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

(11) **EP 3 816 946 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
05.05.2021 Patentblatt 2021/18

(51) Int Cl.:
G07C 9/00 *(2020.01)*

(21) Anmeldenummer: **19205968.1**

(22) Anmeldetag: **29.10.2019**

(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

(71) Anmelder: **GIRA GIERSIEPEN GmbH & Co. KG**
42477 Radevormwald (DE)

(72) Erfinder:
- **Schimmelpfennig, Frank**
  42477 Radevormwald (DE)
- **Hellenbroich, Fabian**
  50321 Brühl (DE)
- **Dornseiff, André**
  51688 Wipperfürth (DE)

(74) Vertreter: **Angerhausen, Christoph**
Boehmert & Boehmert
Anwaltspartnerschaft mbB
Pettenkoferstrasse 22
80336 München (DE)

(54) ZUTRITTSKONTROLLSYSTEM FÜR EIN GEBÄUDE SOWIE EIN ENTSPRECHENDES VERFAHREN

(57) Die Erfindung betrifft ein Zutrittskontrollsystem (1) für ein Gebäude (100), mit einer Authentifizierungseinheit (2), die über eine Datenverbindung (3) mit einem Aktor (4) zum Ansteuern eines Türschlosses (5) verbunden ist, wobei die Authentifizierungseinheit (2) dazu eingerichtet ist, im Falle einer erfolgreichen Authentifizierung ein Zugangsberechtigungssignal über die Datenverbindung (3) an den Aktor (4) zu übertragen, und wobei der Aktor (4) dazu eingerichtet ist, aus dem Zugangsberechtigungssignal ein Steuersignal zur Ansteuerung eines Türschlosses (5) des Zutrittskontrollsystems (1) zu erzeugen und an das Türschloss (5) zu übertragen oder das Zugangsberechtigungssignal unverändert als das Steuersignal an das Türschloss (5) zu übertragen. Es werden weiterhin ein entsprechendes Gebäude sowie ein entsprechendes Verfahren beschrieben.

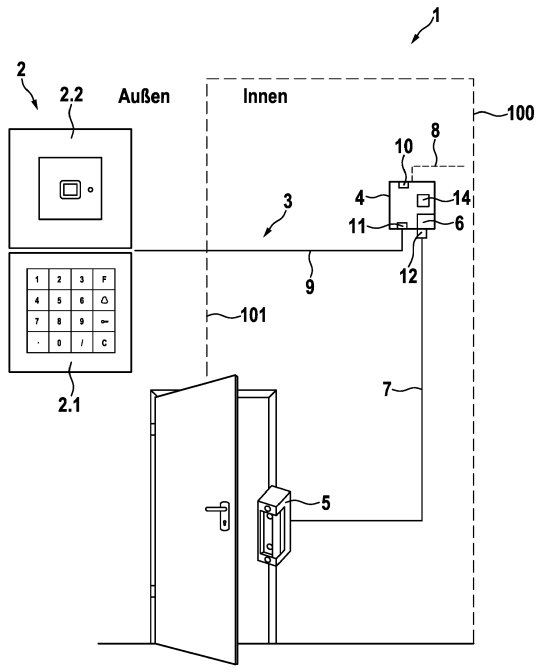

Fig. 1

EP 3 816 946 A1

Beschreibung

[0001] Die Erfindung betrifft ein Zutrittskontrollsystem für ein Gebäude sowie ein entsprechendes Verfahren.

[0002] Die aus dem Stand der Technik bekannten Zutrittskontrollsysteme haben häufig den Nachteil, dass sie vergleichsweise einfach zu manipulieren sind, was insbesondere daran liegt, dass von der Authentifizierungseinheit, beispielsweise von einem Fingerprintsensor oder einer Codetastatur, lediglich ein leicht zu reproduzierender Signalimpuls über eine Bus- oder sonstige Signalleitung an ein Steuergerät übersendet wird, um die Betätigung eines Türschlosses zu bewirken. Um dieser Manipulation vorzubeugen ist es bekannt, die Authentifizierungseinheit vergleichsweise mechanisch stabil auszubilden beziehungsweise sie mit geeigneten Maßnahmen manipulationssicher in der Gebäudewand zu verankern, um den Zugriff auf die Signalleitung zu verhindern.

[0003] Die EP 2 584 539 B1 beschreibt ein Verfahren zum manipulationsgesicherten Konfigurieren eines elektromechanischen Schlosses, welches über einen RFID-Transponder angesteuert werden kann und bei dem vorgesehen ist, dass die RFID-Schnittstelle unter Verwendung eines Protokolls für die drahtlose Übertragung einer Parametrisierung an das Schloss verwendet wird. Die DE 20 2014 103 128 U1 thematisiert die manipulationssichere Anordnung eines Sensors einer Zutrittskontrollvorrichtung.

[0004] Es ist die Aufgabe der Erfindung, ein Zutrittskontrollsystem der eingangs beschriebenen Art derart weiterzuentwickeln, dass einerseits manipulationssicher ausgebildet ist, andererseits jedoch zur Sicherstellung der Manipulationssicherung keine Veränderung am Bauwerk erfordert und darüber hinaus auch selbst mit einfachen technischen Mitteln realisierbar ist und dadurch die Möglichkeit bietet, eine weitestgehend nach ästhetischen Erwägungen gewählte äußere Gestaltungsform aufzuweisen.

[0005] Diese Aufgabe wird durch ein Zutrittskontrollsystem mit den Merkmalen des Anspruchs 1 gelöst. Der nebengeordnete Anspruch 11 betrifft ein entsprechendes Gebäude und der nebengeordnete Anspruch 13 ein entsprechendes Verfahren für den Betrieb eines derartigen Zutrittskontrollsystems. Die abhängigen Ansprüche betreffen jeweils vorteilhafte Ausführungsformen der Erfindung.

[0006] Demgemäß ist bei einem Zutrittskontrollsystem vorgesehen, dass es eine Authentifizierungseinheit aufweist, die über eine verschlüsselte oder unverschlüsselte Datenverbindung mit einem Aktor zum Ansteuern eines Türschlosses verbunden ist, wobei die Authentifizierungseinheit dazu eingerichtet ist, im Falle einer erfolgreichen Authentifizierung ein Zugangsberechtigungssignal über die Datenverbindung an den Aktor zu übertragen. Dabei ist der Aktor dazu eingerichtet, aus dem Zugangsberechtigungssignal ein Steuersignal zur Ansteuerung eines Türschlosses des Zutrittskontrollsystems zu erzeugen und an das Türschloss zu übertragen oder das Zugangsberechtigungssignal unverändert als das Steuersignal an das Türschloss zu übertragen.

