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

(11) **EP 2 423 885 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
29.02.2012 Patentblatt 2012/09

(51) Int Cl.:
G07B 15/00 *(2011.01)*

(21) Anmeldenummer: **10450129.1**

(22) Anmeldetag: **06.08.2010**

(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 SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME RS

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

(72) Erfinder:
- **Tijink, Jasja**
2380 Perchtoldsdorf (AT)
- **Nagy, Oliver**
1190 Wien (AT)
- **Kersten, Jan**
71570 Oppenweiler (DE)

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

Bemerkungen:
Geänderte Patentansprüche gemäss Regel 137(2) EPÜ.

(54) Vorrichtung und Verfahren zur Funktionsüberwachung eines Strassenmautsystems

(57) Die Erfindung betrifft eine Vorrichtung zur Funktionsüberwachung eines Straßenmautsystems (1), das zumindest ein seine Position in Form von rohen Positionsdaten (3) aufzeichnendes Fahrzeuggerät (2) und einen stationären Proxyrechner (7) umfaßt, der die rohen Positionsdaten (3) vom Fahrzeuggerät (2) empfängt und daraus durch Mautkartenabgleich kartenabgeglichene Mautdaten (8) erzeugt, mit zumindest einem ersten mit einer Signatur (10') ausgestatteten und kryptographisch zugangsgesicherten Prozessorelement (10), welches einerseits die rohen Positionsdaten (3) oder daraus extrahierte Streckendaten (9) vom Fahrzeuggerät (2) und anderseits die kartenabgeglichenen Mautdaten (8) vom Proxyrechner (7) empfängt und dafür ausgebildet ist, die kartenabgeglichenen Mautdaten (8) gegenüber den rohen Positions- bzw. den daraus extrahierten Streckendaten (3, 9) zu plausibilisieren und bei erfolgreicher Plausibilisierung mit seiner Signatur (10') versehen auszugeben. Die Erfindung betrifft ferner ein Verfahren für eine derartige Funktionsüberwachung.

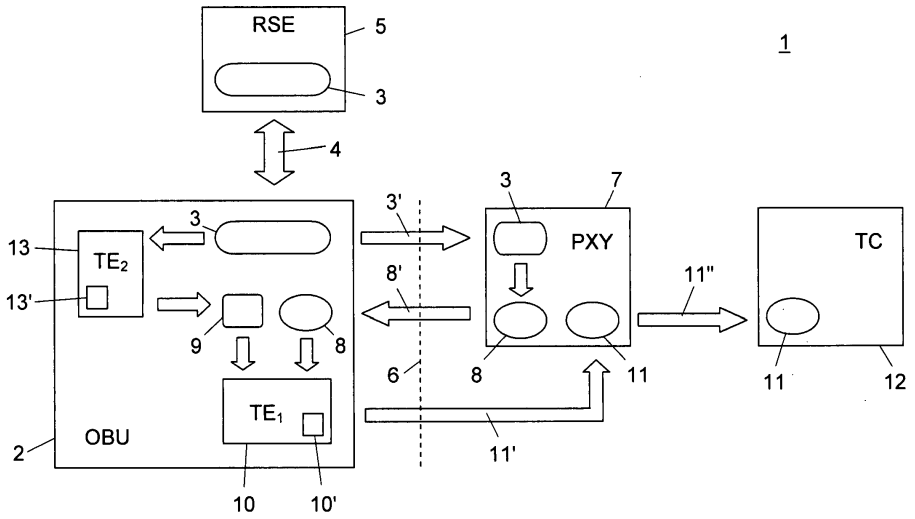

Fig. 1

EP 2 423 885 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren zur Funktionsüberwachung eines Straßenmautsystems, das zumindest ein seine Position in Form von rohen Positionsdaten aufzeichnendes Fahrzeuggerät und einen stationären Proxyrechner umfaßt, der die rohen Positionsdaten vom Fahrzeuggerät empfängt und daraus durch Mautkartenabgleich kartenabgeglichene Mautdaten erzeugt.

[0002] Derartige Straßenmautsysteme werden auch als Thin-client-Systeme bezeichnet. Das Fahrzeuggerät, auch On-board-Unit bzw. OBU genannt, kann kostengünstig mit geringer Rechenleistung ("thin-client") ausgeführt werden, weil der rechenintensive Mautkartenabgleich, d.h. der Abgleich der Positionsdaten mit für die Mauterhebung relevanten geographischen Elementen z.B. auf einer entsprechend vorbereiteten oder geeigneten digitalen Straßenkarte, in leistungsfähige stationäre Proxyrechner des Straßenmautsystems ausgelagert ist. Thin-Client-OBUs ermitteln dabei ihre Position beispielsweise mit Hilfe von Satellitennavigation oder Funklokalisierung in terrestrischen Funkbaken- oder Mobilfunknetzen.

[0003] Auch wenn Thin-client-Mautsysteme für den einzelnen Benutzer aufgrund der geringen Kosten einer Thin-client-OBU erhebliche Vorteile bringen, haben sie für den Betreiber des Stra-βenmautsystems den Nachteil, daß eine durchgehende sichere Funktionsüberprüfung ("secure monitoring") nicht möglich ist: So ist z.B. die Zuverlässigkeit des Mautkartenabgleichs im Proxyrechner für den Mautbetreiber nicht nachprüfbar und damit auch für Systemlieferanten schwer oder nicht nachweisbar.

[0004] Hingegen ist eine solche Funktionsüberwachung bei sog. Thick-client-Mautsystemen möglich: Bei diesen Mautsystemen werden kostspielige Thick-client-OBUs eingesetzt, welche über ihr eigenes Mautkartenmaterial und hohe Rechenleistung verfügen, um selbst den Mautkartenabgleich durchzuführen und die kartenabgeglichenen Mautdaten an ein Zentralsystem abzusetzen. Für solche Systeme sind Konzeptüberlegungen bekannt, die von den Thick-client-OBUs berechneten Mautdaten mit einer vom Mautbetreiber ausgegebenen und in der OBU installierten Signatur zu versehen, um die Authentizität der Daten gegenüber dem Zentralsystem des Mautbetreibers zu gewährleisten. Diese Lösung erfordert OBUs mit hoher Rechenleistung, welche die vom Mautbetreiber geforderten Authentifizierungsfunktionen ausführen können, und ist für herkömmliche Thin-client-Systeme nicht geeignet.

[0005] Die Erfindung setzt sich zum Ziel, eine Secure-Monitoring-Lösung für Thin-client-Straßenmautsysteme zu schaffen, welche die Vorteile der Betreibersicherheit von signierenden Thick-client-Systemen mit den Kostenvorteilen von Thin-client-Systemen verbindet.

