



(10) **DE 10 2018 103 101 A1** 2018.08.16

(12)

Offenlegungsschrift

(21) Aktenzeichen: **10 2018 103 101.7**

(22) Anmeldetag: **12.02.2018**

(43) Offenlegungstag: **16.08.2018**

(51) Int Cl.: **H04L 9/00 (2006.01)**

H04L 9/32 (2006.01)

(30) Unionspriorität:

15/432,886

14.02.2017

US

(71) Anmelder:

**Ford Global Technologies, LLC, Dearborn, Mich.,
US**

(74) Vertreter:

**Bonsmann · Bonsmann · Frank Patentanwälte,
41063 Mönchengladbach, DE**

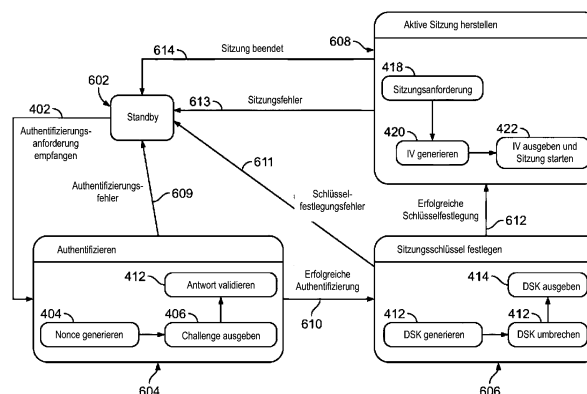
(72) Erfinder:

**Smyth, Cameron, Wyandotte, Mich., US;
Southern, Robert James, Madison Heights,
Mich., US; van Wiemeersch, John Robert, Novi,
Mich., US; Erkkila, David Ray, Brighton, Mich.,
US; Westra, Mike Raymond, Plymouth, Mich.,
US; Caushi, Aldi, Northville, Mich., US; Turner,
John William, Gregory, Mich., US; Shahidehpour,
Bobak, Ann Arbor, Mich., US; Elangovan,
Vivekanandh, Canton, Mich., US**

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **SICHERE SITZUNGSKOMMUNIKATION ZWISCHEN EINEM MOBILGERÄT UND EINER
BASISSTATION**

(57) Zusammenfassung: Ein Fahrzeug schließt Folgendes ein: (i) ein Haupttelematikmodul, (ii) ein Konnektivitätsmodul einschließlich Antenne(n) und Prozessor(en). Das Konnektivitätsmodul ist zu Folgendem konfiguriert: (a) Authentifizieren eines Mobilgeräts über einen Fahrzeugzugangsschlüssel (VAK); (b), falls (a), Ausgeben eines kurzlebigen Sitzungsschlüssels (DSK) an das Mobilgerät; (c), falls (b), Herstellen einer aktiven Sitzung mit dem Mobilgerät; (d) Verschlüsseln aller Nachrichten an das Mobilgerät mit dem VAK während (a) und mit dem DSK während (c). Das Konnektivitätsmodul ist zum automatischen Aufheben des DSK bei Ablauf eines vorgegebenen Zeitintervalls konfiguriert.



Beschreibung

TECHNISCHES GEBIET

[0001] Diese Anmeldung betrifft sichere Kommunikation zwischen einem Mobilgerät, wie etwa einem Smartphone, und einer Basisstation, wie etwa einem Fahrzeug, einem Server oder einem zweiten Mobilgerät.

ALLGEMEINER STAND DER TECHNIK

[0002] Mobilgeräte (z. B. Smartphones) sind mittlerweile allgegenwärtig und werden für mehr als mündliche Gespräche und Textnachrichten genutzt. Die zunehmende Verfügbarkeit von Hochgeschwindigkeitsinternet in Verbindung mit neuen Techniken, wie etwa Bluetooth und Nahfeldkommunikation (near-field communication - NFC), haben neue Verwendungen, wie etwa mobiles Bezahlen, Gesundheitsüberwachung und mehr, ermöglicht. Diese Techniken sind jedoch nicht absolut sicher und sind allein nicht ausreichend vertrauenswürdig, um sensible oder potentiell sicherheitskritische Informationen zwischen zwei Geräten zu übermitteln.

[0003] Zusätzliche Verwendungsfälle für ein Mobilgerät schließen das Interagieren mit einem Fahrzeug (oder einer anderen Basisstation, wie etwa einem Haus, einem Server, einem zweiten Mobilgerät usw.) ein, um das Fahrzeug (oder die andere Basisstation) dazu zu veranlassen, Eingabe, Start, Verriegeln/Entriegeln und andere Funktionen auszuführen. Einige Bezugnahmen auf den Stand der Technik offenbaren diese Verwendungsfälle. Diese Bezugnahmen stellen jedoch keine effiziente und wirksame Sicherheit für die Kommunikation zwischen dem Mobilgerät und dem Fahrzeug bereit. Standardisierte Kommunikationstechniken wie etwa Bluetooth und W-LAN sichern die Kommunikation nicht in ausreichendem Maße ab.

[0004] Neue und verbesserte Techniken für die sichere Kommunikation zwischen einem Mobilgerät und einem Fahrzeug (oder einer anderen Basisstation) werden daher benötigt.

KURZDARSTELLUNG

[0005] Es wird ein effizientes Verfahren zum Sichern von Befehls- und Steuerkommunikation zwischen dem Mobilgerät und dem Fahrzeug ohne Angewiesenheit auf eine vom drahtlosen Zugangsmechanismus (z. B. Bluetooth oder W-LAN) bereitgestellte Sicherheit offenbart.

[0006] Das Verfahren kann auf der Kenntnis eines vorab freigegebenen kryptografischen Schlüssels beruhen, der als der VAK bezeichnet wird. Dieser Schlüssel wird dem Mobilgerät und dem Fahrzeug auf eine bandexterne, sichere Weise von einem Backend-System mitgeteilt. Der Schlüssel ist eindeutig für das Mobilgerät und/oder den Benutzer des Mobilgeräts (z. B. Benutzer A des Mobilgeräts wird ein erster VAK zugeordnet und Benutzer B des Mobilgeräts wird ein zweiter VAK zugeordnet). Ferner kann jedem Benutzer des Mobilgeräts ein anderer VAK für jedes aus einer Mehrzahl von Fahrzeugen zugeordnet werden. Die Benutzer können sich in das Mobilgerät einloggen (z. B. eine App auf dem Mobilgerät). Das Mobilgerät kann erkennen, welche VAK einem Benutzer auf Grundlage der Login-Informationen zugeordnet sind. Das Mobilgerät den Benutzer davon abhalten, VAK zu verwenden, die anderen Benutzern zugeordnet sind. Somit kann der VAK zum Bestätigen der Identität eines Geräts verwendet werden. Das Fahrzeug kann mehrere Schlüssel speichern, die für mehrere unterschiedliche Mobilgeräte und/oder Benutzer stehen.

[0007] Die Lösung setzt außerdem einen kurzlebigen, als DSK bezeichneten Sitzungsschlüssel um, der zum Schützen von Nachrichten nach der Authentifizierung des Mobilgeräts verwendet wird. Ein temporärer und kurzlebiger Schlüssel beugt der Wiedereinspielung ganzer Sitzungen vor und gewährleistet die Geheimhaltung von Nachrichten zwischen den Sitzungen - die Kenntnis eines Sitzungsschlüssels erlaubt einem nicht, die Nachrichten aus einer beliebigen anderen Sitzung zu entschlüsseln.

[0008] Es wird außerdem ein optionaler Zähler bereitgestellt. Der Zähler nutzt dem Vorbeugen von Replay-Angriffen auf Nachrichten. Der Zähler kann optional als eine Nonce während der Authentifizierung verwendet werden.

[0009] Ein Fahrzeug gemäß der vorliegenden Offenbarung schließt daher Folgendes ein: (i) ein Haupttelematikmodul, (ii) ein Konnektivitätsmodul einschließlich Antenne(n) und Prozessor(en). Das Konnektivitätsmodul ist zu Folgendem konfiguriert: (a) Authentifizieren eines Mobilgeräts über einen Fahrzeugzugangsschlüssel (VAK); (b), falls (a), Ausgeben eines kurzlebigen Sitzungsschlüssels (DSK) an das Mobilgerät; (c), falls (b), Herstellen einer aktiven Sitzung mit dem Mobilgerät; (d) Verschlüsseln einiger oder aller Nachrichten an das

Mobilgerät mit dem VAK während (a) und mit dem DSK während (c). Das Konnektivitätsmodul ist zum automatischen Aufheben des DSK bei Ablauf eines vorgegebenen Zeitintervalls konfiguriert.

Figurenliste

[0010] Zum besseren Verständnis der Erfindung kann auf Ausführungsformen Bezug genommen werden, die in den folgenden Zeichnungen gezeigt sind. Die Komponenten in den Zeichnungen sind nicht zwingend maßstabsgetreu und zugehörige Elemente können weggelassen sein oder in einigen Fällen können Proportionen vergrößert dargestellt sein, um die hierin beschriebenen neuartigen Merkmale hervorzuheben und eindeutig zu veranschaulichen. Außerdem können Systemkomponenten, wie auf dem Fachgebiet bekannt, verschiedenartig angeordnet sein. Ferner sind in den Zeichnungen sich entsprechende Teile in den verschiedenen Ansichten durch gleiche Bezugszeichen gekennzeichnet.

Fig. 1 ist ein Blockdiagramm eines Fahrzeugrechensystems.

Fig. 2 ist eine Draufsicht eines Fahrzeugs, in dem das Fahrzeugrechensystem inbegriffen ist.

Fig. 3 ist ein Blockdiagramm des Fahrzeugrechensystems.

Fig. 4 ist ein Flussdiagramm der Herstellung einer aktiven Sitzung zwischen dem Host-Fahrzeug und einem Mobilgerät. Die Zeit verläuft abwärts.

Fig. 5 ist ein Flussdiagramm der Herstellung einer aktiven Sitzung zwischen dem Host-Fahrzeug und einem Mobilgerät. Die Zeit verläuft abwärts.

Fig. 6 ist ein Flussdiagramm, das die Vorgänge aus **Fig. 4** einschließt.

Fig. 7 ist ein Flussdiagramm des Bereitstellens und Aufhebens von Fahrzeugzugangsschlüsseln.

DETAILLIERTE BESCHREIBUNG VON AUSFÜHRUNGSBEISPIELEN

[0011] Obwohl die Erfindung in verschiedenen Formen ausgeführt sein kann, werden in den Zeichnungen einige beispielhafte und nicht einschränkende Ausführungsformen gezeigt und nachfolgend beschrieben, wobei es sich versteht, dass die vorliegende Offenbarung als eine Erläuterung der Erfindung anhand von Beispielen anzusehen ist und damit nicht beabsichtigt wird, die Erfindung auf die konkreten veranschaulichten Ausführungsformen zu beschränken. In dieser Anmeldung soll die Verwendung der Disjunktion die Konjunktion beinhalten. Die Verwendung von bestimmten oder unbestimmten Artikeln soll keine Kardinalität anzeigen. Insbesondere soll ein Verweis auf „das“ Objekt oder „ein“ Objekt auch eines aus einer möglichen Mehrzahl derartiger Objekte bezeichnen. Ferner kann die Konjunktion „oder“ dazu verwendet werden, Merkmale wiederzugeben, die - als eine Option - gleichzeitig vorhanden sind und - als eine andere Option - sich gegenseitig ausschließende Alternativen darstellen. Anders formuliert ist die Konjunktion „oder“ so aufzufassen, dass sie „und/oder“ als eine Option und „entweder/oder“ als eine weitere Option einschließt.

