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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
31. August 2017 (31.08.2017)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2017/144649 A1

(51) Internationale Patentklassifikation:
G07C 9/00 (2006.01) *H04W 12/12* (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2017/054298

(22) Internationales Anmeldedatum:
24. Februar 2017 (24.02.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2016 103 366.9
25. Februar 2016 (25.02.2016) DE

(71) Anmelder: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Straße 17, 42551 Velbert (DE).

(72) Erfinder: **GENNERMANN, Sven**; Zum Waschenberg 56, 42551 Velbert (DE).

(74) Anwalt: **ZENZ PATENTANWÄLTE PARTNERSCHAFT MBB**; Rüttenscheider Straße 2, 45128 Essen (DE).

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

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

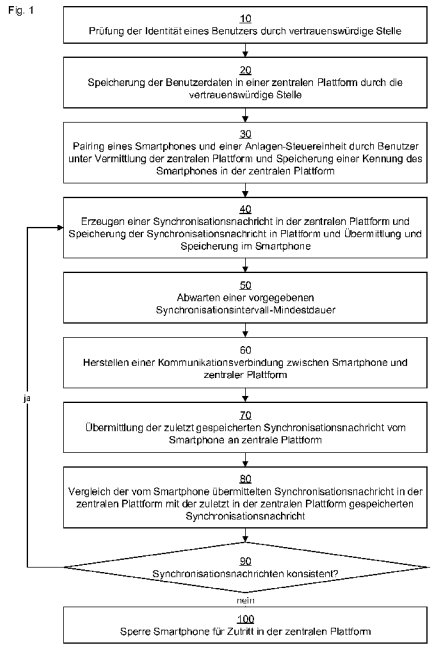
Veröffentlicht:

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

(54) Title: SAFEGUARDING OF ENTRY AUTHORISATIONS FOR FIXED-LOCATION INSTALLATIONS

(54) Bezeichnung : SICHERUNG VON ZUTRITTSBERECHTIGUNGEN ZU ORTSFESTEN ANLAGEN

Fig. 1



10 The identity of a user is checked by trustworthy centre
20 The user data are stored in a central platform by the trustworthy centre
30 A smartphone and an installation control unit are paired by user by means of the central platform, and an identifier of the smartphone is stored in the central platform
40 A synchronisation message is generated in the central platform, and the synchronisation message is stored in the platform and transmitted and stored in the smartphone
50 A prescribed synchronisation interval minimum period is awaited
60 A communication link is set up between smartphone and central platform
70 The most recently stored synchronisation message is transmitted from the smartphone to the central platform
80 The synchronisation message transmitted by the smartphone is compared in the central platform with the synchronisation message most recently stored in the central platform
90 Synchronisation messages consistent?
100 Smartphone blocked from entry in the central platform
ja = yes
nein = no

(57) Abstract: A method for safeguarding entry systems for buildings. A mobile communication device is set up as an access key for the building. To protect against illegal duplication of the communication device, it is repeatedly connected to a remote control device. This involves individual synchronisation data being generated that are stored in the mobile communication device and the remote control device. For each connection between communication device and control device, old synchronisation data from a preceding connection are transmitted from the communication device to the remote control device. There, a consistency check takes place between the old synchronisation data received from the communication device and the old synchronisation data stored in the remote control device. If the data, new synchronisation data are generated and stored. If the data are inconsistent, the communication device is blocked from further access to the building.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2017/144649 A1

Ein Verfahren zum Absichern von Zutriffssystemen für Gebäude. Ein mobiles Kommunikationsgerät ist als Zugangsschlüssel für 10 das Gebäude eingerichtet. Zum Schutz vor einer unerlaubten Vervielfältigung des Kommunikationsgeräts wird es wiederholt mit einer entfernten Steuereinrichtung verbunden. Dabei werden individuelle Synchronisierungsdaten erzeugt, die in dem mobilen Kommunikationsgerät und der entfernten Steuereinrichtung gespeichert werden. Bei jeder Verbindungen zwischen Kommunikationsgerät und Steuereinrichtung werden Alt-Synchronisierungsdaten aus einer vorangehenden Verbindung vom Kommunikationsgerät an die entfernte Steuereinrichtung übermittelt. Dort erfolgt eine Konsistenzprüfung zwischen den vom Kommunikationsgerät empfangenen Alt-Synchronisierungsdaten und den in der entfernten Steuereinrichtung gespeicherten Alt-Synchronisierungsdaten. Wenn die Daten werden neue Synchronisationsdaten erzeugt und gespeichert. Falls die Daten inkonsistent sind, wird das Kommunikationsgerät für den weiteren Zugang zum Gebäude gesperrt.

Sicherung von Zutrittsberechtigungen zu ortsfesten Anlagen

Die Erfindung betrifft ein Verfahren zur Sicherung von Zutrittsverfahren. Insbesondere betrifft die Erfindung den Bereich der Zutritte zu ortfesten Anlagen, wie Gebäuden oder zugangsbeschränkten Geländen.

