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

(11) **EP 2 490 183 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
22.08.2012 Patentblatt 2012/34

(51) Int Cl.:
G07B 15/06 *(2011.01)*

(21) Anmeldenummer: **11450023.4**

(22) Anmeldetag: **16.02.2011**

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

(71) Anmelder: **Kapsch TrafficCom AG**
1120 Wien (AT)

(72) Erfinder: **Nagy, Oliver**
1190 Wien (AT)

(74) Vertreter: **Weiser, Andreas et al**
Patentanwalt
Kopfgasse 7
1130 Wien (AT)

(54) **Fahrzeuggerät, ad-hoc-Netzwerk und Verfahren für ein Strassenmautsystem**

(57) Fahrzeuggerät, Netzwerk und Verfahren für ein Straßenmautsystem, mit einem Satellitennavigationsempfänger (5) zur fortlaufenden Erzeugung von Ortsdaten (p_i) für eine Verarbeitungs- und Sendeempfangseinheit (7, 8) des Fahrzeuggeräts (2) und einem gesonderten Trusted-Element-Prozessor (10) zur Protokollierung (s) eines Zeitabschnitts der erzeugten Ortsdaten (p_i) und zur kryptographischen Signierung (s*) desselben, wobei der Trusted-Element-Prozessor (10) die genannte Protokollierung bei Detektion einer vorgegebenen Zeit (T) oder eines vorgegebenen Orts (P) des Fahrzeuggeräts (2) startet und für einen vorgegebenen Zeitabschnitt durchführt.

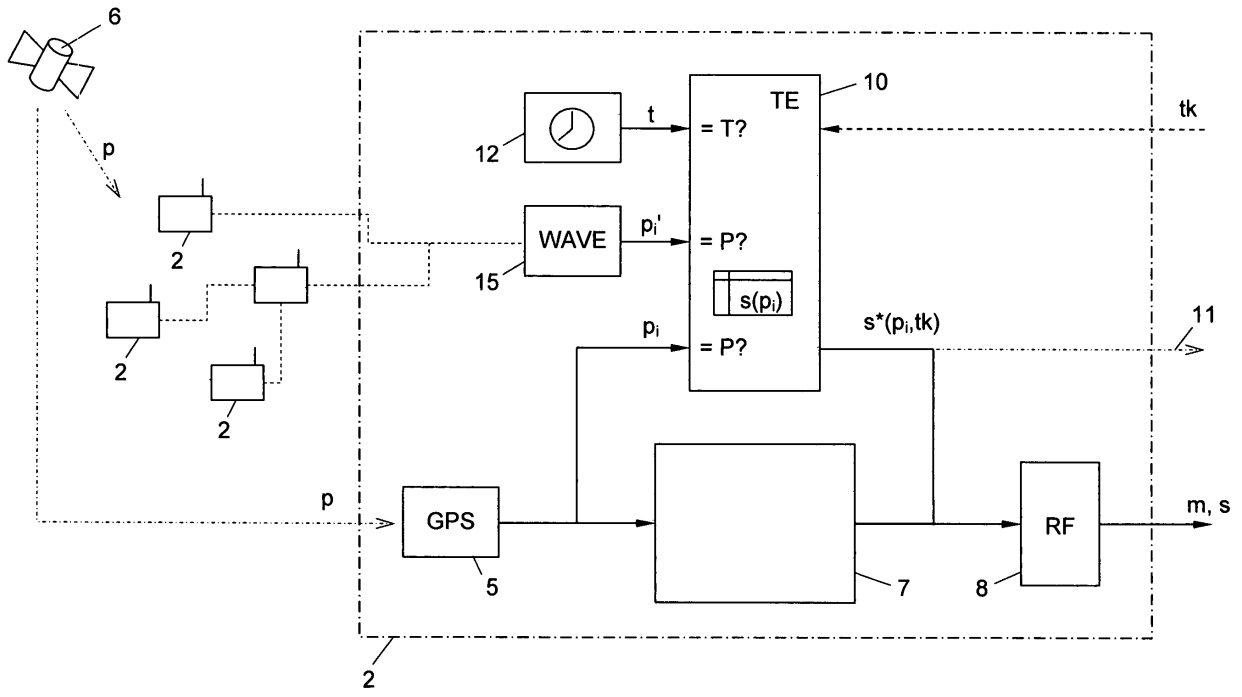

Fig. 2

EP 2 490 183 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Fahrzeuggerät für ein Straßenmautsystem, auch "Onboard-Unit" bzw. OBU genannt, mit einem Satellitennavigationsempfänger zur fortlaufenden Erzeugung von Ortsdaten für eine Verarbeitungs- und Sendeempfangseinheit des Fahrzeuggeräts und einem gesonderten Trusted-Element-Prozessor zur Protokollierung eines Zeitabschnitts der erzeugten Ortsdaten und zur kryptographischen Signierung desselben. Die Erfindung betrifft ferner ein ad-hoc-Netzwerk aus zumindest zwei solchen Fahrzeuggeräten sowie ein Verfahren zur Protokollierung von Ortsdaten eines ortsaufzeichnenden Fahrzeuggeräts eines Straßenmautsystems mit mehreren Fahrzeuggeräten, die drahtlos Ortsdaten austauschen können.