[0012] **Fig. 1** zeigt ein Rechensystem **100** einer Basisstation, wie etwa eines Host-Fahrzeugs **200**. Obwohl erläutert wird, dass die Basisstation das Host-Fahrzeug **200** ist, kann die Basisstation jede beliebige geeignete ausgerüstete Vorrichtung, wie etwa ein Mobiltelefon, ein Tablet, ein Server usw., sein. Das Host-Fahrzeug **200** ist vernetzt, was bedeutet, dass das Host-Fahrzeug **200** dazu konfiguriert ist, (a) drahtlose Daten von externen Instanzen (z. B. Infrastruktur, Server, andere vernetzte Fahrzeuge) zu empfangen und (b) drahtlose Daten an externe Instanzen zu übermitteln. Das Host-Fahrzeug **200** kann autonom, halbautonom oder manuell sein. Das Host-Fahrzeug **200** schließt einen Motor, eine Batterie, mindestens ein Rad, das vom Motor angetrieben wird, und ein Lenksystem, das dazu ausgelegt ist, das mindestens eine Rad um eine Achse zu drehen. Das Host-Fahrzeug **200** kann mit fossilen Brennstoffen (z. B. Diesel, Benzin, Erdgas) betrieben werden, hybridelektrisch oder vollelektrisch sein, mittels Brennstoffzellen betrieben werden usw.

[0013] Fahrzeuge sind z. B. in der US-Patentanm. Nr. 15/076,210 an Miller, im US-Patent Nr. 8,180,547 an Prasad, in der US-Patentanm. Nr. 15/186,850 an Lavoie, in der US-Patentveröffentlichung Nr. 2016/0117921 an D'Amato, und in der US-Patentanm. Nr. 14/972,761 an Hu beschrieben, die hiermit alle durch Bezugnahme vollumfänglich aufgenommen sind. Das Host-Fahrzeug **200** kann jedes der bei Miller, Prasad, Lavoie, D'Amato und Hu beschriebenen Merkmale einschließen.

[0014] Das Rechensystem **100** befindet sich im Host-Fahrzeug **200**. Das Rechensystem **100** ermöglicht unter anderem das automatische Steuern mechanischer Systeme innerhalb des Host-Fahrzeugs **200** und erleichtert die Kommunikation zwischen dem Host-Fahrzeug **200** und externen Instanzen (z. B. vernetzter Infrastruktur, dem Internet, anderen vernetzten Fahrzeugen). Das Rechensystem **100** beinhaltet einen Datenbus **101**, ein

oder mehrere Prozessoren **108**, einen flüchtigen Speicher **107**, einen nichtflüchtigen Speicher **106**, Benutzerschnittstellen **105**, eine Telematikeinheit **104**, Aktoren und Motoren **103** und lokale Sensoren **102**.

[0015] Der Datenbus **101** überträgt elektronische Signale oder Daten zwischen den elektronischen Komponenten. Der Prozessor **108** führt an elektronischen Signalen oder Daten Operationen aus, um modifizierte elektronische Signale oder Daten zu erzeugen. Der flüchtige Speicher **107** speichert Daten für einen nahezu sofortigen Abruf durch den Prozessor **108**. Der nichtflüchtige Speicher **106** speichert Daten für einen Abruf in dem flüchtigen Speicher **107** und/oder dem Prozessor **108**. Der nichtflüchtige Speicher **106** schließt eine Reihe nichtflüchtiger Speicher ein, darunter Festplatten, SSDs, DVDs, Blu-Rays usw. Die Benutzerschnittstelle **105** schließt Anzeigen, Touchscreen-Anzeigen, Tastaturen, Tasten und andere Vorrichtungen ein, die eine Benutzerinteraktion mit dem Rechensystem ermöglichen. Die Telematikeinheit **104** ermöglicht sowohl eine drahtgebundene als auch eine drahtlose Kommunikation mit externen Instanzen über Bluetooth, Mobilfunkdaten (z. B. 3G, LTE), USB usw.

[0016] Aktoren/Motoren **103** erzeugen greifbare Ergebnisse. Zu Beispielen für Aktoren/Motoren **103** gehören Kraftstoffeinspritzungen, Scheibenwischer, Bremslichtschaltungen, Getriebe, Airbags, an Sensoren montierte Motoren (z. B. ein zum Schwenken eines lokalen Sensors **102** ausgelegter Motor), Verbrennungsmotoren, Antriebsstrangmotoren, eine Lenkanlage, Toter-Winkel-Warnleuchten usw.

[0017] Die lokalen Sensoren **102** übertragen digitale Ablesungen oder Messungen an die Prozessoren **108**. Zu Beispielen für lokale Sensoren **102** gehören Temperatursensoren, Rotationssensoren, Sicherheitsgurtsensoren, Geschwindigkeitssensoren, Kameras, Lidarsensoren, Radarsensoren, Infrarotsensoren, Ultraschallsensoren, Zeitmesser, Feuchtigkeitssensoren, Regensensoren, Lichtsensoren usw. Es versteht sich, dass jede der unterschiedlichen elektronischen Komponenten aus **Fig. 1** separate oder dedizierte Prozessoren und Speicher einschließen kann. Weitere Details hinsichtlich Struktur und Operationen des Rechensystems **100** werden beispielsweise bei Miller, Prasad, Lavoie und Hu beschrieben.

[0018] **Fig. 2** zeigt und veranschaulicht allgemein das Host-Fahrzeug **200**, das das Rechensystem **100** einschließt. Manche der lokalen Sensoren **102** sind außen an einem Host-Fahrzeug **200** angebracht (andere befinden sich im Inneren des Fahrzeugs **200**). Der lokale Sensor **102a** ist dazu ausgelegt, Objekte vor dem Fahrzeug **200** zu erkennen. Der lokale Sensor **102b** ist dazu ausgelegt, Objekte hinter dem Fahrzeug **200**, welche durch den hinteren Erfassungsbereich **109b** angegeben werden, zu erkennen. Der linke Sensor **102c** und der rechte Sensor **102d** sind dazu ausgelegt, ähnliche Funktionen für die linke und die rechte Seite des Fahrzeugs **200** durchzuführen.

[0019] Wie oben erläutert, können die lokalen Sensoren **102a** bis **102d** Ultraschallsensoren, Lidarsensoren, Radarsensoren, Infrarotsensoren, Kameras, Mikrophone und jedwede Kombination davon usw. sein. Das Host-Fahrzeug **200** schließt eine Mehrzahl anderer lokaler Sensoren **102** ein, die sich im Fahrzeuginneren oder am Fahrzeugäußeren befinden. Die lokalen Sensoren **102** können einen oder alle der bei Miller, Prasad, Lavoie, D'Amato und Hu offenbarten Sensoren einschließen. Die allgemeine Anordnung von in den **Fig. 1** und **Fig. 2** gezeigten Komponenten stellt den Stand der Technik dar.

[0020] Es versteht sich, dass das Host-Fahrzeug **200** und insbesondere die Prozessoren **108** des Host-Fahrzeugs **200** dazu konfiguriert ist/sind, die hier beschriebenen Verfahren und Operationen durchzuführen. In manchen Fällen ist das Host-Fahrzeug **200** dazu ausgelegt, diese Funktionen über Computerprogramme durchzuführen, die in dem flüchtigen **107** und/oder nichtflüchtigen **106** Speicher des Rechensystems **100** gespeichert sind.

[0021] Ein oder mehrere Prozessoren sind „dazu ausgelegt“, einen offenbarten Verfahrensschritt, -block oder eine solche Operation durchzuführen, wenn wenigstens einer von dem einen oder den mehreren Prozessoren in Wirkverbindung mit einem Speicher steht, in dem ein Softwareprogramm mit Code oder Anweisungen gespeichert ist, der oder die den offenbarten Verfahrensschritt oder -block verkörpern. Eine weitere Beschreibung dessen, wie die Prozessoren, der Speicher und die Software zusammenwirken, findet sich bei Prasad. Gemäß einigen Ausführungsformen führt (führen) ein Mobiltelefon oder ein externe(r) Server, das oder der (die) in Wirkverbindung mit dem Host-Fahrzeug **200** steht (stehen), einige oder alle der nachfolgend erläuterten Verfahren und Operationen durch.

[0022] Das Host-Fahrzeug **200** kann einige oder alle der Merkmale des Fahrzeugs nach Prasad einschließen. Das Rechensystem **100** kann einige oder alle der Merkmale des VCCS nach Prasad einschließen. Das Host-Fahrzeug **200** kann mit einigen oder allen der in **Fig. 1** bei Prasad gezeigten Vorrichtungen, einschließlich der

nomadischen oder mobilen Vorrichtung, des Sendemasts, des Telekommunikationsnetzwerks, des Internets und des Datenverarbeitungszentrums (d. h. eines oder mehrerer Server), in Verbindung stehen. Jede der in dieser Anmeldung beschriebenen Instanzen (z. B. die vernetzte Infrastruktur, die anderen Fahrzeuge, Mobiltelefone, Server) kann eines oder alle der unter Bezugnahme auf **Fig. 1** und **Fig. 3** beschriebenen Merkmale gemein haben.

[0023] Im in den Ansprüchen verwendeten Sinne wird der Ausdruck „beladenes Fahrzeug“ hiermit mit folgender Bedeutung definiert: „ein Fahrzeug, beinhaltend einen Motor, eine Vielzahl von Rädern, eine Leistungsquelle und eine Lenkanlage; wobei der Motor Drehmoment auf wenigstens eines aus der Vielzahl von Rädern überträgt, wodurch das wenigstens eine aus der Vielzahl von Rädern angetrieben wird; wobei die Leistungsquelle den Motor mit Energie versorgt; und wobei das Lenksystem dazu ausgelegt ist, mindestens eines aus der Vielzahl von Rädern zu lenken“. Bei dem Host-Fahrzeug **200** kann es sich um ein beladenes Fahrzeug handeln.

[0024] Im in den Ansprüchen verwendeten Sinne wird der Ausdruck „ausgerüstetes Elektrofahrzeug“ hiermit mit folgender Bedeutung definiert: „ein Fahrzeug, beinhaltend: eine Batterie, eine Vielzahl von Rädern, einen Motor, ein Lenksystem; wobei der Motor Drehmoment auf wenigstens eines aus der Vielzahl von Rädern überträgt, wodurch das wenigstens eine aus der Vielzahl von Rädern angetrieben wird; wobei die Batterie wiederaufladbar und dazu ausgelegt ist, den Motor mit elektrischer Energie zu versorgen, wodurch der Motor angetrieben wird; und wobei das Lenksystem dazu ausgelegt ist, mindestens eines aus der Vielzahl von Rädern zu lenken“. Bei dem Host-Fahrzeug **200** kann es sich um ein ausgerüstetes Elektrofahrzeug handeln.

[0025] **Fig. 3** zeigt eine spezifischere Umsetzung des Rechensystems **100**. Wie veranschaulicht schließt das Rechensystem **100** ein Konnektivitätsmodul **300**, ein Haupttelematikmodul **320** und eine Mehrzahl von anderen Modulen **340** ein.

[0026] Das Konnektivitätsmodul **300** schließt einen oder mehrere Prozessoren **301**, einen flüchtigen Speicher **302**, einen nichtflüchtigen Speicher **303**, eine oder mehrere Antennen **304** und einen Datenbus **305** ein. Das Haupttelematikmodul **320** schließt einen oder mehrere Prozessoren **322**, einen flüchtigen Speicher **323**, einen nichtflüchtigen Speicher **324**, eine oder mehrere Antennen **321** und einen Datenbus **325** ein.

