(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
26. Januar 2012 (26.01.2012)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2012/010381 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2011/060489

(22) Internationales Anmeldedatum:
22. Juni 2011 (22.06.2011)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2010 031 931.7 22. Juli 2010 (22.07.2010) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **FALK, Rainer** [DE/DE]; Parkstraße 43, 85435 Erding (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

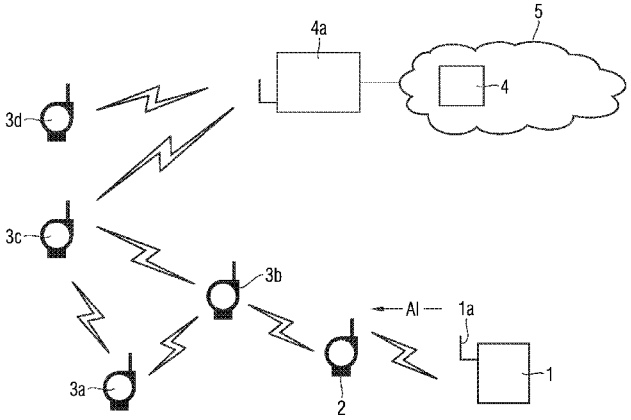
— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD FOR REGISTERING A WIRELESS COMMUNICATION DEVICE AT A BASE DEVICE AND CORRESPONDING SYSTEM

(54) **Bezeichnung** : VERFAHREN ZUM REGISTRIEREN EINER DRAHTLOSEN KOMMUNIKATIONSEINRICHTUNG AN EINER BASISEINRICHTUNG SOWIE ENTSPRECHENDES SYSTEM

FIG 1



(57) **Abstract**: The invention relates to a method for registering a wireless communication device at a base device. The method comprises the steps of: transmitting, by means of a wireless authentication device, a piece of authentication information; receiving, by means of the wireless communication device, a piece of authentication information, in particular using in-band communication; transferring, by means of the wireless communication device, the piece of authentication information to the base device; analyzing, by means of the base device, the transferred piece of authentication information; and incorporating the wireless communication device into a network depending on the result of the analysis. The invention further relates to a corresponding system and to a use thereof.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2012/010381 A1

Die Erfindung betrifft ein Verfahren zum Registrieren einer drahtlosen Kommunikationseinrichtung an einer Basiseinrichtung. Das Verfahren umfasst die Schritte: Aussenden einer Authentisierungsinformation durch eine drahtlose Authentisierungseinrichtung, Empfangen einer Authentisierungsinformation durch die drahtlose Kommunikationseinrichtung, insbesondere mittels In-Band-Kommunikation, Übertragen der Authentisierungsinformation durch die drahtlose Kommunikationseinrichtung zu der Basiseinrichtung, Überprüfen der übertragenen Authentisierungsinformation durch die Basiseinrichtung, Einbinden der drahtlosen Kommunikationseinrichtung in ein Netzwerk in Abhängigkeit des Ergebnisses der Überprüfung. Die Erfindung betrifft ebenfalls ein entsprechendes System sowie eine Verwendung.

Beschreibung

Verfahren zum Registrieren einer drahtlosen Kommunikationseinrichtung an einer Basiseinrichtung sowie entsprechendes System

Die Erfindung betrifft ein Verfahren zum Registrieren einer drahtlosen Kommunikationseinrichtung sowie ein entsprechendes System.

Steuergeräte, Sensoren, Aktoren werden heutzutage zunehmend drahtlos miteinander verbunden bzw. vernetzt, um größtmögliche Flexibilität zu gewährleisten. Dabei ist auch eine Wartung der Geräte bzw. Sensoren einfacher, da beispielsweise im Falle einer Störung keine Kabelschächte, etc. geöffnet werden müssen, sondern lediglich das Gerät direkt. Zur Verbindung der genannten Steuergeräte, Sensoren, etc. werden üblicherweise offene Protokolle wie IEEE 802.11 WLAN, IEEE 802.15.4, Bluetooth, ZigBee oder auch Wireless HART verwendet. Um möglichst eine Manipulation der Sensoren oder Anweisungen der Steuergeräte bei der drahtlosen Verbindung zu vermeiden, wird die Kommunikation vom Steuergerät oder Sensor von der entsprechen Punktschnittstelle kryptographisch verschlüsselt, beispielsweise durch eine WLAN-Verbindung mittels TKIP oder CCMP, oder bei 802.15.4 mittels AES-CCM. Um ein Steuergerät, einen Sensor oder Ähnliches mit einer Funkstation zu verbinden und eine verschlüsselte Verbindung zu etablieren, muss das Steuergerät, der Sensor oder allgemein die drahtlose Kommunikationseinrichtung so konfiguriert werden, dass die entsprechende Verschlüsselung verwendet wird, also beispielsweise ein kryptographischer Schlüssel eingerichtet werden. Eine derartige Einrichtung eines Schlüssels wird auch als Bootstrapping oder Pairing bezeichnet.

Aus der US 2006/282885 ist bekannt, dass ein Administratorgerät eines zu konfigurierenden Drahtlosgeräts einen Berechtigungsnachweis drahtlos bereitstellt. Das Drahtlosgerät wird

von dem Administratorgerät mit dem vom Administratorgerät bereitgestellten Berechtigungsnachweis konfiguriert.

