

(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. März 2020 (26.03.2020)



(10) Internationale Veröffentlichungsnummer
WO 2020/058059 A1

(51) Internationale Patentklassifikation:

G07C 9/00 (2006.01) E05B 65/10 (2006.01)

BRUHN, Karen; c/o Continental Automotive GmbH, Thomas-Dehler-Str. 27, 81737 München (DE).

(21) Internationales Aktenzeichen: PCT/EP2019/074203

(74) **Anwalt: BONN, Roman**; Continental Automotive GmbH, Postfach 22 16 39, 80506 München (DE).

(22) Internationales Anmeldedatum:
11. September 2019 (11.09.2019)

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

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2018 215 835.5
18. September 2018 (18.09.2018) DE

(71) Anmelder: **CONTI TEMIC MICROELECTRONIC GMBH** [DE/DE]; Sieboldstraße 19, 90411 Nürnberg (DE).

(72) Erfinder: **KÄUFL, Georg**; c/o Continental Automotive GmbH, Thomas-Dehler-Str. 27, 81737 München (DE).

(54) Title: ACCESS SYSTEM AND ACCESS VERIFICATION METHOD

(54) Bezeichnung: ZUGANGSSYSTEM UND VERFAHREN ZUR ZUGANGSVERIFIZIERUNG

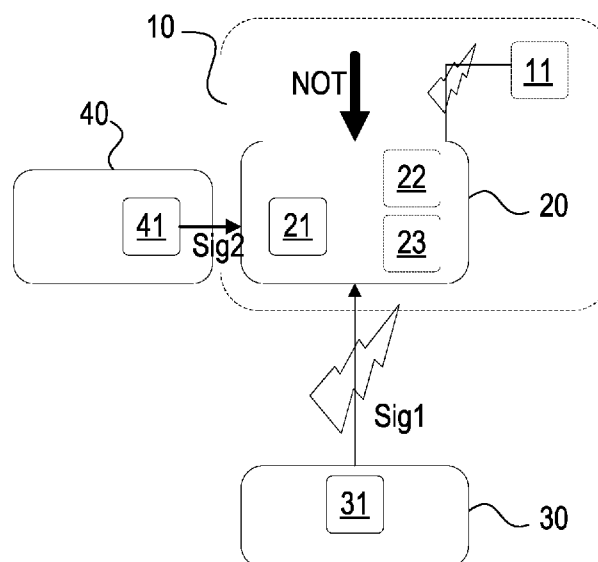


FIG 2

(57) **Abstract:** An access system comprises a control device (20) arranged in an object (10), wherein the control device (20) is designed to receive a first signal (NOT) in the event of a triggering event, which signal contains first information indicating an emergency situation, to store the first information, and to change from a normal state into an emergency state. The control device (20) is also designed to receive a second signal (Sig1, Sig2) from a wearable electronic device (30, 40). If the control device (20) is in the normal state, an authorisation of the wearable electronic device (30, 40) is checked based on the received second signal (Sig1, Sig2) and a first secret authentication key. If the control device (20) is in the emergency state, an authorisation of the wearable electronic device (30, 40) is checked based on the received second signal (Sig1, Sig2) and either a public key or a second secret authentication key. At least

(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)

one door of the object (10) is unlocked if an authorisation of the wearable electronic device (30, 40) is established.

(57) Zusammenfassung: Ein Zugangssystem weist ein in einem Objekt (10) angeordnetes Steuergerät (20) auf, wobei das Steuergerät (20) dazu ausgebildet ist, auf ein auslösendes Ereignis hin ein erstes Signal (NOT) zu empfangen, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt, die erste Information zu speichern, und von einem Normalzustand in einen Notzustand zu wechseln. Das Steuergerät (20) ist weiterhin dazu ausgebildet, ein zweites Signal (Sig1, Sig2) von einem tragbaren elektronischen Gerät (30, 40) zu empfangen. Wenn sich das Steuergerät (20) in dem Normalzustand befindet, wird eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und eines ersten geheimen Authentifizierungsschlüssels geprüft. Wenn sich das Steuergerät (20) in dem Notzustand befindet, wird eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und entweder eines öffentlichen Schlüssels oder eines zweiten geheimen Authentifizierungsschlüssels geprüft. Wenigstens eine Tür des Objektes (10) wird entriegelt, wenn eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) festgestellt wurde.

Beschreibung

Zugangssystem und Verfahren zur Zugangsverifizierung

- 5 Die Erfindung betrifft ein Zugangssystem und ein Verfahren zur Zugangsverifizierung, insbesondere ein System zur Notentriegelung eines Fahrzeugs.

Fahrzeuge werden heutzutage meist unter Verwendung elektro-
10 nischer Schlüssel entriegelt. Dabei wird entweder eine Entriegelungstaste am Schlüssel betätigt oder das Fahrzeug wird schlüssellos, also ohne jegliche Betätigung des Fahrzeugschlüssels, entriegelt wenn sich der vom Nutzer mitgeführte Fahrzeugschlüssel innerhalb einer bestimmten Reichweite um das
15 Fahrzeug befindet. Derartige schlüssellose Fahrzeugzugangssysteme werden auch als Keyless-Entry-Systeme bezeichnet. Immer häufiger übernehmen dabei auch tragbare elektronische Geräte wie beispielsweise Smartphones die Funktion des Fahrzeugschlüssels.

- 20 Im Falle eines Unfalls können derartige elektronisch entriegelte Schlösser („e-Schlösser“) häufig mit einem mechanischen Schlüssel notentriegelt werden. Um das Design der Fahrzeuge für die Nutzer noch ansprechender zu gestalten, weisen Fahrzeuge heutzutage jedoch teilweise keine Türgriffe und mechanischen
25 Schlösser mehr auf, so dass eine mechanische Entriegelung im Notfall nicht mehr möglich ist.

Andere Systeme sind bekannt, bei welchen im Falle eines Unfalls, z.B. wenn detektiert wurde, dass die Airbags ausgelöst wurden,
30 die Türschlösser automatisch entriegelt werden. Dies ist jedoch nur dann möglich, wenn die entsprechenden Türsteuergeräte zu diesem Zeitpunkt zum einen noch mit der Fahrzeugbatterie

verbunden sind und von dieser mit Energie versorgt werden.
Zusätzlich ist es auch erforderlich, dass das Türsteuergerät ein
entsprechendes Signal zum Öffnen der Türen noch empfangen kann.
Sind entsprechende Verbindungen im Fahrzeug abgerissen, ist ein
5 automatisches Entriegeln nicht mehr möglich.