[0027] Die anderen Module **340** schließen eine Mehrzahl von Modulen, wie etwa Aktoren-/Elektromotorenmodule **341**, Benutzerschnittstellenmodule **342** und lokale Sensormodule **343**, ein. Jedes der anderen Module **340** schließt einen oder mehrere Prozessoren, einen flüchtigen Speicher und einen nichtflüchtigen Speicher ein. Mindestens einige der Aktoren-/Elektromotorenmodule sind mit Elektromotoren/Aktoren **103**, wie etwa Elektromotoren, Verbrennungsmotoren usw., verbunden.

[0028] Die anderen Module **340** steuern das grundlegende Fahren und die Sicherheitsfunktionen des Host-Fahrzeugs **200**, wie etwa das Versorgen der Räder mit Leistung, Ausführen von Sicherheitsfunktionen (z. B. Auslösen von Airbags), Bedienen des Radios, Abbilden der Route des Fahrzeugs usw.

[0029] Das Haupttelematikmodul **320** ist die primäre Kommunikationsbrücke zwischen dem Host-Fahrzeug **200** und den externen Instanzen (z. B. Servern, anderen Fahrzeugen, dem Internet, Mobilgeräten usw.). Das Konnektivitätsmodul **300** ist (a) die primäre Kommunikationsbrücke zwischen dem Host-Fahrzeug **200** und spezifischen Mobilgeräten und (b) einer Authentifizierungsvorrichtung mindestens einiger externer Instanzen in Verbindung mit dem Host-Fahrzeug **200**. Wie unten beschrieben kommuniziert das Konnektivitätsmodul **300** über Antennen **304** direkt mit spezifischen Mobilgeräten und erlaubt den spezifischen Mobilgeräten, das Haupttelematikmodul **320** und/oder einige oder alle der anderen Module **340** zu steuern. Daher können Antennen **321** des Haupttelematikmoduls **320** für Fernbereichskommunikation über das Internet (z. B. Mobilfunkkommunikation) ausgerüstet sein, während Antennen **304** des Konnektivitätsmoduls **300** nur für Nahbereichskommunikation (z. B. Bluetooth-Low-Energy-Kommunikation) ausgerüstet sein können. Das Konnektivitätsmodul **300** kann dazu konfiguriert, nur Nachrichten anzunehmen und auszustrahlen, die von den Prozessoren **301** des Konnektivitätsmoduls erstellt wurden, während das Haupttelematikmodul **320** dazu konfiguriert sein kann, Nachrichten anzunehmen und auszustrahlen, die von einem beliebigen Modul erstellt wurden.

[0030] **Fig. 4** zeigt Operationen, die mit dem Vermitteln einer Sitzung zwischen dem Mobilgerät **380** und dem Host-Fahrzeug **200** einhergehen. Beim Vermitteln der Sitzung kommt es zu einer aktiven Sitzung sowohl auf dem Mobilgerät **380** und als auch dem Host-Fahrzeug **200**. Während der aktiven Sitzung leitet das Konnektivitätsmodul **300** Befehle, die vom Mobilgerät **380** abgegeben wurden, an die anderen Module **340** weiter. Beispielsweise kann das Host-Fahrzeug **200** beim Pairing dem Mobilgerät **380** ermöglichen, folgende Befehle

auszugeben: einen Entriegelungsbefehl, der das Host-Fahrzeug **200** dazu veranlasst, seine Türen zu entriegeln, einen Verriegelungsbefehl, der das Host-Fahrzeug **200** dazu veranlasst, seine Türen zu verriegeln, einen Befehl zum Starten des Elektromotors, einen Befehl zum Starten des Verbrennungsmotors, einen Befehl zum Einstellen eines Fensters, einen Panikbefehl usw. Bevor das Konnektivitätsmodul **300** die aktive Sitzung beginnt, kann das Konnektivitätsmodul **300** Nachrichten, einschließlich Befehle für die anderen Module **340**, abweisen.

[0031] Die Verbindungen in Figur 4 können ausschließlich zwischen dem Mobilgerät **380** und dem Konnektivitätsmodul **300** erfolgen, bis auf die Authentifizierungsanforderung **402**, die vom Mobilgerät **380** an das Haupttelematikmodul **320** gesendet und dann vom Haupttelematikmodul **320** an das Konnektivitätsmodul **300** weitergeleitet werden kann. Alternativ können alle Verbindungen durch das Haupttelematikmodul **320** geleitet werden. Die Authentifizierungsanforderung **402** ist eine Anforderung an das Konnektivitätsmodul **300**, das Mobilgerät **380** zu authentifizieren. Die Authentifizierungsanforderung **402** schließt (a) eine (VAK)-ID des Fahrzeugzugangsschlüssels („VAK_id“) und (b) einen Tag der VAK-ID („tag_VAK“) ein.

[0032] Wenngleich nicht gezeigt, können eine, mehrere oder alle der Nachrichten, die vom Mobilgerät **380** stammen, und eine, mehrere oder alle der Nachrichten, die vom Konnektivitätsmodul **300** des Host-Fahrzeugs **200** stammen, unverschlüsselte Routing-Metadaten einschließen. Die Routing-Metadaten können (i) die empfangende Instanz (Mobilgerät **380** oder Host-Fahrzeug **200**) anweisen, die Nachricht an eine bestimmte Stelle in der empfangenden Instanz zu leiten (z. B. ein bestimmtes Programm oder eine bestimmte Hardware). Die Routing-Metadaten können (ii) die übermittelnde Instanz anweisen, die Nachricht an eine bestimmte empfangende Instanz zu leiten.

[0033] Beispielsweise und unter Bezugnahme auf Figur 3 können dem Konnektivitätsmodul **300** Antennen fehlen. Daher kann das Konnektivitätsmodul, wenn es Nachrichten übermittelt, erste Routing-Metadaten in den Nachrichten einschließen, die die Haupttelematik **320** anweisen, die Nachricht zu einem bestimmten Mobilgerät zu leiten. Das Konnektivitätsmodul kann zweite Routing-Metadaten in den Nachrichten einschließen, die die Telematik des Mobilgeräts anweisen, die Nachricht zu einer bestimmten Hardware oder Software im Mobilgerät **380** zu leiten. Daher können dem Konnektivitätsmodul **300** Antennen **304** fehlen und kann es mit dem Mobilgerät **380** über die Haupttelematik **320** kommunizieren.

[0034] Der Fahrzeugzugangsschlüssel ist ein kryptografischer Schlüssel, der dazu verwendet wird, die Vermittlungssitzung aus Fig. 4 zu ermöglichen. Im Sinne von Fig. 4 speichern sowohl das Mobilgerät **380** als auch das Konnektivitätsmodul **300** (d. h., kennen) bereits den VAK. Die VAK-ID ist eine eindeutige Kennung (d. h., Name) des bestimmten VAK, der im Mobilgerät **380** und Konnektivitätsmodul **300** gespeichert ist. Das Generieren und Austeilen des VAK und der VAK-ID an das Mobilgerät **380** und das Host-Fahrzeug **200** wird nachstehend unter Bezugnahme auf Fig. 7 erläutert.

[0035] Der Tag der VAK-ID ist ein Hashwert der VAK-ID, der mit einer Hashfunktion ausgeführt wird, die vorab auf dem Mobilgerät **380** gespeichert ist. Wenn die vorliegende Patentschrift angibt, dass ein Hashwert auf etwas ausgeführt wurde (z. B. dass der Hashwert auf der VAK-ID ausgeführt wurde), bestehen mindestens zwei Möglichkeiten: erstens, die aufgelisteten Eingaben sind die einzigen Eingaben in die Hashfunktion; zweitens, die Hashfunktion verwendet die aufgelisteten Eingaben und möglicherweise andere Eingaben, wenn sie den Hashwert generiert.

[0036] Es versteht sich, dass, damit das Hashing funktioniert, die Hashfunktion und die Eingaben am Mobiltelefon darein mit der Hashfunktion und den Eingaben am Host-Fahrzeug darein identisch sein müssen. Daher muss, soweit das Mobilgerät andere Eingaben in den Hashwert (z. B. das Datum) einschließt, das Host-Fahrzeug dieselben Eingaben einschließen, wenn es den reziproken Hashwert berechnet (untenstehend erläutert).

[0037] Allgemein wenden Hashfunktionen beliebige mathematische Operationen auf Eingaben an. Beispielsweise kann eine Hashfunktion eine Ausgabe durch Multiplizieren aller Eingaben und dann Subtrahieren von sieben vom Multiplikationsergebnis generieren. Somit wäre, wenn die Eingaben in die Hashfunktion **127**, **434** und **22** sind, die Ausgabe der Hashfunktion $(127 \cdot 434 \cdot 22 - 7) = 1212589$. Als ein weiteres Beispiel kann eine Hashfunktion den ersten Wert jeder Eingabe addieren. Somit wäre, wenn die Eingaben der Hashfunktion **127**, **434** und **22** sind, die Ausgabe der Hashfunktion $(1 + 4 + 2) = 7$. Es bestehen zahlreiche andere Möglichkeiten.

[0038] Bei Hashfunktionen geht es darum, zu bestätigen, dass Eingaben in eine Operation (z. B. eine auf dem Mobilgerät **380** durchgeführte Operation) gleich den Eingaben in eine andere Operation sind (z. B. eine auf dem Host-Fahrzeug **200** durchgeführte Operation), ohne jemals die genauen Werte der Eingaben zu offenbaren.

Wenn das Host-Fahrzeug **200** einen Hashwert von 1212589 vom Mobilgerät **380** empfängt, einen reziproken Hashwert auf Werte ausführt, die auf dem Host-Fahrzeug **200** gespeichert sind, und einen reziproken Hashwert von 1212589 ausgibt, weiß das Host-Fahrzeug **200** somit, dass die Eingaben am Mobilgerät **380** (hier 127, 434 und 22) die gleichen wie die Eingaben am Host-Fahrzeug **200** sind (wieder 127, 434 und 22). Jemand, der den Hashwert von 1212589 abfängt (z. B. ein Hacker), wäre nicht in der Lage, die Eingaben von 127, 434 und 22 zu rekonstruieren, da der Hashwert von 1212589 das Ergebnis aus einer Reihe von Eingaben sein könnte (z. B. 4, 7, 43307; oder 2, 14, 44307; usw.) oder das Ergebnis einer beliebigen Hashfunktion sein könnte.

[0039] Bei Block **404** führt das Host-Fahrzeug **200** den reziproken Hashwert aus (d. h., wendet die gleiche Hashfunktion an) auf die VAK-ID und vergleicht den bei 402 empfangenen Hashwert mit dem reziproken Hashwert, der bei 404 generiert wurde. Passen die Hashwerte zusammen, dann antwortet das Host-Fahrzeug **200** mit einer Challenge **406**. Die Challenge **406** schließt (a) einen Zähler (der einem Wechselcode ähnelt) („ctr“) und eine zufällig generierte Nonce („N“), die gemäß dem VAK („enc_VAK“) individuell verschlüsselt sind, und (b) einen Hashwert des VAK („tag_VAK“) ein. Der Zähler kann als die Nonce verwendet werden. Bei Block **404** kann der Zähler zufällig generiert werden.

[0040] Bei Block **408** entschlüsselt das Mobilgerät **380** den Zähler und die Nonce, führt einen reziproken Hashwert auf den verschlüsselten Zähler und die verschlüsselte Nonce aus und vergleicht den reziproken Hashwert mit dem in der Challenge **406** eingeschlossenen Hashwert. Passen die Hashwerte zusammen, dann berechnet das Mobilgerät **380** eine mobile Antwort („r_ph“), die eine Funktion der Nonce und des VAK ist, und sendet eine Antwort 410 auf die Challenge. Die Antwort **410** auf die Challenge schließt (a) den erhöhten Zähler („ctr + 1“) und die berechnete mobile Antwort („r_ph“), die gemäß dem VAK („enc_VAK“) individuell verschlüsselt sind, und (b) einen Hashwert des VAK („tag_VAK“) ein.

