(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) **1-0041395**

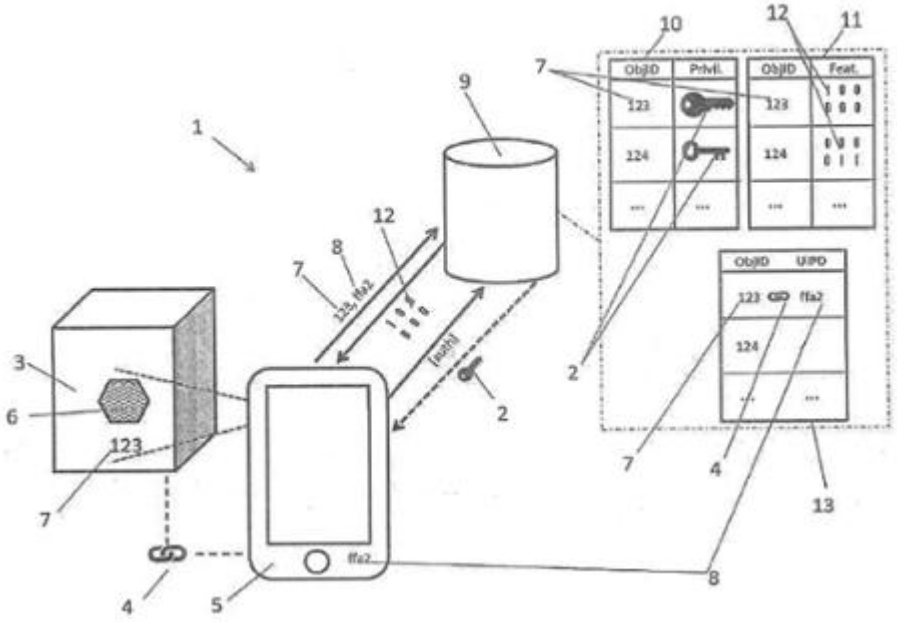
(51)[19] **H04L 29/06**

(13) **B**

(21) 1-2019-07158
(22) 25/05/2018
(86) PCT/EP2018/063746 25/05/2018
(87) WO2018/215637 29/11/2018
(30) 17173099.7 26/05/2017 EP
(45) 25/10/2024 439
(43) 27/04/2020 385
(73) AUTHENTIC VISION GMBH (AT)
Josef-Mayburger-Kai 114/10 5020 Salzburg, Austria
(72) WEISS, Thomas (AT); BERGMÜLLER, Thomas (AT).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP QUẢN LÝ CÁC ĐẶC QUYỀN

(57) Sáng chế đề xuất hệ thống (1) và phương pháp quản lý các đặc quyền, trong đó các đặc quyền được gán cho các đối tượng có thể nhận diện được duy nhất và liên kết (4) giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) được thiết lập, trong đó liên kết được thiết lập (4) cho phép thiết bị lập trình được có thể nhận diện duy nhất (5) tận dụng ít nhất một phần của các đặc quyền (2) được gán cho đối tượng có thể nhận diện được duy nhất (3) và trong đó liên kết (4) được thiết lập dưới tập các điều kiện trước, trong đó ít nhất điều kiện trước của độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) được kiểm chứng và đối tượng có thể nhận diện được duy nhất (3) bao gồm thiết bị bảo mật không sao chép được (6), mà được đăng ký với đối tượng có thể nhận diện được duy nhất (3) và có thể được sử dụng để kiểm chứng độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) bằng cách xác thực thiết bị bảo mật không sao chép được (6) nhờ phương tiện xác thực quang học, trong đó ít nhất một phần quá trình xác thực được thực hiện bởi thiết bị lập trình được có thể nhận diện duy nhất (5).


1
2
3
4
5
6
7
8
9
10
11
12
13
123
ffa2
[auth]
ObjID
Privil.
Feat.
UIPD
124

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống và phương pháp quản lý các đặc quyền.

Tình trạng kỹ thuật của sáng chế

Đầu những năm 2000, cụm từ "Internet vạn vật" (IoT) đã trở nên phổ biến, mô tả sự liên kết mạng của các đối tượng vật lý. Trong khi có sự phổ biến của các khái niệm, tầm nhìn và tham vọng tích hợp các đối tượng vật lý vào các mạng máy tính hiện tại, thì việc nhận xét rằng IoT chưa sẵn sàng để sử dụng thực tế là một sự cần trọng. Một trong các vấn đề đầu tiên xuất hiện là cách nhận diện và đánh địa chỉ một cách duy nhất tất cả các bên tham gia/các đối tượng. Vấn đề này đã được khắc phục với IPv6. Thách thức khác là việc các đối tượng (vật), mà phải tương tác, cần được có phần cứng bổ sung, tức là, giao diện mạng. Trong khi ngày nay liên kết lên mạng có thể được phủ sóng không dây, thì đối tượng tương tác vẫn cần bao gồm giao diện mạng không dây, tốt hơn là khối xử lý (CPU) và – hầu như tất cả – nguồn cấp điện. Trong số đó, các phối cảnh này cản trở việc triển khai IoT ở tốc độ nhanh hơn, dưới dạng các đối tượng, mà có thể tương tác với IoT, trở nên đắt hơn, cần nguồn điện ổn định (hoặc nạp lại được thường xuyên) v.v.. Theo một phương án thực hiện, sáng chế đề xuất việc thiết lập, để có thể tích hợp các đối tượng bình thường, tức là không có khả năng xử lý số và/hoặc nguồn điện, vào IoT. Ý tưởng là chia sẻ phần cứng của thiết bị lập trình được với đối tượng này.

Theo phương án thực hiện khác, các đối tượng sáng chế có thể đóng vai trò là các chìa khóa vật lý cho các nội dung số. Cụ thể là, các đối tượng vật lý có thể được sử dụng để cho phép, chẳng hạn, chủ nhân của nó và/hoặc thiết bị lập trình được cụ thể truy nhập các dịch vụ số định trước cụ thể và/hoặc dữ liệu bằng cách cấp các đặc quyền.

Bản chất kỹ thuật của sáng chế

Sáng chế đề cập đến hệ thống quản lý các đặc quyền. Hệ thống bao gồm các

đối tượng có thể nhận diện được duy nhất (có thể không có các khả năng xử lý số của nó), các thiết bị lập trình được có thể nhận diện duy nhất và phương pháp để đảm bảo ít nhất độ lân cận vật lý giữa các đối tượng có thể nhận diện được duy nhất và các thiết bị lập trình được có thể nhận diện duy nhất. Các đặc quyền cụ thể được đăng ký trước cho các bộ nhận dạng của các đối tượng có thể nhận diện được duy nhất, chẳng hạn, trong cơ sở dữ liệu. Độ lân cận vật lý giữa đối tượng lập trình được có thể nhận diện duy nhất cụ thể và thiết bị lập trình được có thể nhận diện duy nhất cụ thể được đảm bảo nhờ phương tiện xác thực quang học. Nhằm mục đích này, đối tượng có thể nhận diện được duy nhất bao gồm thiết bị bảo mật duy nhất và không sao chép được, cũng được đăng ký trước cho bộ nhận dạng đối tượng. Sau đó, thiết bị bảo mật có thể được xác thực nhờ phương tiện xác thực quang học, chẳng hạn, với camera. Theo phương án thực hiện được ưu tiên, thiết bị bảo mật bao gồm thiết bị biến thiên quang học (optically variable device, OVD) với các đặc tính ngẫu nhiên. Các đặc tính ngẫu nhiên đảm bảo khả năng không sao chép được của thiết bị bảo mật, trong khi đăng ký các đặc tính ngẫu nhiên với bộ nhận dạng đối tượng đảm bảo tính duy nhất của nó. Việc đăng ký có thể được thực hiện với cơ sở dữ liệu lưu trữ các liên kết giữa các biểu diễn dạng số của các thiết bị bảo mật không sao chép được và các bộ nhận dạng đối tượng duy nhất; theo cách khác, bộ nhận dạng đối tượng có thể bao gồm biểu diễn của thiết bị bảo mật không sao chép được đã được đăng ký. Việc sử dụng các OVD đảm bảo rằng thiết bị bảo mật không sao chép được không thể được sao chép bằng phương tiện sao chép. Theo phương án thực hiện được ưu tiên, thiết bị bảo mật có thể được xác thực bằng các lấy ít nhất hai bức ảnh từ các góc nhìn gác nhau, để kiểm chứng nằng nó thực sự là OVD. Ví dụ về các quá trình sản xuất thích hợp để sản xuất các thiết bị bảo mật được nêu trong công bố quốc tế số WO 2015/079014 A1. Theo phương án thực hiện được ưu tiên, các lá bảo mật đặc biệt, chẳng hạn như được nêu chi tiết hơn trong đơn Châu Âu số 16188357.4 hoặc 17162789.6 có thể được sử dụng.

Việc giới thiệu phương án thực hiện IoT có thể được xem là trường hợp đặc biệt cấp các đặc quyền. Thiết bị lập trình được có thể nhận diện duy nhất "chia sẻ" phần cứng của nó với đối tượng vật lý, bằng cách thực hiện chương trình đã

được định trước và đăng ký với đối tượng có thể nhận diện được duy nhất. Điều này tương đối giống với khái niệm máy ảo, trong đó một phần cứng được chia sẻ bởi nhiều máy ảo. Trong trường hợp ảo, máy ảo là chương trình máy tính, được định trước cho đối tượng có thể nhận diện được duy nhất. Theo sáng chế, đặc quyền để thực thi việc chương trình máy tính cụ thể dưới tên của đối tượng có thể nhận diện được duy nhất được cấp cho thiết bị nhận diện được duy nhất, do độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất có thể được kiểm chứng.

Công nghệ đã biết để đảm bảo độ lân cận vật lý giữa hai thiết bị là RFID, như được giới thiệu chẳng hạn trong công bố đơn Mỹ số US 2009/0210940 A1. Có vài khuyết điểm của các giải pháp dựa trên RFID, chẳng hạn các chi phí theo đơn vị, việc phân phối các thiết bị đọc và các trường ứng dụng giới hạn. Các thẻ RFID có các chi phí sản xuất tương đối cao, thường vượt quá $0,05. Đặc biệt nếu các thẻ RFID bảo mật được sử dụng, khó hơn để tái tạo, các chi phí thường cao hơn. Ngược lại, các thiết bị đọc RFID là phổ biến, nhưng không phải chuẩn. Phần lớn điện thoại thông minh ngày nay có các bộ cảm biến RFID cho truyền thông trường gần (NFC), mặc dù một nhà sản xuất chính không tuân theo xu hướng đến giờ. Nhiều người không nhận biết được về tính năng này trong điện thọi thông minh và nó phải được bật rõ ràng, do tiêu thụ công suất khá cao. Một phối cảnh của sáng chế là nhằm vượt qua các khuyết điểm bằng bằng cách sử dụng thiết bị bảo mật, mà có thể được xác thực bằng các bộ cảm biến quang học, tức là, camera, trong đó việc xác thực này được sử dụng để chứng minh độ liền kề giữa thiết bị bảo mật – và do vậy đối tượng này được đính vào hoặc tích hợp vào - và thiết bị lập trình được có thể nhận diện duy nhất, chẳng hạn, điện thoại thông minh. Phạm vi ứng dụng bị giới hạn có thể là gần như không thể vượt qua. RFID dựa trên các sóng điện từ. Kết quả là, nếu thẻ RFID được đặt trên đối tượng kim loại hoặc chai chứa chất lỏng, các vật liệu này trong môi trường quanh thẻ RFID có thể giới hạn việc đọc ra hoặc thậm chí vô hiệu hóa thẻ RFID, so các sóng điện từ bị chặn.

Nếu thiết bị bảo mật được sử dụng để kiểm chứng độ lân cận vật lý giữa hai thực thể có thể nhận diện duy nhất, chẳng hạn, thiết bị lập trình được có thể nhận

diện duy nhất và đối tượng có thể nhận diện được duy nhất, thiết bị bảo mật cũng được đòi hỏi là duy nhất. Thậm chí, cần có khả năng sao chép lại. Trong thiết lập cụ thể, các thiết bị và các đối tượng có thể nhận diện uy nhất bằng cách sử dụng các bộ nhận dạng, chẳng hạn, các số thứ tự, UID hoặc các mã duy nhất khác. Tuy nhiên, tất cả các bộ nhận dạng hoặc các mã này có thể được sao chép và do vậy được tái tạo dễ dàng. Điều này ám chỉ việc nhiều thực thể có cùng bộ nhận dạng duy nhất tương tự có thể được tạo, kết quả là phá bỏ giới hạn tính duy nhất. Một cách tiếp cận là trang bị bộ nhận dạng duy nhất cho thiết bị bảo mật, khó làm giả, chẳng hạn các thẻ RFID. Do vậy miễn là nhà sản xuất hợp pháp của các thiết bị bảo mật sẽ cấp chính xác một thiết bị bảo mật duy nhất cho đối tượng có thể nhận diện được duy nhất, đạt được mức bảo vệ đủ. Ít nhất các chi phí sao chép đối tượng có thể nhận diện được duy nhất cao hơn, do vậy thiết bị bảo mật duy nhất cũng cần được nhân bản (clone).

Các thẻ RFID được sử dụng rộng rãi ở đây, do có thể mã hóa các bộ nhận dạng duy nhất, chẳng hạn được ký bằng mật mã. Việc tái tạo các thể này sẽ ít nhất ám chỉ đọc ra nội dung của thẻ RFID và lập trình thẻ mới với nội dung tương tự. Nếu các thẻ RFID bảo mật được nêu được sử dụng, quá trình đọc ra được ngăn chặn. Tương tự về mặt khái niệm, Công bố đơn Châu Âu số EP 0 266 748 A2 chẳng hạn mô tả các hộp an toàn (dongle) USB, tương đương về mặt chức năng với các thẻ RFID, nhưng độ lân cận vật lý được đảm bảo bằng cách cắm USB-dongle, do vậy thiết bị bảo mật có thể cùng lúc là đối tượng này, vào thiết bị lập trình được có thể nhận diện duy nhất.

