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

(11) **EP 2 816 533 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
24.12.2014 Patentblatt 2014/52

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Anmeldenummer: **14173285.9**

(22) Anmeldetag: **20.06.2014**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME

(30) Priorität: **20.06.2013 DE 102013106445**

(71) Anmelder: **i-Vector Innovationsmanagement GmbH**
10555 Berlin (DE)

(72) Erfinder:
- **Jobst, Steffen**
  13088 Berlin (DE)
- **Herrmann, Christian**
  15834 Rangsdorf (DE)
- **Haberecht, Christian**
  12524 Berlin (DE)
- **Adomeit, Julius**
  10961 Berlin (DE)
- **Conradi, Peter**
  64283 Darmstadt (DE)
- **Bauer, Andreas**
  13053 Berlin (DE)
- **Braun, Uwe Peter**
  14467 Potsdam (DE)
- **Bernard, Walther**
  12357 Berlin (DE)
- **Hetzer, Henning**
  10405 Berlin (DE)
- **Forchert, Carl-Ernst**
  13465 Berlin (DE)
- **Zieme, Christian**
  16540 Hohen Neuendorf (DE)
- **Klenke, Oliver**
  14513 Teltow (DE)

(74) Vertreter: **Seliger, Knut et al**
Schulz Junghans
Patentanwälte PartGmbB
Großbeerenstraße 71
10963 Berlin (DE)

(54) Verfahren zum sicheren Betrieb fahrzeugnaher Applikationen

(57) Die Erfindung betrifft ein Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen, bei dem die Aktivierung eines Steuergerätes (3) mittels einer Identifikation und/ oder Autorisierung des Nutzers erfolgt, wobei das Steuergerät (3) mit einem externen Computer oder einem externen Computernetzwerk (Cloud) (5) verbunden wird.

Des Weiteren betrifft die Erfindung ein System zur Durchführung des Verfahrens.

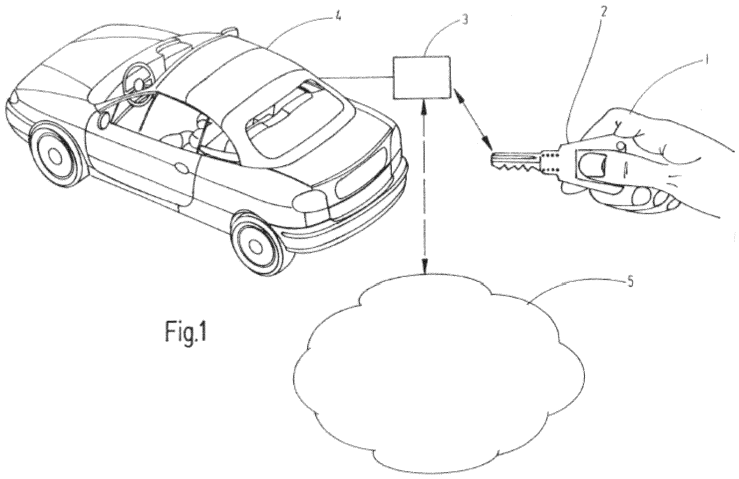

Fig.1

EP 2 816 533 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum sicheren Betrieb fahrzeugnaher Applikationen, bei dem die Aktivierung eines Steuergerätes für Fahrzeugkomponenten und -funktionen mittels einer sicheren und eindeutigen Identifikation und Autorisierung des Nutzers erfolgt. Zudem betrifft die Erfindung ein System zur Durchführung des Verfahrens.

[0002] Unter fahrzeugnahen Applikationen werden jene softwaregestützte fahrzeug-externe und/oder fahrzeug-interne Funktionen gefasst, die über die eigentlichen Fahrfunktionen und Fahrerassistenzsysteme hinausgehen.

[0003] Verfahren der eingangs genannten Art sind aus dem Stand der Technik bekannt und dem Fachmann geläufig.

[0004] Aus der EP 0 645 286 B1 ist ein Verfahren für eine Diebstahlschutzvorrichtung für Fahrzeuge mit mehreren Steuergeräten für Fahrzeugkomponenten, die bei Übereinstimmen einer vorgegebenen Prüfinformation mit einer vorgegebenen Referenzinformation freigeschaltet werden und bei der für mindestens zwei Steuergeräte die Prüf- und die Referenzinformation sich voneinander unterscheiden, bekannt. Die für die Inbetriebnahme notwendige Freischaltung der Steuergeräte erfolgt dabei bei Anwesenheit eines durch ein biometrisches Identifikationsverfahren als berechtigt nachgewiesenen Benutzers. Ein Steuergerät kann beispielsweise für die Aktivierung des Antriebsaggregates des Fahrzeuges vorgesehen sein.

[0005] Für eine Weiterentwicklung der Verfahren der eingangs genannten Art steht die in der EP 1 112 204 B1 offenbarte biometrische Identifikation. Diese vorbekannte biometrische Identifikation zeichnet sich unter anderem dadurch aus, dass eine Berechtigungsfreigabe des Fahrzeuges durch einen Benutzer auch dann erfolgen kann, wenn dessen Biometrieprofil nicht in dem entsprechenden Biometrieprofilspeicher hinterlegt ist.

[0006] Verfahren der eingangs genannten Art ist es gemeinsam, dass auf der Fahrzeugseite über Steuergeräte Funktionalitäten bzw. Komponenten aktiviert und gesteuert werden. Allerdings beschränken sich die herkömmlichen Verfahren im Wesentlichen auf den Diebstahlschutz bzw. auf die Fahrtberechtigung.

[0007] Hier setzt die Erfindung an, deren Aufgabe darin besteht, die Funktionalitäten in einem nicht unerheblichen Maße auszuweiten.

[0008] Mit einem Verfahren der eingangs bezeichneten Art wird diese Aufgabe gemäß der Erfindung durch das erfindungsgemäße Verfahren nach Anspruch 1 und das erfindungsgemäße System nach Anspruch 11 gelöst.

Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen.

[0009] Es wird ein Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen zur Verfügung gestellt, bei dem die Aktivierung eines Steuergerätes mittels einer Identifikation und/ oder Autorisierung des Nutzers erfolgt. Erfindungsgemäß ist vorgesehen, dass das Steuergerät mit einem externen Computer oder einem externen Computernetzwerk (Cloud) verbunden wird.

Das heißt, dass vorzugsweise bei Aktivierung des Steuergerätes wenigstens eine Funktion des Steuergerätes aktiviert wird. Es ist nicht zwingend notwendig, dass die Identifikation und/ oder Autorisierung das Steuergerät in den aktivierten Zustand versetzt.

Das heißt, dass das erfindungsgemäße Verfahren zum sicheren Betrieb fahrzeugnaher Applikationen eingerichtet ist. Dies sind Applikationen, die im Fahrzeug stattfinden oder in der Peripherie des Fahrzeuges stattfinden, zumindest jedoch im Mobilitätszusammenhang mit dem Fahrzeug stehen.

Mit dem erfindungsgemäßen Verfahren lässt sich eine sichere und eindeutige Identifikation bzw. Autorisierung des Nutzers realisieren.

Alternativ oder hinzukommend lässt sich auch eine Identifikation des verwendeten Fahrzeuges realisieren.

In bevorzugter Ausgestaltung des Verfahrens ist vorgesehen, dass zum Betrieb der fahrzeug-externen und/ oder fahrzeug-internen Applikation der externe Computer bzw. das externe Computernetzwerk (Cloud) auf die fahrzeug-externe und/ oder fahrzeug-interne Applikation steuernd einwirkt.

Die zur Steuerung benötigten Daten können gegebenenfalls visualisiert werden.

Insbesondere kann eine Inbetriebnahme und Nutzung der Applikationen mit dem Steuergerät mittels eines auf dem Steuergerät implementierten Rechtemanagements erfolgen. Vorzugsweise erfolgt die Autorisierung mittels eines auf dem Steuergerät implementierten Rechtemanagements.

Die Autorisierung kann z.B. mittels Nutzung von hierarchisch abgestuften Rechteebenen, die das Rechtemanagement umfasst, erfolgen.

Das bedeutet, dass eine elektronische Abbildung des Rechtemanagements erfolgt.