[0002] Zur Überwachung und Kontrolle der Funktionsfähigkeit von interoperablen Straßenmautsystemen, wie dem neuen European Electronic Toll Service (EETS) werden "Secure Monitoring"-Konzepte eingesetzt, die auf einer Protokollierung und abschnittsweisen Signierung ("Real-Time Freezing") der Ortsaufzeichnungen der Fahrzeuggeräte des Straßenmautsystems beruhen. Zur Signierung werden Trusted-Element-Prozessoren verwendet, die eine kryptographische Signatur ("Trusted Element Certificate") des Kontrolleurs, z.B. eines Straßenerhalters, einer Behörde usw. ("Certificate Issuer"), enthalten und daher dessen Vertrauen genießen. Details des Secure Monitoring- bzw. Secure Freezing-Konzepts sind beispielsweise in den Publikationen "Security aspects of the 1,11 EETS", Expert Group 12, Final report V1.0, 5. April 2007; "Electronic fee collection - Application interface definition for autonomous systems - Part 1: Changing", ISO Technical Specification 17575-1, 15. Juni 2010; und "An Example of a view on EETS trust and privacy in GNSS based toll systems", Vis J, Report Ministry of Transport, Public Works and Water Management of The Netherlands, 15. Dezember 2009, enthalten.

[0003] Bei den bekannten Systemen werden alle im Fahrzeuggerät anfallenden Ortsdaten protokolliert und fortlaufend abschnittsweise signiert ("freezed"); anschließend werden mit einem externen Kontrollgerät die signierten Zeitabschnitte zu Kontrollzwecken ausgelesen. Dies bedeutet einen hohen Datenanfall und erfordert einerseits einen entsprechend großen Speicherplatz für die Aufbewahrung der signierten Daten und andererseits gesonderte Kontrollgeräte zu deren Auslesung.

[0004] Die Erfindung setzt sich zum Ziel, die Nachteile des Standes der Technik zu überwinden und eine verbesserte Secure-Monitoring-Lösung für interoperable Straßenmautsysteme zu schaffen. Dieses Ziel wird in einem ersten Aspekt der Erfindung mit einem Fahrzeuggerät der einleitend genannten Art erreicht, das sich dadurch auszeichnet, dass der Trusted-Element-Prozessor dafür ausgebildet ist, die genannte Protokollierung bei Detektion einer vorgegebenen Zeit oder eines vorgegebenen Orts des Fahrzeuggeräts zu starten und für einen vorgegebenen Zeitabschnitt durchzuführen.

[0005] Auf diese Weise wird das Fahrzeuggerät selbst zu seiner eigenen Überwachung eingesetzt: Der in der genannten Weise programmierte Trusted-Element-Prozessor wirkt ähnlich einem Computer-Virus, das zu einer vorgegebenen Zeit oder an einem vorgegebenen Ort für eine begrenzte Zeit Ortsdaten im Fahrzeuggerät sammelt und für Kontrollzwecke bereitstellt. Die genannte Funktionalität des Trusted-Element-Prozessors "schläft" bis zu ihrem Einsatz und führt dann eine einzelne Abschnittsprotokollierung durch. Es erübrigt sich damit, sämtliche Ortsdaten fortlaufend zu protokollieren, zu signieren und aufzubewahren ("einzufrieren"), und es erübrigt sich auch ein gesondertes Kontrollgerät, um den Monitoring-Vorgang auszulösen.

[0006] Es versteht sich, dass der vorgegebene Ort, welcher detektiert wird, nicht notwendigerweise punktförmig sein muss, sondern auch ausgedehnt sein kann, z.B. ein Distrikt, eine bestimmte Straße usw. Gemäß einer ersten Variante der Erfindung detektiert der Trusted-Element-Prozessor den vorgegebenen Ort in den eigenen Ortsdaten seines Fahrzeuggeräts, was den Aufwand gering hält.

[0007] Eine besonders vorteilhafte Ausführungsform der Erfindung zeichnet sich dadurch aus, dass der Trusted-Element-Prozessor den vorgegebenen Ort in fremden Ortsdaten detektiert, die er über ein Drahtlosnetzwerk von benachbarten Fahrzeuggeräten empfängt. Dies stellt einen qualitativen Sprung in der Sicherheit der Überwachung dar: Die Ortsdaten anderer Fahrzeuggeräte sind unabhängig von allfälligen Manipulationen oder Fehlfunktionen des kontrollierten Fahrzeuggeräts; die Verwendung fremder Ortsdaten als Auslösekriterium für das Secure Freezing der eigenen Ortsdaten ermöglicht somit eine hochsichere Kontrolle der Funktionsfähigkeit eines Fahrzeuggeräts für den Kontrolleur bzw. Certificate Issuer. Die genannten benachbarten Fahrzeuggeräte brauchen nicht notwendigerweise von Fahrzeugen mitgeführt werden; sie können auch infrastrukturgestützt ortsfest sein.

[0008] Bevorzugt ist das Drahtlosnetzwerk ein ad-hoc-Netzwerk, insbesondere ein Vehicular-ad-hoc-Network (VANET), besonders bevorzugt nach dem WAVE- (wireless access in a vehicle environment) oder WLAN- (wireless local area network) Standard. Solche Netzwerke können spontan zwischen einer Gruppe benachbarter, sich in gegenseitiger Sendeempfangsreichweite befindlicher Fahrzeuggeräte ausgebildet werden.

[0009] Besonders günstig ist es, wenn der Trusted-Element-Prozessor die fremden Ortsdaten mehrerer benachbarter Fahrzeuggeräte empfängt und miteinander abgleicht, um in den abgeglichenen fremden Ortsdaten den vorgegebenen Ort zu detektieren.

[0010] Um Vertraulichkeitsanforderungen zu erfüllen, kann der Trusted-Element-Prozessor gemäß einem weiteren bevorzugten Merkmal die fremden Ortsdaten der benachbarten Fahrzeuggeräte anonym abfragen, z.B. unter einer zufällig gewählten (anonymen) Netzwerk-Absenderkennunq, einer - ohne Zusatzinformationen nicht

weiter zuordenbaren - MAC-Adresse im ad-hoc-Netzwerk, usw.

