

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. Januar 2024 (25.01.2024)



(10) Internationale Veröffentlichungsnummer
WO 2024/017697 A1

(51) Internationale Patentklassifikation:

H04L 9/40 (2022.01) H04W 12/61 (2021.01)
H04W 4/40 (2018.01) H04W 12/71 (2021.01)
H04W 12/06 (2021.01)

(21) Internationales Aktenzeichen: PCT/EP2023/069117

(22) Internationales Anmeldedatum:
11. Juli 2023 (11.07.2023)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2022 002 638.4
19. Juli 2022 (19.07.2022) DE

(71) Anmelder: **MERCEDES-BENZ GROUP AG** [DE/DE];
Mercedesstraße 120, 70372 Stuttgart (DE).

(72) Erfinder: **BECKER, Patrick**; Kralnstrasse 53, 49074 Os-
nabrück (DE). **ECHARD, Jörg**; Wilhelm-Haspel-Strasse
13, 71065 Sindelfingen (DE). **GERBAN, Mark**; Fuhsbütt-
ler Strasse 312, 22307 Hamburg (DE). **KEPPLER, Mar-
tin**; Zavelsteiner Strasse 20, 75394 Oberreichenbach (DE).

(74) Anwalt: **KOCHER, Klaus-Peter**; Daimler Brand & IP
Management GmbH & Co. KG 063- H512, 70546 Stuttgart
(DE).

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

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD,
SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY,
KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,
IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO,

(54) Title: METHOD FOR STORING AN IDENTIFIER IN A CENTRAL COMPUTING DEVICE

(54) Bezeichnung: VERFAHREN ZUM HINTERLEGEN EINES IDENTIFIKATORS AUF EINER ZENTRALEN
RECHENEINRICHTUNG

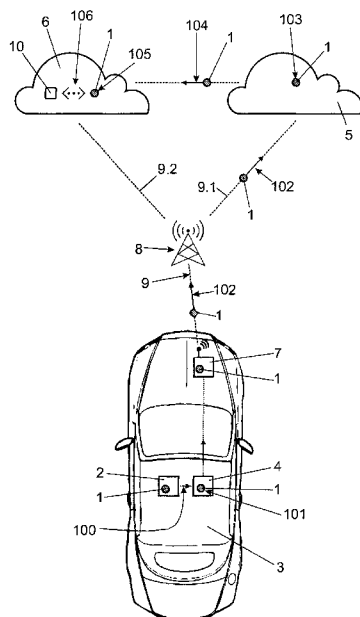


Fig. 1

(57) Abstract: The invention relates to a method for storing an identifier in a central computing device, wherein a first identifier (1) is read out from a control unit (2) of a vehicle (3) and is transmitted to an in-vehicle computing unit (4) for persistent storage and the first identifier (1) is transmitted from the in-vehicle computing unit (4) to a central OEM computing device (5). The method according to the invention is characterized in that the first identifier (1) is transmitted to the central OEM computing device (5) by means of a cryptographically secured transmission channel and is transmitted from the central OEM computing device (5), after the receipt of a transmission order, to a central service-provider computing device (6) by means of a cryptographically secured transmission channel. (Figure 1)

(57) Zusammenfassung: Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung Die Erfindung betrifft ein Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung, wobei ein erster Identifikator (1) aus einem Steuergerät (2) eines Fahrzeugs (3) ausgelesen und an eine fahrzeuginterne Recheneinheit (4) zum persistenten Speichern übertragen wird und der erste Identifikator (1) von der fahrzeuginternen Recheneinheit (4) an eine zentrale OEM-Recheneinrichtung (5) übertragen wird. Das erfindungsgemäße Verfahren ist dadurch gekennzeichnet, dass der erste Identifikator (1) an die zentrale OEM-Recheneinrichtung (5) über einen kryptografisch abgesicherten Übertragungskanal übertragen wird und von der zentralen OEM-Recheneinrichtung (5) nach Empfangen eines Übermittlungsauftrags über einen kryptografisch abgesicherten Übertragungskanal an eine zentrale Dienstleister- Recheneinrichtung (6) übertragen wird. (Figur 1)

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz
3)

Mercedes-Benz Group AG

Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung

Die Erfindung betrifft ein Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung nach der im Oberbegriff von Anspruch 1 näher definierten Art.

Mit zunehmender Digitalisierung nimmt auch die Anzahl von Recheneinheiten und Steuergeräten in Fahrzeugen zu. Solche Geräte erlauben die Bereitstellung von Sicherheits- und Komfortfunktionen.

In einigen Regionen dieser Welt werden automatische Mautsysteme verwendet. So kann ein Mautsteuergerät in ein Fahrzeug integriert werden, welches drahtlos eine charakteristische ID an einen Betreiber einer Mautstrecke übermittelt, wenn das Fahrzeug eine mautpflichtige Strecke betritt und verlässt. Der Mautbetreiber kann somit nachvollziehen zu welchen Zeiten welches Mautsteuergerät und damit welcher Nutzer welchen mautpflichtigen Streckenabschnitt genutzt hat. Durch eine Zuordnung der charakteristischen ID des Mautsteuergeräts zu einem Nutzerkonto kann dann eine Abrechnung der Maut erfolgen. Hierzu muss die ID zuerst mit dem Nutzerkonto verknüpft werden, was mit einem manuellen Aufwand seitens des Nutzers verbunden ist.