[0007] Durch die Verwendung einer verschlüsselten Datenverbindung und/oder durch die Verwendung eines Datentelegramms zur Übertragung von Signalen zwischen der Authentifizierungseinheit und dem Aktor, der insbesondere im Inneren des Gebäudes oder in einer Gebäudewand von außen unzugänglich angeordnet sein kann, ist es nicht ohne Weiteres möglich, beispielsweise durch eine Demontage der Authentifizierungseinheit von einer Gebäudeaußenwand ein simuliertes Auslösesignal für das Türschloss in das System einzuspeisen.

[0008] Der Aktor kann dazu eingerichtet sein, ein über die Datenverbindung übertragenes Signal auf Authentizität zu überprüfen und nur dann ein entsprechendes Steuersignal zur Ansteuerung des Türschlosses an das Türschloss auszusenden beziehungsweise das von der Authentifizierungseinheit erhaltene Signal an das Türschloss als Steuersignal weiterzuleiten, wenn das von der Authentifizierungseinheit empfangene Signal als authentisches Signal erkannt worden ist. Dazu kann die Authentifizierungseinheit einen Codierer zum Codieren eines über die Datenverbindung übertragenen Signals und der Aktor einen Decoder zur Decodierung des über die Datenverbindung erhaltenen codierten Signals aufweisen. Die Codierung kann die Verwendung eines seriellen digitalen Telegramms für die Übertragung des Signals aufweisen, wobei das Telegramm frequenz- oder amplitudenmoduliert sein kann.

[0009] Die Datenverbindung kann eine Busleitung aufweisen, vorzugsweise einen CAN-Bus.

[0010] Der Aktor kann zur Ansteuerung des Türschlosses ein in den Aktor integriertes Relais aufweisen, das über eine Steuerleitung an das Türschloss angeschlossen ist. Nach der ordnungsgemäßen Übertragung eines Signals zur Freigabe des Türschlosses von der Authentifizierungseinheit über die Datenverbindung kann der Aktor das Relais ansteuern, um das Türschloss mit einer Spannung zu beaufschlagen, so dass das Türschloss von einer Verriegelungsstellung in eine Entriegelungsstellung überführt wird. Beispielsweise kann das Türschloss eine in die Schließstellung mechanisch vorgespannte Schließklinke aufweisen, die bei Strombeaufschlagung durch das Relais elektromechanisch aus der Verriegelungsposition in die Entriegelungsposition überführt wird.

[0011] Der TKS-SmartAktor bietet die Möglichkeit, ein mobiles Endgerät, etwa ein Mobiltelefon, als "Schlüssel" zu verwenden und so eine Authentifizierung für eine Zutrittsberechtigung zu ermöglichen, etwa mittels WLAN oder Bluetooth.

[0012] Mittels IP-Knoten kann der TKS-SmartAktor in ein Gebäudenetzwerk eingebunden werden. Über ein Projektierungstool können Datenpunkte direkt logisch über Server mit Aktoren verbunden werden und so "Szenarien" in der Gebäudeautomation (z.B. Außenbeleuchtung einschalten) ausgelöst oder Zustände an der Tür

als Nutzinformation zur Verfügung gestellt werden. Dies kann sowohl im lokalen Netzwerk als auch Standortübergreifend mittels Portalanbindung realisiert sein.

[0013] Der Aktor kann dazu eingerichtet sein, die direkte Einbindung in ein Alarmanlagensystem zu ermöglichen, wodurch eine Scharf-/Unscharfschaltung des Sicherheitssystems erreicht wird. Für die Personalisierung des Zugriffs kann der Aktor eine personalisierte Zugriffsmöglichkeit aufweisen. Dabei können unterschiedliche Administrations- und Anwenderebenen vorgesehen sein. Ist eine Rolle zugewiesen, können über eine Applikation beim Koppeln mit einem Aktor dem Anwender nur die Funktionen und einstellbaren Parameter angezeigt werden, auf die er auch tatsächlich Zugriff hat. Die Personalisierung umfasst z.B. das Hinzufügen von Infotexten oder Abwesenheitsnotizen (z.B. Notdienste von Apotheken) oder auch Bilder für die Ruftaste (Firmenlogo, Familienwappen usw.). Dazu kann eine Authentifizierungseinheit an der Tür ein Display, etwa ein Rufdisplay mit Touch-Eingabe aufweisen, welches auch Ruftasten mit Namenschildern darstellen kann.

[0014] Die Authentifizierungseinheit kann unmittelbar über die Datenverbindung mit dem Aktor verbunden sein. Es ist insbesondere nicht erforderlich, dass das Zutrittskontrollsystem ein weiteres Steuergerät aufweist, um beispielsweise das von der Authentifizierungseinheit empfangene Signal in ein Signal zur Ansteuerung des Aktors oder des Relais des Aktors umzuwandeln. Sämtliche Funktionalität kann in dem Aktor selbst implementiert sein. Dazu kann der Aktor als ein Smartaktor mit mindestens einem Prozessor und mindestens einem Speicher ausgebildet sein. Der Smartaktor kann weiterhin mindestens eine drahtgebundene Schnittstelle, etwa eine LAN-Schnittstelle, und/oder eine Funkschnittstelle, etwa eine WLAN-Schnittstelle, aufweisen.

[0015] Weiterhin kann vorgesehen sein, dass nur der Aktor eine externe elektrische Spannungsversorgung aufweist und zumindest die Authentifizierungseinheit und das Türschloss von dem Aktor mit elektrischer Spannung beaufschlagt sind. Vorzugsweise werden sämtliche eine elektrische Spannungsversorgung benötigenden Komponenten des Zutrittskontrollsystems von dem Aktor mit der jeweils benötigten elektrischen Spannung beaufschlagt. Dabei kann vorgesehen sein, dass die jeweils vorgesehenen Steuer- oder Busleitungen der Datenverbindung für die Signalübertragung zwischen dem Aktor und der jeweiligen Komponente des Zutrittskontrollsystems oder zusätzliche Leitungsadern der Steuer- oder Busleitungen für die Spannungsversorgung verwendet werden. Beispielsweise kann die Datenverbindung eine mehradrige Busleitung für die Signalübertragung aufweisen, von der mindestens eine Ader für die elektrische Spannungsversorgung dient. Demgemäß kann die Authentifizierungseinheit über eine Busleitung zwischen dem Aktor und der Authentifizierungseinheit, entlang welcher die Datenverbindung ausgebildet ist, von dem Aktor mit elektrischer Energie versorgt sein.

[0016] Der Aktor des Zutrittskontrollsystems kann mindestens eine und vorzugsweise sämtliche der folgenden Schnittstellen aufweisen:

a. einen ersten Leitungsanschluss für eine externe elektrische Spannungsversorgung,

b. einen zweiten Leitungsanschluss für eine Busleitung der Datenverbindung, und

c. einen dritten Leitungsanschluss für eine Steuerleitung des Türschlosses.

