(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 203 521 A1** 2017.09.07

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 203 521.5**
(22) Anmeldetag: **03.03.2016**
(43) Offenlegungstag: **07.09.2017**

(51) Int Cl.: ***B60R 25/00*** (2006.01)

(71) Anmelder:
Volkswagen Aktiengesellschaft, 38440 Wolfsburg, DE

(72) Erfinder:
Fontana, Dino, 45968 Gladbeck, DE; Jurthe, Sascha, 45529 Hattingen, DE

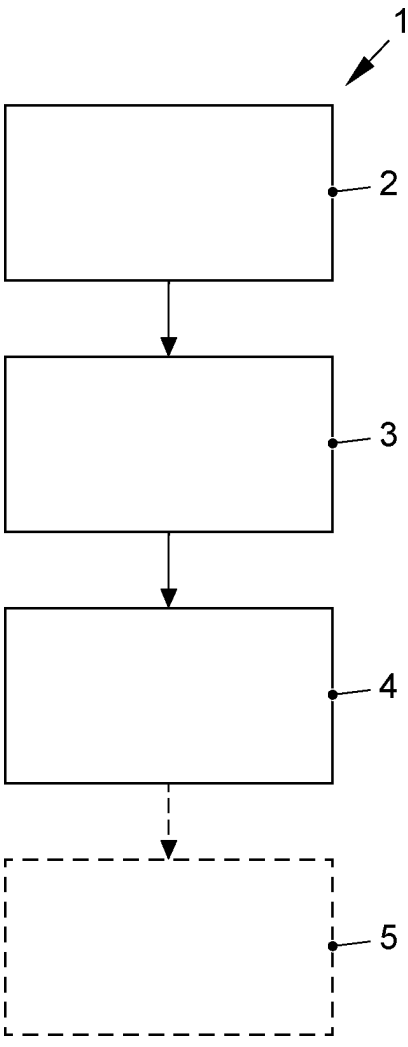
(56) Ermittelter Stand der Technik:

DE	**195 47 560**	**C2**
DE	**10 2013 019 746**	**A1**
DE	**600 04 980**	**T2**
EP	**0 109 184**	**A2**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren und System für ein Authentifizieren eines Benutzers sowie ein Kraftfahrzeug**



(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren (1) für eine Authentifizierung eines Benutzers (13) gegenüber einer Einrichtung (12), beispielsweise gegenüber einem Fahrzeug (12). Er erfolgt ein Einkoppeln (2) eines Signals (11), das eine Information über den Benutzer (13) umfasst, in eine Haut (15) des Benutzers (13) mittels einer Sendeeinrichtung (7). Ferner findet ein Herstellen (3) eines direkten Kontakts zwischen der Haut (15) des Benutzers (13) und einer der Einrichtung zugeordneten Empfangseinrichtung (8) statt, sodass das Signal (11) von der Haut (15) des Benutzers (13) auf die Empfangseinrichtung (8) übertragen wird. Es erfolgt auch ein Authentifizieren (3) des Benutzers (13), basierend auf dem mittels der Empfangseinrichtung (8) empfangen Signals (11).

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und ein System für ein Authentifizieren eines Benutzers sowie ein Kraftfahrzeug.

[0002] Eine Vielzahl von Bereichen oder Einrichtungen können gegenüber einem Benutzer, beispielsweise gegen einen Zugang, gesichert sein. Um dem Benutzer den Zugang zu ermöglichen, kann sich der Benutzer authentisieren. Wenn dies zu einer erfolgreichen Authentifizierung führt, kann dem Benutzer ein Zugang zu dem Bereich oder der Einrichtung gewährt werden. Bei der Einrichtung kann es sich beispielsweise um einen geschlossenen Raum, ein Fahrzeug, eine Maschine oder dergleichen handeln.

[0003] Zum Entriegeln eines Fahrzeugs, aber auch um andere Funktionen an einem Fahrzeug auszulösen, beispielsweise zum Starten eines Motors, sind eine Vielzahl von Systemen bekannt, die berührungslos arbeiten und bei denen ein mechanischer Schlüssel entfallen kann. Bei vielen dieser Systeme wird ein Fahrzeugschlüssel benötigt, zum Beispiel in Form einer Funkfernbedienung, eines Transponders bei einem sogenannten Keyless Entry-System, ein Smartphone oder dergleichen. Bis auf das Keyless Entry-System als kontaktfreies Authentifizierungssystem ist bei anderen Systemen eine Interaktion des Nutzers mit dem Fahrzeugschlüssel notwendig, um das Fahrzeug zu entriegeln oder eine andere Funktion zu starten. Dies ist unerwünscht, weil der Nutzer nach dem Fahrzeugschlüssel suchen muss, um das Fahrzeug zu entriegeln oder um sich zu authentifizieren.

[0004] Mit der EP 1 239 420 A1 wird versucht ein Identifikationssystem und einen dazu passenden Codegeber zu schaffen, durch die eine verbesserte Sicherheit gegen unbefugte Benutzung oder unbefugten Zugang geschaffen wird. Dazu wird bei dem Identifikationssystem ein Frage-Antwort-Dialog zwischen einem Objekt und dem Codegeber durchgeführt, durch den Codeinformationen ausgetauscht und verifiziert werden. Damit nur ein Codegeber in Nähe des Objekts einen Nachweis zur Berechtigung für den Zugang zu dem Objekt oder der Benutzung des Objekts erhalten kann, muss ein Codegeber ein objektseitiges, separat erzeugtes elektromagnetisches Feld erkennen. Dies ist nur dann der Fall, wenn sich der Benutzer mit dem Codegeber in der Nähe des Objekts befindet. Nur dann dient das berechtigte Codesignal als Nachweis für den berechtigten Zugang oder die berechtigte Benutzung des Objekts. Darüber hinaus darf sich der Codegeber nur in der Nähe des Kraftfahrzeugs befinden, wenn Zugang oder Nutzung begehrt wird. Ob sich der Codegeber in der Nähe befindet, wird dadurch festgestellt, dass ein elektromagnetisches Feld im Bereich einer Zugangstür aufgebaut wird. Wenn ein Benutzer beispielsweise seine Hand in die Nähe eines Türgriffs bringt, so wird dieses Feld in den Körper des Benutzers eingekoppelt. Der Aufbau solcher Felder kann unter ungünstigen Umständen zu einem relativ hohen Energieverbrauch führen. Dies ist unerwünscht.

[0005] Es besteht daher ein Bedarf daran, ein Konzept für ein Authentifizieren eines Benutzers gegenüber einer Einrichtung zu verbessern. Diesem Bedarf tragen das Verfahren und das System der unabhängigen Ansprüche Rechnung.

[0006] Die vorliegende Erfindung betrifft ein Verfahren für ein Authentifizieren eines Benutzers gegenüber einer Einrichtung, beispielsweise gegenüber einem Fahrzeug. Dazu wird ein Signal, das eine Information über den Benutzer umfasst, in eine Haut des Benutzers mittels einer Sendeeinrichtung eingekoppelt. Ferner wird ein direkter Kontakt zwischen der Haut des Benutzers und einer der Einrichtung zugeordneten Empfangseinrichtung hergestellt, sodass das Signal von der Haut des Benutzers auf die Empfangseinrichtung übertragen wird. Anschließend erfolgt ein Authentifizieren des Benutzers, basierend auf dem mittels der Empfangseinrichtung empfangen Signals.

