(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
27. Juni 2019 (27.06.2019)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2019/121336 A1

(51) Internationale Patentklassifikation:
*G07C 9/00* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2018/084797

(22) Internationales Anmeldedatum:
13. Dezember 2018 (13.12.2018)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
17209079.7 20. Dezember 2017 (20.12.2017) EP

(71) Anmelder: **INVENTIO AG** [CH/CH]; Seestrasse 55, 6052 Hergiswil (CH).

(72) Erfinder: **TROESCH, Florian**; Rebstrasse 15, 8703 Erlenbach ZH (CH).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT,

(54) **Title:** ACCESS CONTROL SYSTEM HAVING RADIO AUTHENTICATION AND PASSWORD RECOGNITION

(54) **Bezeichnung:** ZUGANGSKONTROLLSYSTEM MIT FUNK-AUTHENTIFIZIERUNG UND KENNWORTERFASSUNG

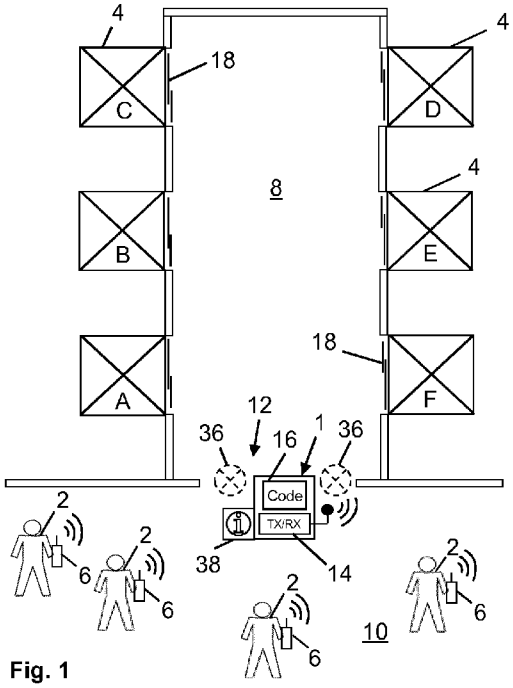


Fig. 1

(57) **Abstract:** The invention relates to an access control system (1) comprising a transmitter and receiver unit (14) for radio communication with a mobile electronic device (6) of a user (2), which is configured for receiving an identifier (Ki) of the mobile electronic device (6) when the mobile electronic device (6) is in a public area (10) from which the user (2) can request access to an access-restricted area (8). A storage unit (26, 28) is configured for creating a dataset (DSi) for the identifier (Ki), which is assigned to the user (2) present in the public area (10), and for storing a password (Ci) in the first dataset (DSi) so that the password (Ci) is assigned to the identifier (Ki). A code processing unit (16, 22) is configured in order to recognise a password (Cd) presented by the user (2), when the user (2) requests access to the access-restricted area (8). A processor unit (20) is configured for determining whether the identifier (Ki) in a database (34) is assigned to a user profile; if it is, authenticating the user (2) as being authorised for access; and determining whether the recognised password (Cd) corresponds with the password (Ci) stored in the dataset (DSi), wherein the user (2) is recognised as a user (2) requesting access if they correspond.

(57) **Zusammenfassung:** Ein Zugangskontrollsystem (1) umfasst eine Sende- und Empfangseinrichtung (14) zur Funkkommunikation mit einem mobilen elektronischen Gerät (6) eines Nutzers (2), die zu einem Empfang einer Kennung (Ki) des mobilen elektronischen Geräts (6) ausgestaltet ist, wenn sich das mobile elektronische Gerät (6) in einer öffentlichen Zone (10) befindet, von der aus der Nutzer (2) Zugang zu einer zugangsbeschränkten Zone (8) ersuchen kann. Eine Speichereinrichtung (26, 28) ist ausgestaltet, um für die Kennung (Ki) einen Datensatz (DSi) anzulegen, der dem in der öffentlichen Zone (10) anwesenden Nutzer (2) zugeordnet ist, und um ein Kennwort (Ci) im ersten Datensatz (DSi) zu

WO 2019/121336 A1

*[Fortsetzung auf der nächsten Seite]*

LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Erklärungen gemäß Regel 4.17:**

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

**Veröffentlicht:**

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

speichern, so dass das Kennwort (Ci) der Kennung (Ki) zugeordnet ist. Eine Codeverarbeitungseinrichtung (16, 22) ist ausgestaltet ist, um ein vom Nutzer (2) präsentiertes Kennwort (Cd) zu erfassen, wenn der Nutzer (2) Zugang zur zugangsbeschränkten Zone (8) ersucht. Eine Prozessoreinrichtung (20) ist ausgestaltet, um zu ermitteln, ob die Kennung (Ki) in einer Datenbank (34) einem Nutzerprofil zugeordnet ist, wenn eine solche Zuordnung besteht, den Nutzer (2) als zugangsberechtigt zu authentifizieren, und zu ermitteln, ob das erfasste Kennwort (Cd) dem im Datensatz (DSi) gespeicherten Kennwort (Ci) übereinstimmt, wobei bei Übereinstimmung der Nutzer (2) als zugangsersuchender Nutzer (2) erkannt wird.

# Zugangskontrollsystem mit Funk-Authentifizierung und Kennworterfassung

Beschreibung

Die hier beschriebene Technologie betrifft allgemein ein Zugangskontrollsystem, das einem berechtigten Nutzer Zugang zu einer zugangsbeschränkten Zone in einem Gebäude oder auf einem Gelände gewährt. Ausführungsbeispiele der Technologie betreffen insbesondere ein Zugangskontrollsystem mit einer Sende- und Empfangseinrichtung und ein Verfahren zum Betreiben eines solchen Zugangskontrollsystems.

Zugangskontrollsysteme können auf verschiedenste Art und Weise ausgestaltet sein. Die Ausgestaltungen können beispielsweise die Art betreffen, wie sich Nutzer (Personen) als zugangsberechtigt auszuweisen haben, z. B. mit einem Schlüssel, einer Magnet-, Chip- oder RFID Karte oder einem mobilen elektronischen Gerät (z. B. Mobiltelefon). WO 2010/112586 A1 beschreibt ein Zugangskontrollsystem, bei dem ein von einem Nutzer mitgeführtes Mobiltelefon einen Identifikationscode an einen Zugangsknoten sendet. Falls der Identifikationscode als gültig erkannt wird, sendet der Zugangsknoten einen Zugangscode an das Mobiltelefon, das den Zugangscode auf einer Anzeige dargestellt. Hält der Nutzer das Mobiltelefon an eine Kamera, so dass diese den dargestellten Zugangscode erfassen kann, überprüft das Zugangskontrollsystem, ob der erfasste Zugangscode gültig ist. Ist er gültig, wird dem Nutzer der Zugang gewährt.

In Gebäuden mit vielen Stockwerken kann es zu bestimmten Tageszeiten zu einem hohen Personenverkehrsaufkommen kommen, beispielsweise in einer Eingangshalle eines Bürogebäudes, wenn morgens oder nach einer Mittagspause eine Vielzahl von Arbeitnehmern das Gebäude betritt, um zu ihren Arbeitsplätzen zu gelangen. Zu diesen Zeiten werden nicht nur hohe Anforderungen an die Effizienz eines im Gebäude installierten Aufzugssystems gestellt, sondern auch an das Zugangskontrollsystem, um z. B. eine Schlangenbildung vor einem Zugang so weit wie möglich zu vermeiden. Es besteht daher ein Bedarf an einem Zugangskontrollsystem, das diese Anforderungen erfüllt, wobei die Zugangskontrolle trotzdem zugangsberechtigte Personen zuverlässig von nicht berechtigten Personen unterscheiden kann.

Ein Aspekt einer solchen Technologie betrifft ein Verfahren zum Betreiben eines Systems zur Kontrolle eines Zugangs zu einer zugangsbeschränkten Zone in einem Gebäude oder

auf einem Gelände. Das System umfasst eine Sende- und Empfangseinrichtung zur Funkkommunikation mit von Nutzern mitgeführten mobilen elektronischen Geräten, eine Speichereinrichtung, eine Prozessoreinrichtung und eine Codeerfassungseinrichtung. Eine erste Kennung eines ersten mobilen elektronischen Geräts eines ersten Nutzers wird durch die Sende- und Empfangseinrichtung empfangen, wenn sich das erste mobile elektronische Gerät in einer öffentlichen Zone befindet, von der aus der erste Nutzer Zugang zur zugangsbeschränkten Zone ersuchen kann. Die empfangene erste Kennung wird in der Speichereinrichtung gespeichert, wobei für die erste Kennung ein erster Datensatz angelegt wird, der dem in der öffentlichen Zone anwesenden ersten Nutzer zugeordnet ist. In der Speichereinrichtung ist eine Vielzahl von Datensätzen speicherbar, wobei jeder Datensatz einem in der öffentlichen Zone anwesenden Nutzern zugeordnet ist. Ein erstes Kennwort wird im ersten Datensatz gespeichert, so dass das erste Kennwort der ersten Kennung zugeordnet ist. Durch die Prozessoreinrichtung wird ermittelt, ob die erste Kennung in einer Datenbank einem Nutzerprofil zugeordnet ist, um, wenn eine solche Zuordnung besteht, den ersten Nutzer als zugangsberechtigt zu authentifizieren. Ein vom ersten Nutzer präsentiertes Kennwort wird durch die Codeerfassungseinrichtung erfasst, wenn der erste Nutzer Zugang zur zugangsbeschränkten Zone ersucht. Durch die Prozessoreinrichtung wird ermittelt, ob das erfasste Kennwort mit dem im ersten Datensatz der Speichereinrichtung gespeicherten ersten Kennwort übereinstimmt, wobei bei Übereinstimmung der erste Nutzer als zugangsersuchender Nutzer erkannt wird.