Vorzugsweise erfolgt die Identifikation und/ oder Autorisierung über ein persönliches, nutzergebundenes Endgerät.

Gegebenenfalls lassen sich zwecks Identifikation und/oder Autorisierung mehrere persönliche nutzergebundene Endgeräte einsetzen.

[0010] Das erfindungsgemäße Verfahren kann derart ausgeführt werden, dass die Identifikation und/ oder Autorisierung die Eingabe eines persönlichen, nutzergebundenen Codes umfasst.

Gegebenenfalls sind aus dem zu übertragenen Datenstrom personalisierte Anteile und anonymisierte Anteile herauszufiltern, dazu können Datenströme an bestimmten Punkten zu trennen sein.

[0011] Insbesondere kann zur Identifikation und/ oder Autorisierung das Steuergerät mit einem Mobilfunkendgerät mit berührungsempfindlichem Bildschirm verbunden werden.

Das heißt, dass vorzugsweise ein Smart-Phone zur Identifikation und/oder Autorisierung eingesetzt wird.

[0012] Das heißt, dass zur Eingabe des persönlichen, nutzergebundenen Codes auch ein Mobilfunkendgerät, insbesondere ein Mobilfunkendgerät mit optischer Aufnahmeeinrichtung, verwendet werden kann.
Vorzugsweise erfolgt die Identifikation und/ oder Autorisierung mittels Erkennung biometrischer Merkmale.
Zu diesem Zweck kann vorgesehen sein, dass das Steuergerät mit einem biometrischen Schlüssel verbunden wird.
Das heißt, dass die Identifikation und/oder Autorisierung mittels biometrischer Methoden erfolgen kann.

[0013] Das erfindungsgemäße Verfahren kann im Einzelnen dazu genutzt werden,

a) Berechtigungen zur Nutzung eines Fahrzeuges und/ oder Nutzung einzelner Fahrzeugfunktionen oder Funktionsbereiche zu realisieren, und/ oder

b) wenigstens einen fahrzeug-externen Bezahlvorgang auszulösen, und/ oder

c) auf Basis beim Fahrzeugbetrieb erhaltener Daten Entgelte, wie z.B. Nutzungsentgelte bzw. Versicherungstarife, zu berechnen, und/ oder

d) beim Versuch nicht-autorisierter Nutzung oder bei nicht-autorisierter Nutzung einen Alarm zu generieren, und/ oder

e) nutzergebundene persönliche Einstellungen im Fahrzeug zu realisieren, und/ oder

f) die Distanz einer jeweiligen Fahrt zu erfassen und zu erfassen, ob es sich dabei um eine Privatfahrt oder eine Geschäftsfahrt handelt.

Zu a): Es lassen sich insbesondere Berechtigungen (z.B. bei Fahrzeugklassen) oder Einschränkungen (z.B. bei Geschwindigkeiten) realisieren, im Fall von Flottenfahrzeugen auch Abrechnungen und weitere Dienste.

Zu b): Bezahlvorgänge, die eng im Zusammenhang mit der Fahrzeugnutzung stehen - im Sinne von "automotive Micropayment" bzw. einer "automobilen Geldbörse", lassen sich durchführen.

Zu c): Es lassen sich Bezahlvorgänge bzw. Gebührenabrechnungen für die Fahrzeugnutzung realisieren, ggf. auch abhängig vom persönlichen Fahrstil oder den realen Fahrbedingungen.

Zu d): Ein biometrischer Schlüssel kann in Notfällen als stiller oder offener Alarmgeber wirken.

Zu e): Über den Schlüssel lassen sich persönliche Einstellungen der Fahrzeugnutzer im Bereich Infotainment (Playlists etc.) und Komfort (Sitze, Spiegel, Klima etc.) managen.

Zu f): Es lässt sich z.B. mittels eines biometrischen Schlüssels (biometrische Identifikation) und dem Steuergerät die kilometergenaue Erfassung von Privat- und Geschäftsfahrten realisieren.

[0014] Das Rechtemanagement kann die Zugriffskontrolle von Nutzern und Anwendungen regeln.
Zum einen können dabei Rechte und Rollen, die ein Nutzer durch seine Authentifizierung gegenüber dem Steuergerät Databox bzw. dem Betriebssystem besitzt, verwaltet werden. Zum anderen lassen sich die Rechte managen, die Anwendungen bezüglich der erfassbaren Daten in dem Steuergerät und deren Weitergabe z.B. in das externe Computernetzwerk haben.
Der erste Aspekt behandelt die Definition verschiedener Nutzer bzw. Rollen, mit unterschiedlichen Befugnissen gegenüber dem System und auch dem Fahrzeug. Das schließt auch das Recht zum Starten bzw. Nutzen von Anwendungen mit ein. Dieses ist ähnlich einer klassischen Nutzerverwaltung auf Rechnersystemen zu verstehen. Der andere Aspekt beschreibt ein Rechtemanagement, mit dem ein Nutzer für Anwendungen festlegen kann, welche Rechte diese besitzen, bzw. welche Funktionalitäten diese benutzen dürfen. Zwischen den beiden genannten Aspekten kann es dabei auch zu Wechselwirkungen kommen.

[0015] Zur Lösung der Aufgabe wird außerdem ein System zur Verfügung gestellt, welches zur Durchführung des Verfahrens dient zwecks sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen.
Dieses System umfasst ein Fahrzeug, dem ein Steuergerät zugeordnet ist, sowie eine Einrichtung zur Aufnahme von Identifikations- und/ oder Autorisierungsinformationen eines Nutzers und mit wenigstens einer fahrzeug-extern und/ oder fahrzeug-intern angeordneten Applikation.
Das System weist weiterhin einen externen Computer oder ein externes Computernetzwerk (Cloud) auf, welcher bzw. welches mit dem Steuergerät verbindbar oder verbunden ist.

[0016] Vorzugsweise ist der externe Computer bzw. das externe Computernetzwerk (Cloud) derart eingerichtet und mit der fahrzeug-extern und/ oder fahrzeug-intern angeordneten Applikation derart verbindbar oder verbunden, dass mit dem externen Computer bzw. dem externen Computernetzwerk (Cloud) auf den Betrieb der fahrzeug-externen und/ oder fahrzeug-internen Applikation steuernd einwirkbar ist.
Das Steuergerät kann sowohl im Montageprozess des Fahrzeuges bei dessen Fabrikation eingebaut werden, als auch als zusätzliche Hardware nachgerüstet werden.
Das Fahrzeug kann als Träger unterschiedlicher Sensoren zur Erfassung von Daten zu Verkehrsumgebungszu-

ständen eingerichtet sein. Diese Daten betreffen die Umgebungsbedingungen für den Verkehr und das Fahrzeug selbst.

[0017] Zudem lässt sich ein Abgleich der realen Verkehrsumgebungszustände mit virtuellen Abbildern (maps, Topologiemodelle, ...) durchführen, aus dem heraus weitere Dienste entwickelt werden.
Die virtuellen Abbilder können im Steuergerät und/ oder in dem externen Computer bzw. externen Computernetzwerk gespeichert sein.

Aus diesen virtuellen Abbildern heraus können vielfältige Dienste bzw. Anwendungen realisiert werden, mit denen relevante und nutzbare Daten in Form von Signalen einzelnen Fahrzeugen (personalisiert), Gruppen von Fahrzeugen in einem Gebiet bzw. der Umgebung einer interessierenden Stelle oder Flotten übermittelt und verfügbar gemacht werden.
Das Fahrzeug wirkt also als (Car-)Sensor in einem übergreifenden Geschehen, bei dem im externen Computernetzwerk die reale Welt mit der virtuellen Welt verglichen wird und auf Modellbasis analysiert wird. In der entstehenden Sammlung der virtuellen Abbilder kann die verkehrsrelevante Situation jeder einzelnen Entität (d.h. Fahrzeuge, Verkehrsteilnehmer, Infrastruktur) in Echtzeit oder nahezu Echtzeit erfasst und ggf. auch vorrausschauend (Prediction) analysiert werden, um alle angeschlossenen Entitäten mit Diensten vor allem mit situativen Hinweisen zu versorgen. Dabei wirken sowohl die Fahrzeuge als auch die Dateninfrastruktur in dem externen Computernetzwerk und die Verkehrsinfrastruktur selbst je nach Situation und Dienst bzw. Anwendung als Sender und/oder Empfänger.

