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

(11) **EP 2 360 647 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
24.08.2011 Patentblatt 2011/34

(51) Int Cl.:
G07B 15/02 *(2011.01)* ***G08G 1/017*** *(2006.01)*
G08G 1/054 *(2006.01)*

(21) Anmeldenummer: **10450005.3**

(22) Anmeldetag: **21.01.2010**

(84) Benannte Vertragsstaaten:
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:
AL BA RS

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

(72) Erfinder:
- **Nagy, Oliver**
1190 Wien (AT)
- **Abl, Alexander**
9073 Viktring (AT)

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

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

(54) Verfahren zur Erfassung von Durchfahrten von Fahrzeugen

(57) Verfahren zur Erfassung von Durchfahrten von Fahrzeugen (1) mit eindeutigen Kennungen (5) von einer Einfahrt (3) zu einer Ausfahrt (4), mit den Schritten:
Erfassen der Kennung (5) eines Fahrzeugs (1) an der Einfahrt (3) als Einfahrtskennung (6), Verschlüsseln vorgegebener und/oder fahrzeugkennungsbezogener Daten (7) mit Hilfe der Einfahrtskennung (6) zu verschlüsselten Einfahrtsdaten (8), Bereitstellen der verschlüsselten Einfahrtsdaten (8), und Vernichten der Einfahrtskennung (6);
Erfassen der Kennung (5) eines Fahrzeugs (1) an der Ausfahrt (4) als Ausfahrtskennung (15), Ermitteln der bereitgestellten verschlüsselten Einfahrtsdaten (8) und Entschlüsseln der verschlüsselten Einfahrtsdaten (8) mit Hilfe der Ausfahrtskennung (15), um die genannten Daten (7) zu erhalten; und
Validieren der genannten Daten (7) gegenüber ihrer Vorgabe (DAT) bzw. der Ausfahrtskennung (15), wobei eine erfolgreiche Validierung die Durchfahrt des Fahrzeugs (1) anzeigt.

Fig. 1a

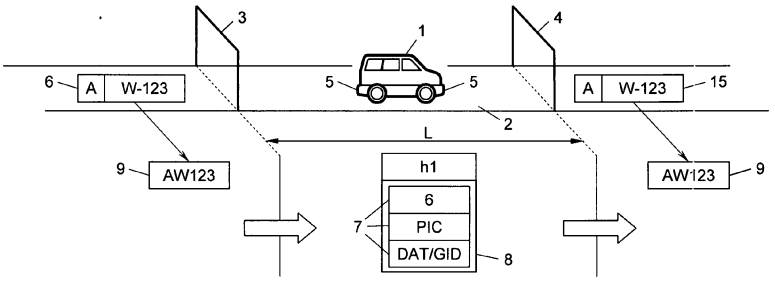


Fig. 1b

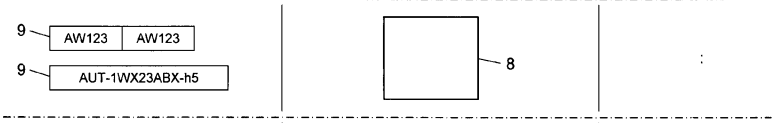


Fig. 1c

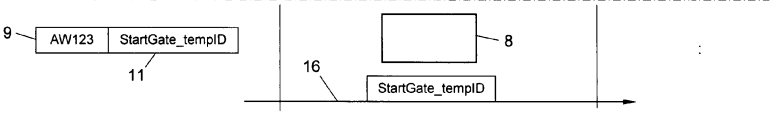
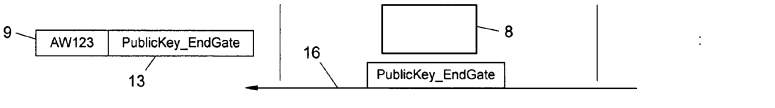


Fig. 1d



EP 2 360 647 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Erfassung von Durchfahrten von Fahrzeugen mit eindeutigen Kennungen von einer Einfahrt zu einer Ausfahrt.

[0002] Bestimmte Verkehrsüberwachungsaufgaben erfordern eine zweimalige Erfassung ein und desselben Fahrzeugs an zwei verschiedenen Punkten, hier allgemein als "Einfahrt" und "Ausfahrt" des vom Fahrzeug durchfahrenen Streckenabschnitts bezeichnet. Beispiele hiefür sind die sog. "Section Control", bei welcher die Ein- und Ausfahrtszeiten des Fahrzeugs gemessen und zur Geschwindigkeitsbestimmung herangezogen werden; die sog. "Video-Maut", bei der das Fahrzeug an der Ein- und Ausfahrt identifiziert wird, um den Streckenabschnitt wegabhängig zu vergebühren; oder die sog. "City-Maut", bei welcher die Ein-und Ausfahrt an Stadtgrenzen kontrolliert wird, um z.B. die Verweildauer in der Innenstadt zeitabhängig zu vergebühren.

[0003] Die dazu eingesetzten Verkehrsüberwachungssysteme müssen strengen Datenschutzauflagen genügen, um eine unzulässige Erstellung von Bewegungsprofilen der Verkehrsteilnehmer möglichst auszuschließen. Beispielsweise erfordern die gesetzlichen Regelungen in Österreich und Deutschland für die Durchführung der Section Control, daß eine dauerhafte Identifizierung eines Fahrzeugs und seiner Durchfahrtsdaten nur im Falle einer Geschwindigkeitsübertretung erfolgen darf.