Bei den bekannten Systemen besteht daher die Gefahr, dass
Rettungskräfte die Fahrzeugtüren im Falle eines Unfalls nicht
oder nur schwer öffnen, und im Fahrzeug befindliche Personen
10 nicht schnell genug retten können, wenn die Türschlösser noch
verriegelt sind.

Die Druckschrift DE 10 2016 209 379 A1 offenbart ein Fahrzeug dem
eine primäre Autorisierungsvorrichtung und eine sekundäre
15 Autorisierungsvorrichtung zur Autorisierung einer Bedienung des
Fahrzeugs zugeordnet sind. Die sekundäre Autorisierungsvor-
richtung weist dabei einen digitalen Hilfsschlüssel auf. Bei dem
Verfahren wird ein Aktivierungssignal durch die primäre Au-
torisierungsvorrichtung bereitgestellt, das repräsentativ ist
20 für eine Aktivierung des digitalen Hilfsschlüssels. Abhängig von
dem Aktivierungssignal wird die Autorisierung der Bedienung des
Fahrzeugs mittels des digitalen Hilfsschlüssels freigegeben und
im Falle eines Empfangs eines Autorisierungsanfragesignals durch
das Fahrzeug die Bedienung des Fahrzeugs abhängig von der
25 Freigabe und dem digitalen Hilfsschlüssel autorisiert.

Aufgabe der Erfindung ist es, ein Zugangssystem und ein kor-
respondierendes Verfahren zur Zugangsverifizierung bereitzu-
stellen, welches es Rettungskräften im Falle eines Unfalls
30 ermöglicht die Türschlösser zu entriegeln und verunfallte
Personen aus dem Fahrzeug zu retten.

Diese Aufgabe wird gelöst durch ein Zugangssystem gemäß Anspruch 1, ein Verfahren gemäß Anspruch 9, beziehungsweise ein Fahrzeug gemäß Anspruch 10.

- 5 Das erfindungsgemäße Zugangssystem weist ein in einem Objekt angeordnetes Steuergerät auf, wobei das Steuergerät dazu ausgebildet ist, auf ein auslösendes Ereignis hin ein erstes Signal zu empfangen, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt, die erste Information
- 10 zu speichern, und von einem Normalzustand in einen Notzustand zu wechseln. Das Steuergerät ist weiterhin dazu ausgebildet, ein zweites Signal von einem tragbaren elektronischen Gerät zu empfangen. Wenn sich das Steuergerät in dem Normalzustand befindet, wird eine Berechtigung des tragbaren elektronischen
- 15 Gerätes anhand des empfangenen zweiten Signals und eines ersten geheimen Authentifizierungsschlüssels geprüft, indem das empfangene zweite Signal mittels dem ersten geheimen Authentifizierungsschlüssel decodiert wird. Wenn sich das Steuergerät in dem Notzustand befindet, wird eine Berechtigung des tragbaren
- 20 elektronischen Gerätes anhand des empfangenen zweiten Signals und entweder eines öffentlichen Authentifizierungsschlüssels oder eines zweiten geheimen Authentifizierungsschlüssels geprüft, indem das empfangene zweite Signal entweder mittels dem öffentlichen Authentifizierungsschlüssel oder mittels dem
- 25 zweiten geheimen Authentifizierungsschlüssel decodiert wird. Wenigstens eine Tür des Objektes wird entriegelt, wenn eine Berechtigung des tragbaren elektronischen Gerätes festgestellt wurde.
- 30 Im Normalzustand können nur berechtigte tragbare elektronische Geräte das Objekt entriegeln, welche den ersten geheimen Authentifizierungsschlüssel kennen. Im Notzustand können auch

andere tragbare elektronische Geräte das Objekt entriegeln, welche im Normalzustand keine Berechtigung aufweisen. Dadurch können im Notzustand Rettungsmaßnahmen schneller erfolgen und in dem Objekt befindliche Personen schneller gerettet werden.

5

Der öffentliche Schlüssel und der zweite geheime Authentifizierungsschlüssel können sich von dem ersten geheimen Authentifizierungsschlüssel unterscheiden.

10 Dadurch ist es möglich, unterschiedliche tragbare Geräte in unterschiedlichen Situationen zu autorisieren das Objekt öffnen zu können.

Das Steuergerät kann dazu ausgebildet sein, im Normalzustand
15 betrieben zu werden, solange die erste Information nicht gespeichert wurde.

Das Objekt kann ein Fahrzeug sein, wobei das Steuergerät in dem Normalzustand von einer Fahrzeugbatterie mit Energie versorgt
20 wird, und wobei das Steuergerät einen Energiespeicher aufweist, der dazu ausgebildet ist das Steuergerät mit Energie zu versorgen, wenn die Verbindung des Steuergeräts mit der Fahrzeugbatterie getrennt wurde.

25 Das Steuergerät kann somit auch im Falle eines Unfalls, wenn die Verbindung zur Fahrzeugbatterie abgerissen ist, noch die Türen entriegeln.

Das tragbare elektronische Gerät kann beispielsweise ein Mobiltelefon, Tablet, SmartWatch, Laptop oder Personal Digital
30 Assistant sein.

Solche tragbaren Geräte werden heutzutage von den meisten Nutzern zusätzlich zu verschiedenen Schlüsseln mitgeführt oder ersetzen die Schlüssel komplett, indem sie die Funktion eines oder mehrerer Schlüssel übernehmen.

5

Das Signal von dem tragbaren Gerät kann über eine drahtlose Verbindung zwischen dem tragbaren Gerät und dem Steuergerät übertragen werden. Die meisten tragbaren Geräte verfügen bereits über entsprechende Schnittstellen und auch viele Objekte, z.B. Fahrzeuge, weisen verschiedenste Schnittstellen auf. Eine drahtlose Verbindung kann daher unter Verwendung bereits vorhandener Komponenten hergestellt werden.

Die drahtlose Verbindung kann eine Verbindung nach einem Bluetooth-Standard oder einem Nahfeldkommunikations-Standard sein. Solche Verbindungen werden häufig zur Übertragung von Signalen, bzw. zur Kommunikation zwischen zwei Geräten verwendet.

Das Objekt kann beispielsweise ein Bus, ein Lastkraftwagen, ein Gebäude oder eine Garage sein.