Darüber hinaus ist es bekannt, eine In-Band-Kommunikation während einer schwach geschützten Phase vorzunehmen. Das entsprechende drahtlose einzurichtende Kommunikationsgerät benötigt hierfür jedoch spezielle modifizierte Übertragungsverfahren. Schließlich ist es bekannt, ein Pairing gesichert durch einen Out-Of-Band-Kanal, wie beispielsweise menschliche Interaktion (also Eingabe bzw. Prüfen einer PIN, etc.) vorzunehmen.

Nachteilig dabei ist, dass die vorgenannten Verfahren einen hohen Arbeitsaufwand erfordern und kompliziert gestaltet sind, insbesondere bei Einsatz im industriellen Bereich, da dort eine große Anzahl von drahtlosen Kommunikationseinrichtungen eingerichtet werden. Dabei ist es gleichzeitig erforderlich, dass das Pairing geschützt bzw. gesichert erfolgt, da dabei die Sicherheitskonfigurationsparameter eingerichtet werden.

Eine Aufgabe der vorliegenden Erfindung ist daher, ein Verfahren und ein System zum Registrieren einer drahtlosen Kommunikationseinrichtung an einer Basiseinrichtung zur Verfügung zu stellen, bei dem der Vorgang des Pairings für eine Vielzahl von zu registrierenden drahtlosen Geräten einfacher und mit geringem Arbeitsaufwand durchführbar ist und gleichzeitig der Pairing-Vorgang geschützt abläuft.

Diese Aufgabe wird durch ein Verfahren gemäß dem Anspruch 1 und einem System gemäß dem Anspruch 7 gelöst. Der erzielte Vorteil dabei ist, dass zum Registrieren der drahtlosen Kommunikationseinrichtung an der Basiseinrichtung keine zusätzliche Interaktion notwendig ist, es muss nur eine entsprechende Authentisierungseinrichtung, beispielsweise von einem Monteur etc., mitgeführt werden, um die drahtlose Kommunikationseinrichtung für ein Pairing mit der Basiseinrichtung vorzubereiten.

Vorteilhafterweise erfolgt das Aussenden einer Authentisierungsinformation mittels einer reduzierten Sendeleistung und/oder gerichtet, so dass die Authentisierungsinformation nur räumlich begrenzt empfangbar ist. Der Vorteil hierbei ist, dass damit die Sicherheit der Registrierung der drahtlosen Kommunikationseinrichtung weiter verbessert wird, da die Authentisierungsinformation nur in einem bestimmten Bereich empfangbar ist, der aufgrund der begrenzten Reichweite und/oder der gerichteten Ausstrahlung räumlich begrenzt ist. Einem potentiellen Angreifer wird so das Abhören bzw. Belauschen von übertragenen Authentisierungsinformationen erschwert.

Zweckmäßigerweise erfolgt vor dem Aussenden der Authentisierungsinformation ein Überwachen und/oder Auswerten von Signalen, insbesondere Kommunikationssignalen, der drahtlosen Kommunikationseinrichtung und/oder von weiteren sich in einer Funkreichweite der Authentisierungseinrichtung befindenden drahtlosen Kommunikationseinrichtungen. Der erzielte Vorteil dabei ist, dass damit zum einen die Sicherheit der Registrierung der drahtlosen Kommunikationseinrichtung insgesamt verbessert wird und gleichzeitig die Zuverlässigkeit gesteigert werden kann. Wird beispielsweise ein Überwachen von Funksignalen im Frequenzbereich der drahtlosen Kommunikationsvorrichtung vorgenommen und ergibt die Überprüfung, dass hier unübliche Funksignale und/oder Kommunikationssignale von der drahtlosen Kommunikationseinrichtung gesendet und/oder empfangen werden, wird einem Benutzer der drahtlosen Authentisierungseinrichtung eine entsprechende Information angezeigt werden, so dass das Aussenden der Authentisierungsinformation erst dann erfolgt, wenn der Grund für die unüblichen Funk- und/oder Kommunikationssignale gefunden ist, um eine Manipulation der drahtlosen Kommunikationseinrichtung oder ein Abhören der Kommunikation der drahtlosen Kommunikationseinrichtung mit der drahtlosen Authentisierungseinrichtung ausschließen zu können.

Vorteilhafterweise werden die überwachten und/oder ausgewerteten Signale der drahtlosen Kommunikationseinrichtung in die Authentisierungsinformation kodiert, wobei insbesondere die kodierten überwachten und/oder ausgewerteten Signale durch die Basiseinrichtung ausgewertet werden. Der Vorteil dabei ist, dass damit die Sicherheit weiter gesteigert wird, da die drahtlose Kommunikationseinrichtung über eine Information über bestimmte Funk- und/oder Signaleigenschaften verfügt, so dass Manipulationen an der drahtlosen Kommunikationseinrichtung festgestellt werden können. Wird die Information der überwachten und/oder ausgewerteten Signale in die durch die Basiseinrichtung ausgewertete Authentisierungsinformation eincodiert, wird vermieden, dass eine manipulierte drahtlose Kommunikationseinrichtung selbst ein gewolltes falsches Prüfergebnis an die Basiseinrichtung sendet und so trotz Manipulation eine Registrierung der drahtlosen Kommunikationseinrichtung an der Basiseinrichtung erfolgt. Dadurch wird die Sicherheit weiter gesteigert.