Ein anderer Aspekt der Technologie betrifft ein System zur Kontrolle eines Zugangs zu einer zugangsbeschränkten Zone in einem Gebäude oder auf einem Gelände. Das System umfasst eine Sende- und Empfangseinrichtung zur Funkkommunikation mit einem von einem ersten Nutzer mitgeführten ersten mobilen elektronischen Gerät, die zu einem Empfang einer ersten Kennung des ersten mobilen elektronischen Geräts ausgestaltet ist, wenn sich das erste mobile elektronische Gerät in einer öffentlichen Zone befindet, von der aus der erste Nutzer Zugang zur zugangsbeschränkten Zone ersuchen kann. Eine Speichereinrichtung des Systems ist ausgestaltet, um für die erste Kennung einen ersten Datensatz anzulegen, der dem in der öffentlichen Zone anwesenden ersten Nutzer zugeordnet ist, und um ein erstes Kennwort im ersten Datensatz zu speichern, so dass das erste Kennwort der ersten Kennung zugeordnet ist. In der Speichereinrichtung ist eine Vielzahl von Datensätzen speicherbar. Das System umfasst ausserdem eine Codeerfassungseinrichtung, die ausgestaltet ist, um ein vom ersten Nutzer präsentiertes

Kennwort zu erfassen, wenn der erste Nutzer Zugang zur zugangsbeschränkten Zone ersucht. Eine Prozessoreinrichtung des Systems ist ausgestaltet zu ermitteln, ob die erste Kennung in einer Datenbank einem Nutzerprofil zugeordnet ist, und wenn eine solche Zuordnung besteht, den ersten Nutzer als zugangsberechtigt zu authentifizieren; sie ist ausserdem ausgestaltet zu ermitteln, ob das erfasste Kennwort mit dem im ersten Datensatz der Speichereinrichtung gespeicherten ersten Kennwort übereinstimmt, wobei bei Übereinstimmung der erste Nutzer als zugangsersuchender Nutzer erkannt wird.

Die hier beschriebene Technologie schafft ein Zugangskontrollsystem, bei dem eine erste Phase einer Überprüfung, ob der Nutzer zugangsberechtigt ist, erfolgt, wenn der Nutzer noch relativ weit vom Zugang entfernt ist. Der Nutzer kann sich beispielsweise in Richtung des Zugangs zur zugangsbeschränkten Zone bewegen, währenddessen in einem Ausführungsbeispiel das mobile elektronische Gerät des Nutzers schon in Kommunikation mit der Sende- und Empfangseinrichtung des Zugangskontrollsystems ist oder bereits war. Die Sende- und Empfangseinrichtung empfängt die Kennung des mobilen elektronischen Geräts des Nutzers. Ist der Nutzer im Zugangskontrollsystem als zugangsberechtigt registriert, ist für den Nutzer ein Nutzerprofil gespeichert. In diesem Nutzerprofil sind nutzerspezifische Daten (z. B. Name und Rechte), die es erlauben, den Nutzer zu authentifizieren. Möchte der Nutzer Zugang zur zugangsbeschränkten Zone, wird in einer zweiten Phase ein vom Nutzer präsentiertes Kennwort erfasst. Das Kennwort kann z. B. ein auf einer Anzeige des mobilen Geräts dargestelltes codiertes Kennwort sein. Stimmt das erfasste Kennwort mit einem gespeicherten Kennwort überein, ist der Nutzer erkannt und es kann für den Nutzer eine Gebäudeaktion veranlasst werden.

Das Kennwort kann je nach Ausgestaltung in einer Speichereinrichtung des mobilen Geräts gespeichert sein, beispielsweise zusammen mit der Kennung des mobilen Geräts. In diesem Fall sendet das mobile Geräts die Kennung und das Kennwort zur Sende- und Empfangseinrichtung (im Wesentlichen zeitgleich oder zeitlich beabstandet). Die Kennung und das Kennwort werden dann im angelegten Datensatz gespeichert. In einer anderen Ausgestaltung erzeugt das Zugangskontrollsystem das Kennwort, sendet es zum mobilen Gerät und speichert es im für die empfangene Kennung angelegten Datensatz. Auch in diesem Fall speichert der Datensatz sowohl die Kennung als auch das Kennwort.

Zu einer zugangsbeschränkten Zone in einem Gebäude oder einem Gebiet kann eine grosse Anzahl von Nutzern (z. B. mehrere Dutzend oder Hundert) zugangsberechtigt sein. In einer solchen Situation empfängt die Sende-und Empfangseinrichtung eine Vielzahl von Kennungen, die in der Speichereinrichtung in Datensätzen gespeichert werden. Trotzdem bietet die hier beschriebene Technologie den Vorteil, dass die Überprüfung auf Übereinstimmung schnell erfolgt, weil das vor Ort erfasste Kennwort nur mit den Kennwörtern der tatsächlich anwesenden Nutzer auf Übereinstimmung überprüft wird. Ein anwesender Nutzer kann somit ohne wesentliche Stockung oder Verzögerung in die zugangsbeschränkte Zone gelangen. Dies reduziert vor allem bei hohem Verkehrsaufkommen das Risiko, dass sich vor dem Zugang eine Warteschlange bildet.

Die Technologie bietet nicht nur eine schnellere Überprüfung, sie kann auch bei hohen Anforderungen an die Sicherheit eingesetzt werden, weil beispielsweise eine Authentifizierung über eine gesicherte (verschlüsselte) Funkverbindung erfolgt. Die per Funk übertragene Kennung muss im System zu einem registrierten Nutzer gehören; dadurch kann der Nutzer erkannt und die für den Nutzer festgelegten Rechte können ermittelt werden. Neben der Funkverbindung wird ein davon getrennter Kanal (z. B. Erfassen eines optischen Codes) genutzt, für den eine von mehreren anwendbaren Technologien verwendet werden kann. Durch diesen Kanal kann erkannt werden, welcher der möglicherweise zahlreichen anwesenden Nutzer tatsächlich Zugang wünscht, so dass nur diesem Nutzer Zugang gewährt und die für diesen Nutzer festgelegte Gebäudeaktion ausgeführt wird.

Bei der hier beschriebenen Technologie ist zum einen die Überprüfung auf Übereinstimmung auf eine begrenzte Menge von Kennwörtern beschränkt. Zum anderen erfolgt die Authentifizierung und Sicherheitsüberprüfung eines Nutzers basierend auf der empfangenen Kennung, die im Fall eines zugangsberechtigten Nutzers einem gespeicherten Nutzerprofil zugeordnet ist. Für die Erfassung und Verarbeitung von Kennwörtern bedeutet dies, dass an die Kennwörter relativ geringe Anforderungen gestellt werden, beispielsweise hinsichtlich Codierung (z. B. (alpha-) numerisch, PIN, QR Code, Strichcode). Es besteht daher grössere Flexibilität hinsichtlich der Wahl der Art des Kennworts; die Anforderungen an die Sicherheit können aber trotzdem gewährleistet werden.

In einem Ausführungsbeispiel umfasst das Prüfen auf Übereinstimmung ein Erzeugen eines Ergebnissignals. Bei Übereinstimmung veranlasst ein Ausführen einer Gebäudeaktion. Die Gebäudeaktion ist spezifisch für den erkannten Nutzer. Um diese Gebäudeaktion zu ermitteln, wird ein in der Speichereinrichtung gespeichertes Nutzerprofil des erkannten Nutzers gelesen; dort kann beispielsweise das Stockwerk angegeben sein, zu dem der Nutzer zugangsberechtigt ist. Die nutzerspezifische Gebäudeaktion kann ein Entriegeln einer Gebäudetür (z. B. Büro- oder Wohnungstür einschliesslich einer oder mehrerer Türen, die sich auf dem Weg vom Zugang zur Büro- oder Wohnungstür befinden) umfassen. In Verbindung mit einer Aufzugsanlage kann die nutzerspezifische Gebäudeaktion auch ein Registrieren eines Zielrufs auf ein für den Nutzer festgelegtes Zielstockwerk umfassen. Dadurch wird die Benutzerfreundlichkeit verbessert, weil der Nutzer direkt zu einer zugeteilten Aufzugskabine gehen kann, ohne selbst einen Aufzugsruf eingeben zu müssen. Die nutzerspezifische Gebäudeaktion kann auch eine Kombination aus dem Entriegeln einer Gebäudetür und dem Registrieren eines Zielrufs umfassen.

Ausserdem gibt das Ergebnissignal an, dass der Nutzer Zugang zur zugangsbeschränkten Zone hat, während es bei Nichtübereinstimmung angibt, dass der Nutzer keinen Zugang zur zugangsbeschränkten Zone hat. Als Funktion des Ergebnissignals kann in einem Ausführungsbeispiel ein Steuersignal erzeugt werden, um eine (physische) Barriere (z. B. Schranke, Tür oder Drehkreuz) freizugeben. Eine nicht freigegebene Barriere bleibt blockiert. In einem anderen Ausführungsbeispiel aktiviert das Steuersignal bei einer Zugangsverwehrung eine Informationseinrichtung. Die Informationseinrichtung kann z. B. in Verbindung mit einem Zugang ohne eine physische Barriere eingesetzt werden. Wird ein unberechtigter Nutzer am Zugang erkannt, kann in einem Fall die Informationseinrichtung einen Alarm erzeugen, der am Zugang wahrnehmbar (akustisch und/oder visuell) ist. Das Steuersignal kann in einem anderen Fall einen Sicherheitsdienst alarmieren, der daraufhin den als nicht zugangsberechtigt erkannten Nutzer überprüft.

In einem Ausführungsbeispiel erfolgt die Funkverbindung zwischen der Sende- und Empfangseinrichtung und einem mobilen elektronischen Gerät eines Nutzers gemäss einem Bluetooth-Standard oder einem WLAN/WiFi-Standard. Dies ist von Vorteil, weil handelsübliche Mobiltelefone oder Smartphones bereits mit Technologie gemäss einem dieser Standards ausgestattet sind und somit keine speziellen Geräte benötigt werden.