Ein Verfahren zur Zugangsverifizierung weist auf: mittels eines in einem Objekt angeordneten Steuergeräts, auf ein auslösendes Ereignis hin, Empfangen eines ersten Signals, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt,

Speichern der ersten Information, und Wechseln von einem Normalzustand in einen Notzustand; Empfangen eines zweiten Signals von einem tragbaren elektronischen Gerät; wenn sich das Steuergerät in dem Normalzustand befindet, Prüfen einer Berechtigung des tragbaren elektronischen Gerätes anhand des

empfangenen zweiten Signals und eines ersten geheimen Authentifizierungsschlüssels, indem das empfangene zweite Signal mittels dem ersten geheimen Authentifizierungsschlüssel decodiert wird; wenn sich das Steuergerät in dem Notzustand befindet, Prüfen einer Berechtigung des tragbaren elektronischen Gerätes anhand des empfangenen zweiten Signals und entweder eines öffentlichen Authentifizierungsschlüssels oder eines zweiten geheimen Authentifizierungsschlüssels, indem das empfangene zweite Signal entweder mittels dem öffentlichen Authentifizierungsschlüssel oder mittels dem zweiten geheimen Authentifizierungsschlüssel decodiert wird; und Entriegeln wenigstens einer Tür des Objektes, wenn eine Berechtigung des tragbaren elektronischen Gerätes festgestellt wurde.

Ein Fahrzeug weist ein Zugangssystem auf, wobei das Zugangssystem ein in einem Objekt angeordnetes Steuergerät aufweist, und wobei das Steuergerät dazu ausgebildet ist, auf ein auslösendes Ereignis hin ein erstes Signal zu empfangen, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt, die erste Information zu speichern, und von einem Normalzustand in einen Notzustand zu wechseln. Das Steuergerät ist weiterhin dazu ausgebildet, ein zweites Signal von einem tragbaren elektronischen Gerät zu empfangen. Wenn sich das Steuergerät in dem Normalzustand befindet, wird eine Berechtigung des tragbaren elektronischen Gerätes anhand des empfangenen zweiten Signals und eines ersten geheimen Authentifizierungsschlüssels geprüft, indem das empfangene zweite Signal mittels dem ersten geheimen Authentifizierungsschlüssel decodiert wird. Wenn sich das Steuergerät in dem Notzustand befindet, wird eine Berechtigung des tragbaren elektronischen Gerätes anhand des empfangenen zweiten Signals und entweder eines öffentlichen Authentifizierungsschlüssels oder eines zweiten geheimen Authentifi-

zierungsschlüssels geprüft, indem das empfangene zweite Signal entweder mittels dem öffentlichen Authentifizierungsschlüssel oder mittels dem zweiten geheimen Authentifizierungsschlüssel decodiert wird. Wenigstens eine Tür des Objektes wird entriegelt, wenn eine Berechtigung des tragbaren elektronischen Gerätes festgestellt wurde.

Die Erfindung wird nachfolgend anhand der in den Figuren der Zeichnung dargestellten Ausführungsbeispiele näher erläutert. Es zeigt:

Figur 1 beispielhaft ein Fahrzeug mit einem Zugangssystem,

Figur 2 beispielhaft in einem Blockschaltbild ein Zugangssystem gemäß einer Ausführungsform, und

Figur 3 in einem Ablaufdiagramm ein Verfahren gemäß einer Ausführungsform.

Figur 1 zeigt in schematischer Darstellung das grundsätzliche Prinzip eines schlüssellosen Fahrzeug-Zugangs- und Startsystems. In dem Fahrzeug 10 ist ein Steuergerät 20 angeordnet, das dazu ausgebildet ist, Signale auszusenden. Dies sind beispielsweise elektromagnetische Signale im LF (Low Frequency)- oder HF (High Frequency)-Bereich. Diese Signale werden von einer Transpondereinheit 30 empfangen, wenn diese sich in der Nähe des Fahrzeugs 10 befindet, und anschließend ausgewertet und/oder weiter verarbeitet. Im Anschluss an die Auswertung und/oder Weiterverarbeitung in der Transpondereinheit 30 können entsprechende Antwortsignale wieder an das Steuergerät 20 zurückgesendet werden. Die Antwortsignale werden beispielsweise im UHF-Frequenzband gesendet und können im Fahrzeug 10 von dem

Steuergerät 20 oder einer mit dem Steuergerät 20 verbundenen Auswerteeinheit ausgewertet werden. Die Transpondereinheit 30 kann beispielsweise in einem elektronischen Fahrzeugschlüssel angeordnet sein, welchen der Fahrer des Fahrzeugs 10 mit sich führt. Die zwischen dem Fahrzeug 10 und der Transpondereinheit 30 gesendeten Signale können beispielsweise auch Signale gemäß einem Nahfeldkommunikationsstandard (NFC) oder gemäß einem Bluetooth-Standard, zum Beispiel dem Bluetooth Low Energy (BLE)-Standard sein.

10

NFC ermöglicht einen kontaktlosen Datenaustausch zwischen Geräten über eine Distanz von wenigen Zentimetern, z.B. weniger als 20cm oder weniger als 10cm. Mittels NFC können bis zu 424 kBit/s übertragen werden. Bei der Nahfeldkommunikation erfolgt der Datenaustausch über eine induktive Kopplung zwischen zwei Induktivitäten (z.B. Antennen). Die Induktivität eines Kommunikationsgerätes fungiert dabei als sogenannter Initiator, die Induktivität des anderen Kommunikationsgerätes als sogenanntes Target. Die elektro-magnetischen Felder strahlen mit einer Frequenz von 13,56MHz vom Initiator zum Target.

20

Zum Empfangen der von dem Steuergerät 20 gesendeten Signale muss sich die Transpondereinheit 30 innerhalb eines bestimmten Radius um das Fahrzeug 10 befinden, da sowohl Signale im LF- und HF-Bereich als auch NFC- und BLE-Signale nur eine begrenzte Reichweite haben. Dieser Radius kann, in Abhängigkeit vom gewählten Übertragungsstandard, zum Beispiel 10cm, 2m, 5m oder 10m betragen. Dies sind jedoch lediglich Beispiele. Die Reichweite kann, abhängig von den verwendeten Signalen und Antennen, auch größer oder kleiner sein.

25

30

Das Steuergerät 20 kann kontinuierlich Signale aussenden oder nur auf ein bestimmtes Ereignis hin. Ein solches Ereignis kann beispielsweise das Berühren oder Betätigen eines Türgriffes oder eines Fahrzeug-Startknopfes sein. Jegliche andere geeignete Art von Ereignis ist ebenfalls möglich. Sendet die Transpondereinheit 30 auf ein von dem Steuergerät 20 empfangenes Signal ein korrektes Antwort-signal, wird das Fahrzeug 10 entriegelt.