Do các khuyết điểm nêu trên của RFID, các cách tiếp cận với các thiết bị bảo mật xác thực được bằng quang học và duy nhất đã được biết đến. Chẳng hạn, patent Mỹ số US 7 650 009 B2 mô tả phương pháp chụp ảnh, bằng kỹ thuật dấu tin tăng cường nó với khóa số ("ảnh bông tuyết") và sử dụng với các thiết bị bảo mật duy nhất ngẫu nhiên. Tính ngẫu nhiên đạt được bằng cách chụp ảnh ngẫu nhiên trong khi khóa số thêm vài biến thể bổ sung ở đây. Một cách tương tự, patent Mỹ số US 7 986 806 B2 trình bày phương pháp sử dụng phương tiện dấu tin để nhúng nội dung số (chẳng hạn các bộ nhận dạng duy nhất) vào ảnh (có thể được xem là ngẫu nhiên). Một khuyết điểm chính của các thiết bị bảo mật này là

việc húng có thể được sao chép. Thực tế điều này có thể dễ dàng được kiểm chứng, chẳng hạn sử dụng máy sao chép hoặc lấy viđeo của thiết bị bảo mật này, trong đó bản sao chép hoặc viđeo cho phép xác thực từ đó.

Công bố đơn số US 2012/1694 61 A1 đề cập đến hệ thống điều khiển truy nhập điện tử cho các phòng bảo mật. Trong trường hợp này, điện thoại tế bào được sử dụng làm thiết bị tác nghiệp. Để cho phép truy nhập qua cổng/cửa, điện thoại được đưa vào lân cận của dấu nhận diện. Do vậy, hệ thống điều khiển truy nhập xác định cửa mà có thể truy nhập dựa trên dấu nhận diện được ghi nhận bởi điện thoại. Bên cạnh việc nhận diện cửa hoặc cổng, điện thoại cần xác thực người dùng.

Có một phối cảnh của tất cả các công nghệ được đưa vào; chúng có thể sao chép được. Một cách thỏa thuận được, trong khi các thẻ RFID khó sao chép bởi các bên thứ ba không hợp pháp, tất cả các công nghệ đó có thể được tái tạo bởi người cấp hợp pháp theo định nghĩa, một cách đơn giản do chúng đều dựa trên nội dung số. Điều khiển các tính năng bảo mật này dễ xâm nhập, đặc biệt nếu rò dữ liệu, tạo hai lần, đút lót và các vectơ tấn công phi dữ liệu khác được xem xét. Đặc biệt scacs thiết bị bảo mật này không thể được tận dụng trong các trường hợp sử dụng tuân theo cấp phép, trong đó số lượng các thiết bị bảo mật được cấp phép tương ứng với phí phải nộp. Phối cảnh khác của sáng chế là đề xuất thiết bị bảo mật không sao chép được, có thể được xác thực bằng các phương tiện xác thực quang học thông thường, tức là, không cần các thiết bị đặc biệt chẳng hạn kính phóng đại, v.v.. Các thiết bị bảo mật được đưa vào có thể được xác thực bằng thiết bị lập trình bất kỳ được bao gồm camera, tức là, điện thoại thông minh, máy tính tablet hoặc với máy tính cá nhân bao gồm web-cam. Bằng cách sử dụng thiết bị chuẩn và phổ biến, chẳng hạn camera thường, số lượng lớn người có thể tham gia sáng chế mà không cần có hoặc mua thiết bị bổ sung.

Mô tả vắn tắt các hình vẽ

Sáng chế sẽ được mô tả chi tiết hơn dưới đây nhờ các phương án thực hiện lấy làm ví dụ ưu tiên, mà không bị giới hạn ở đó, tuy nhiên, và dựa vào các hình vẽ. Một cách chi tiết:

Fig.1 là hình vẽ tổng quan của hệ thống quản lý các đặc quyền theo sáng chế;

Fig.2 là sơ đồ thay đổi liên kết riêng biệt giữa đối tượng có thể nhận diện được duy nhất và các thiết bị lập trình được khác nhau theo thời gian;

Fig.3 giống như Fig.2, ngoại trừ việc hệ thống cho phép nhiều thiết bị lập trình được được liên kết với cùng đối tượng có thể nhận diện được duy nhất;

Fig.4 là hình vẽ minh họa dưới dạng lược đồ việc gán các đặc quyền bị giới hạn về thời gian cho các thiết bị lập trình được khác theo thời gian;

Fig.5 là hình vẽ minh họa dưới dạng lược đồ việc gán các đặc quyền sử dụng một lần (hoặc truy nhập giới hạn) cho các thiết bị lập trình được khác nhau theo thời gian; và

Fig.6 là hình vẽ thể hiện lưu đồ của phương pháp theo phương án thực hiện được ưu tiên của sáng chế.

Mô tả chi tiết sáng chế

Sáng chế đề cập đến hệ thống quản lý các đặc quyền, trong đó các đặc quyền được gán cho đối tượng có thể nhận diện được duy nhất và liên kết giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất được thiết lập, trong đó liên kết được thiết lập cho phép thiết bị lập trình được có thể nhận diện duy nhất tận dụng ít nhất một phần của các đặc quyền được gán cho đối tượng có thể nhận diện được duy nhất và trong đó liên kết được thiết lập dưới tập các điều kiện trước, trong đó ít nhất điều kiện trước của độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất được kiểm chứng và đối tượng có thể nhận diện được duy nhất bao gồm thiết bị bảo mật không sao chép được, mà được đăng ký với đối tượng có thể nhận diện được duy nhất và có thể được sử dụng để kiểm chứng độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất bằng cách xác thực thiết bị bảo mật không sao chép được nhờ phương tiện xác thực quang học trong đó ít nhất một phần quá trình xác thực được thực hiện bởi thiết bị lập trình được có thể nhận diện duy nhất.

Cụ thể là, đối tượng có thể nhận diện được duy nhất có thể là mặt hàng nhận diện được duy nhất hoặc sản phẩm nhận diện được duy nhất.

Theo phương án thực hiện được ưu tiên của sáng chế, một hoặc nhiều nhóm các điều kiện trước bổ sung được kiểm chứng để thiết lập liên kết, nhóm các điều kiện trước bổ sung bao gồm: vị trí địa lý của thiết bị lập trình được có thể nhận diện duy nhất trong khu vực địa lý được định trước; hoặc dữ liệu khác có thể được truy xuất từ các bộ cảm biến hoặc bộ nhớ của thiết bị lập trình được có thể nhận diện duy nhất, trong đó liên kết chỉ có thể được thiết lập, nếu dữ liệu này tương ứng với các giá trị được tiền cấu hình cụ thể.

Một cách có lợi, các đặc quyền được lưu trữ trong cơ sở dữ liệu tập trung hoặc phân tán.

Theo một phương án thực hiện, đặc quyền là quyền truy nhập chương trình máy tính, mà có thể được thực thi trên thiết bị lập trình được, hoặc quyền kích hoạt thực thi chương trình máy tính trên thiết bị thứ ba, cụ thể là trên máy tính, bằng thiết bị lập trình được có thể nhận diện duy nhất và/hoặc quyền để thiết lập liên kết.

Bên cạnh đó hoặc theo cách khác, đặc quyền có thể cấp truy nhập vào cơ sở dữ liệu và cho phép thay đổi các phép gán đặc quyền.

Theo phương án thực hiện được ưu tiên, các liên kết được thiết lập được ghi nhận trong cơ sở dữ liệu phân tán hoặc tập trung.

Cơ sở dữ liệu có thể bao gồm cấu trúc chuỗi khối, mà đảm bảo tính toàn vẹn của tất cả các giao dịch (các liên kết được thiết lập) trong hệ thống mà không đòi hỏi ủy quyền tin cậy, tức là, cơ sở dữ liệu tin cậy của các liên kết được thiết lập.

Theo phương án thực hiện được ưu tiên của sáng chế, khả năng không sao chép đạt được trong đó thiết bị bảo mật bao gồm cấu trúc ba chiều có phân tán ngẫu nhiên của các đặc tính quang học phụ thuộc phối cảnh được đăng ký với bộ nhận dạng đối tượng và thiết bị lập trình được có thể nhận diện duy nhất bao gồm camera có thể được sử dụng để chụp ít nhất hai ảnh của thiết bị bảo mật từ ít nhất hai phối cảnh khác nhau hoặc với hai điều kiện chiếu sáng khác nhau.

Đối tượng có thể nhận diện được duy nhất có thể bao gồm bộ nhận dạng đối tượng, trong đó bộ nhận dạng đối tượng được mã hóa ở định dạng người đọc

được hoặc máy đọc được, cụ thể là dưới dạng số dạng số hoặc số chữ cái hoặc dưới dạng mã vạch hoặc mã hai chiều. Việc sử dụng các mã máy đọc được, chẳng hạn mã vạch hoặc mã 2D, trở nên có lợi, do bộ nhận dạng phải được đọc bởi thiết bị lập trình được có thể nhận diện duy nhất. Theo phương án thực hiện khác, các biểu diễn người đọc được và máy đọc được của bộ nhận dạng tương tự có thể được sử dụng song song.

Theo phương án thực hiện được ưu tiên, liên kết giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất bao gồm hai hoặc nhiều liên kết trung gian được kết nối, cụ thể là liên kết trung gian thứ nhất giữa đối tượng có thể nhận diện được duy nhất và tài khoản người dùng và liên kết trung gian thứ hai giữa tài khoản người dùng và thiết bị lập trình được có thể nhận diện duy nhất. Liên kết giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất được thiết lập bằng cách thiết lập và kết nối các liên kết trung gian, trong đó để thiết lập ít nhất một trong các liên kết trung gian, các điều kiện trước được định nghĩa trên đây phải được thỏa mãn. Các liên kết trung gian còn lại có thể hoặc không thể được thiết lập độc lập với các điều kiện trước.

Nói chung, sáng chế đề cập đến hệ thống để quản lý (tức là, cấp và tạo) các đặc quyền, bao gồm:

ít nhất một đối tượng (hoặc mặt hàng hoặc sản phẩm) có

bộ nhận dạng đối tượng duy nhất và

thiết bị bảo mật không sao chép được;

ít nhất một thiết bị lập trình được

có bộ nhận dạng thiết bị duy nhất và

bao gồm phương tiện xác thực bằng quang học (chẳng hạn, camera được kết nối với máy tính); và

cơ sở dữ liệu

lưu trữ một hoặc nhiều đặc quyền được liên kết với bộ nhận dạng đối tượng duy nhất, và

lưu trữ một hoặc nhiều liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối tượng duy nhất;

trong đó hệ thống được tạo cấu hình để thiết lập liên kết mới giữa bộ nhận dạng thiết bị duy nhất của thiết bị lập trình được và bộ nhận dạng đối tượng duy nhất của đối tượng chỉ sau khi kiểm chứng thành công các điều kiện trước cụ thể, bao gồm ít nhất việc xác thực thiết bị bảo mật không sao chép được của đối tượng có phương tiện xác thực quang học của thiết bị lập trình được,

và trong đó hệ thống được tạo cấu hình để xác định các đặc quyền của thiết bị lập trình được bằng cách xác định một hoặc nhiều bộ nhận dạng đối tượng duy nhất được liên kết với bộ nhận dạng thiết bị duy nhất của thiết bị lập trình được và xác định một hoặc nhiều đặc quyền được liên kết với một hoặc nhiều bộ nhận dạng đối tượng duy nhất được xác định dưới dạng các đặc quyền của thiết bị lập trình được.

Sáng chế cũng đề cập đến phương pháp thu thập các đặc quyền với thiết bị lập trình được có bộ nhận dạng thiết bị duy nhất, bao gồm:

– chụp bằng thiết bị lập trình được ít nhất hai ảnh, trong đó ít nhất một ảnh chụp bộ nhận dạng đối tượng duy nhất của đối tượng (hoặc mặt hàng hoặc sản phẩm) và ít nhất hai ảnh chụp thiết bị bảo mật không sao chép được của đối tượng;

– xác thực thiết bị bảo mật không sao chép được dựa trên ít nhất hai ảnh;

– nếu tất cả các điều kiện trước của tập các điều kiện trước được hoàn thành, thiết lập liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối tượng duy nhất, trong đó tập các điều kiện trước bao gồm ít nhất điều kiện trước mà thiết bị bảo mật không sao chép được có thể được xác thực,

trong đó một hoặc nhiều đặc quyền are được liên kết với bộ nhận dạng đối tượng duy nhất,

trong đó ít nhất một phần của một hoặc nhiều đặc quyền được cấp cho thiết bị lập trình được bất kỳ có bộ nhận dạng thiết bị duy nhất được liên kết với bộ nhận dạng đối tượng duy nhất.

Như nêu trên, thiết lập liên kết có thể đạt được bằng cách thiết lập liên kết trung gian (chẳng hạn, giữa bộ nhận dạng đối tượng duy nhất và bộ nhận dạng tài khoản duy nhất), trong đó hai hoặc nhiều liên kết trung gian được kết nối cùng nhau tạo thành liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối

tượng duy nhất (chẳng hạn, liên kết trung gian khác giữa bộ nhận dạng tài khoản duy nhất và bộ nhận dạng thiết bị duy nhất có thể đã được thiết lập trước đó, chẳng hạn bằng cách đăng ký thiết bị lập trình được với tài khoản người dùng).

Theo phương án thực hiện được ưu tiên của phương pháp hiện tại, việc xác thực thiết bị bảo mật không sao chép được bao gồm các bước:

– trích rút biểu diễn dạng số của một hoặc nhiều dấu hiệu bảo mật quang học từ ít nhất hai ảnh;

– so sánh biểu diễn dạng số với tham chiếu;

– xác thực thiết bị bảo mật không sao chép được nếu biểu diễn dạng số so khớp (chính xác hoặc bằng cách có số đo khoảng cách thích hợp nhỏ hơn ngưỡng cụ thể) tham chiếu.

Cụ thể hơn là, việc xác thực thiết bị bảo mật không sao chép được có thể bao gồm bước:

– thu được tham chiếu từ cơ sở dữ liệu, tốt hơn là bằng cách truy vấn cơ sở dữ liệu với bộ nhận dạng đối tượng duy nhất được chụp.

