(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 748 590 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
09.12.2020 Patentblatt 2020/50

(51) Int Cl.:
G07C 9/23 *(2020.01)* ***G07C 9/25*** *(2020.01)*

(21) Anmeldenummer: **20177544.2**

(22) Anmeldetag: **29.05.2020**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
KH MA MD TN

(30) Priorität: **03.06.2019 DE 102019114850**

(71) Anmelder: **ABUS Security Center GmbH & Co. KG**
86444 Affing (DE)

(72) Erfinder:
- **REICHHERZER, Martin**
  86343 Königsbrunn (DE)
- **LEUTE, Ralf**
  86456 Gablingen (DE)

(74) Vertreter: **Manitz Finsterwald**
Patent- und Rechtsanwaltspartnerschaft mbB
Martin-Greif-Strasse 1
80336 München (DE)

(54) **WANDMONTIERBARES AUTHENTIFIZIERUNGSGERÄT**

(57) Die Erfindung betrifft ein wandmontierbares Authentifizierungsgerät zur Authentifizierung eines Nutzers eines Gebäudeschließsystems, welches eine Steuereinheit umfasst sowie jeweils damit verbunden eine Bilderfassungseinrichtung, eine Ton-Aufnahme/Ausgabeeinrichtung, eine Einrichtung zum drahtlosen Senden/Empfangen von Daten, einen berührungsempfindlichen Bildschirm sowie ein Schnittstellenmodul zur Verbindung des Authentifizierungsgeräts mit mindestens einem Türaktor. Die Erfindung betrifft auch ein Verfahren zum Authentifizieren eines Nutzers eines Gebäudeschließsystems.

EP 3 748 590 A1

Beschreibung

[0001] Die Erfindung betrifft ein wandmontierbares Authentifizierungsgerät zur Authentifizierung eines Nutzers eines Gebäudeschließsystems sowie ein Verfahren zur Authentifizierung eines Nutzers eines Gebäudeschließsystems.

[0002] Wandmontierbare Türkommunikationssysteme sind grundsätzlich bekannt, insbesondere solche, die eine Sprachkommunikation zwischen einem Nutzer des Türkommunikationssystems im Außenbereich eines Gebäudes und einem Bewohner im Innenbereich des Gebäudes ermöglichen sowie eine Kamera umfassen, die es dem Bewohner erlaubt, den Nutzer anhand eines übertragenen Bildes zu identifizieren. Ist der Bewohner abwesend, so hat er keine Möglichkeit mit einem solchen Gerät Aktivitäten im Türbereich zu verfolgen oder zu beeinflussen. Durch zugangsberechtigte Personen werden Türen vom Außenbereich her üblicherweise mittels eines Schlüssels, einer Chipkarte oder eines PIN-Codes geöffnet. Ein Öffnen der Tür kann in diesen Fällen auch durch eine nicht zugangsberechtigte Person erfolgen, wenn diese Zugriff auf Schlüssel, Chipkarte oder PIN-Code erlangt hat.

[0003] Davon ausgehend liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein Authentifizierungsgerät und ein Authentifizierungsverfahren bereitzustellen, das eine erhöhte Sicherheit gegen unbefugten Zugang zu einem Gebäude bietet und sich außerdem durch einen erhöhten Bedienkomfort auszeichnet.

[0004] Die Aufgabe wird durch ein wandmontierbares Authentifizierungsgerät mit den Merkmalen des Anspruchs 1 und ein Verfahren zur Authentifizierung eines Nutzers eines Gebäudeschließsystems mit den Merkmalen des Anspruchs 9 gelöst.

[0005] Erfindungsgemäß umfasst ein wandmontierbares Authentifizierungsgerät zur Authentifizierung eines Nutzers eines Gebäudeschließsystems eine Steuereinheit, eine mit der Steuereinheit verbundene Bilderfassungseinrichtung, eine mit der Steuereinheit verbundene Ton-Aufnahme/Ausgabeeinrichtung, eine mit der Steuereinheit verbundene Einrichtung zum drahtlosen Senden/Empfangen von Daten, einen mit der Steuereinheit verbundenen berührungsempfindlichen Bildschirm sowie ein mit der Steuereinheit verbundenes Schnittstellenmodul zur Verbindung des Authentifizierungsgeräts mit mindestens einem Türaktor.

[0006] Bei einem erfindungsgemäßen Verfahren zur Authentifizierung eines Nutzers eines Gebäudeschließsystems mittels eines mit einem Türaktor verbundenen Authentifizierungsgeräts der voranstehenden Art, wird in einem ersten Authentifizierungsschritt ein erstes Sicherheitsmerkmal des Nutzers erfasst und das erfasste Sicherheitsmerkmal mit wenigstens einem ersten vorgegebenen Sicherheitsmerkmal verglichen und, sofern das erfasste erste Sicherheitsmerkmal mit dem ersten vorgegebenen Sicherheitsmerkmal übereinstimmt, in einem zweiten Authentifizierungsschritt ein zweites Sicherheitsmerkmal des Nutzers erfasst und das erfasste zweite Sicherheitsmerkmal mit wenigstens einem zweiten vorgegebenen Sicherheitsmerkmal verglichen und, sofern das erfasste zweite Sicherheitsmerkmal mit dem zweiten vorgegebenen Sicherheitsmerkmal übereinstimmt, durch die Steuereinheit ein Entriegeln und/oder Öffnen einer dem Türaktor zugeordneten Tür veranlasst.

[0007] Mit Hilfe des erfindungsgemäßen Authentifizierungsgeräts und Authentifizierungsverfahrens werden eine erhöhte Sicherheit bei der Authentifizierung eines Nutzers und entsprechend eine erhöhte Sicherheit gegenüber unbefugtem Zugang zu einem Gebäude erreicht, nämlich dadurch dass zumindest zwei Sicherheitsmerkmale des Nutzers positiv verifiziert werden können bzw. müssen, bevor ein Entriegeln und/oder ein Öffnen einer Tür erfolgt. Im Allgemeinen ist das erste erfasste Sicherheitsmerkmal vom zweiten erfassten Sicherheitsmerkmal verschieden, um eine erhöhte Sicherheit im Authentifizierungsverfahren bereitzustellen. Als Resultat einer erfolgreichen Authentifizierung ist ein Entriegeln und/oder Öffnen der Tür ohne manuelles Eingreifen des Nutzers vorgesehen, was zu einem erhöhten Bedienkomfort für den Nutzer führt.

[0008] Das erfindungsgemäße Authentifizierungsgerät ist wandmontierbar, das heißt, es ist dazu vorgesehen, an einer Wand, insbesondere an einer Gebäudewand und bevorzugt neben einer Tür, angebracht zu werden. Das Authentifizierungsgerät kann auch an einem Eingangstor zu einem Gelände angebracht sein. Es kann sich in beiden Fällen sowohl um ein privat als auch um ein geschäftlich genutztes Gelände und/oder Gebäude handeln. Das Authentifizierungsgerät kann zur Nutzerauthentifizierung in Einparteien- oder Mehrparteiengebäuden genutzt werden. Entsprechend kann das Authentifizierungsgerät mehrere Türaktoren ansteuern, die gegebenenfalls unterschiedlichen Türen zugeordnet sein können. Für verschiedene anzusteuernde Türaktoren können unterschiedliche Nutzer mit gegebenenfalls unterschiedlichen Berechtigungen am Authentifizierungsgerät registriert sein.

[0009] Als Ergebnis eines Authentifizierungsvorgangs werden Aktionen von dem Authentifizierungsgerät ausgeführt, die von den Berechtigungen und Konfigurationen abhängen, die für den jeweils authentifizierten Nutzer hinterlegt sind. Dies kann beispielsweise ein Entriegeln eines Türschlosses und gegebenenfalls automatisches Öffnen der zugeordneten Tür für einen zugangsberechtigten Nutzer oder ein Anzeigen eines Klingelknopfes für einen nicht zugangsberechtigten Nutzer umfassen.

[0010] Als Nutzer werden in diesem Zusammenhang alle Personen bezeichnet, die mit dem Authentifizierungsgerät interagieren. Dies können unter anderem Bewohner eines Privathaushalts, Personal im Privathaushalt, Mitarbeiter einer Firma, bekannte Besucher mit oder ohne Zugangsberechtigung und unbekannte Besucher sein, welche üblicherweise keine Zugangsberechtigung

aufweisen, wie z.B. Postboten oder Paketzusteller sowie Dienstleister und Handwerker. Ebenso können die Nutzer in verschiedene Kategorien eingeteilt sein: Ein Masternutzer kann dazu berechtigt sein, Konfigurationen am Authentifizierungsgerät vorzunehmen, während ein Standardnutzer beispielsweise nur eine Zugangsberechtigung besitzt oder nur auf einen durch den Masternutzer konfigurierbaren, beschränkten Funktionsumfang des Authentifizierungsgeräts zugreifen kann. Ein unbekannter Nutzer kann beispielsweise nur dazu berechtigt sein, eine Signaleinheit zu betätigen, eine Nachricht zu hinterlassen sowie konfigurationsabhängig beispielsweise eine Beleuchtung anzuschalten, bestimmte vernetzte Geräte wie zum Beispiel eine Gartenbewässerung zu starten oder einen Sicherheitscode einzugeben. Ebenso können durch einen Masternutzer Nutzergruppen erstellt werden, für die spezifische Funktionsumfänge und -abläufe konfiguriert werden können, beispielsweise Nutzergruppen wie 'Kinder eines Bewohners' oder 'Mitarbeiter 1. Stock'. Im Folgenden werden alle Personen, die sich in einem Gebäude, Gelände oder Haushalt, welche mit einem erfindungsgemäßen Gebäudeschließsystem gesichert sind, erwartungsgemäß und regelmäßig aufhalten, als Bewohner bezeichnet. Das kann entsprechend Mitarbeiter eines Unternehmens in erfindungsgemäß gesicherten Räumlichkeiten umfassen, ebenso wie Bewohner eines Privathaushalts.

[0011] Die Steuerung des Authentifizierungsverfahrens und der Funktionen des Authentifizierungsgeräts, umfassend die Verarbeitung von eingehenden Signalen und Befehlen, sowie das Generieren von passenden Aktionen, erfolgt durch die Steuereinheit, die entsprechend mit den Komponenten des Authentifizierungsgeräts verbunden ist. Diese Komponenten umfassen eine Bilderfassungseinrichtung, eine Ton-Aufnahme/Ausgabeeinrichtung, welche mindestens ein Mikrofon und mindestens einen Lautsprecher umfasst, eine Einrichtung zum drahtlosen Senden/Empfangen von Daten, nachfolgend auch als Sende/Empfangseinrichtung bezeichnet, einen berührungsempfindlichen Bildschirm, welcher zur Ausgabe von Informationen und Nachrichten sowie zur Eingabe von Befehlen und zur Interaktion mit dem Authentifizierungsgerät konfiguriert ist, sowie ein Schnittstellenmodul zur Verbindung des Authentifizierungsgeräts mit einem Türaktor. Das Schnittstellenmodul ist so beschaffen, dass die Verbindung mit dem Türaktor mittels Funk, insbesondere beispielsweise mittels Sub-1 GHz-Frequenzen, oder auch kabelgebunden hergestellt werden kann.

[0012] Die Ton-Aufnahme/Ausgabeeinrichtung ist dazu vorgesehen, eine Türkommunikation zwischen einem Nutzer des Authentifizierungsgeräts und einem Bewohner des Gebäudes zu ermöglichen, Tonaufnahme und -wiedergäbe für Sprach- und Videonachrichten oder -anrufe zur Verfügung zu stellen und eine biometrische Stimmenerkennung zu ermöglichen. Zudem kann das Mikrofon dazu konfiguriert sein, auffällige Geräusche im Türbereich aufzunehmen und mittels Geräuscherkennung durch die Steuereinheit des Authentifizierungsgeräts entsprechende Warnungen für den Bewohner des Gebäudes zu generieren.