Die zwischen dem Steuergerät 20 und der Transpondereinheit 30 gesendeten Signale können beispielsweise mittels eines geheimen Authentifizierungsschlüssels codiert werden. Gemäß einem Beispiel wird über mindestens eine am Fahrzeug befindliche Antenne ein mittels einer ersten Codiertabelle codiertes Anfragesignal ausgesendet. Befindet sich der zu dem Fahrzeug 10 gehörige Fahrzeugschlüssel 30 innerhalb der Reichweite der Anfragesignale, empfängt dieser das Anfragesignal, decodiert es und sendet es unter Verwendung einer zweiten Codiertabelle mit einer neuen Codierung wieder aus. Das Antwortsignal wird im Fahrzeug 10 mittels eines geheimen Authentifizierungsschlüssels decodiert. Da das Fahrzeug 10 beide Codiertabellen kennt, kann es die eigene ursprüngliche Aussendung mit dem gerade empfangenen Antwortsignal vergleichen. Stimmen diese überein, kann das Fahrzeug 10 entriegelt werden.

Bei dem anhand Figur 1 beschriebenen Zugangssystem besteht die Gefahr, dass im Falle eines Unfalls des Fahrzeugs 10, die Fahrzeugtüren nicht mehr entriegelt werden können. Viele Fahrzeuge verriegeln die Fahrzeugtüren beispielsweise automatisch sobald das Fahrzeug eine bestimmte Geschwindigkeit überschritten hat. Verletzte und eingeklemmte Personen können dann beispielsweise von Rettungskräften nur sehr schwer befreit werden. Erschwerend kann hierbei hinzukommen, dass viele

Fahrzeuge heutzutage keine Türgriffe und/oder mechanischen Türschlösser mehr aufweisen, so dass ein Entriegeln mittels eines mechanischen Schlüssels nicht mehr möglich ist.

5 Bezugnehmend auf Figur 2 wird anhand eines Blockschaltbildes ein Zugangssystem gemäß einem Beispiel beschrieben. In dem Blockschaltbild ist schematisch das in einem Fahrzeug 10 angeordnete Steuergerät 20 dargestellt. Das Steuergerät 20 kann beispielsweise eine erste Kommunikationseinheit 21 aufweisen.
10 Die Kommunikationseinheit 21 kann beispielsweise eine Antenne aufweisen, die dazu ausgebildet ist Signale auszusenden und zu empfangen.

Das Steuergerät 20 kann in zwei verschiedenen Betriebsmodi
15 betrieben werden. Ein erster Betriebsmodus ist dabei ein Normalzustand. Ein zweiter Betriebsmodus ist ein Notzustand. Liegt eine Notsituation vor, kann das Steuergerät 20 ein Signal NOT empfangen, welches eine Information darüber enthält, dass eine Notsituation vorliegt. Eine Notsituation kann bei-
20 spielsweise vorliegen, wenn das Fahrzeug 10 verunfallt ist. Das Signal NOT kann beispielsweise von anderen im Fahrzeug 10 angeordneten Komponenten oder Steuergeräten ausgesendet werden. Beispielsweise kann eine Airbag-Steuereinheit ein Signal NOT an das Steuergerät 20 senden, wenn einer oder mehrere Airbags
25 ausgelöst wurden. Ein Signal NOT kann beispielsweise auch ausgesendet werden, wenn eine Verbindung wichtiger Komponenten zu der Fahrzeugbatterie getrennt wurde. Jegliche andere geeignete auslösende Ereignisse sind dabei ebenfalls möglich. Die Information, dass eine Notsituation vorliegt, kann von dem
30 Steuergerät 20 gespeichert werden. Beispielsweise kann das Steuergerät 20 einen internen oder externen Speicher aufweisen, in welchem die Information gespeichert wird. Das Steuergerät 20

kann solange im Notzustand verbleiben, solange die Information gespeichert ist. Von autorisierten Personen, beispielsweise einem Nutzer oder einer autorisierten Werkstatt, kann die Information beispielsweise wieder gelöscht werden wenn keine
5 Notsituation mehr vorliegt und das Steuergerät 20 kann in den Normalzustand zurückkehren.

Empfängt das Steuergerät 20 ein Signal Sig1, Sig2 von einem tragbaren elektronischen Gerät 30, 40, verwendet es, solange es
10 sich im Normalzustand befindet, einen ersten geheimen Authentifizierungsschlüssel um die Authentizität des Signals Sig1, Sig2 bzw. des Gerätes 30, 40 zu prüfen. Im Normalzustand kann dabei nur ein berechtigter Fahrzeugschlüssel, also ein zum Fahrzeug 10 gehöriger Schlüssel, als berechtigt erkannt werden.
15 Anderen elektronischen Geräten 40 ist der geheime Authentifizierungsschlüssel nicht bekannt. Empfängt das Steuergerät 20 im Normalzustand ein Signal Sig2 von einem unberechtigten tragbaren Gerät 40, bleibt das Fahrzeug 10 verschlossen. Das Fahrzeug 10 wird nur dann entriegelt, wenn ein tragbares Gerät
20 30, 40 als berechtigt erkannt wird.

Empfängt das Steuergerät 20 ein Signal Sig1, Sig2 von einem tragbaren elektronischen Gerät 30, 40 und befindet sich im Notzustand, kann es zur Authentifizierung einen unterschied-
25 lichen Schlüssel verwenden. Dies kann beispielsweise ein öffentlicher Schlüssel oder ein zweiter geheimer Schlüssel sein.

Handelt es sich um einen öffentlichen Schlüssel, kann das Fahrzeug 10 von jedem geeigneten tragbaren Gerät 40 entriegelt
30 werden. Im Falle eines Unfalls ist das tragbare elektronische Gerät 40 in der Regel ein Gerät 40, beispielsweise eines Passanten oder von Rettungskräften, welches im Normalzustand nicht be-

rechtigt ist das Fahrzeug 10 zu entriegeln. Beispielsweise kann der öffentliche Schlüssel ein allgemeiner NFC-Schlüssel sein. Das Fahrzeug 10 kann dann beispielsweise entriegelt werden, wenn ein beliebiges NFC-Signal von einem NFC-fähigen Gerät 40
5 empfangen wurde. Das tragbare Gerät 40 muss in diesem Fall lediglich eine Kommunikationseinheit 41 aufweisen, welche nach dem notwendigen Standard, z.B. NFC-Standard, kommunizieren kann. Eine weitere Authentifizierung findet nicht statt.