Zweckmäßigerweise erfolgt vor dem Aussenden der Authentisierungsinformation ein Überprüfen von zumindest einem Parameter einer Funkumgebung. Durch die Überwachung zumindest eines Parameters der Funkumgebung können beispielsweise weitere drahtlose Geräte oder Störsignale in der Umgebung einfach erkannt werden, so dass beim Vorliegen von Störsignalen oder anderen Geräten in der Umgebung gegebenenfalls ein Aussenden der Authentisierungsinformation unterbunden werden kann, um Manipulationen oder eine fehlerhafte Übertragung der Authentisierungsinformation von der drahtlosen Authentisierungseinrichtung zur drahtlosen Kommunikationseinrichtung zu vermeiden.

Um sicherzustellen, dass die drahtlose Authentisierungseinrichtung nicht zu manipulativen Zwecken, beispielsweise aus einem Gebäude oder einer vordefinierten Umgebung entfernt wird, ist es vorteilhaft, dass vor dem Aussenden der Authentisierungsinformation ein Lokalisieren der drahtlosen Authentisierungseinrichtung erfolgt.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Figuren.

Dabei zeigt

Fig. 1 ein Verfahren bzw. ein System zum Registrieren einer drahtlosen Kommunikationseinrichtung in einer ersten Ausführungsform der vorliegenden Erfindung;

Fig. 2a ein Übertragungsverfahren gemäß der ersten Ausführungsform der vorliegenden Erfindung;

Fig. 2b ein Übertragungsverfahren für ein Verfahren gemäß einer zweiten Ausführungsform der vorliegenden Erfindung; sowie

Fig. 3 ein Übertragungsdiagramm für ein Verfahren gemäß einer dritten Ausführungsform der vorliegenden Erfindung.

Fig. 1 zeigt ein Verfahren bzw. ein System zum Registrieren einer drahtlosen Kommunikationseinrichtung in einer ersten Ausführungsform der vorliegenden Erfindung.

In Fig. 1 bezeichnet ein Bezugszeichen 1 eine drahtlose Authentisierungseinrichtung 1, die über eine Funkschnittstelle 1a verfügt. Die drahtlose Authentisierungseinrichtung 1 überträgt eine Authentisierungsinformation AI über die Funkschnittstelle 1a zu einer drahtlosen Kommunikationseinrichtung 2, die an einer Basiseinrichtung 4 registriert werden soll. Bereits an der Basiseinrichtung 4 registriert sind weitere drahtlose Kommunikationseinrichtungen in Form von Sensorknoten 3a, 3b, 3c, 3d, die untereinander drahtlos verbunden sind zur Übertragung von Sensordaten und ggf. auch direkt mit der Funkschnittstelle 4a der Basiseinrichtung 4. Die Ba-

siseinrichtung 4 ist wiederum mit einem Netzwerk 5 verbunden und erlaubt den Sensorknoten 3a, 3b, 3c, 3d den Zugriff auf das Netzwerk 5 nach erfolgreicher Anmeldung bzw. Authentisierung (Network Join) an der Basiseinrichtung 4. Nur ein an der Basiseinrichtung 4 registrierter Sensorknoten 3a, 3b, 3c, 3d kann sich an der Basiseinrichtung 4 erfolgreich anmelden. Die Basiseinrichtung 4 greift dazu auf gespeicherte Information über registrierte Sensorknoten 3a, 3b, 3c, 3d zu. Nach dem Übertragen der Authentisierungsinformation AI von der drahtlosen Authentisierungseinrichtung 1 zu der drahtlosen Kommunikationseinrichtung 2 sendet diese die erhaltenen Authentisierungsinformationen AI gemäß Fig. 1 über den Sensorknoten 3b und 3c sowie über die Funkschnittstelle 4a an die Basiseinrichtung 4, die die Authentisierungsinformation AI überprüft. Dazu kann z.B. eine in der Authentisierungsinformation AI enthaltene kryptographische Prüfsumme (Message Authentication Code, Digitale Signatur) geprüft werden. Die kryptographische Prüfsumme kann durch die drahtlose Authentisierungseinrichtung 1 unter Verwendung eines gespeicherten kryptographischen Schlüssels berechnet werden. Ist die Authentisierungsinformation AI gültig, wird durch die Basiseinrichtung 4 ein Zugriffsschlüssel JK (Join Key) erzeugt und über die jeweiligen Sensorknoten 3a, 3b, 3c, 3d schließlich zur drahtlosen Kommunikationseinrichtung 2 zurückgesendet. Die drahtlose Kommunikationseinrichtung 2 ist nun bei der Basiseinrichtung 4 registriert und hat nun Zugriff auf das Netzwerk 5 der Basiseinrichtung 4.

Fig. 2 zeigt ein Übertragungsverfahren gemäß der ersten Ausführungsform der vorliegenden Erfindung.

In Fig. 2a ist im Detail die Übertragung der Information zu den einzelnen Geräten in zeitlicher Abfolge gezeigt. Die drahtlose Authentisierungseinrichtung 1 sendet eine Authentisierungsinformation AI an die zu registrierende drahtlose Kommunikationseinrichtung 2. Die drahtlose Kommunikationseinrichtung 2 sendet nun die empfangene Authentisierungsinformation AI zusammen mit einer entsprechenden Identifikationsnum-