Die hier beschriebene Technologie ermöglicht auch Flexibilität bezüglich der Kennung eines mobilen Geräts. Die Kennung eines mobilen Geräts kann beispielsweise eine dem Gerät fest zugeordnete Geräteidentifikationsnummer oder eine dem mobilen Gerät zugeordnete Telefonnummer umfassen. In einem Ausführungsbeispiel ist jedes mobile Gerät mit einer anwendungsspezifischen Software ausgestattet, die eine für das mobile Gerät einzigartige und zeitlich unveränderliche Kennung erzeugt. Die Kennung (unabhängig davon, ob sie eine Geräteidentifikationsnummer oder eine Telefonnummer umfasst oder durch Software erzeugt ist) ermöglicht die eindeutige Identifikation eines mobilen Geräts.

Im Folgenden sind verschiedene Aspekte der verbesserten Technologie anhand von Ausführungsbeispielen in Verbindung mit den Figuren näher erläutert. In den Figuren haben gleiche Elemente gleiche Bezugszeichen. Es zeigen:

Fig. 1 eine schematische Darstellung eines Anwendungsbeispiels eines Zugangskontrollsystems in Verbindung mit einem Gebäude;

Fig. 2 eine schematische Darstellung eines Ausführungsbeispiels eines Zugangskontrollsystems; und

Fig. 3 ein Ablaufdiagram eines Ausführungsbeispiels eines Zugangskontrollverfahrens als ein Aspekt eines Verfahrens zum Betreiben des Zugangskontrollsystems.

Fig. 1 ist eine schematische Darstellung eines Anwendungsbeispiels eines Zugangskontrollsystems 1 in Verbindung mit einer Situation in einem Gebäude, von dem aus Darstellungsgründen lediglich einige Wände, Räume 4 und Zonen 8, 10 gezeigt sind. Die Räume 4 können z. B. Büros, Wohnungen, Hallen und/oder Aufzugskabinen eines Aufzugsystems sein. In der in Fig. 1 gezeigten Anwendung des Zugangskontrollsystems 1 befinden sich in der Zone 10 mehrere Nutzer 2, die mobile elektronische Geräte 6 (im Folgenden auch als mobile Geräte 6 bezeichnet), mit sich führen. Die Zone 10 unterliegt in diesem Beispiel keiner Zugangsbeschränkung und wird im Folgenden auch als öffentliche Zone 10 bezeichnet. Die öffentliche Zone 10 kann ein Bereich im oder ausserhalb des Gebäudes sein. Ein Zugang 12 trennt die öffentliche Zone 10 von der Zone 8, die einer Zugangsbeschränkung unterliegt und an die Räume 4 angrenzt. Der Fachmann erkennt, dass das Zugangskontrollsystem 1 nicht auf Anwendungen innerhalb

eines Gebäudes beschränkt ist, sondern in analoger Weise auch zur Kontrolle des Zugangs zu einer zugangsbeschränkten Zone auf einem Gelände verwendet werden kann. Unter dem Begriff "Gebäude" sind in dieser Beschreibung z. B. Wohngebäude, Geschäftsgebäude, Sportarenen, Einkaufszentren, aber auch Schiffe zu verstehen.

Das Zugangskontrollsystem 1 überwacht den Zugang 12, sodass nur berechtigte Nutzer 2 in die Zone 8 gelangen können, beispielsweise durch Blockieren oder Freigeben einer Tür, einer Schranke, eines Drehkreuzes, oder einer anderen physischen Barriere oder Schleuse, durch Ansteuern (z. B. Aktivieren) einer Informationseinrichtung 38 im Fall eines Zugangs ohne physische Barriere, wenn ein unberechtigter Nutzer 2 erkannt wird, oder durch Kombinieren dieser Massnahmen. Die Informationseinrichtung 38 kann z. B. einen optischen und/oder akustischen Alarm auslösen oder eine Benachrichtigung eines Sicherheitsdienstes veranlassen. In Fig. 1 ist das Zugangskontrollsystem 1 zur Veranschaulichung als im Zugang 12 angeordnet eingezeichnet. Je nachdem für welches Verkehrsaufkommen das Zugangskontrollsystem 1 vorgesehen ist, besteht der Zugang 12 aus mehreren einzelnen Schleusen; in Fig. 1 kann z. B. jedes der beiden Drehkreuze 36 eine Schleuse darstellen. Der Fachmann erkennt, dass in einer konkreten Implementierung das Zugangskontrollsystem 1 bzw. seine Komponenten auf verschiedene Art und Weise angeordnet sein können.

Die in Fig. 1 dargestellten Räume 4 können beispielsweise zu einer Gruppe von Aufzügen gehören, die z. B. sechs Aufzüge (A-F) umfasst. Wird ein Nutzer 2 am Zugang 12 erkannt, bedeutet dies in einem Ausführungsbeispiel, dass der Nutzer 2 mit einem der Aufzüge auf ein für diesen Nutzer 2 festgelegtes Zielstockwerk transportiert werden möchte. Mit dem Erkennen des Nutzers 2 wird ein Zielruf veranlasst, dem eine Aufzugssteuerung einen Aufzug zuweist. Der zugewiesene Aufzug wird dem Nutzer 2 mitgeteilt, beispielsweise mittels einer Anzeigeeinheit. In der in Fig. 1 gezeigten Situation kann jedem Drehkreuz 36 jeweils eine Anzeigeeinheit zugeordnet sein. Nutzt der Nutzer 2 beispielsweise eines der in Fig. 1 gezeigten Drehkreuze 36, erkennt das Zugangskontrollsystem 1, an welchem Drehkreuz 36 sich der Nutzer 2 befindet und steuert die dort angeordnete Anzeigeeinheit an, um den zugeteilten Aufzug (z. B. "A") anzuzeigen.

Wie in Fig. 1 angedeutet, umfasst das Zugangskontrollsystem 1 gemäss einem Ausführungsbeispiel eine Sende- und Empfangseinrichtung 14 (in Fig. 1 als TX/RX dargestellt) und eine Codeverarbeitungseinrichtung (16); weitere Komponenten des Zugangskontrollsystem 1 sind in Fig. 2 gezeigt. In einem hier beschriebenen Ausführungsbeispiel ist die Sende- und Empfangseinrichtung zum Empfang von Funksignalen ausgestaltet, sie ist im Folgenden auch als Transceiver 14 bezeichnet. Der Transceiver 14 kommuniziert mit den mobilen elektronischen Geräten 6, wenn sie sich in Funkreichweite zum Transceiver 14 befinden, d. h. ein von einem mobilen Gerät 6 ausgesendetes Funksignal hat am Ort des Transceivers 14 eine Signalstärke (beispielsweise ausgedrückt durch einen RSSI-Wert (Received Signal Strength Indicator)), die grösser als ein für einen sicheren Empfang festgelegter Schwellenwert ist. Die Kommunikation erfolgt beispielsweise über ein Nahfeld-Funknetz wie z. B. ein Bluetooth-Funknetz, WLAN/WiFi- oder ein ZigBee-Funknetz. Bluetooth ist ein Standard gemäss IEEE 802.15.1, WLAN/WiFi ist ein Standard gemäss IEEE 802.11, Zig-Bee ist ein Standard gemäss IEEE 802.15.4; solche Funknetze gemäss diesen Standards dienen der kabellosen Vernetzung von Geräten über eine kurze Distanz von ca. einigen Metern bis ca. hundert Meter. Das Funknetz bildet dabei die Schnittstelle, über die das mobile elektronische Gerät 6 und der Transceiver 14 miteinander kommunizieren können.

In der in Fig. 1 gezeigten Situation ist die hier beschriebene Technologie in vorteilhafter Weise anwendbar, um das Zugangskontrollsystem 1 mit möglichst geringer Komplexität zu betreiben und dem Nutzer 2 komfortabel Zugang zur zugangsbeschränkten Zone 8 zu gewähren. Kurz und beispielhaft zusammengefasst erfolgt der Betrieb des Zugangskontrollsystems 1 gemäss einem Ausführungsbeispiel wie folgt: Sobald ein Nutzer 2 in Funkreichweite zum Transceiver 14 ist, kommuniziert sein mobiles Gerät 6 über eine Funkverbindung automatisch mit dem Transceiver 14 und das mobile Gerät 6 sendet seine gerätespezifische Kennung zum Transceiver 14. In der Situation gemäss Fig. 1 empfängt der Transceiver 14 eine Vielzahl von Kennungen. Das Zugangssystem 1 speichert diese Kennungen in dafür angelegten Datensätzen und "weiss" daher, wie viele mobile Geräte 6 sich zu einem bestimmten Zeitpunkt in Funkreichweite befinden und, wenn deren Nutzer 2 für das Gebäude registrierte Nutzer 2 sind, zu welchen Nutzern 2 die mobilen Geräte 6 gehören. Zu diesem Zeitpunkt kann das Zugangskontrollsystem 1 für jeden registrierten Nutzer 2 prüfen, welche Rechte für den Nutzer im Gebäude

festgelegt sind (z. B. Zutrittsberechtigung zu einem oder mehreren Räumen 4 und/oder Stockwerken, einschliesslich evtl. zeitlicher Beschränkungen).

Die so erfassten Nutzer 2 stellen eine Gruppe von anwesenden Nutzern 2 dar. Möchte nun einer der anwesenden Nutzer 2 Zugang zur zugangsbeschränkten Zone 8, bewegt sich der Nutzer 2 in Richtung des Zugangs 12. Dort angekommen, präsentiert der Nutzer 2 der Codeverarbeitungseinrichtung (16, 22) ein Kennwort. Das Zugangskontrollsystem 1 ermittelt im Rahmen eines Codeerfassungs- und Codeauswerteverfahrens das Kennwort und vergleicht es mit gespeicherten Kennwörtern, die den anwesenden Nutzern 2 zugeordnet sind. Dieser Vergleich ist auf die Gruppe der anwesenden Nutzer 2 beschränkt; es werden somit nur die Datensätze dieser Gruppe daraufhin durchsucht, ob das ermittelte Kennwort zu einem der gespeicherten Datensätze passt. Dadurch kann erkannt werden, welcher der anwesenden Nutzer 2 zu diesem Zeitpunkt tatsächlich Zugang wünscht und – je nach Ausgestaltung – an welcher Schleuse (z. B. Drehkreuz 36) sich der Nutzer 2 befindet. Für diesen Nutzer 2 kann beispielsweise eine in einem Nutzerprofil festgelegte Gebäudeaktion veranlasst werden; für den Nutzer 2 können beispielsweise ein Zielruf registriert und daran anschliessend ein Aufzug zugeteilt werden, der den Nutzer 2 auf das Stockwerk transportiert, auf dem sich der Arbeitsplatz des Nutzers 2 befindet.