10 Der während des Notzustands verwendete unterschiedliche Schlüssel kann jedoch beispielsweise auch ein zweiter geheimer Authentifizierungsschlüssel sein. Dieser zweite geheime Authentifizierungsschlüssel kann beispielsweise nur tragbaren
15 Geräten bestimmter Organisationen bekannt sein, z.B. Feuerwehr, Rotes Kreuz, Technisches Hilfswerk, o.ä. Das Fahrzeug 10 könnte dann nicht von jedem beliebigen tragbaren Gerät 40 entriegelt werden, sondern nur von tragbaren Geräten 40 von Rettungskräften berechtigter Organisationen. Entsprechende Schlüssel könnten
20 beispielsweise beim Kauf eines Fahrzeugs 10 automatisch an entsprechende Rettungsdienste weitergeleitet werden. Die entsprechenden Schlüssel könnten dort in einer Datenbank gespeichert und im Notfall abgerufen werden. Beispielsweise könnte auf dem tragbaren Gerät 40 der Rettungskräfte eine entsprechende Applikation installiert sein.

25

Bei dem beispielhaften Zugangssystem werden somit im Normalzustand und im Notzustand unterschiedliche Authentifizierungsschlüssel verwendet. Im Normalzustand wird ein erster geheimer Authentifizierungsschlüssel verwendet, welcher in der
30 Regel nur zum Fahrzeug 10 gehörigen tragbaren Geräten 30 bekannt ist. Im Notzustand wird entweder ein öffentlicher Schlüssel oder ein zweiter geheimer Authentifizierungsschlüssel verwendet,

welche sich beide von dem ersten geheimen Authentifizierungsschlüssel unterscheiden.

Das tragbare Gerät 30, 40 kann beispielsweise ein Mobiltelefon, Tablet, SmartWatch, Laptop oder Personal Digital Assistant (PDA) sein. Um mit dem Steuergerät 20 kommunizieren zu können kann eine drahtlose Verbindung zwischen dem tragbaren Gerät 30, 40 und dem Steuergerät 20 hergestellt werden. Die drahtlose Verbindung kann beispielsweise eine Bluetooth-Verbindung sein. Es ist jedoch auch möglich, dass das tragbare Gerät 30, 40 mittels NFC (Nahfeldkommunikation, engl. Near Field Communication) oder jeglicher anderer geeigneter drahtloser Verbindung mit dem Steuergerät 20 kommuniziert.

Wird beispielsweise NFC zur Kommunikation zwischen dem tragbaren elektronischen Gerät 30, 40 und dem Fahrzeug 10 verwendet, ist die Reichweite der Signale, wie oben bereits erläutert, eingeschränkt. In diesem Fall wäre es erforderlich, dass das tragbare elektronische Gerät 30, 40 mit der entsprechenden Kommunikationseinheit 31, 41 in die Nähe der Kommunikationseinheit 21 des Steuergerätes gebracht wird. Hierfür könnte am Fahrzeug 10 eine entsprechende Markierung angebracht werden, damit Nutzer und Rettungskräfte wissen, in welchem Bereich sich das Steuergerät 20 befindet.

Das Steuergerät 20 kann in dem Normalzustand beispielsweise von einer Fahrzeugbatterie 11 mit Energie versorgt werden. Das Steuergerät 20 kann optional jedoch auch einen eigenen Energiespeicher 23 aufweisen, der dazu ausgebildet ist das Steuergerät 20 mit Energie zu versorgen, wenn die Verbindung des Steuergeräts 20 mit der Fahrzeugbatterie 11 getrennt wurde. Das Steuergerät 20 kann optional auch eine Notentriegelungseinheit

22 aufweisen. Die Notentriegelungseinheit 22 kann beispielsweise den oder die öffentlichen oder geheimen Authentifizierungsschlüssel aufweisen, welche im Notzustand verwendet werden. Im Normalzustand kann die Notentriegelungseinheit 22 deaktiviert
5 sein. Das Steuergerät 20 kann im Normalzustand dann beispielsweise dem in Figur 1 erläuterten Steuergerät 20 entsprechen. Im Notzustand kann die Notentriegelungseinheit 22 aktiviert werden und die Authentifizierung übernehmen. Die Notentriegelungseinheit 22 kann beispielsweise mit dem Ener-
10 giespeicher 23 verbunden sein und von diesem mit Energie versorgt werden. Das Freigeben des öffentlichen Schlüssels und/oder des zweiten geheimen Schlüssels im Notzustand kann beispielsweise mittels einer entsprechenden Software erfolgen.

15 Das Zugangssystem kann auch in anderen Bereichen zum Einsatz kommen und ist nicht auf die Anwendung in Fahrzeugen beschränkt. Insbesondere ist das Zugangssystem nicht auf die Anwendung in Personenkraftwagen beschränkt. Beispielsweise kann das Zu-
gangssystem auch zum Öffnen und/oder Schließen von Bussen,
20 Lastkraftwägen, Gebäuden oder Garagen verwendet werden.

Auch viele Gebäude werden heutzutage bereits mittels tragbarer elektronischer Geräte anstatt herkömmlicher Schlüssel ent-
riegelt. In einem Notfall, z.B. Brand, könnten Rettungskräfte mit
25 dem oben beschriebenen Zugangssystem schnell in Gebäude gelangen um notwendige Rettungsmaßnahmen durchführen zu können. Ein in einem Objekt angeordnetes Steuergerät 20 könnte beispielsweise in den Notzustand wechseln, wenn Rauchmelder ausgelöst wurden. Andere geeignete auslösende Ereignisse sind ebenfalls möglich.

30 Die in Figur 2 schematisch in einem Blockschaltbild dargestellten Komponenten können daher nicht nur in oder an einem Fahrzeug,

insbesondere einem Personenkraftwagen, angeordnet sein.

Vielmehr kann ein Steuergerät 20 beispielsweise auch in einem Bus oder einem Lastkraftwagen oder einem Gebäude angeordnet sein. Allgemein gesagt kann das Steuergerät 20 überall dort angebracht
5 werden, wo mittels eines elektronischen Schlüssels Türen oder Zugänge ent- oder verriegelt werden sollen.

Figur 3 zeigt anhand eines Ablaufdiagramms das Prinzip eines Verfahrens zur Zugangsverifizierung. Bei dem Verfahren wird
10 mittels eines in einem Objekt 10 angeordneten Steuergeräts 20, auf ein auslösendes Ereignis hin, ein erstes Signal NOT empfangen, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt. Die erste Information wird gespeichert, und das Steuergerät wechselt von einem Normalzustand in einen
15 Notzustand. Wird ein zweites Signal Sig1, Sig2 von einem tragbaren elektronischen Gerät 30, 40 empfangen (Schritt 301), wird geprüft, ob sich das Steuergerät in dem Normalzustand oder in dem Notzustand befindet (Schritt 302). Wenn sich das Steuergerät 20 in dem Normalzustand befindet, wird eine Be-
20 rechtigung des tragbaren elektronischen Gerätes 30, 40 anhand des empfangenen zweiten Signals Sig1, Sig2 und eines ersten geheimen Authentifizierungsschlüssels überprüft (Schritt 303). Handelt es sich um ein berechtigtes Gerät, wird das Objekt entriegelt (Schritt 306). Ist das Gerät 30, 40 nicht berechtigt passiert
25 nichts und das Objekt bleibt verschlossen (Schritt 305).

