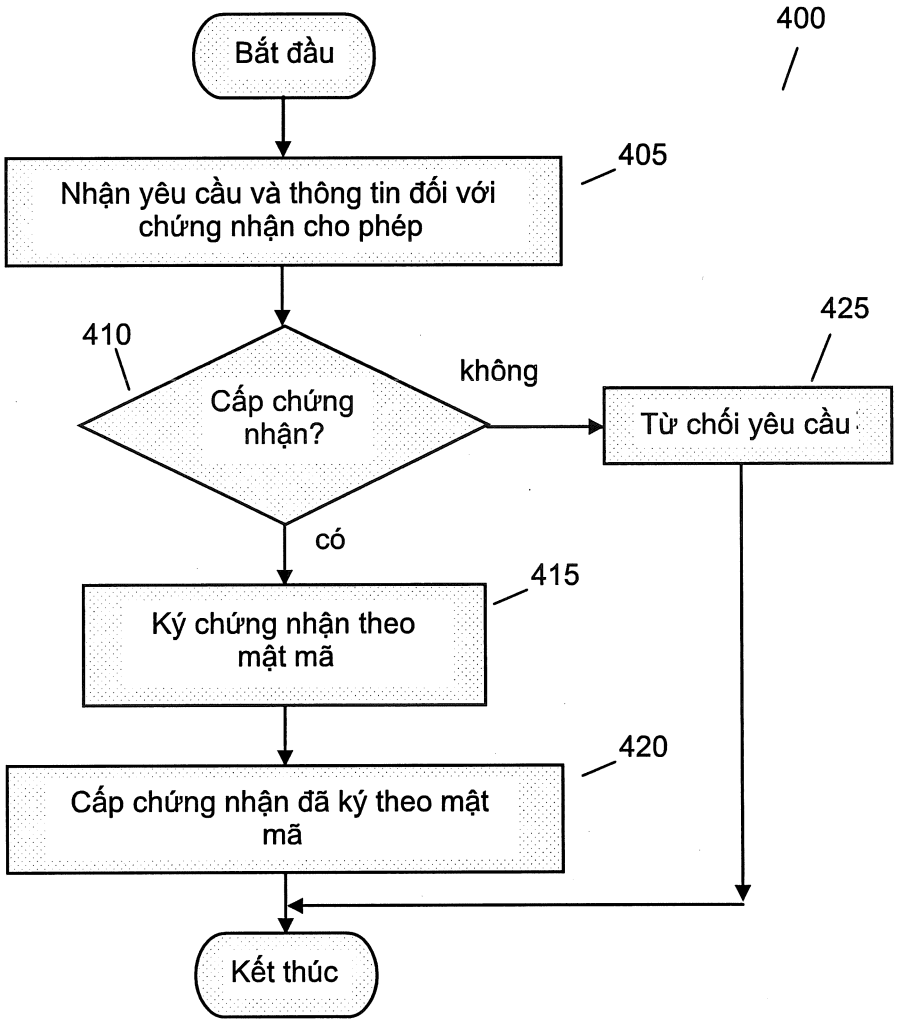

400
Bắt đầu
405
Nhận yêu cầu và thông tin đối với chứng nhận cho phép
410
Cấp chứng nhận?
không
425
Từ chối yêu cầu
có
415
Ký chứng nhận theo mật mã
420
Cấp chứng nhận đã ký theo mật mã
Kết thúc