[0013] Unter Türaktoren werden in diesem Kontext sowohl Türschlösser als auch Türantriebe zum automatischen Öffnen beziehungsweise Schließen einer Tür verstanden. Insbesondere kann ein Türaktor durch eine in ein Türschloss integrierte Vorrichtung wie beispielsweise ein Motorschloss, einen elektronischen Türzylinder, einen motorischen Türschlossantrieb oder einen elektrischen Türsummer, ein elektromagnetisches Türschloss oder eine elektrische Türöffnungsvorrichtung gebildet sein. Ferner kann der Türaktor eine Vorrichtung zum automatischen Ver- und Entriegeln der Tür sowie eine Vorrichtung zum automatischen Öffnen und Schließen der Tür umfassen, sodass als Resultat eines erfolgreichen Authentifizierungsverfahrens ein automatisches, d.h. keinen manuellen Eingriff erforderndes, und somit besonders komfortables Entriegeln und Öffnen bzw. Schließen und Verriegeln der Tür erfolgen kann.

[0014] Das erfindungsgemäße Authentifizierungsverfahren basiert auf der Erfassung von Sicherheitsmerkmalen eines Nutzers des Authentifizierungsgeräts. Geeignete Sicherheitsmerkmale umfassen personenbezogene Merkmale, welche insbesondere biometrische Merkmale sein können, sowie elektronische Sicherheitsschlüssel und/oder Sicherheitscodes. Unter den Begriff des biometrischen Merkmals fallen in diesem Zusammenhang unter anderem Fingerabdrücke, Handgeometrie und Handvenenmuster, Iris- oder Retinacharakteristika, charakteristische Augenbewegungen, charakteristische Merkmale der Stimme, sowie zwei- und/oder dreidimensionale Gesichtsgeometrie. Elektronische Sicherheitsschlüssel umfassen in diesem Zusammenhang unter anderem QR-Codes, Bluetooth-Schlüssel, WLAN-Schlüssel sowie NFC- oder RFID-Tags, während als Sicherheitscodes PIN-Codes oder auch Passwörter und -phrasen denkbar sind. Biometrische Merkmale, insbesondere Handvenenmuster oder charakteristische Augenbewegungen, weisen gemeinhin im Vergleich zu herkömmlichen Schlüsseln, Chipkarten oder PIN-Codes eine deutlich erhöhte Sicherheit gegenüber Fälschung und Missbrauch auf.

[0015] Eine besonders hohe Sicherheit wird erfindungsgemäß dadurch erzielt, dass in zwei Authentifizierungsschritten insbesondere unterschiedliche Sicherheitsmerkmale des Nutzers abgefragt werden. Das im ersten Authentifizierungsschritt abgefragte Sicherheitsmerkmal wird mit vorgegebenen gespeicherten Sicherheitsmerkmalen der bekannten Nutzer verglichen. Sofern eine Übereinstimmung zwischen dem erfassten und einem ersten vorgegebenen Sicherheitsmerkmal besteht, wird die Abfrage eines zweiten Sicherheitsmerkmals des Nutzers getriggert, das von dem ersten Sicherheitsmerkmal verschieden ist. Nur bei zusätzlicher Übereinstimmung des zweiten Sicherheitsmerkmals mit einem zweiten vorgegebenen Sicherheitsmerkmal wird ein Entriegeln und/oder Öffnen der Tür veranlasst. Eine sol-

che Zweifachauthentifizierung verringert das Risiko eines unbefugten Öffnens der Tür erheblich.

[0016] Es versteht sich, dass zusätzliche Authentifizierungsschritte in das Authentifizierungsverfahren aufgenommen werden können, um die Sicherheit noch weiter zu erhöhen.

[0017] Vorteilhafte Ausbildungen der Erfindung sind den Unteransprüchen, der Beschreibung und der Zeichnung zu entnehmen.

[0018] Gemäß einer Ausführungsform weist das Authentifizierungsgerät eine mit der Steuereinheit verbundene Sensorik zur Erfassung der Annäherung einer Person an das Authentifizierungsgerät auf. Eine Erhöhung der Lebensdauer sowie eine Verringerung des Energieverbrauchs des Authentifizierungsgeräts können dadurch bewerkstelligt werden, dass eine Aktivierung des Authentifizierungsgeräts nur bei Detektion einer sich annähernden Person innerhalb eines Erkennungsabstands d_{rec} vom Authentifizierungsgerät erfolgt. Die Sensorik zur Erfassung der Annäherung einer Person kann beispielsweise einen pyroelektrischen (PIR) Sensor, einen Ultraschallsensor oder eine Kamera als Näherungssensor umfassen.

[0019] Das Authentifizierungsgerät weist bevorzugt eine Datenbank auf, in der vorgegebene Sicherheitsmerkmale der registrierten Nutzer hinterlegt sind, insbesondere biometrische Merkmale, elektronische Sicherheitsschlüssel und/oder Sicherheitscodes.

[0020] Gemäß einer weiteren Ausführungsform des Authentifizierungsgeräts ist das Schnittstellenmodul zur Verbindung der Steuereinheit mit einem lokalen Netzwerk,einem externen Server, einer Türklingel, einer Sensorik zur Erfassung eines Öffnungszustandes einer dem Türaktor zugeordneten Tür, einem Smart Home System und/oder einer Alarmanlage ausgebildet. Die Verbindung kann drahtgebunden, beispielsweise über Ethernet, oder drahtlos erfolgen, beispielsweise mittels WLAN und/oder mittels Funk, insbesondere mittels Sub-1 GHz-Frequenzen. Der externe Server kann in diesem Zusammenhang durch eine oder mehrere zentrale Rechnereinheiten oder alternativ durch eine Cloud gebildet sein. Bei einer solchen Cloud kann es sich um eine vom Hersteller des Authentifizierungsgeräts bereitgestellte Cloud handeln, welche die Nutzung und Konfigurierung des vollen Funktionsumfangs des Authentifizierungsgeräts gewährleistet, oder um eine von einem Drittanbieter bereitgestellte Cloud. Des Weiteren kann der externe Server eine Datenbank umfassen, in der vorgegebene Sicherheitsmerkmale hinterlegt sind. Zudem kann der externe Server eine Internetverbindung für das Authentifizierungsgerät bereitstellen, um einen Austausch von Nachrichten und Informationen zwischen dem Authentifizierungsgerät und mobilen Endgeräten, mobilen Applikationen oder Datenbanken sowie das Herunterladen von Informationen aus dem Internet zu ermöglichen. Beispielsweise kann das Authentifizierungsgerät über das Schnittstellenmodul auch mit einem hausinternen System wie zum Beispiel einer Alarm-, Überwachungs- oder Sicherheitsanlage, einem Smart Home System und/oder einer ABUS Sicherheitsplattform verbunden werden.

[0021] Vorteilhafterweise erfasst die Sensorik zur Erfassung eines Öffnungszustandes einer dem Türaktor zugeordneten Tür sowohl, ob und wann die Tür geöffnet oder geschlossen wird, als auch, ob sich das Türschloss in einem verriegelten oder entriegelten Zustand befindet.

[0022] Bevorzugt umfasst die Bilderfassungseinrichtung des Authentifizierungsgeräts zumindest eine Kamera zur zweidimensionalen Bilderfassung, beispielsweise eine RGB-Kamera. Besonders bevorzugt umfasst die Bilderfassungseinrichtung des Authentifizierungsgeräts eine Kamera zur dreidimensionalen Bilderfassung, beispielsweise eine 3D-TOF-Kamera zur Bilderfassung mittels Laufzeitverfahren. Eine 3D-TOF-Kamera stellt eine erhöhte Sicherheit gegen unbefugten Zugang bereit durch die Möglichkeit einer dreidimensionalen Gesichtserkennung sowie eines Venenscans im Authentifizierungsprozess und bietet eine Erweiterung des Funktionsumfangs des Authentifizierungsgeräts durch die Möglichkeit der Erfassung von Gesten. Im Gegensatz zu Aufnahmen mit einer 2D-RGB-Kamera ist die dreidimensionale Bilderfassung mittels Laufzeitverfahren unempfindlich gegenüber ungünstigen Lichtverhältnissen. Alternativ oder zusätzlich kann die Bilderfassungseinrichtung eine Infrarot-Kamera aufweisen, um beispielsweise mittels dieser oder einer vorstehend genannten Kamera eine Erkennung von Personen, eine Blickerfassung oder eine Verfolgung einer Pupillenbewegung zu ermöglichen.

[0023] Gemäß einer weiteren Ausführungsform weist die Einrichtung zum drahtlosen Senden/Empfangen von Daten ein Bluetooth-Modul, ein RFID-Modul, ein NFC-Modul und/oder ein WLAN-Modul auf, welche einzeln oder in beliebiger Kombination in dem Authentifizierungsgerät verbaut sein können, zur Abfrage von entsprechenden Sicherheitsmerkmalen dienen können und/oder eine Kommunikation zwischen dem Authentifizierungsgerät und einem externen Server bereitstellen können.

[0024] Weiterer Gegenstand der Erfindung ist ein Gebäudeschließsystem mit einem Authentifizierungsgerät der voranstehend beschriebenen Art und einem mit dem Authentifizierungsgerät verbundenen Türaktor, wobei die Verbindung drahtlos, beispielsweise mittels Funk, oder auch kabelgebunden erfolgen kann.

[0025] Bevorzugt weist das Gebäudeschließsystem einen externen Server auf, der mit dem Authentifizierungsgerät verbunden ist. Wie bereits erwähnt, kann es sich bei dem externen Server auch um eine Cloud handeln.

[0026] Das Verfahren zur Authentifizierung eines Nutzers eines Gebäudeschließsystems mittels eines mit einem Türaktor verbundenen Authentifizierungsgeräts ist vorteilhafterweise so ausgestaltet, dass das erste und/oder zweite erfasste Sicherheitsmerkmal ein biometrisches Merkmal ist. Die erhöhte Fälschungssicherheit von biometrischen Merkmalen, insbesondere beispielsweise

von Venenscans, trägt zu einer erhöhten Sicherheit des Authentifizierungsverfahrens bei. In einem ersten Authentifizierungsschritt kann beispielsweise ein biometrisches Merkmal erfasst werden und bei Übereinstimmung dieses erfassten biometrischen Merkmals mit einem vorgegebenen Sicherheitsmerkmal die automatisierte Abfrage eines weiteren personenbezogenen Sicherheitsmerkmals in einem zweiten Authentifizierungsschritt getriggert werden, beispielsweise der Austausch eines digitalen Schlüssels mit einem mobilen Endgerät des Nutzers mittels Bluetooth oder WLAN, die Erfassung eines weiteren biometrischen Merkmals oder eines anderen Sicherheitsmerkmals.

[0027] Gemäß einer Ausführungsform ist vorgesehen, dass die Steuereinheit ein Verriegeln der dem Türaktor zugeordneten Tür veranlasst, wenn das Authentifizierungsgerät innerhalb eines vorbestimmten Zeitraums vor dem ersten Authentifizierungsschritt ein Öffnen der Tür erfasst hat und bereits das im ersten Authentifizierungsschritt erfasste Sicherheitsmerkmal mit einem entsprechend vorgegebenen Sicherheitsmerkmal übereinstimmt. Dies dient der Erhöhung des Bedienkomforts, da auf diese Weise ein verlässliches Verriegeln der Tür ohne manuellen Eingriff nach dem Verlassen des Gebäudes sichergestellt werden kann. Die Authentifizierung durch ein einzelnes Sicherheitsmerkmal ist beim Verriegeln ausreichend, da hier üblicherweise geringere Sicherheitsanforderungen bestehen. Der vorbestimmte Zeitraum vor dem ersten Authentifizierungsschritt, in welchem ein Öffnen der Tür erfasst wird, kann durch einen Masternutzer konfigurierbar oder herstellerseitig voreingestellt sein, beispielsweise derart, dass ein Verriegeln der Tür bei positiver Authentifizierung eines Nutzers nur innerhalb von 2 Minuten, bevorzugt 1 Minute, nach dem Öffnen der Tür erfolgt.

