(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 219 014 A1** 2018.04.05

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 219 014.8**
(22) Anmeldetag: **30.09.2016**
(43) Offenlegungstag: **05.04.2018**

(51) Int Cl.: ***G06F 21/60*** (2013.01)
G06F 21/44 (2013.01)

(71) Anmelder:
VOLKSWAGEN AKTIENGESELLSCHAFT, 38440 Wolfsburg, DE

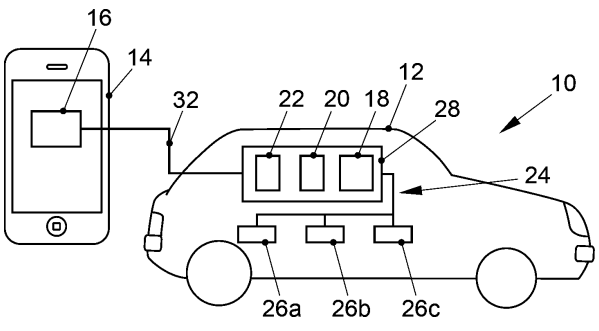
(72) Erfinder:
Meier, Andreas, Dr., 39106 Magdeburg, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs (12), mit den Schritten: Bereitstellen eines mobilen Endgeräts (14), auf welchem eine Anwendung (16) installiert ist, welche dazu eingerichtet ist, Daten des Fahrzeugs (12) zu verwenden, und Bereitstellen eines gesonderten Speichers (18), auf welchen mittels eines Steuergeräts (20) des Fahrzeugs (12) Daten des Fahrzeugs (12) zum Abruf durch das mobile Endgerät (14) bereitgestellt werden.
Es ist vorgesehen, dass das Verfahren das Authentifizieren der Anwendung (16) an einem hierzu eingerichteten Authentifizierungsmodul (22) mittels eines Identifikationsmerkmals und das Bereitstellen eines Lesezugriffs auf den gesonderten Speicher (18) für die Anwendung (16) auf dem mobilen Endgerät (14) nach erfolgter Authentifizierung umfasst.
Der Erfindung liegt die Aufgabe zugrunde, eine Möglichkeit zu schaffen, fahrzeugeigene Daten kontrolliert für die Verwendung mit Anwendungen auf mobilen Endgeräten bereitzustellen.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs und ein System zum gesicherten Zugriff auf Daten eines Fahrzeugs.

[0002] Fahrzeugbezogenen mobilen Online-Diensten stehen, anders als gewöhnlichen Anwendungen für mobile Endgeräte, wie Smartphones oder Tablets, fahrzeugeigene Daten zur Verfügung, welche beispielsweise durch Sensoren des betreffenden Fahrzeugs aufgezeichnet werden. Unter Verwendung solcher Daten lassen sich attraktive Programme für Fahrzeughalter und Fahrzeugnutzer realisieren, deren Verfügbarkeit und/oder Kompatibilität mit bestimmten Fahrzeugen zukünftig auch die Kaufentscheidung von Kaufinteressierten beeinflussen wird.

[0003] Die Entwicklung von mobilen Online-Diensten ist jedoch in Vergleich zu der Entwicklung von gewöhnlichen Anwendungen für mobile Endgeräte vergleichsweise kosten- und zeitintensiv. Der Nachteil der bekannten Anwendungen ist, dass diese keinen Zugriff auf fahrzeugeigene Daten haben. Es besteht das Bedürfnis, die Entwicklung von mobilen Online-Diensten, welche Zugriff auf fahrzeugeigene Daten haben, auch externen Entwicklern zu ermöglichen, um den Fahrzeughaltern und Fahrzeugnutzern entsprechende Programme zu attraktiven Konditionen zur Verfügung stellen zu können.

[0004] Es besteht jedoch stets die Gefahr, dass durch eine Freigabe der fahrzeugeigenen Daten ein Datenmissbrauch begünstigt wird. Aus diesem Grund muss vermieden werden, dass entsprechende Anwendungen unbeschränkten Zugriff auf die Daten von Fahrzeugen erlangen, welcher nicht durch den Hersteller oder eine andere Instanz kontrolliert werden kann.

[0005] Aus der Druckschrift DE 10 2011 100 938 A1 ist ein Fahrzeuginformations- und Unterhaltungssystem zur Ausführung von Anwendungen bekannt. Das System umfasst ein Betriebssystem, das eingerichtet ist, Anwendungen auszuführen, eine Überwachungseinheit, die eingerichtet ist, aktuelle Zustandsgrößen des Fahrzeugs zu ermitteln und eine Genehmigungseinheit, die eingerichtet ist, das Ausführen von Anwendungen durch das Betriebssystem abhängig von den ermittelten aktuellen Zustandsgrößen des Fahrzeugs zu verhindern oder zuzulassen.

[0006] Ferner offenbart die Druckschrift DE 10 2014 218 225 A1 ein Verfahren zum Aufbau einer gesicherten, authentifizierten Verbindung zwischen einem Gegenstand und einer zentralen Recheneinheit, bei dem die Verbindung durch eine mobile Recheneinheit aufgebaut wird, wobei eine Authentifizierung eines Nutzers an der zentralen Recheneinheit durch ein Client Zertifikat, das in eine App auf der mobilen Recheneinheit geladen wurde, sichergestellt wird.