Aus der US 2020/0327218 A1 sind ein Verfahren zum Authentifizieren eines Fahrzeugs, eine Authentifizierungseinheit, eine Serviceeinheit und eine fahrzeugexterne zentrale Computereinheit bekannt. Das Verfahren sieht für eine sichere und komfortable Authentifizierung des Fahrzeugs gegenüber der Serviceeinheit vor, dass ein Initialwert von der Serviceeinheit an die Authentifizierungseinheit im Fahrzeug gesendet wird, woraufhin die Authentifizierungseinheit einen Fahrzeugprüfwert generiert und diesen zusammen mit dem Initialwert an die zentrale Computereinheit übermittelt. Die zentrale Computereinheit generiert wiederum einen weiteren Fahrzeugprüfwert und vergleicht diesen mit dem empfangenen Fahrzeugprüfwert. Stimmen beide Werte überein so wird

das Fahrzeug bzw. der Nutzer des Fahrzeugs authentifiziert. Während der Erzeugung des weiteren Fahrzeugprüfwerts verarbeitet die zentrale Computereinheit eine Tabelle mit charakteristischen Werten. In dieser Tabelle sind charakteristische Werte von Fahrzeugkomponenten gespeichert. Zur Erzeugung der Tabelle mit den charakteristischen Werten liest die Authentifizierungseinheit aus der entsprechenden Fahrzeugkomponente den jeweiligen charakteristischen Wert aus und überträgt diesen zum Speichern an die zentrale Computereinheit. Das in der Druckschrift offenbarte Verfahren ist jedoch aufgrund der häufigen Berechnung von Prüfwerten rechenaufwändig.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde ein verbessertes Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung anzugeben, mit dessen Hilfe ein Nutzerkomfort zum Hinterlegen des Identifikators auf der zentralen Recheneinrichtung gesteigert wird und dabei unter Einhaltung der Cybersicherheit ein Rechenaufwand minimiert wird.

Erfindungsgemäß wird diese Aufgabe durch ein Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung mit den Merkmalen des Anspruchs 1 gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen ergeben sich aus den hiervon abhängigen Ansprüchen.

Ein gattungsgemäßes Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung, wobei ein erster Identifikator aus einem Steuergerät eines Fahrzeugs ausgelesen und an eine fahrzeuginterne Recheneinheit zum persistenten Speichern übertragen wird und der erste Identifikator von der fahrzeuginternen Recheneinheit an eine zentrale OEM-Recheneinrichtung übertragen wird, wird erfindungsgemäß dadurch weitergebildet, dass der erste Identifikator an die zentrale OEM-Recheneinrichtung über einen kryptografisch abgesicherten Übertragungskanal übertragen wird und von der zentralen OEM-Recheneinrichtung nach Empfangen eines Übermittlungsauftrags über einen kryptografisch abgesicherten Übertragungskanal an eine zentrale Dienstleister-Recheneinrichtung übertragen wird.

Mit Hilfe des erfindungsgemäßen Verfahrens ist ein besonders komfortables und sicheres Hinterlegen des ersten Identifikators auf der zentralen Dienstleister-

Recheneinrichtung unter Wahrung der Cybersicherheit möglich. Bei dem ersten Identifikator handelt es sich um eine kodierte Information. Diese Information kann beliebig kodiert sein, beispielsweise in einem beliebigen Dateiformat. Bei dem Steuergerät kann es sich um ein beliebiges Steuergerät wie ein Mautsteuergerät oder dergleichen handeln. Der erste Identifikator kann beispielsweise eine Identifikationsnummer, Seriennummer, ID oder dergleichen des Steuergeräts umfassen oder dadurch ausgebildet sein. Weitere Beispiele für den ersten Identifikator können sein: eine Fahrzeugidentnummer, ein Kennzeichen, ein Land oder Bundesstaat in dem das Kennzeichen registriert ist, ein Fahrzeugtyp, Fahrzeugabmessungen, ein zulässiges Fahrzeuggewicht, Bezahlinformationen wie die Kennung eines PayPal-, WeChat-, Alipay-, Applepay- oder Googlepay-Accounts, eine Kreditkarteninformation wie eine Kreditkartennummer oder eine Prüfziffer, eine IBAN oder dergleichen. Zum Übertragen von Informationen zwischen der fahrzeuginternen Recheneinheit und der zentralen OEM-Recheneinrichtung besteht typischerweise eine Kommunikationsverbindung. Über diese Kommunikationsverbindung werden Computerdaten kryptografisch abgesichert übertragen. Hierdurch kann der Fahrzeughersteller Diagnosedaten aus dem Fahrzeug empfangen oder Softwareupdates auf die fahrzeuginterne Recheneinheit aufspielen. Dieser Übertragungskanal ist ohnehin vorhanden und wird erfindungsgemäß auch dazu genutzt, um den ersten Identifikator ohne einen zusätzlichen Transformationsaufwand zum kryptografischen Absichern abgesichert an die zentrale OEM-Recheneinrichtung zu übermitteln. Hierzu kann der erste Identifikator beispielsweise auch in einen Fahrzeug-Datensatz, beispielsweise einen Diagnosedatensatz integriert oder an diesen angehängt werden. Der erste Identifikator kann jedoch auch einen separaten Datensatz ausbilden.