[0004] Bislang bekannte Systeme versuchen diese Datenschutzanforderungen zu erfüllen, indem nach einer Identifizierung des Fahrzeugs an der Ein- und Ausfahrt und einer darauf basierenden Geschwindigkeitsmessung dann, wenn kein Geschwindigkeitsdelikt vorliegt, alle aufgezeichneten Daten innerhalb einer garantierten Zeit, z.B. 8 Minuten, spurlos gelöscht werden (siehe F. Albrecht, "Section Control in Deutschland", Straßenverkehrsrecht, Zeitschrift für die Praxis des Verkehrsjuristen, 2009). Diese Vorgehensweise ist weiterhin mit Unsicherheiten verbunden, weil alle Durchfahrtsdaten zu einem bestimmten Zeitpunkt in den Einfahrts- und Ausfahrtstationen in unverschlüsselter Form vorliegen, unabhängig davon, ob es sich um einen Delikatfall handelt oder nicht. Die bekannten Systeme können daher die Gefahr eines Datenmißbrauchs und Datenschutzbedenken nicht mit Sicherheit ausräumen.

[0005] Die Erfindung setzt sich zum Ziel, ein Verfahren zur Erfassung der Durchfahrten von Fahrzeugen zwischen einer Einfahrt und einer Ausfahrt zu schaffen, welches höchstmöglichen Datenschutz für die sensiblen Durchfahrtsdaten bietet.

[0006] Dieses Ziel wird mit einem Verfahren der einleitend genannten Art erreicht, das die folgenden Schritte umfaßt:

[0007] Erfassen der Kennung eines Fahrzeugs an der Einfahrt als Einfahrtskennung, Verschlüsseln vorgegebener und/oder fahrzeugkennungsbezogener Daten mit Hilfe der Einfahrtskennung zu verschlüsselten Einfahrtsdaten, Bereitstellen der verschlüsselten Einfahrtsdaten, und Vernichten der Einfahrtskennung;

[0008] Erfassen der Kennung eines Fahrzeugs an der Ausfahrt als Ausfahrtskennung, Ermitteln der bereitgestellten verschlüsselten Einfahrtsdaten, und Entschlüsseln der verschlüsselten Einfahrtsdaten mit Hilfe der Ausfahrtskennung, um die genannten Daten zu erhalten; und

[0009] Validieren der genannten Daten gegenüber ihrer Vorgabe bzw. der Ausfahrtskennung, wobei eine erfolgreiche Validierung die Durchfahrt des Fahrzeugs anzeigt.

[0010] Die Erfindung beruht auf der überraschenden Erkenntnis, daß die bei der Einfahrt des Fahrzeugs erfaßte Fahrzeugkennung, in der Regel das Fahrzeugkennzeichen, *selbst* als Schlüssel zur Verschlüsselung der Einfahrtsdaten verwendet werden kann. Dieser Schlüssel kann *sofort* nach der Verschlüsselung in der Einfahrtsstation vernichtet werden, weil er physisch, in Form des Fahrzeugs selbst, von der Einfahrt zur Ausfahrt "transportiert" und damit dort oder in nachgeordneten Auswertestationen zur Entschlüsselung zur Verfügung steht. Dadurch wird die Datensicherheit entscheidend erhöht: Die Einfahrtsstation erzeugt ausschließlich verschlüsselte Einfahrtsdaten ohne jedweden elektronischen Schlüssel zu deren Entschlüsselung und kann damit z.B. als "Black Box" versiegelt und datenschutzzertifiziert werden. Das Vorliegen unverschlüsselter Durchfahrtsdaten wird auf einen wesentlich kürzeren Zeitraum begrenzt, was die Gefahr von Manipulationen und unberechtigten Datenzugriffen signifikant reduziert.

[0011] Die Daten, welche zu den Einfahrtsdaten verschlüsselt werden, können im einfachsten Fall vorgegebener Art sein, d.h. eine Vorgabe, die auch bei der Ausfahrt bekannt ist und damit das Erkennen einer erfolgreichen Entschlüsselung gestattet. Die Vorgabe kann ein beliebiger bekannter Wert sein oder umfaßt bevorzugt eine Identifikation der Einfahrt, so daß an der Ausfahrt auch festgestellt werden kann, von welcher Einfahrt das Fahrzeug kommt.

[0012] Alternativ oder zusätzlich können die genannten Daten auf die Fahrzeugkennung bezogen sein, weil diese ebenso - in Form der Ausfahrtskennung - an der Ausfahrt bekannt ist. In einer weiteren Ausführungsform der Erfindung umfassen daher die genannten Daten die Einfahrtskennung selbst und/oder ein Einfahrtsbild des Fahrzeugs, aus dem die Einfahrtskennung ableitbar ist.

[0013] Ein solches Einfahrtsbild kann auch beim Entschlüsseln der Einfahrtsdaten wiedergewonnen und zusammen mit einem Ausfahrtsbild und der Kennung des Fahrzeugs zu Beweiszwecken archiviert werden.