[0007] Ferner betrifft die vorliegende Erfindung auch ein System für ein Authentifizieren, das auch als Authentifizierung bezeichnet werden kann, eines Benutzers gegenüber einer Einrichtung. Das System umfasst eine Sendeeinrichtung, die ausgebildet ist, um ein Signal mit einer Information über den Benutzer in die Haut des Benutzers einzukoppeln. Ferner umfasst das System eine Empfangseinrichtung, die der Einrichtung zugeordnet ist und die ausgebildet ist, um bei einem direkten Kontakt zwischen der Haut des Benutzers und der Empfangseinrichtung das Signal zu empfangen. Das System umfasst auch eine Steuereinrichtung, die ausgebildet ist, um den Benutzer zu authentifizieren, basierend auf dem mittels der Empfangseinrichtung empfangenen Signals.

[0008] Bei manchen Ausführungsbeispielen kann dadurch, dass eine Signalübertragung über die Haut des Benutzer stattfindet, wenn dieser mit der Einrichtung bzw. einer dieser zugeordneten Empfangseinrichtung in Kontakt steht, eine Sicherheit, bei einer Authentifizierung erhöht werden. Gleichzeitig kann eventuell auch ein Komfort erhöht werden, da für eine Kommunikation bzw. eine Signalübertragung ein Benutzer lediglich eine Empfangseinrichtung berühren muss. Ein aktives Betätigen oder Auslösen der Sendeeinrichtung durch den Benutzer kann beispielsweise entfallen.

[0009] Bei manchen Ausführungsbeispielen kann die Sendeeinrichtung zum Einkoppeln des Signals in einem direkten Kontakt mit der Haut des Benutzers stehen. Bei manchen Ausführungsbeispielen kann dadurch auch der Aufbau eines Feldes für eine ka-

pazitive Kopplung, das eine Signalübertragung auch ohne direkten Kontakt ermöglicht, entfallen. Natürlich kann bei manchen Ausführungsbeispielen das Signal in die Haut auch ohne einen direkten Kontakt zwischen der Sendeinrichtung und der Haut eingekoppelt werden. Beispielsweise kann die Sendeeinrichtung dann auch in einer Tasche und nicht direkt am Körper des Benutzers mitgeführt werden.

[0010] Ergänzend oder alternativ kann es sich bei dem Signal um eine Spannung und/oder einen Strom handeln. Bei manchen Ausführungsbeispielen können dadurch alle möglichen Informationen, die codiert und/oder moduliert sind, mit einem geringen Energieaufwand und eventuell auch einem geringen Aufwand bezüglich der Sendeeinrichtung zuverlässig übertragen werden. Die Sendeeinrichtung kann beispielsweise wenigstens eine Elektrode umfassen, die mit der Haut des Benutzers in Kontakt steht. Ergänzend oder alternativ kann die Empfangseinrichtung beispielsweise wenigstens eine Elektrode umfassen, die mit der Haut des Benutzers in Kontakt steht.

[0011] Optional kann es sich bei dem Signal um ein Ultraschallsignal handeln. Bei manchen Ausführungsbeispielen kann dieses Verfahren auch für einen Personenkreis, der eventuell unter ungünstigen Umständen nicht oder nur bedingt für eine Übertragung von Strom- und/oder Spannungssignalen über die Haut geeignet ist, eingesetzt werden, beispielsweise Personen, die einen Herzschrittmacher tragen. Die Sendeeinrichtung kann beispielsweise wenigstens einen Ultraschallgeber und/oder die Empfangseinrichtung einen Ultraschallsensor oder -empfänger umfassen.

[0012] Ergänzend oder alternativ kann die Sendeeinrichtung einem tragbaren Gerät, beispielsweise einem Wearable, einem Smartphone, einer Smartwatch, einem Fahrzeugschlüssel, einem Implantat, einer elektronischen Hautprothese oder dergleichen zugeordnet sein. Bei manchen Ausführungsbeispielen kann dadurch erreicht werden, dass die Sendeeinrichtung nahe an dem Körper des Benutzers getragen werden kann. Der Benutzer muss dann bei manchen Ausführungsbeispielen das Gerät mit der zugeordneten Sendeeinrichtung nicht suchen, um mit der Einrichtung in Kommunikation zu treten. Bei Ausführungsbeispielen, bei denen das Gerät mit der Sendeeinrichtung direkt am Körper bzw. an der Haut getragen wird, beispielsweise als Smartwatch, kann die Sendeeinrichtung das Signal direkt in die Haut einkoppeln.

[0013] Ergänzend oder alternativ kann anschließend an eine erfolgreiche Authentifizierung dem Benutzer ein Zugriff auf eine Funktion ermöglicht werden. Bei manchen Ausführungsbeispielen kann dadurch ermöglicht werden, dass nur ein authentifizierter Benutzer die Funktion ausführen kann, beispielsweise eine Fahrzeugtür entsperren und/oder einen Motor starten, Verschließen des Fahrzeugs, eine einzelne Klappe eines Fahrzeugs öffnen oder dergleichen. Unter Umständen kann so die Sicherheit bei einer Bestimmung, ob ein Benutzer die Funktion ausführen darf, erhöht werden.

[0014] Ergänzend kann ein weiteres Authentifizieren des Benutzers mittels einer weiteren Information über den Benutzer erfolgen. Bei manchen Ausführungsbeispielen kann die Sicherheit dadurch weiter erhöht werden. Erst nachdem eine erste Authentifizierungsstufe überwunden ist, werden Informationen ausgetauscht, die einen Zugriff auf die Funktion erlauben. Es wird also eine zweite Authentifizierungsstufe eingeführt. Unter Umständen kann dadurch die Gefahr eines Abhörens der Information, die zum Zugriff auf die Funktion notwendig ist, zumindest reduziert, wenn nicht völlig vermieden werden.

[0015] Ergänzend kann das weitere Authentifizieren mittels eines drahtlosen Signalübertragungsverfahrens erfolgt. Bei manchen Ausführungsbeispielen kann dadurch erreicht werden, dass die Signalübertragung über die Haut so kurz wie möglich und/oder nur mit einer geringen Intensität durchgeführt wird. Zur Übertragung der Information für die zweite Authentifizierungsstufe können dann eventuell Signalübertragungsverfahren gewählt werden, die eine bessere Signalübertragung erlauben und zum Beispiel eine größere Übertragungsgeschwindigkeit und/oder das Übertragen einer größeren Menge an Daten erlauben. Bei manchen Ausführungsbeispielen kann es erforderlich sein, dass die Hand des Benutzers auch während der zweiten Authentifizierung in einem direkten Materialkontakt mit der Empfangseinrichtung steht. Alternativ kann natürlich das weitere Authentifizieren bei manchen Ausführungsbeispielen auch über die Haut und bei einem direkten Kontakt mit der Empfangseinrichtung erfolgen.

[0016] Die vorliegende Erfindung betrifft auch ein System für ein Authentifizieren eines Benutzers gegenüber einer Einrichtung. Das System umfasst eine Sendeeinrichtung, die ausgebildet ist, um ein Signal mit einer Information über den Benutzer in die Haut des Benutzers einzukoppeln. Ferner umfasst das System eine Empfangseinrichtung, die der Einrichtung zugeordnet ist und die ausgebildet ist, um bei einem direkten Kontakt zwischen der Haut des Benutzers und der Empfangseinrichtung das Signal zu empfangen. Das System umfasst auch eine Steuereinrichtung, die ausgebildet ist, um den Benutzer zu authentifizieren, basierend auf dem mittels der Empfangseinrichtung empfangen Signals.