Eine Berechtigung für den Zutritt zu ortsfesten Anlagen wurde bislang oft über eine Schlüsselkomponente, beispielsweise einen Funkschlüssel oder sogenannten ID-Geber, z.B. eine Chipkarte geprüft. Derjenige Benutzer, der den Schlüssel bei sich trägt, ist autorisiert, sich Zutritt zu einem gesicherten Bereich, insbesondere einem Gebäude oder Gelände zu verschaffen. Dabei sind auch Systeme bekannt, die drahtlos wirken und auch solche, die gar keinen aktiven Entsperr- oder Autorisierungsvorgang erfordern, sogenannte Keyless-Entry-Systeme.

Es ist außerdem bekannt, dass nach einem Registrierungsvorgang der Zutritt zu ortsfeste Anlagen mit einer Schlüsselkarte oder auch einem registrierten Mobiltelefon erfolgen kann. Hinsichtlich der Zutrittsmöglichkeiten zu ortsfesten Anlagen über Mobilgeräte bestehen allerdings Vorbehalte hinsichtlich der Sicherheit solcher Konzepte.

Es gibt dabei verschiedene Ansätze, die Berechtigungsinformationen zum Zutritt zu einer Anlage in ein mobiles Kommunikationsgerät (beispielsweise ein Smartphone) zu verlagern. Der Eigentümer oder Manager eines Gebäudes oder Geländes kann einem Benutzer Rechte einräumen, diese Rechte werden mit einer entsprechenden Applikation und Daten auf einem dem Benutzer zugeordneten mobilen Kommunikationsgerät abrufbar hinterlegt. In einem grundlegenden Konzept verfügt dann eine ortsfeste Anlage über eine Steuereinrichtung, die in Kommunikation mit dem mobilen Kommunikationsgerät tritt (beispielsweise über eine Bluetooth- oder NFC-Verbindung). Diese Steuereinrichtung hat dazu eine Schnittstelle im Zugriffsbereich des Benutzers, z.B. am Eingang zu einem Gebäude oder Gelände.

Bei Zutritt wird die gespeicherte Legitimation geprüft und in Abhängigkeit davon wird Zutritt gewährt.

In fortgeschrittenen Systemen kommunizieren sowohl eine Steuereinheit in der ortsfesten Anlage als auch das mobile Kommunikationsgerät mit einer zentralen und gesicherten Plattform, die beispielsweise ein Dienstprovider oder ein Verwalter des Zutrittssystems vorhält. Durch diese Vermittlungsposition kann eine höhere Sicherheitsstufe gewährleistet werden.

Es kann außerdem vorgesehen sein, dass der Benutzer eines mobilen Kommunikationsgerät sich gegenüber diesem mobilen Kommunikationsgerät mittels einer Kennung (kognitiv memorierten Daten) oder biometrischer Daten identifizieren muss, bevor er Zugriff auf die im mobilen Kommunikationsgerät gespeicherten Daten und damit zu einer Anlage erhält.

Die vorgenannten Konzepte bieten zwar bezüglich üblicher Angriffe eine robuste Sicherheit, es ist jedoch erstrebenswert, die Sicherheit weiter zu verbessern. So bieten beispielsweise Systeme noch keine umfassende Sicherheit im Falle des Klonens eines Mobilgerätes (Smartphones) durch einen böswilligen Dritten. Es ist grundsätzlich (mit erheblichem Aufwand) möglich, eine exakte Kopie eines Mobilgerätes, insbesondere eines Smartphones anzulegen. Dafür kann zum Beispiel identische Hardware verwendet werden, auf welche ein Software-Systemabbild des geklonten Mobilgerätes aufgespielt wird. Die in der Hardware selbst gespeicherten Kennungen, die grundsätzlich nicht manipulierbar sind da sie hardwareseitig gespeichert sind, können über einen Software-Layer, zum Beispiel unterhalb der Betriebssystemebene abgefangen und manipuliert werden, so dass auch eine identische Hardware sowohl dem Betriebssystem als auch verbundenen Dritten vorgespielt wird. Die Absicherung eines solchen Vorgangs ist in den bisherigen Konzepten noch nicht realisiert.

Aufgabe der Erfindung ist es, eine zusätzliche Sicherheit bei Autorisierungsvorgängen zum Zutritt zu ortsfesten Anlagen bereitzustellen.

Die Aufgabe wird erfindungsgemäß gelöst durch ein Verfahren mit den Merkmalen des Patentanspruchs 1.

Gemäß der Erfindung wird ein mobiles Kommunikationsgerät, insbesondere ein Smartphone mit einer darauf laufenden Applikation verwendet, um den Zutritt zu ortsfesten Anlagen zu managen. Ein derart ausgestattetes Smartphone ist dazu vorbereitet, sowohl mit einer zentralen Plattform zu kommunizieren als auch mit einer Sicherheitseinrichtung an einer Anlage, z.B. einem Gebäude. Es ist jedoch auch möglich, dass nur eine Anlagen-Steuereinheit und das mobile Kommunikationsgerät ohne zentrale Plattform eingesetzt werden. Das mobile Kommunikationsgerät enthält in jedem Fall Daten, die bei Übermittlung an eine gekoppelte Sicherheitseinrichtung (z.B. Türzugangssystem) eine Legitimation des Besitzers des mobilen Kommunikationsgerätes bewirken. Das mobile Kommunikationsgerät ist also als Schlüssel für ein Zutrittssystem der ortsfesten Einrichtung ausgebildet.