[0028] Vorteilhafterweise ist das Authentifizierungsverfahren so gestaltet, dass, wenn ein in einem der Authentifizierungsschritte erfasstes Sicherheitsmerkmal nicht mit einem entsprechend vorgegebenen Sicherheitsmerkmal übereinstimmt, auf dem berührungsempfindlichen Bildschirm wenigstens ein Eingabefeld für eine Nutzereingabe angezeigt wird, das es dem Nutzer ermöglicht, ein Klingelsignal zu erzeugen, eine Video-, Sprach- oder Textnachricht für einen anderen Nutzer des Authentifizierungsgeräts auf dem Authentifizierungsgerät zu hinterlassen, einen Video- oder Sprachanruf über das Authentifizierungsgerät zu einem mobilen Endgerät eines anderen Nutzers des Authentifizierungsgeräts herzustellen, eine Textnachricht über das Authentifizierungsgerät zu einem mobilen Endgerät eines anderen Nutzers des Authentifizierungsgeräts zuzustellen, eine Video-, Sprach- oder Textnachricht, die ein anderer Nutzer auf dem Authentifizierungsgerät hinterlegt hat, abzurufen sowie mittels Eingabe eines Sicherheitscodes ein Entriegeln und/oder Öffnen der dem Türaktor zugeordneten Tür zu veranlassen. Im Falle einer nicht erfolgreichen Authentifizierung kann auf dem berührungsempfindlichen Bildschirm für den Nutzer ebenso eine Information darüber bereitgestellt werden, ob eine Störung im Authentifizierungsprozess vorliegt, und welcher Art diese Störung ist. Beispielsweise kann darauf hingewiesen werden, dass keine Datenverbindung vorliegt, oder es kann im Fall einer fehlgeschlagenen biometrischen Authentifizierung eine Aufforderung und/oder Anleitung für den Nutzer angezeigt werden, sich korrekt im Erfassungsbereich des Authentifizierungsgeräts zu positionieren. Ein vom Nutzer am Authentifizierungsgerät generiertes Klingelsignal kann beispielsweise an einer Signaleinheit im Inneren des Gebäudes oder auch auf einem mobilen Endgerät des Bewohners des Gebäudes wiedergegeben werden. Zur Erhöhung von Sicherheit und Bedienkomfort kann ein Bewohner also auch während seiner Abwesenheit über Aktivitäten an dem Authentifizierungsgerät informiert werden bzw. über sein mobiles Endgerät und das Authentifizierungsgerät mit dem Nutzer kommunizieren. Auf dem Authentifizierungsgerät für andere Nutzer hinterlassene Video-, Sprach- und Textnachrichten können insbesondere beispielsweise an einen Bewohner des Gebäudes oder ein Kind des Bewohners gerichtet sein, ebenso wie die auf mobile Endgeräte übertragenen Video- und Sprachanrufe und Textnachrichten. Nachrichten, die zum Abrufen für einen Nutzer auf dem Authentifizierungsgerät von einem anderen Nutzer hinterlassen werden, können insbesondere von einem Bewohner hinterlegt werden und beispielsweise Informationen darüber enthalten, wann der Bewohner wieder erreichbar ist oder wer ersatzweise zu kontaktieren ist.

[0029] Besonders vorteilhafterweise kann ein Besucher ein Klingelsignal am Authentifizierungsgerät auslösen, welches in Abwesenheit des Bewohners vom Gebäude, dem Bewohner auf sein mobiles Endgerät weitergeleitet wird. Der Bewohner hat dann die Möglichkeit, das Klingelsignal in Form eines Video- oder Sprachanrufs anzunehmen und über das Authentifizierungsgerät mit dem Besucher zu kommunizieren. Mittels seines mobilen Endgeräts könnte der Bewohner dann dem Besucher auch während seiner Abwesenheit die Tür öffnen oder dem Besucher einen Sicherheitscode zum einmaligen Öffnen der Tür zukommen lassen.

[0030] Die Bilderfassungseinrichtung kann dazu ausgebildet sein, von nicht registrierten und/oder nicht zugangsberechtigten Nutzern, die am Authentifizierungsgerät detektiert werden, eine Fotoaufnahme inklusive Zeitstempel anzufertigen, damit ein Bewohner des Gebäudes über Besuche informiert werden kann. Gegebenenfalls kann ein entsprechendes Eingabefeld angezeigt werden, das es dem Nutzer des Authentifizierungsgeräts ermöglicht, per Nutzereingabe der Fotoaufnahme zuzustimmen beziehungsweise diese gezielt auszulösen.

[0031] Die angezeigten Eingabefelder können auch eine Rückfalloption für einen zugangsberechtigten Nutzer bieten, um die Tür zu öffnen, falls die regulär vorgesehenen Authentifizierungsschritte ausnahmsweise nicht erfolgreich abgeschlossen werden können. Das kann beispielsweise passieren, wenn in einem Schritt des Au-

thentifizierungsverfahrens durch das Authentifizierungsgerät ein elektronischer Sicherheitsschlüssel angefordert wird, der Akku des entsprechend benötigten mobilen Endgeräts des Nutzers aber leer ist. In diesem Fall kann ein zugangsberechtigter Nutzer über den berührungsempfindlichen Bildschirm einen Sicherheitscode, beispielsweise einen PIN-Code oder ein Passwort eingeben, um dennoch die Tür öffnen zu können. Um zu verhindern, dass ein Nutzer anhand von Fingerabdrücken, die bei einer vorausgegangenen Nutzung des Authentifizierungsgeräts auf dem berührungsempfindlichen Bildschirm hinterlassen wurden, ableiten kann, welche Ziffern, Buchstaben und/oder Symbole ein gültiger Sicherheitscode enthält, kann ein entsprechendes Tastaturfeld zur Codeeingabe auf dem berührungsempfindlichen Bildschirm so dargestellt werden, dass die Tasten bei jedem Aufruf in zufälliger Anordnung angezeigt werden.

[0032] Bevorzugt geht das Authentifizierungsgerät nach der Benutzung in einen Ruhemodus über. Es wechselt erst dann in einen Aktivmodus und startet den ersten Authentifizierungsschritt, wenn die Annäherung eines Nutzers an das Authentifizierungsgerät detektiert wird. Der berührungsempfindliche Bildschirm kann im Ruhemodus deaktiviert sein und erst bei Detektion eines Nutzers aktiviert werden. Denkbar ist, dass ein Einschalten des Bildschirms bei einer Entfernung des Nutzers erfolgt, die kleiner ist als 10 Meter und bevorzugt kleiner als 5 Meter. Dies verlängert die Lebensdauer des Bildschirms und reduziert den Energieverbrauch des Authentifizierungsgeräts.

[0033] Wird durch eine geeignete Sensorik die Annäherung eines Nutzers an das Authentifizierungsgerät detektiert, können dem Nutzer in Abhängigkeit von einem Abstand zwischen dem Nutzer und dem Authentifizierungsgerät unterschiedliche Visualisierungen auf dem berührungsempfindlichen Bildschirm angezeigt werden. Beispielsweise kann bei einem Abstand von mehr als einem Meter ein konfigurierbarer Begrüßungsbildschirm angezeigt werden, der Informationen wie Adressdaten oder Bewohnerdaten, Warnhinweise, beispielsweise auf eine Videoüberwachung des Türbereichs, Klingelbereiche für zumindest eine Partei im Gebäude und andere Informationen beinhalten kann. Bei einem verringerten Abstand des Nutzers zum Authentifizierungsgerät, beispielsweise kleiner als 1 Meter, kann das Authentifizierungsverfahren mit der Erfassung eines Sicherheitsmerkmals gestartet werden.

[0034] Gemäß einer bevorzugten Ausführungsform können, sofern alle im Authentifizierungsverfahren erfassten Sicherheitsmerkmale mit entsprechend vorgegebenen Sicherheitsmerkmalen übereinstimmen, weitere konfigurierbare Funktionen, insbesondere Smart-Home-Geräte sowie Sicherheitssysteme, aktiviert oder deaktiviert werden und/oder Informationen über deren Zustand sowie erfasste Ereignisse und Warnungen auf dem berührungsempfindlichen Bildschirm angezeigt werden und/oder Informationen über Aktivitäten am Authentifizierungsgerät und damit verbundenen Geräten oder Sensoriken auf dem berührungsempfindlichen Bildschirm angezeigt werden.

[0035] Dies kann umfassen, dass einzelne Smart-Home-Geräte, beispielsweise Beleuchtungen, Musikanlagen, Klimageräte, etc. durch das Authentifizierungsgerät steuerbar sind. Entsprechend können diese Geräte beispielsweise ausgeschaltet werden, wenn das Authentifizierungsgerät detektiert, dass alle Bewohner das Gebäude verlassen haben, oder umgekehrt aktiviert werden, wenn ein Bewohner das Gebäude betritt. Ebenso können Sicherheitssysteme, beispielsweise eine Alarmanlage, durch das Authentifizierungsgerät steuerbar sein, beispielsweise aktiviert werden, wenn das Authentifizierungsgerät detektiert, dass alle Bewohner das Gebäude verlassen haben, und umgekehrt deaktiviert werden, wenn ein Bewohner das Gebäude betritt. Weitere haus- oder gebäude- oder geländeinterne Geräte können durch das Authentifizierungsgerät steuerbar sein, beispielsweise ein Garagentor, ein Einfahrtstor, eine Gartenbewässerung und weitere Geräte, die im Rahmen eines smarten Zuhauses vernetzt vorliegen.

[0036] Zudem können durch einen Masternutzer des Authentifizierungsgeräts Szenarien konfiguriert werden, die mehrere Funktionen vernetzter Geräte gleichzeitig umfassen. Diese Szenarien können durch das Authentifizierungsgerät aktiviert oder deaktiviert werden, abhängig davon welcher Nutzer am Authentifizierungsgerät authentifiziert wird. Beispielsweise kann ein Szenario 'Haus ist leer' gestartet werden, wenn das Authentifizierungsgerät detektiert hat, dass alle Bewohner das Gebäude verlassen haben, was ein Aktivieren einer Alarmanlage, ein Ausschalten aller Beleuchtungen im Gebäude und ein Herunterregeln einer Heizung umfassen kann.

[0037] Ferner kann ein Szenario 'Kind kommt nach Hause' bei Authentifizierung eines Kindes am Authentifizierungsgerät bewirken, dass die Eltern eine Benachrichtigung über das Heimkommen des Kindes auf einem mobilen Endgerät empfangen und/oder eine Nachricht der Eltern für das Kind auf dem berührungsempfindlichen Bildschirm des Authentifizierungsgeräts abgespielt wird und/oder die Beleuchtung im Haus eingeschaltet wird.

[0038] Es können zudem für Personen mit unterschiedlichen Berechtigungen unterschiedliche Optionen am Authentifizierungsgerät bereitgestellt werden. Beispielsweise kann, wenn ein bestimmter registrierter Nachbar am Authentifizierungsgerät authentifiziert wird, ein Eingabefeld auf dem berührungsempfindlichen Bildschirm angezeigt werden, welches es dem Nachbarn ermöglicht, beispielsweise eine Gartenbewässerung einzuschalten ohne das Gebäude zu betreten.

[0039] Ebenso können Informationen über den Zustand der verbundenen Smart-Home-Geräte sowie erfasste Ereignisse und Warnungen auf dem berührungsempfindlichen Bildschirm angezeigt werden und/oder Informationen über Aktivitäten am Authentifizierungsgerät und damit verbundenen Geräten oder Sensoriken während der Abwesenheit des Bewohners auf dem berührungsempfindlichen Bildschirm angezeigt werden, wenn

der Bewohner selbst oder andere entsprechend autorisierte Nutzer vom Authentifizierungsgerät authentifiziert werden. Dies kann unter anderem eine Mitteilung über bekannte oder unbekannte Besucher in Abwesenheit, Fotoaufnahmen der Besucher oder von den Besuchern hinterlassene Videonachrichten, eine Nachricht, dass Post in den Briefkasten eingeworfen wurde, wenn dieser über eine entsprechende Sensorik mit dem Authentifizierungsgerät verbunden ist, ebenso wie Informationen über auffällige Geräusche im Türbereich oder andere Warnhinweise umfassen.

[0040] In Kombination mit entsprechenden Überwachungssystemen kann das Authentifizierungsgerät in einem Alarmfall eine Notfallöffnung der mit dem Authentifizierungsgerät verbundenen Tür möglichen. Diese kann entweder mittels einer pauschal im Alarmfall freigeschalteten Notöffnungsfunktion, beispielsweise mittels eines entsprechenden Eingabefelds, das auf dem berührungsempfindlichen Bildschirm angezeigt wird, erfolgen oder nur für Einsatzkräfte zugänglich sein, die beispielsweise eine Fernöffnung durch einen hinterlegten Notfallkontakt anfordern können.