[0017] Die vorliegende Erfindung betrifft ebenfalls ein Kraftfahrzeug mit einem Schließmechanismus, der ausgebildet ist, um ansprechend auf eine erfolgreiche Authentifizierung gemäß wenigstens ei-

nem der beschriebenen Ausführungsbeispiele entsperrt zu werden. Bei manchen Ausführungsbeispielen kann dadurch ein für einen Benutzer sehr sicheres und komfortables Entriegeln oder Entsperren einer Fahrzeugtür, einer Fahrzeugklappe oder einer anderen Klappe, beispielsweise Tankdeckel, Motorhaube oder Heckklappe, eines Kraftfahrzeugs erreicht werden.

[0018] Die vorliegende Erfindung betrifft ebenfalls ein Kraftfahrzeug mit einem Startmechanismus, der ausgebildet ist, um ansprechend auf eine erfolgreiche Authentifizierung mit einem Verfahren nach einem der vorhergehenden Ausführungsbeispiele ein Starten zu erlauben, beispielsweise nach einem Drücken eines Startknopf und/oder ohne Drücken des Startknopfs direkt nach einer erfolgreichen Authentifizierung.

[0019] Weitere vorteilhafte Ausgestaltungen werden nachfolgend anhand der in den Zeichnungen dargestellten Ausführungsbeispiele, auf welche Ausführungsbeispiele generell jedoch nicht insgesamt beschränkt sind, näher beschrieben. Es zeigen:

[0020] **Fig.** 1 zeigt ein Flussdiagram für ein Verfahren gemäß einem Ausführungsbeispiel;

[0021] **Fig.** 2 zeigt eine schematische Darstellung eines Systems gemäß einem Ausführungsbeispiel;

[0022] **Fig.** 3 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs, an dem ein Benutzer gemäß einem Ausführungsbeispiel authentifiziert wird;

[0023] **Fig.** 4 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs, an dem ein Benutzer gemäß einem weiteren Ausführungsbeispiel authentifiziert wird;

[0024] **Fig.** 5 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs, an dem ein Benutzer gemäß einem weiteren Ausführungsbeispiel authentifiziert wird; und

[0025] **Fig.** 6 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs, an dem ein Benutzer gemäß einem weiteren Ausführungsbeispiel authentifiziert wird.

[0026] Verschiedene Ausführungsbeispiele werden nun ausführlicher unter Bezugnahme auf die beiliegenden Zeichnungen beschrieben, in denen einige Ausführungsbeispiele dargestellt sind. In den Figuren können die Dickenabmessungen von Linien, Schichten und/oder Regionen um der Deutlichkeit Willen übertrieben dargestellt sein.

[0027] Die **Fig.** 1 zeigt ein Flussdiagram für ein Verfahren **1** gemäß Ausführungsbeispiel für ein Authentifizieren eines Benutzers gegenüber einer Einrichtung, beispielsweise gegenüber einem Fahrzeug. In einem ersten Vorgang **2** des Verfahrens **1** wird ein Signal, das eine Information über den Benutzer umfasst, in die Haut des Benutzers mittels einer Sendeeinrichtung eingekoppelt. In einem weiteren Vorgang **3** wird ein direkter Kontakt zwischen der Haut des Benutzers und einer der Einrichtung zugeordneten Empfangseinrichtung hergestellt, sodass das Signal von der Haut des Benutzers an die Empfangseinrichtung übertragen wird. Anschließend erfolgt in einem Vorgang **4** ein Authentifizieren des Benutzers, basierend auf dem mittels der Empfangseinrichtung empfangenen Signals.

[0028] Die Vorgänge **1** und **2** können dabei gleichzeitig, zeitlich zumindest teilweise überlappend oder nacheinander ausgeführt werden. Beispielsweise kann der Benutzer den direkten Kontakt zwischen seiner Haut und der Empfangseinrichtung auch herstellen, bevor ein Signal in seine Haut eingekoppelt wird. Unter Umständen können dazwischen auch andere Vorgänge liegen. Beispielsweise kann der Benutzer, nachdem er einen direkten Hautkontakt mit der Empfangseinrichtung hergestellt hat, auch ein weiteres Signal von der Einrichtung oder deren Empfangseinrichtung erhalten, bei der es sich dann um eine Sende- /Empfangseinrichtung handeln kann. Dieses weitere Signal kann eventuell die Sendeeinrichtung dazu veranlassen, das Signal in die Haut des Benutzers einzukoppeln. Dazu kann die Sendeinrichtung ebenfalls als Sende-/Empfangseinrichtung ausgebildet sein, die Signale der Einrichtung empfangen kann. Des Weiteren kann das Signal auch bereits in die Haut eingekoppelt sein, bevor der Benutzer den direkten Hautkontakt mit der Einrichtung herstellt.

[0029] Bei dem Benutzer kann es sich beispielsweise um eine Person handeln, die eine Berechtigung für eine Nutzung oder für einen Zugang zu der Einrichtung hat, beispielsweise einen Fahrer, einen Beifahrer, einen Besitzer der Einrichtung. Bei der Einrichtung kann es sich beispielsweise um jedwede Einrichtung handeln, für die eine Berechtigung erforderlich ist, um eine Funktion auszuüben und/oder um einen Zugang zu erhalten, beispielsweise einen Raum, eine Maschine, ein Fahrzeug, eine Fahrzeugtür, eine Heckklappe, einen Schließmechanismus eines Fahrzeugs, ein Startmechanismus des Fahrzeugs oder dergleichen.

[0030] Für das Authentifizieren kann beispielsweise ein Vergleichen mit einem Vergleichswert und/oder einem Vergleichsbereich mit der Information über den Benutzer vorgenommen werden. Wenn der Vergleich ergibt, dass die Information über den Benutzer dem Vergleichswert entspricht und/oder in dem Vergleichsbereich liegt, kann eine Authentifizierung

erfolgreich sein. Ergibt der Vergleich, dass die Information über den Benutzer nicht mit dem Vergleichswert übereinstimmt und/oder in dem Vergleichsbereich liegt, schlägt eine Authentifizierung fehl. Beispielsweise kann dem Benutzer dann ein Zugang zu der Einrichtung und/oder einer Funktion der Einrichtung verwehrt werden.

[0031] Die Information über den Benutzer kann beispielsweise jedwede Information umfassen, die eine Aussage darüber zulässt, ob der Benutzer zugangsberechtigt für die Einrichtung ist. Bei der Information kann es sich beispielsweise um einen vorgegeben Wert, beispielsweise einen festeingestellten, statischen Wert wie einen PIN oder eine Identifikationsnummer handeln. Optional kann es sich bei der Information auch um einen für einen Benutzer individualisierten und/oder angelernten Wert handeln, den ein berechtigter Benutzer der Einrichtung, beispielsweise der Fahrzeuginhaber, dem Fahrzeug oder einer Fahrzeugsteuerung anlernen kann, beispielsweise eine Nummer, einen PIN oder dergleichen. Unter Umständen kann eine Mehrzahl von Benutzern eine Berechtigung für die Einrichtung erhalten. Dabei kann die Information über den Benutzer spezifisch für jeden Benutzer sein oder aber auch eine allgemeine Information sein, die nur eine Zugangsberechtigung betrifft. Die Information über den Benutzer kann selbstverständlich signalverarbeitet sein und auf jedwede Art und Weise codiert und/oder moduliert sein. Ein Einkoppeln eines Signals in die Haut kann beispielsweise dadurch erfolgen, dass die leitfähige Haut als Signalübertragungsmedium genutzt wird.