[0006] Dieses Ziel wird in einem ersten Aspekt der Erfindung mit einer Vorrichtung der eingangs genannten Art erreicht, die sich gemäß der Erfindung durch zumindest ein erstes mit einer Signatur ausgestattetes und kryptographisch zugangsgesichertes Prozessorelement auszeichnet, welches einerseits die rohen Positionsdaten oder daraus extrahierte Streckendaten vom Fahrzeuggerät und anderseits die kartenabgeglichenen Mautdaten vom Proxyrechner empfängt und dafür ausgebildet ist, die kartenabgeglichenen Mautdaten gegenüber den rohen Positions- bzw. den daraus extrahierten Streckendaten zu plausibilisieren und bei erfolgreicher Plausibilisierung mit seiner Signatur versehen auszugeben.

[0007] Die Erfindung schafft damit erstmals eine durchgehende Zertifizierungslösung für von Thin-client-OBUs erzeugte Mautdaten. Ein mit einer Signatur ausgestattetes und kryptographisch zugangsgesichertes Prozessorelement stellt ein "trusted element" für den Mautbetreiber dar, welches mit einer ihm vertrauenswürdigen Signatur, z.B. einem Zertifikat einer vertrauenswürdigen Ausgabestelle, ausgestattet und für seinen alleinigen Zugang gesichert werden kann. Prozessorelemente dieser Art können kostengünstig als Single-Chip-Module hergestellt werden, wie sie bei SIM-Karten, Chipkarten usw. in breitem Umfang verwendet werden. Im Gegensatz zu dem bei Thick-client-OBUs erforderlichen Kartenabgleich in der OBU erfordert die erfindungsgemäße Plausibilitätsprüfung der kartenabgeglichenen Mautdaten gegenüber den Positions- bzw. Streckendaten eine nur geringe Rechenleistung des Trusted Elements, wie sie von handelsüblichen SIM- bzw. Chipkarten-Prozessorelementen ohne weiteres aufgebracht werden kann.

[0008] Unter dem Begriff "Plausibilisieren" wird in der vorliegenden Beschreibung eine grobe Überprüfung bzw. ein ungefährer Vergleich verstanden, ob die vom Proxyrechner erstellten Mautdaten den Positionsdaten bzw. daraus extrahierten Streckendaten entspringen können, d.h. *plausibel* sind: So lassen sich beispielsweise gebietsbezogene Mautdaten plausibilisieren, indem überprüft wird, ob die zugrundegelegenen Positionsdaten in dem Gebiet der Mautdaten liegen. Wenn die Mautdaten auf einer zurückgelegten Wegstrecke oder Wegzeit beruhen, kann die Plausibilität z.B. mit Hilfe einer überschlagsmäßigen Kumulierung der zwischen einzelnen Positionen der Positionsdaten liegenden Entfernungen geprüft werden.

[0009] In einer ersten bevorzugten Ausführungsform der Erfindung ist das erste Prozessorelement im Proxyrechner des Mautbetreibers angeordnet. Dadurch kann das Prozessorelement direkt in der Verfügungsgewalt des Betreibers (oder eines vertrauenswürdigen Dritten) stehen und auch betreiberspezifisch ausgeführt werden.

[0010] Eine alternative bevorzugte Ausführungsform der Erfindung für ein Straßenmautsystem, dessen Proxyrechner die kartenabgeglichenen Mautdaten zurück an das Fahrzeuggerät sendet, zeichnet sich dadurch aus, daß das erste Prozessorelement im Fahrzeuggerät angeordnet ist. Diese Lösung hat den Vorteil, daß das Pro-

zessorelement mit verschiedenen Proxyrechnern unterschiedlicher Mautbetreiber zusammenarbeiten kann. Darüber hinaus sind dadurch die von einer Thin-client-OBU abgegebenen Mautdaten in derselben Art und Weise zertifiziert, wie sie von einer herkömmlichen zertifizierten Thick-client-OBU erhaltbar sind.

[0011] Besonders günstig ist es, wenn das erste Prozessorelement in das Fahrzeuggerät modular austauschbar eingesetzt ist, beispielsweise in der Art einer SIM-Karte. Dadurch können z.B. von Drittlieferanten gefertigte Thin-client-OBUs vom Betreiber mit Prozessorelementen seines Vertrauens ausgestattet werden.

[0012] Wie bereits erörtert, kann das Prozessorelement entweder die rohen Positionsdaten oder daraus extrahierte Streckendaten mit den Mautdaten abgleichen. Bevorzugt werden aus den Positionsdaten extrahierte Streckendaten verwendet, d.h. das Fahrzeuggerät ist dafür ausgebildet, aus den rohen Positionsdaten Streckendaten zu extrahieren und an das erste Prozessorelement zu senden, welches die kartenabgeglichenen Mautdaten gegenüber den extrahierten Streckendaten plausibilisiert. Dies stellt einen Zugewinn an Vertraulichkeit ("privacy") dar: Das dem Mautbetreiber zur Zertifizierung dienende Prozessorelement erfährt damit nicht die rohen Positionsdaten der OBU ("position fix track"), sondern nur Auszüge bzw. Verallgemeinerungen derselben, was die Bewegungshistorie des Benutzers vor Datenmißbrauch schützt.

[0013] Zu diesem Zweck sind bevorzugt die extrahierten Streckendaten aus den rohen Positionsdaten akkumulierte Wegstrecken oder Wegzeiten, aus welchen sich keine direkten Rückschlüsse auf die einzelnen Bewegungen des Benutzers mit seinem Fahrzeuggerät ziehen lassen.

[0014] Bei Verwendung solcher Streckendaten zeichnet sich eine weitere bevorzugte Ausführungsform der Erfindung durch zumindest ein zweites mit einer Signatur ausgestattetes und kryptographisch zugangsgesichertes Prozessorelement aus, das im Fahrzeuggerät angeordnet und dafür ausgebildet ist, die genannten extrahierten Streckendaten aus den rohen Positionsdaten zu erzeugen und mit seiner Signatur zu versehen. Dadurch kann eine zusätzliche Funktionsüberwachungsstufe eingeführt werden, welche auch den Schritt der Extrahierung der Streckendaten umfaßt.

[0015] Bevorzugt ist auch das zweite Prozessorelement in das Fahrzeuggerät modular austauschbar eingesetzt, und besonders bevorzugt können das erste und das zweite Prozessorelement sogar ident sein.