[0011] Zur Erhöhung der Kontrollsicherheit kann der Trusted-Element-Prozessor die fremden Ortsdaten unter Austausch eines Schlüssels mit zeitlich und/oder örtlich begrenzter Gültigkeit abfragen und nur jene fremden Ortsdaten, die unter einem gültigen Schlüssel empfangen werden, berücksichtigen. Dadurch kann die Aktualität der als Auslösekriterium verwendeten Ortsdaten und/oder ihr Nachbarschaftsbereich verifiziert werden; in einem hochmobilen Umfeld wie einem VANET kann damit die Genauigkeit der Verortung des protokollierten Fahrzeuggeräts erhöht werden.

[0012] In einer weiteren Variante der Erfindung kann der Trusted-Element-Prozessor den signierten Zeitabschnitt mittels der Sendeempfangseinheit des Fahrzeuggeräts an eine Zentrale des Straßenmautsystems absenden. Alternativ kann der Trusted-Element-Prozessor den signierten Zeitabschnitt über eine Schnittstelle des Fahrzeuggeräts zur Abfrage bereitstellen.

[0013] In einem zweiten Aspekt schafft die Erfindung auch ein ad-hoc-Netzwerk aus zumindest zwei Fahrzeuggeräten von jener Art, bei der als Auslösekriterium für das Secure Freezing Daten benachbarter Fahrzeuggeräte verwendet werden, gemäß den Merkmalen des Anspruchs 10.

[0014] In einem dritten Aspekt schafft die Erfindung ein Verfahren zur Protokollierung von Ortsdaten eines ortsaufzeichnenden Fahrzeuggeräts eines Straßenmautsystems mit mehreren Fahrzeuggeräten, die drahtlos Ortsdaten austauschen können, umfassend, in einem ersten Fahrzeuggerät:

Empfangen von Ortsdaten eines zweiten Fahrzeuggeräts,
Detektieren eines vorgegebenen Orts in den empfangenen Ortsdaten des zweiten Fahrzeuggeräts,
Starten der Protokollierung eines Zeitabschnitts der Ortsdaten des ersten Fahrzeuggeräts, und
Signieren des protokollierten Zeitabschnitts mit einer kryptographischen Signatur.

[0015] Bevorzugt erfolgt das Detektieren, Protokollieren und Signieren in einem Trusted-Element-Prozessor des ersten Fahrzeuggeräts.

[0016] Wenn die Protokollierung der eigenen Ortsdaten zeitgesteuert ausgelöst wird, können die Ortsdaten der anderen Fahrzeuggeräte als zusätzliche Validierungsdaten verwendet werden, indem sie beim Secure Freezing der eigenen Ortsdaten "miteingefroren" werden. Demgemäß schafft die Erfindung in einer alternativen Ausführungsform auch ein Verfahren zur Protokollierung von Ortsdaten eines ortsaufzeichnenden Fahrzeuggeräts eines Straßenmautsystems mit mehreren Fahrzeuggeräten, die drahtlos Ortsdaten austauschen können, umfassend, in einem ersten Fahrzeuggerät:

Detektieren einer vorgegebenen Zeit,
Starten der Protokollierung eines Zeitabschnitts der Ortsdaten des ersten Fahrzeuggeräts und Empfangen von Ortsdaten eines zweiten Fahrzeuggeräts, und
Signieren des protokollierten Zeitabschnitts und der empfangenen Ortsdaten mit einer kryptographischen Signatur.

[0017] Hinsichtlich der Vorteile des ad-hoc-Netzwerks und der Verfahren der Erfindung wird auf die obigen Ausführungen zum erfindungsgemäßen Fahrzeuggerät verwiesen.

[0018] Die Erfindung wird nachstehend anhand eines in den beigeschlossenen Zeichnungen dargestellten Ausführungsbeispiels näher erläutert. In den Zeichnungen zeigt

Fig. 1 ein Straßenmautsystem mit Fahrzeuggeräten in einem erfindungsgemäßen ad-hoc-Netzwerk unter Verwendung des Verfahrens der Erfindung in Blockschaltbildform; und
Fig. 2 eines der Fahrzeuggeräte von Fig. 1 in Blockschaltbildform im Detail.

[0019] Fig. 1 zeigt ein interoperables Straßenmautsystem 1, das sich aus einer Vielzahl von Fahrzeuggeräten (onboard units, OBUs, O_1 - O_6) 2, einer Mehrzahl verschiedener Mautbetreiberzentralen (Toll Charger, TC_1, TC_2) 3 und einer Mehrzahl verschiedener Verrechnungszentralen (Certificate Issuer, CI_1 - CI_3) 4 zusammensetzt. Die Fahrzeuggeräte 2 bestimmen mittels Satellitennavigationsempfängern 5 (Fig. 2) fortlaufend ihren Ort p in einem globalen Satellitennavigationssystem (global navigation satellite system, GNSS) 6 und erzeugen daraus einen fortlaufenden Strom (track) von Ortsdaten (position fixes) p_i.

[0020] Mit Hilfe einer Verarbeitungs- und Sendeempfangseinheit 7, 8 (Fig. 2) sendet jedes Fahrzeuggerät 2 seine Ortsdaten p_i entweder in "roher Form" oder - bevorzugt - verarbeitet zu Mautdaten m über eine Betreiberzentrale 3 an eine Verrechnungszentrale 4. Der Verarbeitungsteil 7 der Einheit 7, 8 ist beispielsweise ein Mikroprozessor, und die Sendeempfangseinheit 8 der Einheit 7, 8 ein DSRC- (dedicated short range communication), WAVE-, WLAN- oder bevorzugt PLMN- (public land mobile network) Sendeempfänger.