[0041] Gemäß bevorzugten Ausführungsformen kann der Hashwert (d. h. „tag_“ der Verschlüsselungsschlüssel) durch einen Nachrichtenauthentifizierungscode (message authentication code - MAC) ersetzt werden. Dies gilt optional für jede Verwendung des Ausdrucks „Hashwert“ oder „tag_“ in der Patentschrift.

[0042] Der MAC kann einige oder alle der folgenden einschließen: **(1)** Eine unverschlüsselte ID des Verschlüsselungsschlüssels. Wie an anderer Stelle erläutert, kann jeder Verschlüsselungsschlüssel (z. B. der VAK und der DSK) beim Generieren mit einer eindeutigen ID gekoppelt werden. **(2)** Einen unverschlüsselten ersten Hashwert aller Daten in der Nachricht, die gemäß dem Verschlüsselungsschlüssel verschlüsselt wurde. Der erste Hashwert kann ferner die unverschlüsselte ID einschließen. **(3)** Einen zweiten unverschlüsselten Hashwert des unverschlüsselten Verschlüsselungsschlüssels. **(4)** Einen dritten unverschlüsselten Hashwert mit **(2)** und **(3)** als Eingaben in die Hashfunktion. Gemäß einer besonders bevorzugten Ausführungsform schließt der MAC nur **(1)**, **(2)** und **(4)** aber nicht **(3)** ein. Wenn die vorliegende Patentschrift reziproke Hashwerte erläutert, gelten solche reziproken Hashwert für den MAC. Anders ausgedrückt, kann das Mobilgerät **300** oder das Host-Fahrzeug **200** nach dem Erhalt einer Nachricht mit einem MAC die folgenden reziproken Hashing-Schritte ausführen: (a) Sicherstellen, dass die unverschlüsselte ID korrekt ist, (b) auf Grundlage der ID Sicherstellen, dass **(3)** der zweite unverschlüsselte Hashwert des unverschlüsselten Verschlüsselungsschlüssel korrekt ist, (c) Entschlüsseln der Nachricht, falls (a) und (b) bestätigt werden, und (d) Bestätigen, dass **(4)** der dritte unverschlüsselte Hashwert nach (c) korrekt ist.

[0043] Bei Block **412** entschlüsselt das Host-Fahrzeug **200** den erhöhten Zähler und die berechnete Antwort, führt einen reziproken Hashwert des VAK aus oder verweist auf diesen und vergleicht den reziproken Hashwert des VAK mit dem Hashwert des VAK in der Antwort **410** auf die Challenge. Passen die Hashwerte zusammen und überschreitet der erhöhte Zähler den ursprünglichen Zähler, der über die Challenge **406** gesendet wurde, dann berechnet das Host-Fahrzeug **200** eine Fahrzeug-Antwort („r_veh“), die eine Funktion der Nonce und des VAK ist.

[0044] Die zum Berechnen der Fahrzeug-Antwort verwendete Funktion, r_veh, ist die gleiche wie die zum Berechnen der Mobilgerät-Antwort, r_ph, verwendete Funktion. Das Host-Fahrzeug **200** vergleicht die Fahrzeug-Antwort, r_veh, mit der Mobilgerät-Antwort, r_ph. Passen die Antworten zusammen, dann erzeugt das Host-Fahrzeug **200** einen zufälligen, kurzlebigen Sitzungsschlüssel („DSK“). Der Sitzungsschlüssel weist eine begrenzte Gültigkeitsdauer auf, um die Gefährdung für den Fall, dass ein Hacker den DSK berechnet, zu begrenzen. Anders ausgedrückt, erkennt das Host-Fahrzeug **200** den DSK nur und somit nur Nachrichten, die gemäß dem DSK verschlüsselt sind, für einen vorgegebenen Zeitraum (z. B. 6 Stunden).

[0045] Nach dem Generieren des DSK übermittelt das Host-Fahrzeug **200** eine Bestätigung **414**. Die Bestätigung **414** schließt den gemäß dem VAK verschlüsselten DSK („enc_VAK“) und einen Hashwert des VAK („tag_“

VAK“) ein. Bei Block **416** bestätigt das Mobilgerät **380**, dass der Hashwert des VAK gültig ist (wie oben beschrieben durch Vergleichen des Hashwerts des VAK in der Bestätigung **414** mit einem reziproken Hashwert, der vom Mobilgerät **380** ausgeführt wird). Ist der Hashwert gültig, entschlüsselt das Mobilgerät **380** den DSK mit dem VAK, speichert den DSK und übermittelt eine Sitzungsanforderung **418**.

[0046] Die Sitzungsanforderung **418** schließt den zweimal erhöhten Zähler („ctr + 2“) ein, der gemäß dem DSK und einem Hashwert des DSK verschlüsselt ist. Bei Block **420** bestätigt das Host-Fahrzeug **200**, dass der Hashwert des DSK gültig ist, indem es einen reziproken Hashwert mit dem DSK generiert, und bestätigt, dass der zweimal erhöhte Zähler den einmal erhöhten Zähler („ctr + 1“) übersteigt. Ist dies der Fall, erkennt das Host-Fahrzeug **200**, dass die Sitzung begonnen hat, und übermittelt das Host-Fahrzeug **200** eine Nachricht **422** über den Start der Sitzung.

[0047] Die Nachricht **422** über den Start der Sitzung schließt (a) einen dreimal erhöhten Zähler („ctr + 3“), einen Initialisierungsvektor („IV“), die gemäß dem DSK individuell verschlüsselt werden, und (b) einen Hashwert des DSK ein. Bei Block **424** entschlüsselt das Mobilgerät **380** den Initialisierungsvektor und den dreimal erhöhten Zähler. Das Mobilgerät **380** bestätigt, dass der Hashwert des DSK gültig ist und der dreimal erhöhte Zähler den zweimal erhöhten Zähler übersteigt. Ist dies der Fall, dann erkennt das Mobilgerät **380**, dass die Sitzung begonnen hat.

[0048] Es versteht sich, dass zusätzlich zu den obenstehenden Verschlüsselungsverfahren jede Nachricht verschlüsselte Grunddaten einschließen kann (unten erläutert), die den Zweck der Nachricht angeben. Alternativ kann jede Nachricht keine Grunddaten einschließen und kann jede empfangende Instanz den Zweck der Nachricht anhand deren Ordnung im Vermittlungsprozess erkennen. Um diesen Effekt zu verstärken, und wie in Figur den 4 und 5 dargestellt, sind keine zwei Nachrichten identisch. Somit kann der Zweck einer Nachricht an der Struktur der Nachricht ermittelt werden.

[0049] Es werden verschiedene signierte Nachrichten (wie etwa Heartbeat-Challenges, Heartbeat-Antworten, Fahrzeugbefehle und Empfangsbestätigungen) während der aktiven Sitzung übermittelt. Eine signierte Nachricht kann (a) Grunddaten, die gemäß dem DSK verschlüsselt sind, und (b) einen Hashwert des DSK (der durch den zuvor erläuterten Authentifizierungscode ersetzt werden kann) einschließen. Alternativ oder zusätzlich kann die signierte Nachricht Folgendes einschließen: (a) einen Hashwert des Initialisierungsvektors, (b) die Grunddaten, die zuerst mit einem vom DSK und Initialisierungsvektor verschlüsselt wurden und dann erneut mit dem anderen vom DSK und Initialisierungsvektor verschlüsselt wurden, und (c) den erneut erhöhten Zähler, der gemäß einem beliebigen der obenstehenden Verfahren verschlüsselt wurde (z. B. DSK allein, DSK dann IV, oder IV dann DSK).

[0050] Als Reaktion auf den Erhalt einer signierten Nachricht (a) verifiziert die empfangende Instanz (Mobilgerät **380** oder Host-Fahrzeug **200**) die signierte Nachricht (durch Validieren von Hashwerten mit reziproken Hashwerten und Bestätigen, dass der erneut erhöhte Zähler den letzten dem Mobilgerät **380** bekannten Zähler übersteigt) und (b) führt sie eine Grundfunktion (z. B. Steuern eines Motors, Entriegeln einer Tür, Starten eines Motors, Nachuntenfahren eines Fensters, Erstellen und Versenden einer Nachricht) gemäß den Grunddaten aus.

[0051] Wie in **Fig. 4** dargestellt, treten Heartbeat-Ereignisse **436** während der aktiven Sitzung auf. Heartbeat-Ereignisse **436** ermöglichen dem Host-Fahrzeug **200** und dem Mobilgerät **380** zu bestätigen, dass die drahtlose Verbindung zwischen den beiden noch gegeben ist. Bei Block **426** ermittelt das Host-Fahrzeug **200**, dass eine Heartbeat-Bedingung eingetreten ist. Eine Heartbeat-Bedingung kann derart eingestellt sein, dass sie zu einem vorgegebenen Zeitpunkt eintritt. Die Zählung der Zeit wird auf null zurückgesetzt, wenn eine signierte Nachricht vom Mobilgerät **380** empfangen wird (z. B. gemäß dem obenstehenden Beispiel von sechzig Sekunden, wenn eine neue Heartbeat-Bedingung so eingestellt wurde, in 30 Sekunden einzutreten, das Konnektivitätsmodul **300** aber eine signierte Heartbeat-Antwort oder einen signierten Fahrzeugbefehl empfing, dann kann der Zähler auf null zurückgesetzt werden, sodass die neue Heartbeat-Bedingung in 60 Sekunden eintritt).

[0052] Das Konnektivitätsmodul **300** zählt eine Heartbeat-Zeitüberschreitung, die die Zeit überschreitet, die der Heartbeat-Bedingung zugeordnet ist (z. B. kann die Heartbeat-Zeitüberschreitung nach drei Minuten auftreten, während die Heartbeat-Bedingung nach einer Minute eintreten kann). Die Heartbeat-Zeitüberschreitung wird jedes Mal auf null zurückgesetzt, wenn eine signierte Nachricht vom Mobilgerät **380** empfangen wird.

[0053] Das Konnektivitätsmodul **300** kann Heartbeat-Challenges **428** übermitteln, sobald eine Heartbeat-Bedingung eingetreten ist, jedoch bevor es zu einer sehr häufigen Heartbeat-Zeitüberschreitung kommt. Bei-

spielsweise wartet das Konnektivitätsmodul **300** gemäß dem obenstehenden Beispiel sechzig Sekunden nach der letzten signierten Nachricht, bevor es eine erste Heartbeat-Challenge **428** ausgibt. Nach sechzig Sekunden jedoch kann das Konnektivitätsmodul **300** wiederholt Heartbeat-Challenges **428** abgeben (z. B. einmal alle fünf Sekunden), bis es zur Heartbeat-Zeitüberschreitung kommt. Wie unten erläutert, kehrt das Konnektivitätsmodul **300** in den Standby **602** zurück und hebt den DSK aus, sobald es zu einem Heartbeat-Zeitpunkt kommt.

[0054] Das Host-Fahrzeug **200** übermittelt eine signierte Heartbeat-Challenge **428** als Reaktion auf Block **426**. Bei Block **430** validiert das Mobilgerät **380** die signierte Heartbeat-Challenge **428** und gibt eine signierte Heartbeat-Antwort **432** aus. Bei Block **434** validiert das Host-Fahrzeug **200** die signierte Heartbeat-Antwort **432**. Das Host-Fahrzeug **200** kann Mobilgerätbefehle (nicht dargestellt) gemäß dem Heartbeat-Befehlsprozess **436** durch Einschließen verschiedener Grunddaten generieren.

