(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) **1-0031865**

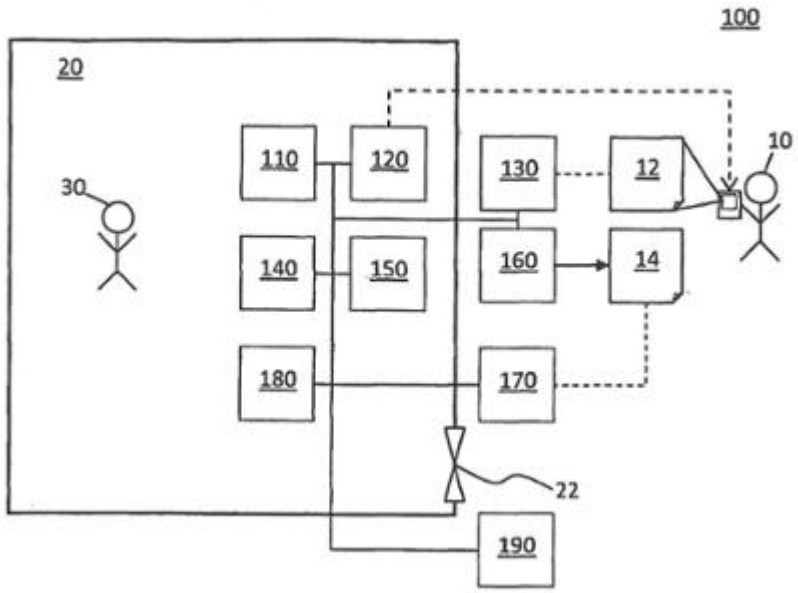
(51)[7] **G05B 19/00**; H04M 11/00

(13) **B**

(21) 1-2017-00254
(22) 25/06/2014
(86) PCT/SG2014/000302 25/06/2014
(87) WO 2015/199609 30/12/2015
(45) 25/05/2022 410
(43) 25/04/2017 349A
(73) CONCORDE ASIA PTE. LTD. (SG)
3 Ang Mo Kio Street 62, #07-12 LINK@AMK Singapore 569139, Singapore
(72) CHUA, Swee Kheng (SG).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP KIỂM SOÁT AN NINH

(57) Sáng chế đề cập đến phương pháp để cấp phép vào khu tòa nhà cho khách. Phương pháp kiểm soát an ninh bao gồm bước xác định nhãn nhận dạng, truyền nhãn nhận dạng đến khách, quét nhãn nhận dạng của khách, xác thực nhãn nhận dạng, tạo tín hiệu chấp thuận khi xác thực chắc chắn được nhãn nhận dạng, phân phát token nhận dạng cho khách khi nhận tín hiệu chấp thuận, quét token nhận dạng của khách, và xác thực token nhận dạng để cấp phép vào khu tòa nhà cho khách. Sáng chế còn đề cập đến hệ thống kiểm soát an ninh áp dụng phương pháp kiểm soát an ninh này.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống kiểm soát an ninh được tạo cấu hình để cấp phép vào khu tòa nhà cho khách và phương pháp kiểm soát an ninh của hệ thống này.

Tình trạng kỹ thuật của sáng chế

Trong các khu tòa nhà cần chức năng an ninh thì thường sẽ có nhân viên an ninh ở vị trí nhất định, ví dụ lối vào tòa nhà, quầy lễ tân, sân bốc xếp hàng, lối vào nơi đỗ xe v.v. của khu tòa nhà. Thông thường, có ít nhất một nhân viên bảo vệ/nhân viên hướng dẫn ở vị trí để kiểm tra khách mà sẽ sử dụng một số hình thức nhận dạng để đổi các thẻ an ninh để vào khu tòa nhà.

Trong một số trường hợp, mức độ kiểm tra an ninh là tương đối thấp. Việc kiểm tra khách có thể không được thực hiện đúng do các yếu tố con người. Như vậy, quy trình đăng ký ở vị trí an ninh có thể có ý nghĩa không đáng kể hoặc không có ý nghĩa. Hơn nữa, việc kiểm soát vị trí/sự di chuyển của khách cũng rất ít sau khi phát các thẻ an ninh. Thường thấy rằng các khu tòa nhà với độ anh ninh cao có các thiết bị an ninh được trang bị đầy đủ gặp phải những sự vi phạm an ninh. Để nâng cao an ninh của các khu tòa nhà, các chủ sở hữu tòa nhà có thể tăng thêm số lượng nhân viên an ninh. Tuy nhiên, thường xuyên hơn không, việc tăng số lượng nhân viên an ninh không làm cho an ninh tốt hơn trong các khu tòa nhà. Trong một số trường hợp, nhân viên an ninh thậm chí còn không kiểm tra khách và để khách vào khu tòa nhà tự do. Trong trường hợp như vậy, không thể biết ai và khi nào vào hoặc rời khỏi các khu tòa nhà, chưa kể đến việc biết ai không rời khỏi khu tòa nhà sau giờ làm việc.

Do đó, điều cần thiết là bổ sung hệ thống kiểm soát an ninh và phương pháp kiểm soát an ninh để khắc phục các vấn đề trên.

Bản chất kỹ thuật của sáng chế

Theo các phương án khác nhau, sáng chế đề xuất phương pháp kiểm soát an ninh để cấp phép vào khu tòa nhà cho khách. Phương pháp kiểm soát an ninh bao gồm bước xác định nhãn nhận dạng; truyền nhãn nhận dạng đến khách; quét nhãn nhận dạng của khách; xác thực nhãn nhận dạng; tạo tín hiệu chấp thuận khi xác thực chắc chắn được nhãn nhận dạng; phân phát token nhận dạng cho khách khi nhận tín hiệu

chấp thuận; quét token nhận dạng của khách; và xác thực token nhận dạng để cấp phép vào khu tòa nhà cho khách.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh bao gồm bước nhận dữ liệu cá nhân của khách.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh còn bao gồm bước xác thực dữ liệu cá nhân.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh còn bao gồm bước nhận token (thẻ) nhận dạng từ khách.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh còn bao gồm bước xác thực token nhận dạng.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh bao gồm bước truyền nhãn nhận dạng bao gồm việc truyền dẫn điện tử.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh bao gồm bước quét nhãn nhận dạng bao gồm việc quét nhãn nhận dạng bằng quang học.