mer der zu registrierenden drahtlosen Kommunikationseinrichtung 2 an einen benachbarten Sensorknoten 3b, der wiederum gegebenenfalls über weitere benachbarte Sensorknoten 3a, 3c, 3d und die Funkschnittstelle 4a der Basiseinrichtung 4 diese Authentisierungsinformation AI und die entsprechende Identifikationsnummer der zu registrierenden drahtlosen Kommunikationseinrichtung 2 an die Basiseinrichtung 4 sendet. Die Basiseinrichtung 4 überprüft bei der Registrierung R_1 nun die erhaltene Authentisierungsinformation AI und erzeugt einen Zugriffsschlüssel JK bei erfolgreicher Überprüfung und trägt die Identifikationsnummer der zu registrierenden drahtlosen Kommunikationseinrichtung 2 in eine interne Tabelle der Basiseinrichtung 4 ein, in der die zugriffsberechtigten Sensorknoten 3a, 3b, 3c, 3d ebenfalls eingetragen sind. Der erzeugte Zugriffsschlüssel JK wird dann über die Funkschnittstelle 4a, die Sensorknoten 3a, 3c, 3d gegebenenfalls und den benachbarten Sensorknoten 3b der drahtlosen Kommunikationseinrichtung 2 an diese übertragen. Damit ist der Registrierungsvorgang abgeschlossen. In einer Variante trägt die Basiseinrichtung 4 bei der Registrierung R_1 zusätzlich den Zugriffsschlüssel JK in die interne Tabelle der Basiseinrichtung 4 ein. In einer weiteren, nicht dargestellten Variante wird durch die Basiseinrichtung 4 statt der internen Tabelle der Basiseinrichtung 4 eine externe Tabelle der Basiseinrichtung 4 verwendet, z.B. eine Datenbank oder ein Verzeichnisdienst.

In Fig. 2b wird von der drahtlosen Kommunikationseinrichtung 2 im Unterschied zur Fig. 2a zusätzlich von der drahtlosen Kommunikationseinrichtung 2 ein Zugriffsschlüssel JK, der entweder vorkonfiguriert ist bzw. selbst erzeugt wird, über den benachbarten Sensorknoten 3b gegebenenfalls über weitere Sensorknoten 3a, 3c, 3d und über die Funkschnittstelle 4a der Basiseinrichtung 4 zusammen mit der Authentisierungsinformation AI und einer Identifikationsnummer an die Basiseinrichtung 4 übertragen. Die Registrierung R_2 an der Basiseinrichtung 4 erfolgt nun folgendermaßen: Die Basiseinrichtung 4 prüft die erhaltene Authentisierungsinformation AI und trägt im Falle einer positiven Überprüfung die Identifikationsnum-

mer und den Zugriffsschlüssel JK in eine Tabelle für zugriffsberechtigte Sensorknoten ein. Schließlich übermittelt die Basisstation 4 über die Funkschnittstelle 4a und Sensorknoten 3a, 3b, 3c, 3d ein entsprechendes Signal, dass die Registrierung erfolgreich war, an die drahtlose Kommunikationseinrichtung 2.

Fig. 3 zeigt ein Übertragungsdiagramm für ein Verfahren gemäß einer zweiten Ausführungsform der vorliegenden Erfindung. In Fig. 3 führt die drahtlose Authentisierungseinrichtung 1 ein Beobachten B eines Voranmeldeverfahrens einer drahtlosen Kommunikationseinrichtung 2 durch. Diese übermittelt ihre Identifikationsnummer und einen Zugriffsschlüssel JK über den benachbarten Sensorknoten 3b und gegebenenfalls weitere Sensorknoten 3a, 3c, 3d, über die Funkschnittstelle 4a zu der Basiseinrichtung 4. Es erfolgt ein Speichern R_3 der Identifikationsnummer und des Zugriffsschlüssels JK durch die Basiseinrichtung 4. Die Basiseinrichtung 4 übermittelt weiter ein Voranmeldesignal, enthaltend die Information, dass die Vorregistrierung erfolgreich war, an die drahtlose Kommunikationseinrichtung 2 zurück. Dieses Voranmeldeverfahren wird das Beobachten B durch die drahtlose Authentisierungseinrichtung 1 beobachtet (Beobachten B) und analysiert. In Abhängigkeit des Ergebnisses der Analyse wird dann entscheiden, ob eine Authentisierungsinformation AI an die drahtlose Kommunikationseinrichtung 2 übermittelt wird. Im Falle eines positiven Ergebnisses des Analysierens A wird eine Authentisierungsinformation AI an die drahtlose Kommunikationseinrichtung 2 übermittelt. Diese wiederum übermittelt die erhaltene Authentisierungsinformation und die Identifikationsnummer der drahtlosen Kommunikationseinrichtung 2 über die Sensorknoten 3b, 3a, 3c, 3d und die Funkschnittstelle 4a an die Basiseinrichtung 4. An der Basiseinrichtung 4 erfolgt ein Registrieren R_4, in dem die Authentisierungsinformation AI prüft und im Falle eines positiven Prüfergebnisses wird die Identifikationsnummer der drahtlosen Kommunikationseinrichtung 2 und des Zugriffsschlüssels JK in eine entsprechende Zugriffstabelle gemäß der Beschreibung zu den vorstehenden Figuren eingetra-

gen. Weiterhin übermittelt die Basiseinrichtung 4 eine entsprechende Information zurück zu der drahtlosen Kommunikationseinrichtung 2, dass ein Registrieren der drahtlosen Kommunikationseinrichtung 2 an der Basiseinrichtung 4 erfolgreich war.

Obwohl die vorliegende Erfindung durch vorstehende bevorzugte Ausführungsbeispiele beschrieben wurde, ist sie nicht darauf beschränkt, sondern auf vielfältige Weise modifizierbar.