[0021] Die Mautdaten m sind bevorzugt akkumulierte und ortsanonymisierte Mauttransaktions-Datensätze, welche beispielsweise eine Anzahl gefahrener Kilometer, ein befahrenes Streckensegment eines Straßennetzes, die Aufenthaltszeit in einem Mautgebiet (z.B. Citymaut) usw. angeben. Zur Generierung der Mautdaten m aus den Ortsdaten p_i können letztere beispielsweise mit vorgespeicherten Mautkarten abgeglichen werden ("map matching"). Zu diesem Zweck können sich die Fahrzeuggeräte 2 beispielsweise auch eines externen Kartenabgleichs-Servers (map matching proxy) 9 bedienen, an den map matching-Aufgaben unter anonymisier-

ten Taskkennungen ausgelagert werden, um die Vertraulichkeit der Ortsdaten p_i gegenüber den Betreiber- und Abrechnungszentralen 3, 4 zu wahren, wie dem Fachmann bekannt. Die Mautdaten m können vom proxy 9 auch direkt an die Betreiber- oder Verrechnungszentralen 3, 4 gesandt werden.

[0022] Zur Überwachung und Kontrolle der Funktionen der Fahrzeuggeräte 2 und auch Betreiberzentralen 3 wird gemäß Fig. 2 jedes Fahrzeuggerät 2 mit einem Trusted-Element-Prozessor 10 ausgestattet, der eine kryptographische Signatur (trusted key) tk enthält. Die Signatur tk wird z.B. von einem Contract Issuer CI, Inhaber einer der Verrechnungszentralen 4, ausgestellt und ist für diesen vertrauenswürdig. Unter einem "Trusted-Element-Prozessor" 10 wird in der vorliegenden Beschreibung ein mit einer kryptographischen Signatur ausgestattetes und kryptographisch- bevorzugt auf Hardwareniveau - zugangsgesichertes Prozessorelement verstanden. Prozessorelemente dieser Art erfüllen hohe Sicherheitsanforderungen, wie sie beispielsweise an die auf SIM-Karten, Kreditkarten, Bankkarten usw. integrierten Single-Chip-Prozessoren gestellt werden.

[0023] Der Trusted-Element-Prozessor 10 empfängt den Strom von Ortsdaten p_i aus dem Satellitennavigationsempfänger 5 des Fahrzeuggeräts 2 direkt oder über den Verarbeitungsteil 7 und ist dafür ausgebildet bzw. programmiert, jederzeit auf spezifische Anforderungen bzw. Auslösung (Triggerung) über einen vorgegebenen Zeitabschnitt s, z.B. eine, fünf oder zehn Minuten lang, die Ortsdaten p_i aufzuzeichnen. Der aufgezeichnete Zeitabschnitt $s(p_i)$ wird vom Trusted-Element-Prozessor 10 anschließend mit seiner kryptographischen Signatur tk signiert und damit "eingefroren".

[0024] Bei der Signierung oder auch unmittelbar davor kann eine Datenreduktion am Zeitabschnitt s vorgenommen werden, beispielsweise durch Bildung eines Hashwerts desselben. Unter einem Hashwert wird in der folgenden Beschreibung die Anwendung einer praktisch unumkehrbaren n:1-Abbildungsfunktion auf einen Eingangsdatensatz verstanden, d.h. einer Funktion, die nur (extrem) vieldeutig umkehrbar ist, so dass aus der Kenntnis des Hashwerts praktisch nicht mehr auf den Eingangsdatensatz geschlossen werden kann. Beispiele solcher Hashfunktionen sind die Quersummenfunktion, die Modulofunktion usw.

[0025] Der signierte protokollierte Zeitabschnitt, hier mit $s^*(p_i,tk)$ bezeichnet, wird anschließend über die Sendeempfangseinheit 8 des Fahrzeuggeräts 2 an eine Betreiberzentrale 3 und von dieser an eine Verrechnungszentrale 4 gesandt. Die Verrechnungszentrale 4 kann anhand der Signatur tk des signierten Zeitabschnitts s* auf dessen authentischen Ursprung aus einem Trusted-Element-Prozessor 10 ihres Vertrauens schließen. Alternativ oder zusätzlich kann der signierte protokollierte Zeitabschnitt s* auf einer Schnittstelle 11 des Fahrzeuggeräts 2 zur Abfrage bereitgestellt werden.

[0026] Das Starten des Zeitabschnitts s der Protokollierung der Ortsdaten p_i im Trusted-Element-Prozessor 10 kann auf verschiedene Arten ausgelöst werden. Eine erste Ausführungsform besteht darin, dass das Fahrzeuggerät 2 einen Zeitgeber 12 enthält, in der Art eines "Watchdog", welcher zu einem vorgegebenen Zeitpunkt T die genannte Protokollierung auslöst, d.h. den Trusted-Element-Prozessor 10 zu der genannten Funktionalität "aufweckt", wenn die aktuelle Zeit t = T ist.

[0027] Ein zweites Startkriterium besteht darin, dass der Trusted-Element-Prozessor 10 das Auftreten eines vorgegebenen Orts P in den Ortsdaten p_i detektiert. Bei dem vorgegebenen Ort P kann es sich um einen punktuellen Ort handeln, z.B. um eine "virtuelle Mautstation", oder um einen ausgedehnten Ort wie einen Parkplatz, eine Innenstadt, ein Autobahnteilstück usw. Sobald der Trusted-Element-Prozessor 10 den Ort P in den Ortsdaten p_i detektiert, d.h. feststellt, dass eine Position p in den Ortsdaten p_i in den Grenzen oder in die Nähe des vorgegebenen Orts P gelangt, startet die Protokollierung über den genannten vorgegebenen Zeitabschnitts, z.B. über zehn Minuten. Nach Abschluss der Protokollierung liegt der signierte protokollierte Zeitabschnitt s* der Ortsdaten p_i zur Versendung und Abfrage vor.