Theo các phương án khác nhau, phương pháp kiểm soát an ninh còn bao gồm bước tái tạo nhãn nhận dạng.

Theo các phương án khác nhau, bước tái tạo nhãn nhận dạng bao gồm ít nhất một bước trong số in nhãn nhận dạng trên phương tiện in được hoặc hiển thị nhãn nhận dạng trên màn hình của thiết bị điện tử.

Theo các phương án khác nhau, nhãn nhận dạng bao gồm ảnh đọc được bằng quang học.

Theo các phương án khác nhau, ảnh đọc được bằng quang học bao gồm ít nhất một loại trong số mã vạch hoặc mã đáp ứng nhanh.

Theo các phương án khác nhau, bước quét token nhận dạng bao gồm ít nhất một công đoạn trong số quét tần số vô tuyến hoặc quét từ tính.

Theo các phương án khác nhau, token nhận dạng bao gồm ít nhất một loại trong số vi mạch nhận dạng tần số vô tuyến hoặc phần đọc được bằng từ tính.

Theo các phương án khác nhau, sáng chế đề xuất hệ thống kiểm soát an ninh được tạo cấu hình để cấp phép vào khu tòa nhà cho khách. Hệ thống kiểm soát an ninh

này bao gồm mạch xác định được tạo cấu hình để xác định nhãn nhận dạng; bộ truyền được tạo cấu hình để truyền nhãn nhận dạng đến khách; máy quét thứ nhất được tạo cấu hình để quét nhãn nhận dạng của khách; mạch xác thực thứ nhất được tạo cấu hình để xác thực nhãn nhận dạng; bộ tạo được tạo cấu hình để tạo ra tín hiệu chấp thuận khi xác thực chắc chắn được nhãn nhận dạng; bộ phân phát được tạo cấu hình để phân phát token nhận dạng; máy quét thứ hai được tạo cấu hình để quét token nhận dạng; và mạch xác thực thứ hai được tạo cấu hình để xác thực token nhận dạng để cấp phép vào khu tòa nhà cho khách.

Theo các phương án khác nhau, hệ thống kiểm soát an ninh được tạo cấu hình để nhận dữ liệu cá nhân của khách.

Theo các phương án khác nhau, mạch xác thực thứ nhất được tạo cấu hình để xác thực dữ liệu cá nhân.

Theo các phương án khác nhau, hệ thống kiểm soát an ninh còn bao gồm bộ nhận được làm thích ứng để nhận token nhận dạng.

Theo các phương án khác nhau, nhãn nhận dạng bao gồm ảnh đọc được bằng quang học.

Theo các phương án khác nhau, ảnh đọc được bằng quang học bao gồm ít nhất một loại trong số mã vạch hoặc mã đáp ứng nhanh.

Theo các phương án khác nhau, token nhận dạng bao gồm ít nhất một loại trong số vi mạch nhận dạng tần số vô tuyến hoặc phần đọc được bằng từ tính.

Sáng chế đề xuất hệ thống kiểm soát an ninh và phương pháp kiểm soát an ninh để khắc phục các vấn đề trên đây. Sáng chế đề xuất mức kiểm tra an ninh cao hơn cho khu tòa nhà và biết được vị trí của khách trong khu tòa nhà. Hệ thống kiểm soát an ninh và phương pháp kiểm soát an ninh cũng có thể cho phép giảm thiểu, nếu không nói là, không cần nhân viên an ninh ở các vị trí an ninh. Theo cách này, yêu cầu đối với nhân lực có thể được giảm đi nhờ đó tiết kiệm chi phí về nguồn nhân lực.

Hệ thống kiểm soát an ninh theo sáng chế cung cấp buồng tự phục vụ (Self Service Kiosk) mà có thể được sử dụng để bổ sung cho các hệ thống an ninh sẵn có do nó có thể được sử dụng cùng với các hệ thống an ninh sử dụng các token nhận dạng, ví dụ thẻ an ninh, và lối vào cổng để phân phát các token nhận dạng. Buồng tự phục vụ

có thể được sử dụng cùng với hệ thống lối vào an ninh, ví dụ hệ thống thẻ an ninh, để trở thành buồng an ninh (Security Kiosk), mà là sự tích hợp của hệ thống lối vào an ninh tòa nhà và buồng tự phục vụ. Buồng tự phục vụ có thể được sử dụng để nâng cao các hệ thống lối vào an ninh sẵn có và có thể được sử dụng để khắc phục các nhược điểm của các trường hợp an ninh hiện nay như được mô tả trên đây và cung cấp thủ tục kiểm tra an ninh tốt hơn và giảm sai sót an ninh đến mức tối thiểu. Mục đích của sáng chế là đạt được sự kiểm tra an ninh cao, ví dụ, đạt được sự kiểm tra an ninh 100%, và cung cấp giải pháp an ninh có độ tin cậy cao để đảm bảo việc kiểm soát ra vào tốt hơn và giám sát sự di chuyển của khách trong khu tòa nhà.

Mô tả vắn tắt các hình vẽ

Fig.1 thể hiện sơ đồ giản lược của hệ thống kiểm soát an ninh theo các phương án khác nhau;

Fig.2 thể hiện sơ đồ giản lược của hệ thống kiểm soát an ninh theo các phương án khác nhau; và

Fig.3 thể hiện phương pháp kiểm soát an ninh khi sử dụng hệ thống kiểm soát an ninh trên Fig.1.

Mô tả chi tiết sáng chế

Fig.1 thể hiện hệ thống kiểm soát an ninh 100. Hệ thống kiểm soát an ninh 100 được tạo cấu hình để cấp phép cho khách 10 vào khu tòa nhà 20, ví dụ khu dân cư biệt lập, tòa nhà, văn phòng. Hệ thống kiểm soát an ninh 100 bao gồm mạch xác định 110 được tạo cấu hình để xác định nhãn nhận dạng 12, bộ truyền 120 được tạo cấu hình để truyền nhãn nhận dạng 12 đến khách 10, máy quét thứ nhất 130 được tạo cấu hình để quét nhãn nhận dạng 12 của khách 10, mạch xác thực thứ nhất 140 được tạo cấu hình để xác thực nhãn nhận dạng 12, bộ tạo tín hiệu 150 được tạo cấu hình để tạo ra tín hiệu chấp thuận khi xác thực chắc chắn được nhãn nhận dạng 12, bộ phân phát 160 được tạo cấu hình để phân phát token nhận dạng 14, máy quét thứ hai 170 được tạo cấu hình để quét token nhận dạng 14 và mạch xác thực thứ hai 180 được tạo cấu hình để xác thực token nhận dạng 14 để cấp phép cho khách 10 vào khu tòa nhà 20.