[0007] Darüber hinaus ist aus der Druckschrift US 2012/0324482 A1 ein Verfahren bekannt, welches Anwendungen auf einem mobilen Endgerät erlaubt, auf eine sichere Art und Weise auf einer Fahrzeugunterhaltungseinrichtung bereitgestellt zu werden. Hierzu wird eine Erlaubnisprüfung durchgeführt, mittels welcher die Freigabe eines Benutzer für bestimmte Daten geprüft wird.

[0008] Diese und andere bekannte Lösungen stellen jedoch keine Möglichkeit bereit, wie eine Freigabe von fahrzeugeigenen Daten für Anwendungen auf mobilen Endgeräten erfolgen kann, ohne dass ein Kontrollverlust hinsichtlich der freigegebenen Daten erfolgt.

[0009] Der Erfindung liegt nun die Aufgabe zugrunde, eine Möglichkeit zu schaffen, fahrzeugeigene Daten kontrolliert für die Verwendung mit Anwendungen auf mobilen Endgeräten bereitzustellen.

[0010] Diese Aufgabe wird gelöst durch ein Verfahren gemäß Anspruch 1 beziehungsweise ein System gemäß Anspruch 10.

[0011] Bei dem erfindungsgemäßen Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs wird ein mobiles Endgerät bereitgestellt, auf welchem eine Anwendung installiert ist, welche dazu eingerichtet ist, Daten des Fahrzeugs zu verwenden. Ferner wird ein gesonderter Speicher bereitgestellt, auf welchen mittels eines Steuergeräts des Fahrzeugs Daten des Fahrzeugs zum Abruf durch das mobile Endgerät bereitgestellt werden. Erfindungsgemäß authentifiziert sich die Anwendung an einem hierzu eingerichteten Authentifizierungsmodul mittels eines Identifikationsmerkmals und der Anwendung auf dem mobilen Endgerät wird nach erfolgter Authentifizierung ein Lesezugriff auf den gesonderten Speicher für die bereitgestellt.

[0012] Das erfindungsgemäße Verfahren hat den Vorteil, dass kein direkter Zugriff auf ein fahrzeuginternes Kommunikationssystem, wie einem fahrzeuginternen Ethernet oder einem Fahrzeug-Bus, etwa einem Controller Area Network (CAN) Bus, einem Media Oriented Systems Transport (MOST) Bus oder einem FlexRay Bus, erfolgt. Durch die Verwendung eines gesonderten Speichers wird die Kommunikationsschnittstelle des Fahrzeugs, welche mit dem mobilen Endgerät kommuniziert, von den fahrzeuginternen Kommunikationssystemen entkoppelt. Es können somit nur die Daten zur Nutzung durch die Anwendung auf dem mobilen Endgerät freigegeben werden, welche sich auf dem gesonderten Spei-

cher befinden. Zusätzlich ist ein Authentifizierungsmodul vorgesehen, welches vor der Bereitstellung der Daten die Autorisierung des mobilen Endgerät und/oder der Anwendung auf dem mobilen Endgerät prüft. Das verwendete Identifikationsmerkmal ist vorzugsweise nur für eine ausgewählte Kombination aus Anwendung, mobilen Endgerät und Fahrzeug gültig. Auf diese Weise wird verhindert, dass eine manipulierte Anwendung das Identifikationsmerkmal einer anderen Anwendung nutzen kann und dass durch Kopieren des Identifikationsmerkmals auf ein anderes mobiles Endgerät und/oder durch eine Manipulationen der Anwendung auf Daten eines fremden Fahrzeugs zugegriffen werden kann. Vorzugsweise umfasst das Authentifizieren der Anwendung an dem hierzu eingerichteten Authentifizierungsmodul mittels des Identifikationsmerkmals ebenfalls das Autorisieren der Anwendung auf ausgewählte Daten auf dem gesonderten Speicher zuzugreifen. Insbesondere wird der Anwendung ausschließlich ein Lesezugriff auf den gesonderten Speicher erteilt. Vorzugsweise wird der Lesezugriff für sämtliche Daten oder nur für einen Teil der Daten, welche auf dem gesonderten Speicher gespeichert sind, erteilt. Insbesondere wird der Lesezugriff nur für Daten erteilt, für welche die Anwendung zuvor autorisiert wurde. Alternativ kann der Anwendung neben dem Lesezugriff auf den gesonderten Speicher auch ein Schreibzugriff auf den gesonderten Speicher erteilt werden.