Để đạt được quyền sở hữu riêng của các đặc quyền được liên kết với đối tượng, phương pháp có thể còn khác biệt bởi:

– trước khi thiết lập liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối tượng duy nhất, xác định liệu bộ nhận dạng đối tượng duy nhất đã được liên kết với một hoặc nhiều bộ nhận dạng thiết bị duy nhất khác nhau;

– thiết lập liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối tượng duy nhất chỉ nếu bộ nhận dạng đối tượng duy nhất không được liên kết với bộ nhận dạng thiết bị duy nhất khác nhau bất kỳ.

Theo phương án thực hiện được ưu tiên của sáng chế, thiết lập liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối tượng duy nhất bao gồm lưu trữ liên kết giữa bộ nhận dạng thiết bị duy nhất và bộ nhận dạng đối tượng duy nhất trong cơ sở dữ liệu.

Ngoài ra, và tương ứng với các phương pháp nêu trên, sáng chế cũng đề cập đến phương pháp xác định các đặc quyền của thiết bị lập trình được có bộ nhận dạng thiết bị duy nhất, bao gồm các bước:

– truy xuất danh sách các liên kết hợp lệ của bộ nhận dạng thiết bị duy nhất

từ cơ sở dữ liệu phân tán hoặc tập trung;

– xác định một hoặc nhiều bộ nhận dạng đối tượng duy nhất được liên kết với bộ nhận dạng thiết bị duy nhất theo danh sách truy xuất của các liên kết hợp lệ;

– xác định một hoặc nhiều đặc quyền được liên kết với một hoặc nhiều bộ nhận dạng đối tượng duy nhất được xác định như là các đặc quyền của thiết bị lập trình được.

Việc truy xuất danh sách các liên kết hợp lệ và xác định các bộ nhận dạng đối tượng duy nhất được liên kết và của các đặc quyền được liên kết có thể được thực hiện bằng cách truy vấn cơ sở dữ liệu với bộ nhận dạng thiết bị duy nhất và/hoặc các bộ nhận dạng đối tượng duy nhất một cách lần lượt.

Danh sách các liên kết hợp lệ là tập hợp của tất cả các liên kết được thiết lập bằng cách xác thực thiết bị bảo mật không sao chép được với thiết bị lập trình được; chi tiết hơn, các liên kết được thiết lập theo phương pháp thu thập các đặc quyền như nêu trên. Các liên kết không hợp lệ có thể bị bỏ qua khỏi danh sách; tức là, tốt hơn là, chỉ các liên kết hợp lệ được truy xuất để xác định các đặc quyền của thiết bị lập trình được có bộ nhận dạng thiết bị duy nhất.

Sáng chế bao gồm hệ thống 1 quản lý các đặc quyền 2, trong đó các đặc quyền 2 được gán cho đối tượng có thể nhận diện được duy nhất 3. Liên kết 4 giữa đối tượng có thể nhận diện được duy nhất 3 và thiết bị lập trình được có thể nhận diện duy nhất 5 được thiết lập theo các điều kiện trước cụ thể, ít nhất điều kiện trước của độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất 3 và thiết bị lập trình được có thể nhận diện duy nhất 5. Liên kết được thiết lập 4 có thể kích hoạt thiết bị lập trình được có thể nhận diện duy nhất 5 sử dụng ít nhất một phần các đặc quyền 2 được gán cho đối tượng có thể nhận diện được duy nhất 3. Độ lân cận vật lý được đảm bảo bằng cách xác thực thiết bị bảo mật không sao chép được 6 của đối tượng có thể nhận diện được duy nhất 3 nhờ phương tiện xác thực quang học, chẳng hạn bằng cách chụp với camera, của thiết bị lập trình được có thể nhận diện duy nhất 5. Sau đó ảnh được xử lý, chẳng hạn, trên thiết bị lập trình được có thể nhận diện duy nhất 5 và được sử dụng để xác thực thiết bị bảo mật không sao chép được 6. Thiết bị bảo mật không sao chép

được 6 được đăng ký với đối tượng có thể nhận diện được duy nhất 3, và do vậy kết quả xác thực tính cực chứng minh độ lân cận vật lý giữa thiết bị bảo mật không sao chép được 6, mà được đính kèm hoặc một phần đối tượng có thể nhận diện được duy nhất 3, và thiết bị lập trình được có thể nhận diện duy nhất 5.

Trong thiết lập ưu tiên, đối tượng có thể nhận diện được duy nhất 3 bao gồm bộ nhận dạng đối tượng duy nhất 7. Theo phương án thực hiện, bộ nhận dạng đối tượng duy nhất 7 là số thứ tự, có thể được mật mã hóa hoặc được ký dưới dạng mật mã. Tương tự, phương pháp khác bất kỳ để tạo các bộ nhận dạng đối tượng duy nhất có thể được sử dụng. Thiết bị lập trình được 5 có thể được nhận diện bởi bộ nhận dạng thiết bị duy nhất 8 thích hợp bất kỳ, chẳng hạn qua địa chỉ MAC, băm phần cứng hoặc các phương pháp đã biết tương tự tạo UID cho các giải pháp phần cứng hoặc phần mềm.

Các đặc quyền 2 được gán cho đối tượng có thể nhận diện được duy nhất 3 qua bộ nhận dạng đối tượng duy nhất 7. Trong thiết lập ưu tiên, các đặc quyền 2 có thể được lưu trữ – cùng với bộ nhận dạng đối tượng duy nhất 7 – trong cơ sở dữ liệu 9, mà có thể được truy nhập bởi thiết bị lập trình được có thể nhận diện duy nhất 5. Ngay khi liên kết 4 được đề cập được thiết lập giữa đối tượng có thể nhận diện được duy nhất 3 và thiết bị lập trình được có thể nhận diện duy nhất 5, thiết bị lập trình được có thể nhận diện duy nhất 5 là hợp pháp để tận dụng các đặc quyền 2 được đăng ký với đối tượng có thể nhận diện được duy nhất 3 via bộ nhận dạng đối tượng duy nhất 7 theo bảng thứ nhất 10 của cơ sở dữ liệu 9. Nói theo cách khác, các đặc quyền 2 được "truyền" đến thiết bị lập trình được có thể nhận diện duy nhất 5. Do các đặc quyền 2 và các liên kết 4 là các khái niệm trừu tượng, bản chất và các thuộc tính sẽ được đề cập trong phần tiếp theo dựa trên nhưng không bị giới hạn ở một số ví dụ.

Thiết lập liên kết 4 bị giới hạn bởi ít nhất kết quả xác thực dương của thiết bị bảo mật không sao chép được 6. Cần xem xét khi lựa chọn thiết bị bảo mật thích hợp. Tiếp theo, sẽ có danh sách các kịch bản tấn công và từ đó sẽ kết luận về các yêu cầu cho công nghệ xác thực sản phẩm thích hợp. Trước hết, thiết bị bảo mật cần chống lại sao chép và nhân bản. Cơ bản, nếu thiết bị bảo mật có thể được sao chép hoặc nhân bản, người ta có thể dễ dàng trang bị cho nhiều đối

tượng thiết bị bảo mật được sao chép. Theo sáng chế, thiết bị bảo mật được sử dụng – giữa các thiết bị khác – để kiểm chứng tính xác thực (và do vậy tính duy nhất) của bộ nhận dạng đối tượng duy nhất 7. Điều này ám chỉ, nếu thiết bị bảo mật có thể được sao chép hoặc nhân bản, bên thứ ba không hợp pháp có thể phát hành nhiều đối tượng vật lý không giới hạn về mặt lý thuyết, tất cả chia sẻ cùng bộ nhận dạng đối tượng 7, mà tất cả sẽ – do thiết bị bảo mật được sao cho - kích hoạt liên kết với thiết bị lập trình được 5.

Như định nghĩa, thiết bị bảo mật bất kỳ có thể là giả mạo. Chỉ là vấn đề về tài nguyên/chi phí mà phân biệt thiết bị bảo mật tốt với thiết bị không thích hợp. Thiết bị bảo mật được xem xét là bảo mật, nếu các chi phí giả mạo nó cao hơn giá trị thu được bằng cách phát hành thực thể giả mạo của đối tượng được bảo vệ bằng thiết bị bảo mật này. Trong trường hợp sử dụng này, thiết bị bảo mật giả mạo nên đòi hỏi tài nguyên vượt quá giá trị đạt được bởi các đặc quyền thu được không hợp pháp thu được qua liên kết không hợp pháp được thiết lập dựa trên đối tượng giả mạo, tức là, thiết bị bảo mật giả mạo. Trong thiết lập có lợi, các thiết bị bảo mật duy nhất được ưu tiên trên các thiết bị tĩnh (do chúng có thể được sao cho theo định nghĩa). Hình dung rằng thiết bị bảo mật tĩnh được sử dụng, cụ thể là một thiết bị độc lập với bộ nhận dạng đối tượng. Như đã nêu, bộ nhận dạng đối tượng thường là số thứ tự hoặc tổ hợp (số) khác bất kỳ, nói chung dễ tái tạo. Kết quả là, nếu thiết bị bảo mật độc lập với bộ nhận dạng đối tượng, thì có thể sẵn sàng trao đổi bộ nhận dạng đối tượng và do vậy có các đặc quyền không hợp pháp được đăng ký với bộ nhận dạng đối tượng được sử dụng không hợp pháp. Giả thiết bộ nhận dạng đối tượng "123" nhận dạng đối tượng được liên kết với các đặc quyền cơ bản, trong khi bộ nhận dạng đối tượng "124" nhận diện đối tượng có các đặc quyền giá trị rất cao. Hiện tại, nếu cùng thực thể thiết bị bảo mật xác thực các bộ nhận dạng đối tượng, "123" và "124", thì kịch bản tấn công sau xuất hiện: Người ta có thể mua đối tượng được nhận diện bởi "123", có thiết bị bảo mật hợp lệ và giả sử là rẻ hơn đối tượng có các đặc quyền giá trị cao hơn. Sau đó, bộ nhận dạng đối tượng không hợp pháp được thay đổi từ "123" đến "124". Do thiết bị bảo mật tĩnh cũng xác thực bộ nhận dạng đối tượng "124", nên có thể tạo liên kết không hợp pháp giữa bộ nhận dạng đối tượng "124" và

thiết bị lập trình được có thể nhận diện duy nhất, sau đó có thể sử dụng các đặc quyền được dăng ký. Phối cảnh chính của cuộc tấn công này là, việc khoogn cần giả mạo thiết bị bảo mật, do nó xác thực nhiều hơn một bộ nhận dạng đối tượng. Do vậy, thiết bị bảo mật nên được thiết kế theo cách nó xác thực chính xác một bộ nhận dạng đối tượng cụ thể. Các thiết bị bảo mật này thường được gọi là các thiết bị bảo mật duy nhất. Theo sáng chế, thiết bị bảo mật cũng không thể sao chép được. Các thiết bị bảo mật không sao chép được 6 này khác biệt bởi có các thuộc tính ba chiều và ngẫu nhiên. Ngoài ra, thiết bị bảo mật không sao chép được 6 được đăng ký với bộ nhận dạng đối tượng duy nhất 7 theo bảng thứ hai 11 của cơ sở dữ liệu 9. Bảng thứ hai 11 lưu trữ các liên kết giữa các bộ nhận dạng đối tượng duy nhất 7 và các biểu diễn dạng số 12 của các thiết bị bảo mật không sao chép được 6 tương ứng (chẳng hạn, đính kèm). Điều này giúp đảm bảo rằng bộ nhận dạng đối tượng 7 cụ thể được bảo mật bởi thực thể cụ thể của thiết bị bảo mật không sao chép được 6. Thiết lập này tăng độ bảo mật đáng kể. Nếu các thiết bị bảo mật có thể sao chép hoặc tất định được sử dụng, việc sao chép gian lận thiết bị bảo mật có thể được tận dụng để trang bị cho nó không hợp pháp nhiều đối tượng có thể nhận diện được duy nhất. Các thiết bị bảo mật có khả năng sao chép được là, chẳng hạn, các tính năng bảo mật được tạo dưới dạng số, trong đó các thuộc tính phổ thông giữa nhiều thực thể được sử dụng để xác thực, chẳng hạn, vi in, đánh dấu (watermark) hoặc cá theiets bị biến thiên quang học tĩnh (tức là, không ngẫu nhiên). Thậm chí, việc sử dụng các thiết bị bảo mật có khả năng sao chép cho phép trang bị nhiều đối tượng với cùng bộ nhận dạng đối tượng và thiết bị bảo mật, mà kết quả là bỏ trống ràng buộc về tính duy nhất, giả sử các thuộc tính thiết bị bảo mật đã được biết. Các thuộc tính này có thể đã biết do những nhà sản xuất hợp pháp cấp các phiên bản sao chép không hợp pháp (chẳng hạn, hối lộ, sản xuất hai lần) hoặc do chúng đã được chế tạo lại từ thực thể đối tượng khác.

Do vậy, các thiết bị bảo mật không sao chép được 6, được đăng ký với bộ nhận dạng đối tượng duy nhất 7, giúp đảm bảo rằng mỗi đối tượng có thể được nhận diện duy nhất.