Fig. 2 zeigt eine schematische Darstellung eines Ausführungsbeispiels des Zugangskontrollsystems 1. Das Zugangskontrollsystem 1 ist in einem Ausführungsbeispiel modular aufgebaut und umfasst die Codeverarbeitungseinrichtung, die eine Codeerfassungseinrichtung 16 (Code in Fig. 2) und ein Codeauswertemodul 22 (Codeauswertung in Fig. 2) umfasst. Zusätzlich umfasst das Zugangskontrollsystem 1 den Transceiver 14, einen Prozessor 20, eine Speichereinrichtung 26 (Speicher in Fig. 2) und eine Zwischenspeichereinrichtung 28 (Zwischenspeicher in Fig. 2). Der Fachmann erkennt, dass mindestens eine der Speichereinrichtungen 26, 28 auch der Codeverarbeitungseinrichtung (16, 22) zugeordnet werden kann oder dass die Funktion der Zwischenspeichereinrichtung 28 durch die Speichereinrichtung 26 wahrgenommen werden kann und somit die Zwischenspeichereinrichtung 28 in einem Ausführungsbeispiel entfallen kann.

Der Prozessor 20 hat einen Ausgang 32 für ein Steuersignal und einen Eingang 30 für ein vom Codeauswertemodul 22 erzeugtes Ergebnissignal. Abhängig vom Ergebnissignal steuert der Prozessor 20 das Zugangskontrollsystem 1 so, dass dem Nutzer 2 Zugang gewährt oder verwehrt wird. Bei Zugangsgewährung kann beispielsweise auch ein Zielruf veranlasst werden und der diesem Zielruf zugeteilte Aufzug kann dem Nutzer 2 angezeigt werden. Trennt beispielsweise eine physische Barriere (z. B. Drehkreuz 36 in Fig. 1) die Zonen 8, 10, gibt das Steuersignal die Barriere frei (beispielsweise in Verbindung mit der Anzeige des zugeteilten Aufzugs) oder blockiert diese. Erfolgt die Zonentrennung dagegen ohne eine physische Barriere, steuert das Steuersignal im Fall eines unberechtigten Nutzers 2 beispielsweise die Informationseinrichtung 38 für eine Alarmerzeugung an oder alarmiert einen Sicherheitsdienst. Die Informationseinrichtung 38 kann auch angesteuert werden, um in Verbindung mit einer Barriere dem Nutzer 2 oder einem Sicherheitsdienst anzuzeigen, dass die Barriere freigegeben oder blockiert wurde.

Die Codeerfassungseinrichtung 16 kann ein Lesegerät umfassen, das Daten basierend auf einer von unterschiedlichen bekannten Technologien erfassen kann. Das Lesegerät kann beispielsweise Daten von Magnetkarten, Chipkarten, RFID Karten oder mobilen elektronischen Geräten (z. B. Mobiltelefone, Smartphone, Tablet) lesen, oder Daten von optischen Codes (Barcodes, QR Codes, Farbcodes), die auf verschiedenen Trägermaterialien aufgedruckt sind oder auf Anzeigen von mobilen elektronischen Geräten (z. B. Mobiltelefone, Smartphone, Tablet) dargestellt werden, erfassen. Das Lesegerät kann in einem anderen Ausführungsbeispiel eine Vorrichtung zum Erfassen und/oder Erkennen von biometrischen Parametern (z. B. Muster von Fingerkuppen, Handflächen oder Augen (Iris), oder Charakteristika von Stimmen) umfassen.

Kommt im Lesegerät beispielsweise die Radio Frequency Identification (RFID) Technologie zur Anwendung, ist das Lesegerät ein RFID Leser, der Daten von einer in Funkreichweite platzierten RFID Karte empfängt. Die Daten, beispielsweise einen Identifikationscode umfassend, sind in einem Datenspeicher der RFID Karte gespeichert. Die vom RFID Leser und der RFID Karte verwendete Funkfrequenz beträgt beispielsweise 125 kHz, 13,56 MHz oder 2,45 GHz. Kommt dagegen eine optische Technologie zur Anwendung, ist das Lesegerät ein optisches Lesegerät (z. B. eine Kamera oder ein Scanner), das das Muster eines optischen Codes, der auf einem

Trägermaterial aufgedruckt ist oder auf einem elektronischen Gerät angezeigt wird, erfasst. Eine beispielhafte Technologie zum Erzeugen und Erfassen eines auf einem elektronischen Gerät angezeigten optischen Farbcodes ist in WO 2015/049186 beschrieben.

Der Transceiver 14 und die Codeerfassungseinrichtung 16 (einschliesslich anderer Komponenten der Codeverarbeitungseinrichtung) können in einem Gehäuse, das z. B. wie in Fig. 1 gezeigt im Zugang 12 angeordnet ist, angeordnet sein. Alternativ dazu können der Transceiver 14 und die Codeerfassungseinrichtung 16 (einschliesslich anderer Komponenten der Codeverarbeitungseinrichtung) auch getrennt voneinander als separate Einheiten angeordnet sein, beispielsweise räumlich voneinander getrennt in einem Bereich um den Zugang 12, wobei die Codeerfassungseinrichtung 16 so anzuordnen ist, dass sie für die Nutzer 2 zugänglich ist und zwar so, dass die Nutzer 2 der Reihe nach ihre Kennwörter präsentieren können. In einer Ausgestaltung des Zugangskontrollsystems 1 ist an jeder Barriere (z. B. Drehkreuz 36) eine Codeerfassungseinrichtungen 16 vorhanden.

Das Codeauswertemodul 22 ist zur Veranschaulichung als separate Einheit gezeigt, die mit dem Prozessor 20 und der Zwischenspeichereinrichtung 28 verbunden ist. In einem Ausführungsbeispiel bilden das Codeauswertemodul 24 und die Codeerfassungseinrichtung 16 eine Einheit. Die Speichereinrichtungen 26, 28 sind ebenfalls zur Veranschaulichung als separate Einheiten gezeigt; je nach Ausgestaltung können sie in einer Speichereinrichtung zusammengefasst sein, wo sie beispielsweise getrennte Speicherbereiche belegen. Unabhängig davon können die Speichereinrichtungen 26, 28 beispielsweise ein Festplatten (HDD)- oder CD/DVD-Laufwerk, ein Halbleiterlaufwerk/Solid-State-Disk (SSD), oder Kombinationen davon, oder andere Speichereinrichtungen für digitale Daten umfassen.

Gemäss der hier beschriebenen Technologie sendet das mobile Gerät 6 seine gerätespezifische Kennung zum Transceiver 14 sobald es in Funkreichweite zum Transceiver 14 ist. Der Prozessor 20 steuert die Speicherung der empfangenen Kennung als Datensatz in der Zwischenspeichereinrichtung 28. In der in Fig. 1 gezeigten Situation halten sich mehrere Nutzer 2 in der öffentlichen Zone 10 auf. Dabei ist beispielhaft angenommen, dass die mobilen Geräte 6 der anwesenden Nutzer 2 für die Nutzung der

hier beschriebenen Technologie, u.a. Senden einer Kennung, ausgestaltet sind. Von den anwesenden Nutzern 2 können einige Zugang zur zugangsbeschränkten Zone 8 wünschen, einige können von der Zone 8 kommend auf dem Weg zu einem Gebäudeausgang sein und wiederum andere können auf dem Weg zu einem anderen Teil des Gebäudes sein. Das bedeutet in der gezeigten Situation, dass nicht jeder Nutzer 2, der sich in der öffentlichen Zone 10 aufhält, auch tatsächlich in die Zone 8 gelangen möchte. Aus Sicht des Zugangskontrollsystems 1 sind jedoch alle anwesenden Nutzer 2 potentielle Nutzer 2, die früher oder später Zugang wünschen könnten.

Die Zwischenspeichereinrichtung 28 speichert in einer solchen Situation für jeden anwesenden Nutzer 2 einen Datensatz, der die Kennung des dem Nutzer 2 zugeteilten mobilen Geräts 6 und das Kennwort enthält. Dabei kann es sich sowohl um mobile Geräte 6 handeln, deren Nutzer 2 als zugangsberechtige Nutzer 2 im Zugangskontrollsystem 1 registriert sind, als auch um mobile Geräte 6, deren Nutzer 2 nicht registriert sind. Verlässt ein Nutzer 2 die öffentliche Zone 10, so dass sich das zugehörige mobile Gerät 6 ausserhalb der Funkreichweite befindet, wird der für diesen Nutzer 2 angelegte Datensatz in der Zwischenspeichereinrichtung 28 gelöscht und die Zwischenspeichereinrichtung 28 aktualisiert.