[0041] Nachfolgend wird die Erfindung rein beispielhaft anhand einer möglichen Ausführungsform unter Bezugnahme auf die beigefügte Zeichnung beschreiben. Es zeigen:

Fig. 1 ein Gebäudeschließsystem mit einem erfindungsgemäßen Authentifizierungsgerät und einem elektrischen Türaktor;

Fig. 2 eine schematische Darstellung eines Grundaufbaus des Authentifizierungsgeräts von Fig. 1;

Fig. 3 eine schematische Darstellung einer ersten konkreten Ausführungsform des Authentifizierungsgeräts von Fig. 1;

Fig. 4A ein schematisches Ablaufdiagramm eines Authentifizierungsverfahrens mit dem Authentifizierungsgerät von Fig. 3 für den Fall 'Ankommen' für einen registrierten Nutzer;

Fig. 4B eine schematische Darstellung einer Bildschirmvisualisierung mit dem Authentifizierungsgerät von Fig. 3 für den Fall 'Ankommen' für einen unbekannten Nutzer;

Fig. 4C ein schematisches Ablaufdiagramm eines Authentifizierungsverfahrens mit dem Authentifizierungsgerät von Fig. 3 für den Fall 'Verlassen';

Fig. 5 eine schematische Darstellung einer zweiten konkreten Ausführungsform des Authentifizierungsgeräts von Fig. 1.

[0042] Fig. 1 zeigt ein Gebäude 10 mit einer Gebäudewand 12, in die eine Tür 18 eingelassen ist. Die Tür 18 ist mit zwei Türaktoren versehen, welche hier in Form einer elektrischen Türöffnungsvorrichtung 22 und eines motorisiertes Türschlosses 24 ausgebildet sind. Die Türaktoren 22, 24 sind Teil eines Gebäudeschließsystems 14, das zudem einen externen Server 26, der hier als Cloud ausgebildet ist, und ein Authentifizierungsgerät 16 umfasst. Das Authentifizierungsgerät 16 ist neben der Tür 18 an der Gebäudewand 12 montiert und dazu vorgesehen, einen Nutzer des Gebäudeschließsystems 14 zu authentifizieren.

[0043] In Fig. 2 ist ein Grundaufbau des Authentifizierungsgeräts 16 genauer dargestellt. Das Authentifizierungsgerät 16 umfasst eine Steuereinheit 30, welche mit weiteren Komponenten des Authentifizierungsgeräts 16 verbunden ist, nämlich mit einer Bilderfassungseinrichtung 32, einer Ton-Aufnahme/Ausgabeeinrichtung 34, einer Einrichtung zum drahtlosen Senden/Empfangen 36 von Daten, einem berührungsempfindlichen Bildschirm 38 und einem Schnittstellenmodul 40 zur drahtgebundenen oder drahtlosen Verbindung des Authentifizierungsgeräts 16 mit den Türaktoren 22, 24.

[0044] Fig. 3 zeigt eine erste konkrete Ausführungsform des Authentifizierungsgeräts 16. Die Bilderfassungseinrichtung 32 umfasst hier eine 2D-Kamera 42, welche dazu vorgesehen ist, Foto- oder Videoaufnahmen eines Nutzers aufzunehmen. Diese Aufnahmen können prinzipiell einer zweidimensionalen Gesichtserkennung oder einer Erfassung charakteristischer Augenbewegungen zugrunde gelegt werden sowie einem Bewohner des Gebäudes 10 zu Informationszwecken vorgespielt werden. Überdies weist die gezeigte Bilderfassungseinrichtung 32 eine 3D-TOF-Kamera 44 auf, welche dazu vorgesehen ist, dreidimensionale Aufnahmen mittels eines Laufzeitverfahrens aufzunehmen. Diese können in einem Authentifizierungsverfahren vorteilhaft für eine dreidimensionale Gesichtserkennung und/oder einen Scan des Handvenenmusters eines Nutzers genutzt werden.

[0045] Die Ton-Aufnahme/Ausgabeeinrichtung 34 umfasst ein Mikrofon 46 sowie einen Lautsprecher 48, welche dazu vorgesehen sind, Nachrichten für andere Nutzer, insbesondere für einen Bewohner des Gebäudes 10 auf dem Authentifizierungsgerät zu hinterlassen und/oder Tonaufnahmen abzuspielen sowie auch zur biometrischen Stimmenerkennung genutzt zu werden.

[0046] Die Sende/Empfangseinrichtung 36 umfasst ein Bluetooth-Modul 50 sowie ein WLAN-Modul 52, welche in einem Authentifizierungsverfahren zum Austausch eines digitalen Schlüsselpaars mit einem mobilen Endgerät des Nutzers vorgesehen sind. Wahlweise kann der Schlüsselaustausch entsprechend mittels Bluetooth oder WLAN erfolgen.

[0047] Das Authentifizierungsgerät 16 weist überdies einen Sensor 54 zur Detektion einer Annäherung eines Nutzers an das Authentifizierungsgerät 16 auf, der hier als PIR-Sensor ausgebildet ist. Die Detektion eines Nut-

zers kann dazu führen, dass das Authentifizierungsgerät 16 aus einem Ruhemodus mit ausgeschaltetem berührungsempfindlichen Bildschirm 38 in einen Aktivmodus versetzt wird.

[0048] Die Steuereinheit 30 ist über das Schnittstellenmodul 40 mit einem lokalen Netzwerk verbunden, beispielsweise mittels Ethernet oder mittels WLAN. Über das lokale Netzwerk kann eine Internetverbindung zu einem externen Server 26 hergestellt werden, welche eine Kommunikation zwischen einem Nutzer des Authentifizierungsgeräts 16 und einem Bewohner des Gebäudes 10, insbesondere auch in dessen Abwesenheit, beispielsweise über eine mobile Applikation auf einem mobilen Endgerät des Bewohners in Form von Video-, Sprach- oder Textnachrichten oder in Form von Internettelefonie ermöglicht.

[0049] Das Authentifizierungsgerät 16 ist zudem über das Schnittstellenmodul 40 mit einem Sensor 56 verbunden, der den Öffnungszustand der Tür 18 und hier mit der Steuereinheit 30 verbunden ist. Der Sensor 56 kann grundsätzlich drahtgebunden oder drahtlos mit dem Authentifizierungsgerät 16 verbunden sein.

[0050] Das Schnittstellenmodul 40 weist hier auch ein Sub-1 GHz-Modul 64 auf, das dazu vorgesehen ist, beispielsweise den Türaktor 24 in Form eines elektronischen Schließzylinders und/oder benötigte Sensoriken an die Steuereinheit 30 des Authentifizierungsgeräts 16 anzubinden.

[0051] Das Authentifizierungsgerät 16 weist ferner eine mit der Steuereinheit 30 verbundene Datenbank 58 auf, in der vorgegebene Sicherheitsmerkmale hinterlegt sind, insbesondere biometrische Merkmale, elektronische Sicherheitsschlüssel und/oder Sicherheitscodes. Die in der Datenbank 58 hinterlegten Sicherheitsmerkmale können durch die Steuereinheit 30 mit den in einem Authentifizierungsvorgang erfassten Sicherheitsmerkmalen verglichen werden, um einen Nutzer zu identifizieren und gegebenenfalls Funktionen am Authentifizierungsgerät 16 zu starten.

[0052] Nachfolgend wird die Authentifizierung eines Nutzers mit Hilfe des Authentifizierungsgeräts 16 beschrieben. Grundsätzlich kann zwischen den Situationen 'Ankommen' (Fig. 4A,B), bei der ein Nutzer sich dem Authentifizierungsgerät 16 von der Außenseite des Gebäudes 10 her nähert und 'Verlassen' (Fig. 4C), bei der ein Nutzer das Gebäude 10 von der Innenseite her verlässt, unterschieden werden.

[0053] Bei der Situation 'Ankommen' nähert sich zunächst ein Nutzer von außen dem Gebäude oder Gelände 10 und somit dem Authentifizierungsgerät 16 des Gebäudeschließsystems 14. Der PIR-Sensor 54 detektiert die Annäherung 100 und bringt das Authentifizierungsgerät 16 von einem Ruhemodus in einen Aktivmodus, wenn der Nutzer sich dem Authentifizierungsgerät 16 bis auf einen Abstand d nähert, der nicht größer ist als ein Erkennungsabstand d_{rec}. Während im Ruhemodus der berührungsempfindliche Bildschirm 38 deaktiviert ist, wird er im Aktivmodus eingeschaltet. Solange der Abstand des Nutzers zum Authentifizierungsgerät 16 mehr als einen von einem Masternutzer konfigurierten Mindestabstand d_{min} beträgt, im gezeigten Ausführungsbeispiel 1 Meter, wird auf dem berührungsempfindlichen Bildschirm 38 ein Begrüßungsbildschirm angezeigt 102. Dieser kann z.B. einen Warnhinweis enthalten, dass der Nutzer sich in einem videoüberwachten Bereich befindet, sowie die Hausnummer des Gebäudes 10 und den Namen der Bewohner.

[0054] Sobald sich der Nutzer dem Authentifizierungsgerät 16 bis auf weniger als den Mindestabstand d_{min} nähert, startet das Authentifizierungsgerät 16 einen Authentifizierungsvorgang 104 (Fig. 4A).

[0055] In einem ersten Authentifizierungsschritt 106 wird ein erstes Sicherheitsmerkmal des Nutzers ermittelt. Im gezeigten Ausführungsbeispiel soll hierzu mittels der 2D-Kamera 42 eine zweidimensionale Gesichtserkennung des Nutzers durchgeführt werden. Eine entsprechende Aufforderung und eine Anleitung zur korrekten Positionierung des Gesichts vor der 2D-Kamera 42 werden auf dem berührungsempfindlichen Bildschirm 38 angezeigt und eine entsprechende Aufnahme des Gesichts wird erstellt. Charakteristische Merkmale der Aufnahme werden durch die Steuereinheit 30 mit vorgegebenen charakteristischen Merkmalen der am Authentifizierungsgerät 16 registrierten Nutzer verglichen, welche in der Datenbank 58 hinterlegt sind. Beispielsweise kann abhängig von den Lichtverhältnissen auf eine zweidimensionale Gesichtserfassung mittels der 2D-Kamera 42 verzichtet werden und stattdessen eine dreidimensionale Gesichtserkennung mittels der 3D-TOF-Kamera 44 im Laufzeitverfahren eingesetzt werden.

[0056] Sofern die erfasste Gesichtsgeometrie mit einer in der Datenbank 58 hinterlegten Gesichtsgeometrie eines registrierten Nutzers übereinstimmt, wird ein zweiter Authentifizierungsschritt 108 durchgeführt. In dem gezeigten Ausführungsbeispiel wird hierzu durch das Bluetooth-Modul 50 des Authentifizierungsgeräts 16 automatisch mittels Bluetooth ein Sicherheitsschlüssel von dem mobilen Endgerät des Nutzers abgefragt. Der von dem mobilen Endgerät empfangene Sicherheitsschlüssel wird durch die Steuereinheit 30 mit in der Datenbank 58 hinterlegten Sicherheitsschlüsseln verglichen.

[0057] Sofern der empfangene Sicherheitsschlüssel mit einem in der Datenbank 58 hinterlegten Sicherheitsschlüssel eines registrierten Nutzers übereinstimmt, wird durch die Steuereinheit 30 überprüft, welche Berechtigungen der identifizierte Nutzer besitzt. Ist der identifizierte Nutzer zugangsberechtigt, veranlasst die Steuereinheit 30 ein automatisiertes Entriegeln und Öffnen 110 der Tür 18 mittels der verbundenen Türaktoren 22, 24.

[0058] Auf dem berührungsempfindlichen Bildschirm 38 werden zusätzlich konfigurationsabhängig nutzerspezifische Informationen für den authentifizierten Nutzer bereitgestellt 112. Wird ein Bewohner erkannt, kann dies folgende Informationen über Ereignisse am Authentifizierungsgerät 16 und an damit verbundenen Geräten und Sensoriken umfassen:

- Verpasste Besuche, gegebenenfalls einschließlich Zeitstempel, wann die Besuche erfolgt sind, Fotoaufnahmen der Besucher und eventuell von den Besuchern hinterlassene Video-, Sprach- oder Textnachrichten, welche über den berührungsempfindlichen Bildschirm abgerufen werden können;
- Informationen über erkannte Ereignisse, wie z.B. eine Unterbrechung eines Öffnungskontakts eines mit dem Authentifizierungsgerät 16 verbundenen Briefkastens, weshalb ein Hinweis auf Post im Briefkasten angezeigt wird;
- Warnungen eines mit dem Authentifizierungsgerät 16 verbundenen Sicherheitssystems, die anzeigen, ob ein Alarm in Abwesenheit stattgefunden hat oder ob sich eine unbekannte Person auf dem Grundstück befindet.