[0032] Die **Fig.** 2 zeigt eine schematische Darstellung eines Systems **6** für ein Authentifizieren eines Benutzers gegenüber einer Einrichtung **12**, die hier strichliniert und beispielhaft als Kraftfahrzeug **10** dargestellt ist, gemäß einem Ausführungsbeispiel. Das System **6** umfasst eine Sendeeinrichtung **7**, die ausgebildet ist, um ein Signal **11** mit einer Information über den Benutzer in die Haut des Benutzers einzukoppeln. Hier und im Folgenden kann das Signal **11** beispielsweise einen binären, analogen, digitalen oder elektrischen Wert repräsentieren oder eine Information, die durch einen Wert repräsentiert ist. Bei dem Signal **11**, das in die Haut eingekoppelt wird, kann es sich beispielsweise um ein elektrisches Signal, beispielsweise einen Strom und/oder eine Spannung und oder ein Ultraschallsignal handeln. Das Signal **11** kann beispielsweise auf jedwede Art und Weise moduliert und/oder codiert sein. Das Einkoppeln des Signals **11** kann beispielsweise permanent oder in regelmäßigen Abständen erfolgen. Alternativ kann das Einkoppeln des Signals **11** basierend auf einem Ereignis ausgelöst werden. Ein Ereignis, das das Einkoppeln des Signals **11** triggert, kann beispielsweise eine Bewegung des Benutzers, ein Empfangen des Signals von der Einrichtung **12** bzw. deren Empfangseinrichtung oder dergleichen sein.

[0033] Bei der Sendeeinrichtung **7** kann es sich um alle möglichen Vorrichtungen handeln, die ausgebildet sind, um das Signal **11** mit der Information über den Benutzer zu erzeugen und in die Haut des Benutzers einzukoppeln. Beispielsweise kann die Sendeinrichtung **7** ausgebildet sein, um ein elektrisches Signal, beispielsweise einen Strom oder eine Spannung, zu erzeugen. Dazu kann die Sendeinrichtung **7** beispielsweise wenigstens eine oder zwei Elektroden umfassen. Über diese kann ein kleiner Wechselstrom, beispielsweise kleiner als 2 mA, in die Haut eingeprägt werden. Beispielsweise kann das Einkoppeln des Signals **11** nach dem Prinzip einer Körperfettmessung erfolgen. Die Sendeeinrichtung **7** kann auch ausgebildet sein, um ein Ultraschallsignal als Signal **7** zu erzeugen. Als Sendeeinrichtung **7** kann dann ein Ultraschallerzeuger oder ein Ultraschallsensor eingesetzt werden.

[0034] Ferner umfasst das System **6** eine Empfangseinrichtung **8**, die der Einrichtung **12** zugeordnet ist. Die Empfangseinrichtung **8** kann der Einrichtung **12** beispielsweise dadurch zugeordnet sein, dass sie mit einer Steuereinrichtung **9** der Einrichtung **12** gekoppelt ist. Die Empfangseinrichtung **9** kann beispielsweise über eine Signalübertragung mit der Einrichtung **12** gekoppelt sein, es kann sich dabei beispielsweise um eine drahtlose, aber auch um eine Kopplung über Leitungen, handeln. Die Empfangseinrichtung **8** kann beispielsweise an der Einrichtung **12** angeordnet sein, beispielsweise an einer Fahrzeugtür, aber auch räumlich unabhängig und außerhalb der Einrichtung **12**, beispielsweise an einem Ort, an dem sich die Einrichtung **12** zumindest zeitweilig befindet, wie in einer Garage.

[0035] Die Empfangseinrichtung **8** ist ferner ausgebildet, um bei einem direkten Kontakt zwischen der Haut des Benutzers und der Empfangseinrichtung **8** das Signal **11** zu empfangen. Ein direkter Kontakt zwischen zwei Komponenten, beispielsweise der Haut des Benutzers und der Empfangseinrichtung, kann beispielsweise dann vorliegen, wenn sich diese berühren und unmittelbar aneinander anliegen. Beispielsweise können diese dann nicht durch einen Luftspalt oder ein anderes Medium voneinander getrennt sein. Bei der Empfangseinrichtung **8** kann es sich um alle möglichen Einrichtungen handeln, die ausgebildet, um das Signal **11** zu empfangen, beispielsweise eine Elektrode, einen Ultraschallempfänger oder dergleichen.

[0036] Das System **6** umfasst auch eine Steuereinrichtung **9**, die ausgebildet ist, um den Benutzer zu authentifizieren, basierend auf dem mittels der Empfangseinrichtung **8** empfangen Signals. Dazu können die Steuereinrichtung **9** und die Empfangseinrichtung **8** über eine Signalübertragung gekoppelt sein, beispielsweise mittels einer drahtlosen, wie Funk, W-LAN, Mobilfunk, Bluetooth oder dergleichen oder

über einen Leiter, wie ein internes Netzwerk der Einrichtung, beispielsweise ein Fahrzeugnetzwerk, ein Bussystem, LAN (Local Area Network) oder dergleichen. Bei der Steuereinrichtung **9** kann es sich beispielsweise um eine programmierbare Hardwarekomponente handeln, beispielsweise einen Prozessor, einen Computerprozessor (CPU = Central Processing Unit), einen Grafikprozessor (GPU = Graphics Processing Unit), einen Computer, ein Computersystem, einen anwendungsspezifischen integrierten Schaltkreis (ASIC = Application-Specific Integrated Circuit), einen integrierten Schaltkreis (IC = Integrated Circuit), ein Ein-Chip-System (SOC = System on Chip), ein programmierbares Logikelement oder ein feldprogrammierbares Gatterarray mit einem Mikroprozessor (FPGA = Field Programmable Gate Array) oder dergleichen handeln.

[0037] Obwohl die Sendeeinrichtung **7** und die Empfängereinrichtung **8** bzw. die Einrichtung **12** in der **Fig.** 2 in einem gemeinsamen System **6** dargestellt und beschrieben sind, können die Sendeeinrichtung **7** und die Empfängereinrichtung **8** auch getrennt voneinander Ausführungsbeispiele der Erfindung sein.

[0038] Die **Fig.** 3 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs **10** als Einrichtung **12** an der ein Benutzer **13**, dessen Hand dargestellt ist, nach einem Ausführungsbeispiel des Verfahrens **1** mit dem System **6** authentifiziert wird. Die Authentifizierung und eine Entriegelung des Fahrzeugs **10** erfolgt dabei durch einen Berührungskontakt des Benutzers **13** mit dem Fahrzeug **10**. Der Benutzer **13** trägt dabei eine Smartwatch, welche die Sendeeinrichtung **7** umfasst. Bei einigen weiteren, nicht dargestellten Ausführungsbeispielen kann die Sendeinrichtung auch in einem anderen tragbaren Gerät, beispielsweise einem Wearable, angeordnet sein. Über die Haut **15** des Benutzers **13** wird dann ein elektrischer Kontakt, beispielsweise über den Türgriff **16**, zu dem Fahrzeug **10** hergestellt. Über den elektrischen Kontakt wird beispielsweise das Signal **11** übertragen. Die Empfangseinrichtung **8** ist dabei in oder an dem Türgriff **16** angeordnet. Als Empfangseinrichtung **8** wird dabei der Bereich des Fahrzeugs **10** oder der Einrichtung **12** verstanden, an dem das Signal **11** von der Haut **15** des Benutzers **13** auf das Fahrzeug **10** oder die Einrichtung **12** übertragen wird. Die Kommunikation läuft ausschließlich bzw. nur mittels Hautkontakt ab. Eine direkte Datenkommunikation über die Haut **15** erlaubt die Authentifizierung. Über diesen elektrischen Kontakt wird die eigentliche Authentifizierung initiiert und durchführt. Es erfolgt also ein Smartwatch-Hand-Türgriff Kontakt, über den das Authentifizieren im Vorgang **4** durchgeführt wird, das auch als Initiierung bezeichnet werden kann. Als Vorgang **5**, der gestrichelt in der **Fig.** 1 dargestellt ist, kann ein weiteres Authentifizieren erfolgen. Das weitere Authentifizieren erfolgt mittels einer weiteren Information über den Benutzer. Bei Ausführungsbeispielen, bei denen das weitere Authentifizieren im Vorgang **5** durchgeführt wird, kann es sich bei dem Vorgang **4**, wenn er erfolgreich war, lediglich um einen Vorgang handeln, der das weitere Authentifizieren des Vorgangs **5** auslöst