Das Zugangskontrollsystem 1 ermittelt die anwesenden Nutzer 2 mit Hilfe der Kommunikation zwischen den mobilen Geräten 6 und dem Transceiver 14. In jedem mobilen Gerät 6 ist ein Funkmodul, beispielsweise ein Modul gemäss einem Bluetooth Standard, aktiviert, um mit dem Transceiver 14 kommunizieren zu können, sobald es sich in Funkreichweite zum Transceiver 14 befindet. Das mobile Gerät 6 ist zum Senden der gerätespezifischen Kennung und, je nach Ausgestaltung, auch des Kennworts entsprechend konfiguriert. Es kann z. B. eine anwendungsspezifische Softwareanwendung (auch als App bezeichnet) aufweisen, die beispielsweise durch den Nutzer 2 aktivierbar ist. Die anwendungsspezifische Softwareanwendung wird in einem Ausführungsbeispiel in Verbindung mit der Zugangskontrolle und der Nutzung von Aufzügen verwendet. Die anwendungsspezifische Software erzeugt in einem Ausführungsbeispiel eine für das mobile Gerät 6 einzigartige und zeitlich unveränderliche Kennung. Eine solche durch Software erzeugte Kennung stellt eine Alternative zu der oben genannten Geräteidentifikationsnummer und einer Telefonnummer dar. Das Kennwort kann in entsprechender Weise erzeugt werden. In einem Ausführungsbeispiel

empfängt das mobile Gerät 6 das Kennwort vom Zugangskontrollsystem 1 und speichert es in einer Speichereinrichtung des mobilen Geräts 6.

Für jeden registrierten Nutzer 2 ist im Zugangskontrollsystem 1 ein Nutzerprofil angelegt, d. h. es ist als Datensatz in einer Datenbank 34 gespeichert. Die Datenbank 34 ist in einem Ausführungsbeispiel in der Speichereinrichtung 26 eingerichtet. Das Nutzerprofil umfasst persönliche Daten des Nutzers 2 (z. B. Name, Berechtigungsgrund (Bewohner, Mitarbeiter, externer Dienstleister, Besucher)), Zugangsberechtigungen (z. B. bestimmte Räume 4 und Stockwerke) und evtl. zeitliche Zugangsbeschränkungen (z. B. Zugang von Montag bis Freitag, von 7:00 bis 20:00). Im Nutzerprofil ist dem Nutzer 2 ausserdem mindestens ein mobiles Gerät 6 zugeordnet. Alternativ zum Anlegen des Nutzerprofils im Zugangskontrollsystem 1 kann das Nutzerprofil in einer Datenbank eines Gebäudeverwaltungssystems angelegt sein, wobei das Zugangskontrollsystem 1 auf diese Datenbank mittels eines Kommunikationsnetzes zugreifen kann.

Wünscht einer der anwesenden Nutzer 2 Zugang zur zugangsbeschränkten Zone 8, präsentiert der Nutzer 2 das Kennwort, das die Codeerfassungseinrichtung 16 erfasst und dem Codeauswertemodul 22 zuführt. Das Codeauswertemodul 24 startet einen Suchalgorithmus, um zu ermitteln, ob das erfasste Kennwort in der Zwischenspeichereinrichtung 28 einem anwesenden Nutzer 2 zugeordnet werden kann. Stimmt das erfasste Kennwort mit einem gespeicherten Kennwort überein, ist aus der Gruppe der Nutzer 2 derjenige Nutzer 2 erkannt, der zu diesem Zeitpunkt Zugang wünscht.

Das mobile Gerät 6 kann beispielsweise ein Mobiltelefon, ein Smartphone, ein Tablet PC oder eine Smartwatch sein, wobei diese Geräte üblicherweise mit Hardware ausgestattet sind, die eine Kommunikation über ein Nahfeld-Funknetz ermöglichen. Das mobile Gerät 6 kann aber auch eine Brille mit Miniaturcomputer oder ein anderes am Körper getragenes, computergestütztes Gerät (auch als "Wearable Device" bezeichnet) sein, wenn diese Geräte für eine Nahfeld-Kommunikation und zur Speicherung von Daten vorgesehen sind. Je nach Ausgestaltung des mobilen Geräts 6 kann es z. B. über ein graphisches Nutzerinterface (auch als Graphical User Interface, GUI, bezeichnet) verfügen, um das mobile Gerät 6 und dessen Funktionen selektiv aktivieren und deaktivieren zu können.

Mit dem Verständnis der oben beschriebenen prinzipiellen Systemkomponenten und deren Funktionalitäten, erfolgt im Folgenden in Verbindung mit Fig. 3 eine Beschreibung eines beispielhaften Zugangskontrollverfahrens als ein Aspekt eines Verfahrens zum Betreiben des Zugangskontrollsystems 1. Die Beschreibung erfolgt mit Bezug auf einen Nutzer 2, der am Zugang 12 die zugangsbeschränkte Zone 8 zu betreten wünscht, beispielsweise um dort einen Aufzug zu benutzen. Der Nutzer 2 trägt das mobile Gerät 6 bei sich und hat dessen Funkmodul (z. B. für Bluetooth-Kommunikation) aktiviert. Eine dazugehörige Softwareanwendung ist ebenfalls aktiviert. Das Verfahren beginnt in einem Schritt **S1** und endet in einem Schritt **S12**.

Befindet sich der Nutzer 2 mit seinem mobilen Gerät 6 in der öffentlichen Zone 10 und in Funkreichweite zum Transceiver 14, empfängt der Transceiver 14 in einem Schritt **S2** eine vom mobilen Gerät 6 ausgesendete gerätespezifische Kennung Ki. Der Transceiver 14 und das mobile Gerät 6 kommunizieren gemäss dem gleichen Kommunikationsstandard, in diesem Ausführungsbeispiel über eine Funkverbindung gemäss einem Bluetooth Standard.

Die empfangene Kennung Ki wird in einem Schritt **S3** gespeichert. Die Kennung Ki wird in einem dafür angelegten Datensatz DSi in der Zwischenspeichereinrichtung 28 gespeichert.

In einem Schritt **S4** wird ausserdem ein Kennwort Ci im für die Kennung Ki angelegten Datensatzes DSi gespeichert. In einem Ausführungsbeispiel sendet das mobile Gerät 6 das Kennwort Ci. Der Transceiver 14 empfängt in diesem Fall ausserdem das Kennwort Ci des Nutzers 2. Die Kennung Ki und das Kennwort Ci können im Wesentlichen gleichzeitig oder zeitlich nacheinander vom mobilen Gerät 6 gesendet werden. Entsprechend dazu kann deren Speicherung im Wesentlichen gleichzeitig oder zeitlich nacheinander erfolgen.

In einem Ausführungsbeispiel erzeugt das Zugangskontrollsystem 1 das Kennwort Ci und speichert es im für die empfangene Kennung Ki angelegten Datensatz DSi sobald sich der Nutzer 2 mit seinem mobilen Gerät 6 in der öffentlichen Zone 10 und in Funkreichweite zum Transceiver 14 befindet. Das Zugangskontrollsystem 1 sendet das Kennwort Ci zum

mobilen Gerät 6 des Nutzers 2. Auch in diesem Fall speichert der Datensatz DSi für diesen Nutzer 2 sowohl die Kennung Ki als auch das Kennwort Ci

Die Schritte **S2** – **S4** werden für jedes mobile Gerät 6 ausgeführt, das sich in Funkreichweite zum Transceiver 14 befindet und gemäss dem gleichen Kommunikationsstandard arbeitet wie der Transceiver 14. Je nach Anzahl der Nutzer 2 in der öffentlichen Zone 10 kann zu einem bestimmten Zeitpunkt eine Vielzahl von Kennungen und dazugehörigen Kennwörtern, entsprechend einer Gruppe von anwesenden Nutzern 2, in der Zwischenspeichereinrichtung 28 gespeichert sein. Der Fachmann erkennt, dass die Zwischenspeichereinrichtung 28 aktualisiert wird, wenn ein mobiles Gerät 6 nicht mehr in Funkreichweite ist, z. B. weil der dazugehörige Nutzer 2 die öffentliche Zone 10 verlassen hat ohne Zugang zur zugangsbeschränkten Zone 8 zu wünschen oder weil der dazugehörige Nutzer 2 bereits die zugangsbeschränkte Zone 8 betreten hat. Die Zwischenspeichereinrichtung 28 speichert somit die Datensätze für Nutzer 2, die zu einem bestimmten Zeitpunkt in der öffentlichen Zone 10 anwesend sind.

In einem Schritt S5 wird ermittelt, ob der Nutzer 2 authentifiziert werden kann. Dies erfolgt mittels der empfangenen Kennung Ki. Kann die empfangene Kennung Ki einem im Zugangskontrollsystem 1 gespeicherten Nutzerprofil zugeordnet werden, ist der Nutzer 2 als zugangsberechtigt authentifiziert. Kann der Nutzer 2 authentifiziert werde, schreitet das Verfahren entlang des Ja-Zweiges zu einem Schritt **S6**. Kann der Nutzer 2 dagegen nicht authentifiziert werden, schreitet das Verfahren entlang des Nein-Zweiges zu einen Schritt **S10**, in dem der Nutzer 2 als nicht zugangsberechtigt betrachtet wird. Ein solche Authentifizierung erfolgt für jeden anwesenden Nutzer 2.

Im Schritt **S6** wird ermittelt, ob einer der anwesenden Nutzer 2 Zugang zur zugangsbeschränkten Zone 8 wünscht. Das Zugangskontrollsystem 1 erkennt diesen Wunsch mit Hilfe der Codeerfassungseinrichtung 16, wenn der Nutzer 2 das ihm zugeordnete Kennwort Cd präsentiert. In einem Ausführungsbeispiel hält der Nutzer 2 das mobile Gerät 6 in die Nähe der Codeerfassungseinrichtung 16, damit sie das auf der Anzeigeeinrichtung des mobilen Geräts 6 als optischen Code dargestellte Kennwort Cd erfassen kann. Wird ein Zugangswunsch erkannt, schreitet das Verfahren entlang des Ja-Zweiges zu einem Schritt **S7**. Andernfalls schreitet das Verfahren entlang des Nein-Zweiges zurück zum Schritt **S2**.