[0016] Eine weitere besonders vorteilhafte Ausführungsform der Erfindung zeichnet sich dadurch aus, daß das Fahrzeuggerät dafür ausgebildet ist, die mit der Signatur versehenen extrahierten Streckendaten auf einer Schnittstelle zur Abfrage durch eine straßenseitige Infrastruktur bereitzustellen. Dadurch ermöglicht das Prozessorelement bzw. "trusted element" gleichzeitig auch einen "secure freezing service" für die im Fahrzeuggerät fortlaufend anfallenden Positions- bzw. daraus extrahierten Streckendaten. Straßenseitige Infrastruktur wie Mautbaken, Kontrollfahrzeuge usw. können auf diese Weise vertrauenswürdige ("trusted") Kontrolldaten von passierenden Fahrzeuggeräten einholen.

[0017] In einem zweiten Aspekt schafft die Erfindung ein Verfahren zur Funktionsüberwachung eines Straßenmautsystems der genannten Art, welches sich dadurch auszeichnet, daß in einem mit einer Signatur ausgestatteten und kryptographisch zugangsgesicherten Prozessorelement die kartenabgeglichenen Mautdaten des Proxyrechners gegenüber den rohen Positionsdaten des Fahrzeuggeräts oder daraus extrahierten Streckendaten plausibilisiert und bei erfolgreicher Plausibilisierung mit der Signatur versehen ausgegeben werden.

[0018] Wenn der Proxyrechner die kartenabgeglichenen Mautdaten zurück an das Fahrzeuggerät sendet, erfolgt das genannte Plausibilisieren bevorzugt in einem Prozessorelement des Fahrzeuggeräts.

[0019] Gemäß einem weiteren Merkmal der Erfindung werden im Fahrzeuggerät aus den rohen Positionsdaten die Streckendaten extrahiert und im Prozessorelement die kartenabgeglichenen Mautdaten gegenüber den extrahierten Streckendaten plausibilisiert.

[0020] Dabei sind bevorzugt die extrahierten Strekkendaten Wegstrecken oder Wegzeiten, die aus den Positionsdaten akkumuliert werden.

[0021] Besonders günstig ist es, wenn in demselben oder einem weiteren mit einer Signatur ausgestatteten und kryptographisch zugangsgesicherten Prozessorelement die extrahierten Streckendaten aus den rohen Positionsdaten erzeugt und mit der Signatur versehen werden.

[0022] Bevorzugt werden die mit der Signatur versehenen extrahierten Streckendaten im Fahrzeuggerät für eine Abfrage durch eine straßenseitige Infrastruktur bereitgestellt.

[0023] Hinsichtlich weiterer Merkmale und Vorteile des erfindungsgemäßen Verfahrens wird auf die obigen Ausführungen zur erfindungsgemäßen Vorrichtung verwiesen.

[0024] Die Erfindung wird nachstehend anhand von in den beigeschlossenen Zeichnungen dargestellten Ausführungsbeispielen näher erläutert. In den Zeichnungen zeigt

Fig. 1 ein Blockschaltbild einer ersten Vorrichtung der Erfindung, in dem gleichzeitig die Datenflüsse des erfindungsgemäßen Verfahrens dargestellt sind; und

Fig. 2 ein Blockschaltbild einer zweiten Ausführungsform der Vorrichtung der Erfindung, welches gleichzeitig die Datenflüsse einer zweiten Ausführungsform des erfindungsgemäßen Verfahrens wiedergibt.

[0025] Fig. 1 zeigt eine Vorrichtung und ein Verfahren zur sicheren Funktionsüberwachung ("secure monitoring") im Rahmen eines schematisch dargestellten Stra-

ßenmautsystems 1. Das Straßenmautsystem 1 umfaßt eine Vielzahl von Fahrzeuggeräten bzw. O-BUs 2 (nur eine OBU stellvertretend dargestellt) in Form von Thin-Clients, welche auf an sich bekannte Weise fortlaufend ihr eigene geographische Position bestimmen, z.B. mit Hilfe von Satellitennavigation oder Funklokalisation in einem Netz von Funkbaken, Mobilfunkstationen usw. Die von einer OBU 2 bestimmten Positionen ("position fixes") werden als "rohe" Positionsdaten ("position fix tracks") 3 in einem Speicher der OBU aufgezeichnet. Die Positionsdaten 3 können durch die Kombination der Sensordaten verschiedenster Sensoren des Fahrzeuges, in dem die OBU 2 verbaut ist, wie Tachometer-, Kompaß- oder Beschleunigungsmeßdaten, ergänzt oder verbessert werden, wie dem Fachmann bekannt.

[0026] Die OBUs 2 können über eine Funkschnittstelle 4 z.B. nach dem DSRC-Standard (dedicated short range communication) mit einer straßenseitigen Infrastruktur 5 (roadside equipment, RSE) in Verbindung stehen, beispielsweise DSRC-Funkbaken, WLAN-Accesspoints (wireless local aerea network), WAVE-Basisstationen (wireless access in a vehicle environment) usw., die sie auf ihrem Weg passieren und an welche sie eine Kopie der Positionsdaten 3 zu Kontrollzwecken übermitteln können.

[0027] Über dieselbe Funkschnittstelle 4 oder über eine weitere Funkschnittstelle 6, z.B. eine Datenverbindung in einem Mobilfunknetz, stehen die OBUs 2 ferner mit (zumindest) einem Proxyrechner 7 des Straßenmautsystems 1 in Verbindung, welchem sie - fortlaufend oder stapelweise, z.B. periodisch oder im Anlaßfall - ihre Positionsdaten 3 übermitteln. Der Proxyrechner 7 verfügt über eine hohe Rechenleistung, z.B. in Form einer Serverfarm, und umfangreiches Land- bzw. Mautkartenmaterial, um einen Kartenabgleich ("map matching") zwischen den rohen Positionsdaten 3 einerseits und vorgegebenen geographischen Positionen wie Straßenverläufen, virtuellen Mauterhebungsstellen usw. durchzuführen. Durch diesen Mautkartenabgleich wird die Genauigkeit der Positionsbestimmung der OBU 2 verbessert, weil streuende bzw. abweichende Positionsbestimmungen (position fixes) jeweils korrekten Positionen in einem Straßennetz zugeordnet werden können. Beispielsweise könnte die Genauigkeit der rohen Positionsdaten 3 hinsichtlich der zurückgelegten Wegstrecke ("driven distance") bei herkömmlicher GPS-Bestimmung etwa ± 5% betragen, wogegen sie nach dem Kartenabgleich im Proxyrechner 7 eine Genauigkeit von ± 1% aufweisen könnte.