[0039] Mit anderen Worten kann eine Initiierung, eine Authentifizierung und eine Entriegelung eines nicht dargestellten Schließmechanismus eines Fahrzeugs **10** oder nur einer Fahrzeugtür direkt über die Hand erfolgen. Im der Ausgestaltung der **Fig.** 3 wird die eigentliche Authentifizierung direkt mittels Datenkommunikation über die Haut durchgeführt. Das Fahrzeug **10** ist verschlossen. Der Nutzer **13** des Fahrzeugs **10** trägt das Wearable **14** an seinem Handgelenk und berührt den Türgriff **16**. Daraufhin baut eine Sensorik des Fahrzeugs **10** in Form der Empfangsvorrichtung **8** über die Haut **15** des Nutzers **13** eine Verbindung zu dem Wearable **14** auf und durchläuft die Authentifizierung am Fahrzeug **10**.

[0040] Ferner kann der Schlüssel oder die Information über den Benutzer in einem sicheren Speicher sowohl hartcodiert als auch über eine Datenverbindung provisionierbar ausgelegt sein. Das Wearable, das die Sendeeinrichtung **7** umfasst, kann mit Kontakten ausgerüstet sein, die eine elektrische Leitung über die Haut **15** des Trägers ermöglichen. Bei einer Smartwatch können diese Kontakte beispielsweise in einem Uhrendeckel, einem Armband, einer Schnalle oder einer anderen Position mit Kontakt zur Haut des Benutzers **13**, der auch als Träger bezeichnet werden kann, sitzen. Die Sendeeinrichtung **7** kann in unterschiedliche Wearables angeordnet sein. Unter Umständen kann das Wearable keine Smartwatch sein, sondern ein anderes elektronisches Gerät mit Hautkontakt, zum Beispiel eine Kette, ein Implantat oder dergleichen. Das Fahrzeug **12** kann als Empfangseinrichtung **8** ebenfalls geeignete Aktoren und Sensoren aufweisen, um eine Datenkommunikation mittels elektrischer Leitung über die Haut **15** zu ermöglichen. Diese kann zum Beispiel im Türgriff **16** integriert sein, aber auch andere Verbauorte an oder in dem Fahrzeug **10** sind möglich. Beispielsweise kann die Empfangseinrichtung **8** an einem Kotflügel des Fahrzeugs **10** angeordnet sein, sodass bei einem über den Kotflügel streicheln das Fahrzeug **10** entsperrt werden kann. Es ist aber auch eine Vielzahl von unterschiedlichen Berührungspunkten denkbar. Der Berührungspunkt der Hand am Fahrzeug **10** muss nicht der Türgriff **16** sein, es ist auch eine andere Kontaktfläche, die die Empfangseinrichtung **8** umfasst, möglich. Eventuell kann das ganze Fahrzeug **10** als Kontaktfläche zur Hautleitung benutzt werden.

[0041] Die **Fig.** 4 zeigt eine schematische Darstellung eines Ausschnitts des Kraftfahrzeugs **10**, an dem der Benutzer **13** gemäß einem weiteren Ausführungsbeispiel authentifiziert wird. Das Ausführungsbeispiel der **Fig.** 4 ist im Wesentlichen ähnlich zu dem

Ausführungsbeispiel der **Fig.** 3. Gleiche oder ähnliche Bauteil werden deshalb mit gleichen Bezugszeichen bezeichnet. Das Fahrzeug **10** ist verschlossen. Neben der Sendeeinrichtung **7**, die auch als Hautkontaktsteuergerät bezeichnet werden kann, und ausgebildet ist, um das Signal in die Haut einzukoppeln, umfasst die Smartwatch **14** auch eine Schnittstelle **17** für eine drahtlose Signalübertragung, beispielsweise eine W-LAN- oder Bluetooth-Schnittstelle. Der Nutzer **13** des Fahrzeugs **10** trägt das Wearable **14** an seinem Handgelenk und berührt den Türgriff **16**. Daraufhin registriert die Empfangseinrichtung **8** des Fahrzeugs **10** einen Kontakt zum Wearable über die Haut **15** des Benutzers **13** und initiiert über die Schnittstelle **17**, die auch als Luftschnittstelle bezeichnet werden kann, eine sichere Verbindung, über die dann die Authentifizierung des Nutzers **13** stattfindet. An dem Fahrzeug **10** ist eine Schnittstelle **18** vorgesehen, die dazu dient, die über die Schnittstelle **17** versandten Daten zu empfangen. Mit anderen Worten kann durch den Hautkontakt nur initiiert werden. Die eigentliche Datenübertragung findet dann über eine drahtlose Signalübertragung zwischen den Schnittstellen **17** und **18**, beispielsweise als konventionelle Funktechnologie als weitere Authentifizierung in dem Vorgang **5** statt. Eine Initiierung erfolgt direkt über die Hand, eine Authentifizierung und eine Entriegelung erfolgt über Funk. Mit anderen Worten erfolgt eine Kommunikation über einen Hautkontakt und eine Funkverbindung. Die Datenkommunikation über die Haut wird nur zur Initiierung einer konventionellen Funkdatenkommunikation benutzt. Die eigentliche Authentifizierung findet über einen geeigneten Funkkanal statt. Bei manchen Ausführungsbeispielen kann, beispielsweise um eine Sicherheit zu erhöhen, die Authentifizierung über den Hautkontakt, die Funkverbindung und ein Geheimnis erfolgen. Die Datenkommunikation über die Haut überträgt ein Geheimnis, beispielsweise ein Token oder eine Zufallszahl, welches die konventionelle Funkdatenkommunikation sicherer macht. Natürlich kann auch ohne Funkverbindung, also bei Ausführungsbeispielen, bei denen keine drahtlose Signalübertragung genutzt wird, ein Geheimnis übertragen werden.

[0042] Bei manchen Ausführungsbeispielen kann die Authentifizierung an einem Fahrzeug vereinfacht werden und ohne zusätzliche Nutzerinteraktion ermöglicht werden. Dies wird mit Hilfe eines Berührungskontakts zwischen dem Benutzer und dem Fahrzeug erreicht. Der Benutzer trägt dabei beispielsweise eine Smartwatch, die die Sendeinrichtung **7** umfasst, am Handgelenk, welche über die Haut des Nutzers einen elektrischen Kontakt zu dem Fahrzeug **10** herstellt und eine Authentifizierung initiiert, startet und/oder durchführt. Die eigentliche Authentifizierung kann bei manchen Ausführungsbeispielen direkt über die Haut zum Türgriff, über eine Luftschnittstelle mit drahtlosen Signalübertragungsverfahren, beispielswiese herkömmliche Funktechnologien, oder durch eine Mischung aus beidem durchgeführt werden.