[0014] Eine besonders vorteilhafte Ausführungsform der Erfindung zeichnet sich dadurch aus, daß die Einfahrtsdaten mit der Einfahrtszeit des Fahrzeugs versehen und aus der Menge der bereitgestellten Einfahrtsdaten gelöscht werden, sobald die aktuelle Zeit ein mit der Einfahrtszeit beginnendes Zeitfenster überschreitet. Diese Ausführungsform hat den entscheidenden Vorteil,

daß eine Entschlüsselung der Einfahrtsdaten stets nur im Deliktfall erfolgt: Das Zeitfenster wird so gewählt, daß es der minimalen zulässigen Fahrzeit für den Streckenabschnitt entspricht, d.h. wenn ein Fahrzeug mit der höchstzulässigen Geschwindigkeit fährt. Wenn somit das "Alter" eines Objekts verschlüsselter Einfahrtsdaten größer ist als das Zeitfenster, dann kann es sich nicht um eine Geschwindigkeitsüberschreitung (Delikt) handeln, und diese Einfahrtsdaten werden gelöscht (verworfen) und damit auch niemals entschlüsselt. Ein regelkonformes Fahrzeug hinterläßt somit keine identifizierbaren Spuren im System, was höchste Datensicherheit gewährleistet.

[0015] Bevorzugt wird bei dieser Ausführungsform auch eine erfaßte Ausfahrtskennung verworfen, wenn sich dazu keine damit entschlüsselbaren Einfahrtsdaten in der Menge von bereitgestellten Einfahrtsdaten ermitteln lassen, so daß sich an der Ausfahrt keine "unzuordenbaren" Ausfahrtskennungen anhäufen.

[0016] In einer einfachen Ausführungsform der Erfindung können die erfaßten Ausfahrtskennungen an allen vorhandenen verschlüsselten Einfahrtsdaten "ausprobiert" werden, "bis der Schlüssel paßt".

[0017] In einer bevorzugten Ausführungsform der Erfindung werden die verschlüsselten Einfahrtsdaten unter einem aus der Einfahrtskennung berechneten Hashwert bereitgestellt und es wird aus der Ausfahrtskennung auf dieselbe Weise ein Hashwert berechnet, anhand dessen die unter diesem Hashwert bereitgestellten verschlüsselten Einfahrtsdaten ermittelt werden. Auf diese Weise sind die verschlüsselten Einfahrtsdaten jeweils durch den genannten Hashwert identifiziert, sodaß bei der Entschlüsselung die Ausfahrtskennung nicht mehr an allen Einfahrtsdaten durchprobiert werden muß, sondern sofort auf die durch den Hashwert identifizierten Einfahrtsdaten zugegriffen werden kann.

[0018] Unter einem "Hashwert" wird in der vorliegenden Beschreibung eine praktisch unumkehrbare n:1-Abbildungsfunktion verstanden, d.h. eine Funktion, die nur (extrem) vieldeutig umkehrbar ist, sodaß aus der Kenntnis des Hashwerts praktisch nicht mehr auf den Ausgangswert geschlossen werden kann. Beispiele solcher Hashfunktionen sind die Quersummenfunktion, die Modulofunktion usw.

[0019] Letztgenannte Variante der Erfindung ermöglicht auch eine alternative Ausführung der Section Control: Dazu werden zu jedem Hashwert auch die Ein- bzw. Ausfahrtszeit des Fahrzeugs aufgezeichnet und die verschlüsselten Einfahrtsdaten werden nur dann entschlüsselt, wenn die zum Hashwert gehörige Ausfahrtszeit innerhalb eines mit der zugehörigen Einfahrtszeit beginnenden Zeitfensters liegt. Diese Ausführungsform eignet sich auch für eine zeitverzögerte bzw. Offline-Auswertung der Einfahrtsdaten-Objekte, weil anstelle der aktuellen Zeit die mittels des Hashwerts zuordenbare Ausfahrtszeit berücksichtigt werden kann.

[0020] Bevorzugt kann dabei aus der Einfahrts- und Ausfahrtszeit eines Fahrzeugs und der Streckenlänge zwischen Ein- und Ausfahrt auch gleich seine Geschwindigkeit ermittelt werden.

[0021] Als Kennung des Fahrzeugs kann jedes für eine Identifizierung geeignete Merkmal des Fahrzeugs verwendet werden, z.B. eine fernauslesbare Fahrgestellnummer, eine Funk-Kennung eines mitgeführten RFID-Transponderchips usw. Bevorzugt ist die Kennung einfach das Fahrzeugkennzeichen und wird durch optische Zeichenerkennung (optical character recognition, OCR) in Einfahrts- und Ausfahrtsbildern des Fahrzeugs erfaßt. Zweckmäßigerweise können dazu dieselben Einfahrts- und Ausfahrtsbilder verwendet werden, welche auch zu Beweiszwecken archiviert werden, sodaß an der Ein- und Ausfahrt jeweils nur eine einzige Bildaufnahme erforderlich ist.

[0022] Gemäß einer weiteren bevorzugten Ausführungsform der Erfindung erfolgt das genannte Verschlüsseln und Bereitstellen der Einfahrtsdaten in einer Einfahrtsstation, das genannte Erfassen der Ausfahrtskennung in einer Ausfahrtsstation, und das genannte Entschlüsseln der Einfahrtsdaten und Validieren der entschlüsselten Daten in einer gesonderten Auswertestation. Dadurch können sowohl die Einfahrts- als auch die Ausfahrtsstation z.B. in der Art von Black Boxes versiegelt und datenschutzzertifiziert werden; da sie jeweils nur Teilinformationen verarbeiten, sind sie hinsichtlich der Gefahr einer unzulässigen Erstellung von Bewegungsprofilen unbedenklich. Die Auswertestation kann überdies so aufgebaut werden, daß sie völlig autark ist und damit gesondert zertifiziert werden kann.