Wenn sich das Steuergerät 20 in dem Notzustand befindet, wird eine Berechtigung des tragbaren elektronischen Gerätes 30, 40 anhand des empfangenen zweiten Signals Sig1, Sig2 und entweder eines
30 öffentlichen Schlüssels oder eines zweiten geheimen Authentifizierungsschlüssels durchgeführt (Schritt 307). Handelt es sich um ein berechtigtes Gerät, wird das Objekt entriegelt

(Schritt 306). Ist das Gerät 30, 40 nicht berechtigt passiert nichts und das Objekt bleibt verschlossen (Schritt 305).

Bezugszeichenliste

	10	Fahrzeug
	11	Fahrzeugbatterie
5	20	Steuergerät
	21	Kommunikationseinheit
	22	Notentriegelungseinheit
	23	Energiespeicher
	30	erstes tragbares Gerät
10	31	Kommunikationseinheit
	40	zweites tragbares Gerät
	41	Kommunikationseinheit
	NOT	erstes Signal
	Sig1, Sig2	zweites Signal
15		

Patentansprüche

1. Zugangssystem mit einem in einem Objekt (10) angeordneten Steuergerät (20), wobei das Steuergerät (20) dazu ausgebildet ist,

auf ein auslösendes Ereignis hin ein erstes Signal (NOT) zu empfangen, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt, die erste Information zu speichern, und von einem Normalzustand in einen Notzustand zu wechseln;

ein zweites Signal (Sig1, Sig2) von einem tragbaren elektronischen Gerät (30, 40) zu empfangen;

wenn sich das Steuergerät (20) in dem Normalzustand befindet, eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und eines ersten geheimen Authentifizierungsschlüssels zu prüfen indem das empfangene zweite Signal (Sig1, Sig2) mittels dem ersten geheimen Authentifizierungsschlüssel decodiert wird;

wenn sich das Steuergerät (20) in dem Notzustand befindet, eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und entweder eines öffentlichen Authentifizierungsschlüssels oder eines zweiten geheimen Authentifizierungsschlüssels zu prüfen indem das empfangene zweite Signal (Sig1, Sig2) entweder mittels dem öffentlichen Authentifizierungsschlüssel oder mittels dem zweiten geheimen Authentifizierungsschlüssel decodiert wird; und

wenigstens eine Tür des Objektes (10) zu entriegeln, wenn eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) festgestellt wurde.

2. Zugangssystem nach Anspruch 1 wobei sich der öffentliche Schlüssel und der zweite geheime Authentifizierungsschlüssel von dem ersten geheimen Authentifizierungsschlüssel unterscheiden.

5 3. Zugangssystem nach Anspruch 1 oder 2, wobei das Steuergerät (20) dazu ausgebildet ist im Normalzustand betrieben zu werden, solange die erste Information nicht gespeichert wurde.

10 4. Zugangssystem nach einem der vorhergehenden Ansprüche, wobei das Objekt (10) ein Fahrzeug ist;
wobei das Steuergerät (20) in dem Normalzustand von einer Fahrzeugbatterie (11) mit Energie versorgt wird; und
wobei das Steuergerät (20) einen Energiespeicher (23) aufweist, der dazu ausgebildet ist das Steuergerät (20) mit
15 Energie zu versorgen, wenn die Verbindung des Steuergeräts (20) mit der Fahrzeugbatterie (11) getrennt wurde.

5. Zugangssystem nach einem der vorherigen Ansprüche, wobei das tragbare elektronische Gerät (30, 40) ein Mobiltelefon,
20 Tablet, SmartWatch, Laptop oder Personal Digital Assistant ist.

6. Zugangssystem nach einem der vorhergehenden Ansprüche, wobei das zweite Signal (Sig1, Sig2) von dem tragbaren elektronischen Gerät (30, 40) über eine drahtlose Verbindung
25 zwischen dem tragbaren elektronischen Gerät (30, 40) und dem Steuergerät (20) übertragen wird.

7. Zugangssystem nach Anspruch 6, wobei die drahtlose Verbindung eine Verbindung nach einem Nahfeldkommunikations-Standard oder einem Bluetooth-Standard ist.
30

8. Zugangssystem nach einem der vorhergehenden Ansprüche, wobei das Objekt (10) ein Bus, ein Lastkraftwagen, ein Gebäude oder eine Garage ist.

5 9. Verfahren zur Zugangsverifizierung, wobei das Verfahren aufweist:

mittels eines in einem Objekt (10) angeordneten Steuergeräts (20), auf ein auslösendes Ereignis hin, Empfangen eines ersten Signals (NOT), welches eine erste Information darüber
10 enthält, dass eine Notsituation vorliegt, Speichern der ersten Information, und Wechseln von einem Normalzustand in einen Notzustand;

Empfangen eines zweiten Signals (Sig1, Sig2) von einem tragbaren elektronischen Gerät (30, 40);

15 wenn sich das Steuergerät (20) in dem Normalzustand befindet, Prüfen einer Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und eines ersten geheimen Authentifizierungsschlüssels, indem das empfangene zweite Signal (Sig1, Sig2) mittels dem
20 ersten geheimen Authentifizierungsschlüssel decodiert wird;

wenn sich das Steuergerät (20) in dem Notzustand befindet, Prüfen einer Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und
25 entweder eines öffentlichen Authentifizierungsschlüssels oder eines zweiten geheimen Authentifizierungsschlüssels, indem das empfangene zweite Signal (Sig1, Sig2) entweder mittels dem öffentlichen Authentifizierungsschlüssel oder mittels dem zweiten geheimen Authentifizierungsschlüssel decodiert wird;
und

30 Entriegeln wenigstens einer Tür des Objektes (10), wenn eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) festgestellt wurde.