[0013] Das Steuergerät kann mit einem oder mehreren fahrzeuginternen Kommunikationssystemen verbunden sein und dazu eingerichtet sein, Daten des Fahrzeugs zum Speichern auf dem gesonderten Speicher über das eine oder die mehreren fahrzeuginternen Kommunikationssysteme abzurufen. Auf diese Weise können fahrzeugeigene Daten, welche beispielsweise bereits von einem anderen fahrzeugeigenen Gerät verwendet werden, von dem Steuergerät abgerufen und auf dem gesonderten Speicher gespeichert werden. Dies können beispielsweise Sensordaten zur Position, Geschwindigkeit und/oder der Beschleunigung des Fahrzeugs sein. Ferner können die Daten den Energie- oder Kraftstoffverbrauch des Fahrzeugs oder den Zustand einzelner Fahrzeugsysteme betreffen. Ferner können die Daten auch Sensordatenhistorien und/oder -verläufe betreffen. Alternativ oder zusätzlich können die Daten Bild- und/oder Audiosignale betreffen, welche von fahrzeugeigenen Kameras, Radarsensoren, Laserscannern, Ultraschallsensoren und/oder anderen bildgebenden Sensoren beziehungsweise Mikrofonen aufgezeichnet werden.

[0014] Das Steuergerät kann den Zugriff der Anwendung auf dem mobilen Endgerät auf das eine oder die mehreren fahrzeuginternen Kommunikationssysteme verhindern. Dadurch, dass das Steuergerät den Zugriff der Anwendung auf dem mobilen Endgerät auf das eine oder die mehreren fahrzeuginternen Kommunikationssysteme verhindern kann, wird das Risiko des Kontrollverlusts über die Daten des Fahrzeugs weiter reduziert. Das Steuergerät kann den Zugriff der Anwendung auf dem mobilen Endgerät auf das eine oder die mehreren fahrzeuginternen Kommunikationssysteme vollständig oder teilweise verhindern. Einige Daten, welche innerhalb des Fahrzeugs kommuniziert werden, wie beispielsweise die Uhrzeit, das Datum oder andere öffentlich zugängliche und/oder nicht fahrzeugspezifische Daten, sind nicht besonders schützenswert, sodass in bestimmten Situationen eine teilweise Zugriffverhinderung sinnvoll sein kann.

[0015] Das Authentifizierungsmodul kann als Bestandteil eines fahrzeugeigenen Medienwiedergabesystems oder einer fahrzeugeigenen Kommunikationseinheit mit Internetkonnektivität ausgebildet sein. Die Authentifizierung kann somit bereits im Fahrzeug erfolgen, sodass keine gesonderte Verbindung zu einer Authentifizierungsinstanz notwendig ist. Insbesondere, wenn das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit dazu eingerichtet sind, direkt mit dem mobilen Endgerät zu kommunizieren, beispielsweise über Bluetooth, kann die Authentifizierung auch stattfinden, wenn eine Internetverbindung nicht zur Verfügung steht. Alternativ kann das Authentifizierungsmodul als Bestandteil eines Zentralrechners, welcher dazu eingerichtet ist, mit dem mobilen Endgerät und dem Fahrzeug zu kommunizieren, ausgebildet sein. Der Zentralrechner ist beispielsweise ein Backend eines Fahrzeugherstellers oder eines Drittanbieters. Dadurch, dass das Authentifizierungsmodul als Bestandteil eines Zentralrechners ausgebildet ist, kann eine zentrale Authentifizierung erfolgen. Insbesondere bei einer zertifikatsbasierten Authentifizierung kann dies vorteilhaft sein, wenn der Zentralrechner dazu eingerichtet ist, die Echtheit und Gültigkeit eines verwendeten Zertifikats zu prüfen.

[0016] Das Authentifizieren der Anwendung an dem hierzu eingerichteten Authentifizierungsmodul mittels eines Identifikationsmerkmals kann das Übertragen des Identifikationsmerkmals von dem mobilen Endgerät an das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit und/oder das Übertragen des Identifikationsmerkmals von dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit an den Zentralrechner umfassen. Vorzugsweise ist der Zentralrechner dazu eingerichtet, eine Berechtigungsdatei, welche beispielsweise einen Token oder ein Zertifikat umfasst, zu erzeugen und an das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit zu senden. Das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit leitet die Berechtigungsdatei dann an die Anwendung auf dem mobilen Endgerät weiter. Die Berech-

tigungsdatei kann eine beschränkte Gültigkeit haben und Informationen über den Umfang der für die Anwendung freizugebenden Daten umfassen. Ferner kann der Zentralrechner das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit darüber informieren, welche Daten der Anwendung auf dem mobilen Endgerät freizugeben sind. Das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit kann auf Grundlage dieser Information dann das Steuergerät dazu veranlassen, die entsprechenden Daten über ein oder mehrere fahrzeuginterne Kommunikationssysteme, etwa über einen Fahrzeug-Bus, abzurufen und auf dem gesonderten Speicher zu speichern. Das mobile Endgerät kann mittels der Berechtigungsdatei dann auf die entsprechenden Daten auf dem gesonderten Speicher zugreifen. Wenn eine Anwendung nachträglich als schadhaft identifiziert wird, kann die Berechtigungsdatei beziehungsweise das Zertifikat oder der Token innerhalb der Berechtigungsdatei als ungültig erklärt werden, sodass der Zentralrechner die Datenfreigabe sperrt. Die Anwendung auf dem mobilen Endgerät kann zuvor durch den Hersteller oder einen Drittanbieter untersucht und geprüft worden sein, um den Umfang der für die Anwendung freizugebenden Daten des Fahrzeugs zu definieren.