[0043] Die **Fig.** 5 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs **10**, an dem ein Benutzer **13** gemäß einem weiteren Ausführungsbeispiel authentifiziert wird. Das Ausführungsbeispiel der **Fig.** 5 ist im Wesentlichen ähnlich zu dem Ausführungsbeispiel der **Fig.** 3. Gleiche oder ähnliche Bauteil werden deshalb mit gleichen Bezugszeichen bezeichnet. Die Funktion, die nach einer erfolgreichen Authentifizierung angesteuert wird, ist jedoch kein Schließmechanismus des Fahrzeugs **10**, sondern ein Startmechanismus für einen Motor des Fahrzeugs **10**. Ein Startknopf **19** umfasst dazu die Empfangseinrichtung **8**. Eine Initiierung, eine Authentifizierung und eine Start-/Stop-Funktion, also ein Starten des Motors und/oder ein Ausschalten des Motors kann dabei wie bei dem Ausführungsbeispiel der **Fig.** 3 direkt über die Hand und/oder die Haut des Benutzers **13** erfolgen. Bei manchen Ausführungsbeispielen kannum eine Starten des Motors zu bewirken ein mechanisches Betätigen oder Drücken des Startknopfs **19** notwendig sein. Bei anderen Ausführungsbeispielen kann ein mechanisches Betätigen oder ein Drücken des Startknopfs **19** entfallen.

[0044] Die **Fig.** 6 zeigt eine schematische Darstellung eines Ausschnitts eines Kraftfahrzeugs **10**, an dem ein Benutzer **13** gemäß einem weiteren Ausführungsbeispiel authentifiziert wird. Das Ausführungsbeispiel der **Fig.** 6 ist im Wesentlichen ähnlich zu dem Ausführungsbeispiel der **Fig.** 5. Gleiche oder ähnliche Bauteil werden deshalb mit gleichen Bezugszeichen bezeichnet. Bei der Funktion, die nach einer erfolgreichen Authentifizierung angesteuert wird, handelt es sich wie bei dem Ausführungsbeispiel der **Fig.** 5 um den Startmechanismus für einen Motor des Fahrzeugs **10**. Das Verfahren umfasst jedoch wie das Verfahren der **Fig.** 4 zwei Authentifizierungsstufen. Die weitere Authentifizierung des Vorgangs **5** wird über die drahtlosen Signalübertragungsschnittstellen **17** und **18** durchgeführt. Mit anderen Worten erfolgt eine Initiierung direkt über die Hand und/oder die Haut **15**. Eine Authentifizierung und eine Start-/Stop-Funktion erfolgt über Funk oder ein anderes drahtloses Signalübertragungsverfahren. Über die Haut können bei manchen Ausführungsbeispielen nur Informationen übertragen werden, welche relevant für eine sichere Kommunikation von anderen bestehenden Funktechnologien sind, wie zum Beispiel Bluetooth (BT), eine Aufforderung ein Bluetooth-Profil zu aktivieren, einen Pairing Code, oder dergleichen oder wenn als drahtlose Signalübertragung W-LAN genutzt wird, eine Aufforderung ein WiFi-Profil zu aktivieren, ein Passwort, etc. Bei anderen Ausführungsbeispielen erfolgt eine vollständige Authentifizierung über die Haut ohne Hilfe weiterer Funktechnologien.

[0045] Bei manchen Ausführungsbeispielen kann also eine Fahrzeugkommunikation über Hautkontakt ermöglicht werden. Eine Fahrzeugkommunikation kann durch eine Berührung eines Nutzers mit dem Fahrzeug erreicht werden. Die Haut des Nutzers kann als Datenkommunikationsmedium genutzt werden. Eine Datenübertragung kann mit Sensoren und/oder Aktoren eines Wearables möglich sein, welche direkt oder indirekt Kontakt mit der Haut des Besitzers haben. Vorstellbar ist beispielsweise eine Smartwatch, welche Sensoren und/oder Aktoren an einem Gehäuse oder in einem Armband aufweist oder aber auch ein Smartphone, das der Benutzer **13** beispielsweise in seiner Hosentasche mit trägt. Ebenfalls sind auch Implantate oder elektronische Hautprothesen denkbar. Die Wearables oder Smartphones können dabei eventuell direkt auf lokal gespeicherte, sichere Informationen zugreifen oder durch weitere Funktechnologien oder drahtlose Übertragungsverfahren auf andere oder äußere Speicher, beispielsweise andere Smart-Devices wie Smartphones oder Cloud-Lösungen, zum Beispiel übergeordnete Server- oder Speichereinrichtungen, zugreifen, die sichere Informationen aufweisen. Bei manchen Ausführungsbeispielen weist die Sendeinrichtung, die dem Wearable zugeordnet ist oder von diesem umfasst ist, einen integrierten sicheren Schlüssel auf. Bei dem Wearable kann es sich beispielsweise um eine Smartwatch handeln, welche beispielsweise den Schlüssel in einem sicheren Speicher integriert hat. Alternativ kann der Schlüssel auch in einem elektrisch verbundenem Zubehörteil, beispielsweise einem Armband, integriert und/oder gespeichert sein. Optional kann der Schlüssel in einem per Funk verbundenem Zubehörteil, beispielsweise ein per Bluetooth gekoppeltes Smartphone integriert oder gespeichert sein. Diese Datenkommunikation kann zur Authentifizierung eines Nutzers genutzt werden, um in der Folge das Fahrzeug zu entriegeln oder zu starten. Die Authentifizierung durch ein Wearable, das die Sendeeinrichtung umfasst, kann eventuell keine zusätzliche Interaktion benötigen, wie beispielsweise das Starten einer App oder dergleichen. Ferner muss die Sendeeinrichtung bei manchen Ausführungsbeispielen nicht an einen bestimmten Punkt, beispielsweise einen NFC-Reader (Abk.: von engl. Near Field Communication, Nahfeldkommunikation), gehalten werden.

[0046] Aktuell können Smartwatches, die die Sendeinrichtung umfassen, vom Handling vorteilhaft sein, beispielsweise weil sie interaktionslos benutzbar und/oder weil sie technisch weit genug entwickelt sind, um diese Funktion zu unterstützen. Auch stellt der Türgriff einen „natürlichen“ Berührungspunkt an dem Fahrzeug dar. Ein großer Vorteil kann bei manchen Ausführungsbeispielen in der Kommunikation zwischen einem Schlüsselspeicher als Sendeeinrichtung und dem Fahrzeug über die Haut der Person liegen. Mit anderen Worten erfolgt eine Datenkommunikation über die leitfähige Haut zum Fahrzeug. Es wird kein Feld im Objekt, also beispielsweise zur Initialisierung benötigt, in das der Benutzer gelangen muss. Stattdessen ist jeder Mechanismus denkbar, der eine Interaktion eines Benutzers erkennt, beispielsweise ein berührungsempfindlicher Sensor im Türgriff. Eventuell kann keine kapazitive Feldkopplung stattfinden, um ein Codesignal für die Berechtigung zu senden. Die Kommunikation findet entweder komplett über die Haut statt oder mindestens initial über die Haut mit anschließender durch die Initialisierung gesicherter Funkverbindung, beispielsweise Bluetooth oder W-LAN. Das System und das Verfahren gemäß Ausführungsbeispielen können jedoch nicht nur, wie beschrieben, bei Fahrzeugtüren, sondern bei allen möglichen Fahrzeugzugangssystemen aber auch bei jeglicher Art von Zugangssystemen, Haus, Fahrzeug, Reisen oder dergleichen, eingesetzt werden.