Nói cách khác, hệ thống kiểm soát an ninh 100 có thể là quầy tự phục vụ để phát token nhận dạng, ví dụ thẻ an ninh, cho khách. Hệ thống kiểm soát an ninh 100

cho phép chủ 30 từ khu tòa nhà 20 phát nhãn nhận dạng 12 cho khách 10 từ trước, ví dụ trước khi đến khu tòa nhà 20, và cho phép khách 10 sử dụng nhãn nhận dạng 12 để đổi lấy token nhận dạng 14 để được phép vào khu tòa nhà 20. Chủ 30 có thể là người khởi tạo việc truyền nhãn nhận dạng 12. Chủ 30 có thể là người thuê của khu tòa nhà và/hoặc nhân viên an ninh. Hệ thống kiểm soát an ninh 100 có thể xác định nhãn nhận dạng 12 khi được yêu cầu bởi chủ 30. Nhờ xác định nhãn nhận dạng 12, chủ có thể truyền nhãn nhận dạng 12 đến khách 10 nhờ sử dụng bộ truyền 120. Khách 10 có thể quét nhãn nhận dạng 12 ở máy quét thứ nhất 130 khi khách 10 đang ở khu tòa nhà 20. Khi được quét, mạch xác thực thứ nhất 140 xác thực nhãn nhận dạng 12 để xác định liệu nhãn nhận dạng 12 có hợp lệ hay không. Nếu hợp lệ, tín hiệu chấp thuận sẽ được gửi đến bộ phân phát 160 để phân phát token nhận dạng 14. Khách 10 sau đó có thể sử dụng token nhận dạng 14 để được phép vào khu tòa nhà 20.

Hệ thống kiểm soát an ninh 100 có thể bao gồm môđun đăng ký (không được thể hiện trên Fig.1) để đăng ký danh tính của chủ 30 khi khởi tạo việc xác định và truyền nhãn nhận dạng 12 đến khách 10. Chủ 30 có thể có mã truy cập bảo mật, ví dụ mật khẩu, để đăng nhập vào môđun đăng ký trước khi khởi tạo. Khi chủ 30 đăng nhập vào môđun đăng ký để khởi tạo việc xác định và truyền, hệ thống kiểm soát an ninh 100 sẽ có thể thu thập dữ liệu cá nhân của chủ 30 mà được gắn với mã truy cập bảo mật để nhận dạng chủ 30. Theo cách này, có thể thu được danh tính của người cho phép khách vào.

Mạch xác định 110 có thể được nối với bộ truyền 120. Mạch xác định 110 có thể được nối với bộ truyền 120 qua đường truyền, ví dụ dây, sợi quang. Mạch xác định 110 có thể xác định nhãn nhận dạng 12 và truyền nhãn nhận dạng 12. Mạch xác định 110 có thể truyền nhãn nhận dạng theo kiểu điện tử đến bộ truyền 120. Bộ truyền 120 sau đó có thể truyền nhãn nhận dạng 12 theo kiểu điện tử đến khách 10.

Fig.2 thể hiện sơ đồ giản lược theo các phương án khác nhau. Như được thể hiện trên Fig.2, mạch xác định 110 có thể được nối với bộ xử lý trung tâm 102, ví dụ CPU, được tạo cấu hình để xử lý các tín hiệu. Bộ xử lý trung tâm 102 có thể được nối với bộ lưu trữ dữ liệu 104 được tạo cấu hình để lưu trữ dữ liệu, ví dụ nhãn nhận dạng, dữ liệu ra vào và cá nhân của khách. Mạch xác định 110 có thể tạo ra nhãn nhận dạng 12. Mạch xác định 110 có thể thu được nhãn nhận dạng 12 từ bộ lưu trữ dữ liệu 104.

Bộ truyền 120 có thể là thiết bị điện tử được tạo cấu hình để truyền nhãn nhận dạng 12 đến khách 10. Bộ truyền 120 có thể được nối với bộ xử lý trung tâm 102. Bộ truyền 120 có thể là đầu cuối máy tính có ứng dụng thư điện tử được tạo cấu hình để cho phép chủ 30 truyền thư điện tử đến khách 10. Bộ truyền 120 có thể là thiết bị truyền thông được tạo cấu hình để cho phép chủ 30 truyền nhãn nhận dạng 12, ví dụ ảnh, đến khách. Thiết bị truyền thông có thể là thiết bị di động, ví dụ điện thoại di động.

Nhãn nhận dạng 12 có thể bao gồm ảnh đọc được bằng quang học. Ảnh đọc được bằng quang học có thể bao gồm ít nhất một loại trong số mã vạch hoặc mã đáp ứng nhanh. Ảnh đọc được bằng quang học có thể được truyền qua internet hoặc hệ thống truyền thông di động. Ảnh đọc được bằng quang học có thể được truyền qua thư điện tử đến khách hoặc qua dịch vụ nhắn tin ngắn (short message service - SMS) hoặc loại tương tự.

Máy quét thứ nhất 130 có thể là máy quét quang học được tạo cấu hình để quét nhãn nhận dạng 12. Khách 10 có thể tái tạo nhãn nhận dạng 12 nhằm mục đích làm cho nhãn nhận dạng 12 được quét bằng máy quét thứ nhất 130. Máy quét thứ nhất 130 có thể là thiết bị chụp ảnh, ví dụ camera. Như được thể hiện trên Fig.2, máy quét thứ nhất 130 có thể được nối với bộ xử lý trung tâm 102 sao cho máy quét thứ nhất 130 có thể truyền tín hiệu ảnh của nhãn nhận dạng 12 đến bộ xử lý trung tâm 102. Bộ xử lý trung tâm 102 có thể truyền tín hiệu ảnh đến mạch xác thực thứ nhất 140.

Khách 10 có thể tái tạo nhãn nhận dạng 12 bằng cách in lên phương tiện in được, ví dụ giấy, hoặc hiển thị nhãn nhận dạng 12 lên màn hình của thiết bị di động, ví dụ điện thoại di động. Đối với phương tiện in được, máy quét thứ nhất 130 có thể là máy quét quang học để quét nhãn nhận dạng 12 hoặc thiết bị chụp ảnh để chụp nhãn nhận dạng 12. Đối với màn hình của thiết bị di động hiển thị nhãn nhận dạng 12, máy quét thứ nhất 130 có thể là thiết bị chụp ảnh để chụp ảnh của nhãn nhận dạng 12 trên màn hình trước khi xác thực nó.