[0028] Die derart kartenabgeglichenen, verbesserten Positionsdaten werden im Proxyrechner 7 als Grundlage für kartenabgeglichen Mautdaten 8 verwendet. Diese Mautdaten lassen in der Regel keine individuellen Rückschlüsse mehr auf die einzelnen Positionen der Positionsdaten 3 zu, denn sie stellen je nach Prinzip und Ausführungsform des Mautsystems eine zusammenfassende bzw. abstrahierende und "ortsanonymisierte" Auswertung derselben dar, beispielsweise in Form der befahrenen Streckenabschnitte eines Straßennetzes oder der zurückgelegten Wegstrecke ("driven distance") oder Wegzeit. Letztere können z.B. zur wegeabhängigen Vergebührung von Mautstraßen ("pay as you drive") oder zeitabhängigen Vergebührung von gebührenpflichtigen Parkplätzen usw. verwendet werden. Die kartenabgeglichenen Mautdaten 8 können im Proxyrechner 7 optional mit solchen Mautgebühreninformationen versehen werden.

[0029] Die kartenabgeglichenen, ortsanonymisierten Mautdaten 8 werden vom Proxyrechner 7 in der Ausführungsform von Fig. 1 zurück an die OBU 2 gesandt, siehe Pfeil 8'. Wie dem Fachmann bekannt, kann auf diese Weise, wenn sich die OBU 2 gegenüber dem Proxyrechner 7 für den Mautdatenabgleich mit einer anonymen temporären Kennung identifiziert, Anonymität ("privacy") für die sensiblen Positionsdaten 3 und damit den Weg des Fahrzeuges gewährleistet werden.

[0030] Um diesen Vorgang für einen Mautbetreiber, welcher die Mautdaten 8 zur Vergebührung benötigt, in seiner Funktionsweise nachprüfbar zu machen und die Systemfunktionalität ihm gegenüber gewährleisten zu können, dienen die folgenden Vorrichtungen und Verfahren.

[0031] Die OBU 2 erzeugt unabhängig vom Proxyrechner 7 - ohne Mautkartenabgleich und nur mit einfachen Rechenmitteln, u.zw. bevorzugt mit einem später noch ausführlich beschriebenen Prozessorelement 13 - eine grobe Schätzung der Mautdaten, in weiterer Folge als aus den Positionsdaten 3 *extrahierte* Streckendaten 9 bezeichnet. Die Streckendaten 9 dienen dazu, eine Plausibilitätsprüfung der vom Proxyrechner 7 erzeugten Mautdaten 8 durchführen zu können. Die Streckendaten sind demgemäß mit den Mautdaten 8 vergleichbar, wenn auch weit weniger genau, weil sie ja auf den unverbesserten, rohen Positionsdaten 3 beruhen. Wenn die Mautdaten 8 z.B. die zurückgelegte Wegstrecke ("driven distance") bzw. Wegzeit wiedergeben, dann sind die von der OBU 2 aus den Positionsdaten 3 extrahierten Strekkendaten 9 ebenfalls eine daraus berechnete zurückgelegte Wegstrecke bzw. Wegzeit. In dem zuvor genannten Beispiel von GPS-bestimmten Positionsdaten 3 und mautkartenabgeglichenen Mautdaten 8 ist die Genauigkeit der Streckendaten 9 z.B. ± 5% und jene der Mautdaten 8 z.B. ± 1%.

[0032] Die Mautdaten 8 können aufgrund dieser Genauigkeitsunterschiede damit zwar nicht direkt mit den Streckendaten 9 verglichen werden, jedoch gegenüber diesen plausibilisiert werden, d.h. es kann geprüft werden, ob die Mautdaten 8 auf Grundlage der Streckendaten 9 *plausibel* sind.

[0033] Zu diesem Zweck ist in der OBU 2 ein speziell geschütztes Prozessorelement 10 vorgesehen, das z.B. vom Mautbetreiber selbst in die OBU 2 eingesetzt werden kann, beispielsweise in Form einer SIM- oder Chipkarte. Das Prozessorelement 10 ist auf Hardwareniveau kryptographisch zugangsgesichert, sodaß beispielsweise nur der Mautbetreiber Zugang zu den darin enthalte-

nen Daten und Programmen hat. Das Prozessorelement 10 stellt damit ein für den Mautbetreiber vertrauenswürdiges Element ("trusted element") dar und erfüllt ähnlich hohe Sicherheitsanforderungen, wie sie beispielsweise an die auf SIM-Karten, Kreditkarten, Bankkarten usw. integrierten Single-Chip-Prozessoren gestellt werden.

[0034] Das kryptographisch zugangsgesicherte Prozessorelement 10 ist ferner in an sich bekannter Weise mit einer kryptographischen Signatur 10', z.B. einem kryptographischen Zertifikat, ausgestattet, d.h. einem kryptographischen Datenelement 10', welches vom Prozessorelement 10 all seinen Datenausgaben hinzugefügt werden kann, um deren Authentizität gegenüber der Ausgabestelle der Signatur bzw. des Zertifikats, z.B. dem Mautbetreiber, nachweisen zu können.

[0035] In dem Prozessorelement 10 wird der geschilderte Plausibilitätsvergleich der Mautdaten 8 mit den Streckendaten 9 durchgeführt. Für diesen Plausibilitätsvergleich ist keine hohe Rechenleistung - wie sie etwa für den Mautkartenabgleich im Proxyrechner 7 erforderlich ist - notwendig, weil hier lediglich z.B. eine grobe Abschätzungsrechnung zwischen einer in den Mautdaten 8 genau und in den Streckendaten 9 ungenau angegebenen Wegstrecke durchgeführt werden muß. Die Plausibilitäts- überprüfung im Prozessorelement 10 kann daher mit der in einem einfachen Trusted-Element-Single-Chip-Prozessor zur Verfügung stehenden Rechenleistung durchgeführt werden.

[0036] Bei erfolgreicher Plausibilisierung der Mautdaten 8 versieht das Prozessorelement 10 diese mit seiner Signatur 10' und gibt sie als signierte Mautdaten 11 aus, siehe Pfad 11'. Die signierten Mautdaten 11 können vom Prozessorelement 10 der OBU 2 beispielsweise wieder über die Funkschnittstelle 6 an den Proxyrechner 7 zurückgesandt und von diesem an einen Zentralrechner 12 des Straßenmautsystems 1 weitergeleitet werden, siehe Pfad 11'. Alternativ können sie auch direkt von der OBU 2 an den Zentralrechner 12 abgesetzt werden, u.zw. sowohl "online" z.B. über die Funkschnittstelle 4 oder 6 als auch "offline" über einen Datenträger.

[0037] Auf diese Weise plausibilisiert und signiert bzw. zertifiziert das Prozessorelement 10 die in einem fortlaufenden Strom einlangenden Mautdaten 8 jeweils einzeln oder fortlaufend abschnittsweise.