[0018] In günstiger Ausgestaltung des Systems ist vorgesehen, dass die Einrichtung zur Aufnahme von Identifikations- und/ oder Autorisierungsinformationen eine Einrichtung zur Biometriedatenerfassung ist.
Daneben sollte eine Audit-Funktionalität integriert sein.
Das System kann dabei auch derart ausgestaltet sein, dass nicht mehr konkrete Nutzer gegenüber dem System authentifiziert werden, sondern nur ein Token, das bestimmte Rechte beinhaltet.
Zusätzlich zur Einrichtung zur Biometriedatenerfassung kann das System auch eine Einrichtung zum Lesen des NFC-Chip im Führerschein aufweisen.

[0019] Das Computernetzwerk kann eine Cloud (Cloud-Computing) sein.

[0020] Das erfindungsgemäße System kann zur Ausführung einzelner Funktionen die folgenden Einrichtungen umfassen:

a) eine Einrichtung zur Erfassung der Berechtigung einer Person zur Nutzung eines Fahrzeuges und/ oder Nutzung einzelner Fahrzeugfunktionen oder Funktionsbereiche, und/ oder

b) eine Einrichtung zur Auslösung eines fahrzeugexternen Bezahlvorganges, und/ oder

c) eine Einrichtung zur Berechnung von Entgelten, wie z.B. Nutzungsentgelten bzw. Versicherungstarifen, auf Basis beim Fahrzeugbetrieb erhaltener Daten, und/ oder

d) eine Einrichtung zur Generierung eines Alarms beim Versuch nicht-autorisierter Nutzung oder bei nicht-autorisierter Nutzung des Fahrzeuges, und/ oder

e) wenigstens eine Einrichtung zur Realsierung nutzergebundener persönlicher Einstellungen im Fahrzeug, und/ oder

f) eine Einrichtung zur Erfassung der Distanz einer jeweiligen Fahrt sowie zur Erfassung, ob es sich dabei um eine Privatfahrt oder eine Geschäftsfahrt handelt.

Es soll dabei nicht ausgeschlossen sein, dass eine der erwähnten Einrichtungen auch die Funktion wenigstens einer der anderen Einrichtungen übernehmen kann.

[0021] Grundlegende Idee der Erfindung ist es, Fahrzeugnutzer in die Lage zu versetzen, nicht nur den sicheren Zugang zu Fahrzeugen zu realisieren, sondern auch auf eine Vielzahl von zusätzlichen Anwendungen bzw. "Diensten" im automobilen Umfeld und darüber hinaus zuzugreifen, und zwar über Softwareproduktionen von verschiedenen Herstellern, was sich wiederum insbesondere über eine Cloud realisieren lässt. Hierzu ist das Steuergerät vorzugsweise mit einem externen Computer oder Computernetzwerk, mit einer Cloud (Cloud-Computing) oder aber auch mit einem Smartphone verbunden. Eine vorteilhafte Ausgestaltung der Erfindung sieht dabei vor, dass die biometrische Identifikation über einen biometrischen Schlüssel, wie er beispielsweise in DE 20 2009 017 293 U1 und DE 20 2010 016 729 U1 offenbart ist, erfolgt.

[0022] Dieser biometrische Schlüssel ist eine externe Vorrichtung mit mindestens einem Speicher, der über ein serielles Bussystem mit dem Steuergerät verbindbar ist, wobei er einen Prozessor sowie ein USB-Laufwerk und ein biometrisches Mittel zur Identifikation einer Person aufweist. Der Prozessor, das USB-Laufwerk und das biometrische Mittel sind miteinander gekoppelt.

[0023] Der biometrische Schlüssel weist weiterhin eine ID-Identifizierungseinheit auf, zur Generierung eines Identifizierungscodes.

[0024] Außerdem weist der biometrische Schlüssel einen Microcontroller zum Lesen und Verifizieren des generierten Identifizierungscodes sowie des physiologischen Merkmals mittels Vergleich des Identifizierungscodes und des physiologischen Merkmals mit vorab abgespeicherten Informationen bzw. Daten auf, sowie eine Verschlüsselungseinrichtung zur Verschlüsselung bzw. Codierung des Identifizierungscodes und des physiologischen Merkmals zwecks Versendung des Identifizierungscodes und des physiologischen Merkmals an das

Steuergerät.

[0025] Zudem weist der biometrische Schlüssel eine Verschlüsselungseinheit auf. Somit können verschlüsselte sowie auch unverschlüsselte Bereiche auf einer Festplatte oder einem anderen Datenträger sowie auch Partitionen auf mehreren Festplatten des Steuergerätes verwaltet und vor unerlaubtem Zugriff geschützt werden. Des Weiteren kann der Zugriff auf unterschiedliche Betriebssysteme eines Systems für die verschiedenen Benutzer mit Hilfe des biometrischen Schlüssels geregelt werden.

[0026] Der biometrische Schlüssel weist weiterhin vorteilhafterweise eine ID-Identifizierungseinheit auf. Diese ID-Identifizierungseinheit dient zur Erzeugung von Identifizierungscodes. Dabei ist vorgesehen, weltweit einmalige 48-bit lange Identifizierungscodes mithilfe der ID-Identifizierungseinheit zu erzeugen. Kürzere bzw. längere Identifizierungscodes könnten ebenfalls erzeugt werden.

[0027] Der generierte Identifizierungscode wird ebenso wie das physiologische Merkmal vom Mikrocontroller des biometrischen Schlüssels gelesen und verifiziert. Dazu vergleicht der Mikrocontroller des biometrischen Schlüssels den Identifizierungscode sowie das physiologische Merkmal mit vorab abgespeicherten Informationen bzw. Daten. Zur weiteren Identifizierung durch das Steuergerät wird der Identifizierungscode zusammen mit dem physiologischen Merkmal in verschlüsselter bzw. codierter Form zum Steuergerät gesendet. Abschließend vergleicht das Steuergerät das übermittelte physiologische Merkmal sowie den übermittelten Identifizierungscode mit den auf dem Steuergerät abgelegten Informationen.

[0028] Vorteilhafterweise weist der biometrische Schlüssel einen Chip, insbesondere einen RFID-(Radio-Frequency-Identification) Chip auf. Dieser RFID-Chip, welcher zur Identifizierung mit Hilfe elektromagnetischer Wellen dient, ermöglicht die Realisierung zusätzlicher Funktionen wie z. B. Türöffner, Personenerfassung oder Zugangskontrolle.

[0029] Weiterhin kann der biometrische Schlüssel Mittel zur Temperaturerfassung, insbesondere einen Temperatursensor aufweisen. Der Einsatz eines Temperatursensors erhöht die Sicherheit beim Einlesen des Fingerabdrucks. Somit können z. B. mögliche Kopien eines Abdrucks vom eigentlichen Fingerabdruck unterschieden und erkannt werden.

[0030] In günstiger Ausgestaltung umfasst der biometrische Schlüssel einen USB-Stecker und/ oder einen Internetzugang, insbesondere einen WLAN-Zugang.

[0031] In weiterer vorteilhafter Ausgestaltung umfasst der biometrische Schlüssel mindestens einen Speicher in Form eines Arbeitsspeichers und/oder Festwertspeichers und ist mit einem Gehäuse versehen. Der biometrische Schlüssel kann die Bauform eines USB-Sticks aufweisen.

[0032] Vorzugsweise weist der biometrische Schlüssel des Weiteren ein Funkinterface auf. Bei diesem Funkinterface handelt es sich vorzugsweise um eine serielle Funkverbindung wie z. B. WLAN oder Bluetooth. Das Funkinterface kann dabei zusätzlich zur drahtgebundenen seriellen Schnittstelle, z. B. USB-Schnittstelle, vorgesehen sein.