Hệ thống kiểm soát an ninh 100 có thể được tạo cấu hình để nhận dữ liệu cá nhân của khách 10. Chủ 30 có thể yêu cầu cung cấp dữ liệu cá nhân của khách 10 nhằm mục đích xác thực và/hoặc ghi. Dữ liệu cá nhân có thể được lưu trữ trong bộ lưu trữ dữ liệu 104.

Mạch xác thực thứ nhất 140 có thể được tạo cấu hình để xác thực nhãn nhận dạng 12 khi nhận tín hiệu ảnh. Mạch xác thực thứ nhất 140 có thể được nối với bộ xử lý trung tâm 102. Bộ xử lý trung tâm 102 có thể thu được dữ liệu xác thực của nhãn nhận dạng 12 từ bộ lưu trữ dữ liệu 104. Mạch xác thực thứ nhất 140 có thể xác thực tín hiệu ảnh của nhãn nhận dạng 12 dựa trên dữ liệu xác thực. Mạch xác thực thứ nhất 140 có thể được nối với bộ tạo tín hiệu 150 sao cho dựa trên sự xác thực chắc chắn của tín hiệu ảnh, mạch xác thực thứ nhất 140 có thể kích hoạt bộ tạo tín hiệu 150 để tạo ra tín hiệu chấp thuận. Bộ tạo tín hiệu 150 có thể được nối với bộ xử lý trung tâm 102. Mạch xác thực thứ nhất 140 có thể được nối với bộ phân phát 160. Nhờ tạo tín hiệu chấp thuận, bộ tạo tín hiệu 150 có thể truyền tín hiệu chấp thuận đến bộ phân phát 160 để phân phát token nhận dạng 14.

Mạch xác thực thứ nhất 140 có thể được tạo cấu hình để xác thực dữ liệu cá nhân của khách 10. Vào thời điểm quét nhãn nhận dạng 12, đầu cuối có giao diện người sử dụng có thể được cung cấp cho khách 10 để nhập dữ liệu cá nhân. Khi nhận dữ liệu cá nhân, mạch xác thực thứ nhất 140 có thể xác thực dữ liệu cá nhân dựa trên dữ liệu cá nhân lưu trữ trong bộ lưu trữ dữ liệu 104. Khi xác thực chắc chắn được nhãn nhận dạng 12 và dữ liệu cá nhân, mạch xác thực thứ nhất 140 có thể kích hoạt bộ tạo tín hiệu 150 để tạo ra tín hiệu chấp thuận. Mạch xác thực thứ nhất 140 có thể được nối với bộ phân phát 160. Khi tạo tín hiệu chấp thuận, bộ tạo tín hiệu 150 có thể truyền tín hiệu chấp thuận đến bộ phân phát 160 để phân phát token nhận dạng 14.

Bộ phân phát 160 có thể là máy phân phát được tạo cấu hình để phân phát các token nhận dạng 14. Khách 10 có thể nhận token nhận dạng 14 từ bộ phân phát 160 nhờ quét và xác thực chắc chắn nhãn nhận dạng 12. Bộ phân phát 160 có thể được tạo cấu hình để mã hóa token nhận dạng 14 với dữ liệu ra vào, ví dụ thông tin nhân viên, ngày giờ, khoảng thời gian vào. Bộ phân phát 160 có thể được nối với bộ xử lý trung tâm 102 để thu dữ liệu từ hoặc gửi dữ liệu đến bộ xử lý trung tâm 102.

Token nhận dạng 14 có thể bao gồm ảnh đọc được bằng quang học. Ảnh đọc được bằng quang học có thể bao gồm ít nhất một loại trong số mã vạch hoặc mã đáp ứng nhanh. Token nhận dạng 14 có thể là token từ tính nhờ đó token nhận dạng 14 có thể được "quét" bằng từ tính. Token nhận dạng 14 có thể bao gồm phần đọc được bằng từ tính. Token nhận dạng 14 có thể là nhãn nhận dạng tần số vô tuyến (radio-frequency identification - RFID). Token nhận dạng 14 có thể bao gồm vi mạch RFID. Token

nhận dạng 14 có thể ở dạng thẻ, thỏi, hoặc nút, ví dụ thẻ an ninh. Token nhận dạng 14 có thể được gắn với các đặc tính bảo mật dưới dạng ít nhất một loại trong số vi mạch, dải từ tính hoặc RFID, v.v. Token nhận dạng 14 có thể được quét tại máy quét thứ hai 170.

Máy quét thứ hai 170 có thể là ít nhất một loại trong số máy quét quang học, máy quét từ tính hoặc máy quét RFID. Máy quét thứ hai 170 có thể được nối với mạch xác thực thứ hai 180. Nhờ quét token nhận dạng 14, tín hiệu được quét có thể được truyền đến mạch xác thực thứ hai 180 nhờ đó tín hiệu được quét có thể được xác thực. Mạch xác thực thứ hai 180 có thể được nối với bộ xử lý trung tâm 102. Bộ xử lý trung tâm 102 có thể thu được dữ liệu xác thực từ bộ lưu trữ dữ liệu 104 qua bộ xử lý trung tâm 102 và việc xác thực tín hiệu được quét của token nhận dạng 14 có thể dựa trên dữ liệu xác thực. Khi xác thực chắc chắn được token nhận dạng 14, khách 10 có thể được phép vào khu tòa nhà 20.