[0059] Es versteht sich, dass die voranstehende Aufzählung nicht abschließend ist. Zusätzlich werden konfigurierbare Funktionen oder Szenarien hausinterner Systeme nutzerspezifisch nach der Authentifizierung eines Nutzers durch das Authentifizierungsgerät 16 aktiviert oder deaktiviert 114. Dies betrifft beim Heimkommen eines Bewohners beispielsweise die Deaktivierung einer Alarmanlage, das Anschalten einer Beleuchtung, die Benachrichtigung anderer, abwesender Bewohner auf ihren mobilen Endgeräten über das Heimkommen des authentifizierten Nutzers und weitere Funktionen.

[0060] Im vorliegenden Ausführungsbeispiel wird im ersten Authentifizierungsschritt 106 eine zweidimensionale Gesichtserkennung durchgeführt, im zweiten Authentifizierungsschritt 108 ein mittels Bluetooth übertragener Sicherheitsschlüssel. Das Verfahren kann grundsätzlich aber auch so ausgestaltet sein, dass zwei biometrische Merkmale oder auch gar kein biometrisches Merkmal in den Authentifizierungsschritten 106 und 108 erfasst werden. Mögliche Kombinationen wären hierbei beispielsweise

- eine 3D-Gesichtserkennung gefolgt von einem Handvenenscan, beides mittels der 3D-TOF-Kamera 44,
- eine biometrische Stimmenerkennung mittels des Mikrofons 46 gefolgt von der Abfrage eines Bluetooth-Schlüssels durch das Bluetooth-Modul 50,
- eine Erfassung einer charakteristischen Augenbewegung mittels der 2D-Kamera 42 gefolgt von der Abfrage eines WLAN-Schlüssels durch das WLAN-Modul 52,
- eine Erfassung eines QR-Codes mittels der 2D-Kamera 42 gefolgt von einer 2D-Gesichtserkennung mittels derselben 2D-Kamera 42,
- eine Abfrage eines Bluetooth-Schlüssels durch das Bluetooth-Modul 50 gefolgt von einer Authentifizierung mittels einer manuellen Sicherheitscode-Eingabe mittels des berührungsempfindlichen Bildschirms 38,
- eine biometrische Stimmenerkennung mittels des Mikrofons 46 während der Aussprache eines Code-Worts, welches entweder ein personenbezogenes Passwort sein kann, das in der Datenbank 58 hinterlegt ist, oder ein Zufallswort, das auf dem berührungsempfindlichen Bildschirm 38 angezeigt und vorgelesen werden muss.

[0061] Auch diese Aufzählung ist nicht abschließend, sondern vielmehr beispielhaft für die möglichen Kombinationen von Merkmalen, die sich mit den Komponenten des Authentifizierungsgeräts 16 aus Fig. 3 ausführen lassen. Je nach Anwendungsbereich und -ziel kann eine entsprechend vorteilhafte Kombination von Merkmalen für die konkrete Ausführung des Authentifizierungsgeräts 16 und des Authentifizierungsverfahrens gewählt werden.

[0062] Wird im Authentifizierungsverfahren ein Nutzer erkannt, der am Authentifizierungsgerät 16 registriert, aber nicht zugangsberechtigt ist, wird abhängig vom authentifizierten Nutzer ein entsprechender erweiterter Funktionsumfang auf dem berührungsempfindlichen Bildschirm 38 des Authentifizierungsgeräts 16 angezeigt. Das betrifft beispielsweise den Nachbarn, der in Abwesenheit der Bewohner am Authentifizierungsgerät 16 die mit dem Authentifizierungsgerät 16 verbundene Gartenbewässerungsanlage aktivieren kann.

[0063] Sofern eines der in einem der Authentifizierungsschritte 106 oder 108 erfassten Sicherheitsmerkmale nicht mit einem hinterlegten Sicherheitsmerkmal eines registrierten Nutzers übereinstimmt, werden einem Nutzer auf dem berührungsempfindlichen Bildschirm 38 ein oder mehrere Eingabefelder angezeigt, mittels derer eine Nutzereingabe in das Authentifizierungsgerät 16 erfolgen kann und Informationen für den Nutzer bereitgestellt werden können (Fig. 4B).

[0064] Ein Eingabefeld 116 ermöglicht es dem Nutzer ein Klingelsignal zu erzeugen, das an einem Signalgerät im Innenbereich des Gebäudes 10 wiedergegeben wird, um einen Bewohner über die Anwesenheit eines Besuchers am Authentifizierungsgerät 16 zu informieren. Zusätzlich kann auf dem Signalgerät im Innenbereich ein Foto oder Video des Besuchers angezeigt werden. Der Bewohner kann daraufhin dem Besucher die Tür 18 manuell oder automatisiert öffnen.

[0065] Ist der Bewohner vom Gebäude 10 abwesend, kann mittels des externen Servers 26 das Klingelsignal an einem mobilen Endgerät des Bewohners wiedergegeben werden, ebenso kann ein Foto oder Video des Besuchers übertragen werden. Der Bewohner kann dann auf das Klingelsignal hin einen Video- oder Sprachanruf mit dem Authentifizierungsgerät 16 annehmen.

[0066] Nach einem unbeantworteten Klingelvorgang ermöglicht es ein Eingabefeld 118 dem Besucher, einen Video- oder Sprachanruf mittels des externen Servers 26 mit einem mobilen Endgerät des Bewohners herzustellen. Ein anderes Eingabefeld 120 stellt eine Funktion zum Senden einer Textnachricht an ein mobiles Endgerät des Bewohners mittels des externen Servers 26 be-

reit. Ein Eingabefeld 122 ermöglicht, eine Video-, Sprach-, oder Textnachricht auf dem Authentifizierungsgerät 16 zu hinterlassen. Ein Eingabefeld 124 ermöglicht es, eine Video-, Sprach- oder Textnachricht abzurufen, die der Bewohner auf dem Authentifizierungsgerät 16 hinterlassen hat. Ein Eingabefeld 126 stellt die Möglichkeit bereit, die Tür 18 durch Eingabe eines Sicherheitscodes zu öffnen.

[0067] Es versteht sich, dass die beschriebene Ausführungsform nur beispielhaft zu verstehen ist. Welche der genannten Eingabefelder und Funktionen bereitgestellt werden sollen, ist durch einen Masternutzer des Authentifizierungsgeräts 16 bedarfsgerecht konfigurierbar. Andere Ausführungsformen sind jederzeit möglich. So kann beispielsweise auf dem berührungsempfindlichen Bildschirm 38 des Authentifizierungsgeräts 16 ein Informationsfeld 128 angezeigt werden, das einen Nutzer über Öffnungszeiten informiert, beispielsweise falls das Authentifizierungsgerät 16 nicht in einem Privathaushalt sondern in einem geschäftlichen Umfeld zum Einsatz kommt. Entsprechend kann der berührungsempfindlichen Bildschirm 38 als Werbefläche genutzt werden oder Infotainment für den Besucher bereitstellen.

[0068] Eine Ausführungsform der Situation 'Verlassen' ist in Fig. 4C dargestellt. Gestartet wird der Ablauf durch ein von der Sensorik 56 erfasstes Öffnen 130 der Tür 18. Bei nachfolgender Annäherung eines Nutzers an das Authentifizierungsgerät 16 werden die Schritte 100-106 des Authentifizierungsverfahrens gestartet wie in der Situation 'Ankommen' (Fig. 4A) beschrieben. Sofern die Authentifizierung eines bekannten Nutzers innerhalb eines vorbestimmten Zeitfensters $t < tmax$ von beispielsweise 1 Minute nach dem detektierten Öffnen 130 der Tür 18 erfolgt, erkennt das Authentifizierungsgerät 16, dass es sich um die Situation 'Verlassen' handelt, das heißt, eine Person verlässt das Gebäude 10. Sofern in diesem Fall das Authentifizierungsgerät 16 im ersten Authentifizierungsschritt 106 einen zugangsberechtigten Nutzer erkennt, wird kein weiterer Authentifizierungsschritt 108 durchgeführt, sondern ein automatisches Schließen und/oder Verriegeln 132 der Tür 18 veranlasst.

[0069] Auch diese Funktion des Authentifizierungsgeräts 16 kann durch einen Masternutzer derart konfigurierbar sein, dass beispielsweise die Nutzergruppen konfiguriert werden, für die ein automatisiertes Verriegeln der Tür 132 stattfinden soll, oder dass das automatisierte Verriegeln 132 der Tür 18 nur dann stattfindet, wenn das Authentifizierungsgerät 16 mittels der Sensorik 56 detektiert hat, dass alle Bewohner das Gebäude 10 verlassen haben.

[0070] Ebenso wie beim 'Ankommen' können einem authentifizierten Nutzer beim 'Verlassen' konfigurierbare nutzerspezifische Informationen auf dem berührungsempfindlichen Bildschirm 38 angezeigt sowie Funktionen oder Szenarien an mit dem Authentifizierungsgerät 16 verbundenen Geräten gestartet werden. In diesem Fall wird beim Verlassen des Gebäudes 10 eine Alarmanlage aktiviert, sowie die Beleuchtung ausgeschaltet. Dem Bewohner werden Hinweise angezeigt - basierend auf seinem Kalender beispielsweise eine Erinnerung, eine Sporttasche mitzunehmen oder basierend auf einem aus dem Internet bereitgestellten Wetterbericht ein Hinweis, einen Regenschirm einzupacken.

[0071] Ebenso können konfigurierbare Eingabefelder angezeigt werden, die ein manuelles Ansteuern verbundener Geräte nach Bedarf ermöglichen, beispielsweise ein Öffnen des Garagentors sowie die Weiterleitung von Klingelsignalen, die am Authentifizierungsgerät 16 ausgelöst werden, auf ein mobiles Endgerät.

[0072] Fig. 5 zeigt eine zweite konkrete Ausführungsform des Authentifizierungsgeräts 16, die sich letztlich nur darin von der ersten konkreten Ausführungsform von Fig. 3 unterscheidet, dass die Sende/Empfangseinrichtung 36 ein RFID-Modul 62 zusätzlich zum Bluetooth-Modul 44 und zum WLAN-Modul 46 aufweist. Mit diesem Authentifizierungsgerät 16 sind weitere Ausgestaltungen des Authentifizierungsverfahrens möglich, da es zusätzliche Möglichkeiten bietet, wie ein Nutzer am Authentifizierungsgerät 16 authentifiziert werden kann. So kann entweder im ersten Authentifizierungsschritt 106 oder im zweiten Authentifizierungsschritt 108 ein nutzerbezogener RFID-Tag als erfasstes Sicherheitsmerkmal vom Authentifizierungsgerät 16 ausgelesen werden. Es versteht sich, dass in anderen Ausführungsformen des Authentifizierungsgeräts 16 Übertragungsstandards wie NFC, bereitgestellt durch ein NFC-Modul, zum Einsatz kommen können, wobei eine beliebige Kombination mit den voranstehend genannten weiteren Modulen zum drahtlosen Senden/Empfangen von Daten möglich ist.