[0017] Weiterhin kann der Aktor eine weitere verschlüsselte oder unverschlüsselte Schnittstelle, beispielsweise eine IP-Schnittstelle, vorzugsweise eine Drahtlosschnittstelle, beispielsweise eine WLAN-Schnittstelle, für die Übertragung von Parametrierungsdaten an das Zutrittskontrollsystem aufweisen. Bei dem aus den Stand der Technik bekannten Zutrittskontrollsystemen war es bisher üblich, durch manuelle Eingabe an der Authentifizierungseinheit eine Parametrisierung des Systems vorzunehmen, was aufgrund der nur begrenzten Eingabemöglichkeiten beispielsweise bei einem Fingerprintsensor mit erheblichen Komplikationen verbunden war. Dadurch, dass der Aktor gemäß der zuvor beschriebenen Ausführungsform über eine IP-Schnittstelle verfügt, ist es nunmehr möglich, eine entsprechende Parametrisierung unter Verwendung des Aktors als Gateway zum Zutrittskontrollsystem vorzunehmen. Die Parametrierungsdaten können eine User-Nummer, beliebige User-Daten, mindestens eine Berechtigungszeit und weitere User-spezifische Daten aufweisen. Über die User-Nummer ist ein gezieltes Löschen eines Users, beispielsweise unter Verwendung eines Fingerprintsensors möglich. Die Verwaltung der Parametrierungsdaten kann über eine Applikation auf einem mobilen Endgerät erfolgen.

[0018] Die über die IP-Schnittstelle übertragene Parametrisierung kann beispielsweise in einem Speicher des Aktors oder innerhalb eines Speichers der Authentifizierungseinheit abgelegt werden. In diesem Fall kann der Aktor somit dazu eingerichtet sein, nach dem Empfangen einer Parametrisierung über die IP-Schnittstelle die Parametrisierung über die Datenverbindung an die Authentifizierungseinheit weiterzuleiten beziehungsweise auf den Speicher der Authentifizierungseinheit zuzugreifen, um die Parametrisierung in dem Speicher der Authentifizierungseinheit zu hinterlegen. Demgemäß kann der Aktor dazu eingerichtet sein, über die IP-Schnittstelle mindestens einen Parametrisierungsbefehl zu empfangen und entweder in dem Speicher des Aktors zu hinterlegen oder über die Datenverbindung an die Authentifizierungseinheit zu übertragen.

[0019] Wenn die IP-Schnittstelle eine Drahtlosschnittstelle ist, kann das Zutrittskontrollsystem weiterhin ein mobiles Endgerät, beispielsweise ein Smartphone oder einen Tablet-PC, aufweisen, das eine weitere Drahtlosschnittstelle aufweist, so dass eine Datenverbindung

zwischen dem Aktor und dem mobilen Endgerät hergestellt werden kann und der Aktor sowie das mobile Endgerät über die Drahtlosschnittstellen für die Übertragung einer Parametrisierung von dem mobilen Endgerät an den Aktor miteinander verbunden sind. Beispielsweise kann auf dem mobilen Endgerät eine Applikation vorinstalliert sein, welche die benutzerfreundliche Parametrisierung des Zutrittskontrollsystems erlaubt, indem aus einer Vielzahl möglicher Parametrisierungen des Zutrittskontrollsystems von einem Benutzer eine Auswahl getroffen werden kann. Die Applikation kann dabei dazu eingerichtet sein, nach erfolgter Auswahl durch den Benutzer einen entsprechenden Steuerbefehl über die zwischen den Drahtlosschnittstellen ausgebildete Datenverbindung an den Aktor zu übertragen, so dass der Aktor die Parametrisierung entweder in seinem eigenen Speicher hinterlegen oder über die Datenverbindung an die Authentifizierungseinheit übertragen kann.

[0020] Die Authentifizierungseinheit kann insbesondere außerhalb eines Gebäudes und/oder an einer Gebäudeaußenseite und der Aktor innerhalb des Gebäudes angeordnet sein, wobei eine Datenleitung, etwa eine Busleitung, entlang welcher die Datenverbindung ausgebildet ist, zwischen dem Aktor und der Authentifizierungseinheit durch eine Gebäudewand hindurchgeführt ist. Demgemäß kann der Aktor als zentrales Steuer- und Regelelement des Zutrittskontrollsystems im Inneren des Gebäudes vor unberechtigtem Zugriff gesichert angeordnet werden, während die Authentifizierungseinheit ausschließlich über die Datenverbindung mit dem Aktor kommunikativ in Verbindung steht. Dadurch wird ein besonders hohes Maß an Manipulationssicherheit des Zutrittskontrollsystems erreicht.

[0021] Um die möglichst platzsparende Integration des Zutrittskontrollsystems in die Gebäudeinfrastruktur zu ermöglichen, kann vorgesehen sein, dass der Aktor vollständig in einer Unterputzdose im Inneren des Gebäudes aufgenommen ist. Zum Beispiel kann es sich dabei um eine UP-Dose handeln, die über die im Gebäude vorgesehene Elektroinstallation mit einer Betriebsspannung versorgt ist, so dass durch Einbau des Aktors und Anschluss dieses an die Gebäudespannungsversorgung und gegebenenfalls unter Verwendung eines Netzteils oder sonstigen Spannungswandlers eine zuverlässige und platzsparende Energieversorgung des gesamten Zutrittskontrollsystems erreicht werden kann. Dies kann insbesondere dadurch noch weiter optimiert werden, dass, wie oben beschrieben, der Aktor als zentrales Bauelement für die Stromverteilung in dem Zutrittskontrollsystem dient, indem er sämtliche mit elektrischer Energie zu versorgenden Komponenten des Systems über die jeweils vorgesehene Verbindungsleitung mit dem Aktor mit elektrischer Energie versorgt.

[0022] Gemäß einem anderen Aspekt betrifft die Erfindung ein Verfahren für den Betrieb eines Zutrittskontrollsystems der zuvor beschriebenen Art, dass die Schritte aufweist:

a. Authentifizieren einer Zugangsberechtigung mit einer Authentifizierungseinheit des Zutrittskontrollsystems und Erzeugen eines Zugangsberechtigungssignals im Falle einer erfolgreichen Authentifizierung,
b. optional Herstellen einer Datenverbindung zwischen der Authentifizierungseinheit und einem Aktor des Zutrittskontrollsystems, falls die Datenverbindung noch nicht besteht,
c. Übertragen des Zugangsberechtigungssignals über die Datenverbindung an den Aktor, und
d. Erzeugen eines Steuersignal zur Ansteuerung eines Türschlosses des Zutrittskontrollsystems und Übertragen des Steuersignals an das Türschloss oder Übertragen des Zugangsberechtigungssignals unverändert als Steuersignal an das Türschloss, woraufhin das Türschloss von einer Verriegelungsposition in eine Freigabeposition überführt wird.