Beispielsweise ist es möglich, die Authentisierungsinformation als Broadcast zu übertragen. Auf diese Weise können alle drahtlosen Kommunikationseinrichtungen, die sich in der Nähe befinden, diese Authentisierungsinformation empfangen. Des Weiteren ist es möglich, die Authentisierungsinformation an eine bestimmte drahtlose Kommunikationseinrichtung als Unicast zu übertragen, z.B. nach einer Authentisierung mit einem Gerätezertifikat eines Sensorknotens oder allgemeiner einer drahtlosen Kommunikationseinrichtung. Dabei können weitere Knoten-bezogene Messungen der Übertragungseigenschaften erfolgen, z.B. dessen Signalstärke kann mit einem vorgegebenen Wert verglichen werden oder es kann mittels Entfernungsmessung eine Entfernung zwischen der drahtlosen Authentisierungseinrichtung und der drahtlosen Kommunikationseinrichtung überprüft werden. Die Authentisierungsinformation AI kann beispielsweise ein Passwort, eine zeitlich wechselnde Zufallsfolge bei einem Zeitstempel mit einer kryptographischen Prüfsumme (Message Authentication Code MAC bzw. digitale Signatur) umfassen. Darüber hinaus kann die von der drahtlosen Authentisierungseinrichtung bereitgestellte Autorisierungsinformation aus mehreren Teilinformationen bestehen. Es ist beispielsweise möglich, dass nur eine Teilinformation von der drahtlosen Kommunikationseinrichtung an die Basiseinrichtung übertragen wird. Es ist beispielsweise möglich, dass die drahtlose Autorisierungseinrichtung zum Beispiel ein Tupel bereitstellt, umfassend eine Bestätigungsinformation bzw. Assertion (z.B. eine SAML-Assertion) und einen Schlüssel. Die drahtlose Kommunikationseinrichtung überträgt dann die Asser-

tion an die Basiseinrichtung und verifiziert die Kenntnis des Schlüssels, ohne ihn jedoch an die Basiseinrichtung zu übertragen. Dies kann beispielsweise derart erfolgen, dass die Basiseinrichtung eine Zufallszahl in die drahtlose Kommunikationseinrichtung überträgt. Die drahtlose Kommunikationseinrichtung führt dann eine Berechnung aus, in die die Zufallszahl und der Schlüssel als Parameter eingehen, beispielweise eine HMAC-SHA1(Schlüssel, Zufallszahl) und übermittelt das Ergebnis zurück an die Basiseinrichtung, die dann wiederum überprüft, ob anhand des Ergebnisses die drahtlose Kommunikationseinrichtung Zugriff auf das Netzwerk der Basiseinrichtung erhalten soll.

Eine drahtlose Kommunikation des drahtlosen Kommunikationsgeräts kann beispielsweise mittels WLAN oder Bluetooth erfolgen.

Patentansprüche

1. Verfahren zum Registrieren einer drahtlosen Kommunikationseinrichtung (2) an einer Basiseinrichtung (4), mit den Schritten:
   (a) Aussenden einer Authentisierungsinformation (AI) durch eine drahtlose Authentisierungseinrichtung (1),
   (b) Empfangen der gesonderten Authentisierungsinformation (AI) durch die drahtlose Kommunikationseinrichtung (2), insbesondere mittels In-Band-Kommunikation,
   (c) Übertragen der empfangenen Authentisierungsinformation (AI) durch die drahtlose Kommunikationseinrichtung (2) zu der Basiseinrichtung (4),
   (d) Überprüfen der übertragenen Authentisierungsinformation (AI) durch die Basiseinrichtung (4), und
   (e) Einbinden der drahtlosen Kommunikationseinrichtung (2) in ein Netzwerk (5) in Abhängigkeit des Ergebnisses der Überprüfung.

2. Verfahren gemäß Anspruch 1, wobei
das Aussenden einer Authentisierungsinformation (AI) mittels einer reduzierten Sendeleistung und/oder gerichtet erfolgt, so dass die Authentisierungsinformation nur räumlich begrenzt empfangbar ist.

3. Verfahren gemäß zumindest einem der Ansprüche 1-2, wobei vor dem Aussenden der Authentisierungsinformation (AI) ein Überwachen und/oder Auswerten von Signalen, insbesondere Kommunikationssignalen, der drahtlosen Kommunikationseinrichtung (2) und/oder von weiteren sich in einer Funkreichweite der Authentisierungseinrichtung (1) befindenden drahtlosen Kommunikationseinrichtungen (3a, 3b, 3c, 3d) erfolgt.

4. Verfahren gemäß zumindest Anspruch 3, wobei
die überwachten und/oder ausgewerteten Signale der drahtlosen Kommunikationseinrichtung (2) in die Authentisierungsinformation (AI) codiert wird, insbesondere wobei

die codierte überwachte Kommunikation durch die Basiseinrichtung (4) ausgewertet wird.

5. Verfahren gemäß zumindest einem der Ansprüche 1-4, wobei vor dem Aussenden der Authentisierungsinformation (AI) ein Überprüfen von zumindest einem Parameter einer Funkumgebung erfolgt.

6. Verfahren gemäß zumindest einem der Ansprüche 1-5, wobei vor dem Aussenden der Authentisierungsinformation (AI) ein Lokalisieren der drahtlosen Authentisierungseinrichtung (1) erfolgt.