[0023] Die Funktionen der Auswertestation können alternativ auch ganz oder teilweise in die Ausfahrtsstation integriert sein.

[0024] In jedem Fall ist es besonders günstig, wenn beim Verschlüsseln der Einfahrtsdaten die als Schlüssel verwendete Einfahrtskennung mit weiteren Schlüsseln ergänzt wird, welche für das Entschlüsseln gesondert bereitgestellt werden. Solche weiteren Schlüssel können z.B. ein Zeitstempel, ein temporärer Schlüssel, eine Kennung der Einfahrtsstation oder ein öffentlicher Schlüssel der Ausfahrtsstation sein, wodurch die Datensicherheit auf den Übertragungswegen noch weiter erhöht werden kann.

[0025] Die Erfindung wird nachstehend anhand von in den beigeschlossenen Zeichnungen dargestellten Ausführungsbeispielen näher erläutert. In den Zeichnungen zeigen

die Fig. 1a - 1d verschiedene Ausführungsformen der am Verfahren der Erfindung beteiligten Komponenten in Blockdiagrammform; und

Fig. 2 eine Ausführungsform des Verfahrens der Erfindung in Flußdiagrammform.

[0026] Fig. 1a zeigt ein Fahrzeug 1, das einen Streckenabschnitt 2 der Länge L von einer Einfahrt 3 bis zu einer Ausfahrt 4 durchfährt. Das Fahrzeug 1 besitzt eine eindeutige Kennung 5, beispielsweise in Form seines

Fahrzeugkennzeichens ("License Plate Number", LPN), im gezeigten Beispiel "(A) W-123". Die Kennung 5 könnte alternativ auch durch andere Merkmale des Fahrzeugs 1 gebildet sein, z.B. eine maschinenlesbare Fahrgestellnummer, eine fernauslesbare Funkkennung, z.B. RFID-Kennung, usw.

[0027] An der Einfahrt 3 wird die Kennung 5 des Fahrzeugs 1 zunächst als sog. Einfahrtskennung 6 ("License Plate Number Start", LPS) erfaßt. Die Erfassung kann beispielsweise durch Fernauslesen oder bevorzugt durch optische Zeichenerkennung (OCR) der Kennung 5 in einer Bildaufnahme PIC des Fahrzeugs 1 bei der Einfahrt 3 ("Einfahrtsbild") erfolgen.

[0028] Mit Hilfe ebendieser Einfahrtskennung 6 werden nun Daten 7 zu verschlüsselten Einfahrtsdaten 8 (im weiteren auch "Einfahrtsdaten-Objekt" bzw. "encrypted section control object" genannt) verschlüsselt. Die Daten 7 können dabei verschiedener Art sein: Im einfachsten Fall genügt hiefür eine Vorgabe beliebigen bekannten Werts DAT, welche bei der späteren Entschlüsselung wiedergewonnen werden kann und damit den Erfolg der Entschlüsselung ("der Schlüssel paßt") anzeigt. Die Vorgabe kann aber auch eine Identifikation GID der Einfahrt 3 ("Gate-ID") sein oder umfassen. Alternativ oder zusätzlich können die Daten 7 auf die Kennung 5 der Fahrzeugs 1 bezogen (zurückzuführen) sein. In letzterem Fall können die Daten 7 z.B. die Einfahrtskennung 6 selbst oder das Einfahrtsbild PIC enthalten, aus dem sich z.B. mittels OCR die Einfahrtskennung 6 aus dem Fahrzeugkennzeichen LPN ermitteln läßt.

[0029] Die Einfahrtskennung 6, d.h. die bei der Einfahrt 3 erfaßte Kennung 5 des Fahrzeugs 1, wird somit selbst als Schlüssel 9 für die Verschlüsselung verwendet. Für die Verschlüsselung kann jedes in der Technik bekannte Verschlüsselungsverfahren verwendet werden.

[0030] Nach dem Verschlüsseln der Einfahrtsdaten 8 kann die Einfahrtskennung 6 bzw. der daraus gebildete Schlüssel 9 vernichtet werden.

[0031] Die Fig. 1b - 1d zeigen Varianten für die Generierung des Schlüssels 9 aus der Einfahrtskennung 6. Im Fall von Fig. 1b wird der Schlüssel 9 z.B. aus Abwandlungen, Wiederholungen oder Funktionen der Einfahrtskennung 6 gebildet, um die Schlüssellänge zu erhöhen.

[0032] Bei den Varianten der Fig. 1c und 1d wird der Schlüssel 9 aus der mit weiteren Schlüsseln ergänzten Einfahrtskennung 6 gebildet, um jeweils die Länge des Schlüssels 9 und die Datensicherheit zu erhöhen. Diese weiteren Schlüssel können z.B. ein Zeitstempel TS ("Timestamp_StartGate"), ein (beliebiger) temporärer Schlüssel 11 der Einfahrt ("StartGate_tempID"), eine Kennung der Einfahrt 3 ("StartGate_ID"), oder ein öffentlicher Schlüssel 13 der Ausfahrt 4 ("PublicKey_EndGate") sein.