Các thiết bị bảo mật không sao chép được 6 nên được xác thực nhờ phương

tiện xác thực quang học (không được thể hiện trên hình vẽ), trong thiết lập ưu tiên (nhưng không bị giới hạn ở loại thiết bị bảo mật này) với camera đơn giản mà không có thiết bị đặc biệt bất kỳ. Chẳng hạn, camera điện thoại thông minh bình thường có thể được sử dụng. Các thiết bị bảo mật này đã được biết. Trong phần trên, đã trình bày phương pháp để tạo các tính năng bảo mật này (xem công bố đơn số WO 2015/079014 A1) và giới thiệu hệ thống để xác thực nó (công bố đơn số WO 2016/034555 A1). Ngoài ra, đã trình bày sản phẩm dạng tấm tối ưu và phương pháp xác thực thiết bị bảo mật này (xem đơn Châu Âu số 16188357.4). Tóm lại, trong thiết lập ưu tiên, các thiết bị bảo mật không sao chép được 6 bao gồm các thuộc tính biến thiên quang học ba chiều ngẫu nhiên, đặc biệt thay đổi các đặc tính quang học khi được quan sát từ các phối cảnh khác nhau và/hoặc bằng các nguồn sáng khác nhau. Nhờ camera chụp ít nhất hai ảnh từ ít nhất hai phối cảnh khác nhau, nên các thuộc tính này có thể được thẩm định bằng cách đánh giá hình dạng tương ứng và/hoặc thay đổi hình dạng. Thuộc tính này là quan trọng để khiến tính năng bảo mật chống lại sao chép. Tính ngẫu nhiên bao gồm xuất hiện từ các dung sai sản xuất trong quá trình sản xuất và/hoặc ứng dụng của các thiết bị bảo mật và thể hiện, chẳng hạn ở vị trí, phân tán và/hoặc các đặc tính biến thiên quang học. Bằng cách chụp và thẩm định các tính năng ngẫu nhiên đó và đăng ký các biểu diễn dạng số 12 với bộ nhận dạng đối tượng 7, thiết bị bảo mật không sao chép được 6 có thể được tạo. Thiết bị bảo mật này khác biệt bởi khả năng xác thực được với camera chuẩn. Chẳng hạn (nhưng không bị giới hạn ở) các thiết bị biến thiên quang học nhiễu xạ (DOVID), thường được gọi là ảnh toàn ký, hoặc công nghệ dạng thấu kính có thể được sử dụng ở đây. Ngoài ra, các công nghệ khác dựa vào tính ngẫu nhiên trong các dung sai sản xuất có thể được sử dụng. Cụ thể là, việc sử dụng ít nhất một phần của chính đối tượng làm thiết bị bảo mật có thể được xem xét, như được gợi ý trong, chẳng hạn công bố đơn Mỹ số US 2015/0188706 A1 hoặc đơn Châu Âu số EP 3 154 015 A1.

Ngoài ra, các điều kiện trước bổ sung để thiết lập liên kết 4 có thể được đưa vào. Chẳng hạn, có thể có ích cho một số ứng dụng, nếu liên kết 4 chỉ có thể được thiết lập trong khu vực (địa lý) cụ thể. Điều này tương đương với các đặc

quyền chỉ được cấp, nếu đối tượng có thể nhận diện được duy nhất 3 ở vị trí cụ thể. Vị trí của đối tượng có thể được xác định bởi thiết bị lập trình được có thể nhận diện duy nhất 5, do nó tương ứng (qua độ lân cận vật lý) với vị trí của đối tượng. Về bản chất, cũng đối tượng khác, có thể thu được từ các bộ cảm biến của thiết bị lập trình được có thể nhận diện duy nhất, đầu vào hoặc bộ nhớ, có thể được sử dụng để thêm nhiều điều kiện trước hoặc giới hạn hơn để thiết lập liên kết 4.

Khi sử dụng dữ liệu của thiết bị lập trình được duy nhất ở đây và biến đổi nó thành "các thuộc tính" của đối tượng (do về mặt vật lý nó gần và do vậy dữ liệu của thiết bị lập trình được có thể nhận diện duy nhất tương ứng với các thuộc tính của đối tượng), nên cực kỳ quan trọng khi thiết bị bảo mật có thể được xác thực duy nhất nếu thực sự nó gần về mặt vật lý với thiết bị xác thực, tức là, thiết bị lập trình được có thể nhận diện duy nhất.

Do vậy, hệ thống tận dụng một cách có lợi việc phát hiện lừa đảo. Trong tấn công lừa đảo, chẳng hạn, các tính năng bảo mật ba chiều (quang học) được đánh giá bằng camera có thể được ghi nhận trên viđeo. Sau đó, viđeo có thể được truyền bằng phương tiện chia sẻ tệp tin số và sau đó viđeo được hiển thị đến thiết bị lập trình được 5. Việc dò thấy phát lại có thể đặc biệt liên quan, do việc phát lại, chẳng hạn, viđeo trước camera của thiết bị lập trình được có thể nhận diện duy nhất có thể lừa hệ thống. Phương tiện bất kỳ phát hiện lừa đảo có thể được sử dụng, có vài phương pháp áp dụng được đã biết đến trong lĩnh vực xử lý ảnh, chẳng hạn từ các bộ cảm biến sinh trắc học (nhận dạng mống mắt, …).

Khi tất cả các điều kiện trước áp dụng được được thỏa mãn, thiết bị lập trình được có thể nhận diện duy nhất 5 thông báo cơ sở dữ liệu 9 về việc xác thực thành công và liên kết 4 mới được tạo trong bảng thứ ba 13 của cơ sở dữ liệu 9, trong đó liên kết 4 được biểu diễn dưới dạng liên kết giữa bộ nhận dạng đối tượng duy nhất 7 và bộ nhận dạng thiết bị duy nhất 8.

Các đặc quyền và các liên kết

Liên kết 4 hợp lệ giữa đối tượng có thể nhận diện được duy nhất 3, được tạo, chẳng hạn, bởi sản phẩm vật lý, và thiết bị lập trình được 5 được thiết lập, để

khiến các đặc quyền 2 được đăng ký với đối tượng 3 qua bộ nhận dạng đối tượng 7 mà thiết bị lập trình được có thể nhận diện duy nhất 5 có thể truy nhập được. Nếu liên kết 4 trở nên không hợp lệ, chẳng hạn do thiết bị lập trình được có thể nhận diện duy nhất khác kết nối với sản phẩm vật lý hoặc khoảng thời gian hợp lệ của liên kết đã trôi qua, thiết bị lập trình được có thể nhận diện duy nhất 5 đánh mất các đặc quyền 2. Cách nhìn khác là việc sản phẩm vật lý đóng vai trò khóa, kích hoạt hoặc mở khóa nội dung số hoặc thực thi chương trình máy tính trên thiết bị lập trình được.

Có các chế độ cho các liên kết tương tự liên kết 4 bất kể tính hợp lệ của nó. Tính hợp lệ của các liên kết có thể được quản lý trên thiết bị lập trình được (trường hợp này không được chụp) hoặc trong bảng hoặc bản ghi của các liên kết 13, có thể được đặt trong cơ sở dữ liệu 9 phân tán hoặc tập trung. Như là các ví dụ, Fig.2 đến Fig.5 thể hiện chuỗi liên kết được đơn giản háo theo thời gian 14 và dữ liệu tương ứng trong cơ sở dữ liệu 9 tập trung hoặc phân tán ở các thời điểm khác nhau (để đơn giản, chỉ một bảng 13 của cơ sở dữ liệu 9 lưu trữ các liên kết 4 được chỉ báo):

(Lưu ý rằng các bản ghi của các liên kết được giữ nhằm mục đích minh họa. Các liên kết không hợp lệ được mô tả xám và gạch ngang. Tuy nhiên, cũng có thể có lợp khi giữ các bản ghi này để phân tích trong ứng dụng thực và duy trì cờ "hợp lệ", chỉ báo trạng thái của liên kết)

Các liên kết vĩnh cửu, như được thể hiện trên Fig.3, về cơ bản duy trì danh sách 15 của các liên kết được thiết lập 4. Điều này nghĩa là, ngay khi thiết bị lập trình được 5 thiết lập liên kết 4 dựa trên bộ nhận dạng đối tượng 7 và bộ nhận dạng thiết bị duy nhất 8, nó hợp lệ và vẫn như vậy. Do vậy, nếu thiết bị lập trình được 5 với bộ nhận dạng thiết bị duy nhất 8 "A" thiết lập liên kết ở thời gian xác thực 16, cùng lúc liên kết 4 được thiết lập. Tương tự, danh sách các liên kết hợp lệ được mở rộng ở thời gian xác thực 17 sau với mục cho thiết bị lập trình được 5 với bộ nhận dạng thiết bị duy nhất 8 "B" và v.v.. Do vậy, danh sách 15 của các liên kết 4 hợp lệ được lưu trữ trong cơ sở dữ liệu 9 tăng cố định và ghi nhận lịch sử liên kết. Điều này cho phép chẳng hạn, các giải pháp Track & Trace hoặc lịch sử quét, có thể được sử dụng để quản lý chuỗi cung ứng v.v.. Kết quả là, mỗi

thiết bị lập trình được 5 mà đã được thiết lập liên kết 4, là các đặc quyền 2 được cấp ổn định được đăng ký với bộ nhận dạng đối tượng 7, thậm chí nếu đối tượng không phải lúc nào cũng xuất hiện (do vậy gần về mặt vật lý).

Các liên kết giới hạn về số lượng có thể được sử dụng khi nhiều nhất số lượng cụ thể N liên kết có thể được thiết lập giữa các thiết bị lập trình được và đối tượng. Fig.2 hiển thị trường hợp đặc biệt, trong đó nhiều nhất N=1 thiết bị lập trình được có thể nhận diện duy nhất may liên kết với đối tượng. Trường hợp đặc biệt này có thể được xem như là các thiết bị lập trình được có thể nhận diện duy nhất 5 đòi quyền sở hữu của đối tượng có thể nhận diện được duy nhất 3. Về bản chất, miễn là một thiết bị lập trình được 5 đòi quyền sở hữu trên đối tượng có thể nhận diện được duy nhất 3 (bằng cách có liên kết 4 hợp lệ), không thiết bị lập trình được 5 nào khác có thể làm vậy. Nếu thiết bị lập trình được 5 với bộ nhận dạng thiết bị duy nhất 8 "A" thiết lập liên kết 4 hợp lệ ở thời gian xác thực 16, liên kết 4 này được lưu trữ trong cơ sở dữ liệu 9. Nếu sau đó thiết bị lập trình được 5 khác với bộ nhận dạng thiết bị duy nhất 8 "B" thiết lập liên kết 4 hợp lệ ở thời gian xác thực 17 sau đó, thiết bị lập trình được được liên kết đến giờ 5 với bộ nhận dạng thiết bị duy nhất 8 "A" bị bỏ liên kết khỏi đối tượng có thể nhận diện được duy nhất 3, tức là, liên kết 4 giữa bộ nhận dạng đối tượng 7 và bộ nhận dạng thiết bị 8 "A" trở nên hợp lệ. Sau đó liên kết 4 mới được thêm vào, tạo thành liên kết 4 hợp lệ giữa bộ nhận dạng đối tượng 7 và bộ nhận dạng thiết bị 8 "B" của thiết bị lập trình được 5 khác. Tùy thuộc vào lĩnh vực ứng dụng, các chiến lược khác có thể được sử dụng. Đối với trường hợp sử dụng "đòi quyền sở hữu", có thể có lợi khi không cho phép thiết lập các liên kết 4 mới, nếu đã có liên kết hợp lệ trong cơ sở dữ liệu 9. Kết quả là, liên kết 4 giữa thiết bị lập trình được 5 được nhận diện bởi "A" (thiết bị lập trình được thứ nhất) và bộ nhận dạng đối tượng 7 có thể cần được vô hiệu hóa/xóa/làm sạch cho giao dịch bởi người dùng của thiết bị lập trình được có thể nhận diện duy nhất được nhận diện bởi "A". Chỉ sau đó, thiết bị lập trình được 5 được nhận diện bởi "B" (thiết bị lập trình được thứ hai) có thể thiết lập liên kết 4 mới với cùng bộ nhận dạng đối tượng 7. Với chế độ này, có thể liên kết duy nhất thiết bị lập trình được 5 qua bộ nhận dạng thiết bị 8 với đối tượng có thể nhận diện được duy nhất 3 một cách ổn

định. Kết quả là, các đặc quyền 2 chỉ được cấp quyền cho thiết bị lập trình được 5 cụ thể, nếu nó "sở hữu" đối tượng có thể nhận diện được duy nhất 3, tức là, nếu có liên kết 4 hợp lệ giữa bộ nhận dạng đối tượng duy nhất 7 và bộ nhận dạng thiết bị 8.

Các liên kết truy nhập giới hạn 4, như được thể hiện trên Fig. 4, cho phép sử dụng hoặc thực hiện đặc quyền 2 chỉ một lần hoặc số lần định trước hữu hạn 19, trong đó một hoặc nhiều đặc quyền 2 được gán cho bộ nhận dạng đối tượng 7 có thể được sử dụng bởi thiết bị lập trình được có thể nhận diện duy nhất 5. Fig. 4 thể hiện chế độ thực thi một lần, trong đó cho chép phép chỉnh một lần sử dụng đặc quyền 2. Liên kết 4 là hợp lệ giữa thời gian xác thực 16, 17 và kết thúc hành động, đặc quyền được yêu cầu cho nó. Liên kết 4 trở nên không hợp lệ ở thời gian 20, 21, hành động, được thực thi dựa trên đặc quyền 2, đã dừng. Một cách tương tự, nếu được phép nhiều lần sử dụng đặc quyền 2, bộ đếm sử dụng có thể được duy trì ở cơ sở dữ liệu 9 trung tâm hoặc phân tán và/hoặc trong chính thiết bị lập trình được 5.

Các liên kết giới hạn thời gian 4, như được thể hiện trên Fig.5, là hợp lệ chỉ cho chu kỳ hợp lệ định trước cụ thể 22 sau khi chúng đã được thiết lập. Trong khi chúng được thiết lập ở thời gian xác thực 16, 17, chúng vẫn hợp lệ trong chu kỳ hợp lệ 22. Trong suốt chu kỳ này, đặc quyền 2 có thể được sử dụng hoặc thực thi thường xuyên như mong muốn, tức là, nói chung nhiều lần 19. Sau chu kỳ hợp lệ 22 đó, liên kết 4 được (tốt hơn là không cần tương tác với thiết bị lập trình được 5 bất kỳ) được thiết lập về không hợp lệ và kết quả là thiết bị lập trình được 5 đánh mất các đặc quyền 2 ở thời gian 23, 24 mà ở đó kết thúc chu kỳ hợp lệ 22. Điều này có thể được thực hiện không đồng bộ bởi thiết bị không đồng bộ (không được chụp), mà giám sát và quản lý danh sách 15 của các liên kết 4 hợp lệ trong danh sách hoặc cơ sở dữ liệu 9 tập trung hoặc phân tán. Nếu danh sách 15 các liên kết hợp lệ được duy trì ở chính thiết bị lập trình được có thể nhận diện duy nhất, dịch vụ này có thể hoạt động ở đó hoặc trên lần thử tiếp theo để sử dụng hoặc thực thi đặc quyền 2, tính vô hiệu hóa của liên kết được dò thấy, chẳng hạn trên các giới hạn về thời gian.