7. System zum Registrieren einer drahtlosen Kommunikationseinrichtung (2), insbesondere geeignet zur Durchführung eines Verfahrens gemäß zumindest einem der Ansprüche 1-6, mit:
   (a) einer drahtlosen Authentisierungseinrichtung (1) zum Aussenden einer Authentisierungsinformation (AI), und mit
   (b) einer drahtlosen Kommunikationseinrichtung (2) zum Empfangen der ausgesendeten Authentisierungsinformation (AI), insbesondere mittels In-Band-Kommunikation, und zum Senden der Authentisierungsinformation (AI) an eine Basiseinrichtung (4) zur Registrierung der drahtlosen Kommunikationseinrichtung (2),
   (c) wobei die Basiseinrichtung (4) die drahtlose Kommunikationseinrichtung (2) in ein Netzwerk (5) in Abhängigkeit eines Ergebnisses der Überprüfung der Authentisierungsinformation (2) einbindet.

8. System gemäß zumindest Anspruch 7, wobei
wobei die drahtlose Authentisierungseinrichtung (1) Beobachtungsmittel (1a) zum Beobachten einer Funkumgebung und/oder einer Lokalisierung der drahtlosen Authentisierungseinrichtung (1) aufweist.

9. System gemäß zumindest einem der Ansprüche 7-8, wobei die drahtlose Authentisierungseinrichtung (1) Mittel zum Anpassen einer Sendeleistung aufweist (2).

10. Verwendung eines Systems gemäß zumindest einem der Ansprüche 7-9 zum Registrieren einer drahtlosen Kommunikationseinrichtung.