In einem Schritt **S7** wird mittels des in Schritt **S6** erfassten Kennworts Cd ermittelt, ob dieses einem in der Zwischenspeichereinrichtung 28 gespeicherten Kennwort Ci zugeordnet werden kann. Ist dies der Fall, ist aus der Gruppe der anwesenden Nutzer 2 derjenige Nutzer 2 erkannt, der zu diesem Zeitpunkt Zugang wünscht. In diesem Fall schreitet das Verfahren entlang des Ja-Zweiges zu einem Schritt **S11**, in dem für diesen Nutzer 2 eine nutzerspezifische Gebäudeaktion ausgeführt wird. Die Gebäudeaktion kann beispielsweise darin bestehen, dass für den Nutzer 2 ein Zielruf (gemäss den Daten des für diesen Nutzer 2 bestehenden Nutzerprofils) ausgelöst wird, diesem Zielruf ein Aufzug zugewiesen wird und der zugewiesene Aufzug dem Nutzer 2 am Zugang 12 angezeigt wird. Die Gebäudeaktion kann auch darin bestehen, dass eine oder mehrere Türen entriegelt werden, an denen dieser Nutzer 2 zugangsberechtigt ist. Der Fachmann erkennt, dass diese Gebäudeaktionen auch in Kombination ausgeführt werden können.

Ist dagegen dem erfassten Kennwort Cd kein in der Zwischenspeichereinrichtung 28 gespeicherten Kennwort Ci zugeordnet, schreitet das Verfahren entlang des Nein-Zweiges zum Schritt **S10** und dem Nutzer 2 wird der Zugang verwehrt. Je nach Ausgestaltung kann eine Benachrichtigung den Nutzer 2 beispielsweise darüber informieren, dass dass sich der Nutzer 2 an einen Gebäudeverantwortlichen (z. B. Empfangspersonal, Sicherheitspersonal) wenden soll. Unabhängig davon kann im Schritt **S10** auch das Sicherheitspersonal direkt benachrichtigt werden.

In einem Ausführungsbeispiel ist das Zugangskontrollsystem 1 mit einem Aufzugsystem verbunden, insbesondere mit einer Aufzugsteuerung. Die Kommunikation zwischen dem Zugangskontrollsystem 1 und der Aufzugsteuerung kann über ein im Gebäude vorhandenes Kommunikationsnetzwerk erfolgen. Geschieht die Zugangskontrolle beispielsweise in der Eingangshalle des Gebäudes, die die Nutzer 2 passieren müssen, um zu den Aufzügen zu gelangen, kann bei jeder Zugangsgewährung für den betreffenden Nutzer 2 ein Zielruf veranlasst werden. Die Aufzugsteuerung des Aufzugssystems verarbeitet den Zielruf und teilt ihm einen Aufzug zu. Der dem Zielruf zugeteilte Aufzug kann dem Nutzer 2 beispielsweise durch ein Terminal am Zugang 12 angezeigt und/oder mittels Sprache mitgeteilt werden. Der Nutzer 2 kann somit ohne einen Aufzugsruf eingeben zu müssen direkt zum zugeteilten Aufzug gehen.

Je nach Ausgestaltung des Gebäudes und der Handhabung der Zugangsberechtigungen, kann das Zugangskontrollsystem 1 auch Besuchern Zugang gewähren und für die Besucher festgelegte Gebäudeaktionen veranlassen. In Verbindung mit einer Aufzugssteuerung kann beispielhafte als Gebäudeaktion einen Zielruf für den Besucher erzeugt werden. Ein zugewiesener Aufzug transportiert den Besucher auf das Stockwerk, auf dem sich der Gastgeber befindet. Das Stockwerk des Gastgebers ist beispielsweise in einem für den Besucher temporär angelegten Besucherprofil in Verbindung mit anderen Einladungsdaten (z. B. Datum, Zeit, Gastgeber) gespeichert. Der Besucher, vor allem wenn er erstmalig im Gebäude ist, braucht sich somit nicht mit der Eingabe des Zielstockwerks zu befassen. Dem Besucher kann außerdem weitere Information zur Verfügung gestellt werden, um sich im Gebäude besser orientieren zu können, beispielsweise kann dem Besucher mitgeteilt werden, in welche Richtung (eventuell auch wie weit) er nach dem Aussteigen auf dem Stockwerk gehen soll. Die Mitteilung solcher Wegeleitungs-Information kann beispielsweise mittels des mobilen Geräts 6 des Besuchers und/oder Anzeigen auf den Stockwerken oder in der Aufzugskabine erfolgen. In einem Ausführungsbeispiel erzeugt und sendet das Zugangskontrollsystem 1 eine Nachricht für den Gastgeber, die den Gastgeber darüber informiert, dass dem Besucher Zugang gewährt wurde. Der Gastgeber kann sich somit zeitnah auf das Erscheinen des Besuchers vorbereiten.

Patentansprüche

1. Verfahren zum Betreiben eines Systems (1) zur Kontrolle eines Zugangs zu einer zugangsbeschränkten Zone (8) in einem Gebäude oder auf einem Gelände, wobei das System (1) eine Sende- und Empfangseinrichtung (14) zur Funkkommunikation mit von Nutzern (2) mitgeführten mobilen elektronischen Geräten (6), eine Speichereinrichtung (26, 28), eine Prozessoreinrichtung (20) und eine Codeverarbeitungseinrichtung (16, 22) umfasst, wobei das Verfahren umfasst:

Empfangen einer ersten Kennung (Ki) eines ersten mobilen elektronischen Geräts (6) eines ersten Nutzers (2) durch die Sende- und Empfangseinrichtung (14), wenn sich das erste mobile elektronische Gerät (6) in einer öffentlichen Zone (10) befindet, von der aus der erste Nutzer (2) Zugang zur zugangsbeschränkten Zone (8) ersuchen kann;

Speichern der empfangenen ersten Kennung (Ki) in der Speichereinrichtung (26, 28), wobei für die erste Kennung (Ki) ein erster Datensatz (DSi) angelegt wird, der dem in der öffentlichen Zone (10) anwesenden ersten Nutzer (2) zugeordnet ist, und wobei in der Speichereinrichtung (26, 28) eine Vielzahl von Datensätzen speicherbar ist, wobei jeder Datensatz einem in der öffentlichen Zone (10) anwesenden Nutzern (2) zugeordnet ist;

Speichern eines ersten Kennworts (Ci) im ersten Datensatz (DSi), so dass das erste Codewort (Ci) der ersten Kennung (Ki) zugeordnet ist;

Ermitteln durch die Prozessoreinrichtung (20), ob die erste Kennung (Ki) in einer Datenbank (34) einem Nutzerprofil zugeordnet ist, um, wenn eine solche Zuordnung besteht, den ersten Nutzer (2) als zugangsberechtigt zu authentifizieren;

Erfassen eines vom ersten Nutzer (2) präsentierten Kennworts (Cd) durch die Codeverarbeitungseinrichtung (16, 22), wenn der erste Nutzer (2) Zugang zur zugangsbeschränkten Zone (8) ersucht; und

Ermitteln durch die Prozessoreinrichtung (20), ob das erfasste Kennwort (Cd) mit dem im ersten Datensatz (DSi) der Speichereinrichtung (26, 28) gespeicherten ersten Kennwort (Ci) übereinstimmt, wobei bei Übereinstimmung der erste Nutzer (2) als zugangsersuchender Nutzer (2) erkannt wird.

2. Verfahren nach Anspruch 1, ausserdem umfassend Erzeugen eines Ergebnissignals, das ein Ausführen einer Gebäudeaktion veranlasst, wenn das erfasste Kennwort (Cd) mit dem ersten Kennwort (Ci) übereinstimmt.

3. Verfahren nach Anspruch 2, ausserdem aufweisend Lesen eines in der Datenbank (34) gespeicherten Nutzerprofils des ersten Nutzers (2), um eine nutzerspezifische Gebäudeaktion zu ermitteln.

4. Verfahren nach Anspruch 3, beim dem die nutzerspezifische Gebäudeaktion ein Entriegeln einer Gebäudetür, an der der erste Nutzer (2) zugangsberechtigt ist, oder ein Registrieren eines Zielrufs auf ein für den ersten Nutzer (2) festgelegtes Zielstockwerk, oder eine Kombination aus dem Entriegeln einer Gebäudetür und dem Registrieren eines Zielrufs umfasst.

5. Verfahren nach einem der Ansprüche 2-4, ausserdem aufweisend Erzeugen eines Steuersignals als Funktion des Ergebnissignals, um eine Barriere (18, 36) freizugeben, damit der Nutzer (2) die zugangsbeschränkte Zone (8) betreten kann.

6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Codeverarbeitungseinrichtung (16, 22) ausgestaltet ist, um das Kennwort (Cd) von einer Anzeigeeinrichtung des mobilen elektronischen Geräts (6), die das Kennwort (Cd) in maschinenlesbarer Form darstellt, zu erfassen.

7. Verfahren nach Anspruch 6, bei dem das dargestellte Kennwort ein numerischer Code, ein alphanumerischer Code, ein Strichcode, ein QR-Code oder ein Farbcode ist.

8. Verfahren nach einem der Ansprüche 1-5, bei dem die Codeverarbeitungseinrichtung (16, 22) ausgestaltet ist, um das Kennwort von einem Datenträger, auf dem das Kennwort dargestellt oder gespeichert ist, zu erfassen.

9. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Funkverbindung zwischen der Sende- und Empfangseinrichtung (14) und einem mobilen elektronischen Gerät (6) eines Nutzers (2) gemäss einem Bluetooth-Standard oder einem WLAN/WiFi-Standard erfolgt, und wobei die Sende- und Empfangseinrichtung (14) die

gerätespezifische Kennung (Ki) über die Funkverbindung empfängt, wenn sich das mobile elektronische Gerät (6) in Funkreichweite der Sende- und Empfangseinrichtung (14) befindet.

10. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Kennung (Ki) von einer anwendungsspezifischen Software, die auf dem mobilen Gerät (6) aktiv ist, erzeugt ist, wobei die Kennung (Ki) zeitlich unveränderlich ist.

11. Verfahren nach einem der Ansprüche 1-10, bei dem die Kennung eine Geräteidentifikationsnummer oder eine einem mobilen Gerät (6) zugeordnete Telefonnummer umfasst.

12. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die erste Kennung (Ki) und das erste Kennwort (Ci) durch die Sende- und Empfangseinrichtung (14) empfangen werden, wenn sich das erste mobile elektronische Geräte (6) in der öffentlichen Zone (10) befindet und die erste Kennung (Ki) und das erste Codewort (Ci) aussendet.

13. Verfahren nach einem der vorhergehenden Ansprüche, bei dem, wenn sich eine Vielzahl von mobilen elektronischen Geräten (6) in der öffentlichen Zone (10) befindet, für jedes mobile elektronische Gerät (6) eines Nutzers (2), das eine gerätespezifische Kennung und einen elektronischen Code sendet, in der Speichereinrichtung (26, 28) ein Datensatz gespeichert wird.

14. System (1) zur Kontrolle eines Zugangs zu einer zugangsbeschränkten Zone (8) in einem Gebäude oder auf einem Gelände, wobei das System (1) umfasst:

eine Sende- und Empfangseinrichtung (14) zur Funkkommunikation mit einem von einem ersten Nutzer (2) mitgeführten ersten mobilen elektronischen Gerät (6), die zu einem Empfang einer ersten Kennung (Ki) des ersten mobilen elektronischen Geräts (6) ausgestaltet ist, wenn sich das erste mobile elektronische Gerät (6) in einer öffentlichen Zone (10) befindet, von der aus der erste Nutzer (2) Zugang zur zugangsbeschränkten Zone (8) ersuchen kann;

eine Speichereinrichtung (26, 28), die ausgestaltet ist, um für die erste Kennung (Ki) einen ersten Datensatz (DSi) anzulegen, der dem in der

öffentlichen Zone (10) anwesenden ersten Nutzer (2) zugeordnet ist, und um ein erstes Kennwort (Ci) im ersten Datensatz (DSi) zu speichern, so dass das erste Kennwort (Ci) der ersten Kennung (Ki) zugeordnet ist, wobei in der Speichereinrichtung (26, 28) eine Vielzahl von Datensätzen speicherbar ist;

eine Codeverarbeitungseinrichtung (16, 22), die ausgestaltet ist, um ein vom ersten Nutzer (2) präsentiertes Kennwort (Cd) zu erfassen, wenn der erste Nutzer (2) Zugang zur zugangsbeschränkten Zone (8) ersucht; und

eine Prozessoreinrichtung (20), die ausgestaltet ist,

- zu ermitteln, ob die erste Kennung (Ki) in einer Datenbank (34) einem Nutzerprofil zugeordnet ist,
- wenn eine solche Zuordnung besteht, den ersten Nutzer (2) als zugangsberechtigt zu authentifizieren, und
- zu ermitteln, ob das erfasste Kennwort (Cd) dem im ersten Datensatz (DSi) der Speichereinrichtung (26, 28) gespeicherten ersten Kennwort (Ci) übereinstimmt, wobei bei Übereinstimmung der erste Nutzer (2) als zugangsersuchender Nutzer (2) erkannt wird.

15. System (1) nach Anspruch 14, bei dem die Prozessoreinrichtung (20) ausserdem ausgestaltet ist, um ein Ergebnissignal zu erzeugen, das bei Übereinstimmung ein Ausführen einer Gebäudeaktion veranlasst.

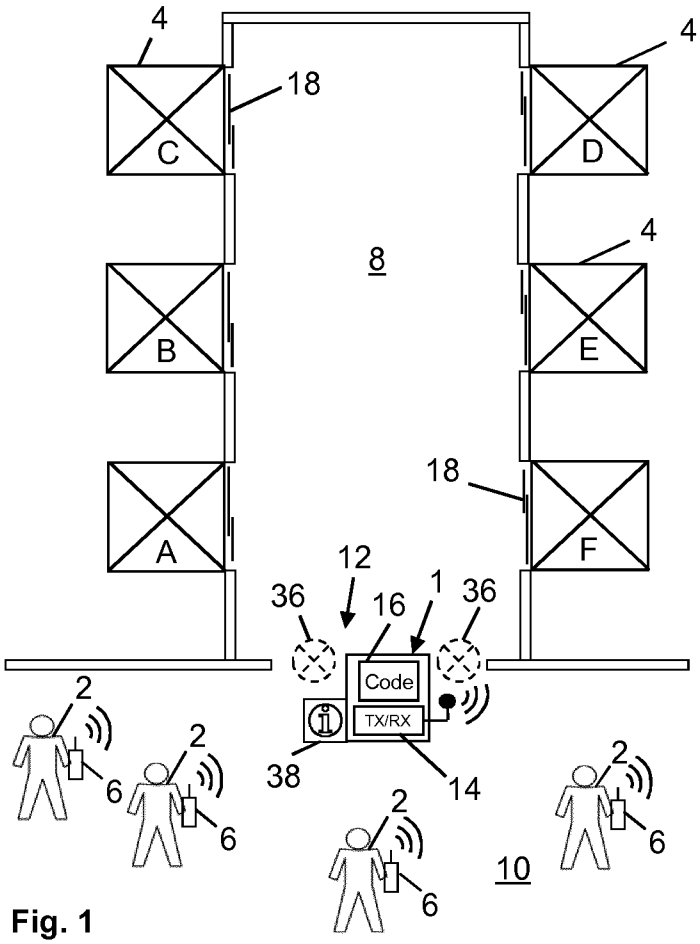
4
18
C
D
4
8
4
B
E
18
A
F
12
36
16
1
36
Code
TX/RX
2
6
2
6
38
14
2
6
2
6
10

Fig. 1

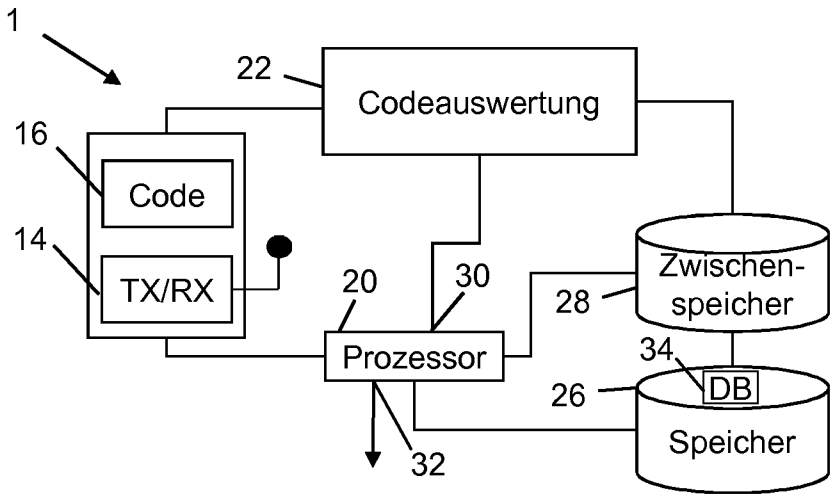
1
22
Codeauswertung
16
Code
14
TX/RX
20
30
Prozessor
28
Zwischen-
speicher
34
DB
26
Speicher
32

Fig. 2

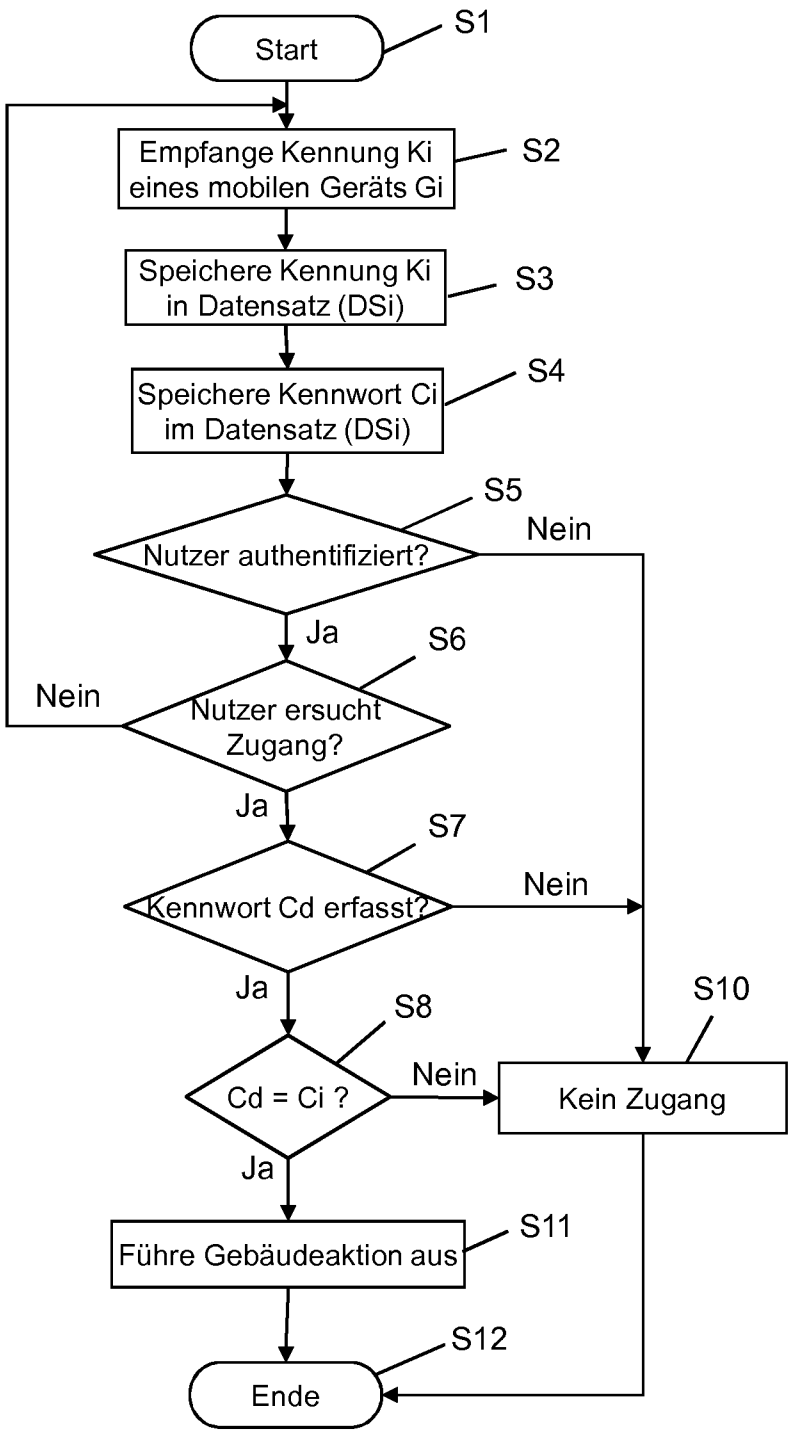
Start
S1
Empfange Kennung Ki eines mobilen Geräts Gi
S2
Speichere Kennung Ki in Datensatz (DSi)
S3
Speichere Kennwort Ci im Datensatz (DSi)
S4
Nutzer authentifiziert?
S5
Nein
Ja
Nutzer ersucht Zugang?
S6
Nein
Ja
Kennwort Cd erfasst?
S7
Nein
Ja
Cd = Ci ?
S8
Nein
Kein Zugang
S10
Ja
Führe Gebäudeaktion aus
S11
Ende
S12