[0033] Wie aus Fig. 1a ersichtlich, können die verschlüsselten Einfahrtsdaten 8 optional mit einem Hashwert h1 versehen bzw. unter diesem für die weiteren Verfahrensschritte bereitgestellt werden. Der Hashwert h1 wird in einer - wie eingangs erörtert - praktisch unumkehrbaren Weise aus der Einfahrtskennung 6 gebildet und erleichtert die Identifizierung der verschlüsselten Einfahrtsdaten 8 bei der späteren Entschlüsselung und Auswertung, wie später noch erläutert wird.

[0034] Nachdem das Fahrzeug 1 den Streckenabschnitt 2 durchfahren hat, wird an der Ausfahrt 4 erneut das Kennzeichen 5 des Fahrzeugs 1 als sog. Ausfahrtskennung 15 erfaßt. Die Erfassung kann wieder auf jede beliebige Art und Weise erfolgen, z.B. durch Fernauslesen oder bevorzugt durch optische Zeichenerkennung des Fahrzeugkennzeichens 5 in einer Bildaufnahme des Fahrzeugs 1 bei der Ausfahrt 4 ("Ausfahrtsbild").

[0035] Da das Fahrzeug 1 auf seinem Weg von der Einfahrt 3 zur Ausfahrt 4 seine Kennung 5 nicht verändert und damit die Einfahrtskennung 6 gleich der Ausfahrtskennung 15 ist, kann die Ausfahrtskennung 15 zur Entschlüsselung der verschlüsselten Einfahrtsdaten 8 verwendet werden. Je nach Variante der Fig. 1a, 1b, 1c und 1d ist dazu die Ausfahrtskennung 15 in entsprechender Weise zum Schlüssel 9 zu ergänzen, sei es durch entsprechende Funktionsabbildung (Fig. 1b), Ergänzung mit einem zu den Einfahrtsdaten 8 erhaltenen Zeitstempel TS, einem von der Einfahrt 3 auf einem gesonderten Übertragungsweg 16 erhaltenen temporären Schlüssel 11, einer Kennung der Einfahrt 3, einem zum öffentlichen Schlüssel 13 passenden privaten Schlüssel ("PrivateKey_EndGate") der Ausfahrt 4, usw.

[0036] Im praktischen Betrieb, wenn eine Vielzahl von Fahrzeugen 1 von der Einfahrt 3 zur Ausfahrt 4 fährt, fällt auch eine Vielzahl von verschlüsselten Einfahrtsdaten(-Objekten) 8 an. Im einfachsten Fall kann zur Entschlüsselung die Ausfahrtskennung 15 bzw. der daraus gebildete Schlüssel 9 an jedem vorhandenen Objekt von verschlüsselten Einfahrtsdaten 8 "ausprobiert" werden, "bis der Schlüssel paßt".

[0037] Bevorzugt werden jedoch die genannten Hashwerte h1 verwendet, unter denen die verschlüsselten Einfahrtsdaten 8 bereitgestellt werden. Dazu wird aus der Ausfahrtskennung 15 - und zwar in derselben Weise wie der Hashwert h1 aus der Einfahrtskennungen 6 - ein Hashwert h2 gebildet. Mit Hilfe des Hashwerts h2 können die unter dem gleichen Hashwert h1 bereitgestellten verschlüsselten Einfahrtsdaten 8 sofort, ohne Probieren, ermittelt werden.

[0038] Mit Hilfe der Ausfahrtskennung 15 bzw. des daraus gebildeten Schlüssels 9 werden die als passend bzw. zugehörig (h1=h2) ermittelten Einfahrtsdaten 8 nun entschlüsselt und daraus auch die Daten 7 wiedergewonnen. Durch Validieren der Daten 7 z.B. wenn sie eine Vorgabe DAT bzw. GID enthalten gegenüber dem bekannten Wert DAT bzw. einer gültigen Gate-ID oder wenn sie die Einfahrtskennung 6 (direkt oder aus dem Einfahrtsbild PIC ableitbar) enthalten gegenüber der Ausfahrtskennung 15 kann bei erfolgreicher Validierung auf eine Durchfahrt eines Fahrzeugs 1 mit der Kennung 5 von der Einfahrt 3 zur Ausfahrt 4 geschlossen werden.

[0039] Wenn bei der Ein- und Ausfahrt 3, 4 jeweils auch die Einfahrtszeit TS und die Ausfahrtszeit TE miterfaßt

wird, kann die Verweildauer das Fahrzeugs 1 auf dem Streckenabschnitt 2 und - in Kenntnis der Länge L des Streckenabschnitts 2 - auch die Geschwindigkeit des Fahrzeugs 1 im Streckenabschnitt 2 ermittelt werden ("Section Control").

[0040] Bevorzugt werden die Ein- und Ausfahrtszeiten TS, TE auch für die Steuerung des Verfahrensablaufs herangezogen, und zwar in der folgenden Art und Weise.

[0041] Die Einfahrtsdaten 8, d.h. jedes Einfahrtsdaten-Objekt 8, werden bzw. wird jeweils auch mit der Einfahrtszeit TS des Fahrzeugs 1 versehen. Sobald ein Einfahrtsdaten-Objekt 8 ein vorgegebenes Alter überschreitet, d.h. die aktuelle Zeit größer ist als ein mit der Einfahrtszeit TS beginnendes Zeitfenster ΔT, wird das betreffende Einfahrtsdaten-Objekt 8 aus der Menge der aller bereitgestellten Einfahrtsdaten-Objekte 8 gelöscht. Das Zeitfenster ΔT wird durch die zulässige Höchstgeschwindigkeit V_{max} auf dem Streckenabschnitt 2 definiert, d.h. $\Delta T = L/V_{max}$. Bei einem "zu alten", d.h. das Zeitfenster ΔT überschreitenden Einfahrtsdaten-Objekt 8 handelt es sich daher um Einfahrtsdaten eines regelkonformen, die zulässige Höchstgeschwindigkeit nicht überschreitenden Fahrzeugs 1, so daß eine Entschlüsselung nicht erforderlich ist. Ein Fahrzeug, das kein Geschwindigkeitsdelikt begeht, hinterläßt somit keine identifizierbaren Spuren im System.