Wesentlich ist, dass gemäß der Erfindung das mobile Kommunikationsgerät und die darauf laufende Applikation so ausgebildet sind, dass das mobile Kommunikationsgerät wiederholt Kontakt zu einer entfernten Stelle, z.B. der zentralen Plattform oder auch der Anlagen-Steuereinheit aufnimmt. Die Zeitabstände dieser Kontaktaufnahmen können in einem gewissen Bereich zufällig variiert werden oder auch auf eine feste Periodendauer vorgegeben werden. Beispielsweise können Zeitabstände der Kontaktaufnahmen von 10 Minuten oder 60 Minuten oder auch mehreren Stunden vorgesehen sein.

Diese Kontaktaufnahmen erfordern keine Benutzereinwirkung, die beteiligten Geräte erledigen die Kontaktaufnahmen und Abwicklung autonom.

Bei jeder Kontaktaufnahme werden sowohl im mobilen Kommunikationsgerät als auch bei entfernten Stellen charakteristische und eindeutige Daten für die jeweilige Kontaktaufnahme gespeichert. Beispielsweise können die charakteristischen Daten in einem Zeitstempel bestehen, welcher die Kontaktaufnahme dokumentiert. Alternativ kann zu dem Mobilgerät von der entfernten Stelle ein kleines Datenpaket mit

zufällig generiertem Inhalt übermittelt werden. Außerdem wird erfindungsgemäß bei jeder Kontaktaufnahme überprüft, ob die Daten einer vorangehenden Kontaktaufnahme, beispielsweise der unmittelbar vorangehenden Kontaktaufnahme, beidseitig konsistent sind. Es wird also bei jeder Kontaktaufnahme beispielsweise festgestellt, ob auf beiden Seiten der identische Zeitstempel oder Datensatz der vorangehenden Kontaktaufnahme vorhanden ist. Dazu übermittelt das Mobilgerät bei jeder Kontaktaufnahme das in der vorangehenden Kontaktaufnahme übermittelte Datenpaket zurück an die entfernte Stelle, die dort einen Vergleich mit dem vorangehend übermittelten Datenpaket durchführt.

Wird bei dieser Kontrolle eine Inkonsistenz festgestellt, so kann darauf reagiert werden, indem der Zutritt für dieses mobile Kommunikationsgerät gesperrt wird. Dazu wird eine Sperrung in der entfernten Stelle veranlasst, also in der zentralen Plattform und/oder unmittelbar in der Steuereinheit der ortsfesten Anlage.

Ein wesentliches Merkmal der Erfindung besteht also darin, in vorgegebenen zeitlichen Abständen eine Auffrischung und Synchronisation von Daten zwischen dem mobilem Kommunikationsgerät und der Anlagen-Steuereinheit oder zwischen Mobilgerät und der zentralen Steuerplattform vorzusehen und automatisiert abzuwickeln. Dies schützt davor, dass ein geklontes Mobilgerät unter Vorspielen einer falschen Identität betrieben werden kann. Der wiederholte Synchronisationsvorgang kann problemlos durch eine Applikation auf dem Mobilgerät initiiert werden. Das Synchronisationsintervall kann und sollte in gewissen Grenzen zufällig variiert werden, um eine Systematik und Berechenbarkeit der Kontaktaufnahmen zu reduzieren.

Greifen beispielswiese zwei Geräte, ein legitimes und ein unberechtigter Geräteklon, gemäß diesem erfindungsgemäßen Synchronisierungsvorgang auf die entfernte Stelle, z.B. die zentrale Plattform zu, so sind die Daten nicht konsistent, da bei jeder Kontaktaufnahme eine neue Synchronisierungsinformation auf beiden Seiten hinterlegt wird. Beim ersten Zugriff eines anderen Gerätes würde festgestellt, dass die Synchronisierungsdaten des vorangehenden Kontaktes nicht

konsistent sind und eine Sperrung des Zutrittes kann veranlasst werden.

Wird ein geklontes Mobilgerät erst nach dem Kopiervorgang und mit erheblicher Zeitverzögerung, also einer Zeitverzögerung die größer als die Abstände der Synchronisation sind, in Betrieb genommen, dann hat inzwischen bereits das Originalgerät neue Synchronisierungsinformationen empfangen und an der entfernten Stelle sind ebenfalls die Synchronisierungsinformation aktualisiert worden.

Beim ersten Synchronisierungsversuch des illegalen Klons würde festgestellt, dass die Synchronisierungsinformationen nicht übereinstimmen und der Zutritt würde gesperrt.

Erfindungsgemäß erfolgt ein Vorgang der wiederholten Sicherheitssynchronisierung zwischen dem Mobilgerät und einer entfernten Stelle und Speicherung von für den jeweiligen Synchronisationsvorgang charakteristischen und eindeutigen Daten. Bei jedem nachfolgenden Synchronisierungsvorgang werden die Daten aus einem vorangehenden, vorzugsweise dem unmittelbar vorangehenden Synchronisierungsvorgang abgeglichen und ein Zutritt wird unterbunden, wenn die abgeglichenen Daten nicht konsistent sind.