[0023] Das Verfahren kann weiterhin die folgenden Schritte aufweisen:

e. Empfangen mindestens eines Parametrisierungsbefehls über eine IP-Schnittstelle, vorzugsweise eine Drahtlosschnittstelle, des Aktors von einem mobilen Endgerät, beispielsweise von einem Smartphone oder einem Tablet-PC, und
f. Hinterlegen des Parametrisierungsbefehls in einem Speicher des Aktors oder Übertragen des Parametrisierungsbefehls über die Datenverbindung an die Authentifizierungseinheit, wobei der Parametrisierungsbefehl gegebenenfalls als modifizierter Parametrisierungsbefehl in dem Speicher hinterlegt oder an die Authentifizierungseinheit übertragen wird.

[0024] Wenn der Aktor eine IP-Schnittstelle, beispielsweise eine Funkschnittstelle, etwa eine WLAN-Schnittstelle, aufweist, kann er auch als Datengateway zum Beispiel für die Übertragung einer Parametrisierung und/oder eines Firmware-Updates der Authentifizierungseinheit und/oder des Aktors an das Zutrittskontrollsystem dienen. Analog zu der oben beschriebenen Parametrisierung kann die Übertragung des Firmware-Updates wiederum mit Hilfe eines mobilen Endgeräts erfolgen, auf dem eine entsprechende Applikation zur Übertragung des Firmware-Updates von dem mobilen Endgerät und über die Drahtlosschnittstelle an den Aktor vorgesehen ist. Demgemäß kann das Verfahren das Empfangen eine Firmware-Updates über die IP-Schnittstelle des Aktors, vorzugsweise eine Drahtlosschnittstelle des Aktors, und das Speichern des Firmware-Updates in einem Speicher des Aktors beziehungsweise das Übertragen des Firmware-Updates an die Authentifizierungseinheit aufweisen.

[0025] Weitere Einzelheiten der Erfindung werden anhand der nachstehenden Figuren erläutert. Dabei zeigt:

Figur 1 eine erste beispielhafte Ausführungsform eines erfindungsgemäßen Zutrittskontrollsystems in schematischer Darstellung;

Figur 2 eine zweite Ausführungsform eines erfindungsgemäßen Zutrittskontrollsystems in schematischer Darstellung; und

Figur 3 eine dritte Ausführungsform eines erfindungsgemäßen Zutrittskontrollsystems in schematischer Darstellung.

[0026] Das in Figur 1 gezeigte Zutrittskontrollsystem 1 weist eine außerhalb des Gebäudes 100 angeordnete Authentifizierungseinheit 2 auf, die in der Darstellung gemäß Figur 1 einmal beispielhaft als Nummernfeld 2.1 zur Eingabe eines Zahlencodes und einmal als Fingerprintsensor 2.2 ausgebildet ist. Bei realen Ausführungsformen wird häufig nur eine der beiden Ausführungsformen der Authentifizierungseinheit 2 wahlweise umgesetzt sein. Die Authentifizierungseinheit 2 kann beispielsweise an einer Außenwand 101 des Gebäudes 100 einer Eingangstür des Gebäudes 100 zugeordnet sein.

[0027] Im Inneren des Gebäudes 100 ist der Aktor 4 des Zutrittskontrollsystems 1 sicher vor dem Zugriff durch Unbefugte angeordnet. Der Aktor 4 kann beispielsweise bauliche Abmessungen aufweisen, die es erlauben, den Aktor 4 in einer Unterputzdose in einer Gebäudewand 101 aufzunehmen. Der Aktor 4 ist über eine sich durch die Gebäudewand 101 hindurch erstreckende Datenverbindung 3 mit der Authentifizierungseinheit 2 für den Datenaustausch verbunden. Da der Aktor 4 in der vorliegenden Ausführungsform als einziges Bauteil des Zutrittskontrollsystems 1 eine externe elektrische Spannungsversorgung 8 aufweist, dient die Datenverbindung 3 beziehungsweise die Busleitung 9 entlang welcher die Datenverbindung 3 ausgebildet ist, gleichfalls als Energieversorgungsleitung für die Authentifizierungseinheit 2. Demgemäß ist der Aktor 4 dazu eingerichtet, die Authentifizierungseinheit 2 mit elektrischer Spannung zu versorgen, so dass die Authentifizierungseinheit 2 keine eigene Spannungsversorgung benötigt.

[0028] Integriert in den Aktor 4 ist ein Relais 6, welches von dem Aktor dazu angesteuert werden kann, über eine Steuerleitung 7 ein Türschloss 5 mit Spannung zu versorgen, so dass das Türschloss 5 beispielsweise elektromagnetisch angetrieben aus einer Schließstellung, in welche das Türschloss 5 vorgespannt sein kann, in eine Freigabeposition überführt wird.

[0029] Der Aktor 4 kann einen Prozessor (nicht dargestellt) und einen Speicher 14 aufweisen, welche dazu eingerichtet sind, ein von der Authentifizierungseinheit 2 über die Datenverbindung 3 von dem Aktor 4 empfangenes Signal auszuwerten, beispielsweise um es zu entschlüsseln und im Falle einer erfolgreichen Entschlüsselung das Relais 6 zur Strombeaufschlagung des Türschlosses 5 anzusteuern. Der Aktor 4 weist einen ersten Leitungsanschluss 10 für die Stromversorgung 8, einen zweiten Leitungsanschluss 11 für die Busleitung 9 und einen dritten Leitungsanschluss 12 für die Steuerleitung 7 auf. Der Aktor 4 kann weitere Schnittstellen aufweisen, beispielsweise eine Drahtlosschnittstelle, um IP-basiert eine Parametrisierung des Zutrittskontrollsystems 1 oder die Übertragung eines Firmware-Updates auf den Aktor 4 zu ermöglichen.