[0047] Die in der vorstehenden Beschreibung, den nachfolgenden Ansprüchen und den beigefügten Figuren offenbarten Merkmale können sowohl einzeln als auch in beliebiger Kombination für die Verwirklichung eines Ausführungsbeispiels in ihren verschiedenen Ausgestaltungen von Bedeutung sein und implementiert werden.

Bezugszeichenliste

1	Verfahren
2	Einkopplen
3	Herstellen
4	Authentifizieren
5	weiteres Authentifizieren
6	System
7	Sendeeinrichtung
8	Empfangseinrichtung
9	Steuereinrichtung
10	Kraftfahrzeug
11	Signal
12	Einrichtung
13	Benutzer
14	Smartwatch
15	Haut
16	Türgriff
17	Schnittstelle
18	Schnittstelle
19	Startknopf

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- EP 1239420 A1 [0004]

Patentansprüche

1. Verfahren (**1**) für eine Authentifizierung eines Benutzers (**13**) gegenüber einer Einrichtung (**12**), beispielsweise gegenüber einem Fahrzeug (**12**), mit folgenden Merkmalen:
Einkoppeln (**2**) eines Signals (**11**), das eine Information über den Benutzer (**13**) umfasst, in eine Haut (**15**) des Benutzers (**13**) mittels einer Sendeeinrichtung (**7**),
Herstellen (**3**) eines direkten Kontakts zwischen der Haut (**15**) des Benutzers (**13**) und einer der Einrichtung zugeordneten Empfangseinrichtung (**8**); sodass das Signal (**11**) von der Haut (**15**) des Benutzers (**13**) auf die Empfangseinrichtung (**8**) übertragen wird;
Authentifizieren (**3**) des Benutzers (**13**), basierend auf dem mittels der Empfangseinrichtung (**8**) empfangen Signals (**11**).

2. Verfahren nach Anspruch 1, wobei die Sendeeinrichtung (**7**) zum Einkoppeln des Signals (**11**) in einem direkten Kontakt mit der Haut (**15**) des Benutzers (**13**) steht.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Signal (**11**) eine Spannung und/oder ein Strom ist.

4. Verfahren nach einem der Ansprüche 1 bis 2, wobei das Signal (**11**) ein Ultraschallsignal ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei anschließend an eine erfolgreiche Authentifizierung dem Benutzer (**13**) ein Zugriff auf eine Funktion ermöglicht wird.

6. Verfahren nach einem der Ansprüche 1 bis 4, ferner umfassend ein weiteres Authentifizieren (**5**) des Benutzers (**13**), mittels einer weiteren Information über den Benutzer (**13**) und/oder ferner umfassend ein weiteres Authentifizieren (**5**) des Benutzers (**13**), wobei das weitere Authentifizieren (**5**) mittels eines drahtlosen Signalübertragungsverfahrens erfolgt.

7. System (**6**) zur Authentifizierung eines Benutzers (**13**) gegenüber einer Einrichtung (**12**) mit folgenden Merkmalen:
einer Sendeeinrichtung (**7**), die ausgebildet ist, um ein Signal (**11**) mit einer Information über den Benutzer (**13**) in die Haut (**15**) des Benutzers (**13**) einzukoppeln;
einer Empfangseinrichtung (**8**), die der Einrichtung (**12**) zugeordnet und die ausgebildet ist, um bei einem direkten Kontakt zwischen der Haut (**15**) des Benutzers (**13**) und der Empfangseinrichtung (**8**) das Signal (**11**) zu empfangen; und
einer Steuereinrichtung (**9**), ausgebildet ist, um den Benutzer (**13**) zu authentifizieren, basierend auf dem mittels der Empfangseinrichtung (**8**) empfangen Signal (**11**).

8. System nach Anspruch 7, wobei die Sendeeinrichtung (**7**) wenigstens eine Elektrode umfasst, und/oder wobei die Sendeeinrichtung (**7**) wenigstens einen Ultraschallgeber und/oder die Empfangseinrichtung (**8**) wenigstens einen Ultraschallsensor oder -empfänger umfasst.

9. System nach einem der vorhergehenden Ansprüche 7 oder 8, wobei die Sendeeinrichtung (**7**) einem Smartphone, einer Smartwatch (**14**) und/oder einem Fahrzeugschlüssel zugeordnet ist.

10. Kraftfahrzeug (**10**) mit einem Schließmechanismus und/oder einem Startmechanismus, wobei der Schließmechanismus und/oder der Startmechanismus (**19**) ausgebildet ist oder sind, um auf eine erfolgreiche Authentifizierung mit einem Verfahren (**1**) nach einem der Ansprüche 1 bis 6 wenigstens eine Fahrzeugtür zu entsperren und/oder zu starten.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