Bezugszeichenliste

[0073]

10	Gebäude
12	Gebäudewand
14	Gebäudeschließsystem
16	Authentifizierungsgerät
18	Tür
22	elektrische Türöffnungsvorrichtung
24	motorisiertes Türschloss
26	externer Server
30	Steuereinheit
32	Bilderfassungseinrichtung
34	Ton-Aufnahme/Ausgabeeinrichtung
36	Einrichtung zum drahtlosen Senden/Empfangen von Daten
38	berührungsempfindlicher Bildschirm
40	Schnittstellenmodul
42	2D-Kamera
44	3D-TOF-Kamera
46	Mikrofon
48	Lautsprecher
50	Bluetooth-Modul
52	WLAN-Modul
54	PIR-Sensor

56 Sensorik zur Erfassung eines Öffnungszustandes einer Tür
58 Datenbank
62 RFID-Modul
64 Sub-1 GHz-Modul
100 Detektion eines Nutzers im Erkennungsabstand $d_{min} < d < d_{rec}$
102 Anzeige eines Begrüßungsbildschirms
104 Start des Authentifizierungsverfahrens bei $d < d_{min}$
106 erster Authentifizierungschritt
108 zweiter Authentifizierungsschritt
110 automatisches Entriegeln und/oder Öffnen einer Tür
112 nutzerspezifische optionale Informationen
114 nutzerspezifische Aktivierung von Funktionen/Szenarien
116 Eingabefeld für Klingelsignal
118 Eingabefeld für Video-/Sprachanruf auf mobiles Endgerät
120 Eingabefeld für Textnachricht auf mobiles Endgerät
122 Eingabefeld zum Hinterlassen einer Video-/Sprach-/Textnachricht
124 Eingabefeld zum Abrufen einer Nachricht
126 Eingabefeld zum Eingeben eines Sicherheitscodes
128 Informationsfeld
130 Erfassung des Öffnens einer Tür
132 automatisches Schließen und/oder Verriegeln einer Tür

Patentansprüche

1. Wandmontierbares Authentifizierungsgerät (16) zur Authentifizierung eines Nutzers eines Gebäudeschließsystems (14), umfassend:

eine Steuereinheit (30),
eine mit der Steuereinheit (30) verbundene Bilderfassungseinrichtung (32),
eine mit der Steuereinheit (30) verbundene Ton-Aufnahme/Ausgabeeinrichtung (34),
eine mit der Steuereinheit (30) verbundene Einrichtung zum drahtlosen Senden/Empfangen von Daten (36),
einen mit der Steuereinheit (30) verbundenen berührungsempfindlichen Bildschirm (38) und
ein mit der Steuereinheit (30) verbundenes Schnittstellenmodul (40) zur Verbindung des Authentifizierungsgeräts (16) mit mindestens einem Türaktor (22, 24).

2. Authentifizierungsgerät (16) nach Anspruch 1,
wobei das Authentifizierungsgerät (16) eine mit der Steuereinheit (30) verbundene Sensorik (54) zur Erfassung der Annäherung einer Person an das Authentifizierungsgerät (16) aufweist.

3. Authentifizierungsgerät (16) nach Anspruch 1 oder 2,
wobei das Authentifizierungsgerät (16) eine Datenbank (58) aufweist, in der vorgegebene Sicherheitsmerkmale hinterlegt sind, insbesondere biometrische Merkmale, elektronische Sicherheitsschlüssel und/oder Sicherheitscodes.

4. Authentifizierungsgerät (16) nach einem der vorherigen Ansprüche,
wobei das Schnittstellenmodul (40) zur Verbindung der Steuereinheit (30) mit einem lokalen Netzwerk, einem externen Server (26), einer Türklingel, einer Sensorik (56) zur Erfassung eines Öffnungszustands einer dem Türaktor (22, 24) zugeordneten Tür (18), einem Smart Home System und/oder einer Alarmanlage ausgebildet ist.

5. Authentifizierungsgerät (16) nach einem der vorherigen Ansprüche,
wobei die Bilderfassungseinrichtung (32) eine 2D-Kamera (42) und/oder eine 3D-Kamera (44), beispielsweise eine TOF-Kamera zur Bilderfassung mittels Laufzeitverfahren, aufweist.

6. Authentifizierungsgerät (16) nach einem der vorherigen Ansprüche,
wobei die Einrichtung zum drahtlosen Senden/Empfangen von Daten (36) ein Bluetooth-Modul (50), ein RFID-Modul (62), ein NFC-Modul und/oder ein WLAN-Modul (52) aufweist.

7. Gebäudeschließsystem (14) mit einem Authentifizierungsgerät (16) nach einem der vorherigen Ansprüche und einem mit dem Authentifizierungsgerät (16) verbundenen Türaktor (22, 24).

8. Gebäudeschließsystem (16) nach Anspruch 7,
wobei das Authentifizierungsgerät (16) mit einem lokalen Netzwerk, einem externen Server (26), einer Sensorik (56) zur Erfassung eines Öffnungszustands einer dem Türaktor (22, 24) zugeordneten Tür (18), einer Türklingel, einem Smart Home System und/oder einer Alarmanlage verbunden ist.

9. Verfahren zur Authentifizierung eines Nutzers eines Gebäudeschließsystems (14) mittels eines mit einem Türaktor (22, 24) verbundenen Authentifizierungsgeräts (16) nach einem der vorherigen Ansprüche,

wobei das Authentifizierungsgerät (16) in einem ersten Authentifizierungsschritt (106) ein erstes Sicherheitsmerkmal des Nutzers erfasst und das erfasste erste Sicherheitsmerkmal mit wenigstens einem ersten vorgegeben Sicherheits-

merkmal vergleicht und,
sofern das erfasste erste Sicherheitsmerkmal mit dem ersten vorgegebenen Sicherheitsmerkmal übereinstimmt, das Authentifizierungsgerät (16) in einem zweiten Authentifizierungsschritt (108) ein zweites Sicherheitsmerkmal des Nutzers erfasst und das erfasste zweite Sicherheitsmerkmal mit wenigstens einem zweiten vorgegeben Sicherheitsmerkmal vergleicht und,
sofern das erfasste zweite Sicherheitsmerkmal mit dem zweiten vorgegebenen Sicherheitsmerkmal übereinstimmt, die Steuereinheit (30) ein Entriegeln und/oder Öffnen (110) einer dem Türaktor (22, 24) zugeordneten Tür (18) veranlasst.

10. Verfahren nach Anspruch 9,
wobei das erste und/oder zweite erfasste Sicherheitsmerkmal ein biometrisches Merkmal ist.

11. Verfahren nach Anspruch 9 oder 10,
wobei, wenn das Authentifizierungsgerät (16) innerhalb eines vorbestimmten Zeitraums vor dem ersten Authentifizierungsschritt (106) ein Öffnen der Tür erfasst hat (130), die Steuereinheit (30) ein Verriegeln (132) der dem Türaktor (22, 24) zugeordneten Tür (18)veranlasst, sofern bereits das im ersten Authentifizierungsschritt (106) erfasste Sicherheitsmerkmal mit einem entsprechend vorgegebenen Sicherheitsmerkmal übereinstimmt.

12. Verfahren nach einem der Ansprüche 9 bis 11,
wobei, wenn ein in einem der Authentifizierungsschritte (106, 108) erfasstes Sicherheitsmerkmal nicht mit einem entsprechend vorgegebenen Sicherheitsmerkmal übereinstimmt, auf dem berührungsempfindlichen Bildschirm (38) wenigstens ein Eingabefeld (116, 118, 120, 122, 124, 126) für eine Nutzereingabe angezeigt wird, das es dem Nutzer ermöglicht,

ein Klingelsignal zu erzeugen,
eine Video-, Sprach- oder Textnachricht für einen anderen Nutzer des Authentifizierungsgeräts (16) auf dem Authentifizierungsgerät (16) zu hinterlassen,
einen Video- oder Sprachanruf über das Authentifizierungsgerät (16) zu einem mobilen Endgerät eines anderen Nutzers des Authentifizierungsgeräts (16) herzustellen,
eine Textnachricht über das Authentifizierungsgerät (16) zu einem mobilen Endgerät eines anderen Nutzers des Authentifizierungsgeräts (16) zuzustellen,
eine Video-, Sprach- oder Textnachricht, die ein anderer Nutzer auf dem Authentifizierungsgerät (16) hinterlegt hat, abzurufen und/oder
mittels manueller Eingabe eines Sicherheitscodes ein Entriegeln und/oder Öffnen der dem Türaktor (22, 24) zugeordneten Tür (18) zu veranlassen.

13. Verfahren nach einem der Ansprüche 9 bis 12,
wobei das Authentifizierungsgerät (16) nach Benutzung in einen Ruhemodus übergeht und erst dann in einen Aktivmodus wechselt und den ersten Authentifizierungsschritt (106) startet, wenn die Annäherung eines Nutzers an das Authentifizierungsgerät (16) detektiert wird (100).

14. Verfahren nach einem der Ansprüche 9 bis 13,
wobei dem Nutzer in Abhängigkeit von einem Abstand zwischen dem Nutzer und dem Authentifizierungsgerät (16) unterschiedliche Visualisierungen (102, 128) auf dem berührungsempfindlichen Bildschirm (38) des Authentifizierungsgeräts (16) angezeigt werden.

15. Verfahren nach einem der Ansprüche 9 bis 14,
wobei, sofern alle erfassten Sicherheitsmerkmale mit entsprechend vorgegebenen Sicherheitsmerkmalen übereinstimmen,

weitere konfigurierbare Funktionen, insbesondere Smart-Home-Geräte sowie Sicherheitssysteme, aktiviert oder deaktiviert werden (114) und/oder
Informationen über deren Zustand sowie erfasste Ereignisse und Warnungen auf dem berührungsempfindlichen Bildschirm (38) des Authentifizierungsgeräts (16) angezeigt werden (112) und/oder
Informationen über Aktivitäten am Authentifizierungsgerät (16) sowie damit verbundenen Geräten oder Sensoriken auf dem berührungsempfindlichen Bildschirm (38) des Authentifizierungsgeräts (16) angezeigt werden (112).