[0042] Ausfahrtskennungen 15, zu denen sich keine damit entschlüsselbaren Einfahrtsdaten 8 in der Menge aller bereitgestellten Einfahrtsdaten (-Objekte) 8 finden lassen, können ebenfalls verworfen werden.

[0043] Gemäß einer alternativen (oder zusätzlichen) Variante des Verfahrens können für diesen Zeitvergleich auch die Hashwerte ausgenützt werden. Bei der Zuordnung und Ermittlung der Einfahrtsdaten 8 anhand des Vergleichs der Hashwerte h1 und h2 werden nur jene Einfahrtsdaten 8 in Betracht gezogen und in weiterer Folge entschlüsselt, deren Ein- und Ausfahrtszeiten TS, TE innerhalb des Zeitfensters ΔT liegen. Dadurch kann das Alter der Einfahrtsdaten-Objekte 8 auch zu einem späteren Zeitpunkt, z.B. offline oder in einer gesonderten Auswertestation, berechnet werden.

[0044] In einer praktischen Ausführungsform wird in der Einfahrtsstation aus der Einfahrtszeit TS und dem Zeitfenster ΔT eine zulässige Mindest-Ankunftszeit TEC (Time-stamp_End_Calculated) berechnet und (gleich anstelle der Einfahrtszeit TS) mit dem Hashwert h1 und den verschlüsselten Einfahrtsdaten 8 bereitgestellt. Wenn die zu einem Hashwert h2 (=h1) zugehörige Ausfahrtszeit TE nun vor der Mindest-Ankunftszeit TEC ist, liegt offensichtlich eine Geschwindigkeitsüberschreitung vor und die Einfahrtsdaten 8 werden entschlüsselt. In diesem Fall werden auch die Ausfahrtskennung 15 = Einfahrtskennung 6 = Kennung 5 des Fahrzeugs 1 zusammen mit dem Einfahrtsbild PIC und dem Ausfahrtsbild zu Beweiszwecken archiviert, z.B. um eine Strafe wegen Geschwindigkeitsüberschreitung verhängen zu können. Wenn anderseits die tatsächliche Ausfahrtszeit TE nach der zulässigen Mindest-Ankunftszeit TEC liegt, d.h. außerhalb des Zeitfensters ΔT, dann handelt es sich um ein regelkonformes, die zulässige Höchstgeschwindigkeit nicht überschreitendes Fahrzeug 1 und die verschlüsselten Einfahrtsdaten 8 und die Ausfahrtskennung 15 werden sofort gelöscht.

[0045] Die genannten Schritte des Verfahrens werden bevorzugt in unterschiedlichen Entitäten ausgeführt. Das Erfassen der Einfahrtskennung 6, Verschlüsseln der Daten 7 zu den verschlüsselten Einfahrtsdaten 8 und Bilden des Hashwerts h1 wird bevorzugt in einer Station an der Einfahrt 3 ("Einfahrtsstation") durchgeführt. Das Erfassen der Ausfahrtskennung 15 und Bilden des Hashwerts h2 wird bevorzugt in einer Station an der Ausfahrt 4 ("Ausfahrtsstation") durchgeführt. Das Ermitteln der zu einer Ausfahrtskennung 15 passenden verschlüsselten Einfahrtsdaten 8 durch Probieren bzw. durch Verwenden der Hashwerte h1=h2, das Entschlüsseln der Einfahrtsdaten 8 und das Auswerten der Daten 7, z.B. Validieren gegenüber der Vorgabe DAT/GID bzw. der Ausfahrtskennung 15, wird bevorzugt in einer sowohl von der Einfahrtsstation 3 als auch von der Ausfahrtsstation 4 gesonderten Auswertestation 20 (Fig. 2) durchgeführt.

[0046] Fig. 2 zeigt eine praktische Ausführungsform des Verfahrens anhand eines Flußdiagramms unter Verwendung der folgenden Abkürzungen:

TS	Timestamp_Start
TEC	Timestamp_End_Calculated
LPS	Einfahrtskennung 6
LPE	Ausfahrtskennung 15
m1	Daten 7 (unverschlüsselt)
m2	Ausfahrtsdaten 15 (unverschlüsselt)
c1	Einfahrtsdaten 8 (verschlüsselt)
E	Verschlüsselungsfunktion
D	Entschlüsselungsfunktion
H	Hashfunktion
h1	Hashwert von 6
h2	Hashwert von 15
21	Temporärer Prozeßspeicher
22	Archivspeicher für Beweisdaten

[0047] Die Erfindung ist nicht auf die dargestellten Ausführungsbeispiele beschränkt, sondern umfaßt alle Varianten und Modifikationen, die in den Rahmen der angeschlossenen Ansprüche fallen.