[0030] In Abwandlung von der in Figur 1 gezeigten Ausführungsform weist die in Figur 2 gezeigte Ausführungsform gerade einen derartigen Aktor 4 mit einer IP-Schnittstelle 13 auf, die als eine Drahtlosschnittstelle und vorliegend als eine WLAN-Schnittstelle ausgebildet ist. Ein mobiles Endgerät 15 des Zutrittskontrollsystems 1 weist eine weitere IP-Schnittstelle auf, die ebenso als Drahtlosschnittstelle und insbesondere als WLAN-Schnittstelle ausgebildet sein kann. Das mobile Endgerät 15 und der Aktor 4 stehen über ihre Drahtlosschnittstellen 13, 16 mit einem Netzwerkrouter 17 für die Datenübertragung kommunikativ in Verbindung. Der Netzwerkrouter 17 kann beispielsweise eine Internetanbindung aufweisen, so dass auf Veranlassung einer auf dem mobilen Endgerät 15 installierten Applikation und infolge einer Eingabe eines Benutzers beispielsweise ein Firmware-Update über den Netzwerkrouter 17 bezogen und von dem mobilen Endgerät 15 oder unmittelbar von dem Router 17 an den Aktor 4 übertragen werden kann. Das mobile Endgerät 15 beziehungsweise die auf diesem installierte Applikation kann somit insbesondere auch dazu eingerichtet sein, den Netzwerkrouter 17 zu veranlassen, ein Firmware-Update oder ein sonstiges Datenpaket aus dem Netzwerk, beispielsweise aus dem Internet, zu beziehen und unmittelbar dem Aktor 4 über seine IP-Schnittstelle 13 zuzuleiten. Nachdem der Aktor 4 über seine Schnittstelle 13 das Datenpaket beziehungsweise das Firmware-Update von dem Netzwerkrouter 17 empfangen hat, kann das Datenpaket beziehungsweise das Firmware-Update auf einem Speicher 14 des Aktors 4 hinterlegt werden. Es kann auch vorgesehen sein, dass der Aktor 4 wiederum dazu eingerichtet ist, nach dem Empfangen des Datenpakets beziehungsweise des Firmware-Updates von dem Netzwerkrouter 17 das Datenpaket beziehungsweise das Firmware-Update über die Datenverbindung 3, insbesondere über die Busleitung 9, an die Authentifizierungseinheit 2 weiterzuleiten. Bei einer solchen Ausführungsform weist die Authentifizierungseinheit 2 zumindest einen Speicher und gegebenenfalls einen Prozessor für die Hinterlegung und Anwendung des Datenpakets beziehungsweise des Firmware-Updates auf. Analog zu der Übertragung eines Firmware-Updates kann auch die Übertragung einer Parametrisierung an die Authentifizierungseinheit 2 und/oder den Aktor 4 umgesetzt sein.

[0031] Der Netzwerkrouter 17 kann als Access-Point für das WLAN dienen und ermöglicht dem mobilen Endgerät 15 sich in das WLAN einzuwählen und eine Verbindung mit dem Aktor 4 herzustellen. Alternativ kann auch eine direkte Verbindung des mobilen Endgeräts 15 mit dem Aktor 4 möglich sein, indem sich letzterer als

Access-Point anbietet. Der Netzwerkrouter 17 wäre dann nicht erforderlich. Die WLAN-Verbindung zwischen Endgerät 15 und Aktor 4 kann in erster Linie der Parametrierung des Aktors 4 bzw. der Authentifizierungseinheit 2 dienen. Ein Firmware-Update kann in diesem Fall lediglich optional möglich sein. Dabei wird die Firmware über den Netzwerkrouter 17 aus dem Internet hochgeladen und wird auf dem mobilen Endgerät 15 vorgehalten.

[0032] Figur 3 zeigt den Einbau einer Authentifizierungseinheit 2 in einer Türstation eines Video-Türsprechsystems. Neben der Video-Übertragung ist auch eine Sprechverbindung möglich. Türstation und Wohnungsstation weisen dazu eine Sprecheinheit mit Lautsprecher und Mikrofon auf. Die Ausführungsform des Zutrittskontrollsystems 1 gemäß Figur 3 zeichnet sich insbesondere dadurch aus, dass das Zutrittskontrollsystem 1 weiterhin eine Videoübertragung aufweist. Dazu weist die Authentifizierungseinheit 2 ein Kameramodul auf und ist über eine 2-Draht-Busleitung 20 einerseits mit einer Wohnungsstation 18, die ein Display aufweist, verbunden und andererseits mit einem Video-Steuergerät 19. Wiederum ist ein Aktor 4 über eine Datenverbindung 3, die entlang einer Busleitung 9 ausgebildet ist, mit der Authentifizierungseinheit 2 verbunden. Der Aktor 4 weist wiederum eine IP-Schnittstelle 13 auf, die als Funkschnittstelle ausgebildet ist, über welche der Aktor 4 mit dem Netzwerkrouter 17 für den Datenaustausch in Verbindung steht. Ein mobiles Endgerät 15 steht ebenso über seine weitere Drahtlosschnittstelle 16 mit dem Router 17 für den Datenaustausch kommunikativ in Verbindung.

[0033] Die in Figur 3 gezeigte Ausführungsform unterscheidet sich insbesondere auch dadurch von den aus dem Stand der Technik bekannten Zutrittskontrollsystemen, dass wiederum in der wie bereits mit Bezug auf Figur 2 beschriebenen Weise unter Anwendung des mobilen Endgeräts 15 eine Parametrisierung und/oder eine Firmware-Aktualisierung erfolgen kann, ohne dass dazu ein Benutzer entsprechende Befehle über die Authentifizierungseinheit 2 mitunter umständlich eingeben muss. Das Video-Steuergerät 19 kann ein Netzteil aufweisen, welches das Video-Türsprechsystem (Kamera, Display, Tür und Wohnungsstation) mit elektrischer Energie versorgt. Der Türöffner 5 ist am Video-Steuergerät 19 und nicht am Aktor 4 angeschlossen. Das Video-Steuergerät 19 kann in diesem Fall ebenfalls ein Relais aufweisen, womit die Türöffnung auch von einer Wohnungsstation aus erfolgen kann. Alternativ ist die Nutzung des Relais im Aktor zu dem genannten Zweck möglich. Die in Figur 3 gezeigte Ausführungsform kann insbesondere auch eine Nachrüstlösung für bekannte Zutrittskontrollsysteme darstellen.

[0034] Die in der vorstehenden Beschreibung, in den Zeichnungen sowie in den Ansprüchen offenbarten Merkmale der Erfindung können sowohl einzeln als auch in beliebiger Kombination für die Verwirklichung der Erfindung wesentlich sein.

Bezugszeichenliste:

[0035]

1	Zutrittskontrollsystem
2	Authentifizierungseinheit
2.1	Nummernfeld
2.2	Fingerprintsensor
2.3	Mikrofon/Lautsprecher
2.4	Kamera
3	Datenverbindung
4	Aktor
5	Türschloss
6	Relais
7	Steuerleitung
8	Spannungsversorgung
9	Busleitung
10	erster Leitungsanschluss
11	zweiter Leitungsanschluss
12	dritter Leitungsanschluss
13	IP-Schnittstelle
14	Speicher
15	mobiles Endgerät
16	Drahtlosschnittstelle
17	Netzwerkrouter
18	Wohnungsstation
19	Video-Steuergerät
20	2-Draht-Busleitung
100	Gebäude
101	Gebäudewand

Patentansprüche

1. Zutrittskontrollsystem (1) für ein Gebäude (100), mit einer Authentifizierungseinheit (2), die über eine Datenverbindung (3) mit einem Aktor (4) zum Ansteuern eines Türschlosses (5) verbunden ist, wobei die Authentifizierungseinheit (2) dazu eingerichtet ist, im Falle einer erfolgreichen Authentifizierung ein Zugangsberechtigungssignal über die Datenverbindung (3) an den Aktor (4) zu übertragen, und wobei der Aktor (4) dazu eingerichtet ist, aus dem Zugangsberechtigungssignal ein Steuersignal zur Ansteuerung eines Türschlosses (5) des Zutrittskontrollsystems (1) zu erzeugen und an das Türschloss (5) zu übertragen oder das Zugangsberechtigungssignal unverändert als das Steuersignal an das Türschloss (5) zu übertragen.