Fig.1

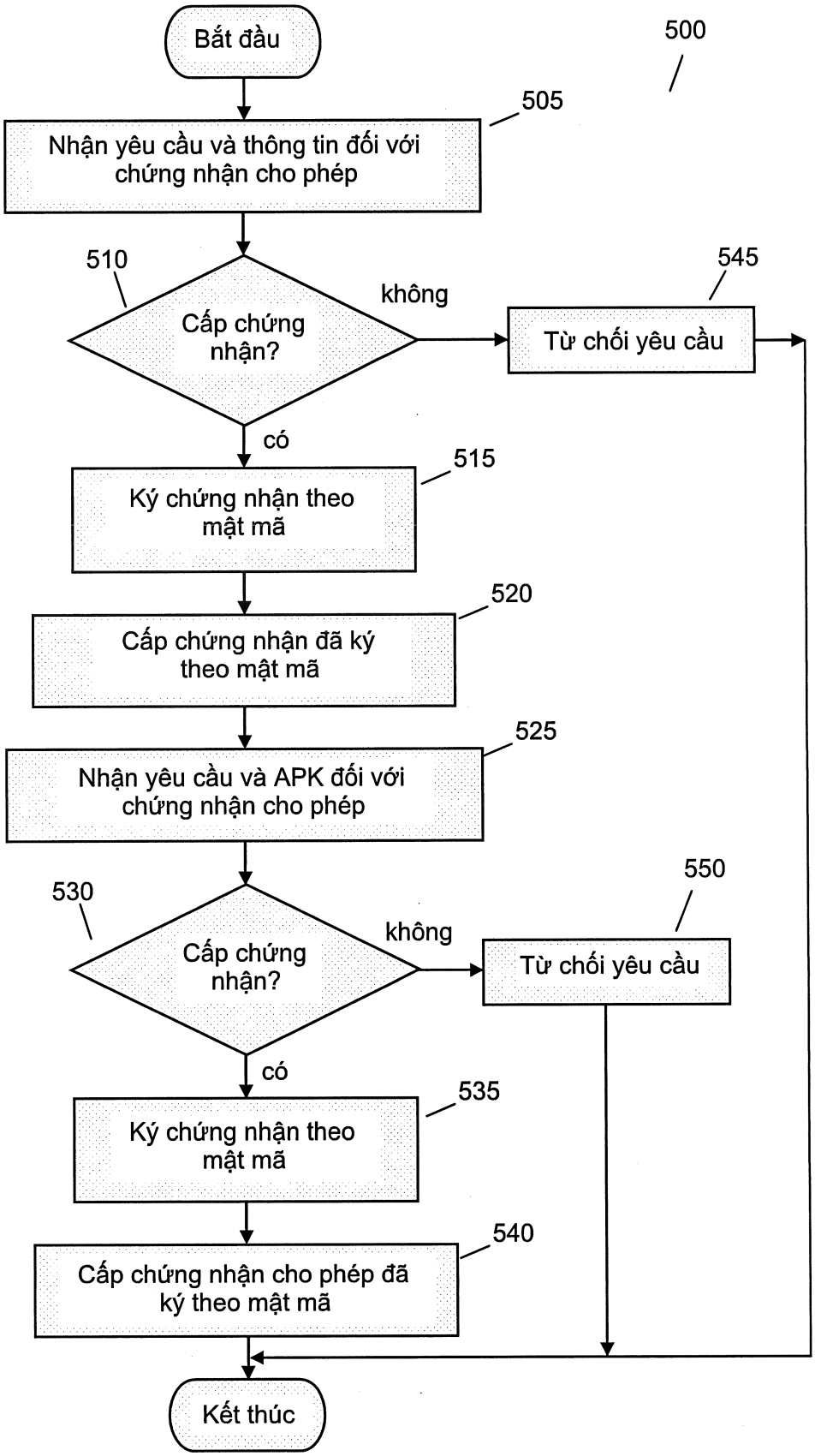

Bắt đầu
500
505
Nhận yêu cầu và thông tin đối với chứng nhận cho phép
510
Cấp chứng nhận?
không
545
Từ chối yêu cầu
có
515
Ký chứng nhận theo mật mã
520
Cấp chứng nhận đã ký theo mật mã
525
Nhận yêu cầu và APK đối với chứng nhận cho phép
530
Cấp chứng nhận?
không
550
Từ chối yêu cầu
có
535
Ký chứng nhận theo mật mã
540
Cấp chứng nhận cho phép đã ký theo mật mã
Kết thúc