Ngoài ra, quan trọng là lưu ý rằng liên kết giữa đối tượng có thể nhận diện

được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất không nhất thiết là liên kết trực tiếp; thay vào đó liên kết có thể bao gồm các liên kết trung gian được liên kết. Theo phương án thực hiện được ưu tiên, liên kết bao gồm liên kết trung gian thứ nhất giữa đối tượng có thể nhận diện được duy nhất và tài khoản người dùng và liên kết trung gian thứ hai giữa tài khoản người dùng và thiết bị lập trình được có thể nhận diện duy nhất. Trong trường hợp này tài khoản người dùng có chức năng như là trung gian giữa đối tượng có thể nhận diện được duy nhất và thiết bị lập trình được có thể nhận diện duy nhất. Tài khoản người dùng được đăng ký với một hoặc nhiều thiết bị nhận diện được là duy nhất (tức là, các liên kết trung gian thứ hai đã được thiết lập). Đối với thiết lập liên kết, các đặc quyền cần chỉ được "truyền" từ đối tượng có thể nhận diện được duy nhất sang tài khoản người dùng (tức là, thiết lập liên kết trung gian thứ nhất và do vậy hoàn thành liên kết). Mỗi thiết bị lập trình được có thể nhận diện duy nhất, được tạo cấu hình để đại diện tài khoản người dùng, sau đó có thể truy nhập hoặc thực thi các đặc quyền được đăng ký với tài khoản người dùng. Điều này có thể truyền hoặc chia sẻ các đặc quyền từ tài khoản người dùng đến thiết bị lập trình được có thể nhận diện duy nhất khác. Cân nhắc chính ở đây là khả năng mà các thiết bị lập trình được có thể nhận diện duy nhất bị phá bỏ. Kết quả là, các liên kết được thiết lập, có thể được xóa sạch cho giao dịch bởi thiết bị lập trình được có thể nhận diện duy nhất, có thẻ đóng băng, ngay khi thiết bị phá bỏ, đơn giản là không có cách nào tuyên bố rằng các thiết bị khác được phép thiết lập các liên kết mới. Các tài khoản người dùng có thể giúp vượt qua vấn đề này.

Do thực tế là ở cùng thời gian nhiều nhất một thiết bị lập trình được có thể được kết nối với sản phẩm vật lý cụ thể (tạo thành đối tượng có thể nhận diện được duy nhất), xuất hiện nhiều ứng dụng;

- Đòi quyền sở hữu. Nếu một thiết bị lập trình được được kết nối hoặc được liên kết với sản phẩm vật lý, nó "sở hữu" sản phẩm. Kết quả là, nếu thiết bị lập trình được khác kết nối với sản phẩm (bằng cách thiết lập liên kết), thì có nó quyền sở hữu. Về bản chất, phải định nghĩa các quy tắc ở đây, chẳng hạn, thiết bị lập trình được có thể chỉ kết nối với sản phẩm vật lý miễn là không thiết bị lập trình được nào khác được kết nối hoặc kết nối mới tự động triệt tiêu kết nối cũ.

Về mặt kỹ thuật, vùng các liên kết hợp lệ phải được duy trì, tốt hơn là trong cơ sở dữ liệu tập trung.

• Các ưu điểm ngắn hạn. Liên kết giữa sản phẩm vật lý và thiết bị lập trình được chỉ hợp lệ trong chu kỳ thời gian cụ thể trước khi dừng. Thiết bị lập trình được có thể truy nhập nội dung số được đăng ký với sản phẩm vật lý trong chu kỳ thời gian cụ thể. Nếu khoảng thời gian này trôi qua, thì chẳng hạn nó có thể quét lại sản phẩm để có khe thời gian khác. Ví dụ khá dễ sẽ là truy nhập 24h Wi-Fi, được kích hoạt bằng cách quét sản phẩm đóng vai trò là token (thẻ), được đặt trong khu vực giới hạn về mặt vật lý, chẳng hạn, trong phòng khách sạn.

• Token giới hạn về mặt vật lý; Đặc đối tượng vật lý trong khu vực giới hạn về mặt vật lý. Chỉ người được phép vào khu vực giới hạn về mặt vật lý có thể xác thực đối tượng token và do vậy chỉ những người được phép truy nhập dịch vụ số cụ thể (tức là, có đặc quyền truy nhập vào dịch vụ qua liên kết với đối tượng vật lý).

Các trường hợp sử dụng

Đoạn sau nên hỗ trợ hiểu sáng chế và trình bày các trường hợp sử dụng, lợi ích nào có thể có bằng cách sử dụng sáng chế. Có hai phân loại trường hợp sử dụng chính và các lợi ích liên quan. Trước hết, đặc quyền để thực thi hoặc kích hoạt việc thực thi chương trình máy tính đòi hỏi sự có mặt của đối tượng vật lý và thứ hai, rằng cầu nối bảo mật giữa thế giới vật lý và thế giới số có thể được thiết lập, tức là, đối tượng này được đăng ký với đặc quyền truy nhập chương trình máy tính, hoạt động như là biểu diễn dạng số của đối tượng. Một cách trừu tượng, điều này cho phép mạng máy tính liên kết với biểu diễn dạng số của đối tượng phi máy tính.

Phần chứa cấp phép: Đối tượng vật lý nhận diện được duy nhất có thể là phần chứa cấp phép. Xem xét công ty muốn phân phối các sản phẩm của mình không phải ở dạng vật lý, mà thay vào đó phân phối nguyên liệu thô và cấp phép cho người mua nguyên liệu thô thay đổi hình dạng của nó. Cụ thể là, xem xét mực 3D. Nếu công ty bán mực 3D, bao bì mực (=đối tượng có thể nhận diện được duy nhất) có thể được trang bị bằng thiết bị bảo mật không sao chép được

6 và bộ nhận dạng đối tượng 7. Chẳng hạn, nếu máy in 3D (hoặc máy tính được gắn với nó) được tạo cấu hình để là thiết bị lập trình được 5 theo sáng chế, bao bì mực có thể truyền giấp phép để truy nhập (và in) các mẫu 3D cụ thể (=đặc quyền). Sau đó, người mua loại mực cụ thể có thể truy nhập các mẫu này, được nhận diện từ bộ nhận dạng đối tượng 7. Điều này có thể bảo vệ nhãn hiệu, đối với chất liệu mực chất lượng cao cụ thể với các mẫu 3D cụ thể bị nhái với mực chất lượng thấp hơn (rẻ hơn). Kết quả là, các mẫu 3D chỉ truy nhập được với mực so khớp. Trường hợp sử dụng này có thể được làm thích ứng với trường hợp sử dụng bất kỳ, trong đó nội dung số cụ thể, chẳng hạn chương trình máy tính, nên chỉ truy nhập được kết hợp với đối tượng vật lý cụ thể. Ví dụ minh họa khác có thể là bán các mặt hàng người hâm hộ vật lý, chẳng hạn gươm có trong trò chơi máy tính, trong đó người mua mặt hàng vật lý có thể liên kết người dùng hoặc nhân vật của mình trong trò chơi máy tính (chương trình máy tính) với đối tượng vật lý nhận diện được duy nhất và do vậy sẽ có đặc quyền sử dụng biểu diễn dạng số của thanh gươm này trong trò chơi.

Sáng chế đề xuất khả năng đòi quyền sở hữu số của đối tượng vật lý. Kết quả là, truyền quyền sở hữu số có thể được gắn với truyền đối tượng vật lý. Một cách lần lượt, các giao dịch số có thể được kiểm chứng bằng cách kiểm tra trạng thái quyền sở hữu số hiện tại của đối tượng. Ví dụ nổi bật là xe đạp hoặc ôtô cũ (đối tượng vật lý). Các đối tượng đó là các đối tượng thường xuyên cho kẻ trộm và thường người mua xe đạp hoặc ô tô cũ không thể báo liệu có phải đang mua xe ăn cắp hay không, tức là, người bán không phải là chủ sở hữu hợp pháp, hoặc liệu người bán có hợp pháp khi bán ôtô này không. Trong trường hợp này có thể có lợi, nếu người mua ô tô mới từ nhà máy đòi quyền sở hữu theo sáng chế. Người chủ hợp pháp liên kết thiết bị lập trình được có thể nhận diện duy nhất 5 của mình (hoặc tài khoản liên quan đến thiết bị lập trình được có thể nhận diện duy nhất) với đối tượng vật lý nhận diện được duy nhất. Nếu anh ta chuẩn bị bán ôtô của mình, thì anh ta có thể giải phóng quyền sở hữu đã đòi, tức là, anh ta vô hiệu hóa liên kết với thiết bị lập trình được có thể nhận diện duy nhất 5. Sau đó trước khi mua, người dùng được thông báo đòi quyền sở hữu của ôtô (đối tượng vật lý) với thiết bị lập trình được có thể nhận diện duy nhất 5 của mình, tức là,

anh ta cố gắng liên kết thiết bị lập trình được 5 của mình với đối tượng vật lý mà anh ta chuẩn bị mua. Nếu không thể đòi quyền sở hữu, tức là, do vẫn có liên kết hợp lệ giữa đối tượng vật lý mong muốn và thiết bị lập trình được có thể nhận diện duy nhất 5 khác, thì điều này có thể chỉ báo rằng phiên này không hợp pháp, tức là, ôtô này có thể là ôtô ăn cắp. Trong thiết lập mong muốn, tức là, việc tất cả ôtô hoặc ít nhất tất cả ôtô của nhãn cụ thể, được trang bị theo sáng chế, điều này nghĩa là lịch sử sở hữu liên tục có thể thu được. Miễn là xe mới vẫn đòi quyền sở hữu, tức là không có liên kết hợp lệ nào được đăng ký, về mặt tiềm năng điều này có thể tăng đáng kể khó khăn khi thỏa thuận hàng ăn cắp, do giao dịch hàng vật lý có thể dễ được kiểm tra bởi người mua trước khi thực hiện giao dịch.

Như đối với các giao dịch, như là nhật ký giao dịch, lịch sử sở hữu đơn giản có thể được duy trì hoặc giao dịch khác tạo thành, mà đảm bảo tính toàn vẹn, có thể được sử dụng làm cơ sở dữ liệu để lưu trữ các liên kết, chẳng hạn các chuỗi khối, cũng có thể được phân tán giữa nhiều thiết bị lập trình được 5 thay cho cơ sở dữ liệu tập trung (tin cậy) giữ các bản ghi.

Ví dụ khác (không được chụp) có thể là xây dựng các dịch vụ thanh toán trực tuyến khác trong mua sắm trực tuyến. Lợi ích lớn nhất ở đây lại là cho giao dịch giữa người mua và người bán không tin cậy hoặc ngược lại, tức là, các giao dịch đồ cũ. Cơ sở dữ liệu 9 đóng vai trò là trung gian tin cậy trong trường hợp này. Người bán, sở hữu hợp pháp đối tượng có thể nhận diện được duy nhất 3 qua liên kết 4 hợp lệ, thiết lập liên kết 4 ở trạng thái báo hiệu rằng anh ta sẵn sáng truyền đối tượng. Bộ nhận dạng giao dịch có thể được cấp, mà anh ta có thể truyền nhờ phương tiện viễn thông đến người mua đối tượng. Sau đó người mua có thể ký quỹ tiền ở trung gian tin cậy, được liên kết với thiết bị lập trình được 5 của người mua và bộ nhận dạng giao dịch. Sau đó, trung gian tin cậy báo hiệu người bán rằng tiền đã ký quỹ, cho phép anh ta thực sự chuyển đối tượng vật lý đến người bán, chẳng hạn, qua dịch vụ bưu điện. Ở điểm này, tiền ký quỹ ở bên ủy thác tin cậy cũng như chính xác có một thiết bị lập trình được có thể nhận diện duy nhất được đăng ký trước, mà có thể đòi quyền sở hữu của đối tượng vật lý. Tất cả các liên kết khác sẽ không được chấp nhận bởi trung gian tin cậy, tức

là, bên thứ ba không hợp pháp không thể đòi quyền sở hữu. Nếu đối tượng vật lý được nhận bởi người mua, anh ta có thể kiểm tra điều kiện và nếu thỏa mãn, anh ta có thể đòi quyền sở hữu, tức là, anh ta liên kết thiết bị lập trình được có thể nhận diện duy nhất 5 của mình với bộ nhận dạng đối tượng 7. Việc thiết lập liên kết 4 mới kích hoạt trung gian tin cậy chuyển tiền đặt cọc cho người bán và giao dịch hoàn thành. Nếu người mua không hài lòng với tình trạng của hàng nhận được, anh ta có thể gửi lại cho người bán. Nếu người bán nhận được yêu cầu đòi bồi thường, anh ta có thể xác nhận việc nhận hàng bằng cách đòi lại quyền sở hữu. Điều này khiến trung gian tin cậy, tức là, cơ sở dữ liệu 9, chuyển lại tiền đặt cọc cho người mua và người bán lại hoàn toàn tự do loại bỏ đối tượng vật lý. Thiết lập này có thể được truyền đến các quá trình mua/thanh toán bất kỳ, trong đó hai nhà thầu không liên lạc trực tiếp, tức là, giao dịch này không thể bị hủy bỏ hoặc kiểm chứng ngay lập tức.