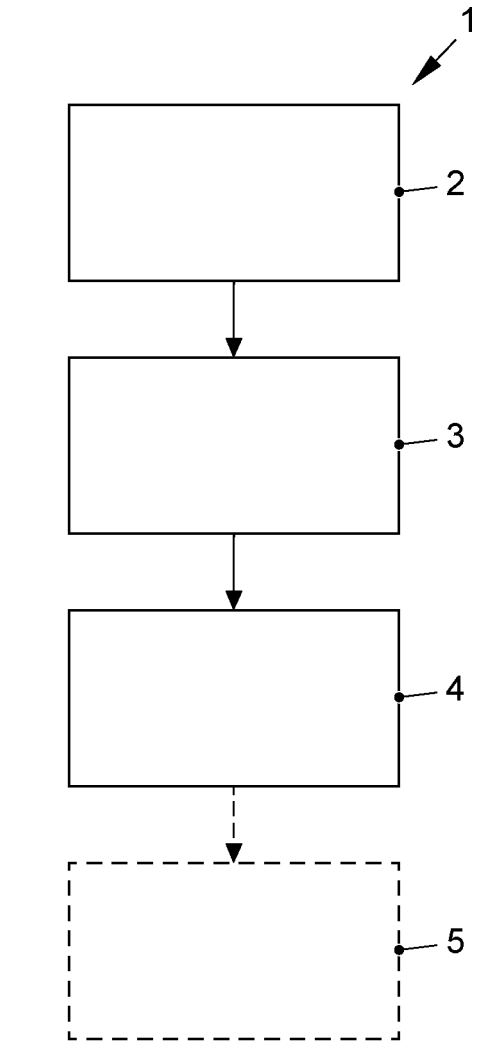


FIG. 1

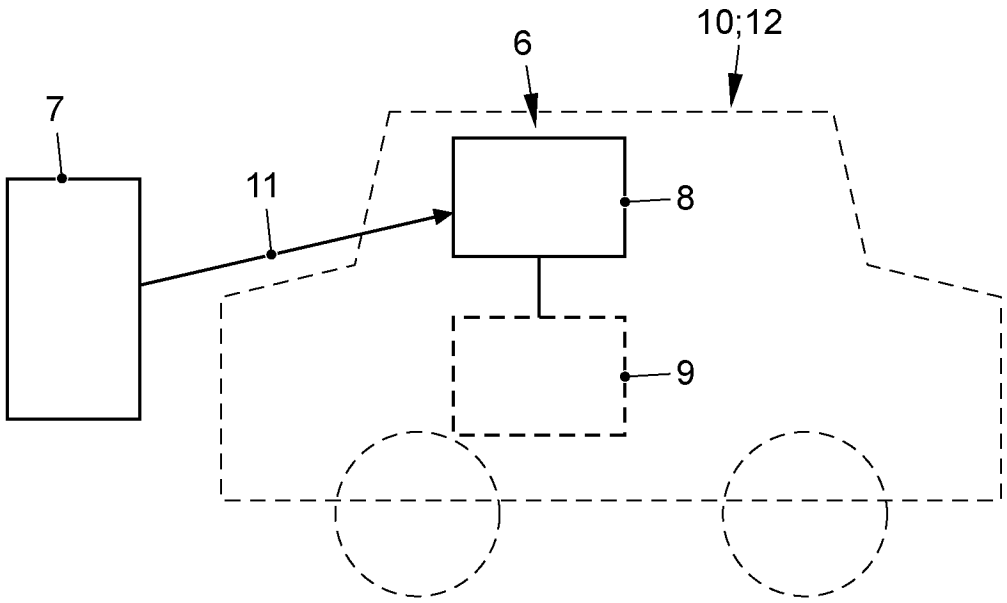


FIG. 2

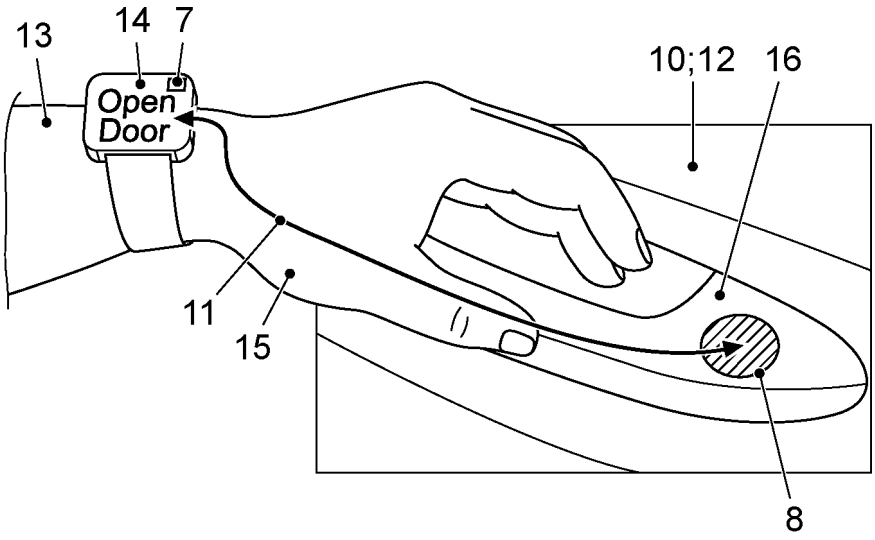

13
14
7
Open
Door
10;12
16
11
15
8

FIG. 3

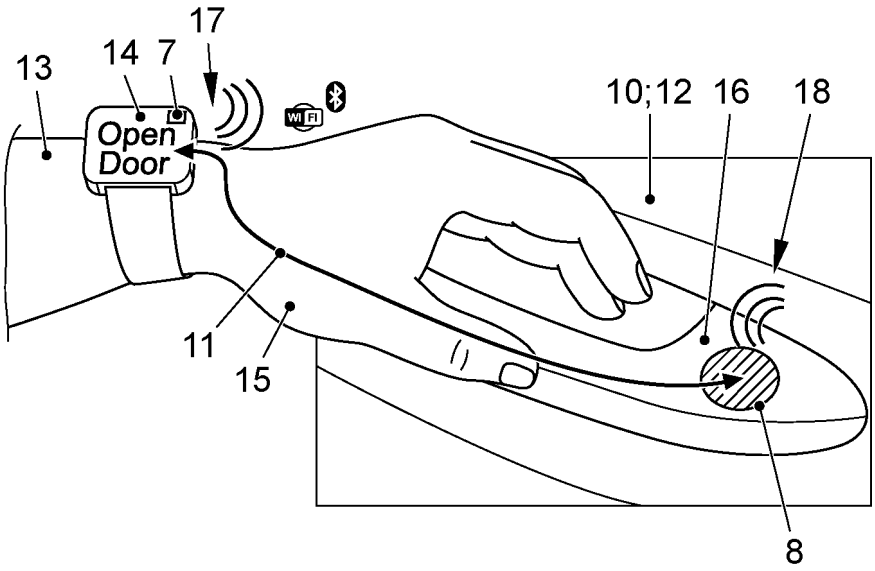

17
13
14
7
Open
Door
WI FI
10;12
16
18
11
15
8

FIG. 4

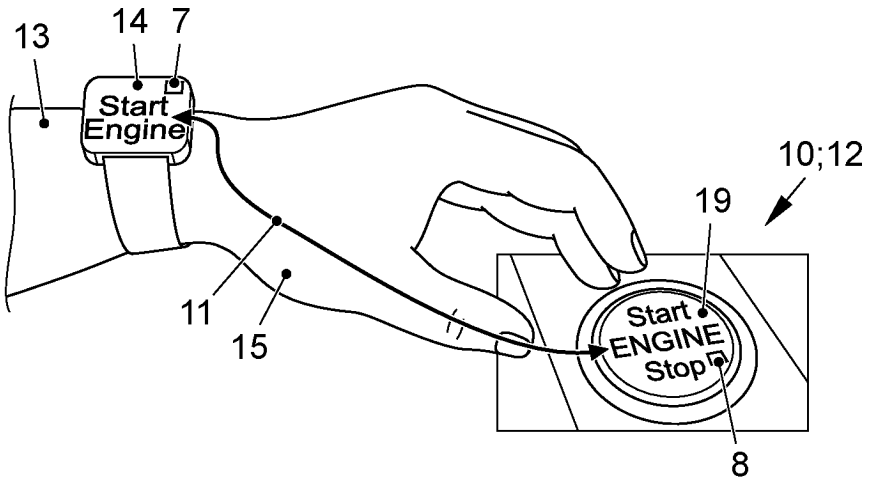

13
14
7
Start
Engine
10;12
19
11
15
Start
ENGINE
Stop
8

FIG. 5

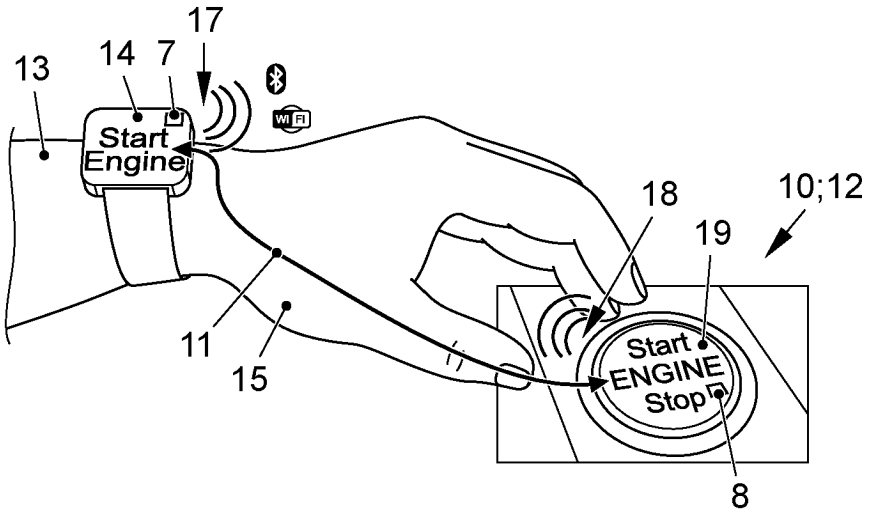

17
13
14
7
Start
Engine
18
10;12
19
11
15
Start
ENGINE
Stop
8

FIG. 6