Fig.5

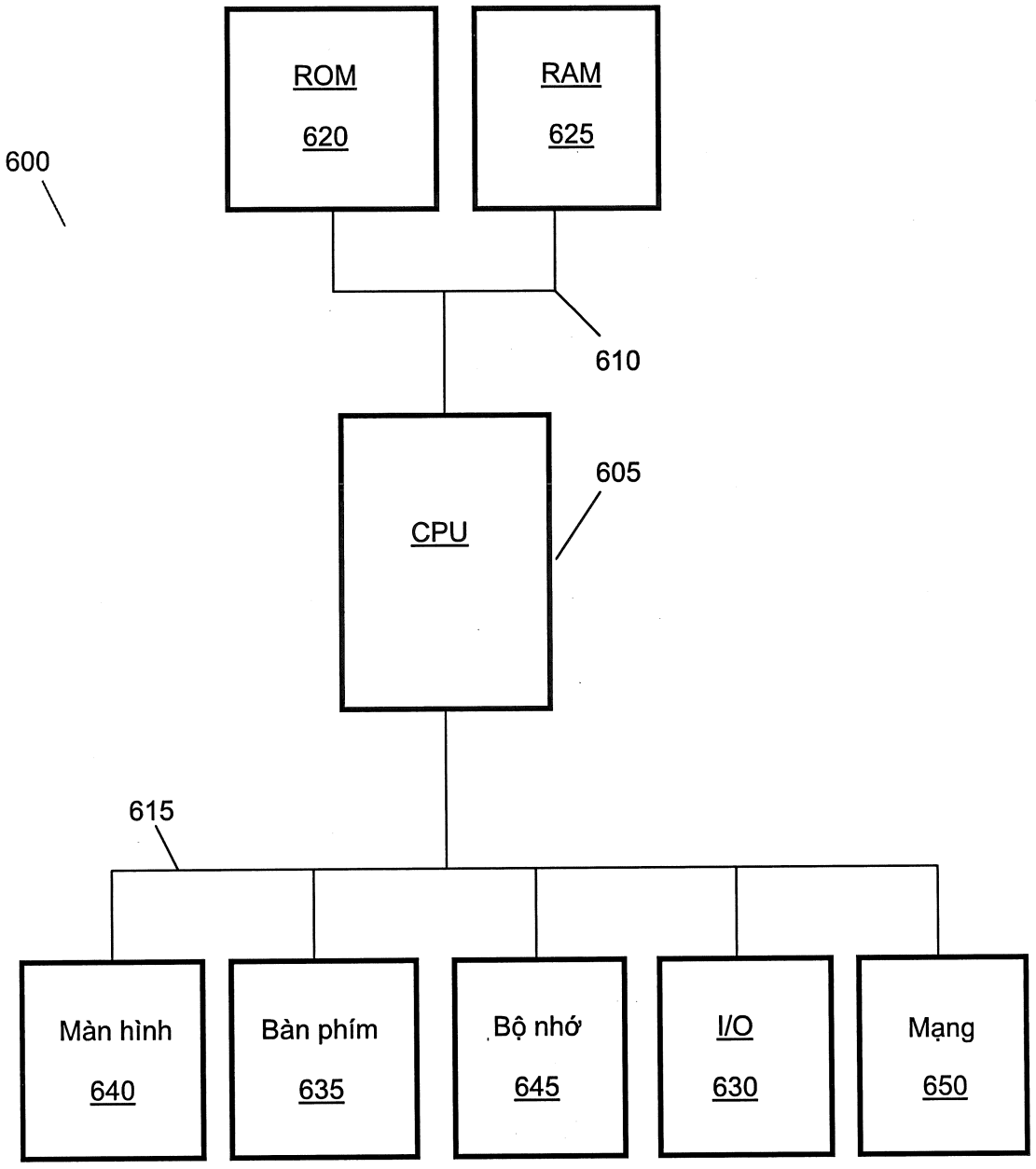

600
ROM
620
RAM
625
610
CPU
605
615
Màn hình
640
Bàn phím
635
Bộ nhớ
645
I/O
630
Mạng
650

Fig.6