[0055] Zu Fahrzeugsteuerung **450** kommt es während der aktiven Sitzung. Das Host-Fahrzeug **200** verarbeitet Fahrzeugsteuerung **450** nur während einer aktiven Sitzung (d. h., nur nachdem Block **420** eingetreten ist). Bei Block **438** (a) generiert das Mobilgerät **380** Grunddaten (z. B. die Türen entriegeln, den Verbrennungsmotor starten, ein bestimmtes Licht anstellen, ein bestimmtes Fenster nach unten fahren) und (b) übermittelt es einen signierten Fahrzeugbefehl auf Grundlage der Grunddaten. Der Signiervorgang ist oben beschrieben. Das Mobilgerät **380** kann Block **438** als Reaktion auf eine Benutzereingabe (z. B. das Berühren eines virtuellen Buttons) ausführen.

[0056] Bei Block **442** validiert das Host-Fahrzeug **200** den Fahrzeugbefehl und führt eine Grundfunktion auf Grundlage der entschlüsselten Grunddaten aus. Das Host-Fahrzeug **200** kann eine signierte Empfangsbestätigung **444** übermitteln. Das Mobilgerät **380** kann die Empfangsbestätigung validieren und eine Grundfunktion ausführen (z. B. eine Nachricht anzeigen) als Reaktion auf die in der Empfangsbestätigung enthaltenen Grunddaten.

[0057] Gemäß einigen Ausführungsformen kann eine andere Hashfunktion für jede Kommunikation während der Vermittlungssitzung **402**, **406**, **410**, **414**, **418** und **422** verwendet werden. Da sowohl das Mobilgerät **380** als auch das Host-Fahrzeug **200** die Art der empfangenen Verbindung kennen (Authentifizierungsanforderung vs. Challenge vs. mobile Antwort vs. Bestätigung vs. Sitzungsanforderung vs. Befehl zum Start der Sitzung), wissen sowohl das Mobilgerät **380** als auch das Host-Fahrzeug **200**, welche Hashfunktion anzuwenden ist, um den reziproken Hashwert zu Validierungszwecken zu generieren.

[0058] Gemäß einigen Ausführungsformen wird nur eine einzelne Hashfunktion vom Host-Fahrzeug **200** und Mobilgerät **380** während der aktiven Sitzung verwendet. Alternativ wird eine erste Hashfunktion für alle Heartbeat-Challenges verwendet, wird eine zweite Hashfunktion für alle Heartbeat-Antworten verwendet, wird eine dritte Hashfunktion für alle Fahrzeugbefehle verwendet, wird eine vierte Hashfunktion für alle Empfangsbestätigungen an diese verwendet, wird eine fünfte Hashfunktion für alle mobilen Befehle verwendet und wird eine sechste Hashfunktion für alle Empfangsbestätigungen an diese verwendet. Alle während der aktiven Sitzung verwendeten Hashfunktionen können sich von allen Hashfunktionen unterscheiden, die während der Vermittlungssitzung verwendet wurden.

[0059] **Fig. 5** zeigt Operationen, die mit dem Pairing von Mobilgerät **380** und Host-Fahrzeug **200** zusammenhängen. **Fig. 5** schließt die gleichen Merkmale wie **Fig. 4** ein, falls nichts anderes in der Patentschrift oder den Figuren angegeben ist. Die Operationen aus **Fig. 5** beruhen darauf, dass der DSK zu groß ist, um in einer einzelnen Nachricht übermittelt zu werden, und trennen den DSK daher in zwei Blöcke: einen ersten Block („DSK1“) und einen zweiten Block („DSK2“).

[0060] Nachdem es den ersten und zweiten Block, DSK1 und DSK2, empfangen hat, setzt das Mobilgerät **380** den DSK zusammen. Als ein Beispiel kann das Mobilgerät DSK2 an DSK1 anfügen (z. B. wenn DSK1 45 wäre und DSK2 875 wäre, dann wäre DSK **45875**). Als andere Beispiele kann das Mobilgerät DSK1 mit DSK2 multiplizieren, DSK1 in die Potenz von DSK2 erheben usw.

[0061] Das Host-Fahrzeug **200** kann dazu konfiguriert sein, die beiden **Fig. 4** und **Fig. 5** umzusetzen und auf Grundlage einer Identität der drahtlosen Verbindung, die zwischen dem Konnektivitätsmodul **300** und dem Mobilgerät **380** hergestellt wurde, zwischen ihnen zu wählen (z. B. falls das Konnektivitätsmodul **300** ermittelt, dass die drahtlose Verbindung über NFC oder eine alte Bluetooth-Version läuft, dann setzt das Konnektivitätsmodul **300** **Fig. 4** um; ermittelt das Konnektivitätsmodul **300**, dass die drahtlose Verbindung über W-LAN oder eine spätere Bluetooth-Version läuft, dann setzt das Konnektivitätsmodul **300** **Fig. 5** um). Bei Block **404** berechnet das Host-Fahrzeug **200** den DSK und teilt dann den DSK in zwei Teile: DSK1 und DSK2 zeigt. Die

Challenge **406** schließt daher den gemäß dem VAK verschlüsselten DSK1 aber nicht DSK2 ein. Bei Block **408** entschlüsselt das Mobilgerät **380** den DSK1. Bei Block **412** schließt das Host-Fahrzeug **200** den gemäß dem VAK verschlüsselten DSK2 und den zweimal erhöhten Zähler in die Bestätigung **414** ein. Bei Block **416** entschlüsselt das Mobilgerät **380** den DSK2 und setzt den DSK auf Grundlage von DSK1 und DSK2 zusammen. Aufgrund des zweimal erhöhten Zählers in der Bestätigung **414** wird der Zähler in der Sitzungsanforderung **418** dreimal erhöht und wird der Zähler im Befehl **422** zum Starten der Sitzung viermal erhöht.

[0062] Wenngleich nicht gezeigt, kann die Bestätigung **414** zusätzlich zu DSK2 eine Zusammensetzungsanweisung einschließen, die gemäß dem VAK verschlüsselt ist. Die Zusammensetzungsanweisung weist, wenn sie bei Block **416** empfangen und geöffnet wurde, das Mobilgerät **380** an, wie DSK1 und DSK2 zu kombinieren sind. Die Prozessoren können dazu konfiguriert sein, zu ermitteln, ob DSK1 oder DSK2 kleiner ist, und die DSK-Zusammensetzungsanweisungen mit dem kleineren von DSK1 und DSK2 zu übermitteln. **Fig. 6** ist ein Flussdiagramm des Verfahrens aus **Fig. 4**. Bei Block **602** ist das Konnektivitätsmodul **300** im Standbymodus. Das Konnektivitätsmodul **300** antwortet nur auf eine Authentifizierungsanforderung **402**, während es sich im Standbymodus befindet (d. h., das Konnektivitätsmodul ignoriert alles, was keine Authentifizierungsanforderung **402** ist, während es sich im Standbymodus **602** befindet).

[0063] Der Standbymodus **602** ist für ein eindeutiges Mobilgerät spezifisch, sodass sich das Konnektivitätsmodul **300** im Standbymodus befinden kann in Bezug auf Mobilgerät A, sich aber nicht im Standbymodus in Bezug auf Mobilgerät B befinden kann. Wie später erläutert wird, kann jedem Mobilgerät ein eindeutiger VAK und daher eine eindeutige VAK-ID zugeordnet werden. Daher kann das Konnektivitätsmodul **300** ein spezifisches Mobilgerät anhand der VAK-ID identifizieren, die von dem spezifischen Mobilgerät bei der Authentifizierungsanforderung **402** ausgegeben wurde. Immer, wenn das Konnektivitätsmodul **300** in den Standbymodus **602** zurückkehrt, wird jeglicher aktiver DSK aufgehoben, was bedeutet, dass das Host-Fahrzeug **200** keine Nachrichten verifiziert, die gemäß dem zuvor aktiven DSK verschlüsselt und/oder ausgezeichnet wurden, und ein neuer DSK ausgegeben werden muss.

[0064] Nach dem Erhalt der Authentifizierungsanforderung **402** fährt das Konnektivitätsmodul **300** mit Block **604** fort, wo das Mobilgerät **380** authentifiziert wird. Ist eine vom Mobilgerät **380** empfangene Nachricht nicht verifiziert (falscher Hashwert oder falscher Zähler), dann kommt es zu einem Authentifizierungsfehler **609** und das Konnektivitätsmodul **300** kehrt in den Standby zurück. Kommt es zu einer Zeitüberschreitung (d. h., es wird keine Nachricht vom Mobilgerät **380** innerhalb einer vorgegebenen Zeit empfangen), dann kommt es zu einem Authentifizierungsfehler **609**. Andernfalls ist die Authentifizierung erfolgreich **610** und das Konnektivitätsmodul fährt mit Block **606** fort.

[0065] Ist eine vom Mobilgerät **380** empfangene Nachricht nicht verifiziert (falscher Hashwert oder falscher Zähler), dann kommt es zu einem Schlüsselfestlegungsfehler **611** und das Konnektivitätsmodul **300** kehrt in den Standby zurück. Kommt es zu einer Zeitüberschreitung (d. h. es wird keine Nachricht vom Mobilgerät **380** innerhalb einer vorgegebenen Zeit empfangen), dann kommt es zu einem Schlüsselfestlegungsfehler **611**. Andernfalls ist die Schlüsselfestlegung erfolgreich **612** und fährt das Konnektivitätsmodul mit Block **608** fort, wo eine aktive Sitzung hergestellt wird.

[0066] Falls während der aktiven Sitzung (a) eine Signatur nicht verifiziert ist oder (b) eine Heartbeat-Zeitüberschreitung eintritt (wie zuvor erläutert), dann kommt es zu einem Sitzungsfehler **613** und das Konnektivitätsmodul **300** kehrt in den Standbymodus **602** zurück. Wie oben erwähnt, ist der DSK kurzlebig und läuft nach einer vorgegebenen Zeit (z. B. einer Stunde) ab, nachdem er bei Block **412** ausgegeben wurde. Bei Ablauf kommt es zur Sitzungsbeendigung **614** und das Konnektivitätsmodul **300** weist Nachrichten mit einer Validierung auf Grundlage des DSK (z. B. mit dem DSK, einschließlich des Tags des DSK, verschlüsselt) ab. Bei Sitzungsbeendigung **614** kann das Host-Fahrzeug **200** eine Nachricht an das Mobilgerät **380** übermitteln, die das Mobilgerät **380** dazu anweist, automatisch eine Authentifizierungsanforderung **402** zum Generieren eines neuen DSK auszugeben. Die Nachricht kann gemäß dem VAK verschlüsselt sein oder kann gemäß dem alten DSK verschlüsselt sein.

[0067] **Fig. 7** ist ein Flussdiagramm des Vorladens des VAK auf das Mobilgerät **380** und das Host-Fahrzeug **200**. Das Backend **390** (eine oder mehrere Server) vermittelt zwischen dem Mobilgerät **380** und dem Host-Fahrzeug **200**. Vor Block **701** kennt das Mobilgerät **200**: (a) einen öffentlichen Schlüssel des Backend **390**, (b) Fahrzeug-Metadaten (eine Identität des Host-Fahrzeugs **200**), (c) Backend-Metadaten, (e) Mobilgerät-Metadaten, (h) einen privaten Schlüssel des Mobilgeräts und (i) ein Schlüsselpaar von Mobilgerät/Backend [das ein privates Passwort ist].

[0068] Vor Block **701** kennt das Backend **390** (b) die Fahrzeug-Metadaten, (c) die Backend-Metadaten, (d) einen symmetrischen Fahrzeugsicherheitsschlüssel, (e) die Metadaten des Mobilgeräts, (f) den privaten Schlüssel des Backend **390**, (g) eine Abbildung des Schlüsselpaars des Mobilgeräts (i) bis (b) und/oder (d) und (i) das private Schlüsselpaar des Mobilgeräts. Vor Block **701** kennt das Host-Fahrzeug **200** (c) die Backend-Metadaten und (d) den symmetrischen Fahrzeugsicherheitsschlüssel [bei der Herstellung eingestellt].