Các trường hợp sử dụng khác xuất hiện, có thể thông qua việc đòi hỏi độ lân cận vật lý giữa thiết bị lập trình được có thể nhận diện duy nhất và đối tượng. Do vậy, các ràng buộc vật lý được áp dụng cho đối tượng đồng thời ràng buộc việc sử dụng hoặc thực thi các đặc quyền được gán. Chẳng hạn, việc phát lại buổi hòa nhạc trực tiếp nên truy nhập được cho người có mặt trong khán giả. Điều này có thể được thực hiện bằng cách đặt đối tượng không di chuyển trong khán phòng, trong đó chỉ người mua vé mới được vào. Sau đó người ta có thể liên kết các thiết bị lập trình được có thể nhận diện duy nhất 5 của họ, tức là, điện thoại thông minh, với đối tượng không di chuyển qua bộ nhận diện của đối tượng 7. Ngay khi liên kết 4 được tạo, thiết bị lập trình được 5 cụ thể được liên kết với đối tượng không di chuyển có thể nhận diện được duy nhất 3 có thể truy nhập bản ghi của buổi hòa nhạc trực tiếp (đặc quyền truy nhập tệp tin hoặc dòng), trong khi không thể truy nhập bản ghi từ thiết bị khác bất kỳ, không thể được liên kết với đối tượng không di chuyển do điều khiển truy nhập vật lý. Trường hợp sử dụng này có thể được khái quát hóa lên ứng dụng bất kỳ, trong đó độ lân cận vật lý giữa thiết bị lập trình được có thể nhận diện duy nhất 5 và đối tượng vật lý có thể cho phép thiết bị lập trình được có thể nhận diện duy nhất 5 thực thi đặc quyền (chẳng hạn, thực thi chương trình máy tính, truy nhập tệp tin hoặc cơ sở dữ liệu, hoặc

phát nhạc hoặc dòng viđeo). Kết quả là, chẳng hạn, thực thi chương trình máy tính có thể bị giới hạn bằng cách sử dụng các biện pháp giới hạn vật lý đến đối tượng kích hoạt. Điều này cũng có thể được sử dụng để kích hoạt chương trình máy tính, do nó yêu cầu rằng ít nhất đối tượng vật lý, đóng vai trò là khóa, được truyền để cho phép chương trình máy tính được thực thi trên thiết bị lập trình được có thể nhận diện duy nhất 5 cụ thể. Kết quả là, sáng chế có thể được tận dụng để chống lại ăn cắp phần mềm bằng cách sử dụng token vật lý không sao chép được để kích hoạt phần mềm.

Các trường hợp sử dụng bổ sung của sáng chế:

• Xác thực các thanh toán thẻ ghi nợ, bằng cách thu được đặc quyền sử dụng thẻ ghi nợ (đối tượng có thể nhận diện được duy nhất) theo sáng chế:

Khe mạnh hơn mã bảo mật ba số và thủ tục kiểm chứng "hợp lệ cho đến khi", vốn là hiện đại nhất trong nhiều giải pháp thanh toán ngày nay. Việc ngăn ngừa sử dụng không hợp pháp thẻ ghi nợ (mà không có thẻ ghi nợ thực sự bị đánh cắp từ chủ thẻ), hiện tại là hoàn toàn có khả năng bằng cách chỉ biết số.

• Giới hạn truy nhập vật lý (chẳng hạn, do khóa riêng tư, mở khóa tài liệu trong đám mây):

Người dùng cần có khóa vật lý (đối tượng có thể nhận diện được duy nhất) gần với thiết bị lập trình được có thể nhận diện duy nhất của họ để có các quyền dạng số cụ thể, các tài liệu truy nhập v.v.. Điều này có thể có ích để chống lại sự miễn cưỡng lưu trữ tài liệu trong đám mây, do các tài liệu có thể chỉ được truy nhập cho các thiết bị gần với token vật lý. Miễn là token vật lý này, chẳng hạn ở trong két, không ai có thể mở tài liệu; điều này tương ứng với trường hợp sử dụng buổi hòa nhạc nêu trên chi tiết hơn.

• Quản lý các quyền dạng số vật lý /phương tiện truy nhập khi token vật lý, tức là, đối tượng có thể nhận diện được duy nhất, có mặt. Chẳng hạn, chiến lược tiếp thị có thể là: người dùng có thể truy nhập dịch vụ (chụp ảnh và đựng nó trên vỏ đồ uống) và mỗi lần họ quét cùng vỏ đồ uống, họ có thể thấy lại ảnh (thu được đặc quyền để truy nhập tệp tin ảnh). Mà không có vỏ đồ uống, họ không thể thấy lại ảnh. Do vậy, ảnh (= bộ nhớ, cảm giác) được "đựng ở" đối tượng vật lý, tăng cường giá trị cảm xúc của đối tượng.

- Quyền hỗ trợ hoặc tính hợp lệ của hợp đồng hỗ trợ

Người dùng chúng tỏ quyền (đặc quyền) để tận hưởng dịch vụ chẳng hạn hỗ trợ/bảo trì phần mềm v.v. bằng cách chứng tỏ họ mua sản phẩm gốc. Tức là, họ có thể thu được hỗ trợ với thiết bị lập trình được có thể nhận diện duy nhất chỉ nếu gần như là sản phẩm dốc hoặc bao bì sản phẩm (đối tượng có thể nhận diện được duy nhất).

- Các tham số máy móc cho các ứng dụng công nghiệp

Khi mua các công cụ gốc, tức là, các chi tiết đệm cacbua cho máy khoan v.v., quét bao bì cho phép người dùng truy nhập các tham số máy tối ưu chẳng hạn tốc độ khoan v.v. và/hoặc máy tự điều chỉnh tự động. Điều này tương tự trường hợp sử dụng mực 3D nêu trên.

Fig.6 minh họa phương pháp theo phương án thực hiện được ưu tiên. Nó thể hiện các nguyên lý cơ bản được bao gồm khi người dùng muốn thực hiện "Hoạt động A" lấy làm ví dụ với thiết bị lập trình được có thể nhận diện duy nhất của nó. Hoạt động này có thể chẳng hạn là việc thực thi chương trình máy tính, truy nhập tài liệu v.v.. Hoạt động này đòi hỏi người dùng có đặc quyền thực hiện nó (tức là, hoạt động này áp dụng các giới hạn truy nhập với thiết bị lập trình được có thể nhận diện duy nhất thực hiện nó). Ở bước thứ nhất 101, bộ nhận dạng đối tượng duy nhất 7 và thiết bị bảo mật không sao chép được 6 được chụp bởi thiết bị lập trình được 5, tức là, ít nhất một ảnh của bộ nhận dạng đối tượng duy nhất và của thiết bị bảo mật không sao chép được 6 được bắt, chẳng hạn, với camera của thiết bị lập trình được 5. Ở bước tiếp theo 102, thiết bị bảo mật không sao chép được 6 được xác thực dựa trên dữ liệu được bắt. Cụ thể là, biểu diễn dạng số được trích rút từ ít nhất ảnh được chụp. Một khả năng xác thực thiết bị bảo mật không sao chép được 6 là: để yêu cầu bước 103 tham chiếu của biểu diễn dạng số của thiết bị bảo mật không sao chép được từ cơ sở dữ liệu bằng cách sử dụng bộ nhận dạng đối tượng duy nhất (tức là, truy vấn cơ sở dữ liệu cho các biểu diễn dạng số được liên kết với bộ nhận dạng đối tượng duy nhất); để trích rút bước 104 các đặc tính riêng biệt của thiết bị bảo mật không sao chép được 6 từ ảnh được chụp, xác định biểu diễn dạng số của thiết bị bảo mật không sao chép được 6 và so sánh biểu diễn dạng số với tham chiếu được yêu cầu. Nếu so

sánh này thành công bước 105 (tức là, so sánh này xác định so khớp), độ lân cận vật lý giữa thiết bị lập trình được có thể nhận diện duy nhất và đối tượng có thể nhận diện được duy nhất được đảm bảo. Một cách tùy chọn, các điều kiện trước khác (chẳng hạn việc vị trí địa lý hoặc các phần đọc bộ cảm biến khác của thiết bị lập trình được trong khoảng chấp nhận được định trước) có thể được thực hiện ở bước 106 trước khi xác thực thiết bị bảo mật không sao chép được. Nếu thiết bị bảo mật không thể được xác thực, thủ tục này bị hủy bỏ mà không thiết lập liên kết mới. Sau đó nó được kiểm tra ở bước 107 liệu liên kết mới giữa đối tượng có thể nhận diện được duy nhất 3 và thiết bị lập trình được có thể nhận diện duy nhất 5 có được phép, tức là có thể. Chẳng hạn, điều này có thể không đúng ở bước 106 nếu chỉ một thiết bị có thể được đăng ký với đối tượng và đã là liên kết hợp lệ. Trong ví dụ này, để xác định liệu liên kết mới có được phép không, các chế độ liên kết được phép được yêu cầu ở bước 108 từ cơ sở dữ liệu bằng cách sử dụng bộ nhận dạng đối tượng duy nhất 7. Chế độ liên kết xác định chính sách liên kết, chẳng hạn, các liên kết ổn định, các liên kết tạm thời, các liên kết giới hạn số lượng, các liên kết một lần sử dụng, v.v.. Nếu liên quan đến chế độ liên kết được xác định, các liên kết hiện tại bao gồm bộ nhận dạng đối tượng duy nhất 7 được yêu cầu ở bước 109 từ cơ sở dữ liệu. Dựa trên chế độ liên kết và một cách tùy chọn, kết quả của yêu cầu này, được xác định ở bước 110 liệu liên kết mới có được phép không. Trong trường hợp liên kết được phép ở bước 111, ở bước tiếp theo 112 liên kết được thiết lập bằng cách lưu trữ liên kết giữa bộ nhận dạng thiết bị duy nhất 8 và bộ nhận dạng đối tượng duy nhất 7 trong cơ sở dữ liệu 9. Các đặc quyền 2 được liên kết với bộ nhận dạng đối tượng duy nhất 7 hiện cũng khả dụng cho thiết bị lập trình được có thể nhận diện duy nhất 5. Nếu người dùng cố gắng thực hiện hành động A, tất cả các đặc quyền được liên kết với thiết bị lập trình được có thể nhận diện duy nhất 5 được thẩm định ở bước 113, tức là liệu ít nhất một đặc quyền có phải là quyền thực hiện hành động A. Chẳng hạn, dựa trên tất cả các liên kết 4 bao gồm bộ nhận dạng thiết bị duy nhất của thiết bị lập trình được liên kết với các bộ nhận dạng đối tượng duy nhất và các đặc quyền được liên kết với các bộ nhận dạng đối tượng duy nhất được liên kết được xác định ở bước 114. Sau đó các đặc quyền được liên kết được

truyền ở bước 115 đến thiết bị lập trình được và được xác định liệu chúng bao gồm đặc quyền thực hiện hành động A. Nếu điều này đúng ở bước 116, thì hành động A có thể được thực thi ở bước 117 bởi thiết bị lập trình được 5, chẳng hạn, chương trình máy tính được chạy hoặc dịch vụ hoặc hành động được kích hoạt qua thiết bị lập trình được có thể nhận diện duy nhất. Trong trường hợp một trong các bước kiểm tra 102, 107, 113 thất bại, hành động A không thể được thực thi và thiết bị lập trình được có thể nhận diện duy nhất có thể hiển thị ở bước 118 thông điệp hoặc mã lỗi chỉ báo phần sai hoặc tại sao hành động A không thể được thực hiện.

YÊU CẦU BẢO HỘ

1. Hệ thống (1) quản lý các đặc quyền (2), trong đó các đặc quyền (2) được gán cho các đối tượng có thể nhận diện được duy nhất và liên kết (4) giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) được thiết lập, trong đó liên kết được thiết lập (4) cho phép thiết bị lập trình được có thể nhận diện duy nhất (5) tận dụng ít nhất một phần của các đặc quyền (2) được gán cho đối tượng có thể nhận diện được duy nhất (3) và trong đó liên kết (4) được thiết lập với tập các điều kiện trước, trong đó ít nhất điều kiện trước về độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) được kiểm chứng và đối tượng có thể nhận diện được duy nhất (3) bao gồm thiết bị bảo mật không sao chép được (6), mà được đăng ký với đối tượng có thể nhận diện được duy nhất (3) và có thể được sử dụng để kiểm chứng độ lân cận vật lý giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) bằng cách xác thực thiết bị bảo mật không sao chép được (6) nhờ phương tiện xác thực quang học, trong đó ít nhất một phần của quá trình xác thực được thực hiện bởi thiết bị lập trình được có thể nhận diện duy nhất (5).

2. Hệ thống (1) theo điểm 1, khác biệt ở chỗ, một hoặc nhiều nhóm các điều kiện trước bổ sung được kiểm chứng để thiết lập liên kết, nhóm các điều kiện trước bổ sung này bao gồm: vị trí địa lý của thiết bị lập trình được có thể nhận diện duy nhất (5) trong khu vực địa lý được định trước; hoặc dữ liệu khác mà có thể được truy xuất từ các bộ cảm biến hoặc bộ nhớ của thiết bị lập trình được có thể nhận diện duy nhất, trong đó liên kết (4) chỉ có thể được thiết lập, nếu dữ liệu này tương ứng với các giá trị được tiền cấu hình cụ thể.

3. Hệ thống (1) theo điểm 1 hoặc 2, khác biệt ở chỗ, các đặc quyền (2) được lưu trữ trong cơ sở dữ liệu tập trung hoặc phân tán (9).

4. Hệ thống (1) theo một trong các điểm 1 đến 3, khác biệt ở chỗ, đặc quyền (2) là quyền truy nhập chương trình máy tính, mà có thể được thực thi trên thiết bị lập trình được (5), hoặc quyền kích hoạt thực thi chương trình máy tính trên thiết bị thứ ba, cụ thể là trên máy chủ, với thiết bị lập trình được có thể nhận diện duy nhất (5) và/hoặc quyền để thiết lập liên kết (4).