2. Zutrittskontrollsystem (1) nach Anspruch 1, bei dem die Datenverbindung (3) eine Datenleitung, beispielsweise eine Busleitung (9), vorzugsweise einen CAN-Bus, aufweist.

3. Zutrittskontrollsystem (1) nach Anspruch 1 oder 2, bei dem der Aktor (4) zur Ansteuerung des Türschlosses (5) ein in den Aktor (4) integriertes Relais

(6) aufweist, das über eine Steuerleitung (7) an das Türschloss (5) angeschlossen ist.

4. Zutrittskontrollsystem (1) nach einem der vorangegangenen Ansprüche, bei dem die Authentifizierungseinheit (2) unmittelbar über die Datenverbindung (3) mit dem Aktor (4) verbunden ist.

5. Zutrittskontrollsystem (1) nach einem der vorangegangenen Ansprüche, bei dem nur der Aktor (4) eine externe elektrische Spannungsversorgung (8) aufweist und zumindest die Authentifizierungseinheit (2) und das Türschloss (5) von dem Aktor (4) mit elektrischer Spannung beaufschlagt sind.

6. Zutrittskontrollsystem (1) nach einem der vorangegangenen Ansprüche, bei dem die Authentifizierungseinheit (2) über eine Busleitung (9) zwischen dem Aktor (4) und der Authentifizierungseinheit (2), entlang welcher die Datenverbindung (3) ausgebildet ist, von dem Aktor (4) mit elektrischer Energie versorgt ist.

7. Zutrittskontrollsystem (1) nach einem der vorangegangenen Ansprüche, bei dem der Aktor (4) zumindest die folgenden Schnittstellen Aufweist:

a. einen ersten Leitungsanschluss (10) für eine externe elektrische Spannungsversorgung (8),
b. einen zweiten Leitungsanschluss (11) für eine Busleitung (9) der Datenverbindung (3), und
c. einen dritten Leitungsanschluss (12) für eine Steuerleitung (7) des Türschlosses (5).

8. Zutrittskontrollsystem (1) nach einem der vorangegangenen Ansprüche, bei dem der Aktor (4) eine IP-Schnittstelle (13), vorzugsweise eine Drahtlosschnittstelle, für die Übertragung einer Parametrisierung an das Zutrittskontrollsystem (1) aufweist.

9. Zutrittskontrollsystem (1) nach Anspruch 8, bei dem der Aktor (4) dazu eingerichtet ist, über die IP-Schnittstelle (13) mindestens einen Parametrisierungsbefehl zu empfangen und entweder in einem Speicher (14) des Aktors (4) zu hinterlegen oder über die Datenverbindung (3) an die Authentifizierungseinheit (2) zu übertragen.

10. Zutrittskontrollsystem (1) nach Anspruch 7 oder 8, bei dem die IP-Schnittstelle (13) eine Drahtlosschnittstelle ist und das Zutrittskontrollsystem (1) ein mobiles Endgerät (15), beispielsweise ein Smartphone oder ein Tablet-PC, aufweist, das eine weitere Drahtlosschnittstelle (16) aufweist, und wobei der Aktor (4) und das mobile Endgerät (15) über die Drahtlosschnittstellen (13, 16) für die Übertragung einer Parametrisierung von dem mobilen Endgerät (15) an den Aktor (4) miteinander verbunden sind.

11. Gebäude (100) mit einem Zutrittskontrollsystem (1) nach einem der vorangegangenen Ansprüche, bei dem die Authentifizierungseinheit (2) außerhalb des Gebäudes (100) und/oder an einer Gebäudeaußenseite und der Aktor (4) innerhalb des Gebäudes (100) angeordnet ist, wobei eine Busleitung (9), entlang welcher die Datenverbindung (3) ausgebildet ist, zwischen dem Aktor (4) und der Authentifizierungseinheit (2) durch eine Gebäudewand (101) hindurch geführt ist.

12. Gebäude (100) nach Anspruch 11, bei dem der Aktor (4) vollständig in einer Unterputzdose im Innern des Gebäudes (100) aufgenommen ist.

13. Verfahren für den Betreib eines Zutrittskontrollsystem (1) nach einem der vorangegangen Ansprüche, das die Schritte aufweist:

a. Authentifizieren einer Zugangsberechtigung mit einer Authentifizierungseinheit (2) des Zutrittskontrollsystems (1) und Erzeugen eines Zugangsberechtigungssignals im Falle einer erfolgreichen Authentifizierung,
b. optional Herstellen einer Datenverbindung zwischen der Authentifizierungseinheit (2) und einem Aktor (4) des Zutrittskontrollsystems (1),
c. Übertragen des Zugangsberechtigungssignals über die Datenverbindung an den Aktor (4), und
d. Erzeugen eines Steuersignal zur Ansteuerung eines Türschlosses (5) des Zutrittskontrollsystems (1) und Übertragen des Steuersignals an das Türschloss (5) oder Übertragen des Zugangsberechtigungssignals unverändert als Steuersignal an das Türschloss, woraufhin das Türschloss (5) von einer Verriegelungsposition in eine Freigabeposition überführt wird.

14. Verfahren nach Anspruch 13, das weiterhin die folgenden Schritte aufweist:

e. Empfangen mindestens eines Parametrisierungsbefehls über eine IP-Schnittstelle (13), vorzugsweise eine Drahtlosschnittstelle, des Aktors (4) von einem mobilen Endgerät (15), beispielsweise von einem Smartphone oder einem Tablet-PC, und
f. Hinterlegen des Parametrisierungsbefehls in einem Speicher (14) des Aktors (4) oder Übertragen des Parametrisierungsbefehls über die Datenverbindung an die Authentifizierungseinheit (2), wobei der Parametrisierungsbefehl gegebenenfalls als modifizierter Parametrisierungsbefehl in dem Speicher (14) hinterlegt oder an die Authentifizierungseinheit (2) übertragen wird.

15. Verfahren nach Anspruch 13 oder 14 das weiterhin das Empfangen eines Firmware-Updates über eine IP-Schnittstelle, vorzugsweise eine Drahtlosschnittstelle, des Aktors (4) und das Speichern des Firmware-Updates in einem Speicher (14) des Aktors (4) oder das Übertragen des Firmware-Updates an die Authentifizierungseinheit (2) aufweist.