Ebenfalls besteht ein kryptografisch abgesicherter Übertragungskanal zwischen der zentralen OEM-Recheneinrichtung und der zentralen Dienstleister-Recheneinrichtung. Hierbei handelt es sich beispielsweise um eine Hypertext Transfer Protocol Secure Verbindung, also eine auf dem HTTPS Internet Kommunikationsprotokoll basierende Kommunikationsverbindung. Somit sind keine separaten Verschlüsselungsmechanismen erforderlich, um eine ausreichende Cybersicherheit zu gewährleisten.

Mit Hilfe des erfindungsgemäßen Verfahrens lässt sich beispielsweise die Geräte-ID eines Mautsteuergeräts komfortabel bei einem Mautsystembetreiber hinterlegen. Somit entsteht kein manueller Aufwand für einen Nutzer des Fahrzeugs, um die Geräte-ID des

Mautsteuergeräts zu bestimmen und diese manuell mit seinem Nutzerkonto bei dem Mautsystembetreiber zu verknüpfen.

Bei der zentralen OEM-Recheneinrichtung handelt es sich beispielsweise um eine Cloudserver, auch als Backend bezeichnet, welcher von einem Fahrzeughersteller betrieben wird. Bei der zentralen Dienstleister-Recheneinrichtung handelt es sich dann beispielsweise um einen Cloudserver bzw. Backend des Mautsystembetreibers. Der erste Identifikator wird von der zentralen OEM-Recheneinrichtung an die zentrale Dienstleister-Recheneinrichtung übertragen, nachdem ein Übermittlungsauftrag an die zentrale OEM-Recheneinrichtung übermittelt wurde. Dieser Übermittlungsauftrag kann beispielsweise vom Nutzer des Fahrzeugs manuell angestoßen werden. Hierzu kann der Nutzer eine beliebige mit der fahrzeuginternen Recheneinheit gekoppelte Bedieneinrichtung, beispielsweise eine fest im Fahrzeug installierte Mensch-Maschine-Schnittstelle, wie ein berührungsempfindliches Display, oder auch ein mit dem Fahrzeug gekoppeltes mobiles Endgerät nutzen.

Eine vorteilhafte Weiterbildung des Verfahrens sieht vor, dass der erste Identifikator aus dem Steuergerät im Zuge der Herstellung des Fahrzeugs ausgelesen und in der fahrzeuginternen Recheneinheit gespeichert wird. Hierdurch kann der Aufwand für den Nutzer des Fahrzeugs zum Hinterlegen des ersten Identifikators auf der zentralen Dienstleister-Recheneinrichtung noch weiter gesenkt werden. So wurde der erste Identifikator bei Ausliefern des Fahrzeugs bereits in der fahrzeuginternen Recheneinheit gespeichert. Dabei ist es auch möglich, dass der erste Identifikator bereits vor Ausliefern des Fahrzeugs an den Kunden, also den Nutzer, von der fahrzeuginternen Recheneinheit bereits an die zentrale OEM-Recheneinrichtung übertragen wird.

Entsprechend einer weiteren vorteilhaften Ausgestaltung des Verfahrens wird der erste Identifikator aus dem Steuergerät während der Nutzungsdauer des Fahrzeugs ausgelesen und in der fahrzeuginternen Recheneinheit gespeichert. Das Auslesen des ersten Identifikators aus dem Steuergerät lässt sich also auch manuell, beispielsweise durch einen Nutzer während dem Betrieb oder auch durch einen Händler oder einen Mechaniker während eines Wartungsintervalls in einer Werkstatt anstoßen. Möchte der Nutzer sein Mautsteuergerät beim Mautsystembetreiber registrieren und entsprechend mit seinem Nutzerkonto verbinden, so kann auch erst dann das Übertragen des ersten

Identifikators stattfinden, wenn der Nutzer dies wünscht. Hierdurch wird ein frühzeitiges Übertragen des ersten Identifikators verhindert, was die Cybersicherheit noch weiter verbessert, da somit der erste Identifikator für einen kürzeren Zeitraum an mehreren Speicherorten gespeichert ist und somit auch ein geringeres Angriffspotenzial vorliegt.

Das Übertragen des ersten Identifikators an die zentrale OEM-Recheneinrichtung kann manuell veranlasst werden, beispielsweise durch Eingabe einer Bedienhandlung über eine Bedieneinrichtung des Fahrzeugs, oder auch automatisch erfolgen, beispielsweise beim Anschließen des Steuergeräts an ein Bordnetz des Fahrzeugs, wodurch dann zuerst die fahrzeuginterne Recheneinheit den ersten Identifikator automatisch aus dem Steuergerät ausliest.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens sieht ferner vor, dass der erste Identifikator auf einer Anzeigevorrichtung im Fahrzeug dargestellt wird und erst nach Bestätigung durch Eingabe einer Bedienhandlung durch einen Nutzer über eine mit der fahrzeuginternen Recheneinheit zusammenwirkende Bedieneinrichtung:

- der erste Identifikator an die zentrale OEM-Recheneinrichtung übertragen wird;
und/oder
- dermittlungsauftrag an die zentralen OEM-Recheneinrichtung übertragen wird.

Dies ermöglicht es dem Nutzer des Fahrzeugs den ersten Identifikator zu überprüfen, bevor der erste Identifikator an die zentrale OEM-Recheneinrichtung bzw. die zentrale Dienstleister-Recheneinrichtung übermittelt wird. Dabei kann die Anzeigevorrichtung als berührungsempfindliches Display ausgeführt sein und somit die Bedieneinrichtung ausbilden.