[0033] Weiterhin ist es bevorzugt, dass der biometrische Schlüssel eine Stromversorgungseinheit aufweist. Dabei besteht die Stromversorgungseinheit aus einem kleinen Ladepuffer, z. B. Akku oder Batterie, sowie vorzugsweise einem zusätzlichen, leistungsstärkeren Akku, welcher sich beispielsweise in der Schutzkappe (z. B. Kappe des USB-Sticks) befindet. Vorzugsweise weist der biometrische Schlüssel eine Echtzeituhr auf, welche somit ständig über den Ladepuffer mit Spannung versorgt werden kann. Bei Betrieb des biometrischen Schlüssels über die drahtgebundene Schnittstelle, z. B. USB-Schnittstelle, findet die Stromversorgung über diese Schnittstelle durch das Steuergerät statt. Des Weiteren ist es vorgesehen, diese Schnittstelle zur Ladung des Ladepuffers sowie des zusätzlich vorgesehenen Akkus zu nutzen. Dazu wird bei Betrieb über die USB-Schnittstelle der Akku, welcher sich z. B. in der Schutzkappe der Vorrichtung befindet, in geeigneter Weise mit dem biometrischen Schlüssel zur Ladung verbunden. Zusätzlich zur Möglichkeit der Ladung über die USB-Schnittstelle ist auch eine Ladung mit einem externen Netzteil vorgesehen. Dies wird insbesondere bei Verwendung des biometrischen Schlüssels über das Funkinterface, z. B. WLAN oder Bluetooth, benötigt. Abhängig von der Kapazität des zusätzlichen Akkus kann der Betrieb über das Funkinterface auch ohne Verwendung eines externen Netzteils über einen längeren Zeitraum geschehen. Vorzugweise ist der biometrische Schlüssel derart ausgebildet, dass er zusätzlich zu den zur Identifikation benötigten sicherheitsrelevanten Daten auch Nutzerdaten in einem internen Speicher aufweist. Dazu hat der biometrische Schlüssel vorteilhafterweise einen zusätzlichen Flash-Baustein, z. B. NOR-Flash-Baustein. Abhängig vom Umfang der abzuspeichernden Nutzerdaten sowie deren Organisation könnte auch ein anderer Speicher, z. B. NAND-Flash-Baustein verwendet werden. Als Nutzerdaten können sämtliche benutzerabhängige Daten, wie z. B. Desktop-Daten abgelegt werden. Dies bietet z. B. den Vorteil, dass jeder Benutzer z. B. von ihm gewünschte bzw. häufig benutzte Informationen definieren und auf dem biometrischen Schlüssel ablegen kann. Z. B. können somit häufig benutzte Programme und Daten auf dem Desktop durch Links für den Nutzer nach erfolgter Identifizierung schnell zugänglich gemacht werden. Des Weiteren können Hierarchieinformationen, wie z. B. benutzerabhängige Rechte abgespeichert werden.

[0034] Dies ermöglicht es, dass sämtliche sicherheitsrelevante Daten auf dem für den Benutzer jederzeit zugreifbaren biometrischen Schlüssel abgelegt und gespeichert sind, so dass maximale Sicherheit gewährleistet ist. Zudem ist gegeben, dass zum Starten des Steuergerätes ein passendes Passwort sowie ein physiologisches Merkmal des Benutzers ausreichend sind.

[0035] Weiterhin kann der biometrische Schlüssel einen Kryptochip aufweisen, wobei der Prozessor, das biometrische Mittel und der Kryptochip miteinander gekoppelt sind. Dadurch lassen sich biometrische Daten des Nutzers und eine entsprechende ID direkt auf den Kryptochip schreiben. Für die Datensicherheit verfügt der Kryptochip über klar strukturierte Sicherheitsarchitekturen und weist eine Vielzahl äußerst flexibler Schutzmechanismen auf, wie zum Beispiel:

- Unterschiedliche Life-Cycle-Phasen zur Kontrolle der zulässigen Kommandos;
- Schutz aller Datenobjekte mit bis zu 127 verschiedenen Zugriffsrechten pro Verzeichnisebene;
- Logische Kombinationen der Zugriffsrechte in hoher Komplexität;
- Schutz aller Datenobjekte mittels eigener feingranularer Access Kondition Schemata;
- Sichere Speicherung von PINs und Schlüssel als Objekte;
- ein eigenes Betriebssystem.

[0036] Mit Hilfe des biometrischen Schlüssels lässt sich eine Verifikation einer Zugangsberechtigung eines Benutzers des Fahrzeuges vornehmen, bei dem zur Verifikation biometrische Daten des Benutzers mittels des biometrischen Schlüssels erfasst und erkannt werden.

[0037] Im Rahmen der Erfindung sind folgende Anwendungsbereiche der Erfindung denkbar:

- Individueller Zugang zum Fahrzeug
- Zugang zu Fahrzeugen im Carsharing
- Mikropayment im automobilen Umfeld und darüber hinaus
- Dienste im Bereich Sicherheit und Comfort im Zusammenwirken insbesondere mit einer Cloud.

Individueller Zugang zum Fahrzeug

[0038] Fahrzeugschlüssel sind heute im Wesentlichen Funkfernbedienungen, mit denen sowohl der "Remote Keyless Entry" als auch zunehmend der "Passive Keyless Entry inkl. KeylessGo" realisiert werden kann - also der Zugang zum Fahrzeug und der Start desselben lediglich auf Basis der mitgeführten Schlüsseleinheit. Derartige Systeme haben nicht nur den Komfort beim Zugang zum Fahrzeug, sondern durch Verschlüsselungsverfahren für die relevanten Signale auch den Diebstahlschutz erheblich verbessert. Die Ergänzung derartiger Systeme durch biometrische Verfahren in Gestalt beispielsweise der in den DE 20 2009 017 293 U1 und DE 20 2010 016 729 U1 offenbarten Vorrichtungen (Schlüssel) erfolgt in Verbindung mit dem erfindungsgemäßen Verfahren. Dabei kann aus dem Fingerabdruck des Nutzers auf dem Schlüssel vorzugsweise ein Zertifikat erzeugt werden, das mit einem in dem Fahrzeug hinterlegten Zertifikat vorzugsweise in einem PKI-Prozess (Public-Key-Infrastruktur) abgeglichen wird und der aufgrund inhärenter Mechanismen eine hohe intrinsische Sicherheit hat. Die Nutzung des Fahrzeuges wird damit nur für identifizierte und autorisierte Personen möglich. Ein derartiger biometrischer Schlüssel in Verbindung mit dem erfindungsgemäßen Verfahren könnte also - bei Beibehaltung aller Komfort- und Sicherheitsmerkmale bisheriger Zugangssysteme - zunächst den Diebstahlschutz für Fahrzeuge deutlich steigern.

Zugang zu Fahrzeugen im Carsharing

[0039] Die Verbreitung des Carsharing in urbanen Ballungsräumen, das mit dem Übergang vom "Besitz" zur "Nutzung" von Fahrzeugen verbunden ist, stellt die Rolle des althergebrachten "Autoschlüssels" in Frage. Dessen Funktionalitäten könnten im Rahmen des erfindungsgemäßen Verfahrens in ein Smartphone integriert werden. Die Integration der biometrischen Identifikation, vorzugsweise über biometrische Schlüssel, in Verbindung mit dem erfindungsgemäßen Verfahren ermöglicht dabei eine eineindeutige Zuordnung des Fahrers/Nutzers zu "seinem" Schlüssel, um in jeder Hinsicht sichere Zugänge zu den Fahrzeugen darzustellen, die er dauerhaft oder temporär fahren will und darf. Dies umfasst neben dem "eigenen" Fahrzeug auch eine Flotte von (vielen) Fahrzeugen - neben Carsharing auch Mietwagen oder Unternehmensflotten - die der Fahrer lediglich "nutzt", aber nicht "besitzt". Damit werden auch Berechtigungen (z.B. bei Fahrzeugklassen) oder Einschränkungen (z.B. bei Geschwindigkeiten) realisiert, im Fall von Flottenfahrzeugen auch Abrechnungen und weitere Dienste.