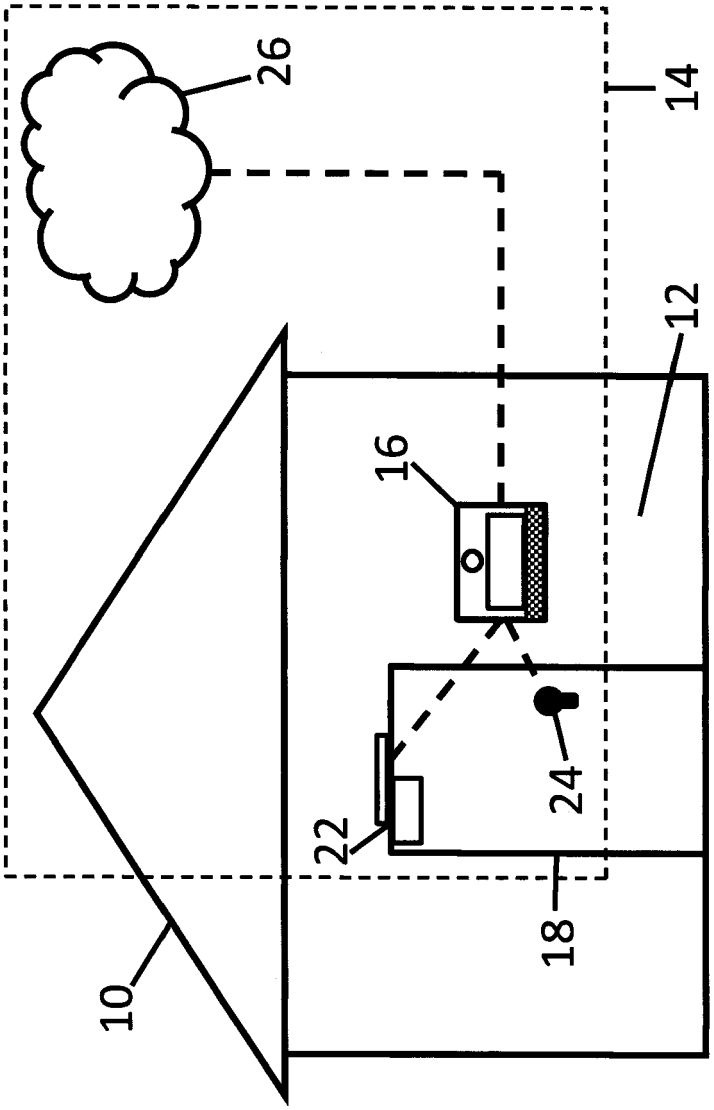


Fig. 1

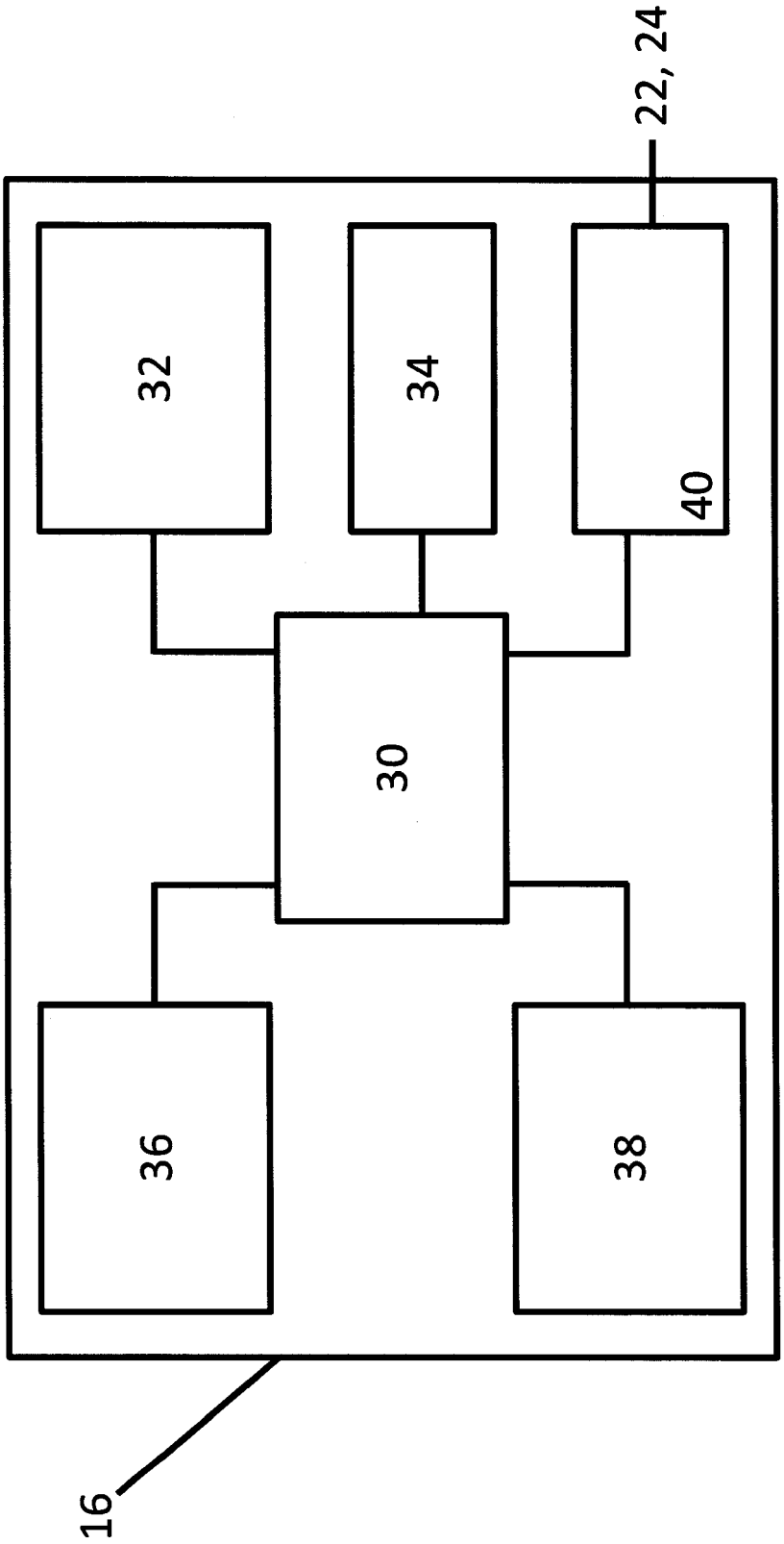


Fig. 2

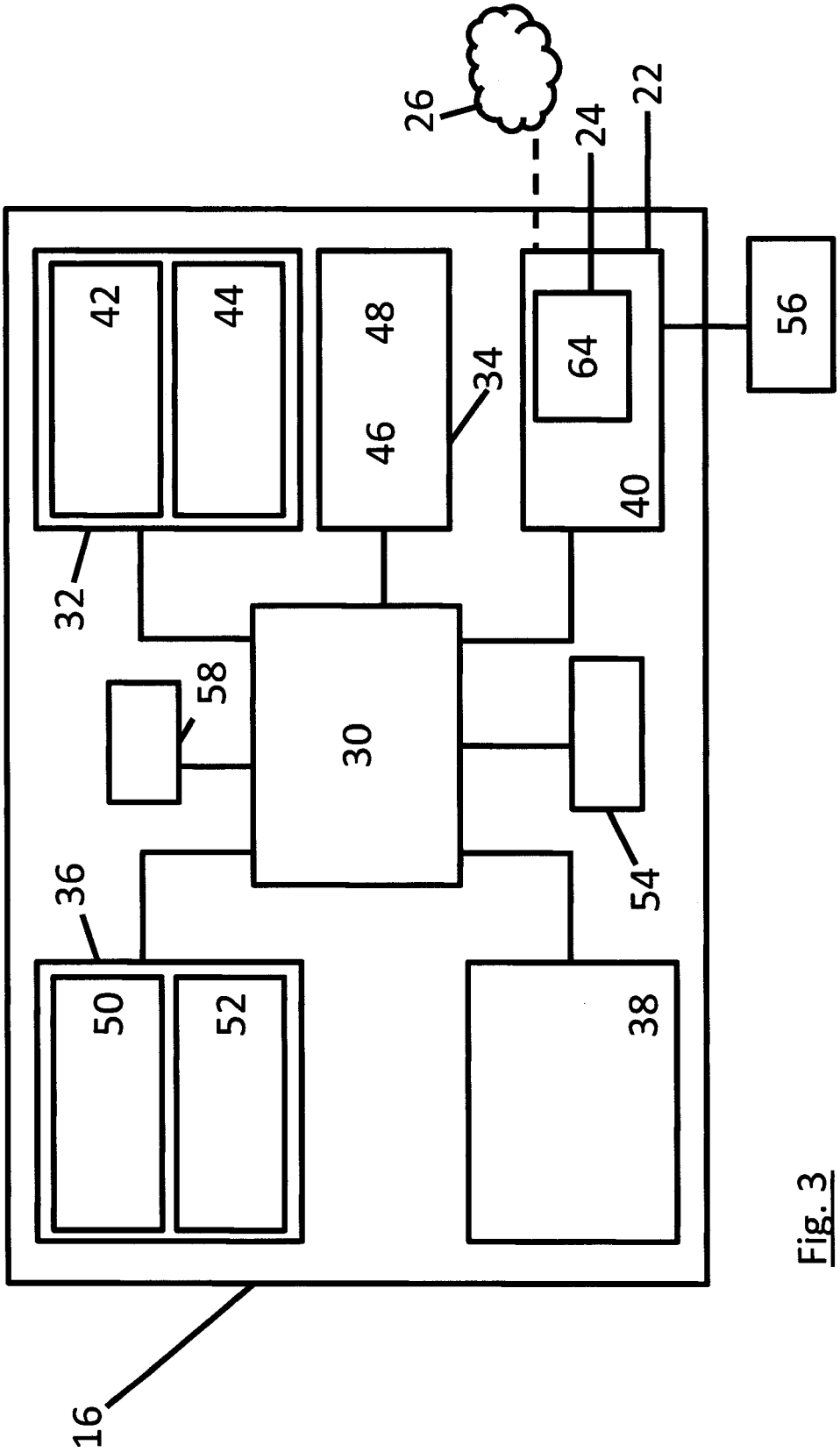


Fig. 3

Fig. 4A

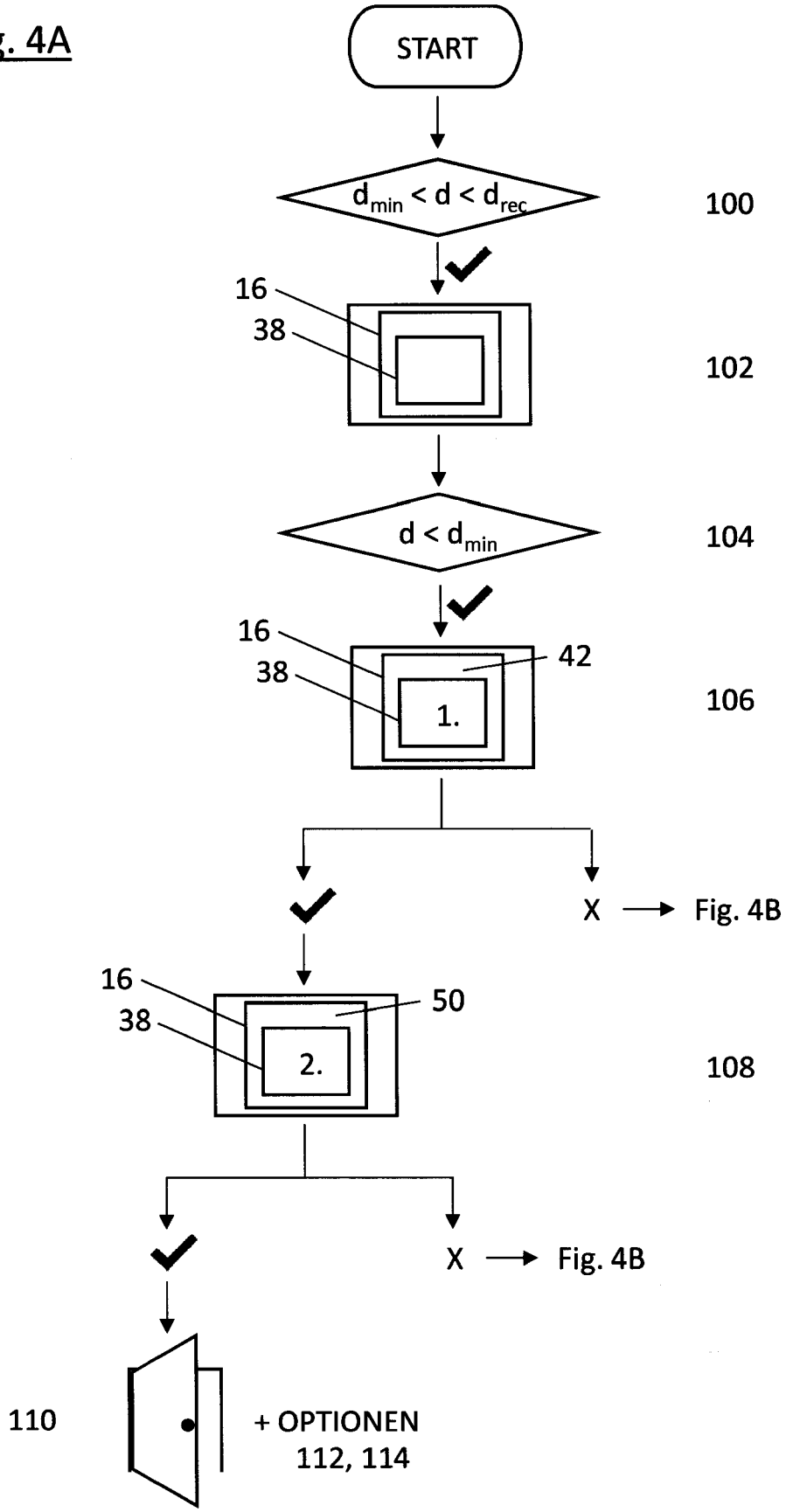

START
$d_{min} < d < d_{rec}$
100
16
38
102
$d < d_{min}$
104
16
38
42
1.
106
X → Fig. 4B
16
38
50
2.
108
X → Fig. 4B
110
+ OPTIONEN
112, 114