Es ist im Rahmen der Erfindung sinnvoll, wenn jeder Synchronisierungsvorgang derart quittiert wird, dass nach einer Übermittlung der Daten eine Kontrolle der gerade übermittelten Daten stattfindet, um eine fehlerhafte Übermittlung und Speicherung auszuschließen. Vorzugsweise wird daher bei jeder Synchronisierung und Übermittlung neuer Synchronisierungsdaten eine wechselseitige Überprüfung der übermittelten und gespeicherten Daten stattfinden. Wird als charakteristische Information beispielsweise ein Zeitstempel verwendet ist es außerdem wichtig, dass die zeitliche Synchronisation der Geräte sichergestellt ist. Einfacher zu realisieren ist es, wenn die vom Mobilgerät entfernte Stelle als Master der Synchronisation ein Datenpaket (beispielsweise den Zeitstempel) an das Mobilgerät übermittelt und dieses Mobilgerät diese Daten als charakteristische Daten der Kontaktaufnahme speichert. In einer nachfolgenden Kommunikation werden diese Daten zurückgeschickt,

an der entfernten Stelle geprüft und bei erfolgreicher Prüfung wird ein neues Datenpaket an das Mobilgerät zurückgesendet.

Da die Daten regelmäßig erneuert werden und nicht nach einem Algorithmus auf dem Mobiltelefon erzeugt werden, entzieht sich eine solche Maßnahme dem illegalen Klon eines Mobilgerätes. Es würde erkannt, wenn mehrere Geräte mit vorgetäuschter Identität auf dieselbe entfernte Stelle zugreifen würden.

Vorzugsweise wird die Erfindung in einem System eingesetzt, wo eine zentrale Rechteverwaltungsstelle die Zutrittsrechte zwischen Mobilgeräten und ortsfesten Anlagen koordiniert. Bei solchen Systemen verifiziert beispielsweise die zentrale Stelle die Identität eines Benutzers. Es ist bei derartigen Systemen oft vorgesehen, dass eine vertrauenswürdige Stelle, zum Beispiel der Verwalter der Anlage, die Eintragung in der zentralen Datenbank vornimmt und von diesen zentralen Eintragungen sowohl die Anlagen-Steuereinheit selbst als auch das mobile Kommunikationsgerät abhängig sind. In einem solchen Fall würde die Synchronisierung vorzugsweise zwischen mobilem Kommunikationsgerät und der zentralen Stelle stattfinden, wobei das mobile Kommunikationsgerät und die zentrale Stelle über eine drahtlose Datenleitung verbindbar sind. Da jedes Synchronisierungsereignis nur sehr kleine Datenmengen austauscht, ist ein solches System ohne wesentliche Belastung des Datenverkehrs oder des Betriebs des Mobilgerätes möglich. Die Art des Datenaustausches ist weitgehend beliebig, es kann sich beispielsweise um Datennachrichten über ein Datennetzwerk handeln, beispielsweise Aufrufe von gesicherten Internetseiten oder ein Datenaustausch über proprietäre Protokolle.

Sobald die zentrale Plattform feststellt, dass übermittelte Synchronisierungsinformationen nicht konsistent sind, sperrt sie die entsprechenden Privilegien des zugeordneten mobilen Kommunikationsgeräts und teilt dies einer Anlagen-Steuereinheit mit, die ebenfalls in Kontakt der zentralen Plattform steht.

Die Sperrung eines solchen Systems wird dem Benutzer in geeigneter Weise mitgeteilt, beispielsweise durch einen Anruf oder Zusendung einer entsprechenden Mitteilung. Es besteht danach die Möglichkeit, die Sperrung durch Nachweis einer

geeigneten Legitimation oder Anmeldung eines anderen mobilen Kommunikationsgerätes aufzuheben.

Auch wenn ein Benutzer veranlasst wird sein mobiles Kommunikationsgerät zurückzusetzen oder eine ältere Sicherung des Mobilgerätes wieder aufzuspielen, kann ein solcher Vorgang erforderlich sein, da dann auch die gespeicherten Synchronisierungsinformationen verloren sind.

Auch für den Fall, dass zum Zeitpunkt des Zugangs am Ort de Anlagen-Steuereinheit keine Verbindung zwischen der zentralen Plattform und der Anlagen-Steuereinheit besteht, ist das Verfahren grundsätzlich einsetzbar. In dem Fall einer solchen Offline-Zugriffsberechtigungserteilung (wobei sich das „Offline" auf die Anlagen-Steuereinheit bezieht), werden von der zentralen Plattform bei einem Kontakt mit dem mobilen Kommunikationsgerät nicht nur die für das mobile Kommunikationsgerät bestimmten Daten zu einer Zugriffsberechtigung gesendet.

Diese für das mobile Kommunikationsgerät bestimmten Daten sind in der mobilen Zugriffseinrichtung lesbar und an die Anlagen-Steuereinrichtung übertragbar, wenn der Nutzer das mobilen Kommunikationsgerät mit der Anlagen-Steuereinheit koppelt. Die zentrale Steuerplattform überträgt für den Fall einer Unerreichbarkeit der Anlagen-Steuereinheit durch die zentrale Plattform aber außerdem wenigstens einen Datencontainer an das mobile Kommunikationsgerät, welcher signiert und verschlüsselt ist und in dem mobilen Kommunikationsgerät nicht veränderbar ist. Dieser Datencontainer wird über das mobile Kommunikationsgerät von der zentralen Plattform an die Anlagen-Steuereinheit übermittelt und enthält die Soll-Daten, welche die Anlagen-Steuereinheit zur Prüfung der Identität des Nutzers und zum Vergleich mit den Ist-Daten benötigt.