Micropayment im automobilen Umfeld und darüber hinaus

[0040] Das erfindungsgemäße Verfahren eröffnet zusammen mit den entsprechenden Cloud-Funktionalitäten und dem fahrzeugseitigen Steuergerät auch Möglichkeiten zu einem universalen Bezahlmechanismus. Dies gilt besonders bei Bezahlvorgängen, die eng im Zusammenhang mit der Fahrzeugnutzung stehen - im Sinne von "automotive Micropayment" bzw. einer "automobilen Geldbörse".

Parkschein- und Maut-Assistent

[0041] Mit einer über das erfindungsgemäße Verfahren realisierten Micropaymentfunktion könnten Bezahlvorgänge beim Parken sowohl im öffentlichen Raum als auch in Parkhäusern realisiert werden. Es würde eine zusammenfassende "Parkrechnung" für alle in einem bestimmten Zeitraum realisierten Parkvorgänge erzeugt werden können. Zudem wären Abrechnungen für verschiedene Mautsysteme möglich, ggf. auch unter Ermittlung optimaler Mautgebühren und der Erstellung einer

turnusmäßigen "Mautrechnung". Mit diesem Assistenten ließen sich also alle Bezahlvorgänge bzw. Gebührenabrechnungen für das "Durchfahren und Parken" bzw. die Straßen- und Parkraumbenutzung oder allgemeiner für die Verkehrsraumbenutzung realisieren.

"Pay-as-you"-Drive-Assistent

[0042] Verschiedene Daten über die Nutzung des Fahrzeugs könnten über die biometrische Identifikation, vorzugsweise über einen biometrischen Schlüssel, das Steuergerät und die Cloud-Funktionalitäten detailliert erfasst und in fahrzeugexterne Zielsysteme übertragen werden. Entsprechend der Nutzung, die auch tatsächliche Fahrstile und -profile umfassen kann, könnten Nutzungsentgelte für Carsharing oder Mietwagenflotten oder auch individuelle Versicherungstarife berechnet werden. Mit diesem Assistenten ließen sich also alle Bezahlvorgänge bzw. Gebührenabrechnungen für die Fahrzeugnutzung an sich realisieren, ggf. auch abhängig vom persönlichen Fahrstil oder den realen Fahrbedingungen.

Lade-/Tank-Assistent

[0043] Mit einer über das erfindungsgemäße Verfahren realisierten Micropaymentfunktion könnten zukünftig auch Ladevorgänge für Elektrofahrzeuge an öffentlichen Ladestationen bzw. - säulen sicher und komfortabel abgewickelt werden. Ähnliches würde für konventionelle Tankstellen gelten, die schon heute ohne Service bzw. Bezahlschalter an Shopping-Centern oder Baumärkten betrieben werden. In beiden Fällen könnten heutige Lösungen (Smartcards, Kreditkarten etc.) ergänzt, ersetzt und perspektivisch vereinheitlicht werden. Mit diesem Assistenten ließen sich also alle Bezahlvorgänge bzw. Gebührenabrechnungen im Umfeld der "Energiebereitstellung für das Fahrzeug" realisieren und eine turnusmäßige "Energierechnung" für das Fahrzeug erzeugen.

Macropayment

[0044] Darüber hinaus könnte das erfindungsgemäße Verfahren noch für vielfältige alltägliche Bezahlfunktionen der Kunden im Sinne einer Kreditkarte genutzt werden, sowohl automobilnah (Tankstellen konventionell, Werkstätten etc.) als auch im Kontext von Mobilität (Fahrkarten für den ÖPNV, die Bahn, Bike-Sharing, Flugzeuge etc., also "Tickets") und in allgemeinen Anwendungen (Supermarkt, Internet etc.).

Fahrberechtigungs-Assistent

[0045] Im Rahmen des erfindungsgemäßen Verfahrens könnte die aktuell gültige Fahrberechtigung bzw. der Führerscheinstatus des Fahrers in einem biometrischen Schlüssel hinterlegt sein inkl. dauerhafter oder temporärer Einschränkungen oder Erweiterungen. Im privaten Bereich könnten z.B. Einschränkungen für Fahranfänger oder Senioren bei zulässigen Höchstgeschwindigkeiten wirksam werden. Über fahrzeugbezogene Funktionen der Databox könnte der Tempomat des Fahrzeugs angesteuert werden. Für Flotten (besonders Carsharing- und Verleihfirmen, auch Unternehmensflotten) wären etwa aktuelle Fahrverbote relevant.

Notfall-Assistent

[0046] Gemäß dem erfindungsgemäßen Verfahren könnte ein biometrischer Schlüssel in Notfällen als stiller oder offener Alarmgeber wirken. In kritischen Situationen wie Carjacking könnte über eine besondere Funktionalität des Schlüssels, den sogenannten "Notfinger" , bei dem ein anderer als der eingelernte Finger aufgelegt wird, ein Notsignal ausgelöst werden, das an eine Alarmzentrale gesendet wird. Neben der Alarmübermittlung können durch die Aufnahme und Übertragung von Bildern und Tönen aus dem Innenraum an die Alarmzentrale Situationen bewertet und geeignete Maßnahmen eingeleitet werden. Im Fall offensichtlicher Notfälle bzw. Notlagen sowohl bei Pannen als auch bei Unfällen könnte über die sichere Authentifizierung des Fahrers die eCall-Funktion von Fahrzeugen aufgewertet werden.

Remote-Assistent

[0047] Das erfindungsgemäße Verfahren kann vorzugsweise auch der Remote-Überwachung des Fahrzeugs dienen. Mit einer indirekten Funkverbindung über ein Smartphone, die auch über mittlere (WLAN) oder größere Distanzen (GPS/LTE) wirksam ist, könnten mit einem biometrischen Schlüssel Diebstähle (das Fahrzeug wird unauthorisiert bewegt) oder Beschädigungen (Parkrempler/Vandalismus) angezeigt werden. Dazu müssten entsprechende Sensorsignale aus dem Fahrzeug über das Steuergerät aufgenommen, interpretiert und (ggf. über den "Umweg" des Smartphones) an den Schlüssel bzw. den Nutzer übertragen werden. Zudem ist eine Ortung und Verfolgung eines gestohlenen Fahrzeuges möglich.

Identitäts- und Einstellungs-Assistent

[0048] Über den Schlüssel könnten persönliche Einstellungen der Fahrzeugnutzer im Bereich Infotainment (Playlists etc.) und Komfort (Sitze, Spiegel, Klima etc.) gemanagte werden - besonders bei der Nutzung von mehreren Fahrzeugen oder bei Flotten bzw. im Carsharing, auch im Sinne von Rollen bzw. Identitäten (als Privatperson oder geschäftlich). Dazu könnten auch die Ermittlung und die Empfehlung einer in Bezug auf die Rückhaltesysteme optimalen Sitzposition inkl. Der Einstellungen des Lenkrads gehören. Diese Position könnte ausgehend von den einmal erfassten biometrischen Daten des Fahrers ebenso für jedes andere Fahrzeug, das von

ihm benutzt wird (Carsharing, Mietwagen etc.), berechnet und angezeigt bzw. empfohlen werden.

Fahrtenbuch(-Assistent)

[0049] Im Rahmen des erfindungsgemäßen Verfahrens könnte zudem über einen biometrischen Schlüssel (biometrische Identifikation) und das Steuergerät die kilometergenaue Erfassung von Privat- und Geschäftsfahrten realisiert werden - entsprechend den Regeln der Finanzämter, ohne Zusatzaufwand bei Fahrern und/ oder Flottenbetreibern und mit sicherer elektronischer Übertragung aller relevanten Daten in geschäftliche und/oder behördliche Datenbanken bzw. Zielsysteme.

Service-Assistent

[0050] Auch wären über den Schlüssel und das Steuergerät bei entsprechender Autorisierung auch spezifische Daten über Fahrzeugzustände, die über schon heute auf Schlüsseln oder in IT-Systemen hinterlegte Daten hinausgehen, abrufbar und sowohl privat als auch im Flottenbetrieb nutzbar. Die sichere Authentifizierung, Autorisierung und Verschlüsselung könnte auch das "Remote-Flashen" von Fahrzeug- Software erleichtern, die "Freischaltung" von Softwarefunktionen oder eine sichere Ansprache der Nutzer etwa im Falle von Rückrufaktionen unterstützen (bidirektionale Nutzung).