[0028] Ein weiteres, besondere Sicherheit bietendes Startkriterium besteht darin, dass der Trusted-Element-Prozessor 10 das Auftreten des vorgegebenen Orts P nicht in den eigenen Ortsdaten p_i des eigenen Fahrzeuggeräts 2, sondern in "fremden" Ortsdaten p_i' detektiert, welche ihm von anderen ("fremden") benachbarten Fahrzeuggeräten 2 mitgeteilt werden. Dies wird nun im Einzelnen erläutert.

[0029] Wie in den Fig. 1 und 2 dargestellt, können eine Gruppe von Fahrzeuggeräten 2 des Straßenmautsystems 1 ein Drahtlosnetzwerk 13 bilden, indem sie untereinander über Drahtlosverbindungen 14 in Verbindung stehen. Die Drahtlosverbindungen 14 können beispielsweise nach dem WAVE- oder WLAN-Standard aufgebaut sein und das Drahtlosnetzwerk 13 ist bevorzugt ein ad-hoc-Netzwerk oder VANET. Zu diesem Zweck verfügt jedes Fahrzeuggerät 2 über einen geeigneten Drahtlos-Sendeempfänger 15. Optional können der Drahtlos-Sendeempfänger 15 und die Sendeempfangseinheit 8 des Fahrzeuggeräts 2 ident sein.

[0030] Innerhalb des Drahtlosnetzwerks 13 können Fahrzeuggeräte 2 sich gegenseitig über ihren jeweiligen aktuellen Ort p informieren oder z. B. fortlaufend ihre Ortsdaten p_i austauschen. Ein Beispiel hiefür ist der Austausch von VST-Nachrichten (Vehicle Service Table Messages) im Rahmen eines VANETs, bei dem sich die einzelnen Netzknoten (Fahrzeuggeräte 2) bei Aufbau einer Drahtlosverbindung 14 über ihre Kommunikationsfähigkeiten und die von ihnen angebotenen Dienste gegenseitig informieren und einander ihre Orte p oder ihre Ortsdaten p_i der letzten Zeit mitteilen.

[0031] Alternativ kann ein Trusted-Element-Prozessor 10 eines Fahrzeuggeräts 2 auch von sich aus jederzeit Positionen p bzw. Ortsdaten p_i' benachbarter Fahrzeuggeräte 2 abfragen. Auch können die in einem Fahrzeuggerät 2 empfangenen Ortsdaten p_i' mehrerer benachbar-

ter Fahrzeuggeräte 2 miteinander abgeglichen werden, z.B. auf Konsistenz, um Ausreißer-Messwerte auszublenden oder um die empfangenen Ortsdaten p_i' zu mitteln.

[0032] Beim Abfragen bzw. Empfangen der fremden Ortsdaten p_i' der benachbarten Fahrzeuggeräte 2 können Abfrage- bzw. Sendeschlüssel mit zeitlich und/oder örtlich begrenzter Gültigkeit verwendet werden, so dass nur jene fremde Ortsdaten p_i', welche innerhalb eines vorgegebenen Zeitbereichs empfangen werden oder aus einem vorgegebenen Ortsbereich rund um das Fahrzeuggerät 2 stammen, Berücksichtigung finden.

[0033] Der Trusted-Element-Prozessor 10 ist nun dafür ausgebildet bzw. programmiert, dass er das Auftreten des vorgegebenen Orts P in den *fremden* Ortsdaten p_i' der benachbarten Fahrzeuggeräte 2 detektiert und dies als Auslösekriterium für das Starten der Protokollierung der Ortsaufzeichnungen p_i seines eigenen Fahrzeuggeräts 2 verwendet. Dadurch bleiben allfällige Manipulationen, Korrumptionen bzw. Störungen der eigenen Ortsdaten p_i bei der Auslösung der Protokollierung des Ortsdatenabschnitts s bzw. s* unberücksichtigt, was das Aufdecken eines Fehlverhaltens erleichtert: Stimmen die im eingefrorenen Zeitabschnitt s* enthaltenen Ortsaufzeichnungen p_i nicht (annähernd) mit jenem vorgegebenen Ort P überein, der in den fremden Ortsdaten p_i' detektiert wurde, liegt eine Manipulation oder eine Fehlfunktion des Fahrzeuggeräts 2 vor.

[0034] Auch ist es möglich, die genannten Ausführungsformen zu kombinieren: So kann der Zeitgeber 12 den Trusted-Element-Prozessor 10 dazu veranlassen, zu einem bestimmten Zeitpunkt t die Ortsdaten p_i' benachbarter Fahrzeuggeräte 2 abzufragen und sie gemeinsam mit dem Zeitabschnitt s der eigenen Ortsdaten p_i aufzuzeichnen und zu signieren, d.h. $s^*(p_i,tk,p_i')$, so dass eine Berücksichtigung der Nachbarorte p_i' bei der Überprüfung der eigenen Ortsaufzeichnungen p_i erfolgen kann.

[0035] Die benachbarten Fahrzeuggeräte 2, deren Ortsdaten p_i' verwendet werden, können unter Umständen auch ortsfest sein, z.B. nicht von einem Fahrzeug mitgeführt, sondern in einer ortsfesten Infrastruktur stationiert. In diesem Fall brauchen sie ihre Ortsdaten p_i' nicht fortlaufend neu bestimmen, sondern können diese einmal bestimmen oder vorgegeben eingespeichert enthalten. Auch solche "infrastrukturgebundene" Fahrzeuggeräte 2 fallen unter den hier verwendeten Begriff der benachbarten Fahrzeuggeräte 2.