5. Hệ thống (1) theo một trong các điểm 1 đến 4, khác biệt ở chỗ, đặc quyền (2) cấp truy nhập vào cơ sở dữ liệu và cho phép thay đổi các phép gán đặc quyền.
6. Hệ thống (1) theo một trong các điểm 1 đến 5, khác biệt ở chỗ, các liên kết được thiết lập (4) được ghi nhận trong cơ sở dữ liệu phân tán hoặc tập trung (9).
7. Hệ thống (1) theo điểm 6, khác biệt ở chỗ, cơ sở dữ liệu (9) bao gồm cấu trúc chuỗi khối.
8. Hệ thống (1) theo một trong các điểm 1 đến 7, khác biệt ở chỗ, thiết bị bảo mật không sao chép được (6) bao gồm cấu trúc ba chiều có phân tán ngẫu nhiên của các đặc tính quang học phụ thuộc phối cảnh được đăng ký với bộ nhận dạng đối tượng (7) và thiết bị lập trình được có thể nhận diện duy nhất (5) bao gồm camera có thể được sử dụng để chụp ít nhất hai ảnh của thiết bị bảo mật không sao chép được (6) từ ít nhất hai phối cảnh khác nhau hoặc với hai điều kiện chiếu sáng khác nhau.
9. Hệ thống (1) theo một trong các điểm 1 đến 8, khác biệt ở chỗ, đối tượng có thể nhận diện được duy nhất (3) bao gồm bộ nhận dạng đối tượng duy nhất (7), trong đó bộ nhận dạng đối tượng (7) được mã hóa ở định dạng người đọc được hoặc máy đọc được, cụ thể là dưới dạng số dạng số hoặc số chữ cái hoặc dưới dạng mã vạch hoặc mã hai chiều.
10. Hệ thống (1) theo một trong các điểm 1 đến 9, khác biệt ở chỗ, liên kết giữa đối tượng có thể nhận diện được duy nhất (3) và thiết bị lập trình được có thể nhận diện duy nhất (5) bao gồm hai hoặc nhiều liên kết trung gian được kết nối, cụ thể là liên kết trung gian thứ nhất giữa đối tượng có thể nhận diện được duy nhất (3) và tài khoản người dùng và liên kết trung gian thứ hai giữa tài khoản người dùng và thiết bị lập trình được có thể nhận diện duy nhất (5).
11. Phương pháp thu thập các đặc quyền (2) với thiết bị lập trình được (5) có bộ nhận dạng thiết bị duy nhất (8), phương pháp bao gồm các bước:

– chụp ít nhất hai ảnh bằng thiết bị lập trình được (5), trong đó ít nhất một ảnh chụp bộ nhận dạng đối tượng duy nhất (7) của đối tượng (3) và ít nhất hai ảnh chụp thiết bị bảo mật không sao chép được (6) của đối tượng (3);

– xác thực thiết bị bảo mật không sao chép được (6) dựa trên ít nhất hai ảnh nêu trên;

– nếu tất cả các điều kiện trước của tập các điều kiện trước được đáp ứng, thì thiết lập liên kết (4) giữa bộ nhận dạng thiết bị duy nhất (8) và bộ nhận dạng đối tượng duy nhất (7), trong đó tập các điều kiện trước bao gồm ít nhất điều kiện trước mà thiết bị bảo mật không sao chép được (6) có thể được xác thực,

trong đó một hoặc nhiều đặc quyền (2) được định trước và liên kết với bộ nhận dạng đối tượng duy nhất (7),

trong đó ít nhất một phần của một hoặc nhiều đặc quyền (2) được cấp cho thiết bị lập trình được (5) bất kỳ có bộ nhận dạng thiết bị duy nhất (8) được liên kết với bộ nhận dạng đối tượng duy nhất (7).

12. Phương pháp theo điểm 11, khác biệt ở chỗ, việc xác thực thiết bị bảo mật không sao chép được (6) bao gồm các bước:

– trích rút biểu diễn dạng số của một hoặc nhiều dấu hiệu bảo mật quang học từ ít nhất hai ảnh nêu trên;

– so sánh biểu diễn dạng số này với tham chiếu;

– xác thực thiết bị bảo mật không sao chép được (6) nếu biểu diễn dạng số so khớp tham chiếu.

13. Phương pháp theo điểm 12, khác biệt ở chỗ, việc xác thực thiết bị bảo mật không sao chép được (6) bao gồm bước:

– thu được tham chiếu từ cơ sở dữ liệu (9), tốt hơn là bằng cách truy vấn cơ sở dữ liệu (9) với bộ nhận dạng đối tượng duy nhất được chụp (7).

14. Phương pháp theo một trong các điểm 11 đến 13, khác biệt ở chỗ:

– trước khi thiết lập liên kết (4) giữa bộ nhận dạng thiết bị duy nhất (8) và bộ nhận dạng đối tượng duy nhất (7), xác định liệu bộ nhận dạng đối tượng duy nhất (7) đã được liên kết với một hoặc nhiều bộ nhận dạng thiết bị duy nhất khác nhau (8) không;

– thiết lập liên kết (4) giữa bộ nhận dạng thiết bị duy nhất (8) và bộ nhận dạng đối tượng duy nhất (7) chỉ nếu bộ nhận dạng đối tượng duy nhất (7) không được liên kết với bộ nhận dạng thiết bị duy nhất khác nhau (8) bất kỳ.

1/6

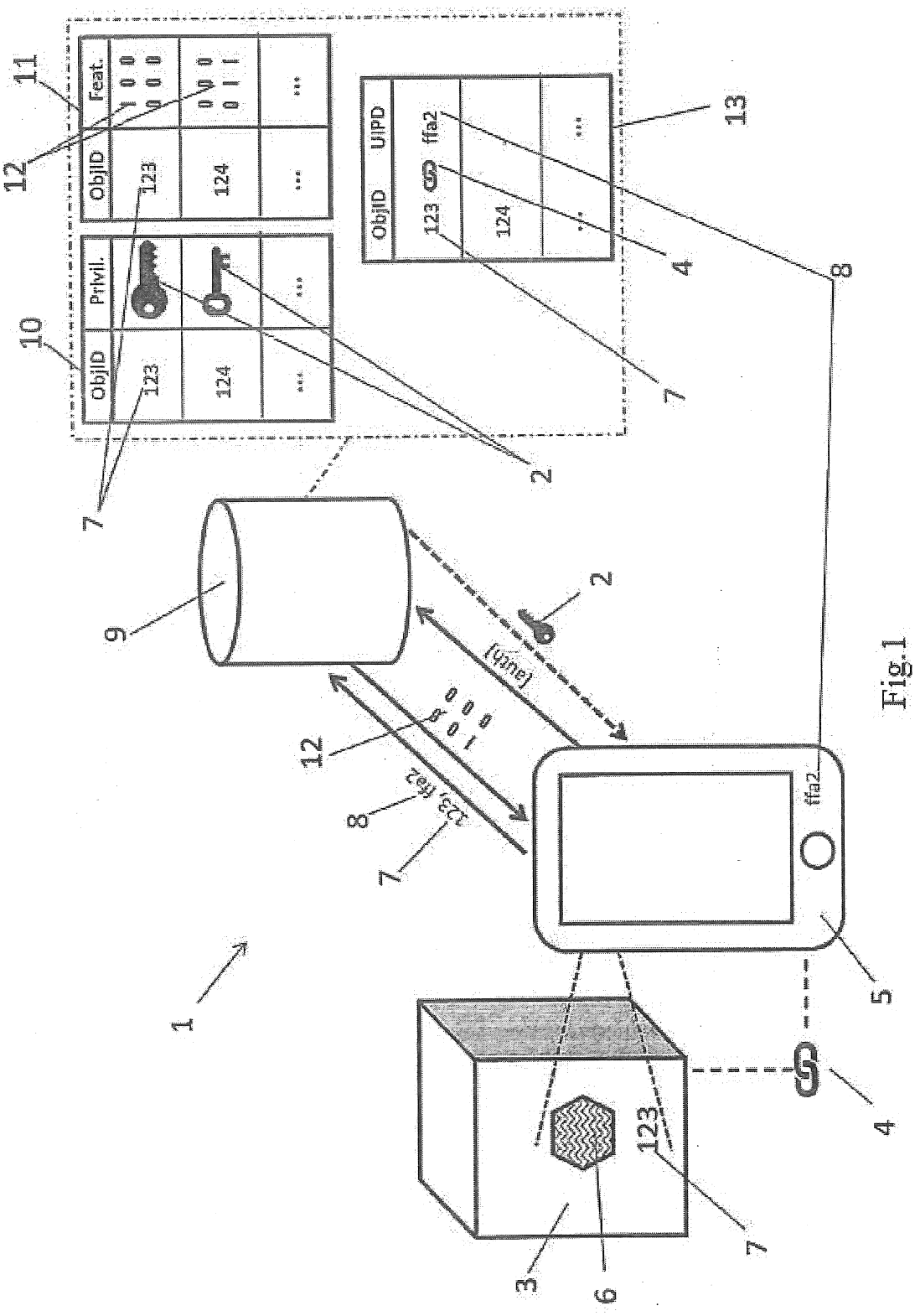

11
12
Feat.
ObjID
123
124
UIPD
ffa2
13
4
8
10
Privil.
7
2
9
[ujme]
12
8
7
1
5
3
6
123