[0051] Ein besonderes Potenzial ergibt sich gemäß der Erfindung aus der möglichen Verknüpfung der beschriebenen Anwendungen aus den vier Bereichen - entweder im Bereich der Dienste und/oder im Bereich der Daten.

[0052] Die Verknüpfung der Dienste im Bereich "Micropayment im automobilen Umfeld" liegt sehr nahe: Die Fahrzeugbenutzung ("Pay-as-you"-Drive-Assistent) ist kaum von Park- und Mautabrechnungen und Lade- oder Tankvorgängen zu trennen, dürfte aber ebenso von einer Verknüpfung mit den beschriebenen Anwendungen bzw. Diensten aus dem Sicherheits- und Komfortbereich profitieren, etwa dem Fahrtenbuch.

[0053] Das "Micropayment" könnte im Rahmen der Erfindung darüber hinaus bei allen Mobilitätsaktivitäten des Nutzers wirksam werden, vor allem bei Mobilitätsangeboten des ÖPNV und der Bahn. Dies entspräche eher dem "Macropayment" und einer Erweiterung der Funktionalitäten. Diese Erweiterung wäre auch beim Anwendungsbereich "Zugang" denkbar: sowohl in andere mobile Bereiche wie den Zugang zu eigenen oder gemieteten Mikromobilen oder Nutzfahrzeugen sowie in andere Domänen wie die Zugänge zu privaten Wohnräumen, Büros bzw. Arbeitsumgebungen oder Hotels ("Türöffner"). Damit wären auch Dienste wie eine Zeiterfassung im beruflichen Umfeld oder in sicherheitskritischen Umgebungen möglich.

[0054] Beim Anwendungsbereich "Dienste für Sicherheit und Komfort" steht vor allem die Verknüpfung und Integration der entstehenden Daten im Vordergrund, mit dem die Dienste an sich verbessert werden können (etwa Integration der Daten für Fahrberechtigungen sowie Identitäten und Einstellungen). Als softwaregestützte Anwendungen sind sie gleichzeitig aber auch "Apps".

[0055] Zudem sieht die Erfindung ein System zur Durchführung des Verfahrens gemäß einem der Ansprüche 1 bis 5 vor, das ein Fahrzeug, dem ein Steuergerät zugeordnet ist, und eine Biometriedatenerfassung aufweist, beinhaltet. Das System zeichnet sich dabei dadurch aus, dass es zusätzlich ein Netzwerk aufweist, das mit dem Steuergerät verbindbar ist.

[0056] Auch ist im Rahmen der Erfindung ein Verfahren denkbar, bei dem das System/die Plattform ein gestuftes und differenziertes Rechtemanagement zur Inbetriebnahme und Nutzung der Applikationen sowie günstigen Funktionalitäten der Plattform realisiert. Hierzu ist vorzugsweise auf dem Steuergerät ein Rechtemanagement implementiert.

[0057] Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aufgrund der nachfolgenden Beschreibung sowie anhand der Zeichnung. Es zeigt in schematischer Darstellung:

Fig.1 System zur Durchführung des erfindungsgemäßen Verfahrens und

Fig.2 die Funktionsweise des erfindungsgemäßen Verfahrens.

[0058] Das System wird im Wesentlichen von den folgenden Komponenten gebildet:

- Mittel zur biometrischen Identifikation 2
- Fahrzeug 4
- Steuergerät 3, das dem Fahrzeug 4 zugeordnet ist,
- Computernetzwerk (Cloud) 5.

[0059] Das Verfahren beginnt mit der biometrischen Erfassung eines Merkmales des Benutzers1 durch ein Mittel 2 zur biometrischen Identifikation.

[0060] In dem in Fig. 1 dargestellten Ausführungsbeispiel liegt das Mittel zur biometrischen Identifikation in Gestalt eines Fahrzeugschlüssels vor. Der Fahrzeugschlüssel beinhaltet die biometrische Sensorik sowie die Signalverarbeitung, ebenso entsprechende Funktechnologien zur Verbindung mit dem Fahrzeug 4, d.h. verschiedene Nieder- und Hochfrequenzfunkstrecken.

[0061] Über das Mittel 2 wird das Steuergerät 3 des Fahrzeuges 4 aktiviert. Das Steuergerät 3 umfasst Technologien wie GPS, GSM-LTE, BT, SD-Cards, CAN-/Antennenanbindung und entsprechende Mikrocontroller sowie eine zentrale Verarbeitungseinheit mit dauerhaften und temporären Speichern, entsprechenden Betriebssystemen und API. Hierdurch ist gewissermaßen ein "universales" Steuergerät mit Cloud-Anbindung ge-

geben, wobei das Steuergerät mit dem Netzwerk 5, welches in Gestalt einer Cloud vorliegt, verbunden ist. Bei dieser Datenverbindung handelt es sich um eine sichere, redundante und teils hochperformante Verbindung, sowohl für ereignisgesteuerte als auch für zeitgesteuerte Prozesse bzw. Datenströme.

[0062] Fig. 2 veranschaulicht das Funktionsprinzip bzw. die Plattform zum sicheren Betrieb fahrzeugnaher Applikationen. Kernbestandteil dieser Plattform sind das Steuergerät 3, das Mittel 2 zur biometrischen Identifikation sowie das angebundene Computernetzwerk (Cloud) 5. Weiterhin zeichnet sich das Verfahren, wie aus Fig. 2 weiter hervorgeht, dadurch aus, dass Schnittstellen 7, 8 zwischen Computernetzwerk (Cloud) 5 und mobilen Endgeräten 11 sowie Schnittstellen 9, 10 zwischen dem Fahrzeug 4 und dem Schloss 12 bzw. zwischen dem Schloss 12 und mobilen Endgeräten 11, wie beispielsweise Smartphone, bestehen. In dem Computernetzwerk (Cloud) 5 werden dabei applikationsspezifische Daten aus dem Steuergerät 3 verarbeitet. Im Rahmen der Erfindung werden auch weitere Datenbestände 6 herangezogen, um weitere Anwendungen zu ermöglichen.
Das Fahrzeug 4 weist typische Fahrzeug-bezogene Funktionen auf, die die Integrität des Fahrzeuges 4 betreffen. Es sollte einen hohen Sicherheitsstandard aufweisen. Vorteilhafterweise ist es für das sogenannte "eCall" eingerichtet, das heißt für ein automatisches Notrufsystem für Kraftfahrzeuge, welches bei einem Unfall einen Notruf auslöst, der einen Minimaldatensatz direkt an eine Notrufzentrale absetzt. Zeitgleich wird eine Sprachverbindung aufgebaut. Das Steuergerät 3 dient dem sicheren Betrieb der erfindungsgemäß zu betreibenden Applikationen und lässt sich vorteilhafterweise anwendungsspezifisch aktualisieren.

[0063] Als Endgerät 11 lässt sich bevorzugt eine typische Mensch-Maschine-Schnittstelle (ein sogenanntes HMI-Device) einsetzen, welches den Vorteil der Mobilität mit flexibler Aktualisierungsmöglichkeit bzw. Austauschbarkeit verbindet. Ein solches Endgerät kann zudem eine Sensor-Funktion übernehmen und / oder für das Datenübertragungsverfahren 3G geeignet sein bzw. entsprechend des Mobilfunkstandard LTE eingerichtet sein. Zudem kann das Endgerät 11 selbst eine Speicherfunktion, z.B. für die Sammlung der virtuellen Abbilder, übernehmen.
Die Schnittstellen 7, 8, 9 und 10 sind vorzugsweise als Funkverbindungen ausgeführt.
Die Datenbestände 6 können Datenmengen sammeln, die zu komplex oder zu groß sind, um sie mit manuellen und klassischen Methoden der Datenverarbeitung auszuwerten, sogenannte Big-Data. Die Verbindung zwischen diesem Datenbestand und dem externen Computer bzw. dem externen Computernetzwerk erfolgt vorzugsweise über das Internet.
Natürlich ist die beschriebene Ausführungsform der Erfindung noch in vielfacher Hinsicht abzuändern, ohne den Grundgedanken der Erfindung zu verlassen. Beispielsweise könnte in das System noch ein Smartphone eingebunden bzw. integriert werden.