[0036] Die vorgegebene Zeit T, der vorgegebene Ort P und/oder die Länge des Zeitabschnitts können bei der Fertigung des Fahrzeuggeräts 2 oder des Trusted-Element-Prozessors 10 in dieses bzw. diesen eingespeichert oder später über die Schnittstelle 11, die Sendeempfangseinheit 8 oder den Sendeempfänger 15 eingegeben werden.

[0037] Die Erfindung ist demgemäß nicht auf die dargestellten Ausführungsformen beschränkt, sondern umfasst alle Varianten und Modifikationen, die in den Rahmen der angeschlossenen Ansprüche fallen.

Patentansprüche

1. Fahrzeuggerät für ein Straßenmautsystem (1), mit einem Satellitennavigationsempfänger (5) zur fortlaufenden Erzeugung von Ortsdaten (p_i) für eine Verarbeitungs- und Sendeempfangseinheit (7, 8) des Fahrzeuggeräts (2) und einem gesonderten Trusted-Element-Prozessor (10) zur Protokollierung (s) eines Zeitabschnitts der erzeugten Ortsdaten (p_i) und zur kryptographischen Signierung (s*) desselben, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) dafür ausgebildet ist, die genannte Protokollierung (s) bei Detektion einer vorgegebenen Zeit (T) oder eines vorgegebenen Orts (P) des Fahrzeuggeräts (2) zu starten und für einen vorgegebenen Zeitabschnitt durchzuführen.

2. Fahrzeuggerät nach Anspruch 1, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) den vorgegebenen Ort (P) in den erzeugten eigenen Ortsdaten (p_i) detektiert.

3. Fahrzeuggerät nach Anspruch 1, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) den vorgegebenen Ort (P) in fremden Ortsdaten (p_i') detektiert, die er über ein Drahtlosnetzwerk (13) von benachbarten Fahrzeuggeräten (2) empfängt.

4. Fahrzeuggerät nach Anspruch 3, **dadurch gekennzeichnet, dass** das Drahtlosnetzwerk (13) ein ad-hoc-Netzwerk ist, bevorzugt nach dem WAVE- oder WLAN-Standard.

5. Fahrzeuggerät nach Anspruch 3 oder 4, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) die fremden Ortsdaten (p_i) mehrerer benachbarter Fahrzeuggeräte (2) empfängt und miteinander abgleicht, um in den abgeglichenen fremden Ortsdaten (p_i') den vorgegebenen Ort (P) zu detektieren.

6. Fahrzeuggerät nach einem der Ansprüche 3 bis 5, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) die fremden Ortsdaten (p_i') anonym abfragt.

7. Fahrzeuggerät nach einem der Ansprüche 3 bis 6, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) die fremden Ortsdaten (p_i') unter Austausch eines Schlüssels mit zeitlich und/oder örtlich begrenzter Gültigkeit abfragt und nur fremde Ortsdaten (p_i'), die unter einem gültigen Schlüssel empfangen werden, berücksichtigt.

8. Fahrzeuggerät nach einem der Ansprüche 1 bis 7,

dadurch gekennzeichnet, dass der Trusted-Element-Prozessor (10) den signierten Zeitabschnitt (s*) mittels der Sendeempfangseinheit (8) des Fahrzeuggeräts (2) an eine Zentrale des Straßenmautsystems (1) absendet.

9. Fahrzeuggerät nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** der Trusted-Element-Prozessor (10) den signierten Zeitabschnitt (s*) über eine Schnittstelle (11) des Fahrzeuggeräts (2) zur Abfrage bereitstellt.

10. Ad-hoc-Netzwerk aus zumindest zwei Fahrzeuggeräten nach einem der Ansprüche 3 bis 9, die über ihre Sendeempfangseinheiten (8) miteinander in Verbindung stehen, wobei zumindest ein Fahrzeuggerät (2) Ortsdaten (p_i) einem anderen Fahrzeuggerät (2) bereitstellt, welches einen vorgegebenen Ort (P) darin detektiert, um die Protokollierung (s) seiner eigenen Ortsdaten (p_i) zu starten.

11. Verfahren zur Protokollierung von Ortsdaten (p_i) eines ortsaufzeichnenden Fahrzeuggeräts (2) eines Straßenmautsystems (1) mit mehreren Fahrzeuggeräten (2), die drahtlos Ortsdaten (p_i) austauschen können, umfassend, in einem ersten Fahrzeuggerät (2):

Empfangen von Ortsdaten (p_i') eines zweiten Fahrzeuggeräts (2) ,
Detektieren eines vorgegebenen Orts (P) in den empfangenen Ortsdaten (p_i') des zweiten Fahrzeuggeräts (2),
Starten der Protokollierung (s) eines Zeitabschnitts der Ortsdaten (p_i) des ersten Fahrzeuggeräts (2), und
Signieren (s*) des protokollierten Zeitabschnitts mit einer kryptographischen Signatur.

12. Verfahren zur Protokollierung von Ortsdaten (p_i) eines ortsaufzeichnenden Fahrzeuggeräts (2) eines Straßenmautsystems (1) mit mehreren Fahrzeuggeräten (2), die drahtlos Ortsdaten (p_i) austauschen können, umfassend, in einem ersten Fahrzeuggerät (2):

Detektieren einer vorgegebenen Zeit (T),
Starten der Protokollierung (s) eines Zeitabschnitts der Ortsdaten (p_i) des ersten Fahrzeuggeräts (2) und Empfangen von Ortsdaten (p_i') eines zweiten Fahrzeuggeräts (2), und
Signieren (s*) des protokollierten Zeitabschnitts und der empfangenen Ortsdaten (p_i) mit einer kryptographischen Signatur.