FIG 1

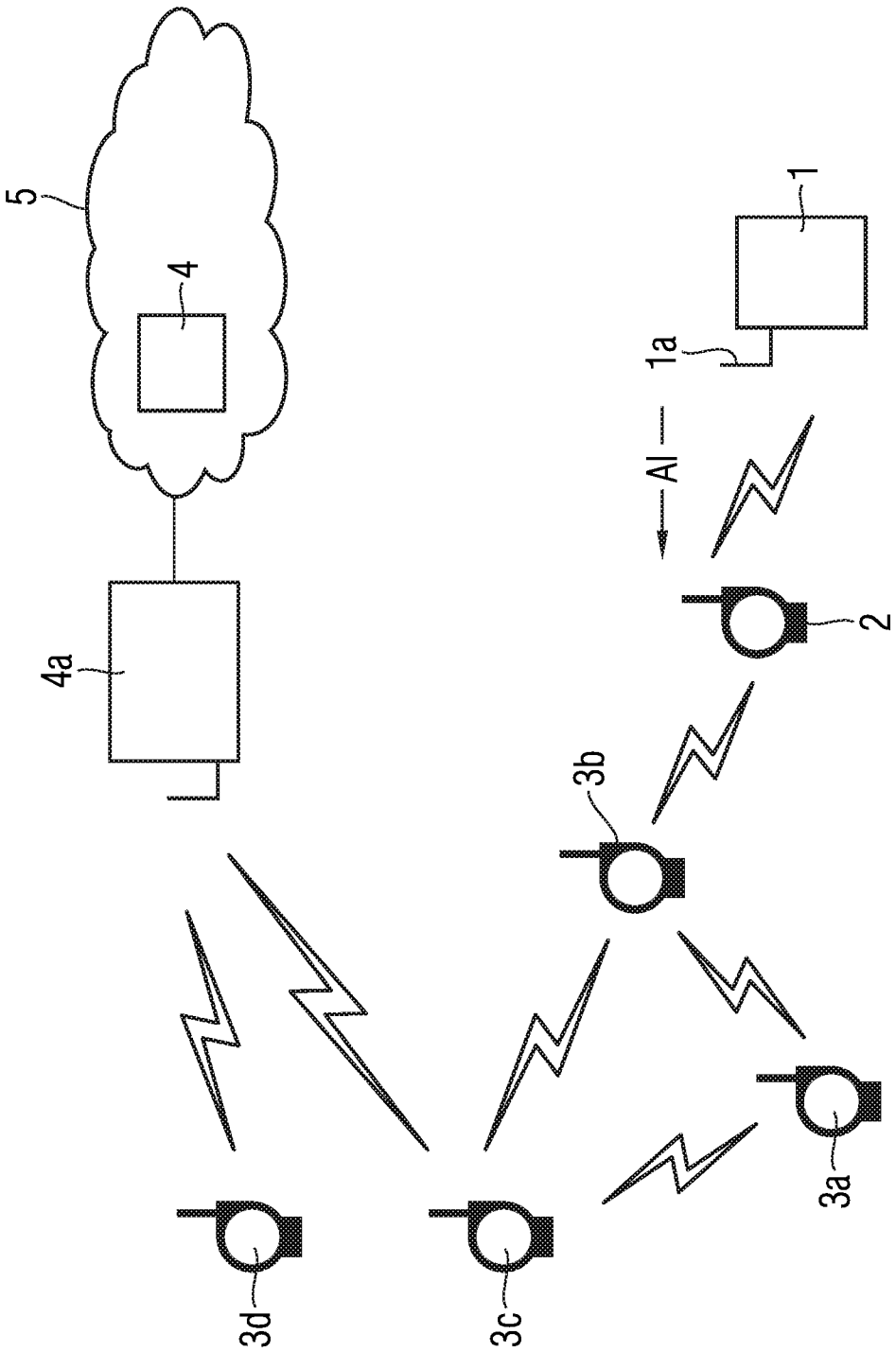


FIG 2A

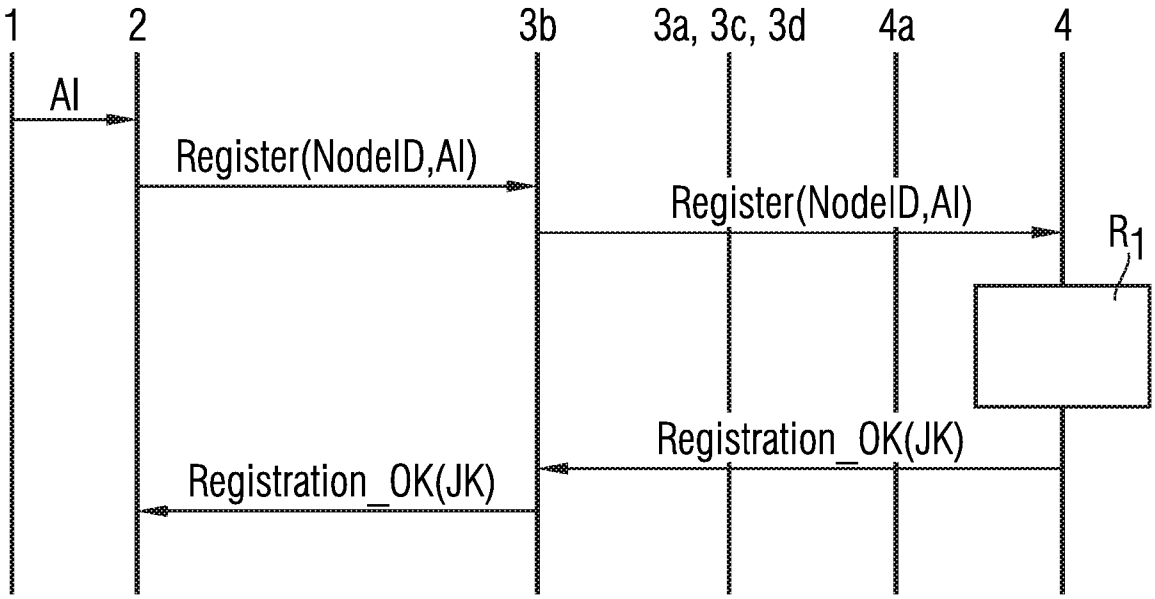

1
2
3b
3a, 3c, 3d
4a
4
AI
Register(NodeID,AI)
Register(NodeID,AI)
R1
Registration_OK(JK)
Registration_OK(JK)

FIG 2B

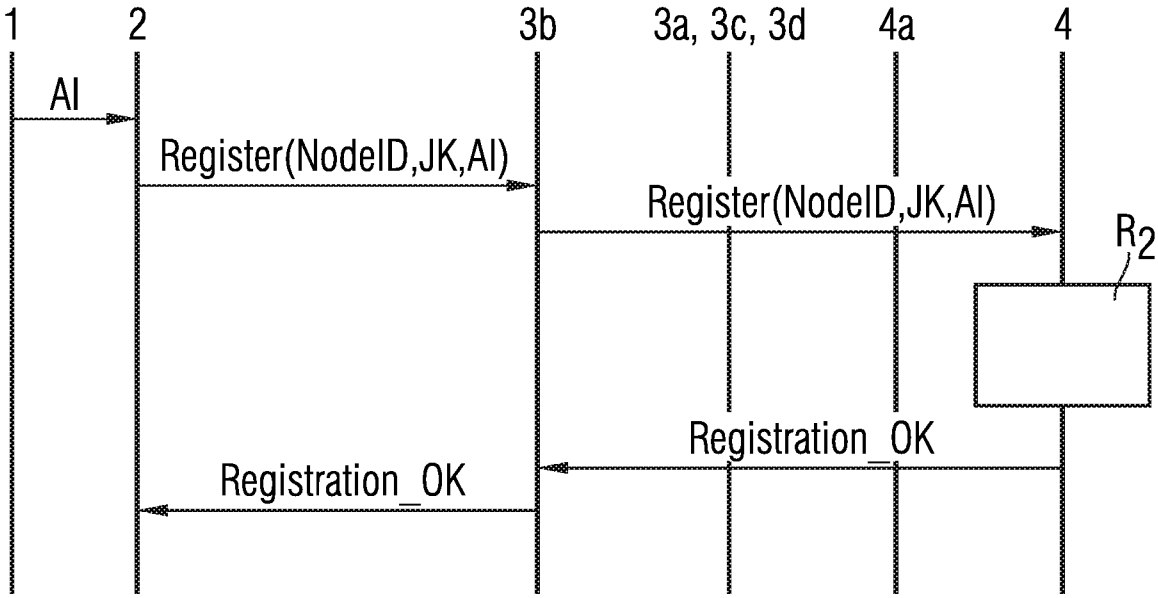
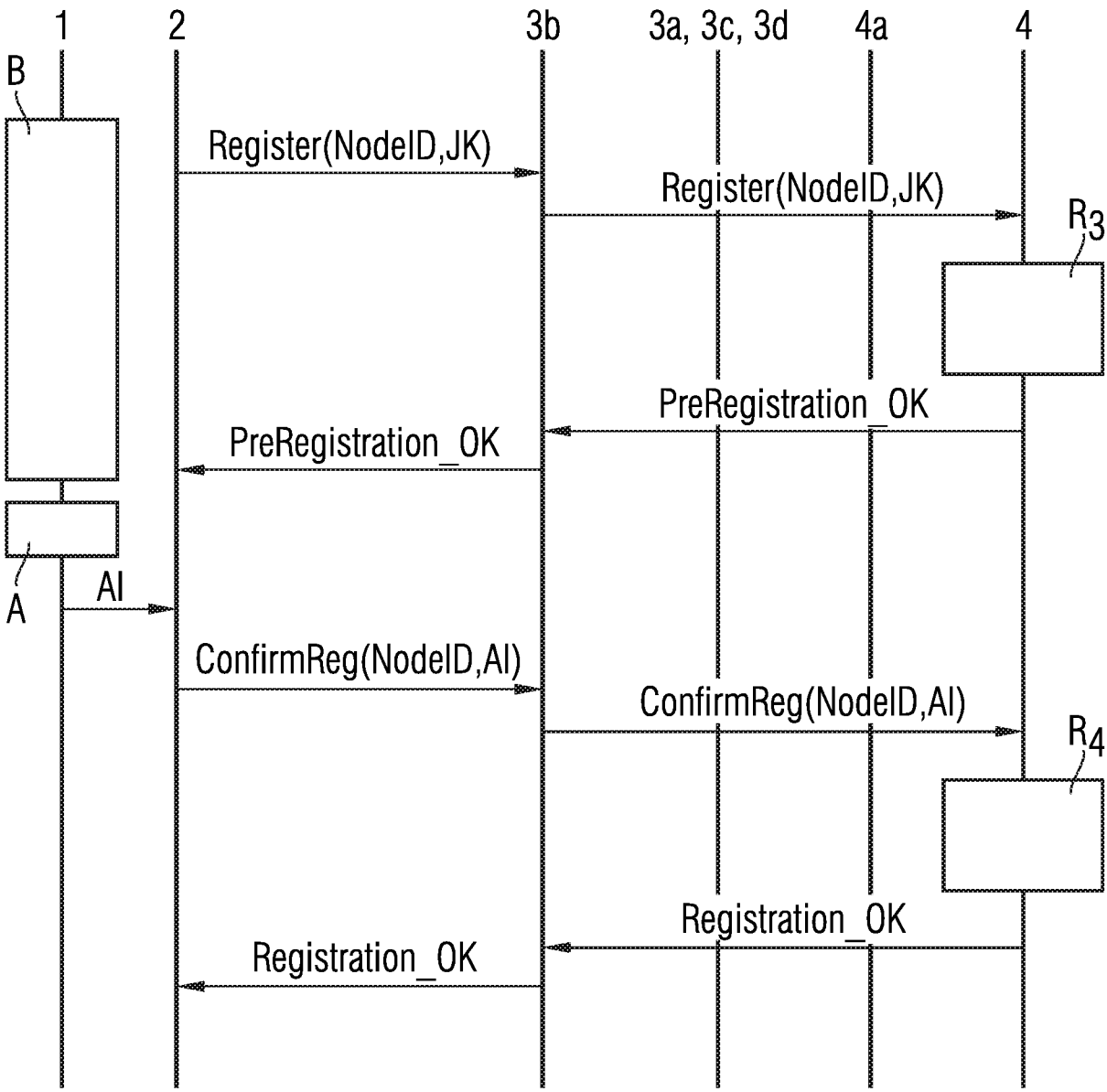