Bezugszeichenliste:

[0064]

1 Benutzer
2 Mittel
3 Steuergerät
4 Fahrzeug
5 Computernetzwerk
6 Datenbestände
7, 8, 9 10 Schnittstellen
11 Endgeräte
12 Schloss

Patentansprüche

1. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen, bei dem die Aktivierung eines Steuergerätes (3) mittels einer Identifikation und/ oder Autorisierung des Nutzers erfolgt,
dadurch gekennzeichnet,
dass das Steuergerät (3) mit einem externen Computer oder einem externen Computernetzwerk (Cloud) (5) verbunden wird.

2. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen,
dadurch gekennzeichnet,
dass zum Betrieb der fahrzeug-externen und/ oder fahrzeug-internen Applikation der externe Computer bzw. das externe Computernetzwerk (Cloud) (5) auf die fahrzeug-externe und/ oder fahrzeug-interne Applikation steuernd einwirkt.

3. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** eine Inbetriebnahme und Nutzung der Applikationen mit dem Steuergerät (3) mittels eines auf dem Steuergerät (3) implementierten Rechtemanagements erfolgt.

4. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach Anspruch 3, **dadurch gekennzeichnet, dass** die Autorisierung mittels Nutzung von hierarchisch abgestuften Rechteebenen, die das Rechtemanagement umfasst, erfolgt.

5. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der vorhergehenden Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** die Identifikation und/ oder Autorisierung über ein persönliches, nutzerge-

bundenes Endgerät erfolgt.

6. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Identifikation und/ oder Autorisierung die Eingabe eines persönlichen, nutzergebundenen Codes umfasst.

7. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der Ansprüche 5 und 6, **dadurch gekennzeichnet, dass** zur Identifikation und/ oder Autorisierung das Steuergerät (3) mit einem Mobilfunkendgerät mit berührungsempfindlichem Bildschirm verbunden wird.

8. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Identifikation und/ oder Autorisierung mittels Erkennung biometrischer Merkmale erfolgt.

9. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach Anspruch 8, **dadurch gekennzeichnet, dass** das Steuergerät (3) mit einem biometrischen Schlüssel verbunden wird.

10. Verfahren zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass**

a) Berechtigungen zur Nutzung eines Fahrzeuges und/ oder Nutzung einzelner Fahrzeugfunktionen oder Funktionsbereiche realisiert werden, und/ oder
b) wenigstens ein fahrzeug-externer Bezahlvorgang ausgelöst wird, und/ oder
c) auf Basis beim Fahrzeugbetrieb erhaltener Daten Entgelte, wie z.B. Nutzungsentgelte bzw. Versicherungstarife, berechnet werden, und/ oder
d) beim Versuch nicht-autorisierter Nutzung oder bei nicht-autorisierter Nutzung ein Alarm generiert wird, und/ oder
e) nutzergebundene persönliche Einstellungen im Fahrzeug realisiert werden, und/ oder
f) die Distanz einer jeweiligen Fahrt erfasst wird und erfasst wird, ob es sich dabei um eine Privatfahrt oder eine Geschäftsfahrt handelt.

11. System zur Durchführung des Verfahrens zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen gemäß einem der Ansprüche 1 bis 10, mit einem Fahrzeug (4), dem ein Steuergerät (3) zugeordnet ist, sowie mit einer Einrichtung zur Aufnahme von Identifikations- und/ oder Autorisierungsinformationen eines Nutzers, und mit wenigstens einer fahrzeug-extern und/ oder fahrzeug-intern angeordneten Applikation,
dadurch gekennzeichnet,
dass das System weiterhin einen externen Computer oder ein externes Computernetzwerk (Cloud) (5) aufweist, welcher bzw. welches mit dem Steuergerät (3) verbindbar oder verbunden ist.

12. System zur Durchführung des Verfahrens zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach Anspruch 11,
dadurch gekennzeichnet,
dass der externe Computer bzw. das externe Computernetzwerk (Cloud) (5) derart eingerichtet und mit der fahrzeug-extern und/ oder fahrzeug-intern angeordneten Applikation derart verbindbar oder verbunden ist, dass mit dem externen Computer bzw. dem externen Computernetzwerk (Cloud) (5) auf den Betrieb der fahrzeug-externen und/ oder fahrzeug-internen Applikation steuernd einwirkbar ist.

13. System zur Durchführung des Verfahrens zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der Ansprüche 11 und 12,
dadurch gekennzeichnet,
dass die Einrichtung zur Aufnahme von Identifikations- und/ oder Autorisierungsinformationen eine Einrichtung zur Biometriedatenerfassung ist.

14. System zur Durchführung des Verfahrens zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der Ansprüche 11 bis 13, **dadurch gekennzeichnet, dass** das Computernetzwerk eine Cloud (Cloud-Computing) ist.

15. System zur Durchführung des Verfahrens zum sicheren Betrieb fahrzeug-externer und/ oder fahrzeug-interner Applikationen nach einem der Ansprüche 11 bis 14, **dadurch gekennzeichnet,**
dass es weiterhin umfasst:

a) eine Einrichtung zur Erfassung der Berechtigung einer Person zur Nutzung eines Fahrzeuges und/ oder Nutzung einzelner Fahrzeugfunktionen oder Funktionsbereiche, und/ oder
b) eine Einrichtung zur Auslösung eines fahrzeug-externen Bezahlvorganges, und/ oder
c) eine Einrichtung zur Berechnung von Entgelten, wie z.B. Nutzungsentgelten bzw. Versicherungstarifen, auf Basis beim Fahrzeugbetrieb erhaltener Daten, und/ oder
d) eine Einrichtung zur Generierung eines Alarms beim Versuch nicht-autorisierter Nut-

zung oder bei nicht-autorisierter Nutzung des Fahrzeuges, und/ oder
e) wenigstens eine Einrichtung zur Realsierung nutzergebundener persönlicher Einstellungen im Fahrzeug, und/ oder
f) eine Einrichtung zur Erfassung der Distanz einer jeweiligen Fahrt sowie zur Erfassung, ob es sich dabei um eine Privatfahrt oder eine Geschäftsfahrt handelt.