[0017] Das Identifikationsmerkmal kann einen Token und/oder ein Zertifikat umfassen. Alternativ oder zusätzlich können auch PINs, Hashes und andere Sicherheitsfunktionen genutzt werden. Das Zertifikat und/oder der Token müssen vor der ersten Benutzung erstellt und auf dem mobilen Endgerät gespeichert werden. Wird das mobile Endgerät dann signalleitend mit dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit verbunden, kann sich die Anwendung direkt an dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit authentifizieren. Die signalleitende Verbindung zwischen dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit und dem mobilen Endgerät kann kabelgebunden oder kabellos sein. Zum Authentifizieren wird das Zertifikat oder der Token an das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit übertragen. Das Zertifikat oder der Token kann dann von dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit verschlüsselt an den Zentralrechner übertragen werden. Der Zentralrechner prüft das Zertifikat oder den Token auf Gültigkeit. Die Prüfung auf Gültigkeit umfasst vorzugsweise die Feststellung, ob die in dem Zertifikat oder dem Token vermerkte Anwendung von dem in dem Zertifikat oder dem Token vermerkten mobilen Endgerät auf das in dem Zertifikat oder dem Token vermerkte Fahrzeug zugreift. Wird dies bestätigt, benachrichtigt der Zentralrechner das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit darüber, auf welche Daten des Fahrzeugs die Anwendung zugreifen darf. Sobald das fahrzeugeigene Medienwiedergabesystem oder die fahrzeugeigene Kommunikationseinheit die Authentizität bestätigt bekommen hat und benachrichtigt wurde, welche Daten zur Verfügung gestellt werden sollen, kann es der Anwendung eine Berechtigungsdatei ausstellen, welche ebenfalls ein Zertifikat oder ein Token umfassen kann. Weiterhin startet ein Speicherprozess, der die angeforderten Daten von dem einen oder den mehreren fahrzeuginternen Kommunikationssystemen abruft und auf dem gesonderten Speicher speichert.

[0018] Der gesonderte Speicher kann als Bestandteil eines fahrzeugeigenen Medienwiedergabesystems oder einer fahrzeugeigenen Kommunikationseinheit mit Internetkonnektivität ausgebildet sein. Alternativ kann der gesonderte Speicher als Bestandteil eines Zentralrechners, welcher dazu eingerichtet ist, mit dem mobilen Endgerät und dem Fahrzeug zu kommunizieren, ausgebildet sein. Wenn der gesonderte Speicher als Bestandteil des fahrzeugeigenen Medienwiedergabesystems oder der fahrzeugeigenen Kommunikationseinheit ausgebildet ist, kann ein direkter Datenaustausch zwischen dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit und dem mobilen Endgerät stattfinden. Ist der gesonderte Speicher als Bestandteil eines Zentralrechners ausgebildet, wird die Datensicherheit weiter erhöht, da die Daten des Fahrzeugs von dem mobilen Endgerät nicht vom Fahrzeug direkt, sondern von einem fahrzeugexternen Speicher abgerufen werden. Das Risiko, dass die Anwendung Zugriff auf weitere Daten des Fahrzeugs erhält, wird somit erheblich reduziert.

[0019] Das Verfahren kann das Übertragen von Daten des Fahrzeugs von dem einen oder den mehreren fahrzeuginternen Kommunikationssystemen zu dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit und/oder das Übertragen von Daten des Fahrzeugs von dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit zu dem mobilen Endgerät umfassen. Alternativ oder zusätzlich kann das Verfahren das Übertragen von Daten des Fahrzeugs von dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit zu dem Zentralrechner und/oder das Übertragen von Daten des Fahrzeugs von dem Zentralrechner zu dem mobilen Endgerät umfassen. Abhängig davon, in welchem Gerät der gesonderte Speicher, auf welchen das mobile Endgerät Zugriff hat, integriert ist, können sich verschiedene Kombinationen der bezeichneten Datenübertragungswege ergeben. Die Übertragung der Daten des Fahrzeugs von dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit direkt zu dem mobilen End-

gerät vereinfacht das Zugriffsverfahren. Die Übertragung der Daten des Fahrzeugs von dem fahrzeugeigenen Medienwiedergabesystem oder der fahrzeugeigenen Kommunikationseinheit über den Zentralrechner zu dem mobilen Endgerät führt zu einer nochmals gesteigerten Kontrolle über die freigegebenen Daten.

[0020] Die Anwendung auf dem mobilen Endgerät kann die Daten des Fahrzeugs über eine Anwendungsprogrammierschnittstelle abrufen. Der Abruf der Daten des Fahrzeugs von dem gesonderten Speicher durch die Anwendung auf dem mobilen Endgerät und/oder der Abruf der Daten des Fahrzeugs von dem einen oder den mehreren fahrzeuginternen Kommunikationssystemen durch das Steuergerät kann regelmäßig oder unregelmäßig erfolgen. Ferner kann der Abruf der Daten des Fahrzeugs von dem gesonderten Speicher durch die Anwendung auf dem mobilen Endgerät und/oder der Abruf der Daten des Fahrzeugs von dem einen oder den mehreren fahrzeuginternen Kommunikationssystemen durch das Steuergerät durch ein Ereignis initiiert werden. Das Ereignis kann beispielsweise das Vorliegen neuer Daten des Fahrzeugs betreffen, sodass der Datenabruf immer dann initiiert wird, wenn neue Daten des Fahrzeugs vorliegen. In einem weiteren Ausführungsbeispiel emuliert das mobile Endgerät, auf welchem die Anwendung installiert ist, fahrzeugeigene Komponenten, wie beispielswiese die fahrzeugeigene Kommunikationseinheit.