[0069] Die folgende Tabelle wird als Hilfestellung für den Leser bereitgestellt:

Tabelle 1

a	öffentlicher Schlüssel des Backend
b	Fahrzeug -Metadaten
c	Backend- Metadaten
d	symmetrischer Fahrzeugsicherheitsschlüssel
c	Mobilgerät-Metadaten
f	privater Schlüssel des Backend
g	Abbildung (z. B. Tabelle) mehrerer (i)s zu mehreren (b)s
h	privater Schlüssel des Mobilgeräts
i	Mobilgerät-/Backend-Schlüsselpaar

[0070] Es wird nun ein Prozess zum Generieren und Anwenden eines neuen VAK der Reihenfolge nach beschrieben. Das Mobilgerät **380** sendet eine neue Schlüsselanforderung **701** an das Backend **390**, die eine Anforderung an das Konnektivitätsmodul **300** des Host-Fahrzeugs **200** ist, um einen neuen VAK für das Mobilgerät **380** zu speichern. Die neue Schlüsselanforderung schließt (b) und (i) ein, die einzeln gemäß (a) verschlüsselt sind. Die neue Schlüsselanforderung schließt (e) ein, die unverschlüsselt sind und somit das Routing der neuen Schlüsselanforderung **701** an das Backend **390** ermöglichen. Die neue Schlüsselanforderung schließt einen unverschlüsselten öffentlichen Schlüssel des Mobilgeräts ein, der auf (h) basiert.

[0071] Bei Erhalt der neuen Schlüsselanforderung **701** entschlüsselt das Backend **390** die Nachricht und bestätigt, dass (i) und (b) zusammenpassen, über (g) die Abbildung (z. B. eine Tabelle oder Tabellenkalkulation). Liegt ein Match vor, dann generiert das Backend **390** einen VAK, die Funktion (die r_ph und r_veh entsprechen) und etwaige Hashfunktionen (zuvor erläutert). Das Backend **390** verschlüsselt individuell den VAK und die Funktionen gemäß (d) dem zu (b) gehörigen symmetrischen Fahrzeugsicherheitsschlüssel.

[0072] Die Bereitstellung **702** des Schlüssels schließt den verschlüsselten VAK, die verschlüsselten Funktionen und unverschlüsselte Metadaten ein. Die unverschlüsselten Metadaten ermöglichen dem Haupttelematikmodul **320**, die Schlüsselbereitstellung an das Konnektivitätsmodul **300** in der internen Nachricht **703** (die mindestens den VAK und die individuell gemäß (d) verschlüsselte Funktion einschließt) zu leiten. Das Konnektivitätsmodul **300** entschlüsselt die interne Nachricht **703** mit (d), speichert den VAK und speichert eine der Funktionen als r_veh, speichert die anderen Funktionen als die Hashfunktionen und sendet eine Antwort **704**. Die Antwort **704** schließt unverschlüsselte Metadaten, die die Nachricht gemäß (c) leiten, und gemäß dem VAK verschlüsselte Grunddaten ein.

[0073] Bei **705** leitet das Haupttelematikmodul **320** eine Antwort **704** an das Backend **390** weiter auf Grundlage (c) der unverschlüsselten Metadaten des Backend **390**. Bei Erhalt der Antwort **705** übermittelt das Backend **390** bei **706** den VAK und die Funktionen an das Mobilgerät **390**. Bei Erhalt der Antwort **705** kann das Backend **390** den VAK und die Funktionen speichern und dieselben den Fahrzeug-Metadaten zuordnen. Alternativ kann das Backend **390** den VAK und die Funktionen dauerhaft löschen.

[0074] In der Nachricht **706** zum Bereitstellen des Schlüssels sind der VAK und die Funktionen gemäß einem öffentlichen Schlüssel des Mobilgeräts verschlüsselt, der als unverschlüsselte Daten in der neuen Schlüsselanforderung **701** bereitgestellt wird. Die Nachricht **706** schließt unverschlüsselte Mobilgerät-Metadaten (e) ein. Das Mobilgerät **380** entschlüsselt die Nachricht **706** mit (h). Das Mobilgerät **380** speichert den VAK, speichert eine der Funktionen als r_ph und speichert die anderen Funktionen als die Hashfunktionen. Das Mobilgerät **380** und das Host-Fahrzeug **200** können nun die Schritte **402** bis **450** wie in den Fig. 5 und Fig. 6 erläutert ausführen.

[0075] Es wird nun ein Prozess zum Aufheben eines VAK der Reihe nach beschrieben. Das Mobilgerät **380** gibt eine Anforderung **721** zum Aufheben des Schlüssels aus, die der neuen Schlüsselanforderung **701** ähnlich ist (d. h., gemäß denselben Verfahren verschlüsselt und übermittelt ist), schließt aber einen Befehl zum Aufheben des Schlüssels anstelle eines neuen Schlüsselbefehls ein. Die Anforderung **721** zum Aufheben des Schlüssels kann die verschlüsselte VAK-ID oder den verschlüsselten VAK einschließen.

[0076] Das Backend **390** empfängt die Anforderung **721** zum Aufheben des Schlüssels, entschlüsselt die VAK-ID oder den VAK und gibt einen Befehl **722** zum Aufheben des Schlüssels ab (wie oben, falls (i) zu (b) führt, der der Nachricht **702** zum Bereitstellen des Schlüssels ähnelt (schließt aber einen Befehl zum Aufheben des Schlüssels und die verschlüsselte VAK-ID oder den verschlüsselten VAK ein). Die Haupttelematik **320** generiert eine interne Nachricht **723** zum Aufheben des Schlüssels auf Grundlage von **722**. Das Konnektivitätsmodul **300** entschlüsselt die interne Nachricht zum Aufheben des Schlüssels, hebt den VAK, die Funktion (*r_veh*) und die Hashfunktionen auf und generiert eine Antwort **724** (die der Antwort **724** ähnelt, aber den verschlüsselten VAK oder die verschlüsselte VAK-ID einschließt).

[0077] Das Haupttelematikmodul **320** leitet die Antwort **704** mit der Antwort **705** an das Backend **390** weiter. Das Backend **390** entschlüsselt die Antwort **705**, markiert den VAK und die Funktion als aufgehoben und übermittelt eine Bestätigung **726** der Aufhebung des Schlüssels an das Mobilgerät **380**. Die Bestätigung **726** der Aufhebung des Schlüssels ähnelt der Nachricht **706** zum Bereitstellen des Schlüssels. Das Mobilgerät **380** entschlüsselt die Bestätigung **726** des Aufhebens des Schlüssels und hebt den VAK, die Funktion (*r_ph*) und die Hashfunktionen auf Grundlage des verschlüsselten VAK oder der verschlüsselten VAK-ID auf.

[0078] Daher versteht sich, dass die folgenden Nachrichtenpaare ähnlich sind (gemäß denselben Verfahren verschlüsselt und geleitet), aber unterschiedliche zugrunde liegende Grunddaten einschließen, die entweder einem Befehl zum Bereitstellen des Schlüssels oder einem Befehl zum Aufheben des Schlüssels entsprechen: (i) Nachrichten **701** und **721**, (ii) Nachrichten **702** und **722**, (iii) Nachrichten **703** und **723**, (iv) Nachrichten **704** und **724**, (v) Nachrichten **705** und **725**, (vi) Nachrichten **706** und **726**. Es versteht sich, dass die folgenden Nachrichtenpaare wenigstens dieselben verschlüsselten Daten einschließen: (i) Nachrichten **702** und **703**, (ii) Nachrichten **704** und **705**, (iii) Nachrichten **722** und **723**, (iv) Nachrichten **724** und **725**. Verschiedene Dinge in dieser Offenbarung können geschützte Marken sein, einschließlich Bluetooth und Blu-Ray.

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

- US 15/076210 [0013]
- US 8180547 [0013]
- US 15/186850 [0013]
- US 2016/0117921 [0013]
- US 14/972761 [0013]

Patentansprüche

1. Rechensystem, umfassend:
ein Haupttelematikmodul,
ein Konnektivitätsmodul, umfassend eine Antenne(n), einen Prozessor(en), wobei das Konnektivitätsmodul zu Folgendem konfiguriert ist:
(a) Authentifizieren eines Mobilgeräts über einen Fahrzeugzugangsschlüssel (VAK);
(b), falls (a), Ausgeben eines kurzlebigen Sitzungsschlüssels (DSK) an das Mobilgerät;
(c), falls (b), Herstellen einer aktiven Sitzung mit dem Mobilgerät;
(d) Verschlüsseln von Nachrichten an das Mobilgerät mit dem VAK während (a) und mit dem DSK während (c).
2. Rechensystem nach Anspruch 1, wobei das Konnektivitätsmodul zum automatischen Aufheben des DSK konfiguriert ist.
3. Rechensystem nach Anspruch 2, wobei das Konnektivitätsmodul zum automatischen Aufheben des DSK bei Ablauf eines vorgegebenen Zeitintervalls konfiguriert ist.
4. Rechensystem nach Anspruch 3, wobei das Zeitintervall während (b) beginnt.
5. Rechensystem nach Anspruch 4, wobei das Konnektivitätsmodul dazu konfiguriert ist, während (c) Nachrichten vom Mobilgerät, die mit dem VAK verschlüsselt sind, abzuweisen, aber Nachrichten von einem anderen Mobilgerät, die mit einem anderen VAK verschlüsselt sind, anzunehmen.
6. Rechensystem nach Anspruch 1, 2, 3, 4 oder 5, wobei das Konnektivitätsmodul dazu konfiguriert ist, zu beginnen, (a) nachdem es eine unverschlüsselte Nachricht empfangen hat, die eine gültige VAK-ID und einen gültigen VAK-Hashwert umfasst.
7. Rechensystem nach Anspruch 1, 2, 3, 4 oder 5, wobei das Konnektivitätsmodul dazu konfiguriert ist, einen unverschlüsselten VAK-Authentifizierungscode in Nachrichten einzuschließen, die mit VAK verschlüsselte Daten einschließen.
8. Rechensystem nach Anspruch 7, wobei das Konnektivitätsmodul dazu konfiguriert ist, einen unverschlüsselten DSK-Hashwert in Nachrichten einzuschließen, die mit DSK verschlüsselte Daten einschließen.
9. Rechensystem nach Anspruch 1, 2, 3, 4 oder 5, wobei das Konnektivitätsmodul dazu konfiguriert ist, den DSK in einen ersten Block (DSK1) und einen zweiten Block (DSK2) zu trennen.
10. Rechensystem nach Anspruch 9, wobei sowohl der DSK1 als auch der DSK2 zum Berechnen des DSK notwendig sind.
11. Rechensystem nach Anspruch 9, wobei das Konnektivitätsmodul dazu konfiguriert ist, den DSK durch Faktorisieren des DSK derart zu trennen, dass DSK1 ein erster Faktor ist und DSK2 ein zweiter Faktor ist.
12. Rechensystem nach Anspruch 9, wobei das Konnektivitätsmodul dazu konfiguriert ist, den DSK1 in einer ersten Nachricht und DSK2 in einer späteren zweiten Nachricht zu übermitteln.
13. Rechensystem nach Anspruch 12, wobei das Konnektivitätsmodul dazu konfiguriert ist, den DSK2 als Erwiderung auf eine gültige Antwort vom Mobilgerät zu übermitteln.
14. Rechensystem nach Anspruch 13, wobei das Konnektivitätsmodul zum Übermitteln einer verschlüsselten Nonce an das Mobilgerät konfiguriert ist und wobei, um gültig zu sein, die Antwort einen Wert auf Grundlage der Nonce einschließen muss.
15. Rechensystem nach Anspruch 14, wobei das Konnektivitätsmodul dazu konfiguriert ist, DSK-Zusammensetzungsanweisungen mit DSK1 oder DSK2 zu übermitteln, und wobei das Konnektivitätsmodul dazu konfiguriert ist, die Nonce zu erhöhen und die erhöhte Nonce vor (c) an das Mobilgerät zu übermitteln.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