Eine Signatur des Datencontainers oder der Daten im Datencontainer durch die zentrale Steuerplattform ist dazu vorgesehen, dass die Anlagen-Steuereinheit die Integrität und Herkunft der Daten im Datencontainer verifizieren kann. Eine Manipulation der Daten auf dem Weg zwischen zentraler Steuerplattform und Anlagen-Steuereinheit ist damit unterbunden. Die Signatur durch die zentrale Steuerplattform wird anhand von

gespeicherten Zertifikaten in der Anlagen-Steuereinheit geprüft. Die Anlagen-Steuereinheit verfügt dazu über gespeicherte Zertifikate. Diese wurden in einer sicheren Umgebung, z.B. Herstellerseitig oder Verwalterseitig gespeichert. Dieses Konzept ist z.B. aus Internet-Browsern bekannt, die bei Installation Informationen zur Verifizierung der Zertifikate von zahlreichen Zertifizierungsstellen mitbringen. Eine Veränderung der Daten ist damit technisch kaum möglich, die Sicherheit sowohl der Integrität der Daten als auch deren Herkunft von der berechtigten zentralen Steuerplattform ist gesichert.

Eine Verschlüsselung der Daten im Container kann insbesondere mit einer symmetrischen oder asymmetrischen Verschlüsselung erfolgen, wobei nur die zentrale Steuerplattform und die Anlagen-Steuereinheit an der elektronisch steuerbaren Einrichtung über die erforderlichen Schlüssel verfügen. Eine Verschlüsselung erfolgt insbesondere mit einem individuellen Schlüssel der betroffenen Anlagen-Steuereinrichtung. Die Entschlüsselung ist dann ausschließlich in der adressierten Anlagen-Steuereinrichtung möglich, zu welcher die zentrale Steuerplattform die Verschlüsselung vorgenommen hat.

Das mobile Kommunikationsgerät wird für diesen Datencontainer als Transportmedium verwendet, ohne dass dieses auf Inhalte des Containers Zugriff hätte. Der Sinn dieser Maßnahme besteht darin, dass in dem unzugänglichen Datencontainer Zugriffsrechte, Buchungsinformationen und Sol-Daten zum Benutzer als Informationen zur Anlagen-Steuereinrichtung transportierbar sind, welche die Anlagen-Steuereinrichtung ansonsten unmittelbar von der zentralen Plattform erhalten würde. Wenn dieser unmittelbare Empfang jedoch nicht möglich ist, z.B., weil die Anlagen-Steuereinheit nicht mit einem Datenübertragungsnetz gekoppelt ist oder nur in größeren Zeitabständen aktualisiert wird, bringt das mobile Kommunikationsgerät die erforderlichen Daten in dem geschützten Container mit. Dabei können in dem geschützten Container Konfigurationsdaten, jedoch auch Programmaktualisierungen enthalten sein.

Sobald das mobile Kommunikationsgerät mit der Anlagen-Steuereinheit koppelt, kann der Container an die Anlagen-Steuereinheit übertragen werden. Dort wird er entschlüsselt, verifiziert und verarbeitet. In diesem Vorgang werden z.B. die gespeicherten Benutzungsrechte in der Anlagen-Steuereinheit aktualisiert und die Soll-Daten des Benutzers werden ausgelesen. Danach kann die Berechtigung des Benutzers, der über das mobile Kommunikationsgerät mit der Anlagen-Steuereinheit gekoppelt ist, anhand der ausgelesenen Soll-Daten und der vom Benutzer eingegebenen Ist-Daten verifiziert werden.

Dieser Vorgang kann für einen Benutzer vollkommen transparent ablaufen. Der Benutzer für das mobile Kommunikationsgerät mit sich. Zur Verhinderung der unerlaubten Vervielfältigung wird in Zeitabständen, wie oben erläutert, Kontakt zwischen dem mobilen Kommunikationsgerät und der zentralen Plattform hergestellt. Bei solchen Verbindungen kann dem mobilen Kommunikationsgerät neben einer Synchronisierungsnachricht auch ein Datencontainer für eine Anlagen-Steuereinheit übermittelt werden, auf welche der Benutzer demnächst zugreifen könnte. Dies geschieht durch Kommunikation der Applikation auf dem mobilen Kommunikationsgerät mit der zentralen Plattform. In einer Kontaktaufnahme wird also das mobile Kommunikationsgerät auf eine unerlaubte Vervielfältigung geprüft und außerdem als Transportmittel für eine Anlagen-Steuereinheit, die von der zentralen Steuereinheit nicht erreichbar ist. In dem Datencontainer kann in diesem Zusammenhang auch die Information hinterlegt sein, dass das zugeordnete Gerät oder ein anderes mobiles Gerät gesperrt wird, da eine unerlaubte Vervielfältigung erkannt wurde.