Dabei kann es erforderlich sein, dass der Nutzer zweimal eine Bestätigung zum Übertragen des ersten Identifikators eingeben muss. So kann einmal eine Bestätigung notwendig sein, um den ersten Identifikator aus dem Fahrzeug an die zentralen OEM-Recheneinrichtung zu übertragen, und eine zweite Bestätigung erforderlich sein, um den ersten Identifikator von der zentralen OEM-Recheneinrichtung an die zentrale Dienstleister-Recheneinrichtung zu übertragen.

Entsprechend einer weiteren vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens werden gemeinsam mit dem ersten Identifikator Nutzdaten von der zentralen OEM-Recheneinrichtung an die zentrale Dienstleister-Recheneinrichtung übertragen. Bei den Nutzdaten kann es sich beispielsweise um persönliche Daten des Nutzers handeln wie Name, Adresse, Bankinformationen und dergleichen. Die entsprechenden Nutzdaten können bereits in der fahrzeuginternen Recheneinheit und/oder der zentralen OEM-Recheneinrichtung vorliegen. So kann der Nutzer des Fahrzeugs über ein entsprechendes Nutzerprofil beim Hersteller des Fahrzeugs verfügen. Hierdurch kann der Komfort für den Nutzer des Fahrzeugs noch weiter gesteigert werden, indem die persönlichen Daten des Nutzers automatisch vom Fahrzeughersteller an den Mautsystembetreiber übermittelt werden. Somit entfällt das Erfordernis für den Nutzer, dass er seine persönlichen Daten zum Verknüpfen der Geräte-ID seines Mautsteuergeräts mit seinem Nutzerkonto beim Mautsystembetreiber erneut eingeben muss.

Dem Nutzer wird zudem volle Kontrolle über seine Daten gegeben. Sollte der Nutzer dies wünschen, beispielsweise über eine entsprechende Einstellung in einem Nutzerprofil, so kann jedes Mal bevor die Nutzdaten von der zentralen OEM-Recheneinrichtung ausgeleitet werden, also auch entsprechend zum Übertragen an die zentrale Dienstleister-Recheneinrichtung, der Nutzer gefragt werden, ob er der Datenübertragung zustimmt. Der Nutzer kann dies durch Eingabe einer entsprechenden Bedienung bestätigen. So wird verhindert, dass unerwünschterweise die persönlichen durch die Nutzdaten beschriebenen Informationen des Nutzers weitergegeben werden.

Eine weitere vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens sieht ferner vor, dass die fahrzeuginterne Recheneinheit den ersten Identifikator und einen Zeitstempel in eine Hashfunktion zur Erzeugung eines Hashwerts einliest und der Hashwert zusammen mit dem Zeitstempel an die zentrale OEM-Recheneinrichtung übertragen wird, woraufhin die zentrale OEM-Recheneinrichtung unter Verwenden derselben Hashfunktion aus dem Hashwert und dem Zeitstempel den ersten Identifikator erzeugt. Hierdurch lässt sich die Cybersicherheit des erfindungsgemäßen Verfahrens weiter steigern. Bei dem Zeitstempel kann es sich beispielsweise um einen Zeitpunkt oder ein Zeitfenster wie ± 10 Sekunden, ± 5 Minuten oder dergleichen um den Zeitpunkt handeln. Bei dem Zeitpunkt selbst kann es sich um den Zeitpunkt handeln, an dem der

Identifikator aus dem Steuergerät des Fahrzeugs ausgelesen wird, an dem der Identifikator in der fahrzeuginternen Recheneinheit gespeichert wird oder an dem der Identifikator an die zentrale OEM-Recheneinrichtung übertragen wird. Handelt es sich bei dem Zeitpunkt um den Zeitpunkt an dem der erste Identifikator an die zentrale OEM-Recheneinrichtung übertragen wird, so kann der Zeitstempel implizit an die zentrale OEM-Recheneinrichtung durch das Übermitteln des ersten Identifikators übertragen werden. Mit anderen Worten kann die zentrale OEM-Recheneinrichtung den Zeitstempel durch Abgleichen des Zeitpunkts an dem der erste Identifikator empfangen wird mit der Uhrzeit auch selbst ermitteln. Das zusätzliche Konkatenieren des ersten Identifikators mit einem Zeitstempel erlaubt die zusätzliche kryptografische Absicherung durch die Verwendung eines sogenannten Time-Based One-Time Password Algorithmus.

Entsprechend einer weiteren vorteilhaften Ausgestaltung des Verfahrens wird zusätzlich wenigstens ein zweiter Identifikator aus dem Steuergerät ausgelesen und über die fahrzeuginterne Recheneinheit an die zentrale OEM-Recheneinrichtung übertragen. Bei dem zweiten Identifikator kann es sich um einen gleichartig zum ersten Identifikator ausgeführtes Merkmal handeln. Das Steuergerät kann auch ein vertrauenswürdiges Plattformmodul, auch als Trusted Platform Module (TPM) aufweisen, aus dem der zweite Identifikator ausgelesen wird. So kann es sich bei dem zweiten Identifikator auch um einen eindeutigen kryptografischen Schlüssel zur Identifizierung des Steuergeräts handeln. Generell kann der zweite Identifikator aus einer geeigneten hierzu eingerichteten Hardware- und/oder Softwarekomponente des Steuergeräts ausgelesen werden.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens sieht ferner vor, dass der zweite Identifikator von der zentralen OEM-Recheneinrichtung an die zentrale Dienstleister-Recheneinrichtung übertragen wird und die zentrale Dienstleister-Recheneinrichtung den zweiten Identifikator als Authentifizierungsmerkmal eines Nutzers verwendet. Hierdurch lässt sich die Cybersicherheit des erfindungsgemäßen Verfahrens noch weiter verbessern und weitere Funktionalitäten zur Steigerung des Komforts des Nutzers bereitstellen. So ist beispielsweise mit dem zweiten Identifikator eine Authentifizierung möglich und kann beispielsweise zum Authentifizieren eines Bezahlaccounts des Nutzers verwendet werden. So kann unter Authentifizierung des zweiten Identifikators