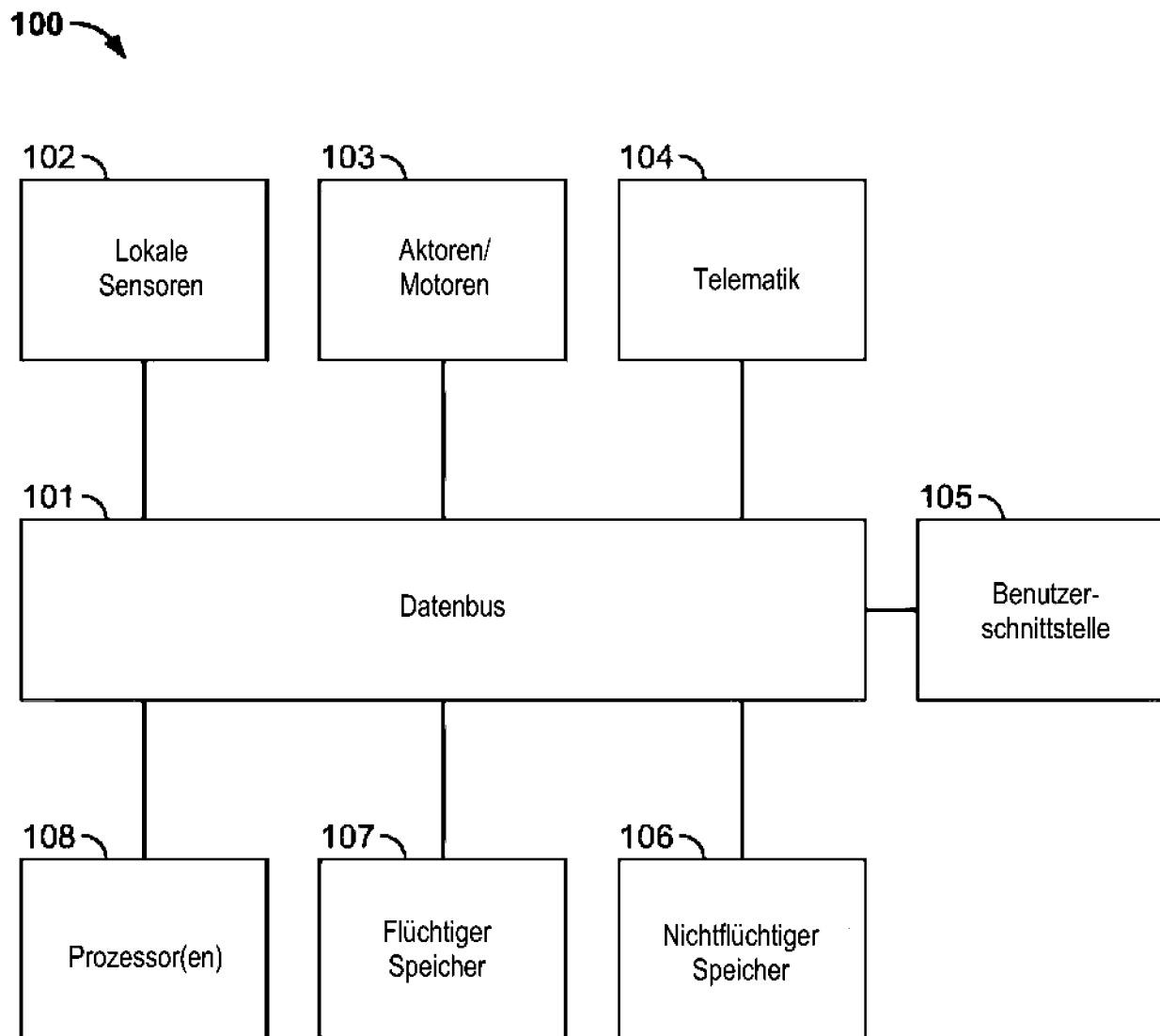


FIG. 1

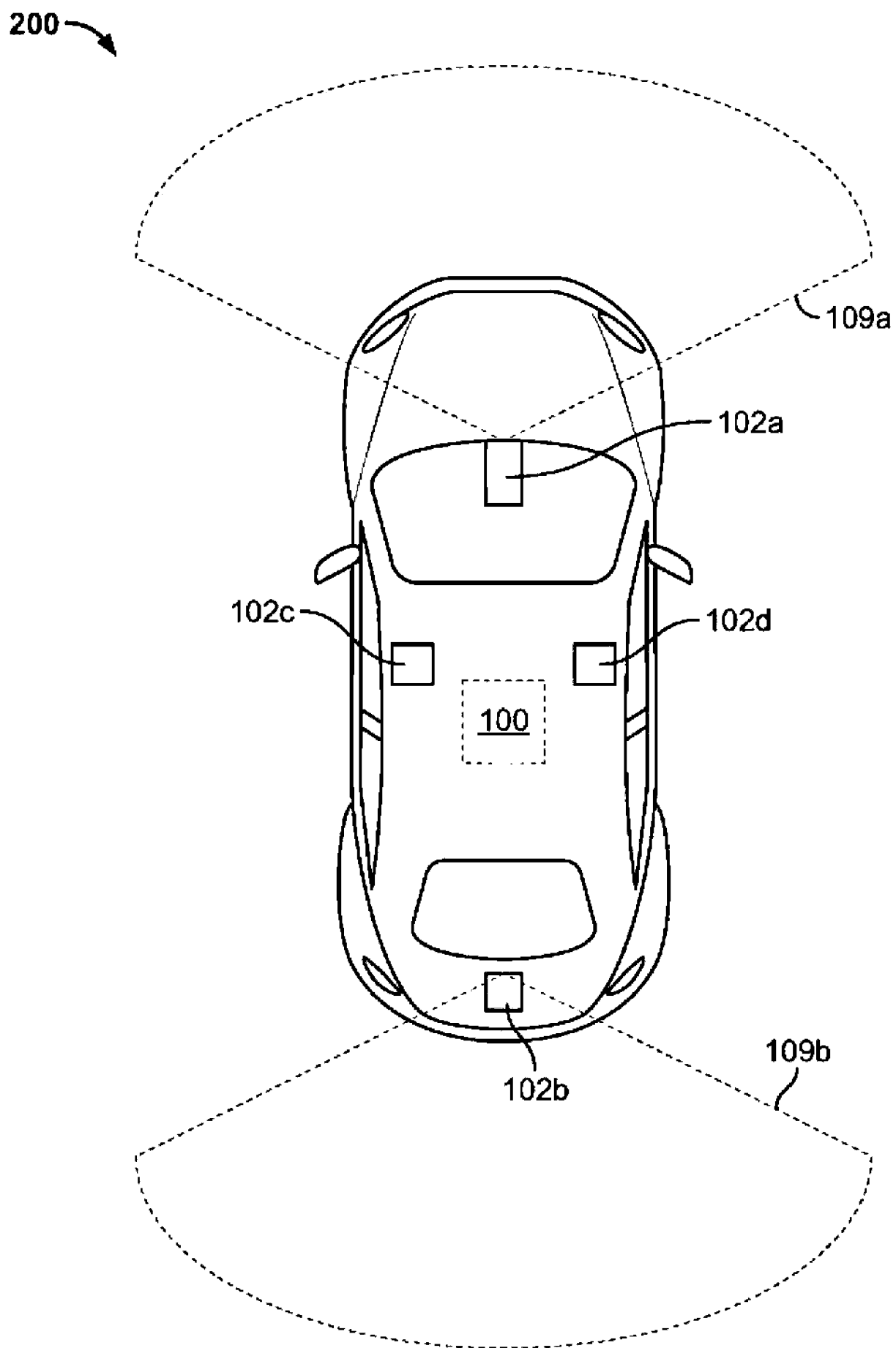


FIG. 2

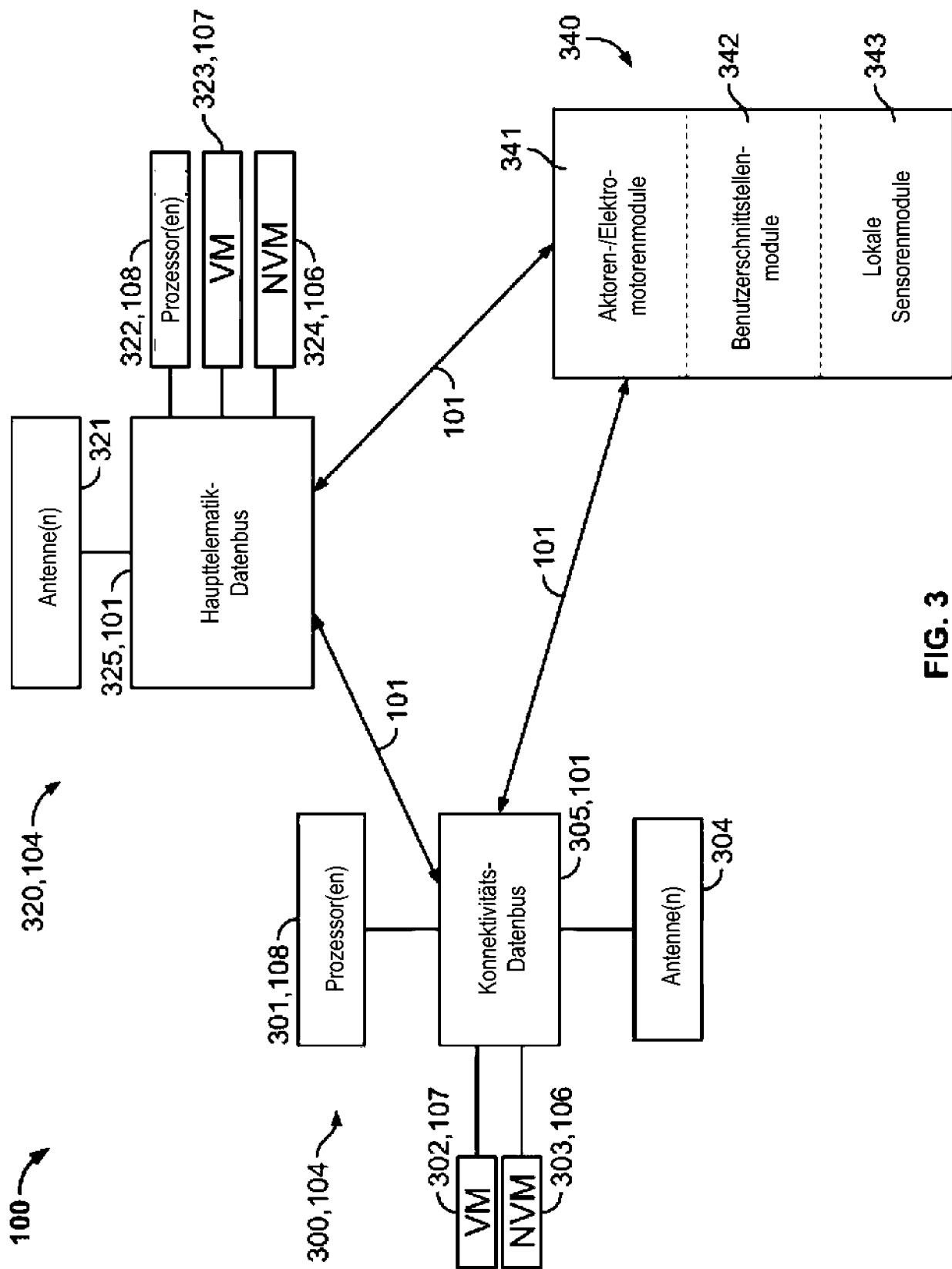