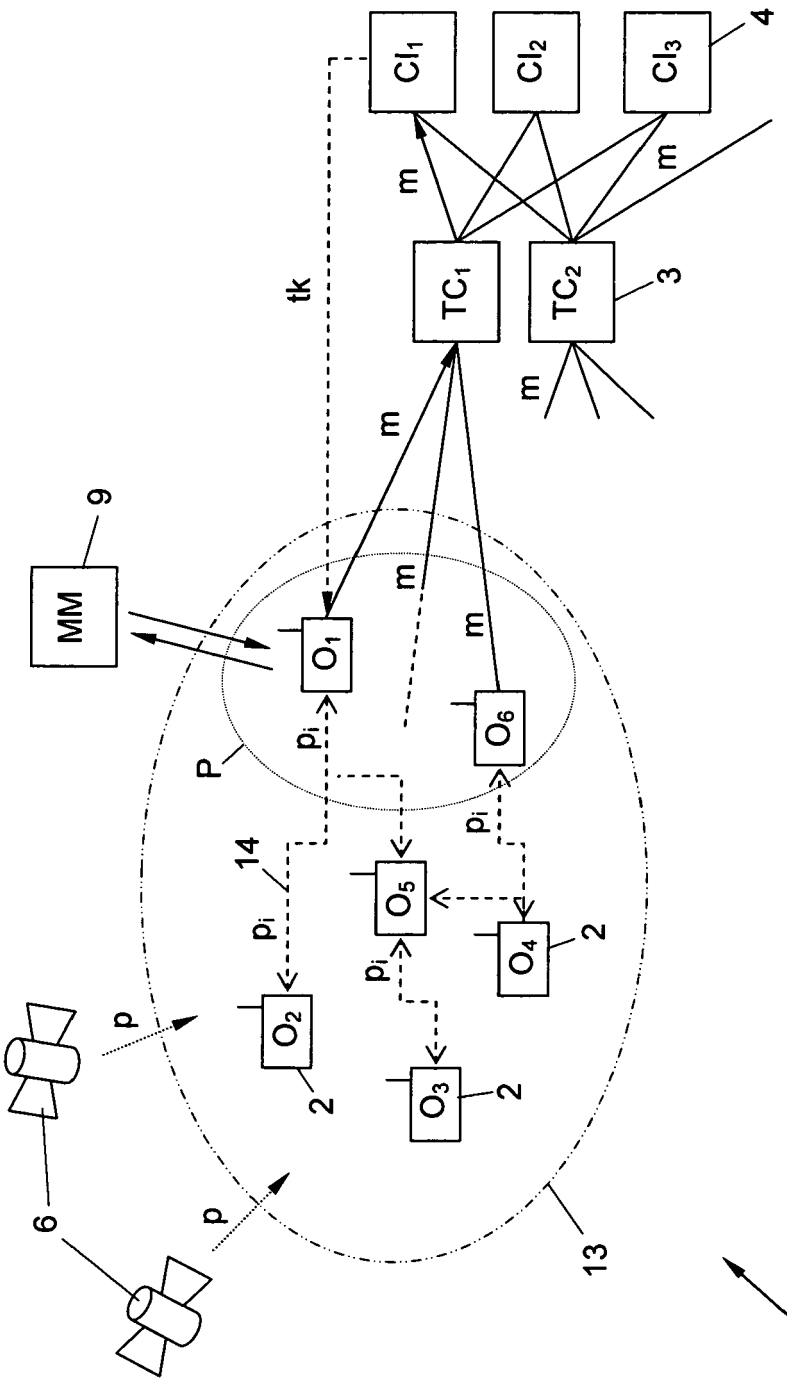

Fig. 1

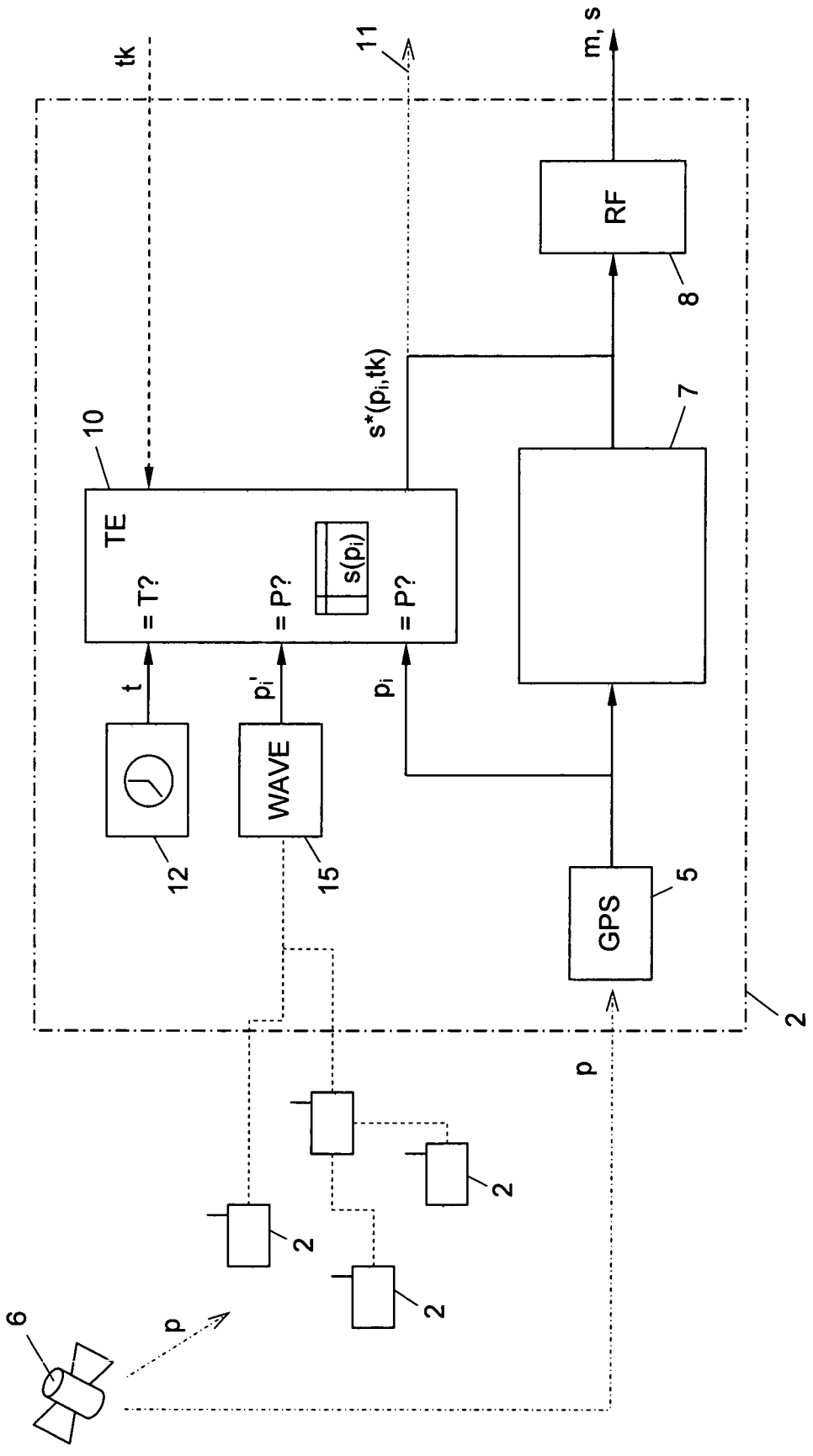

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 11 45 0023

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X Y	EP 2 017 790 A2 (PALMER CHARLES GRAHAM [GB]) 21. Januar 2009 (2009-01-21) * Absatz [0005] - Absatz [0013] * * Absatz [0020] - Absatz [0022] * * Absatz [0032] - Absatz [0035] * * Absatz [0039] * * Absatz [0073] - Absatz [0076] * * Absatz [0096] * * Abbildungen * -----	1,2,8,9 3-7, 10-12	INV. G07B15/06
Y	DE 102 58 653 A1 (DAIMLER CHRYSLER AG [DE]) 11. September 2003 (2003-09-11) * Zusammenfassung * * Absatz [0013] * * Absatz [0017] - Absatz [0018] * * Absatz [0021] - Absatz [0026] * * Abbildungen 1,2 * -----	3-7, 10-12	
E	EP 2 330 562 A1 (NXP BV [NL]) 8. Juni 2011 (2011-06-08) * Absatz [0016] - Absatz [0017] * * Absatz [0025] * * Absatz [0033] - Absatz [0038] * * Absatz [0053] * * Absatz [0066] * * Abbildungen * ----- -/--	1,2,8,9	RECHERCHIERTE SACHGEBIETE (IPC) G07B

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	30. Juni 2011	Königer, Axel

KATEGORIE DER GENANNTEN DOKUMENTE

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

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

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

1
EPO FORM 1503 03.82 (P04C03)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 11 45 0023

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	DE BOER WILLEM ET AL: "Road Pricing: Security architecture KMH Road Pricing System", ROAD PRICING: SECURITY ARCHITECTURE KMH ROAD PRICING SYSTEM, TECHNOLUTION BV , FOR THE MINISTRY OF TRANSPORT,PUBLIC WORKS AND WATER MANAGEMENT, PO BOX 2013 2800 BD GOUDA, THE NETHERLANDS, Bd. 1.1, Nr. MTD02001, 22. August 2002 (2002-08-22), Seiten 1-102, XP001503326, * Seite 29 - Seite 30 * * Seite 33 - Seite 36 * * Seite 39 - Seite 44 * * Seite 79 - Seite 80 * * Seite 87 - Seite 90 * -----	1,2,8,9	