beispielsweise das Durchführen von über ein Kreditkartennetzwerk getätigten Kreditkartenzahlungen erlaubt bzw. bestätigt werden.

Bevorzugt wird der zweite Identifikator dabei für eine Multi-Faktor-Authentifizierung verwendet. So gehen nicht nur der zweite Identifikator sondern beispielsweise auch der erste Identifikator und/oder ein dritter, vierter, oder fünfter Identifikator in einen Authentifizierungsschritt ein. Insbesondere wenn es sich bei den Identifikatoren um zeitlich begrenzt nutzbare kryptografische Schlüssel handelt, wird eine bezüglich der Cybersicherheit besonders sichere Datenübertragung und Authentifizierung ermöglicht.

Weitere vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung ergeben sich auch aus dem Ausführungsbeispiel, welches nachfolgend unter Bezugnahme auf die Figur näher beschrieben wird.

Dabei zeigt Figur 1 eine schematisierte Darstellung eines Übertragungswegs zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung.

In Figur 1 ist ein Fahrzeug 3 dargestellt. Dieses umfasst ein Steuergerät 2, eine damit gekoppelte fahrzeuginterne Recheneinheit 4 und eine damit gekoppelte Kommunikationseinheit 7 zur drahtlosen Datenübertragung. Die Kommunikationseinheit 7 kann beispielsweise per Mobilfunk mit dem Internet verbunden sein. Eine Mobilfunkverbindung kann durch ein Mobilfunkkommunikationsnetzwerk 8 zur Ausbildung eines Kommunikationspfads 9 bereitgestellt werden. Somit ist eine direkte Kommunikation der fahrzeuginternen Recheneinheit 4 über einen ersten Kommunikationspfad 9.1 mit einer zentralen OEM-Recheneinrichtung 5 und über einen zweiten Kommunikationspfad 9.2 mit einer zentralen Dienstleister-Recheneinrichtung 6 möglich.

Zentraler Gedanke eines erfindungsgemäßen Verfahrens ist es, wie auf eine möglichst komfortable und sichere Art und Weise ein erster Identifikator 1, welcher im Steuergerät 2 gespeichert ist, an die zentrale Dienstleister-Recheneinrichtung 6 übermittelt werden kann.

Hierzu wird in einem Verfahrensschritt 100 der erste Identifikator 1 aus dem Steuergerät 2 ausgelesen und an die fahrzeuginterne Recheneinheit 4 übertragen. In einem Verfahrensschritt 101 wird dann der erste Identifikator 1 in der fahrzeuginternen Recheneinheit 4 persistent gespeichert. Hierzu wird insbesondere der erste Identifikator 1 in einem Fahrzeug-Datensatz inkludiert. Der Fahrzeug-Datensatz kann diverse Informationen umfassen, wie das Fahrzeug 3 charakterisierende Informationen, beispielsweise eine Fahrzeugidentnummer, ein Kennzeichen, eine Motorisierung, eine Ausstattung, Fahrzeugdimensionen und dergleichen, Nutzerdaten eines Nutzers des Fahrzeugs, beispielsweise Name, Geburtsdatum, Adresse, Bankdaten und dergleichen, Betriebsdaten des Fahrzeugs 3 wie ein aktueller Tankinhalt, ein aktueller Ladezustand einer Traktionsbatterie, eine aktuelle Fortbewegungsgeschwindigkeit, einen Kilometerstand und dergleichen oder auch sonstige Daten.

Der erste Identifikator 1 wird dann in einem Verfahrensschritt 102 über die Kommunikationseinheit 7 und das Mobilfunkkommunikationsnetzwerk 8, bevorzugt inkludiert in dem Fahrzeug-Datensatz, an die zentrale OEM-Recheneinrichtung 5 übertragen. Hierzu wird ein kryptografisch abgesicherter Kommunikationskanal verwendet, welcher ohnehin vorhanden ist, da das Fahrzeug 3 hierüber den Fahrzeug-Datensatz mit der zentralen OEM-Recheneinrichtung 5 austauscht. Es sind somit keine weiteren kryptografischen Sicherungsmaßnahmen zum sicheren Übertragen des ersten Identifikators 1 aus dem Steuergerät 2 an die zentrale OEM-Recheneinrichtung 5 notwendig. In einem Verfahrensschritt 103 wird dann der erste Identifikator 1 in der zentralen OEM-Recheneinrichtung 5 zumindest temporär gespeichert.