Die bedeutet, dass die zentrale Plattform auch an Anlagen-Steuereinheiten die Sperrung mitteilen kann, welche zeitweise oder dauerhaft nicht unmittelbar erreichbar sind. Ist die Anlagen-Steuereinheit für die zentrale Plattform nicht erreichbar, so packt die zentrale Steuerplattform die Informationen zu gesperrten Geräten in einen Datencontainer, der an die mobilen Kommunikationsgeräte im Rahmen der regelmäßigen

Synchronisation übermittelt wird. Dies kann eine Mehrzahl an mobilen Kommunikationsgeräten betreffen, welche mit denselben Anlagen-Steuereinheiten gekoppelt werden, wie das zu sperrende Gerät. Auf diese Weise werden die Sperrinformationen über ein oder mehrere Mobilgeräte an die Anlagen-Steuereinheiten verteilt.

Geht ein Benutzer nun mit seinem mobilen Kommunikationsgerät zur Anlagen-Steuereinheit initiiert einen Öffnungsdialog, wird neben den Legitimationsdaten auch der Datencontainer vom mobilen Kommunikationsgerät an die Anlagen-Steuereinheit übertragen. Dieser Datencontainer wird in der Anlagen-Steuereinheit entschlüsselt, wo der private Schlüssel zur Decodierung gespeichert ist.

Die Signatur des Containers oder der darin gespeicherten Daten, ausgestellt durch die zentrale Steuerplattform, wird in der Anlagen-Steuereinheit anhand von gespeicherten Zertifikaten geprüft. Nach erfolgreicher Prüfung des Zertifikats werden die Sperrinformationen und die weiteren Daten ausgelesen. Eine Öffnungsberechtigung des Nutzers kann dann verifiziert werden.

Wesentlich ist, dass in der mobilen Zugriffseinrichtung zu keiner Zeit Zugriff auf den Inhalt des Datencontainers gegeben ist oder dieser Inhalt zumindest nicht veränderbar ist, ohne die Signatur zu zerstören. Der Container wird ausschließlich zum Datentransport verwendet. Dadurch kann auch ohne direkte Verbindung zwischen zentraler Plattform und Anlagen-Steuereinrichtung eine Aktualisierung der Konfiguration und Programmierung der Anlagen-Steuereinrichtung erfolgen. So sind Aktualisierungen für Anlagen-Steuereinheiten möglich, welche für die zentrale Steuerplattform unerreichbar sind.

Der Ablauf einer Ausführungsform des Verfahrens ist beispielhaft in der beiliegenden Zeichnung dargestellt.

Fig. 1 zeigt einen beispielhaften Ablauf des Sicherungsverfahrens.

In Schritt 10 erfolgt eine Einrichtung des Systems zur Ausführung des Verfahrens. Die Identität des Benutzers wird durch eine vertrauenswürdige Stelle geprüft und die

Benutzerdaten werden bei Schritt 20 in einer zentralen Plattform, insbesondere einem Datenbankserver gespeichert.

Bei Schritt 30 wird ein Smartphone des Benutzers mit einer Anlagen-Steuereinheit an einem Gebäude gekoppelt, wobei eine eindeutige Kennung des Smartphones in der Anlagen-Steuereinheit und/oder dem zentralen Datenbankserver gespeichert wird, welcher mit der Anlagen-Steuereinheit gekoppelt ist.

In Schritt 40 wird von dem Datenbankserver eine Synchronisationsnachricht erstellt. Die enthält einen Zeitstempel und eine zufällig generierte Datenfolge. Diese Synchronisationsnachricht wird im Datenbankserver gespeichert und an das Smartphone über ein Kommunikationsnetz übermittelt. Auch im Smartphone wird die Synchronisationsnachricht gespeichert.

Bei Schritt 50 wird eine Pause abgewartet bevor bei Schritt 60 erneut eine Kommunikationsverbindung zwischen Smartphone und Datenbankserver aufgebaut wird. Das Smartphone übermittelt die in der vorherigen Kommunikation erhaltene Synchronisationsnachricht bei Schritt 70 und in dem Datenbankserver wird diese mit der dort gespeicherten Synchronisationsnachricht in Schritt 80 verglichen.

Ein Vergleich bei Schritt 90 zeigt, ob die Synchronisationsnachrichten konsistent sind. Falls ja, wird eine neue Synchronisationsnachricht erzeugt und an das Smartphone übermittelt. Falls nein, wird das Smartphone für den Zugriff im zentralen Datenbankserver gesperrt.

Patentansprüche

1. Verfahren zum Sichern eines Zutrittsverfahrens für eine ortsfeste Anlage, wobei das Zutrittsverfahren wenigstens ein mobiles Kommunikationsgerät und eine entfernte Steuereinrichtung zur Verwaltung der Zutrittsrechte aufweist und wobei das mobile Kommunikationsgerät als Schlüssel für die ortsfeste Anlage eingerichtet ist,

aufweisend die Schritte,

wiederholtes Verbinden des mobilen Kommunikationsgerätes mit der entfernten Steuereinrichtung,

Erzeugen von charakteristischen Neu-Synchronisierungsdaten für jede Verbindung,

Speichern wenigstens eines Teils der charakteristischen Neu-Synchronisierungsdaten in dem mobilen Kommunikationsgerät und der entfernten Steuereinrichtung,

Übermitteln von charakteristischen Alt-Synchronisierungsdaten einer vorangehenden Verbindung von dem mobilen Kommunikationsgerät an die entfernte Steuereinrichtung,

Konsistenzprüfung in der entfernten Steuereinrichtung zwischen den vom mobilen Kommunikationsgerät empfangenen Alt-Synchronisierungsdaten und den in der entfernten Steuereinrichtung gespeicherten Alt-Synchronisierungsdaten,

- falls die Daten konsistent sind, unterbrechen der Verbindung und Abwarten eines Synchronisierungsintervalls bevor die Verbindung für die nächste Synchronisation wiederhergestellt wird;
- falls die Daten inkonsistent sind, sperren des mobilen Kommunikationsgeräts für den weiteren Zutritt zu der ortsfesten Anlage.