[0038] In einer alternativen, vereinfachten Ausführungsform könnte die OBU 2 auf die Extraktion der Streckendaten 9 aus den Positionsdaten 3 verzichten und die Positionsdaten 3 könnten dem Prozessorelement 10 direkt zugeführt werden. In diesem Fall plausibilisiert das Prozessorelement 10 die Mautdaten 8 direkt gegenüber den Positionsdaten 3, wobei das Prozessorelement 10 dann vermehrte Rechenschritte ausführen muß oder eine stärker vereinfachte Plausibilisierung durchführt, z.B. lediglich überprüft, ob einzelne Positionen aus den Positionsdaten 3 in eine in den Mautdaten 8 angegebenen Gebietsmaut fallen, USW.

[0039] In einer bevorzugten Ausführungsform wird in der OBU 2 ein zweites kryptographisch zugangsgesichertes Prozessorelement ("trusted element") 13 vorgesehen werden, um aus den Positionsdaten 3 die Streckendaten 9 zu extrahieren. Das Prozessorelement 13 ist mit einer eigenen Signatur 13' ausgestattet, mit welcher es die von ihm erzeugten Streckendaten 9 versieht (signiert).

[0040] Die vom Prozessorelement 13 signierten Streckendaten 9 können überdies in der OBU 2 zur Abfrage durch die Infrastruktur 5 über die Schnittstelle 4 bereitgestellt werden. Dadurch leistet das Prozessorelement ("trusted element") 13 einen "secure freezing service" für die Positionsdaten 3 bzw. die daraus extrahierten Streckendaten 9. Die Signierung bzw. Zertifizierung der Streckendaten 9 gewährleistet gegenüber der Infrastruktur 5, daß die über die Schnittstelle 4 abgefragten Streckendaten 9 von einem entsprechend vertrauenswürdigen Rechenelement, u.zw. Prozessorelement ("trusted element") 13, erzeugt und signiert wurden.

[0041] In Fig. 1 können das erste und das zweite Prozessorelement 10, 13 auch ein und dasselbe physische Prozessorelement sein, in der nachfolgend beschriebenen Ausführungsform von Fig. 2 ist dies nicht möglich. In Fig. 2 bezeichnen gleiche Bezugszeichen gleiche Elemente wie in Fig. 1 und es wird nur auf die Unterschiede gegenüber Fig. 1 eingegangen.

[0042] In der Ausführungsform von Fig. 2 sendet der Proxyrechner 7 die kartenabgeglichenen Mautdaten 8 nicht mehr zurück an die OBU 2. Das erste Prozessorelement 10 ist daher im Proxyrechner 7 angeordnet bzw. mit diesem verbunden, und die OBU 2 sendet hier zusätzlich zu den rohen Positionsdaten 3 auch die extrahierten Streckendaten 9 an den Proxyrechner 7, siehe Pfeil 9'. Die Streckendaten 9 können optional wieder von dem zweiten, in der OBU 2 angeordneten Prozessorelement 13 aus den rohen Positionsdaten 3 erzeugt und mit der Signatur 13' signiert worden sein, sodaß der Proxyrechner 7 bzw. das erste Prozessorelement 10 sicher sein kann, daß die Streckendaten 9 korrekt in der OBU 2 extrahiert wurden. Auch hier können wieder die signierten Streckendaten 9 von der OBU 2 über die Schnittstelle 4 für Kontrollabfragen bereitgestellt werden.

[0043] Das erste Prozessorelement 10 im Proxyrechner 7 plausibilisiert nun wieder die im Proxyrechner 7 kartenabgeglichenen Mautdaten 8 gegenüber den (optional signierten) Streckendaten 9 und versieht sie im Plausibilisierungsfall mit seiner Signatur 10', um signierte Mautdaten 11 auszugeben (Pfeil 11").

[0044] Die Erfindung ist nicht auf die dargestellten Ausführungsformen beschränkt, sondern umfaßt alle Varianten und Modifikationen, die in den Rahmen der angeschlossenen Ansprüche fallen.

Patentansprüche

1. Vorrichtung zur Funktionsüberwachung eines Straßenmautsystems (1), das zumindest ein seine Position in Form von rohen Positionsdaten (3) aufzeich-

nendes Fahrzeuggerät (2) und einen stationären Proxyrechner (7) umfaßt, der die rohen Positionsdaten (3) vom Fahrzeuggerät (2) empfängt und daraus durch Mautkartenabgleich kartenabgeglichene Mautdaten (8) erzeugt, **gekennzeichnet durch** zumindest ein erstes mit einer Signatur (10') ausgestattetes und kryptographisch zugangsgesichertes Prozessorelement (10), welches einerseits die rohen Positionsdaten (3) oder daraus extrahierte Streckendaten (9) vom Fahrzeuggerät (2) und anderseits die kartenabgeglichenen Mautdaten (8) vom Proxyrechner (7) empfängt und dafür ausgebildet ist, die kartenabgeglichenen Mautdaten (8) gegenüber den rohen Positions- bzw. den daraus extrahierten Streckendaten (3, 9) zu plausibilisieren und bei erfolgreicher Plausibilisierung mit seiner Signatur (10') versehen auszugeben.

2. Vorrichtung nach Anspruch 1, **dadurch gekennzeichnet, daß** das erste Prozessorelement (10) im Proxyrechner (7) angeordnet ist.

3. Vorrichtung nach Anspruch 1 für ein Straßenmautsystem (1), dessen Proxyrechner (7) die kartenabgeglichenen Mautdaten (8) zurück an das Fahrzeuggerät (2) sendet, **dadurch gekennzeichnet, daß** das erste Prozessorelement (10) im Fahrzeuggerät (2) angeordnet ist.

4. Vorrichtung nach Anspruch 3, **dadurch gekennzeichnet, daß** das erste Prozessorelement (10) in das Fahrzeuggerät (2) modular austauschbar eingesetzt ist.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, daß** das Fahrzeuggerät (2) dafür ausgebildet ist, aus den rohen Positionsdaten (3) die Streckendaten (9) zu extrahieren und an das erste Prozessorelement (10) zu senden, welches die kartenabgeglichenen Mautdaten (8) gegenüber den extrahierten Streckendaten (9) plausibilisiert.

6. Vorrichtung nach Anspruch 5, **dadurch gekennzeichnet, daß** die extrahierten Streckendaten (9) aus den rohen Positionsdaten (3) akkumulierte Wegstrecken oder Wegzeiten sind.

7. Vorrichtung nach Anspruch 5 oder 6, **dadurch gekennzeichnet**, **gekennzeichnet durch** zumindest ein zweites mit einer Signatur (13') ausgestattetes und kryptographisch zugangsgesichertes Prozessorelement (13), das im Fahrzeuggerät (2) angeordnet und dafür ausgebildet ist, die extrahierten Streckendaten (9) aus den rohen Positionsdaten (3) zu erzeugen und mit seiner Signatur (13') zu versehen.