Fig. 4B

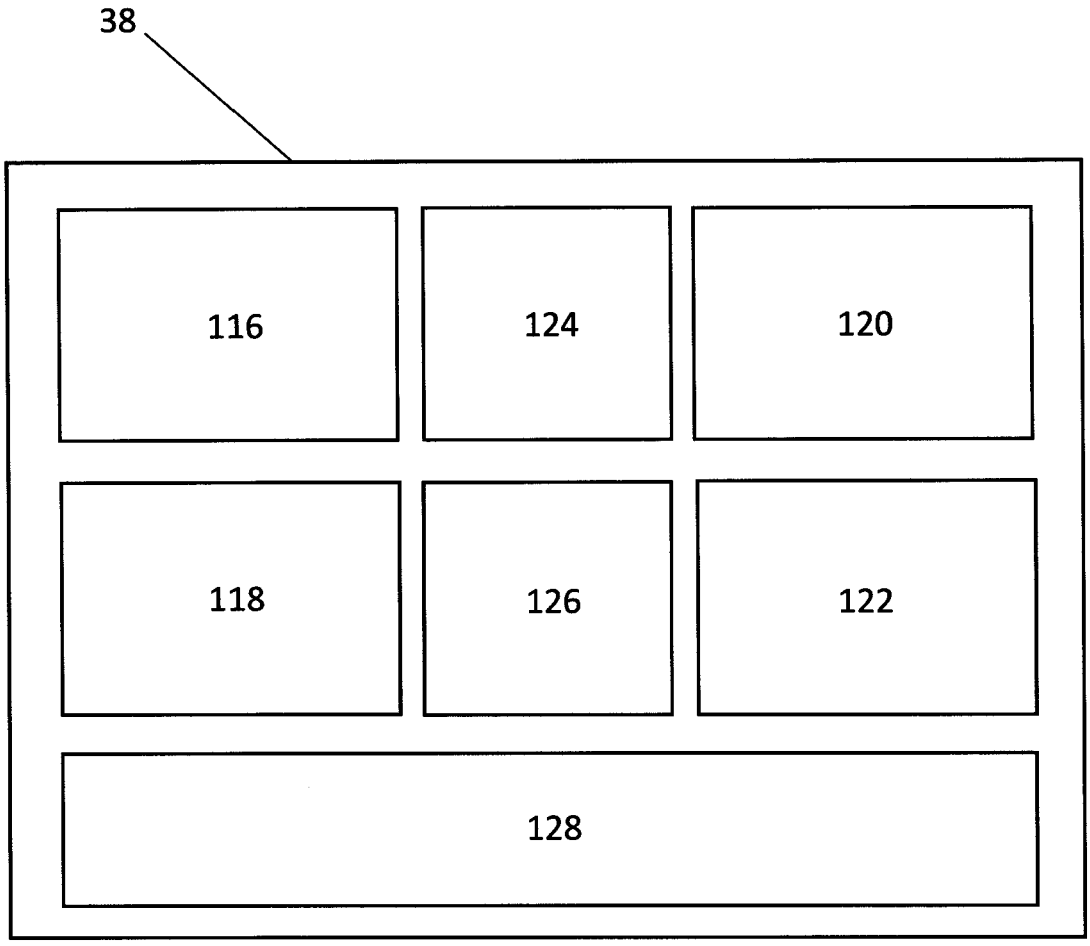
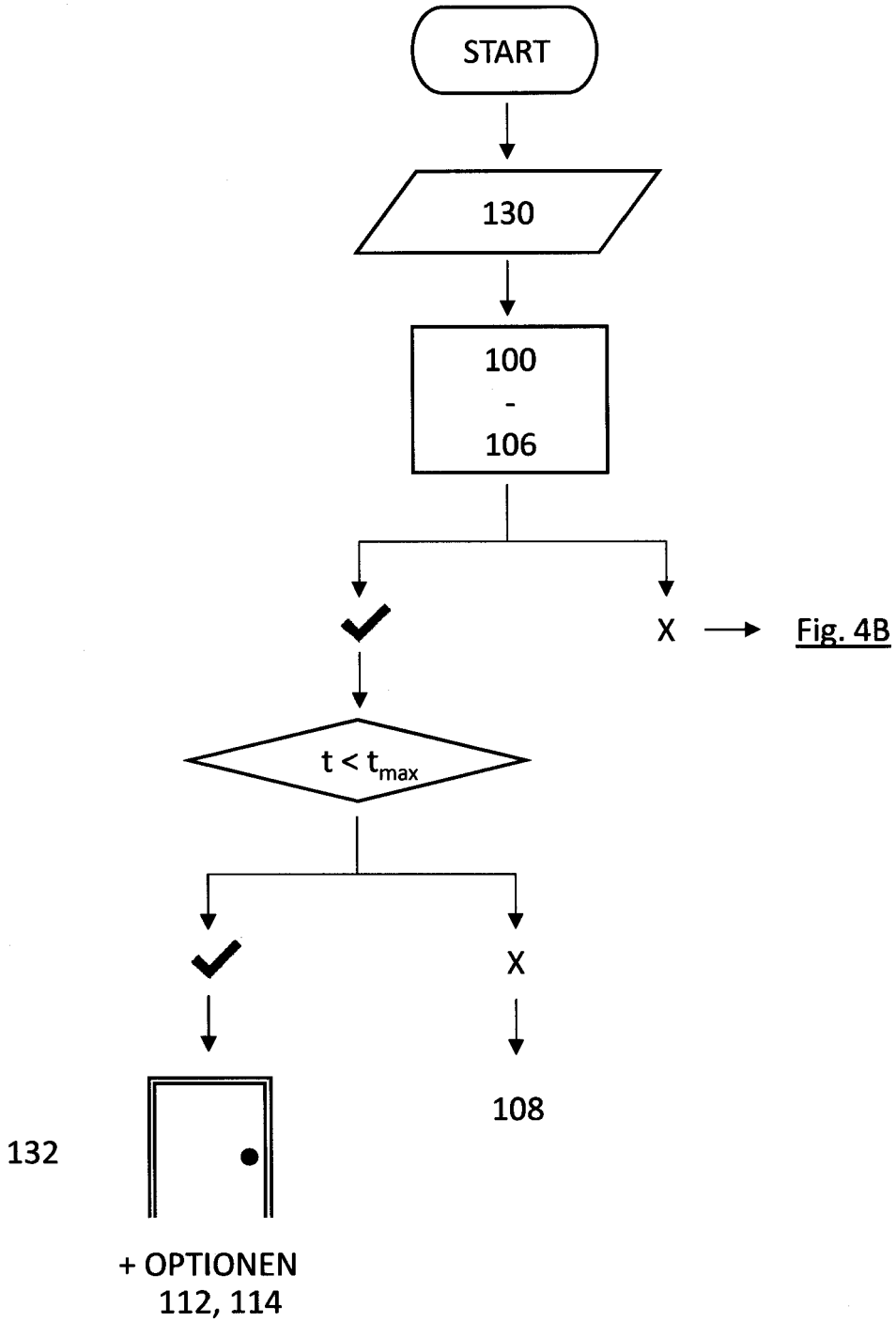


Fig. 4C



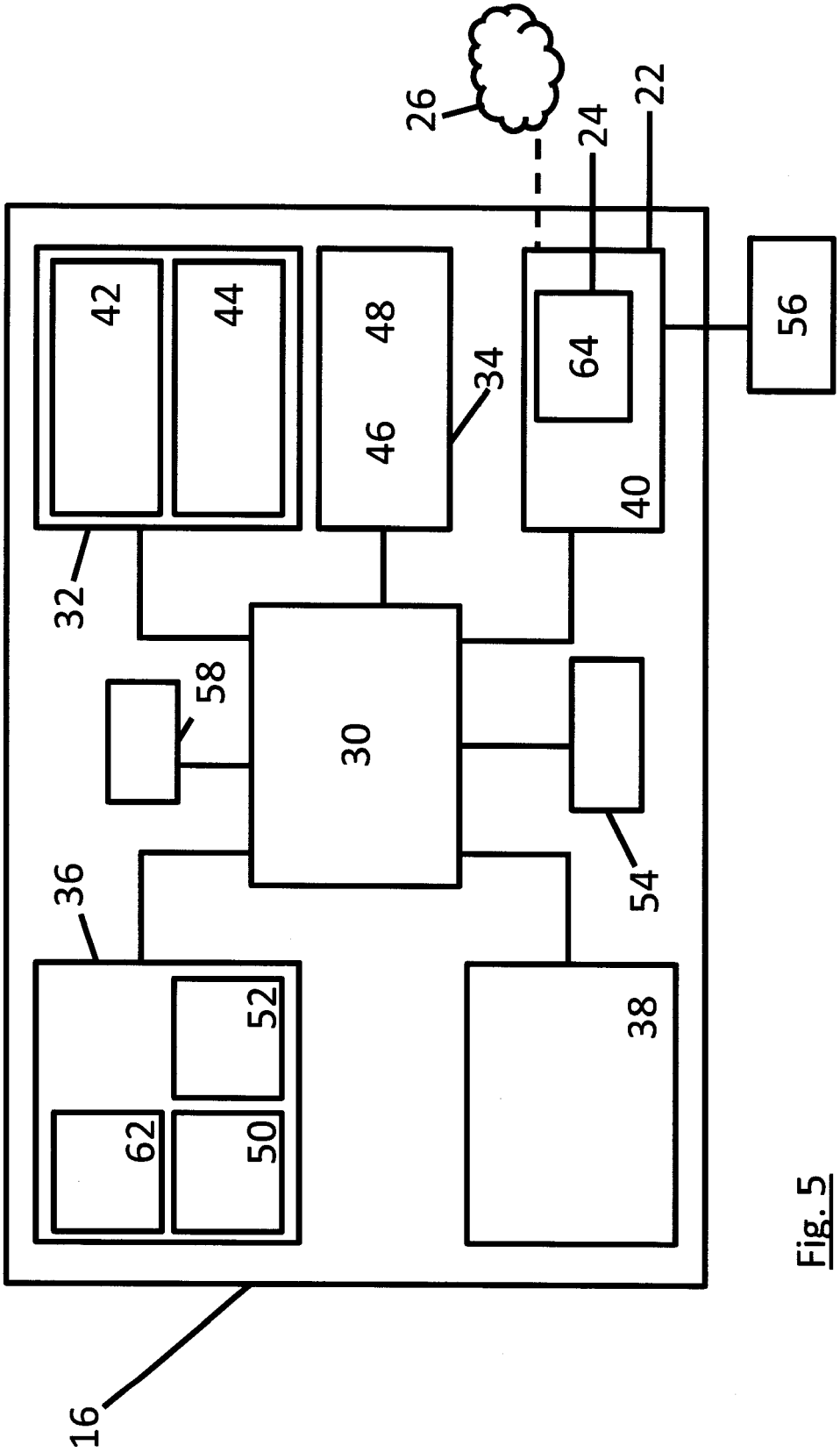


Fig. 5

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 20 17 7544

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X A	EP 3 200 161 A1 (HONEYWELL INT INC [US]) 2. August 2017 (2017-08-02) * Absätze [0015], [0017], [0018], [0019], [0024], [0033], [0034]; Abbildungen 1,2,5 *	1,2,4-7, 9,10 3,8	INV. G07C9/23 G07C9/25
X	US 2016/308859 A1 (BARRY PATRICK J [US] ET AL) 20. Oktober 2016 (2016-10-20) * Absätze [0034], [0035], [0038], [0039], [0043] - Absätze [0047], [0060], [0092], [0120], [0156], [0160], [0161], [0182]; Abbildungen 1-9 *	1,3,5-9, 12-14	
X	US 2017/076518 A1 (PATTERSON KATHY [US] ET AL) 16. März 2017 (2017-03-16) * Absätze [0040], [0057], [0087], [0088]; Abbildung 2 *	1,5-10, 12-15	
X A	DE 20 2011 110280 U1 (TELEGAERTNER GMBH [DE]) 30. April 2013 (2013-04-30) * Absätze [0020], [0026], [0028], [0029], [0036], [0042], [0049]; Abbildungen 1-3 *	1,2,4-8 12,14,15	RECHERCHIERTE SACHGEBIETE (IPC) G07C
X	US 2014/210590 A1 (CASTRO RODRIGO C [BR] ET AL) 31. Juli 2014 (2014-07-31) * Absatz [0043] *	1,3	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	19. Oktober 2020	Harder, Sebastian

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 20 17 7544

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

19-10-2020

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 3200161 A1	02-08-2017	CA 2955657 A1	27-07-2017
		CN 107018124 A	04-08-2017
		EP 3200161 A1	02-08-2017
		US 2017213404 A1	27-07-2017
		US 2019272688 A1	05-09-2019
US 2016308859 A1	20-10-2016	KEINE	
US 2017076518 A1	16-03-2017	US 2017076518 A1	16-03-2017
		US 2019012855 A1	10-01-2019
DE 202011110280 U1	30-04-2013	DE 102011089225 A1	20-06-2013
		DE 202011110280 U1	30-04-2013
		EP 2608511 A1	26-06-2013
US 2014210590 A1	31-07-2014	US 2014210590 A1	31-07-2014
		US 2016040470 A1	11-02-2016
		US 2018195334 A1	12-07-2018

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82