Patentansprüche

1. Verfahren zur Erfassung von Durchfahrten von Fahrzeugen (1) mit eindeutigen Kennungen (5) von einer Einfahrt (3) zu einer Ausfahrt (4), mit den Schritten:

   Erfassen der Kennung (5) eines Fahrzeugs (1) an der Einfahrt (3) als Einfahrtskennung (6), Verschlüsseln vorgegebener und/oder fahrzeugkennungsbezogener Daten (7) mit Hilfe der Einfahrtskennung (6) zu verschlüsselten Einfahrtsdaten (8), Bereitstellen der verschlüsselten Einfahrtsdaten (8), und Vernichten der Einfahrtskennung (6);
   Erfassen der Kennung (5) eines Fahrzeugs (1) an der Ausfahrt (4) als Ausfahrtskennung (15), Ermitteln der bereitgestellten verschlüsselten Einfahrtsdaten (8) und Entschlüsseln der verschlüsselten Einfahrtsdaten (8) mit Hilfe der Ausfahrtskennung (15), um die genannten Daten (7) zu erhalten; und
   Validieren der genannten Daten (7) gegenüber ihrer Vorgabe (DAT, GID) bzw. der Ausfahrtskennung (15), wobei eine erfolgreiche Validierung die Durchfahrt des Fahrzeugs (1) anzeigt.

2. Verfahren nach Anspruch 1 unter Verwendung vorgegebener Daten, **dadurch gekennzeichnet, daß** diese Daten (7) eine Identifikation (GID) der Einfahrt (3) umfassen.

3. Verfahren nach Anspruch 1 oder 2 unter Verwendung fahrzeugkennungsbezogener Daten, **dadurch gekennzeichnet, daß** diese Daten (7) die Einfahrtskennung (6) umfassen.

4. Verfahren nach einem der Ansprüche 1 bis 3 unter Verwendung fahrzeugkennungsbezogener Daten, **dadurch gekennzeichnet, daß** diese Daten (7) ein Einfahrtsbild (PIC) des Fahrzeugs (1) umfassen, aus dem die Einfahrtskennung (6) ableitbar ist.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, daß** das beim Entschlüsseln der Einfahrtsdaten (8) gewonnene Einfahrtsbild (PIC) zusammen mit einem Ausfahrtsbild und der Kennung (5) des Fahrzeugs (1) zu Beweiszwecken archiviert (22) wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, daß** die Einfahrtsdaten (8) mit der Einfahrtszeit (TS) des Fahrzeugs (1) versehen und aus der Menge der bereitgestellten Einfahrtsdaten (8) gelöscht werden, sobald die aktuelle Zeit ein mit der Einfahrtszeit (TS) beginnendes Zeitfenster (ΔT) überschreitet.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, daß** eine erfaßte Ausfahrtskennung (15) verworfen wird, wenn sich dazu keine damit entschlüsselbaren Einfahrtsdaten (8) in der Menge von bereitgestellten Einfahrtsdaten (8) ermitteln lassen.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, daß** die verschlüsselten Einfahrtsdaten (8) unter einem aus der Einfahrtskennung (6) berechneten Hashwert (h1) bereitgestellt und aus der Ausfahrtskennung (15) auf dieselbe Weise ein Hashwert (h2) berechnet wird, anhand dessen die unter diesem Hashwert (h2, h1) bereitgestellten verschlüsselten Einfahrtsdaten (8) ermittelt werden.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, daß** zu jedem Hashwert (h1, h2) auch die jeweilige Ein- bzw. Ausfahrtszeit (TS, TE) des Fahrzeugs (1) aufgezeichnet wird und die verschlüsselten Einfahrtsdaten (8) nur dann entschlüsselt werden, wenn die zum Hashwert (h1, h2) gehörige Ausfahrtszeit (TE) innerhalb eines mit der zugehörigen Einfahrtszeit (TS) beginnenden Zeitfensters (ΔT) liegt.

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, daß** aus der Einfahrts- und Ausfahrtszeit (TS, TE) eines Fahrzeugs (1) und der Streckenlänge zwischen Ein- und Ausfahrt (3, 4) seine Geschwindigkeit ermittelt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, daß** die Kennung (5) das Fahrzeugkennzeichen (LPN) ist und durch optische Zeichenerkennung in Einfahrts-(PIC) und Ausfahrtsbildern des Fahrzeugs (1) erfaßt wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, daß** das genannte Verschlüsseln und Bereitstellen der Einfahrtsdaten (8) in einer Einfahrtsstation (3) erfolgt, das genannte Erfassen der Ausfahrtskennung (15) in einer Ausfahrtsstation (4) erfolgt, und das genannte Entschlüsseln der Einfahrtsdaten (8) und Validieren der entschlüsselten Daten (7) in einer gesonderten Auswertestation (20) erfolgt.

13. Verfahren nach einem der Ansprüche 1 bis 12, **dadurch gekennzeichnet, daß** beim Verschlüsseln der Einfahrtsdaten (8) die als Schlüssel (9) verwendete Einfahrtskennung (6) mit weiteren Schlüsseln (TS, 11, 13) ergänzt wird, welche für das Entschlüsseln gesondert bereitgestellt werden.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet, daß** die weiteren Schlüssel einen Zeitstempel (TS), einen temporären Schlüssel (11), eine Kennung der Einfahrtsstation (3) oder einen öffent-

lichen Schlüssel (13) der Ausfahrtsstation (4) umfassen.

Geänderte Patentansprüche gemäss Regel 137(2) EPÜ.