8. Vorrichtung nach Anspruch 7, **dadurch gekennzeichnet, daß** das zweite Prozessorelement in das Fahrzeuggerät modular austauschbar eingesetzt ist.

9. Vorrichtung nach den Ansprüchen 3 und 7, **dadurch gekennzeichnet, daß** das erste und das zweite Prozessorelement (10, 13) ident sind.

10. Vorrichtung nach einem der Ansprüche 7 bis 9, **dadurch gekennzeichnet, daß** das Fahrzeuggerät (12) dafür ausgebildet ist, die mit der Signatur (13') versehenen extrahierten Streckendaten (9) auf einer Schnittstelle (4) zur Abfrage durch eine straßenseitige Infrastruktur (5) bereitzustellen.

11. Verfahren zur Funktionsüberwachung eines Straßenmautsystems (1), das zumindest ein seine Position in Form von rohen Positionsdaten (3) aufzeichnendes Fahrzeuggerät (2) und einen stationären Proxyrechner (7) umfaßt, der die rohen Positionsdaten (3) vom Fahrzeuggerät (2) empfängt und daraus durch Mautkartenabgleich kartenabgeglichene Mautdaten (8) erzeugt, **dadurch gekennzeichnet, daß** in einem mit einer Signatur (10') ausgestatteten und kryptographisch zugangsgesicherten Prozessorelement (10) die kartenabgeglichenen Mautdaten (8) des Proxyrechners (7) gegenüber den rohen Positionsdaten (3) des Fahrzeuggeräts (2) oder daraus extrahierten Streckendaten (9) plausibilisiert und bei erfolgreicher Plausibilisierung mit der Signatur (10') versehen ausgegeben werden.

12. Verfahren nach Anspruch 11 für ein Straßenmautsystem (1), dessen Proxyrechner (7) die kartenabgeglichenen Mautdaten (8) zurück an das Fahrzeuggerät (2) sendet, **dadurch gekennzeichnet, daß** das genannte Plausibilisieren in einem Prozessorelement (10) des Fahrzeuggeräts (2) erfolgt.

13. Verfahren nach Anspruch 11 oder 12, **dadurch gekennzeichnet, daß** im Fahrzeuggerät (2) aus den rohen Positionsdaten (3) die Streckendaten (9) extrahiert und im Prozessorelement (10) die kartenabgeglichenen Mautdaten (8) gegenüber den extrahierten Streckendaten (9) plausibilisiert werden.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet, daß** die extrahierten Streckendaten (9) Wegstrecken oder Wegzeiten sind, die aus den Positionsdaten (3) akkumuliert werden.

15. Verfahren nach einem der Ansprüche 11 bis 14, **dadurch gekennzeichnet, daß** in demselben oder einem weiteren mit einer Signatur (10', 13') ausgestatteten und kryptographisch zugangsgesicherten Prozessorelement (10, 13) die extrahierten Streckendaten (9) aus den rohen Positionsdaten (3) erzeugt und mit der Signatur (10', 13') versehen werden.

16. Verfahren nach Anspruch 15, **dadurch gekenn-**

zeichnet, daß die mit der Signatur (10', 13') versehenen extrahierten Streckendaten (9) im Fahrzeuggerät (2) für eine Abfrage durch eine straßenseitige Infrastruktur (5) bereitgestellt werden.

Geänderte Patentansprüche gemäss Regel 137(2) EPÜ.

1. Vorrichtung zur Funktionsüberwachung eines Straßenmautsystems (1), das zumindest ein seine Position in Form von rohen Positionsdaten (3) aufzeichnendes Fahrzeuggerät (2) und einen stationären Proxyrechner (7) umfaßt, der die rohen Positionsdaten (3) vom Fahrzeuggerät (2) empfängt und daraus durch Mautkartenabgleich kartenabgeglichene Mautdaten (8) erzeugt, **gekennzeichnet durch** zumindest ein erstes mit einer Signatur (10') ausgestattetes gesondertes Prozessorelement (10), welches einerseits die rohen Positionsdaten (3) oder daraus extrahierte Streckendaten (9) vom Fahrzeuggerät (2) und anderseits die kartenabgeglichenen Mautdaten (8) vom Proxyrechner (7) empfängt und dafür ausgebildet ist, die kartenabgeglichenen Mautdaten (8) gegenüber den rohen Positions- bzw. den daraus extrahierten Streckendaten (3, 9) abschätzend zu vergleichen und bei erfolgreichem Abschätzungvergleich mit seiner Signatur (10') versehen auszugeben.

2. Vorrichtung nach Anspruch 1, **dadurch gekennzeichnet, daß** das erste Prozessorelement (10) im Proxyrechner (7) angeordnet ist.

3. Vorrichtung nach Anspruch 1 für ein Straßenmautsystem (1), dessen Proxyrechner (7) die kartenabgeglichenen Mautdaten (8) zurück an das Fahrzeuggerät (2) sendet, **dadurch gekennzeichnet, daß** das erste Prozessorelement (10) im Fahrzeuggerät (2) angeordnet ist.

4. Vorrichtung nach Anspruch 3, **dadurch gekennzeichnet, daß** das erste Prozessorelement (10) in das Fahrzeuggerät (2) modular austauschbar eingesetzt ist.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, daß** das Fahrzeuggerät (2) dafür ausgebildet ist, aus den rohen Positionsdaten (3) die Streckendaten (9) zu extrahieren und an das erste Prozessorelement (10) zu senden, welches die kartenabgeglichenen Mautdaten (8) gegenüber den extrahierten Streckendaten (9) abschätzend vergleicht.

6. Vorrichtung nach Anspruch 5, **dadurch gekennzeichnet, daß** die extrahierten Streckendaten (9) aus den rohen Positionsdaten (3) akkumulierte Wegstrecken oder Wegzeiten sind.

7. Vorrichtung nach Anspruch 5 oder 6, **dadurch gekennzeichnet**, **gekennzeichnet durch** zumindest ein zweites mit einer Signatur (13') ausgestattetes gesondertes Prozessorelement (13), das im Fahrzeuggerät (2) angeordnet und dafür ausgebildet ist, die extrahierten Streckendaten (9) aus den rohen Positionsdaten (3) zu erzeugen und mit seiner Signatur (13') zu versehen.

8. Vorrichtung nach Anspruch 7, **dadurch gekennzeichnet, daß** das zweite Prozessorelement in das Fahrzeuggerät modular austauschbar eingesetzt ist.

9. Vorrichtung nach den Ansprüchen 3 und 7, **dadurch gekennzeichnet, daß** das erste und das zweite Prozessorelement (10, 13) ident sind.