Khu tòa nhà 20, như được thể hiện trên Fig.1, có thể bao gồm cổng 22 được làm thích ứng để kiểm soát việc khách 10 vào khu tòa nhà 20. Hệ thống kiểm soát an ninh 100 có thể được nối với cổng 22 nhờ đó hệ thống kiểm soát an ninh 100 được tạo cấu hình để kiểm soát hoạt động của cổng 22 giữa cấu hình đóng để ngăn không cho khách 10 vào khu tòa nhà 20 và cấu hình mở để cho phép khách 10 vào khu tòa nhà 20. Khi xác thực chắc chắn được token nhận dạng 14, cổng kiểm soát 22 có thể được mở để cho phép khách 10 vào khu tòa nhà. Cổng 22 có thể là quầy, cửa quay hoặc cổng tín hiệu với đặc tính chống cửa hậu, cửa, v.v…

Trên Fig.1, hệ thống kiểm soát an ninh 100 có thể bao gồm bộ nhận 190 được làm thích ứng để nhận token nhận dạng 14. Khi khách 10 sắp rời khu tòa nhà 20, khách 10 có thể trả lại token nhận dạng 14 cho bộ nhận 190. Bộ nhận 190 có thể được tạo cấu hình để nhận dạng token nhận dạng 14 và trích xuất dữ liệu vào từ bộ lưu trữ dữ liệu 104 dựa trên token nhận dạng 14, ví dụ thời gian xuất phát, các khu vực đã đến. Trên Fig.2, bộ nhận 190 có thể được nối với bộ xử lý trung tâm 102. Bộ nhận 190 và bộ phân phát 160 có thể được nối với nhau. Bộ nhận 190 và bộ phân phát 160 có thể được chứa cùng nhau sao cho các token nhận dạng 14 được nhận bởi bộ nhận 190 có thể được chuyển đến bộ phân phát 160 để được phân phát đến khách tiếp theo. Khu tòa nhà 20 có thể bao gồm các máy quét trong đó để khách 10 quét token nhận dạng 14 khi khách đi vào một khu vực, ví dụ phòng, trong khu tòa nhà 20. Theo cách này, hệ

thống kiểm soát an ninh 100 có thể đăng ký thời gian và khu vực là khi mà và là nơi mà khách 10 đã vào. Chủ 30 có thể có quyền giới hạn việc đi vào các khu vực nhất định trong khu tòa nhà 20, ví dụ thang nâng ôtô, các tầng, các phòng. Trong trường hợp này, chủ 30 có thể có thể cung cấp cho khách 10 quyền đi vào giới hạn chỉ đến các khu vực nhất định trong khu tòa nhà 20. Bằng cách nhận và đăng ký các token nhận dạng 14, hệ thống kiểm soát an ninh 100 có khả năng tìm ra nếu còn có khách 10 trong khu tòa nhà 20 vào cuối ngày làm việc hoặc cuối ngày. Đồng thời, hệ thống kiểm soát an ninh 100 sẽ có thể theo dõi chuyển động của khách 10 trong khu tòa nhà 20.

Fig.3 thể hiện phương pháp kiểm soát an ninh 1000 để cấp phép cho khách 10 vào khu tòa nhà 20. Ở bước 1100, nhãn nhận dạng 12 được xác định. Nhãn nhận dạng 12 được truyền đến khách 10 ở bước 1200. Ở bước 1300, nhãn nhận dạng 12 của khách 10 được quét. Ở bước 1400, nhãn nhận dạng 12 được xác thực. Khi xác thực chắc chắn được nhãn nhận dạng 12, tín hiệu chấp thuận được tạo ra ở bước 1500. Ở bước 1600, token nhận dạng 14 được phân phát cho khách 10 khi nhận tín hiệu chấp thuận. Ở bước 1700, token nhận dạng 14 của khách 10 được quét. Ở bước 1800, token nhận dạng 14 được xác thực để cấp phép cho khách 10 vào khu tòa nhà 20.

Fig.3 thể hiện phương pháp kiểm soát an ninh 1000 được sử dụng cho mục đích an ninh. Khi chủ 30 đang chờ khách 10 thăm khu tòa nhà 20, chủ 30 có thể xác định nhãn nhận dạng 12 nhờ sử dụng mạch xác định 110 và truyền nhãn nhận dạng 12 đến khách 10 nhờ sử dụng bộ truyền 120. Chủ 30, người biết ngày và giờ đến thăm, có thể xác định ngày và giờ mà nhãn nhận dạng 12 có thể là hợp lệ để vào. Chủ 30 cũng có thể xác định khoảng thời gian mà khách 10 có thể ở trong khu tòa nhà. Chủ 30 có thể truyền nhãn nhận dạng 12 thông qua việc truyền dẫn điện tử. Chủ 30 có thể truyền nhãn nhận dạng 12 qua thư điện tử hoặc tin nhắn ngắn từ đầu cuối máy tính và/hoặc thiết bị di động tương ứng của người đó đến khách 10. Khách 10 có thể nhận nhãn nhận dạng 12 trên đầu cuối máy tính và/hoặc thiết bị di động của người đó. Để an toàn hơn, chủ 30 có thể yêu cầu khách 10 cung cấp dữ liệu cá nhân nhằm mục đích xác thực và/hoặc ghi nhận. Sau đó, khách 10 có thể chuyển tiếp dữ liệu cá nhân được yêu cầu cho chủ 30 bằng điện tử hoặc qua điện thoại. Hệ thống kiểm soát an ninh 100 sau đó có thể nhận dữ liệu cá nhân của khách 10 và lưu trữ dữ liệu cá nhân vào bộ lưu trữ dữ liệu.

Khách 10, khi vào thăm khu tòa nhà 20 của chủ 30, có thể tái tạo nhãn nhận

dạng 12 bằng cách in nhãn nhận dạng 12 lên phương tiện in được từ trước hoặc hiển thị nhãn nhận dạng 12 lên màn hình của thiết bị điện tử, ví dụ thiết bị di động. Khách 10 có thể hiển thị nhãn nhận dạng 12 cần được quét bởi máy quét thứ nhất 130.

Nhãn nhận dạng 12 có thể được quét bằng quang học nhờ máy quét thứ nhất 130. Việc quét token nhận dạng 14 có thể bao gồm việc quét tần số vô tuyến và/hoặc quét từ tính. Máy quét thứ nhất 130 có thể quét nhãn nhận dạng 12 và truyền tín hiệu ảnh của nhãn nhận dạng 12 đến bộ xử lý trung tâm 102 mà có thể truyền tín hiệu ảnh đến mạch xác thực thứ nhất 140.

Khách 10 có thể được yêu cầu cung cấp dữ liệu cá nhân qua giao diện người sử dụng của thiết bị đầu cuối. Mạch xác thực thứ nhất 140 có thể xác thực nhãn nhận dạng 12, và dữ liệu cá nhân nếu cần thiết, dựa trên dữ liệu xác thực và dữ liệu cá nhân được lưu trữ trong bộ lưu trữ dữ liệu 104. Nếu việc xác thực là chắc chắn, thì mạch xác thực thứ nhất 140 có thể kích hoạt bộ tạo tín hiệu 150 để tạo ra tín hiệu chấp thuận và truyền tín hiệu chấp thuận đến bộ phân phát 160 để phân phát token nhận dạng 14 cho khách 10. Mặt khác, nếu việc xác thực là không chắc chắn, thì hệ thống kiểm soát an ninh 100 sẽ thông báo cho khách theo đó và từ chối khách 10 vào khu tòa nhà 20.