[0021] Das erfindungsgemäße System zum gesicherten Zugriff auf Daten eines Fahrzeugs umfasst ein mobiles Endgerät und einen gesonderten Speicher. Auf dem mobilen Endgerät ist eine Anwendung installiert, welche dazu eingerichtet ist, Daten des Fahrzeugs zu verwenden. Auf dem gesonderten Speicher werden mittels eines Steuergeräts des Fahrzeugs Daten des Fahrzeugs zum Abruf durch das mobile Endgerät bereitgestellt. Erfindungsgemäß ist das System dazu eingerichtet, das Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs nach einer der vorstehend beschriebenen Ausführungsformen auszuführen. Vorzugsweise weist das System zusätzlich einen Zentralrechner auf. Es gelten die gleichen Vorteile und Modifikationen wie zuvor beschrieben.

[0022] Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den übrigen, in den Unteransprüchen genannten Merkmalen. Die verschiedenen in dieser Anmeldung genannten Ausführungsformen der Erfindung sind, sofern im Einzelfall nicht anders ausgeführt, mit Vorteil miteinander kombinierbar.

[0023] Die Erfindung wird nachfolgend in Ausführungsbeispielen anhand der zugehörigen Zeichnungen erläutert. Es zeigen:

[0024] Fig. 1 ein Ausführungsbeispiel des erfindungsgemäßen Systems zum gesicherten Zugriff auf Daten eines Fahrzeugs in einer schematischen Darstellung; und

[0025] Fig. 2 ein weiteres Ausführungsbeispiel des erfindungsgemäßen Systems zum gesicherten Zugriff auf Daten eines Fahrzeugs in einer schematischen Darstellung.

[0026] Fig. 1 zeigt ein System **10** mit einem Fahrzeug **12** und einem mobilen Endgerät **14**. Auf dem mobilen Endgerät **14** ist eine Anwendung **16** installiert, welche dazu eingerichtet ist, Daten des Fahrzeugs **12** zu verwenden. Das Fahrzeug **12** umfasst ein fahrzeugeigenes Medienwiedergabesystem **28** und ein fahrzeuginternes Kommunikationssystem **24**.

[0027] Das fahrzeuginterne Kommunikationssystem **24** umfasst einen CAN-Bus, mit welchem insgesamt drei Sensoren **26a**–**26c** signalleitend verbunden sind, wobei die drei Sensoren **26a**–**26c** Daten des Fahrzeugs **12** aufzeichnen. Der Sensor **26a** ist ein Beschleunigungssensor und stellt Beschleunigungsdaten des Fahrzeugs **12** bereit. Der Sensor **26b** detektiert den Kraftstoffverbrauch des Fahrzeugs **12** und stellt kraftstoffbezogene Verbrauchsdaten des Fahrzeugs **12** bereit. Der Sensor **26c** ist ein Abstandssensor und stellt Daten bereit, welche den Abstand des Fahrzeugs **12** zu einem vorausfahrenden Fahrzeug betreffen.

[0028] Das fahrzeugeigene Medienwiedergabesystem **28** weist einen gesonderten Speicher **18**, ein Steuergerät **20** und ein Authentifizierungsmodul **22** auf. Auf dem gesonderten Speicher **18** werden mittels des Steuergeräts **20** des Fahrzeugs **12** Daten des Fahrzeugs **12** zum Abruf durch das mobile Endgerät **14** bereitgestellt. Das Steuergerät **20** ist mit dem fahrzeuginternen Kommunikationssystem **24** verbunden und dazu eingerichtet, die Daten des Fahrzeugs **12** zum Speichern auf dem gesonderten Speicher **18** von den Sensoren **26a**–**26c** über das fahrzeuginterne Kommunikationssystem **24** abzurufen. Außerdem verhindert das Steuergerät **20** den direkten Zugriff der Anwendung **16** auf dem mobilen Endgerät **14** auf das fahrzeuginterne Kommunikationssystem **24**.

[0029] Das System **10** ist dazu eingerichtet, dass sich die Anwendung **16** an dem hierzu eingerichteten Authentifizierungsmodul **22** mittels eines Identifikationsmerkmals authentifizieren kann, sodass nach erfolgter Authentifizierung ein Lesezugriffs auf den gesonderten Speicher **18** für die Anwendung **16** auf dem mobilen Endgerät **14** bereitgestellt werden kann. Das Identifikationsmerkmal wurde zuvor auf dem mobilen Endgerät **14** gespeichert und umfasst ein Zertifikat, welches für den Zugriff einer ausgewählten Anwendung **16** auf einem ausgewählten mobilen End-

gerät **14** auf Daten eines ausgewählten Fahrzeugs **12** gültig ist.