**Fig. 3**

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/EP2018/084797**

## A. CLASSIFICATION OF SUBJECT MATTER

***G07C 9/00***(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2016248782 A1 (TROESCH FLORIAN [CH]) 25 August 2016 (2016-08-25)<br>paragraph [0005] - paragraph [0007]<br>paragraph [0019] - paragraph [0036] | 1-13 |
| X | EP 2237234 A1 (INVENTIO AG [CH]) 06 October 2010 (2010-10-06)<br>paragraph [0002] - paragraph [0015]<br>paragraph [0021] - paragraph [0023] | 1,2,4,6-9,11,13-15 |
| X | US 2015178698 A1 (SCHULZ EGAN [US] ET AL) 25 June 2015 (2015-06-25)<br>paragraph [0012] - paragraph [0030]<br>paragraph [0042] | 1,2,4-7,9,13-15 |
| A | WO 2016087483 A1 (INVENTIO AG [CH]) 09 June 2016 (2016-06-09)<br>page 1, line 31 - line 34<br>page 2, line 20 - line 29 | 7 |
| A | WO 2015049186 A1 (INVENTIO AG [CH]) 09 April 2015 (2015-04-09)<br>page 1, line 21 - page 2, line 17 | 7 |

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| **21 February 2019** | **27 February 2019** |

| Name and mailing address of the ISA/EP | Authorized officer |
|---|---|
| **European Patent Office**<br>**p.b. 5818, Patentlaan 2, 2280 HV Rijswijk**<br>**Netherlands**<br>Telephone No. **(+31-70)340-2040**<br>Facsimile No. **(+31-70)340-3016** | **Mechenbier, Bernd**<br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/EP2018/084797**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| US 2016248782 A1 | 25 August 2016 | AU 2014331198 A1 | 14 April 2016 |
| | | BR 112016006755 A2 | 01 August 2017 |
| | | CA 2924381 A1 | 09 April 2015 |
| | | CN 105593911 A | 18 May 2016 |
| | | EP 3053148 A1 | 10 August 2016 |
| | | RU 2016117169 A | 13 November 2017 |
| | | US 2016248782 A1 | 25 August 2016 |
| | | WO 2015049187 A1 | 09 April 2015 |
| EP 2237234 A1 | 06 October 2010 | AU 2010230205 A1 | 03 November 2011 |
| | | AU 2016202519 A1 | 12 May 2016 |
| | | CA 2757405 A1 | 07 October 2010 |
| | | CN 102449667 A | 09 May 2012 |
| | | EP 2237234 A1 | 06 October 2010 |
| | | EP 2415029 A1 | 08 February 2012 |
| | | SG 175010 A1 | 28 November 2011 |
| | | US 2012068818 A1 | 22 March 2012 |
| | | WO 2010112586 A1 | 07 October 2010 |
| US 2015178698 A1 | 25 June 2015 | US 2015178698 A1 | 25 June 2015 |
| | | US 2018293564 A1 | 11 October 2018 |
| | | WO 2015100185 A1 | 02 July 2015 |
| WO 2016087483 A1 | 09 June 2016 | AU 2015357163 A1 | 29 June 2017 |
| | | AU 2018264147 A1 | 06 December 2018 |
| | | CA 2965746 A1 | 09 June 2016 |
| | | CN 107004313 A | 01 August 2017 |
| | | EP 3227866 A1 | 11 October 2017 |
| | | SG 11201703637U A | 29 June 2017 |
| | | US 2017270728 A1 | 21 September 2017 |
| | | WO 2016087483 A1 | 09 June 2016 |
| WO 2015049186 A1 | 09 April 2015 | AU 2014331291 B2 | 02 November 2017 |
| | | BR 112016006499 A2 | 01 August 2017 |
| | | CA 2924380 A1 | 09 April 2015 |
| | | CN 105637537 A | 01 June 2016 |
| | | EP 2858010 A1 | 08 April 2015 |
| | | EP 3053104 A1 | 10 August 2016 |
| | | JP 2017500619 A | 05 January 2017 |
| | | KR 20160065840 A | 09 June 2016 |
| | | MX 356492 B | 31 May 2018 |
| | | PH 12016500548 A1 | 13 June 2016 |
| | | RU 2016117071 A | 10 November 2017 |
| | | SG 11201601907Q A | 28 April 2016 |
| | | TW 201519104 A | 16 May 2015 |
| | | US 2016224877 A1 | 04 August 2016 |
| | | WO 2015049186 A1 | 09 April 2015 |
| | | ZA 201601884 B | 29 November 2017 |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2018/084797

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G07C9/00
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
G07C

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | US 2016/248782 A1 (TROESCH FLORIAN [CH])<br>25. August 2016 (2016-08-25)<br>Absatz [0005] - Absatz [0007]<br>Absatz [0019] - Absatz [0036]<br>----- | 1-13 |
| X | EP 2 237 234 A1 (INVENTIO AG [CH])<br>6. Oktober 2010 (2010-10-06)<br><br>Absatz [0002] - Absatz [0015]<br>Absatz [0021] - Absatz [0023]<br>----- | 1,2,4,<br>6-9,11,<br>13-15 |
| X | US 2015/178698 A1 (SCHULZ EGAN [US] ET AL)<br>25. Juni 2015 (2015-06-25)<br>Absatz [0012] - Absatz [0030]<br>Absatz [0042]<br>-----<br>-/-- | 1,2,4-7,<br>9,13-15 |

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 21. Februar 2019 | 27/02/2019 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Mechenbier, Bernd |

1

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2018/084797

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| A | WO 2016/087483 A1 (INVENTIO AG [CH])<br>9. Juni 2016 (2016-06-09)<br>Seite 1, Zeile 31 - Zeile 34<br>Seite 2, Zeile 20 - Zeile 29<br>----- | 7 |
| A | WO 2015/049186 A1 (INVENTIO AG [CH])<br>9. April 2015 (2015-04-09)<br>Seite 1, Zeile 21 - Seite 2, Zeile 17<br>----- | 7 |

1

## INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2018/084797

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| US 2016248782 A1 | 25-08-2016 | AU 2014331198 A1 | 14-04-2016 |
| | | BR 112016006755 A2 | 01-08-2017 |
| | | CA 2924381 A1 | 09-04-2015 |
| | | CN 105593911 A | 18-05-2016 |
| | | EP 3053148 A1 | 10-08-2016 |
| | | RU 2016117169 A | 13-11-2017 |
| | | US 2016248782 A1 | 25-08-2016 |
| | | WO 2015049187 A1 | 09-04-2015 |
| EP 2237234 A1 | 06-10-2010 | AU 2010230205 A1 | 03-11-2011 |
| | | AU 2016202519 A1 | 12-05-2016 |
| | | CA 2757405 A1 | 07-10-2010 |
| | | CN 102449667 A | 09-05-2012 |
| | | EP 2237234 A1 | 06-10-2010 |
| | | EP 2415029 A1 | 08-02-2012 |
| | | SG 175010 A1 | 28-11-2011 |
| | | US 2012068818 A1 | 22-03-2012 |
| | | WO 2010112586 A1 | 07-10-2010 |
| US 2015178698 A1 | 25-06-2015 | US 2015178698 A1 | 25-06-2015 |
| | | US 2018293564 A1 | 11-10-2018 |
| | | WO 2015100185 A1 | 02-07-2015 |
| WO 2016087483 A1 | 09-06-2016 | AU 2015357163 A1 | 29-06-2017 |
| | | AU 2018264147 A1 | 06-12-2018 |
| | | CA 2965746 A1 | 09-06-2016 |
| | | CN 107004313 A | 01-08-2017 |
| | | EP 3227866 A1 | 11-10-2017 |
| | | SG 11201703637U A | 29-06-2017 |
| | | US 2017270728 A1 | 21-09-2017 |
| | | WO 2016087483 A1 | 09-06-2016 |
| WO 2015049186 A1 | 09-04-2015 | AU 2014331291 B2 | 02-11-2017 |
| | | BR 112016006499 A2 | 01-08-2017 |
| | | CA 2924380 A1 | 09-04-2015 |
| | | CN 105637537 A | 01-06-2016 |
| | | EP 2858010 A1 | 08-04-2015 |
| | | EP 3053104 A1 | 10-08-2016 |
| | | JP 2017500619 A | 05-01-2017 |
| | | KR 20160065840 A | 09-06-2016 |
| | | MX 356492 B | 31-05-2018 |
| | | PH 12016500548 A1 | 13-06-2016 |
| | | RU 2016117071 A | 10-11-2017 |
| | | SG 11201601907Q A | 28-04-2016 |
| | | TW 201519104 A | 16-05-2015 |
| | | US 2016224877 A1 | 04-08-2016 |
| | | WO 2015049186 A1 | 09-04-2015 |
| | | ZA 201601884 B | 29-11-2017 |