1
2
3b
3a, 3c, 3d
4a
4
AI
Register(NodeID,JK,AI)
Register(NodeID,JK,AI)
R2
Registration_OK
Registration_OK

FIG 3


1
2
3b
3a, 3c, 3d
4a
4
B
Register(NodeID,JK)
Register(NodeID,JK)
R3
PreRegistration_OK
PreRegistration_OK
A
AI
ConfirmReg(NodeID,AI)
ConfirmReg(NodeID,AI)
R4
Registration_OK
Registration_OK

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/060489

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06
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)
H04L 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 practical, search terms used)

EPO-Internal, COMPENDEX, INSPEC, PAJ, IBM-TDB, 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 2006/282885 A1 (COMBS HAROLD R [US] ET AL) 14 December 2006 (2006-12-14) abstract paragraph [0021] - paragraph [0030] figures 1-3	1-10
A	US 2005/117752 A1 (IIMA SHIN [JP] ET AL) 2 June 2005 (2005-06-02) abstract paragraph [0039] - paragraph [0041] figures 1, 12	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

"E" earlier document 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
25 August 2011	06/09/2011

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	Horn, Marc-Philipp

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/060489

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006282885 A1	14-12-2006	NONE	
US 2005117752 A1	02-06-2005	CN 1604526 A	06-04-2005
		JP 2005109720 A	21-04-2005
		KR 20050031409 A	06-04-2005
		US 2009088136 A1	02-04-2009

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2011/060489

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 H04W12/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L 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, COMPENDEX, INSPEC, PAJ, IBM-TDB, 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 2006/282885 A1 (COMBS HAROLD R [US] ET AL) 14. Dezember 2006 (2006-12-14) Zusammenfassung Absatz [0021] - Absatz [0030] Abbildungen 1-3 -----	1-10
A	US 2005/117752 A1 (IIMA SHIN [JP] ET AL) 2. Juni 2005 (2005-06-02) Zusammenfassung Absatz [0039] - Absatz [0041] Abbildungen 1, 12 -----	1-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ 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" älteres Dokument, 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 anderen 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
25. August 2011	06/09/2011

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	Horn, Marc-Philipp

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2011/060489

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2006282885 A1	14-12-2006	KEINE	
US 2005117752 A1	02-06-2005	CN 1604526 A	06-04-2005
		JP 2005109720 A	21-04-2005
		KR 20050031409 A	06-04-2005
		US 2009088136 A1	02-04-2009