[0030] Das Authentifizieren der Anwendung **16** an dem hierzu eingerichteten Authentifizierungsmodul **22** mittels des Identifikationsmerkmals umfasst das Übertragen des Identifikationsmerkmals von dem mobilen Endgerät **14** an das fahrzeugeigene Medienwiedergabesystem **28**. Zum Bereitstellen der Daten des Fahrzeugs **12** werden die Daten des Fahrzeugs **12** von dem fahrzeuginternen Kommunikationssystem **24** zu dem fahrzeugeigenen Medienwiedergabesystems **28** übertragen. Von dem fahrzeugeigenen Medienwiedergabesystem **28** werden die Daten des Fahrzeugs **12** dann zu dem mobilen Endgerät **14** übertragen. Die Authentifizierung der Anwendung **16** und das Bereitstellen der Daten des Fahrzeugs **12** für die Anwendung **16** erfolgt über die Kommunikationsverbindung **32**. Die Anwendung **16** auf dem mobilen Endgerät **14** ruft die Daten des Fahrzeugs **12** über eine Anwendungsprogrammierschnittstelle von dem Fahrzeug **12** ab.

[0031] Fig. 2 zeigt ein System **10** mit einem Fahrzeug **12**, einem mobilen Endgerät **14** und einem Zentralrechner **30**. Auf dem mobilen Endgerät **14** ist eine Anwendung **16** installiert, welche dazu eingerichtet ist, Daten des Fahrzeugs **12** zu verwenden. Das Fahrzeug **12** umfasst ein fahrzeugeigenes Medienwiedergabesystem **28** und ein fahrzeuginternes Kommunikationssystem **24**. Der Zentralrechner **30** ist als Backend eines Fahrzeughersteller ausgebildet und umfasst einen gesonderten Speicher **18** und ein Authentifizierungsmodul **22**. Ferner ist der Zentralrechner **30** dazu eingerichtet, über die Kommunikationsverbindung **34** mit dem mobilen Endgerät **14** und über die Kommunikationsverbindung **36** mit dem Fahrzeug **12** zu kommunizieren.

[0032] Das fahrzeuginterne Kommunikationssystem umfasst einen MOST-Bus, mit welchem insgesamt drei Kameras **26a**–**26c** signalleitend verbunden sind, wobei die drei Kameras **26a**–**26c** Daten des Fahrzeugs **12** aufzeichnen. Die Kamera **26a** ist eine Frontkamera und stellt ein Bildsignal für die vordere Fahrzeugumgebung bereit. Die Kamera **26b** ist eine Heckkamera und stellt ein Bildsignal für die hintere Fahrzeugumgebung bereit. Die Kamera **26c** ist eine Innenraumkamera und stellt ein Bildsignal für den Bereich des Fahrersitzes bereit.

[0033] Das fahrzeugeigene Medienwiedergabesystem **28** weist ein Steuergerät **20** auf. Mittels des Steuergeräts **20** des Fahrzeugs **12** werden Daten des Fahrzeugs **12** auf dem gesonderten Speicher **18** des Zentralrechners **30** zum Abruf durch das mobile Endgerät **14** bereitgestellt. Das Steuergerät **20** ist hierzu mit dem fahrzeuginternen Kommunikationssystem **24** verbunden und dazu eingerichtet, die Daten des Fahrzeugs **12** zum Speichern auf dem gesonderten Speicher **18** von den Kameras **26a**–**26c** über das fahrzeuginterne Kommunikationssystem **24** abzurufen. Außerdem verhindert das Steuergerät **20** den direkten Zugriff der Anwendung **16** auf dem mobilen Endgerät **14** auf das fahrzeuginterne Kommunikationssystem **24**.

[0034] Das System **10** ist dazu eingerichtet, dass sich die Anwendung **16** an dem hierzu eingerichteten Authentifizierungsmodul **22** mittels eines Identifikationsmerkmals authentifizieren kann, sodass nach erfolgter Authentifizierung ein Lesezugriff auf den gesonderten Speicher **18** für die Anwendung **16** auf dem mobilen Endgerät **14** bereitgestellt werden kann. Das Identifikationsmerkmal wurde zuvor auf dem mobilen Endgerät **14** gespeichert und umfasst einen Token, welcher für den Zugriff einer ausgewählten Anwendung **16** auf einem ausgewählten mobilen Endgerät **14** auf Daten eines ausgewählten Fahrzeugs **12** gültig ist.

[0035] Das Authentifizieren der Anwendung **16** an dem hierzu eingerichteten Authentifizierungsmodul **22** mittels eines Identifikationsmerkmals umfasst das Übertragen des Identifikationsmerkmals von dem mobilen Endgerät **14** an das fahrzeugeigene Medienwiedergabesystem **28** und das Übertragen des Identifikationsmerkmals von dem fahrzeugeigenen Medienwiedergabesystem **28** an den Zentralrechner **30**.