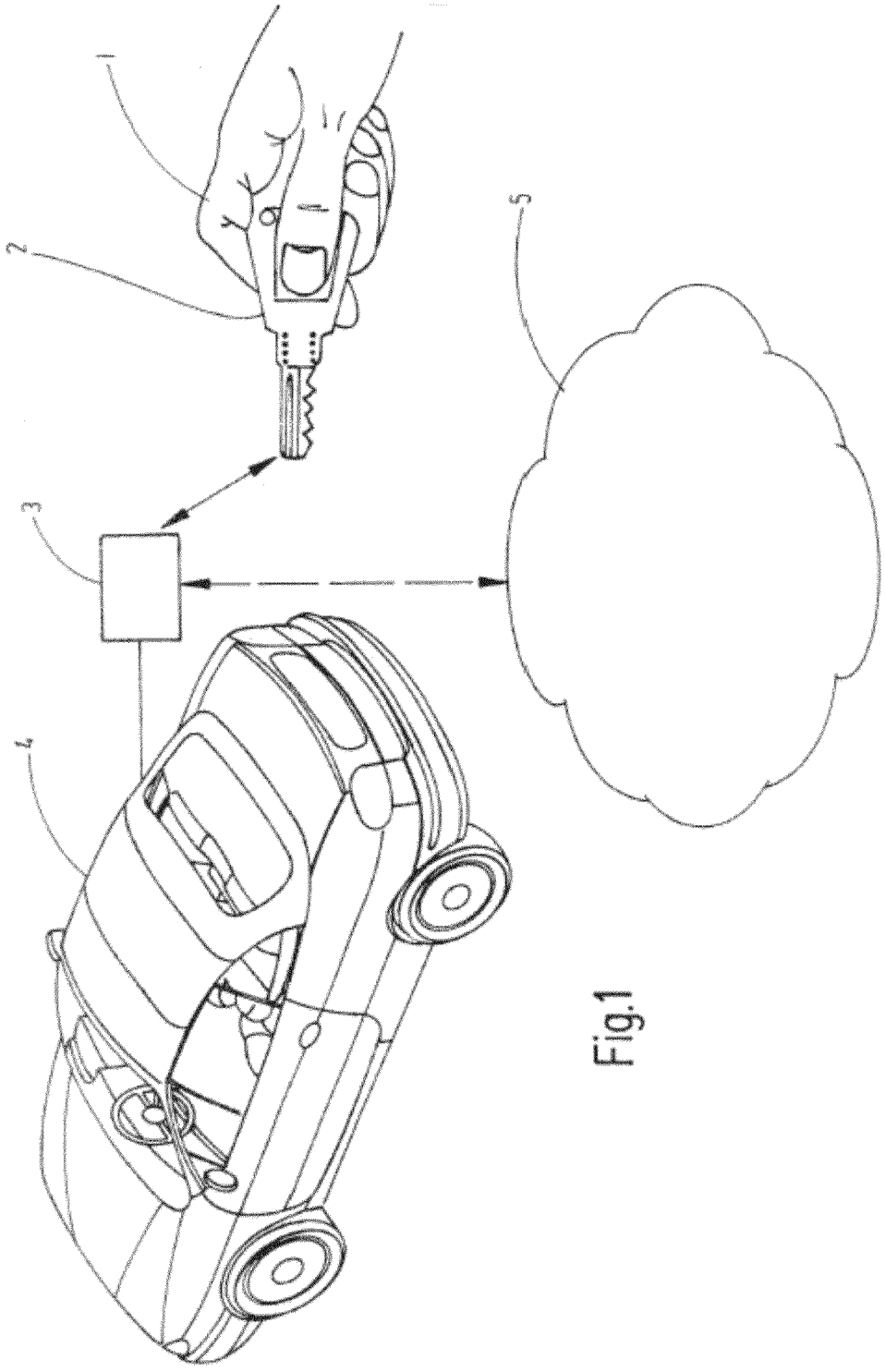

Fig.1

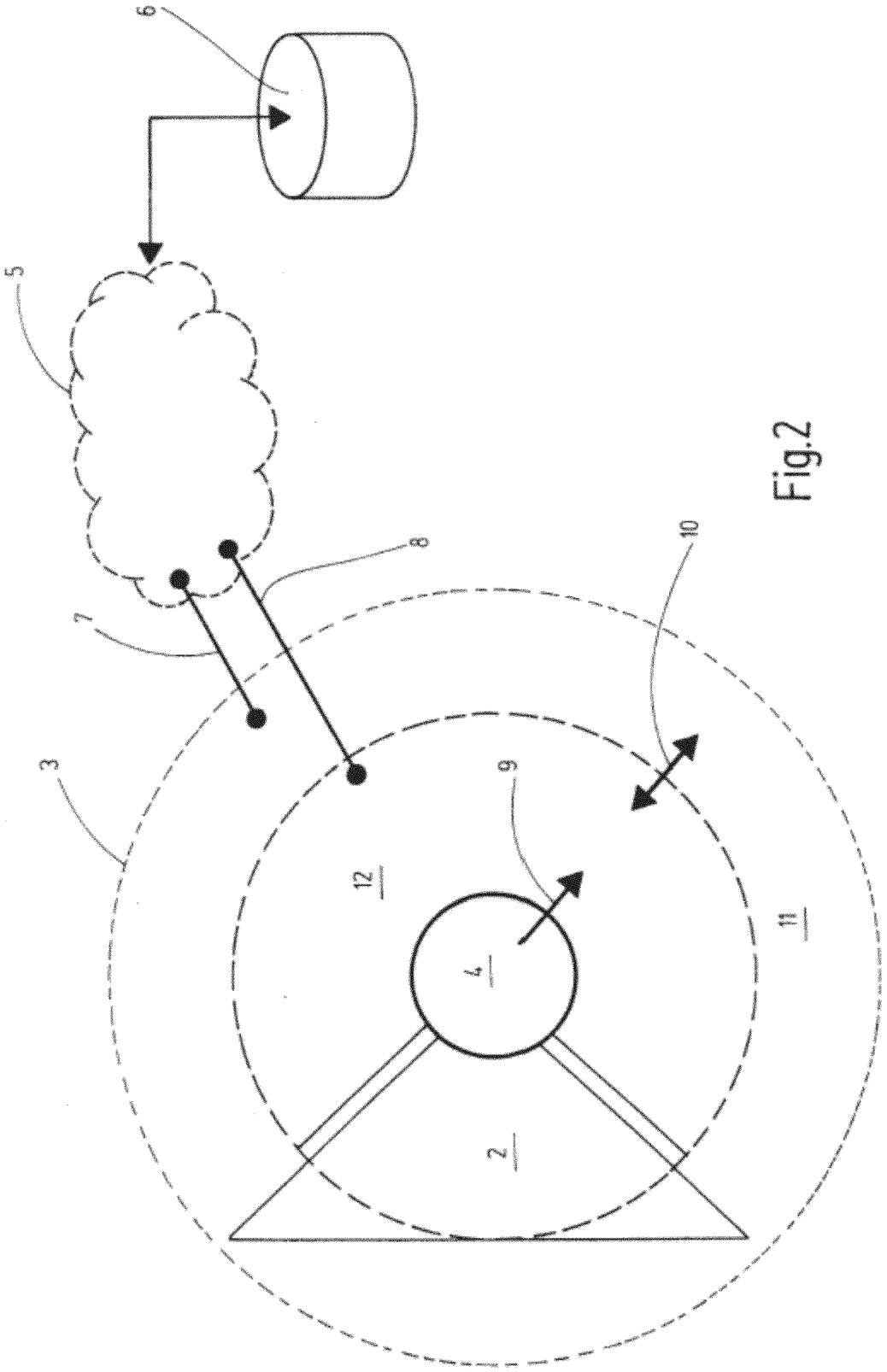

Fig.2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 14 17 3285

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	DE 10 2011 118234 A1 (AUDI NSU AUTO UNION AG [DE]) 16. Mai 2013 (2013-05-16)	1-3,5-7, 10-12, 14,15	INV. G07C9/00
Y	* Zusammenfassung * * Absatz [0011] - Absatz [0017] * * Absatz [0022] - Absatz [0027] * * Absatz [0039] - Absatz [0044] *	4,8,9	

X	DE 20 2010 016729 U1 (BRAUN UWE PETER [DE]) 24. März 2011 (2011-03-24)	1-3,5-7, 10-15	
Y	* Zusammenfassung * * Absatz [0010] - Absatz [0013] * * Absatz [0023] - Absatz [0024] * * Absatz [0028] *	4,8,9	

X	EP 2 602 133 A1 (WESTFALIA AUTOMOTIVE GMBH [DE]) 12. Juni 2013 (2013-06-12) * Zusammenfassung * * Absatz [0001] - Absatz [0033] * * Absatz [0060] - Absatz [0078] *	1-3,5-7, 10-12,15	
	-----		RECHERCHIERTE SACHGEBIETE (IPC)
X	DE 10 2010 052099 A1 (DAIMLER AG [DE]) 7. Juli 2011 (2011-07-07) * Zusammenfassung * * Absatz [0008] - Absatz [0017] *	1,2,5-7, 10-12, 14,15	G07C

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	16. Oktober 2014	Teutloff, Ivo

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 14 17 3285

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

16-10-2014

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102011118234 A1	16-05-2013	CN 103918014 A	09-07-2014
		DE 102011118234 A1	16-05-2013
		EP 2777309 A1	17-09-2014
		US 2014298023 A1	02-10-2014
		WO 2013068074 A1	16-05-2013
DE 202010016729 U1	24-03-2011	KEINE	
EP 2602133 A1	12-06-2013	DE 102011120651 A1	13-06-2013
		EP 2602133 A1	12-06-2013
DE 102010052099 A1	07-07-2011	KEINE	

EPO FORM P0461

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

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- EP 0645286 B1 **[0004]**
- EP 1112204 B1 **[0005]**
- DE 202009017293 U1 **[0021] [0038]**
- DE 202010016729 U1 **[0021] [0038]**