2. Verfahren nach Anspruch 1, wobei die Neu-Synchronisierungsdaten in der entfernten Steuereinrichtung erzeugt werden.

3. Verfahren nach einem der vorangehenden Ansprüche, wobei in dem mobilen Kommunikationsgerät und der entfernten Steuereinrichtung asymmetrische Daten gespeichert werden.

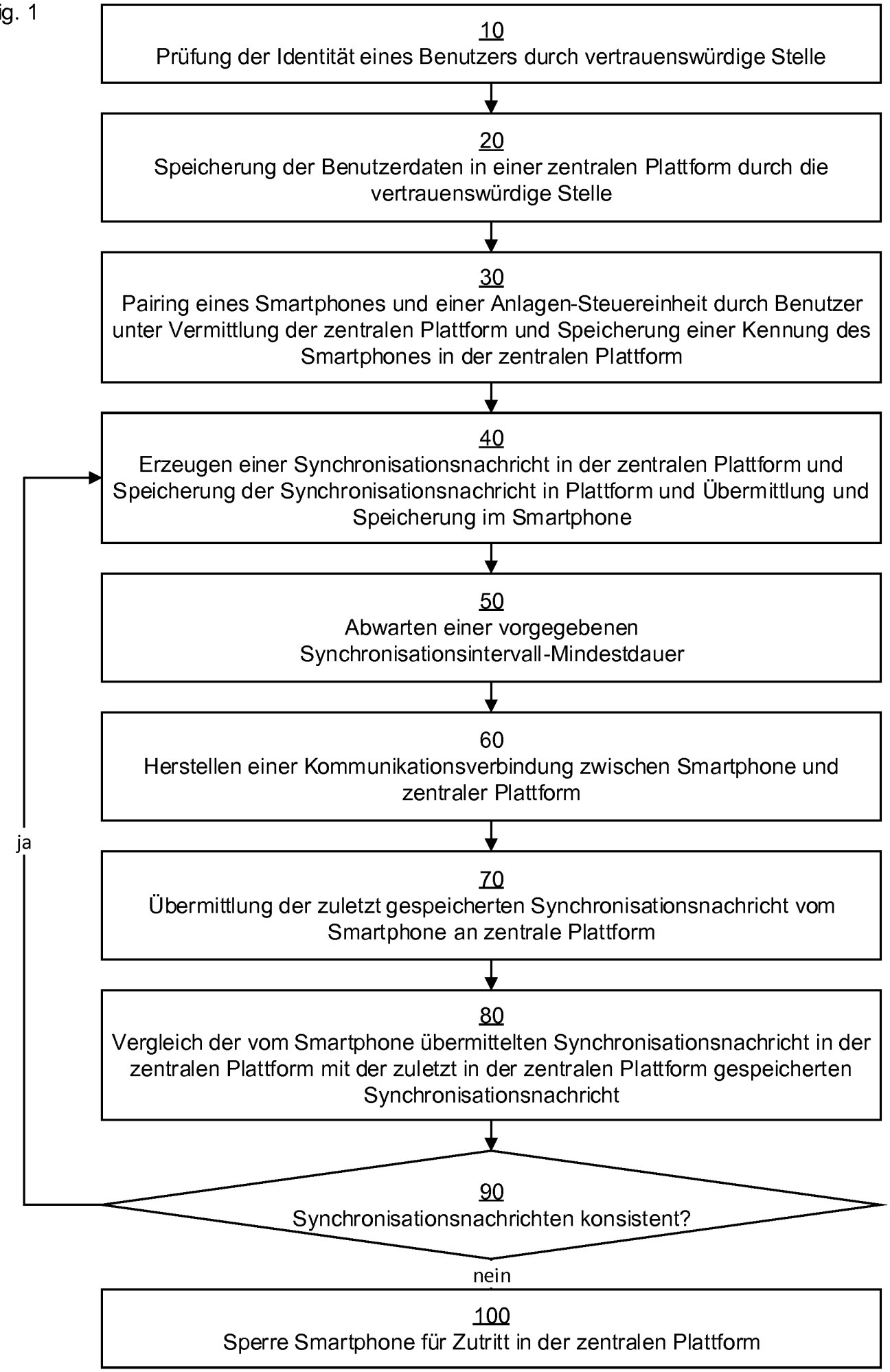
4. Verfahren nach einem der vorangehenden Ansprüche, wobei eine zentrale Plattform als entfernte Steuereinrichtung verwendet wird, welche die Zutrittsrechte für eine Vielzahl von Benutzern, ortsfesten Anlagen und zugeordneten mobilen Kommunikationsgeräten verwaltet und mit einer Vielzahl von Anlagenseitigen Anlagen-Steuereinheiten kommuniziert.