Bei dem ersten Identifikator 1 kann es sich beispielsweise um eine Geräte-ID des Steuergeräts 2 handeln. Es kann sich auch um eine Seriennummer oder eine sonstige charakteristische Bezeichnung handeln. Beispielsweise handelt es sich bei dem Steuergerät 2 um ein Mautsteuergerät. Ein stationäres Mautsystem, welches einen Zugang zu einem mautpflichtigen Streckenabschnitt gewährt, kann bei Annäherung des Fahrzeugs 3 den ersten Identifikator 1 unmittelbar vom Steuergerät 2, beispielsweise per Funk, empfangen und damit eine Abrechnung der Maut ermöglichen. Hierzu muss ein Nutzer des Fahrzeugs 3 jedoch über ein Nutzerkonto beim entsprechenden Mautsystembetreiber verfügen. Der erste Identifikator 1 muss mit dem Nutzerkonto verknüpft werden. Um dies besonders komfortabel durchführen zu können kann vor

einer Annäherung des Fahrzeugs 3 an den entsprechenden mautpflichtigen Streckenabschnitt ein Übermittlungsauftrag vom Nutzer an die zentrale OEM-Recheneinrichtung 5 angestoßen werden. Hierzu kann der Nutzer eine Bedienschnittstelle des Fahrzeugs 3 nutzen. Der Übermittlungsauftrag kann gemeinsam mit einem Befehl zum Übertragen des ersten Identifikators 1 an die zentrale OEM-Recheneinrichtung angestoßen werden. Auch kann der Nutzer zum Anstoßen des Übermittlungsauftrags ein mobiles Endgerät oder einen Desktop-PC nutzen. Die entsprechenden Geräte müssen hierzu lediglich in Kommunikationsverbindung mit der zentralen OEM-Recheneinrichtung stehen. Als Interface kann dabei eine auf einem mobilen Endgerät ausgeführten App oder ein Web-Browser dienen.

In einem Verfahrensschritt 104 wird dann der erste Identifikator 1 nach Empfangen des Übermittlungsauftrags von der zentralen OEM-Recheneinrichtung 5 an die zentrale Dienstleister-Recheneinrichtung 6 übertragen. Auch dies geschieht kryptografisch abgesichert, beispielsweise unter Nutzung des HTTPS Kommunikationsprotokolls.

In einem Verfahrensschritt 105 wird der erste Identifikator 1 in der zentralen Dienstleister-Recheneinrichtung 6 gespeichert.

In einem Verfahrensschritt 106 wird das Konto des Nutzers des Fahrzeugs 3 mit dem ersten Identifikator 1 verknüpft. Zum Verknüpfen des Kontos mit dem ersten Identifikator 1 kann der Nutzer des Fahrzeugs 3 erforderliche Kontoinformationen 10 auch direkt an die zentrale Dienstleister-Recheneinrichtung 6 über den zweiten Kommunikationspfad 9.2 übertragen. Hierbei handelt es sich beispielsweise um eine eindeutige Nutzerkennung und ein Nutzerpasswort. Muss der Nutzer sein Konto neu anlegen, so muss er beispielsweise auch Name, Adresse, Geburtsdatum, Bankabrechnungsinformationen und dergleichen hinterlegen. Diese Kontoinformationen 10 können jedoch auch in der zentralen OEM-Recheneinrichtung 5 vorhanden sein, da auch der Hersteller des Fahrzeugs 3, welcher die zentrale OEM-Recheneinrichtung 5 betreibt, diese Informationen zur Bereitstellung von diversen Funktionalitäten benötigt. Empfängt die zentrale OEM-Recheneinrichtung 5 den Übermittlungsauftrag, so können auch gemeinsam mit dem ersten Identifikator 1 die entsprechenden Kontoinformationen 10 des Nutzers, also Name, Adresse usw., von der zentralen OEM-Recheneinrichtung 5 an die zentrale Dienstleister-Recheneinrichtung 6 übertragen werden. Hierdurch wird der

Komfort für den Nutzer des Fahrzeugs 3 noch weiter verbessert, da der manuelle Aufwand zum Eingeben der entsprechenden Informationen reduziert wird. Das Hinterlegen des ersten Identifikators 1, insbesondere zusammen mit den Kontoinformationen 10, kann besonders bevorzugt durch den Hersteller des Fahrzeugs 3 während der Herstellung des Fahrzeugs 3 erfolgen. Dies kann bereits in einer Fabrik oder auch später bei einem Händler geschehen. Hierzu kann der Nutzer des Fahrzeugs 3 direkt beim Bestellen des Fahrzeugs 3 den Fahrzeughersteller zur Datenübertragung autorisieren. Mit anderen Worten erstellt dann der Fahrzeughersteller ein entsprechendes Nutzerkonto beim Mautsystembetreiber oder ergänzt ein solches Nutzerkonto.