Fig.1

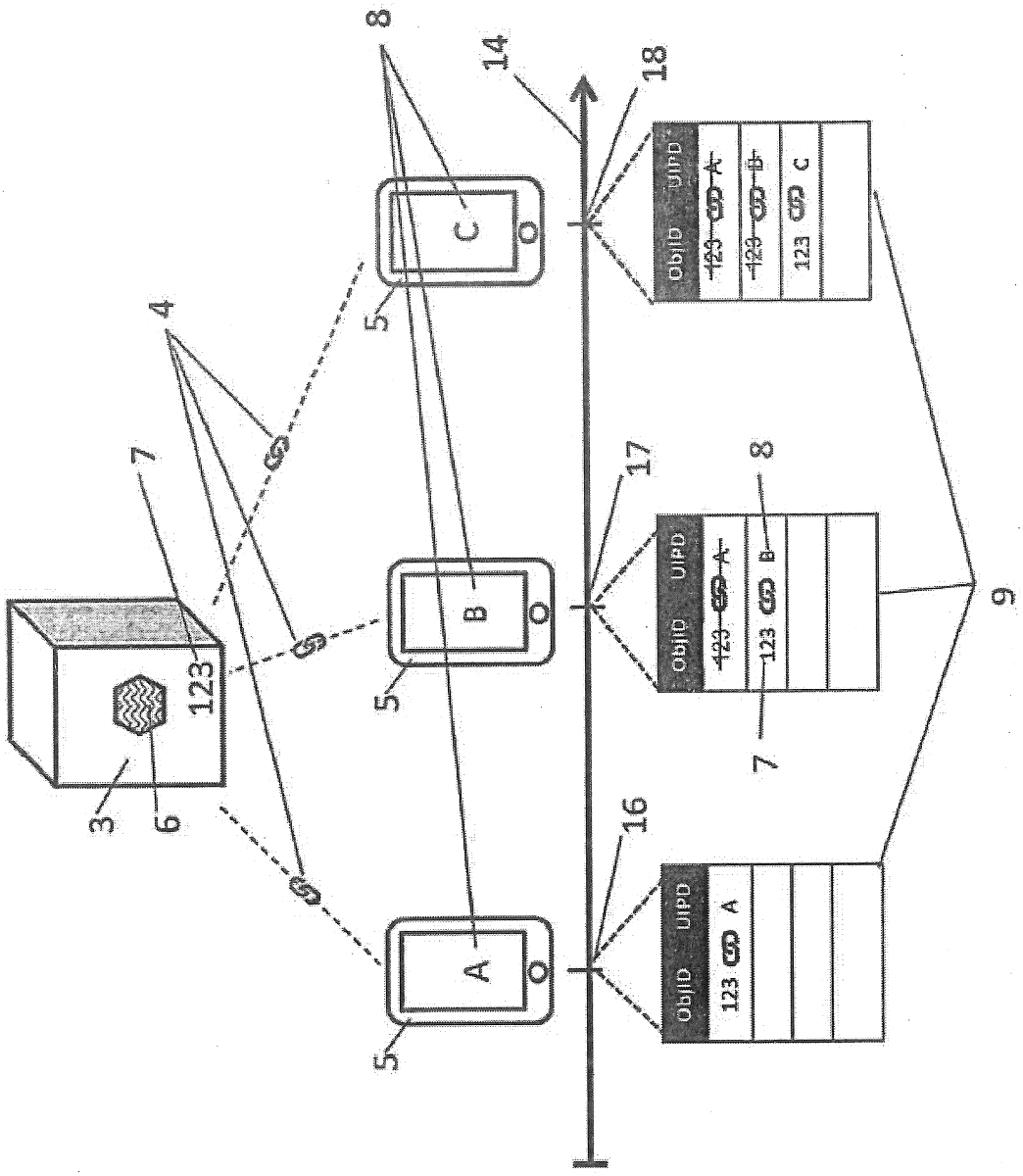

8
14
18
C
5
4
7
123
3
6
B
5
17
8
9
7
A
5
16
ObjID
UIPD
123
A
123
B
123
C
ObjID
UIPD
123
A
123
B
ObjID
UIPD
123
A

Fig.2

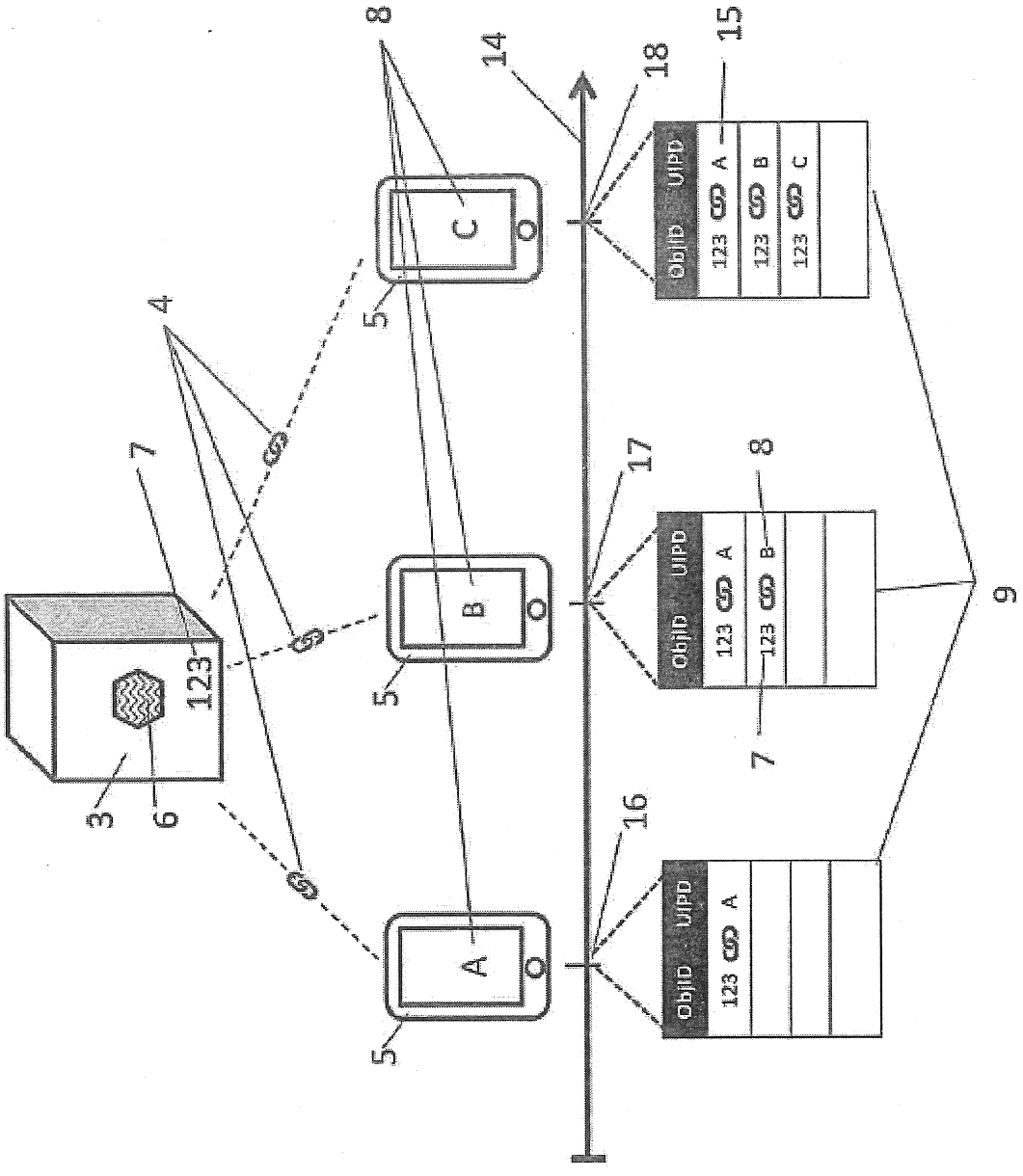


Fig.3

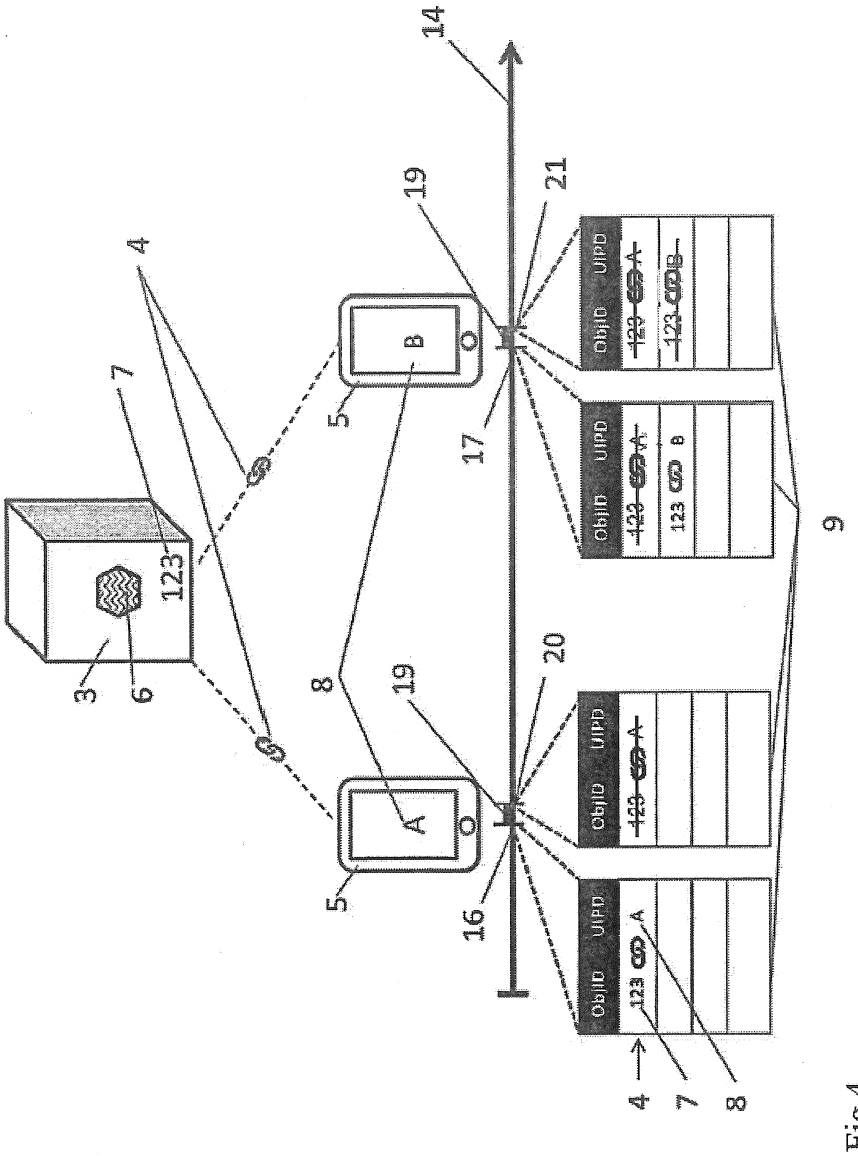


Fig.4

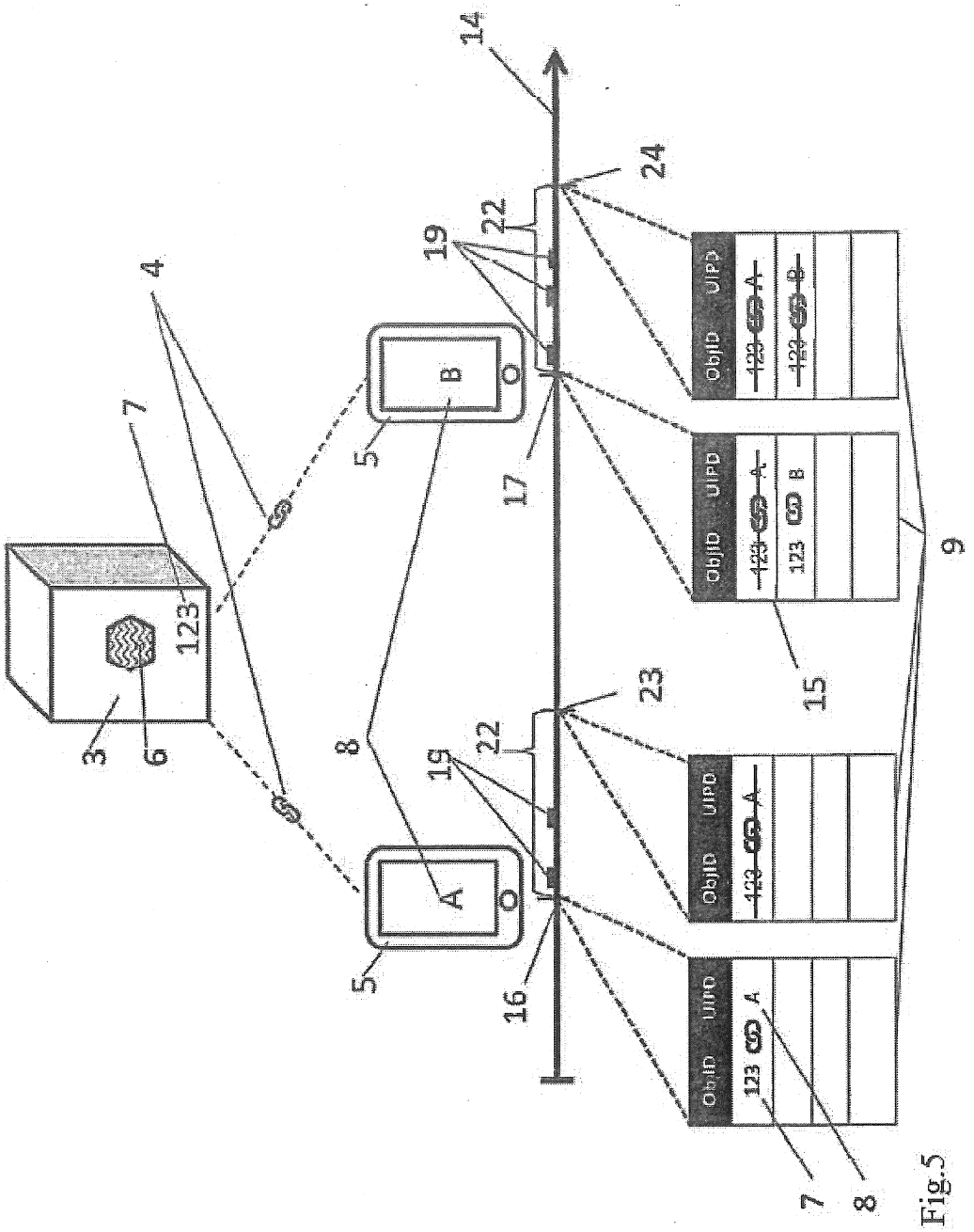


Fig.5

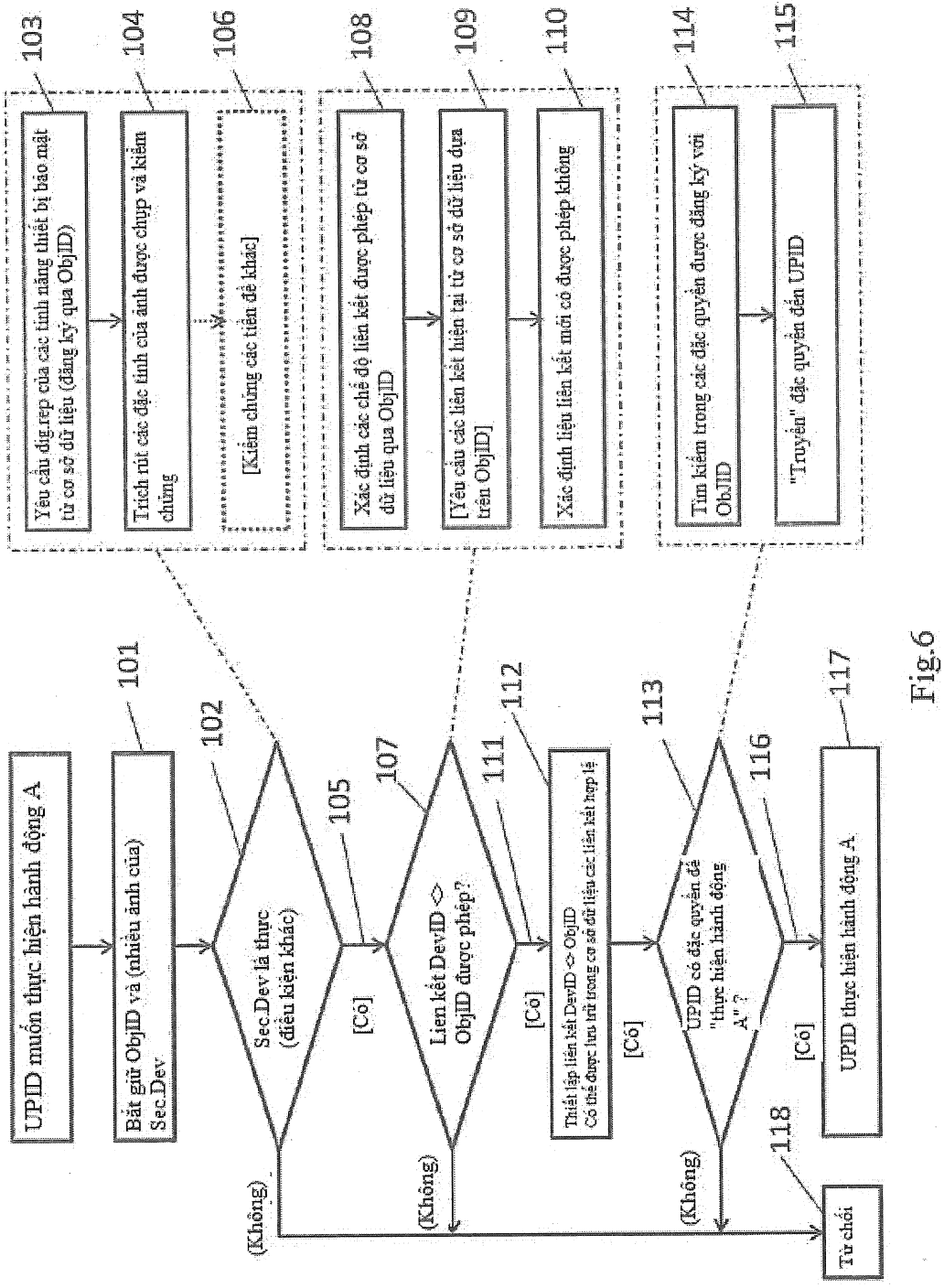

UPID muốn thực hiện hành động A
101
Bắt giữ ObjID và (nhiều ảnh của) Sec.Dev
102
Sec.Dev là thực (điều kiện khác)
(Không)
[Có]
105
Liên kết DevID <> ObjID được phép?
107
(Không)
[Có]
111
Thiết lập liên kết DevID <> ObjID
Có thể được lưu trữ trong cơ sở dữ liệu các liên kết hợp lệ
112
[Có]
113
UPID có đặc quyền để "thực hiện hành động A" ?
116
(Không)
[Có]
117
UPID thực hiện hành động A
118
Từ chối
103
Yêu cầu đọc rep của các tính năng thiết bị bảo mật từ cơ sở dữ liệu (đăng ký qua ObjID)
104
Trích rút các đặc tính của ảnh được chụp và kiểm chứng
106
[Kiểm chứng các tiền đề khác]
108
Xác định các chế độ liên kết được phép từ cơ sở dữ liệu qua ObjID
109
[Yêu cầu các liên kết hiện tại từ cơ sở dữ liệu dựa trên ObjID]
110
Xác định liệu liên kết mới có được phép không
114
Tìm kiếm trong các đặc quyền được đăng ký với ObjID
115
"Truyền" đặc quyền đến UPID

Fig.6