5. Verfahren nach Anspruch 4, wobei bei wenigstens einigen der Verbindungen zwischen dem mobilen Kommunikationsgerät und der zentralen Plattform zusätzlich ein von der zentralen Plattform signierter Datencontainer an die mobile Kommunikationseinrichtung übermittelt wird,

wobei der Datencontainer bei einer Verbindung der mobilen Kommunikationseinrichtung mit einer Anlagen-Steuereinheit an die Anlagen-Steuereinheit übertragen wird,

wobei in der Anlagen-Steuereinheit die Signatur verifiziert wird und nach erfolgreicher Verifikation die Anlagen-Steuereinheit mit dem Inhalt des Datencontainers aktualisiert wird.

Fig. 1


10
Prüfung der Identität eines Benutzers durch vertrauenswürdige Stelle
20
Speicherung der Benutzerdaten in einer zentralen Plattform durch die vertrauenswürdige Stelle
30
Pairing eines Smartphones und einer Anlagen-Steuereinheit durch Benutzer unter Vermittlung der zentralen Plattform und Speicherung einer Kennung des Smartphones in der zentralen Plattform
40
Erzeugen einer Synchronisationsnachricht in der zentralen Plattform und Speicherung der Synchronisationsnachricht in Plattform und Übermittlung und Speicherung im Smartphone
50
Abwarten einer vorgegebenen Synchronisationsintervall-Mindestdauer
60
Herstellen einer Kommunikationsverbindung zwischen Smartphone und zentraler Plattform
70
Übermittlung der zuletzt gespeicherten Synchronisationsnachricht vom Smartphone an zentrale Plattform
80
Vergleich der vom Smartphone übermittelten Synchronisationsnachricht in der zentralen Plattform mit der zuletzt in der zentralen Plattform gespeicherten Synchronisationsnachricht
90
Synchronisationsnachrichten konsistent?
ja
nein
100
Sperre Smartphone für Zutritt in der zentralen Plattform

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/054298

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 H04W12/12
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C H04M H04W

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

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

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 8 380 165 B1 (KOLLER GARY DUANE [US] ET AL) 19 February 2013 (2013-02-19)	1-4
Y	abstract column 1, line 48 - column 2, line 4 column 3, line 31 - column 6, line 21 column 6, line 66 - column 7, line 13 column 7, line 44 - column 8, line 4 column 9, line 1 - line 22 claims 1,10,18 figures 1,3	5

Y	US 2014/049364 A1 (AHEARN JOHN ROBERT [US] ET AL) 20 February 2014 (2014-02-20) abstract paragraph [0016] - paragraph [0020] paragraph [0052] - paragraph [0053] figures 1,3	5

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 May 2017	06/06/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Post, Katharina

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/054298

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	WO 2016/165864 A1 (HUF HÜLSBECK & FÜRST GMBH & CO KG [DE]) 20 October 2016 (2016-10-20) abstract page 2, line 33 - page 3, line 3 claims 1-4 figure 1 -----	1-4

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/054298

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8380165 B1	19-02-2013	NONE	
US 2014049364 A1	20-02-2014	AU 2013302377 A1	02-04-2015
		AU 2017200410 A1	09-02-2017
		EP 2885932 A2	24-06-2015
		NZ 706015 A	29-04-2016
		US 2014049364 A1	20-02-2014
		US 2014049365 A1	20-02-2014
		WO 2014028896 A2	20-02-2014
WO 2016165864 A1	20-10-2016	DE 102015105595 A1	13-10-2016
		WO 2016165864 A1	20-10-2016

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/054298

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G07C9/00 H04W12/12
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G07C H04M H04W

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

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 8 380 165 B1 (KOLLER GARY DUANE [US] ET AL) 19. Februar 2013 (2013-02-19)	1-4
Y	Zusammenfassung Spalte 1, Zeile 48 - Spalte 2, Zeile 4 Spalte 3, Zeile 31 - Spalte 6, Zeile 21 Spalte 6, Zeile 66 - Spalte 7, Zeile 13 Spalte 7, Zeile 44 - Spalte 8, Zeile 4 Spalte 9, Zeile 1 - Zeile 22 Ansprüche 1,10,18 Abbildungen 1,3	5

Y	US 2014/049364 A1 (AHEARN JOHN ROBERT [US] ET AL) 20. Februar 2014 (2014-02-20) Zusammenfassung Absatz [0016] - Absatz [0020] Absatz [0052] - Absatz [0053] Abbildungen 1,3	5

	-/--	

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

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

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. Mai 2017	06/06/2017

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

2

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/054298

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X,P	WO 2016/165864 A1 (HUF HÜLSBECK & FÜRST GMBH & CO KG [DE]) 20. Oktober 2016 (2016-10-20) Zusammenfassung Seite 2, Zeile 33 - Seite 3, Zeile 3 Ansprüche 1-4 Abbildung 1 -----	1-4

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/054298

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 8380165 B1	19-02-2013	KEINE	
US 2014049364 A1	20-02-2014	AU 2013302377 A1	02-04-2015
		AU 2017200410 A1	09-02-2017
		EP 2885932 A2	24-06-2015
		NZ 706015 A	29-04-2016
		US 2014049364 A1	20-02-2014
		US 2014049365 A1	20-02-2014
		WO 2014028896 A2	20-02-2014
WO 2016165864 A1	20-10-2016	DE 102015105595 A1	13-10-2016
		WO 2016165864 A1	20-10-2016