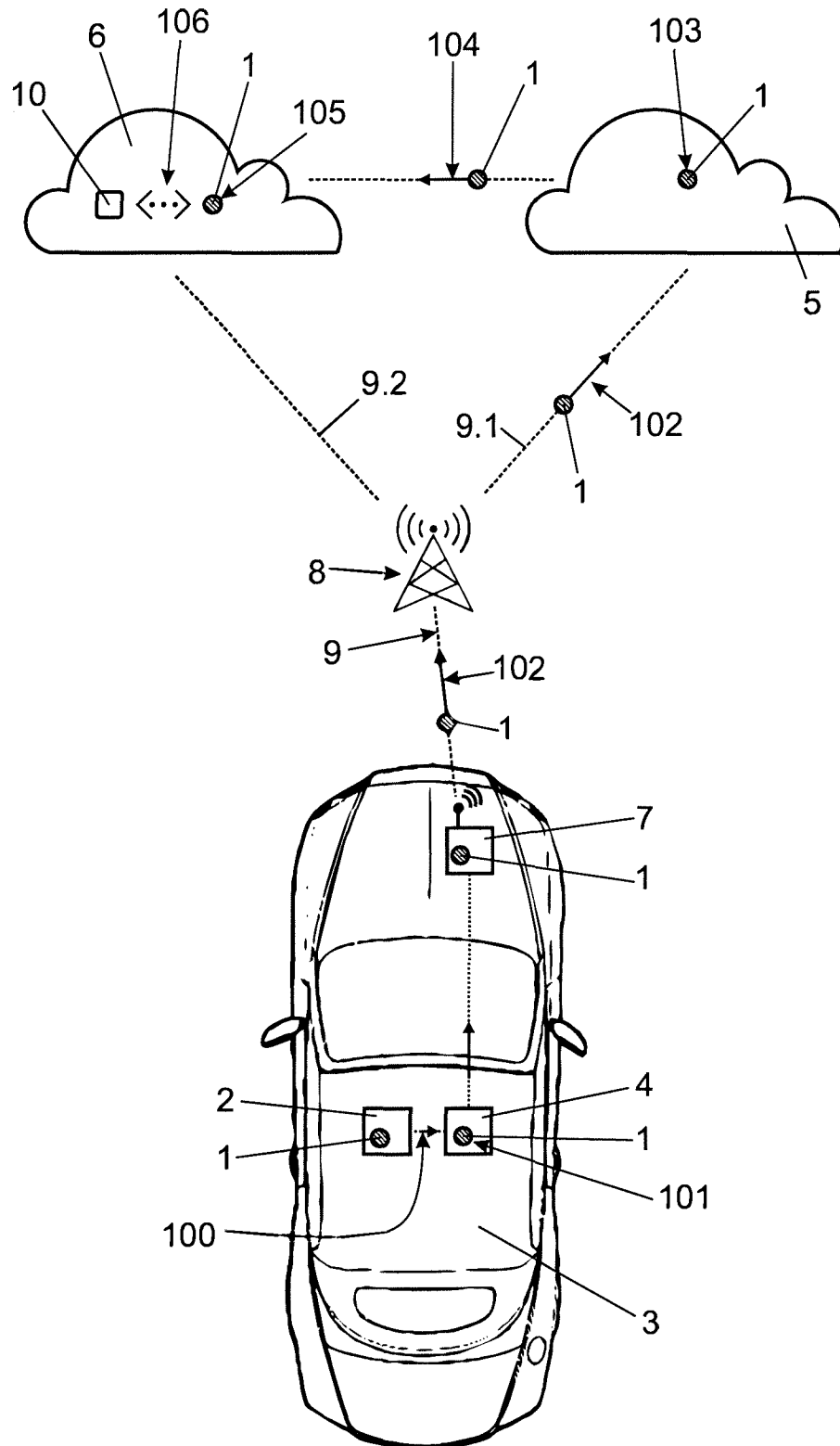
Patentansprüche

1. Verfahren zum Hinterlegen eines Identifikators auf einer zentralen Recheneinrichtung, wobei ein erster Identifikator (1) aus einem Steuergerät (2) eines Fahrzeugs (3) ausgelesen und an eine fahrzeuginterne Recheneinheit (4) zum persistenten Speichern übertragen wird und der erste Identifikator (1) von der fahrzeuginternen Recheneinheit (4) an eine zentrale OEM-Recheneinrichtung (5) übertragen wird, dadurch gekennzeichnet, dass der erste Identifikator (1) an die zentrale OEM-Recheneinrichtung (5) über einen kryptografisch abgesicherten Übertragungskanal übertragen wird und von der zentralen OEM-Recheneinrichtung (5) nach Empfangen eines Übermittlungsauftrags über einen kryptografisch abgesicherten Übertragungskanal an eine zentrale Dienstleister-Recheneinrichtung (6) übertragen wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste Identifikator (1) aus dem Steuergerät (2) im Zuge der Herstellung des Fahrzeugs (3) ausgelesen und in der fahrzeuginternen Recheneinheit (4) gespeichert wird.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste Identifikator (1) aus dem Steuergerät (2) während der Nutzungsdauer des Fahrzeugs (3) ausgelesen und in der fahrzeuginternen Recheneinheit (4) gespeichert wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet, dass
der erste Identifikator (1) auf einer Anzeigevorrichtung im Fahrzeug (3) dargestellt wird und erst nach Bestätigung durch Eingabe einer Bedienhandlung durch einen Nutzer über eine mit der fahrzeuginternen Recheneinheit (4) zusammenwirkenden Bedieneinrichtung:
 - der erste Identifikator (1) an die zentrale OEM-Recheneinrichtung (5) übertragen wird; und/oder
 - der Übermittlungsauftrag an die zentrale OEM-Recheneinrichtung (5) übertragen wird.
5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet, dass
gemeinsam mit dem ersten Identifikator (1) Nutzdaten von der zentralen OEM-Recheneinrichtung (5) an die zentrale Dienstleister-Recheneinrichtung (6) übertragen werden.
6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet, dass
die fahrzeuginterne Recheneinheit (4) den ersten Identifikator (1) und einen Zeitstempel in eine Hashfunktion zur Erzeugung eines Hashwerts einliest und der Hashwert zusammen mit dem Zeitstempel an die zentrale OEM-Recheneinrichtung (5) übertragen wird, woraufhin die zentrale OEM-Recheneinrichtung (5) unter Verwenden derselben Hashfunktion aus dem Hashwert und dem Zeitstempel den ersten Identifikator (1) erzeugt.
7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet, dass
zusätzlich wenigstens ein zweiter Identifikator aus dem Steuergerät (2) ausgelesen und über die fahrzeuginterne Recheneinheit (4) an die zentrale OEM-Recheneinrichtung (5) übertragen wird.
8. Verfahren nach Anspruch 7,
dadurch gekennzeichnet, dass