[0036] Zum Bereitstellen der Daten des Fahrzeugs **12** werden die Daten des Fahrzeugs **12** von dem fahrzeuginternen Kommunikationssystem **24** zu dem fahrzeugeigenen Medienwiedergabesystem **28** übertragen. Von dem fahrzeugeigenen Medienwiedergabesystem **28** werden die Daten des Fahrzeugs **12** dann zu dem Zentralrechner **30** übertragen. Von dem Zentralrechner **30** werden danach die Daten des Fahrzeugs **12** zu dem mobilen Endgerät **14** übertragen. Die Authentifizierung der Anwendung **16** erfolgt somit über die Kommunikationsverbindungen **32** und **36**. Das Bereitstellen der Daten des Fahrzeugs **12** für die Anwendung **16** erfolgt somit über die Kommunikationsverbindungen **34** und **36**. Die Anwendung **16** auf dem mobilen Endgerät **14** ruft die Daten des Fahrzeugs **12** über eine Anwendungsprogrammierschnittstelle von dem Zentralrechner **30** ab.

[0037] Dadurch, dass die Anwendung sich an einem hierzu eingerichteten Authentifizierungsmodul mittels eines Identifikationsmerkmals authentifiziert und daraufhin ein Lesezugriffs auf den gesonderten Speicher für die Anwendung auf dem mobilen Endgerät bereitgestellt wird, erlaubt es die Erfindung, dass fahrzeugeigene Daten kontrolliert für die Verwendung mit Anwendungen auf mobilen Endgeräten bereitgestellt werden können.

Bezugszeichenliste

10	System
12	Fahrzeug
14	mobiles Endgerät
16	Anwendung
18	gesonderter Speicher
20	Steuergerät
22	Authentifizierungsmodul
24	fahrzeuginternes Kommunikationssystem
26a–26c	Sensoren oder Kameras
28	Medienwiedergabesystem
30	Zentralrechner
32	Kommunikationsverbindung
34	Kommunikationsverbindung
36	Kommunikationsverbindung

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

- DE 102011100938 A1 [0005]
- DE 102014218225 A1 [0006]
- US 2012/0324482 A1 [0007]

Patentansprüche

1. Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs (**12**), mit den Schritten:
– Bereitstellen eines mobilen Endgeräts (**14**), auf welchem eine Anwendung (**16**) installiert ist, welche dazu eingerichtet ist, Daten des Fahrzeugs (**12**) zu verwenden; und
– Bereitstellen eines gesonderten Speichers (**18**), auf welchen mittels eines Steuergeräts (**20**) des Fahrzeugs (**12**) Daten des Fahrzeugs (**12**) zum Abruf durch das mobile Endgerät (**14**) bereitgestellt werden;
gekennzeichnet durch die Schritte:
– Authentifizieren der Anwendung (**16**) an einem hierzu eingerichteten Authentifizierungsmodul (**22**) mittels eines Identifikationsmerkmals; und
– Bereitstellen eines Lesezugriffs auf den gesonderten Speicher (**18**) für die Anwendung (**16**) auf dem mobilen Endgerät (**14**) nach erfolgter Authentifizierung.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** dass das Steuergerät (**20**) mit einem oder mehreren fahrzeuginternen Kommunikationssystemen (**24**) verbunden ist und dazu eingerichtet ist, Daten des Fahrzeugs (**12**) zum Speichern auf dem gesonderten Speicher (**18**) über das eine oder die mehreren fahrzeuginternen Kommunikationssysteme (**24**) abzurufen.

3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet,** dass das Steuergerät (**20**) den Zugriff der Anwendung (**16**) auf dem mobilen Endgerät (**14**) auf das eine oder die mehreren fahrzeuginternen Kommunikationssysteme (**24**) verhindert.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass das Authentifizierungsmodul (**22**) als Bestandteil eines fahrzeugeigenen Medienwiedergabesystems (**28**), einer fahrzeugeigenen Kommunikationseinheit mit Internetkonnektivität oder eines Zentralrechners (**30**), welcher dazu eingerichtet ist, mit dem mobilen Endgerät (**14**) und dem Fahrzeug (**12**) zu kommunizieren, ausgebildet ist.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet,** dass das Authentifizieren der Anwendung (**16**) an dem hierzu eingerichteten Authentifizierungsmodul (**22**) mittels eines Identifikationsmerkmals zumindest einen der folgenden Schritte umfasst:
– Übertragen des Identifikationsmerkmals von dem mobilen Endgerät (**14**) an das fahrzeugeigene Medienwiedergabesystem (**28**) oder die fahrzeugeigene Kommunikationseinheit;
– Übertragen des Identifikationsmerkmals von dem fahrzeugeigenen Medienwiedergabesystem (**28**) oder der fahrzeugeigenen Kommunikationseinheit an den Zentralrechner (**30**).

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass das Identifikationsmerkmal einen Token und/oder ein Zertifikat umfasst.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass der gesonderte Speicher (**18**) als Bestandteil eines fahrzeugeigenen Medienwiedergabesystems (**28**), einer fahrzeugeigenen Kommunikationseinheit mit Internetkonnektivität oder eines Zentralrechners (**30**), welcher dazu eingerichtet ist, mit dem mobilen Endgerät (**14**) und dem Fahrzeug (**12**) zu kommunizieren, ausgebildet ist.