10. Fahrzeug (10) mit einem Zugangssystem, wobei das Zugangssystem ein in einem Objekt (10) angeordnetes Steuergerät (20) aufweist, und wobei das Steuergerät (20) dazu ausgebildet ist,

5 auf ein auslösendes Ereignis hin ein erstes Signal (NOT) zu empfangen, welches eine erste Information darüber enthält, dass eine Notsituation vorliegt, die erste Information zu speichern, und von einem Normalzustand in einen Notzustand zu wechseln;
ein zweites Signal (Sig1, Sig2) von einem tragbaren elektronischen Gerät (30, 40) zu empfangen;

10 wenn sich das Steuergerät (20) in dem Normalzustand befindet, eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und eines ersten geheimen Authentifizierungsschlüssels zu prüfen, indem das empfangene zweite Signal (Sig1, Sig2) mittels dem ersten geheimen Authentifizierungsschlüssel decodiert wird;

15 wenn sich das Steuergerät (20) in dem Notzustand befindet, eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) anhand des empfangenen zweiten Signals (Sig1, Sig2) und entweder eines öffentlichen Authentifizierungsschlüssels oder eines zweiten geheimen Authentifizierungsschlüssels zu prüfen, indem das empfangene zweite Signal (Sig1, Sig2) entweder mittels dem öffentlichen Authentifizierungsschlüssel oder mittels dem zweiten geheimen Authentifizierungsschlüssel decodiert wird;
20 und

25 wenigstens eine Tür des Objektes (10) zu entriegeln, wenn eine Berechtigung des tragbaren elektronischen Gerätes (30, 40) festgestellt wurde.

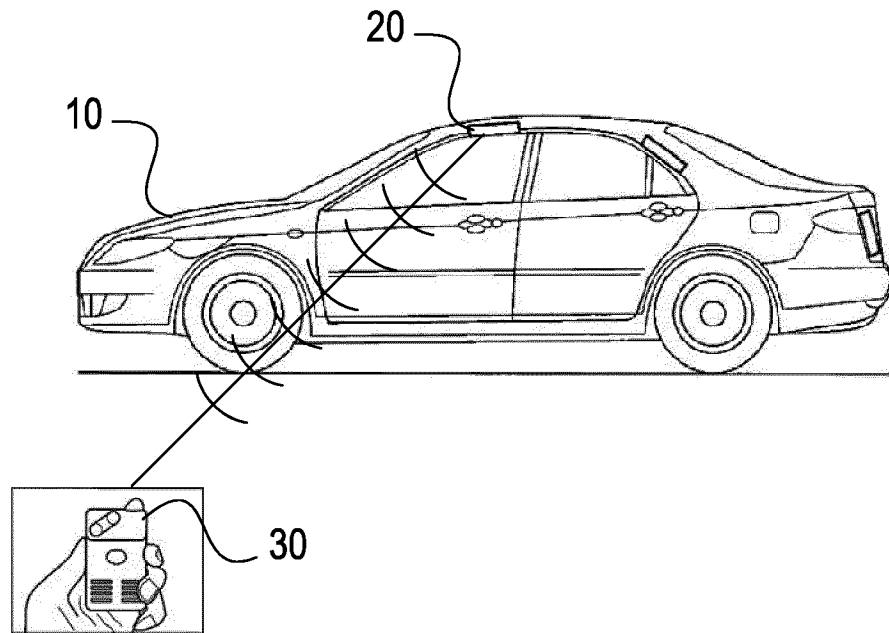


FIG 1

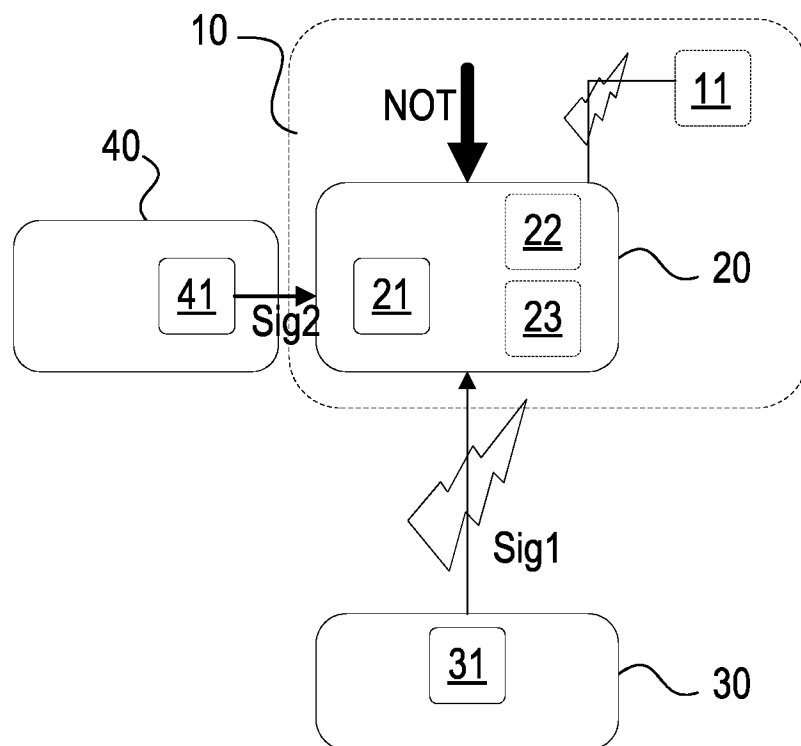
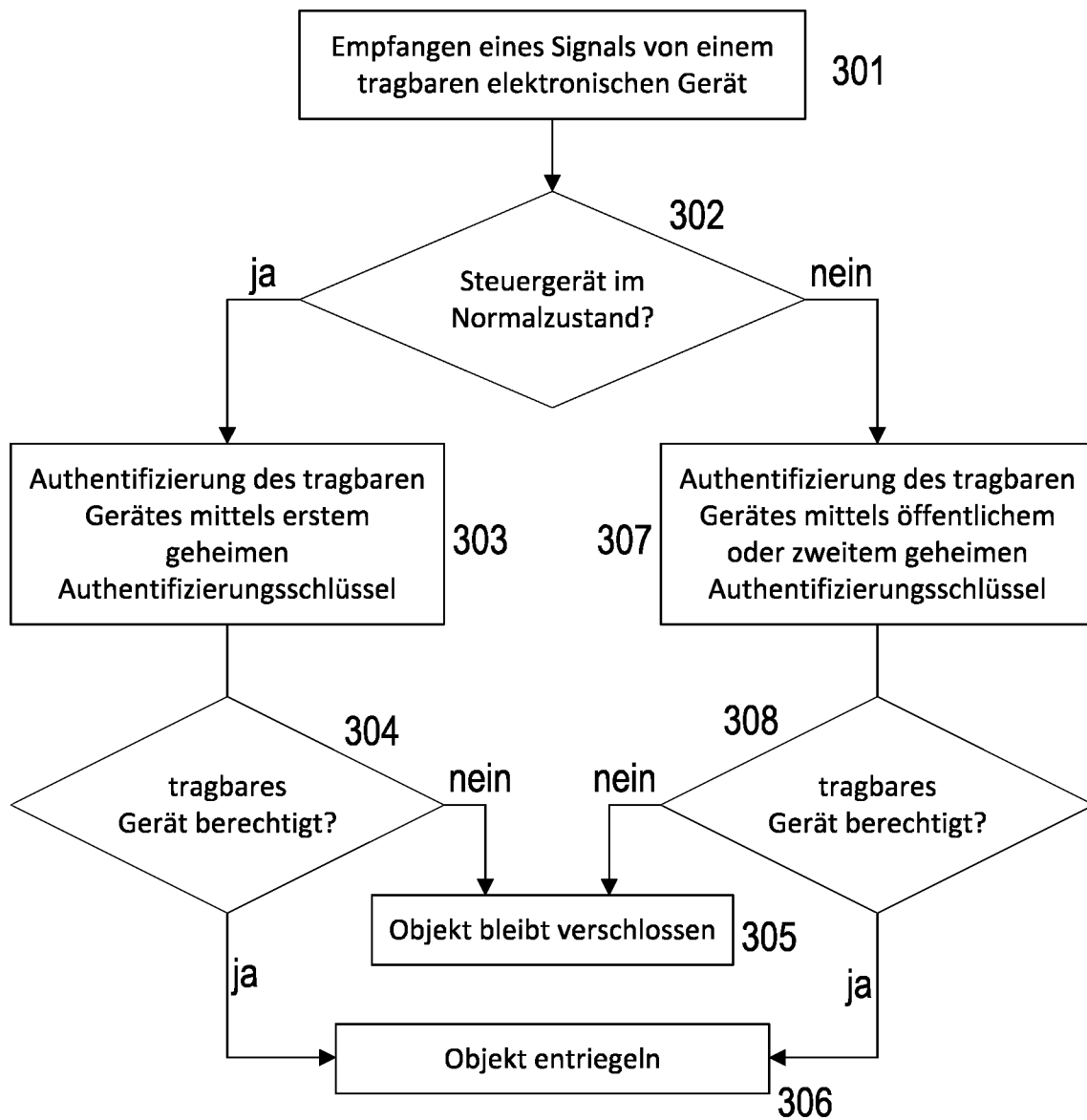