10. Vorrichtung nach einem der Ansprüche 7 bis 9, **dadurch gekennzeichnet, daß** das Fahrzeuggerät (12) dafür ausgebildet ist, die mit der Signatur (13') versehenen extrahierten Streckendaten (9) auf einer Schnittstelle (4) zur Abfrage durch eine straßenseitige Infrastruktur (5) bereitzustellen.

11. Verfahren zur Funktionsüberwachung eines Straßenmautsystems (1), das zumindest ein seine Position in Form von rohen Positionsdaten (3) aufzeichnendes Fahrzeuggerät (2) und einen stationären Proxyrechner (7) umfaßt, der die rohen Positionsdaten (3) vom Fahrzeuggerät (2) empfängt und daraus durch Mautkartenabgleich kartenabgeglichene Mautdaten (8) erzeugt, **dadurch gekennzeichnet, daß** in einem mit einer Signatur (10') ausgestatteten gesonderten Prozessorelement (10) die kartenabgeglichenen Mautdaten (8) des Proxyrechners (7) gegenüber den rohen Positionsdaten (3) des Fahrzeuggeräts (2) oder daraus extrahierten Strekkendaten (9) abschätzend verglichen und bei erfolgreichem Abschätzungsvergleich mit der Signatur (10') versehen ausgegeben werden.

12. Verfahren nach Anspruch 11 für ein Straßenmautsystem (1), dessen Proxyrechner (7) die kartenabgeglichenen Mautdaten (8) zurück an das Fahrzeuggerät. (2) sendet, **dadurch gekennzeichnet, daß** das genannte abschätzende Vergleichen in einem Prozessorelement (10) des Fahrzeuggeräts (2) erfolgt.

13. Verfahren nach Anspruch 11 oder 12, **dadurch gekennzeichnet, daß** im Fahrzeuggerät (2) aus den rohen Positionsdaten (3) die Streckendaten (9) extrahiert und im Prozessorelement (10) die kartenabgeglichenen Mautdaten (8) gegenüber den extrahierten Streckendaten (9) abschätzend verglichen werden.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet, daß** die extrahierten Streckendaten (9) Wegstrecken oder Wegzeiten sind, die aus den Positionsdaten (3) akkumuliert werden.

15. Verfahren nach einem der Ansprüche 11 bis 14, **dadurch gekennzeichnet, daß** in demselben oder einem weiteren mit einer Signatur (10', 13') ausgestatteten gesonderten Prozessorelement (10, 13) die extrahierten Streckendaten (9) aus den rohen Positionsdaten (3) erzeugt und mit der Signatur (10', 13') versehen werden.

16. Verfahren nach Anspruch 15, **dadurch gekennzeichnet, daß** die mit der Signatur (10', 13') versehenen extrahierten Streckendaten (9) im Fahrzeuggerät (2) für eine Abfrage durch eine straßenseitige Infrastruktur (5) bereitgestellt werden.