der zweite Identifikator von der zentralen OEM-Recheneinrichtung (5) an die zentrale Dienstleister-Recheneinrichtung (6) übertragen wird und die zentrale Dienstleister-Recheneinrichtung (6) den zweiten Identifikator als Authentifizierungsmerkmal eines Nutzers verwendet.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass
der zweite Identifikator für eine Multi-Faktor-Authentifizierung verwendet wird.

Fig. 1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2023/069117

A. CLASSIFICATION OF SUBJECT MATTER**H04L 9/40**(2022.01)i; **H04W 4/40**(2018.01)i; **H04W 12/06**(2021.01)i; **H04W 12/61**(2021.01)i; **H04W 12/71**(2021.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013293349 A1 (TEMPL WOLFGANG [DE] ET AL) 07 November 2013 (2013-11-07) paragraphs [0011] - [0012], [0015] - [0020], [0024] - [0029], [0035] - [0040], [0055], [0064], [0066], [0070], [0072] - [0074]; figure 1	1-9
X	US 2012265583 A1 (NAMDAR NADER [AT]) 18 October 2012 (2012-10-18) paragraphs [0018] - [0019], [0022] - [0023], [0029] - [0030], [0033], [0042] - [0051]	1-9
X	DE 202015102311 U1 (OMP TELEMATICS GMBH [DE]) 09 June 2015 (2015-06-09) paragraphs [0002], [0004], [0006] - [0007], [0014] - [0019], [0021] - [0022]	1-9
A	EP 3242205 A1 (TOLL COLLECT GMBH [DE]) 08 November 2017 (2017-11-08) paragraphs [0005] - [0012], [0015], [0042], [0044], [0070]	1-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

“&” document member of the same patent family

Date of the actual completion of the international search

10 October 2023

Date of mailing of the international search report

17 October 2023

Name and mailing address of the ISA/EP

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

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

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

Authorized officer

Betz, Sebastian

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2023/069117

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2013293349	A1	07 November 2013	CN	103329173	A	25 September 2013
				EP	2479731	A1	25 July 2012
				JP	5941066	B2	29 June 2016
				JP	2014515709	A	03 July 2014
				KR	20130114247	A	16 October 2013
				US	2013293349	A1	07 November 2013
				WO	2012097917	A1	26 July 2012
US	2012265583	A1	18 October 2012	CA	2767876	A1	15 October 2012
				DK	2511868	T3	15 July 2013
				EP	2511868	A1	17 October 2012
				SI	2511868	T1	31 July 2013
				US	2012265583	A1	18 October 2012
DE	202015102311	U1	09 June 2015	NONE			
EP	3242205	A1	08 November 2017	NONE			

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES		
INV.	H04L9/40	H04W4/40
		H04W12/06
		H04W12/61
		H04W12/71
ADD.		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
B. RECHERCHIERTE GEBIETE		
Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)		
H04L H04W		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)		
EPO-Internal, WPI Data		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2013/293349 A1 (TEMPL WOLFGANG [DE] ET AL) 7. November 2013 (2013-11-07) Absätze [0011] - [0012], [0015] - [0020], [0024] - [0029], [0035] - [0040], [0055], [0064], [0066], [0070], [0072] - [0074]; Abbildung 1 -----	1-9
X	US 2012/265583 A1 (NAM DAR NADER [AT]) 18. Oktober 2012 (2012-10-18) Absätze [0018] - [0019], [0022] - [0023], [0029] - [0030], [0033], [0042] - [0051] -----	1-9
X	DE 20 2015 102311 U1 (OMP TELEMATICS GMBH [DE]) 9. Juni 2015 (2015-06-09) Absätze [0002], [0004], [0006] - [0007], [0014] - [0019], [0021] - [0022] ----- -/-	1-9
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche		Absendedatum des internationalen Recherchenberichts
10. Oktober 2023		17/10/2023
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Betz, Sebastian

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 3 242 205 A1 (TOLL COLLECT GMBH [DE]) 8. November 2017 (2017-11-08) Absätze [0005] - [0012], [0015], [0042], [0044], [0070] -----	1-9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2023/069117

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2013293349 A1	07-11-2013	CN 103329173 A	25-09-2013
		EP 2479731 A1	25-07-2012
		JP 5941066 B2	29-06-2016
		JP 2014515709 A	03-07-2014
		KR 20130114247 A	16-10-2013
		US 2013293349 A1	07-11-2013
		WO 2012097917 A1	26-07-2012

US 2012265583 A1	18-10-2012	CA 2767876 A1	15-10-2012
		DK 2511868 T3	15-07-2013
		EP 2511868 A1	17-10-2012
		SI 2511868 T1	31-07-2013
		US 2012265583 A1	18-10-2012

DE 202015102311 U1	09-06-2015	KEINE	

EP 3242205 A1	08-11-2017	KEINE	