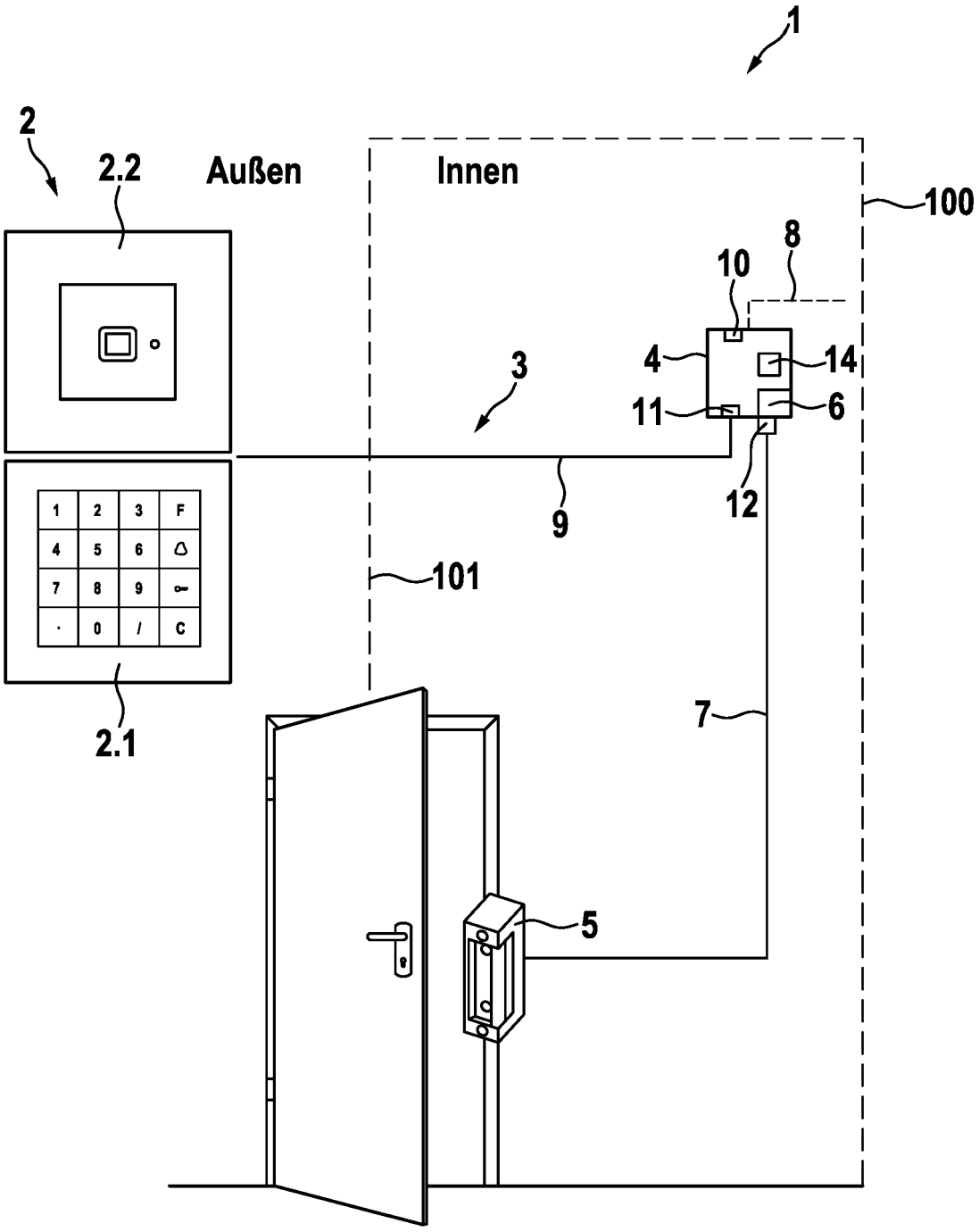

Fig. 1

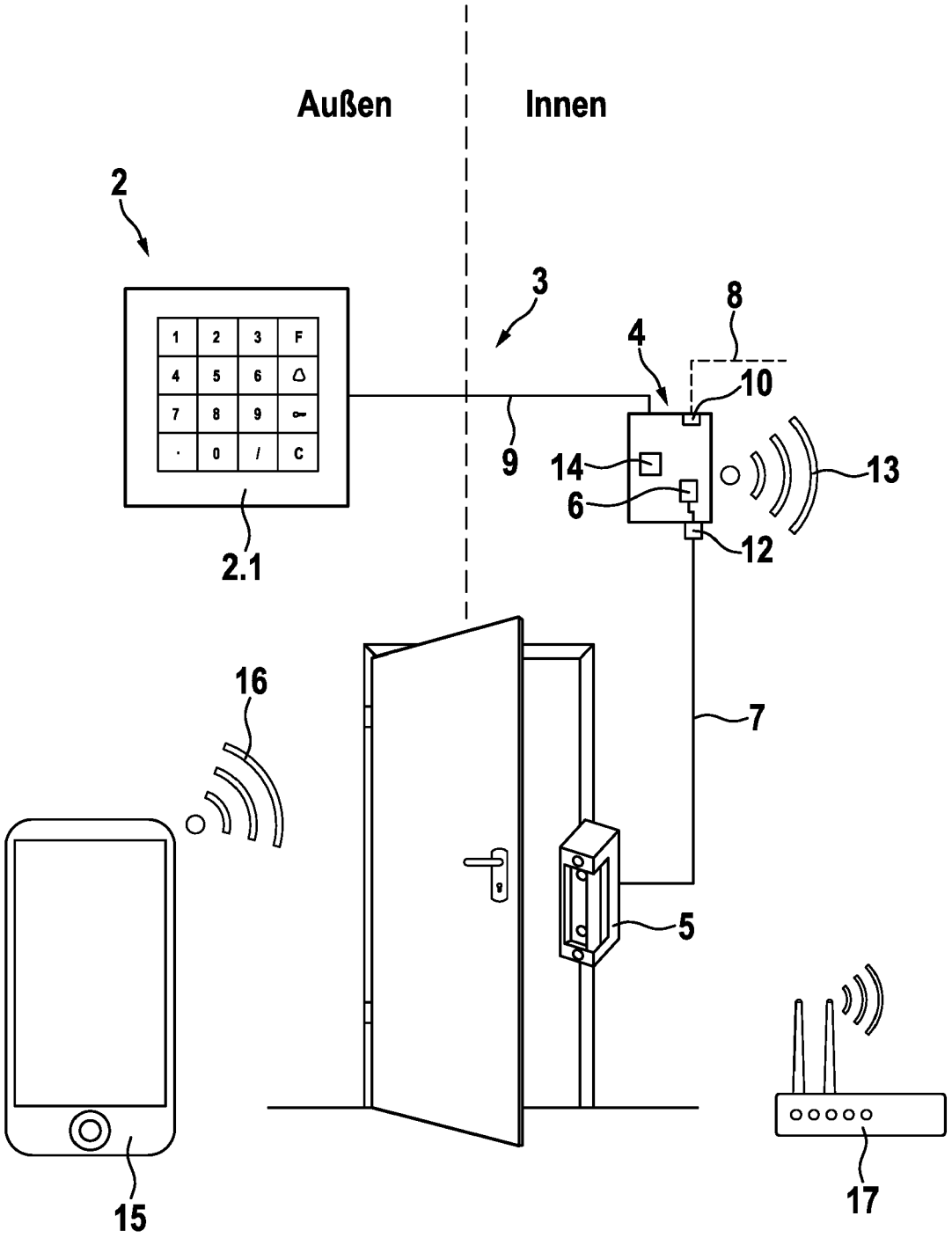

Fig. 2

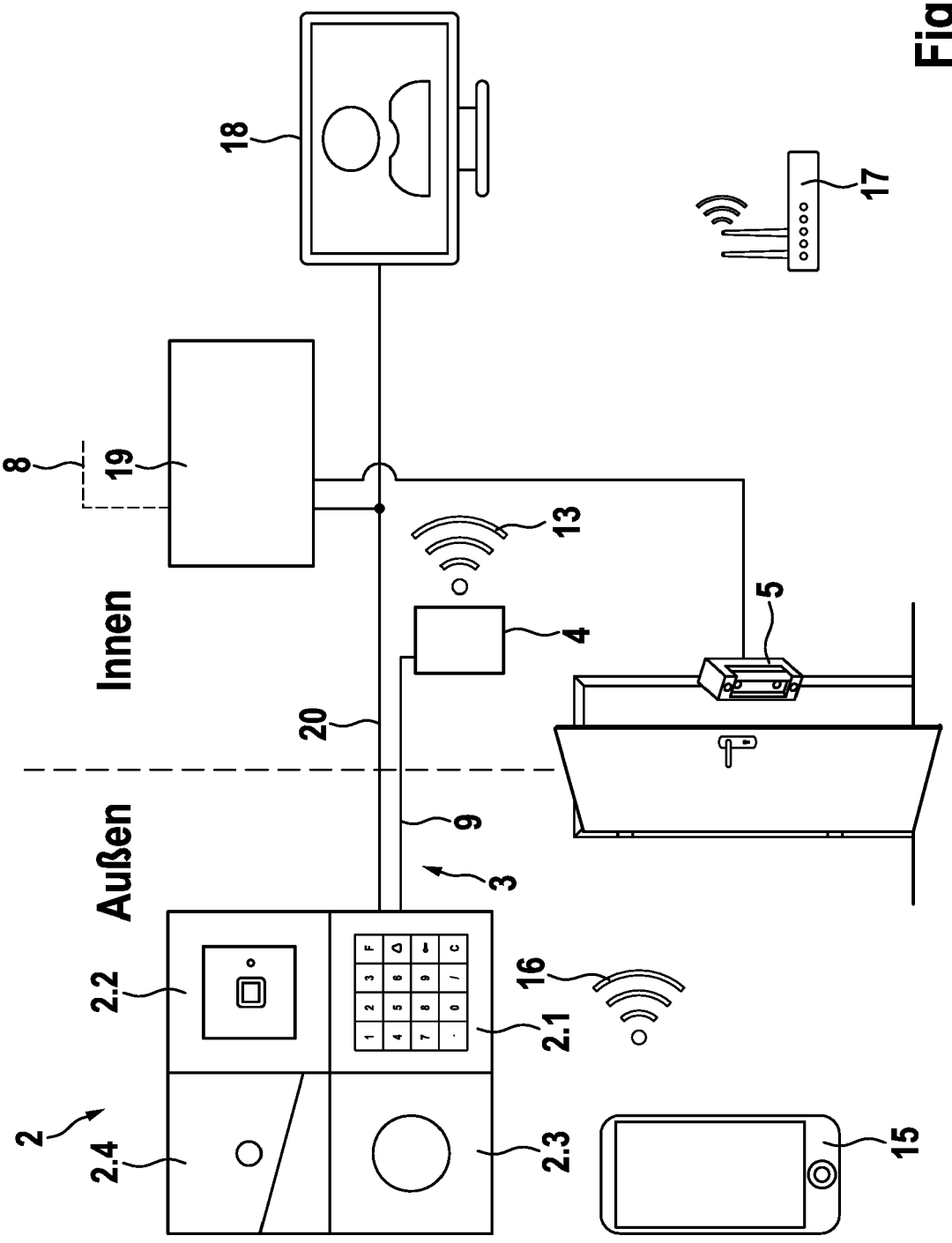

Fig. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 19 20 5968

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	US 2013/305353 A1 (MCMILLAN RYAN [CA] ET AL) 14. November 2013 (2013-11-14) * Absatz [0003] - Absatz [0004] * * Absatz [0014] - Absatz [0018] * * Absatz [0022] * * Absatz [0025] - Absatz [0028] * * Abbildungen 1,2 *	1-15	INV. G07C9/00
X	EP 3 096 299 A1 (FUHR CARL GMBH & CO KG [DE]) 23. November 2016 (2016-11-23) * Abbildungen 1-3 * * Absatz [0001] - Absatz [0003] * * Absatz [0008] * * Absatz [0020] - Absatz [0030] *	1-15	
X	US 5 848 541 A (GLICK MARK [US] ET AL) 15. Dezember 1998 (1998-12-15) * Abbildungen 1,2 * * Spalte 8, Zeile 50 - Spalte 9, Zeile 2 * * Spalte 9, Zeile 17 - Zeile 26 * * Spalte 10, Zeile 27 - Spalte 11, Zeile 56 * * Spalte 15, Zeile 13 - Zeile 19 * * Spalte 21, Zeile 38 - Zeile 65 * * Spalte 25, Zeile 63 - Spalte 26, Zeile 2 *	1-7,11, 13	RECHERCHIERTE SACHGEBIETE (IPC) G07C
A	US 2018/137704 A1 (CATERINO MARK ANTHONY [US] ET AL) 17. Mai 2018 (2018-05-17) * Absatz [0009] * * Absatz [0039] - Absatz [0043] * * Absatz [0050] *	8-10,14, 15	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	7. April 2020	Mechenbier, Bernd

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 19 20 5968

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.

07-04-2020

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2013305353 A1	14-11-2013	KEINE	
EP 3096299 A1	23-11-2016	DE 102015108026 A1	24-11-2016
		EP 3096299 A1	23-11-2016
US 5848541 A	15-12-1998	US 5823027 A	20-10-1998
		US 5848541 A	15-12-1998
US 2018137704 A1	17-05-2018	CN 107667369 A	06-02-2018
		EP 3298593 A1	28-03-2018
		US 2018137704 A1	17-05-2018
		WO 2016185008 A1	24-11-2016
		WO 2016185013 A1	24-11-2016
		WO 2016185283 A1	24-11-2016

EPO FORM P0461

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

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- EP 2584539 B1 **[0003]**
- DE 202014103128 U1 **[0003]**