Khách 10, khi nhận token nhận dạng 14, có thể tạo ra token nhận dạng 14 ở máy quét thứ hai 170 để quét. Dựa trên các hạn chế được thiết lập bởi chủ 30, token nhận dạng 14 có thể được tạo cấu hình để xác định khoảng thời gian và các khu vực trong các khu tòa nhà mà khách 10 có thể ở lại. Nhờ quét, tín hiệu được quét có thể được truyền đến mạch xác thực thứ hai 180 để được xác nhận. Token nhận dạng 14 có thể được xác thực. Việc xác thực token nhận dạng 14 có thể dựa trên dữ liệu xác thực được lưu trữ trong bộ lưu trữ dữ liệu 104. Nếu việc xác thực là chắc chắn, thì cổng 22 có thể được mở để cho phép khách 10 vào khu tòa nhà 20. Tuy nhiên, nếu việc xác thực là không chắc chắn, thì cổng 22 vẫn sẽ ở cấu hình đóng để ngăn không cho vào khu tòa nhà 20.

Khi khách 10 rời khỏi khu tòa nhà 20, khách 10 có thể trả lại token nhận dạng 14 cho bộ nhận 190. Token nhận dạng 14 có thể được nhận từ khách 10 và được giữ lại bởi bộ nhận 190. Khi bộ nhận nhận token nhận dạng 14, bộ nhận 190 có thể thu được thông tin về khách 10, ví dụ thời gian khi khách 10 rời khỏi khu tòa nhà 20, các khu vực trong khu tòa nhà 20 nơi mà khách 10 đã đi vào. Hệ thống kiểm soát an ninh

100 có thể được tạo cấu hình để thông báo cho chủ 30 nếu khách 10 ở lại quá khoảng thời gian xác định hoặc thời gian kết thúc xác định của chuyến thăm. Chủ 30 có thể có quyền trì hoãn thời gian mà khách được phép ở lại. Chủ 30 có thể truy cập, ví dụ đăng nhập, môđun đăng ký để trì hoãn thời gian. Hệ thống kiểm soát an ninh 100 có thể được tạo cấu hình để tạo ra số lượng khách 10 vẫn còn trong khu tòa nhà 20 vào thời điểm bất kỳ. Hệ thống kiểm soát an ninh 100 có thể được tạo cấu hình để tạo ra danh sách tên khách và/hoặc vị trí của khách vào thời điểm bất kỳ khi được yêu cầu bởi chủ 30 hoặc nhân viên an ninh được ủy quyền làm việc đó. Theo cách này, có thể hữu ích cho chủ 30 hoặc nhân viên an ninh để biết ai và nơi nào mà khách hoặc nhiều khách đang ở vào thời điểm bất kỳ khi cần, ví dụ trong khi sơ tán khẩn cấp.

Như được thể hiện, phương pháp kiểm soát an ninh 1000 và hệ thống kiểm soát an ninh 100 cung cấp mức độ an ninh cao cho khu tòa nhà 20. Khách 10 đến khu tòa nhà 20 được biết từ trước bởi chủ 30. Theo một cách, khách 10 được kiểm tra bởi chủ 30 trước khi thăm viếng. Đồng thời, chủ 30 biết khách 10 trước khi cho phép khách 10 đi vào khu tòa nhà 20 và truyền nhãn nhận dạng 12 đến khách 10. Khách 10 thăm viếng khu tòa nhà 20 không cần hỗ trợ từ nhân viên an ninh và có thể vào khu tòa nhà 20 khi thuận tiện trong thời gian thăm viếng được cấp phát dưới dạng được xác định bởi chủ 30. Theo cách này, tất cả các khách 10 đến khu tòa nhà 20 đều được kiểm tra mà không gặp nguy cơ không kiểm tra khách 10 bất kỳ. Ngoài ra, chủ 30 có thể biết được vị trí của khách 10 vào thời điểm bất kỳ và khoảng thời gian thăm viếng của khách 10 có thể được biết. Vào cuối mỗi ngày, chủ 30 sẽ có thể biết liệu tất cả các khách 10 đã rời khỏi khu tòa nhà 20 hay chưa sao cho an ninh vào ban đêm sẽ không bị ảnh hưởng bởi các khách 10 cố ý ở lại. Các khách 10 có thể là người bất kỳ không được cấp phép an ninh hợp lệ và muốn vào khu tòa nhà, bao gồm nhân viên đang làm việc trong khu tòa nhà.

Hệ thống kiểm soát an ninh 100 có thể bao gồm bộ nhớ được sử dụng chẳng hạn khi việc xử lý được thực hiện bởi phương pháp kiểm soát an ninh. Bộ nhớ được sử dụng trong các phương án có thể là bộ nhớ khả biến, ví dụ DRAM (Bộ nhớ truy cập ngẫu nhiên động - Dynamic Random Access Memory) hoặc bộ nhớ bất khả biến, ví dụ PROM (Bộ nhớ chỉ đọc lập trình được - Programmable Read Only Memory), EPROM (PROM xóa được), EEPROM (PROM xóa được bằng điện), hoặc bộ nhớ tác động nhanh (flash memory), ví dụ, bộ nhớ cổng tự do (floating gate memory), bộ nhớ bẫy

điện tích (charge trapping memory), MRAM (Bộ nhớ truy cập ngẫu nhiên từ điện trở - Magnetoresistive Random Access Memory) hoặc PCRAM (Bộ nhớ truy cập ngẫu nhiên đổi pha - Phase Change Random Access Memory).