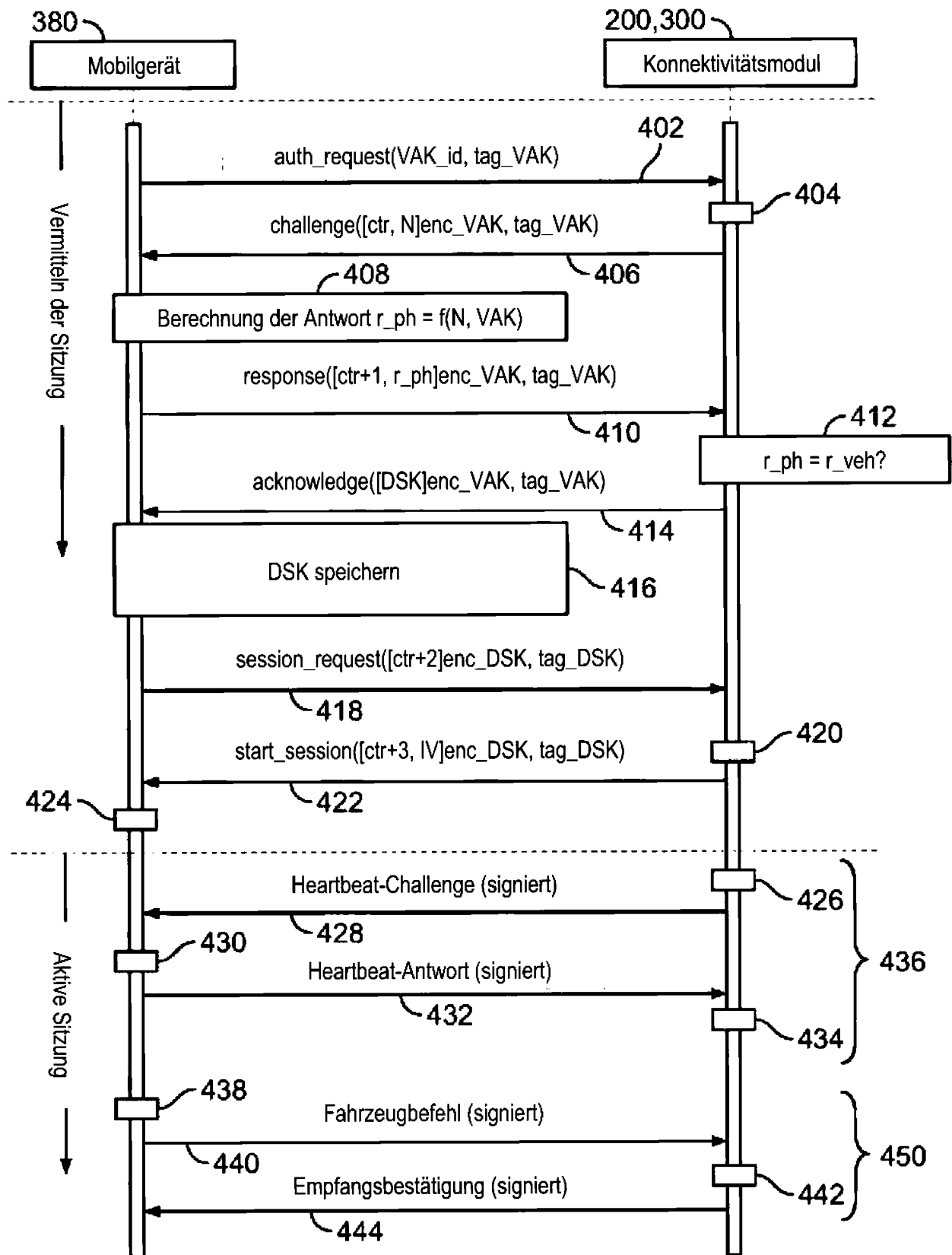


FIG. 3

**FIG. 4**

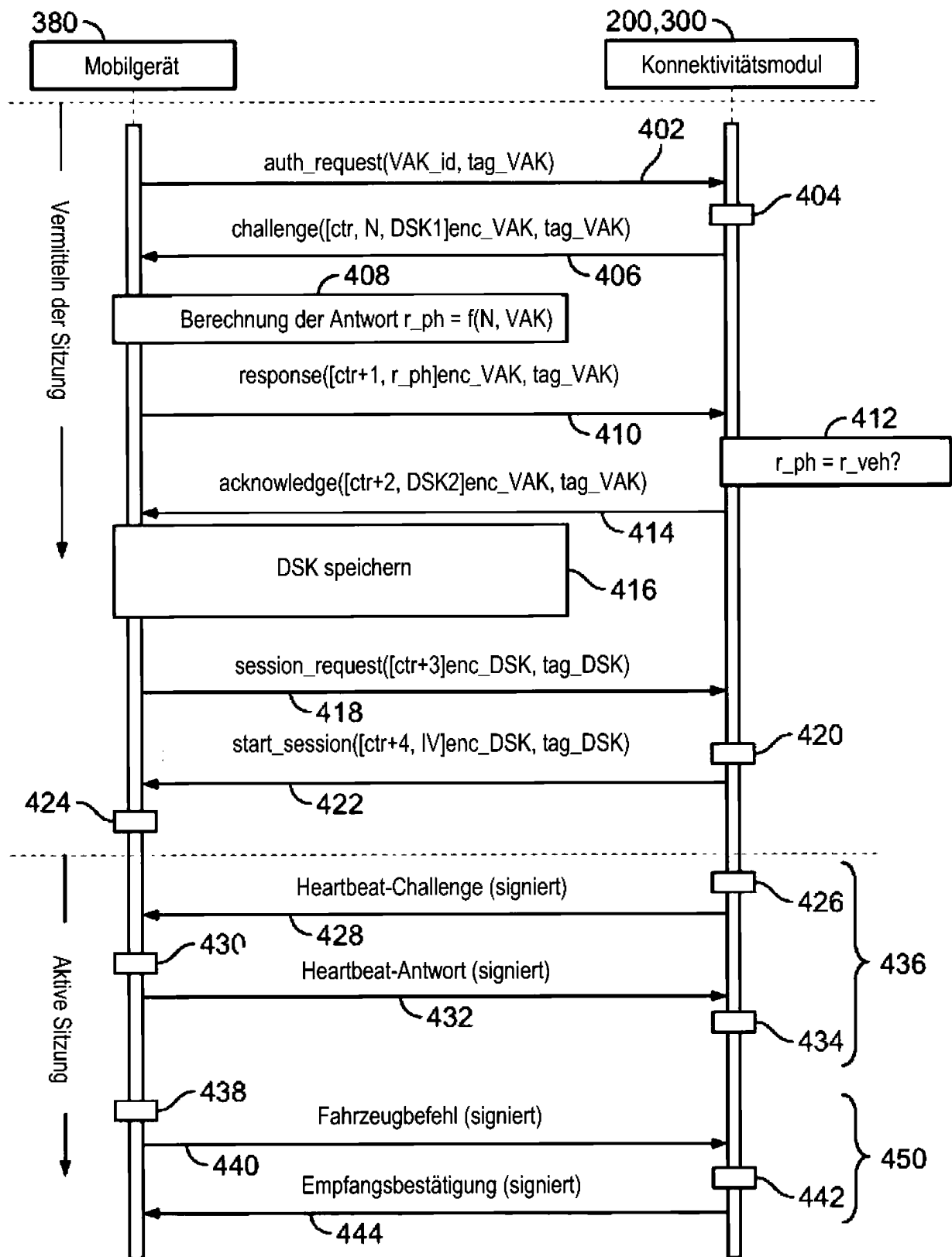


FIG. 5

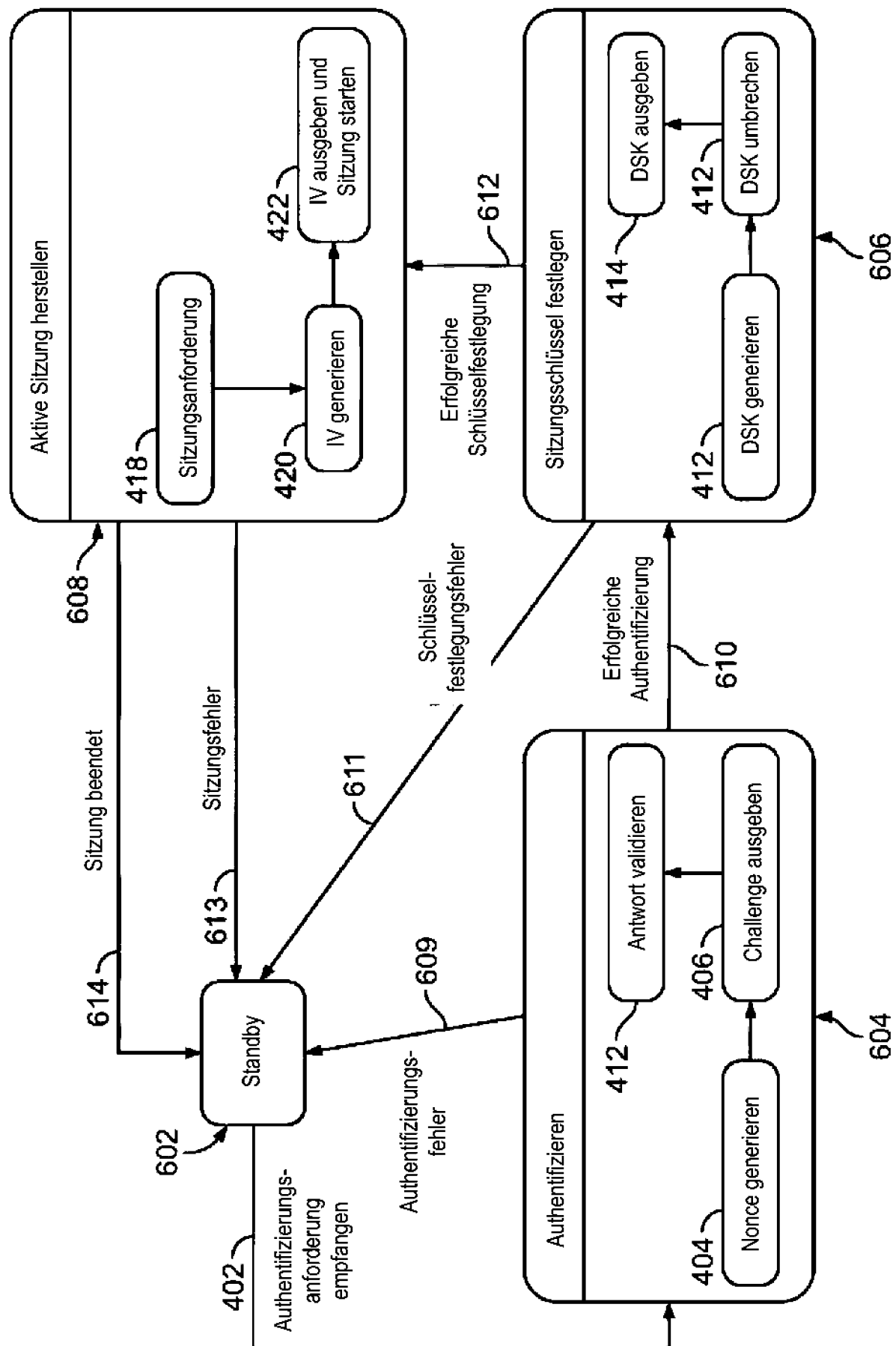


FIG. 6