FIG 2

**FIG 3**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2019/074203

A. CLASSIFICATION OF SUBJECT MATTER**G07C 9/00**(2006.01)i; **E05B 65/10**(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07C; H04W; E05C; E05B; B60R

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016343187 A1 (TRANI JAMES [US]) 24 November 2016 (2016-11-24) paragraph [0013] - paragraph [0021] paragraph [0030] paragraph [0053] - paragraph [0063]	1-10
X	GB 2517527 A (DINKY ASSETS LTD [GB]) 25 February 2015 (2015-02-25) page 4 page 9 page 22 - page 23	1-9
X	EP 1158466 A1 (INVENTIO AG [CH]) 28 November 2001 (2001-11-28) paragraph [0024] - paragraph [0044] page 9 page 22 - page 23	1-9
A	US 2018118166 A1 (MUELLER KARL [DE] ET AL) 03 May 2018 (2018-05-03) paragraph [0007]	4
A	US 2009027194 A1 (MCGRATH LEIGH JASON [AU]) 29 January 2009 (2009-01-29) paragraph [0014]	4

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

“&” document member of the same patent family

Date of the actual completion of the international search

25 November 2019

Date of mailing of the international search report

03 December 2019

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Mechenbier, Bernd

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2019/074203

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2016343187	A1	24 November 2016	EP	3298591	A1	28 March 2018
				EP	3298592	A1	28 March 2018
				US	2016343187	A1	24 November 2016
				US	2016344091	A1	24 November 2016
				WO	2016187573	A1	24 November 2016
				WO	2016187574	A1	24 November 2016
GB	2517527	A	25 February 2015	NONE			
EP	1158466	A1	28 November 2001	NONE			
US	2018118166	A1	03 May 2018	DE	102016005342	A1	10 November 2016
				EP	3292027	A1	14 March 2018
				US	2018118166	A1	03 May 2018
				WO	2016177767	A1	10 November 2016
US	2009027194	A1	29 January 2009	AU	2007219056	A1	30 August 2007
				EP	1991749	A1	19 November 2008
				NZ	571424	A	30 September 2011
				US	2009027194	A1	29 January 2009
				WO	2007095686	A1	30 August 2007

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. G07C9/00 E05B65/10
 ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 G07C H04W E05C E05B B60R

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

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2016/343187 A1 (TRANI JAMES [US]) 24. November 2016 (2016-11-24) Absatz [0013] - Absatz [0021] Absatz [0030] Absatz [0053] - Absatz [0063] -----	1-10
X	GB 2 517 527 A (DINKY ASSETS LTD [GB]) 25. Februar 2015 (2015-02-25) Seite 4 Seite 9 Seite 22 - Seite 23 -----	1-9
X	EP 1 158 466 A1 (INVENTIO AG [CH]) 28. November 2001 (2001-11-28) Absatz [0024] - Absatz [0044] Seite 9 Seite 22 - Seite 23 ----- -/-	1-9

☒ 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" 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

25. November 2019

Absendedatum des internationalen Recherchenberichts

03/12/2019

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

Bevollmächtigter Bediensteter

Mechenbier, Bernd

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2018/118166 A1 (MUELLER KARL [DE] ET AL) 3. Mai 2018 (2018-05-03) Absatz [0007] -----	4
A	US 2009/027194 A1 (MCGRATH LEIGH JASON [AU]) 29. Januar 2009 (2009-01-29) Absatz [0014] -----	4

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2019/074203

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2016343187	A1	24-11-2016	EP 3298591 A1	28-03-2018
			EP 3298592 A1	28-03-2018
			US 2016343187 A1	24-11-2016
			US 2016344091 A1	24-11-2016
			WO 2016187573 A1	24-11-2016
			WO 2016187574 A1	24-11-2016

GB 2517527	A	25-02-2015	KEINE	

EP 1158466	A1	28-11-2001	KEINE	

US 2018118166	A1	03-05-2018	DE 102016005342 A1	10-11-2016
			EP 3292027 A1	14-03-2018
			US 2018118166 A1	03-05-2018
			WO 2016177767 A1	10-11-2016

US 2009027194	A1	29-01-2009	AU 2007219056 A1	30-08-2007
			EP 1991749 A1	19-11-2008
			NZ 571424 A	30-09-2011
			US 2009027194 A1	29-01-2009
			WO 2007095686 A1	30-08-2007