Theo một phương án, "mạch" có thể được hiểu dưới dạng loại thực thể thực hiện logic bất kỳ, mà có thể là mạch chuyên dụng hoặc bộ xử lý thực thi phần mềm được lưu trữ trong bộ nhớ, phần sụn, hoặc sự kết hợp bất kỳ của chúng. Vì vậy, theo một phương án, "mạch" có thể là mạch logic nối dây hoặc mạch logic lập trình được như bộ xử lý lập trình được, ví dụ bộ vi xử lý (ví dụ, bộ xử lý máy tính dùng tập lệnh phức (Complex Instruction Set Computer - CISC) hoặc bộ xử lý máy tính dùng tập lệnh rút gọn (Reduced Instruction Set Computer - RISC). "Mạch" cũng có thể là bộ xử lý thực thi phần mềm, ví dụ loại chương trình máy tính bất kỳ, ví dụ chương trình máy tính sử dụng mã máy ảo như Java chẳng hạn. Cách thực hiện khác bất kỳ đối với các chức năng tương ứng mà sẽ được mô tả chi tiết hơn dưới đây cũng có thể được hiểu là "mạch" theo một phương án khác.

YÊU CẦU BẢO HỘ

1. Phương pháp kiểm soát an ninh để cấp phép vào khu tòa nhà cho khách bao gồm các bước:

nhận yêu cầu từ chủ của khu tòa nhà để xác định nhãn nhận dạng khi chủ khởi tạo việc truyền dẫn nhãn nhận dạng;

xác định nhãn nhận dạng;

truyền nhãn nhận dạng đến khách;

quét nhãn nhận dạng của khách;

xác thực nhãn nhận dạng;

tạo tín hiệu chấp thuận khi xác thực chắc chắn về nhãn nhận dạng;

phân phát token nhận dạng cho khách khi nhận tín hiệu chấp thuận;

quét token nhận dạng của khách; và

xác thực token nhận dạng để cấp phép vào khu tòa nhà cho khách.

2. Phương pháp kiểm soát an ninh theo điểm 1, trong đó phương pháp này còn bao gồm bước nhận dữ liệu cá nhân của chủ.

3. Phương pháp kiểm soát an ninh theo điểm 1 hoặc 2, trong đó phương pháp này còn bao gồm bước nhận biết danh tính của chủ là người cấp phép vào cho khách.

4. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó phương pháp này còn bao gồm bước nhận token nhận dạng từ khách.

5. Phương pháp kiểm soát an ninh theo điểm 4, trong đó phương pháp này còn bao gồm bước xác thực token nhận dạng.

6. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó bước truyền nhãn nhận dạng bao gồm truyền dẫn điện tử.

7. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó bước quét nhãn nhận dạng bao gồm việc quét nhãn nhận dạng bằng quang học.

8. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó phương pháp này còn bao gồm bước tái tạo nhãn nhận dạng.

9. Phương pháp kiểm soát an ninh theo điểm 8, trong đó bước tái tạo nhãn nhận dạng bao gồm ít nhất một công đoạn trong số in nhãn nhận dạng trên phương tiện in được hoặc hiển thị nhãn nhận dạng trên màn hình của thiết bị điện tử.

10. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 9, trong đó phương pháp này còn bao gồm bước nhận ngày giờ mà nhãn nhận dạng còn hiệu lực để vào khu tòa nhà.

11. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 10, trong đó bước quét token nhận dạng bao gồm ít nhất một công đoạn trong số quét tần số vô tuyến hoặc quét từ tính.

12. Phương pháp kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 1 đến 11, trong đó token nhận dạng bao gồm ít nhất một trong số vi mạch nhận dạng tần số vô tuyến hoặc phần đọc được bằng từ tính.

13. Hệ thống kiểm soát an ninh được tạo cấu hình để cấp phép vào khu tòa nhà cho khách, hệ thống kiểm soát an ninh này được tạo cấu hình để nhận yêu cầu từ chủ của khu tòa nhà để xác định nhãn nhận dạng khi chủ khởi tạo truyền dẫn nhãn nhận dạng, hệ thống kiểm soát an ninh này bao gồm:

mạch xác định được tạo cấu hình để xác định nhãn nhận dạng;

bộ truyền được tạo cấu hình để truyền nhãn nhận dạng đến khách;

máy quét thứ nhất được tạo cấu hình để quét nhãn nhận dạng của khách;

mạch xác thực thứ nhất được tạo cấu hình để xác thực nhãn nhận dạng;

bộ tạo được tạo cấu hình để tạo ra tín hiệu chấp thuận khi xác thực chắc chắn được nhãn nhận dạng;

bộ phân phát được tạo cấu hình để phân phát token nhận dạng;

máy quét thứ hai được tạo cấu hình để quét token nhận dạng; và

mạch xác thực thứ hai được tạo cấu hình để xác thực token nhận dạng để cấp phép vào khu tòa nhà cho khách.

14. Hệ thống kiểm soát an ninh theo điểm 13, trong đó hệ thống kiểm soát an ninh được tạo cấu hình để nhận dữ liệu cá nhân của chủ.

15. Hệ thống kiểm soát an ninh theo điểm 13 hoặc 14, trong đó hệ thống kiểm soát an ninh được tạo cấu hình để nhận biết danh tính của chủ là người cấp phép vào cho khách.

16. Hệ thống kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 13 đến 15, trong đó hệ thống này còn bao gồm bộ nhận được tạo phù hợp để nhận token nhận dạng.

17. Hệ thống kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 13 đến 16, trong đó hệ thống kiểm soát an ninh này được tạo cấu hình để nhận ngày giờ mà nhãn nhận dạng còn hiệu lực để vào khu tòa nhà.

18. Hệ thống kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 13 đến 17, trong đó ảnh đọc được bằng quang học bao gồm ít nhất một trong số mã vạch hoặc mã đáp ứng nhanh.

19. Hệ thống kiểm soát an ninh theo điểm bất kỳ trong số các điểm từ 13 đến 18, trong đó token nhận dạng bao gồm ít nhất một trong số vi mạch nhận dạng tần số vô tuyến hoặc phần đọc được bằng từ tính.