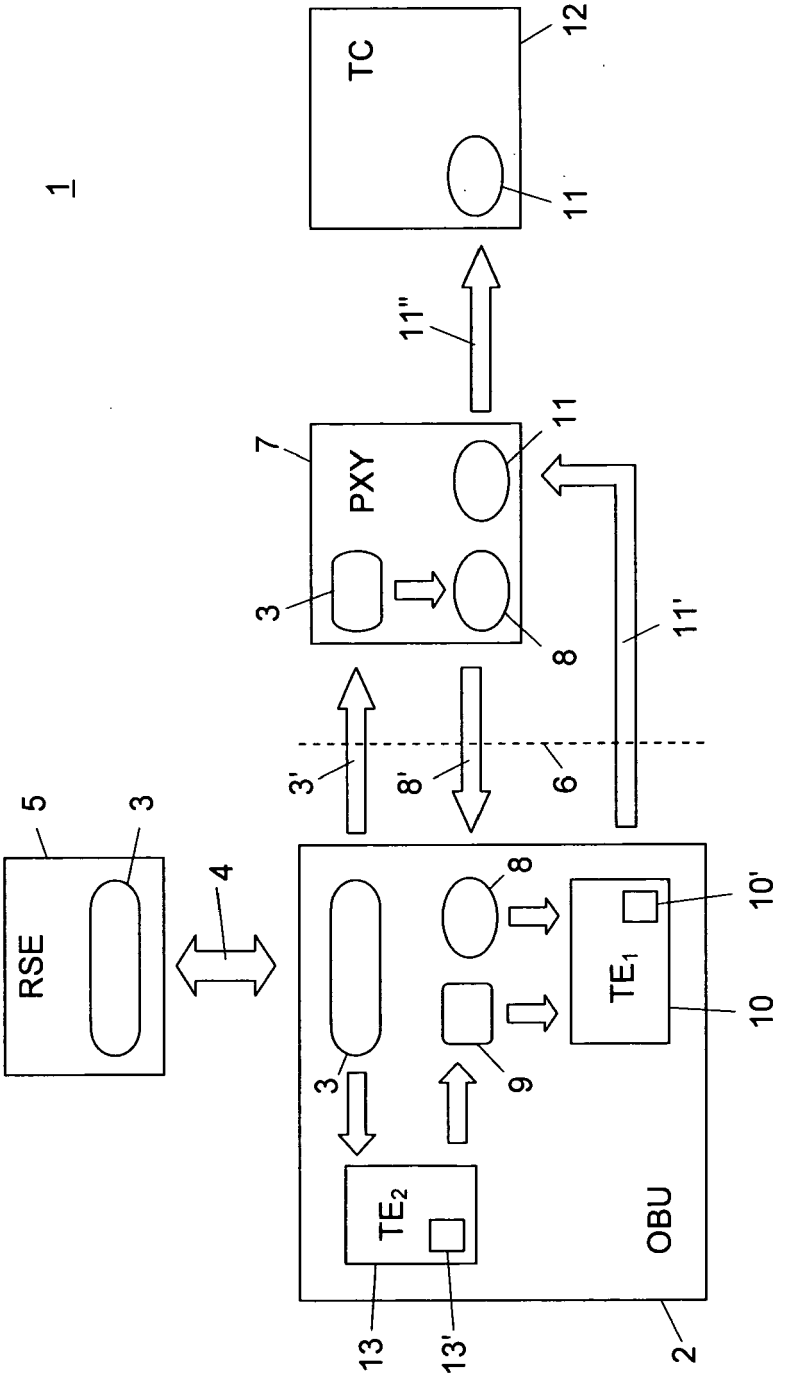

Fig. 1

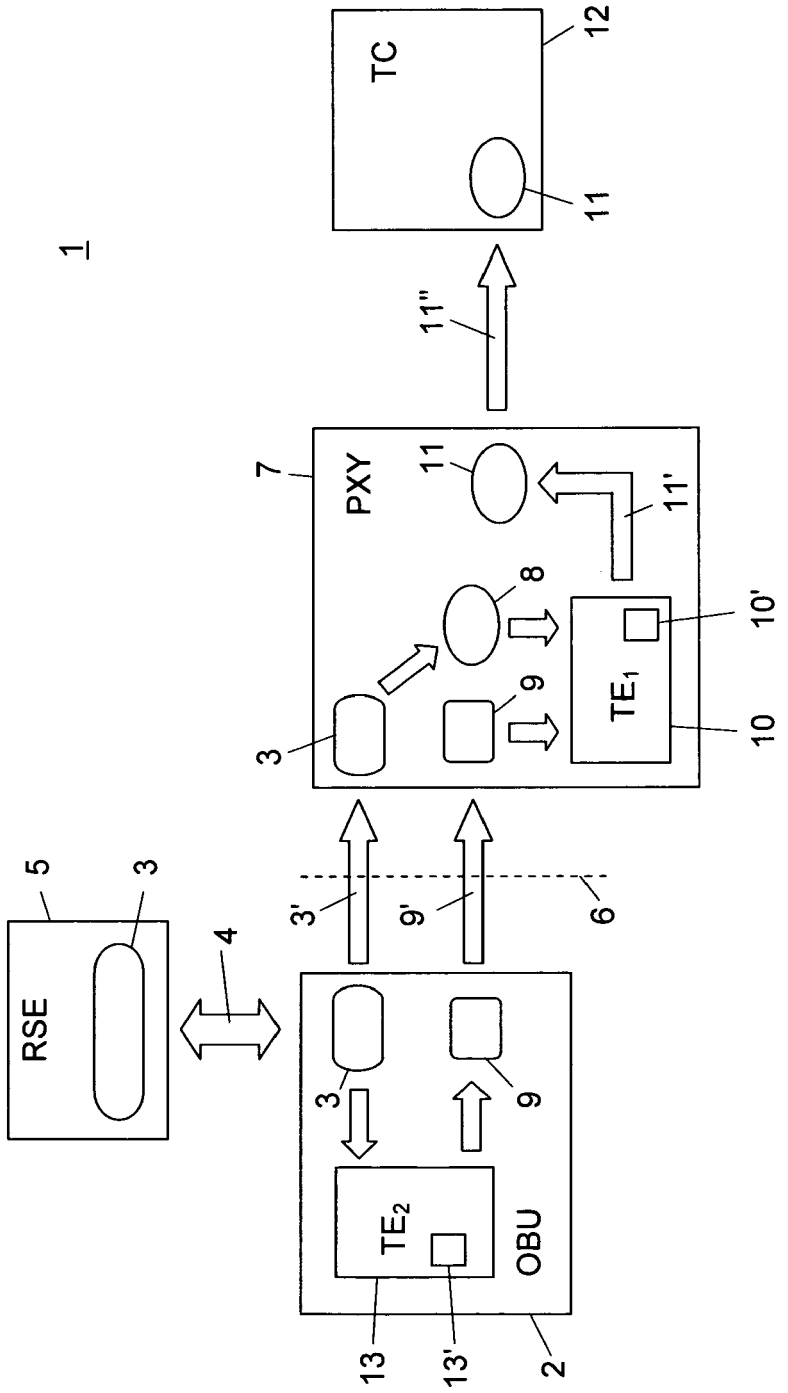

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 10 45 0129

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) * Spalte 2, Zeile 33 - Spalte 3, Zeile 49 * * Spalte 5, Zeile 8 - Spalte 13, Zeile 2 * * Abbildungen 1-3 * -----	1,3-16 2	INV. G07B15/06
Y	"Electronic fee collection - Application interface definition for autonomous systems - Part 1 : Changing", ISO TECHNICAL SPECIFICATION,, Nr. ISO/TS 17575-1, 15. Juni 2010 (2010-06-15), Seiten I-VIII,1, XP008130463, * Seite (vi), Abschnitt : "Technical architecture" * * Abbildung 2 * -----	2	
A	WO 2009/001303 A1 (NXP BV [NL]; DAEMS FRANK C H [BE]; PEETERS MICHAEL M P [BE]) 31. Dezember 2008 (2008-12-31) * Zusammenfassung * * Seite 2, Zeile 8 - Seite 3, Zeile 14 * * Seite 5, Zeile 4 - Seite 7, Zeile 16 * * Seite 8, Zeile 15 - Zeile 30 * * Seite 10, Zeile 4 - Zeile 22 * * Seite 11, Zeile 24 - Seite 12, Zeile 3 * * Abbildungen 2-6 * -----	1-3,5,6, 10-14,16	RECHERCHIERTE SACHGEBIETE (IPC) G07B
A	WO 2006/015792 A1 (DAIMLER CHRYSLER AG [DE]; BEIER WOLFGANG [DE]; LENART SIEGLEIF [DE]) 16. Februar 2006 (2006-02-16) * Zusammenfassung * * Seite 2, Zeile 10 - Seite 3, Zeile 2 * * Seite 4, Zeile 13 - Seite 5, Zeile 11 * * Seite 6, Zeile 8 - Zeile 34 * * Seite 9, Zeile 1 - Zeile 8 * * Abbildungen 1-4 * ----- -/--	1,2,5,6, 11	

1 Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	17. Dezember 2010	Van der Haegen, D

KATEGORIE DER GENANNTEN DOKUMENTE

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

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

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 10 45 0129

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
A	VIS J: "An example of a view on EETS trust and privacy in GNSS based toll systems", REPORT MINISTRY OF TRANSPORT, PUBLIC WORKS AND WATER MANAGEMENT THE NETHERLANDS,, 15. Dezember 2009 (2009-12-15), Seiten 1-28, XP007916365, * Seite 13, Absatz 2.3.3 * * Seite 20, Absatz 3.1.2 * -----	1,11	
A	EXPERT GROUP 12: "Security aspects of the EETS", EG 12 FINAL REPORT V1.0 5APR07,, Nr. v1.0, 5. April 2007 (2007-04-05), Seiten 1-86, XP007916364, * Seite 30 - Seite 38 * -----	1,11	

RECHERCHIERTE SACHGEBIETE (IPC)

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	17. Dezember 2010	Van der Haegen, D

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 10 45 0129

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.

17-12-2010

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
WO 2009001303 A1	31-12-2008	AU 2008269354 A1	31-12-2008
		CN 101689311 A	31-03-2010
		EP 2193504 A1	09-06-2010
		US 2010198665 A1	05-08-2010
WO 2006015792 A1	16-02-2006	DE 102004038170 B3	16-03-2006

EPO FORM P0461

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