A	WO 2009/015989 A1 (BOSCH GMBH ROBERT [DE]; REBSCH JOHANNES-CHRISTOF [DE]; FRIESE MICHAEL) 5. Februar 2009 (2009-02-05) * Seite 2, Zeile 15 - Seite 3, Zeile 25 * * Seite 4, Zeile 26 - Seite 5, Zeile 25 * * Seite 8, Zeile 14 - Zeile 19 * * Abbildungen 1,2 * -----	3-7, 10-12	RECHERCHIERTE SACHGEBIETE (IPC)

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	30. Juni 2011	Königer, Axel

KATEGORIE DER GENANNTEN DOKUMENTE

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

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

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

1

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 11 45 0023

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

30-06-2011

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2017790 A2	21-01-2009	GB 2451167 A	21-01-2009
		US 2009024458 A1	22-01-2009
DE 10258653 A1	11-09-2003	KEINE	
EP 2330562 A1	08-06-2011	US 2011131238 A1	02-06-2011
WO 2009015989 A1	05-02-2009	DE 102007035737 A1	19-02-2009
		EP 2176836 A1	21-04-2010

EPO FORM P0461

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

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Nicht-Patentliteratur

- Security aspects of the 1,11 EETS. *Expert Group 12, Final report V1.0,* 05. April 2007 **[0002]**
- Electronic fee collection - Application interface definition for autonomous systems - Part 1: Changing. *ISO Technical Specification 17575-1,* 15. Juni 2010 **[0002]**
- An Example of a view on EETS trust and privacy in GNSS based toll systems. *Vis J, Report Ministry of Transport, Public Works and Water Management of The Netherlands,* 15. Dezember 2009 **[0002]**