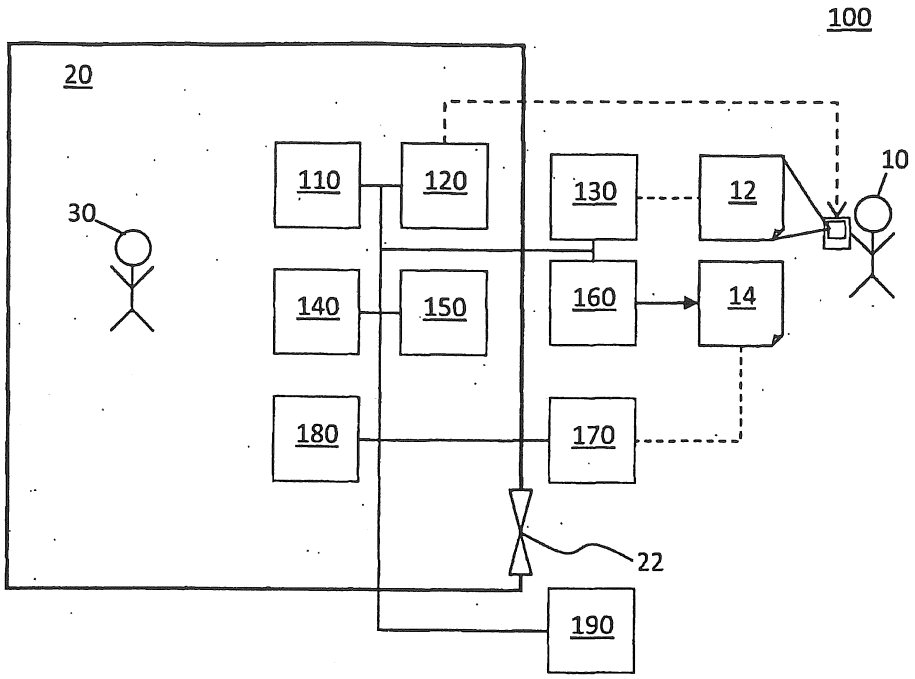

100
20
30
110
120
130
12
10
140
150
160
14
180
170
22
190

Fig. 1

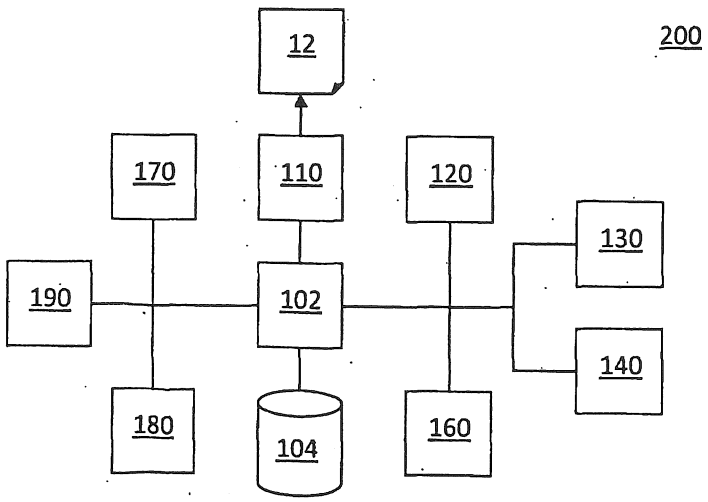

12
200
170
110
120
130
190
102
140
180
104
160

Fig. 2

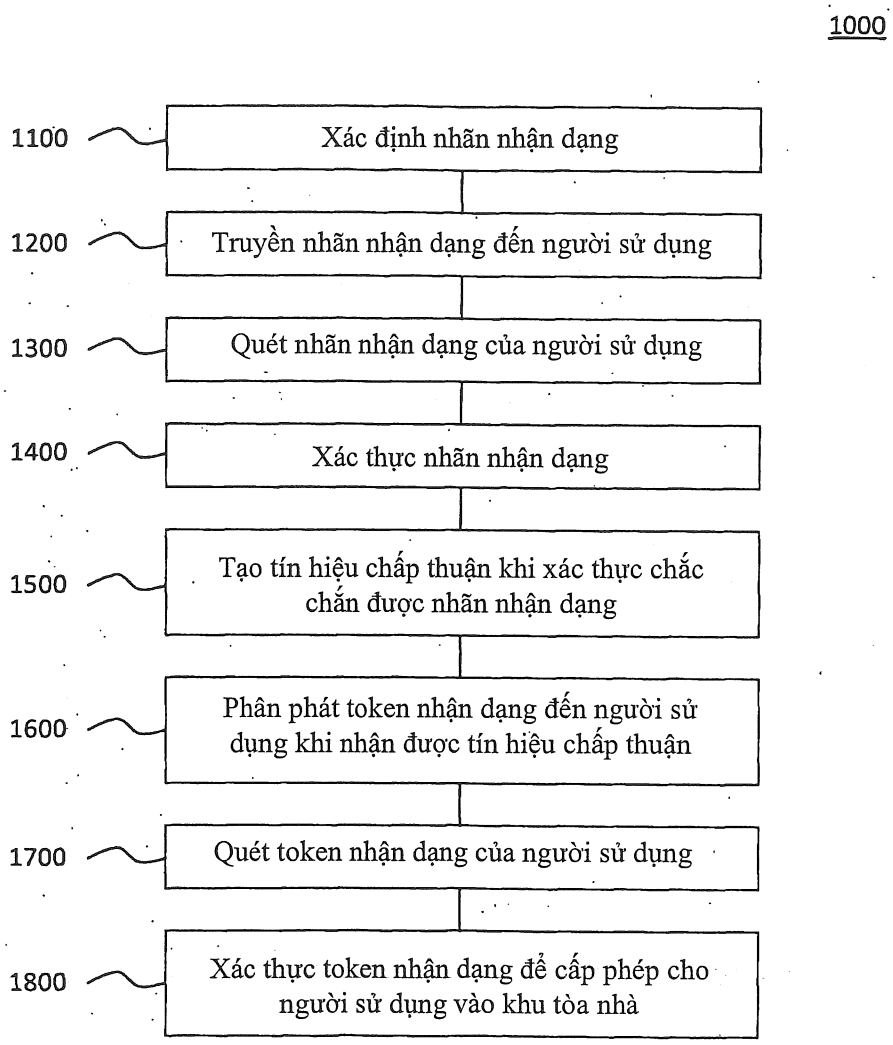

1000
1100
Xác định nhãn nhận dạng
1200
Truyền nhãn nhận dạng đến người sử dụng
1300
Quét nhãn nhận dạng của người sử dụng
1400
Xác thực nhãn nhận dạng
1500
Tạo tín hiệu chấp thuận khi xác thực chắc chắn được nhãn nhận dạng
1600
Phân phát token nhận dạng đến người sử dụng khi nhận được tín hiệu chấp thuận
1700
Quét token nhận dạng của người sử dụng
1800
Xác thực token nhận dạng để cấp phép cho người sử dụng vào khu tòa nhà

Fig. 3