8. Verfahren nach Anspruch 7, gekennzeichnet durch zumindest einen der folgenden Schritte:
– Übertragen von Daten des Fahrzeugs (**12**) von dem einen oder den mehreren fahrzeuginternen Kommunikationssystemen (**24**) zu dem fahrzeugeigenen Medienwiedergabesystem (**28**) oder der fahrzeugeigenen Kommunikationseinheit;
– Übertragen von Daten des Fahrzeugs (**12**) von dem fahrzeugeigenen Medienwiedergabesystem (**28**) oder der fahrzeugeigenen Kommunikationseinheit zu dem mobilen Endgerät (**14**);
– Übertragen von Daten des Fahrzeugs (**12**) von dem fahrzeugeigenen Medienwiedergabesystem (**28**) oder der fahrzeugeigenen Kommunikationseinheit zu dem Zentralrechner (**30**);
– Übertragen von Daten des Fahrzeugs (**12**) von dem Zentralrechner (**30**) zu dem mobilen Endgerät (**14**).

9. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass die Anwendung (**16**) auf dem mobilen Endgerät (**14**) die Daten des Fahrzeugs (**12**) über eine Anwendungsprogrammierschnittstelle abruft.

10. System (**10**) zum gesicherten Zugriff auf Daten eines Fahrzeugs (**12**), mit
– einem mobilen Endgerät (**14**), auf welchem eine Anwendung (**16**) installiert ist, welche dazu eingerichtet ist, Daten des Fahrzeugs (**12**) zu verwenden; und
– einem gesonderten Speicher (**18**), auf welchen mittels eines Steuergeräts (**20**) des Fahrzeugs (**12**) Daten des Fahrzeugs (**12**) zum Abruf durch das mobile Endgerät (**14**) bereitgestellt werden;
dadurch gekennzeichnet, dass das System (**10**) dazu eingerichtet ist, das Verfahren zum gesicherten Zugriff auf Daten eines Fahrzeugs (**12**) nach einem der vorstehenden Ansprüche auszuführen.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

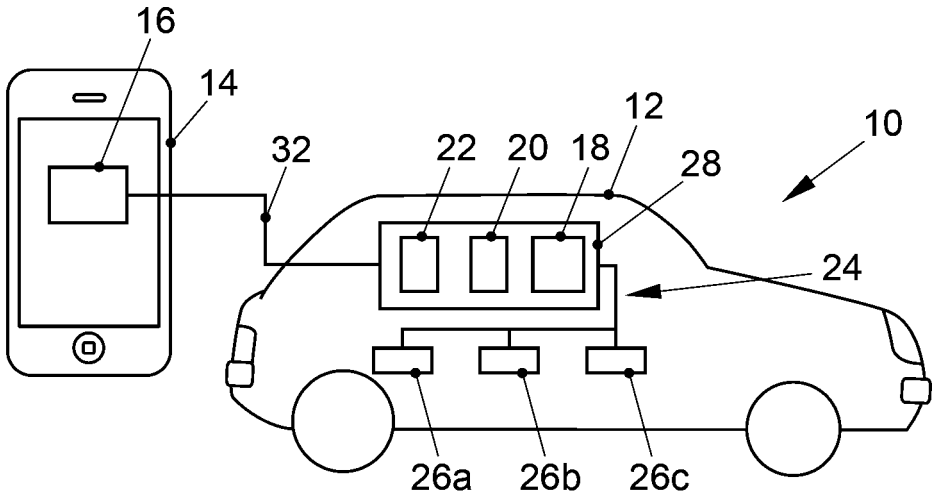


FIG. 1

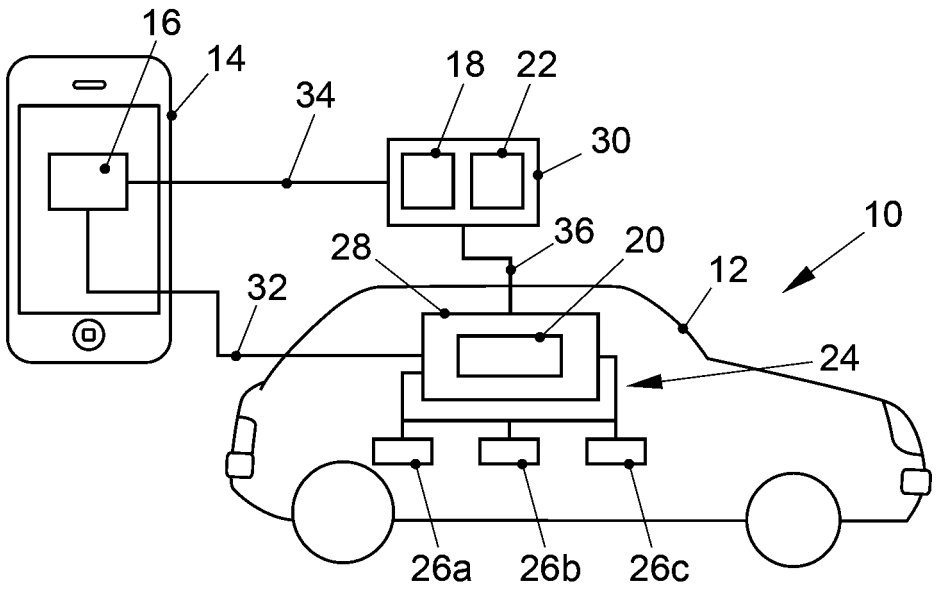


FIG. 2