1. Verfahren zur Erfassung von Durchfahrten von Fahrzeugen (1) mit eindeutigen Kennungen (5) von einer Einfahrt (3) zu einer Ausfahrt (4), mit den Schritten:

Erfassen der Kennung (5) eines Fahrzeugs (1) an der Einfahrt (3) als Einfahrtskennung (6), Verschlüsseln vorgegebener und/oder fahrzeugkennungsbezogener Daten (7) mit Hilfe der Einfahrtskennung (6) zu verschlüsselten Einfahrtsdaten (8), Bereitstellen der verschlüsselten Einfahrtsdaten (8), und Vernichten der Einfahrtskennung (6);
Erfassen der Kennung (5) eines Fahrzeugs (1) an der Ausfahrt (4) als Ausfahrtskennung (15), Ermitteln der bereitgestellten verschlüsselten Einfahrtsdaten (8) und Entschlüsseln der verschlüsselten Einfahrtsdaten (8) mit Hilfe der Ausfahrtskennung (15), um die genannten Daten (7) zu erhalten; und
Validieren der genannten Daten (7) gegenüber ihrer Vorgabe (DAT, GID) bzw. der Ausfahrtskennung (15), wobei eine erfolgreiche Validierung die Durchfahrt des Fahrzeugs (1) anzeigt,

dadurch gekennzeichnet, daß die Einfahrtsdaten (8) mit der Einfahrtszeit (TS) des Fahrzeugs (1) versehen und aus der Menge der bereitgestellten Einfahrtsdaten (8) gelöscht werden, sobald die aktuelle Zeit ein mit der Einfahrtszeit (TS) beginnendes Zeitfenster (ΔT) überschreitet.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** eine erfaßte Ausfahrtskennung (15) verworfen wird, wenn sich dazu keine damit entschlüsselbaren Einfahrtsdaten (8) in der Menge von bereitgestellten Einfahrtsdaten (8) ermitteln lassen.

3. Verfahren nach Anspruch 1 oder 2 unter Verwendung vorgegebener Daten, **dadurch gekennzeichnet, daß** diese Daten (7) eine Identifikation (GID) der Einfahrt (3) umfassen.

4. Verfahren nach einem der Ansprüche 1 bis 3 unter Verwendung fahrzeugkennungsbezogener Daten, **dadurch gekennzeichnet, daß** diese Daten (7) die Einfahrtskennung (6) umfassen.

5. Verfahren nach einem der Ansprüche 1 bis 4 unter Verwendung fahrzeugkennungsbezogener Daten, **dadurch gekennzeichnet, daß** diese Daten (7) ein Einfahrtsbild (PIC) des Fahrzeugs (1) umfassen, aus dem die Einfahrtskennung (6) ableitbar ist.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, daß** das beim Entschlüsseln der Einfahrtsdaten (8) gewonnene Einfahrtsbild (PIC) zusammen mit einem Ausfahrtsbild und der Kennung (5) des Fahrzeugs (1) zu Beweiszwecken archiviert (22) wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, daß** die verschlüsselten Einfahrtsdaten (8) unter einem aus der Einfahrtskennung (6) berechneten Hashwert (h1) bereitgestellt und aus der Ausfahrtskennung (15) auf dieselbe Weise ein Hashwert (h2) berechnet wird, anhand dessen die unter diesem Hashwert (h2, h1) bereitgestellten verschlüsselten Einfahrtsdaten (8) ermittelt werden.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, daß** zu jedem Hashwert (h1, h2) auch die jeweilige Ein- bzw. Ausfahrtszeit (TS, TE) des Fahrzeugs (1) aufgezeichnet wird und die verschlüsselten Einfahrtsdaten (8) nur dann entschlüsselt werden, wenn die zum Hashwert (h1, h2) gehörige Ausfahrtszeit (TE) innerhalb eines mit der zugehörigen Einfahrtszeit (TS) beginnenden Zeitfensters (ΔT) liegt.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, daß** aus der Einfahrts- und Ausfahrtszeit (TS, TE) eines Fahrzeugs (1) und der Streckenlänge zwischen Ein- und Ausfahrt (3, 4) seine Geschwindigkeit ermittelt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, daß** die Kennung (5) das Fahrzeugkennzeichen (LPN) ist und durch optische Zeichenerkennung in Einfahrts-(PIC) und Ausfahrtsbildern des Fahrzeugs (1) erfaßt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, daß** das genannte Verschlüsseln und Bereitstellen der Einfahrtsdaten (8) in einer Einfahrtsstation (3) erfolgt, das genannte Erfassen der Ausfahrtskennung (15) in einer Ausfahrtsstation (4) erfolgt, und das genannte Entschlüsseln der Einfahrtsdaten (8) und Validieren der entschlüsselten Daten (7) in einer gesonderten Auswertestation (20) erfolgt.

12. Verfahren nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, daß** beim Verschlüsseln der Einfahrtsdaten (8) die als Schlüssel (9) verwendete Einfahrtskennung (6) mit weiteren Schlüsseln (TS, 11, 13) ergänzt wird, welche für das Entschlüsseln gesondert bereitgestellt werden.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet, daß** die weiteren Schlüssel einen Zeitstempel (TS), einen temporären Schlüssel (11), eine Kennung der Einfahrtsstation (3) oder einen öffentlichen Schlüssel (13) der Ausfahrtsstation (4) umfassen.

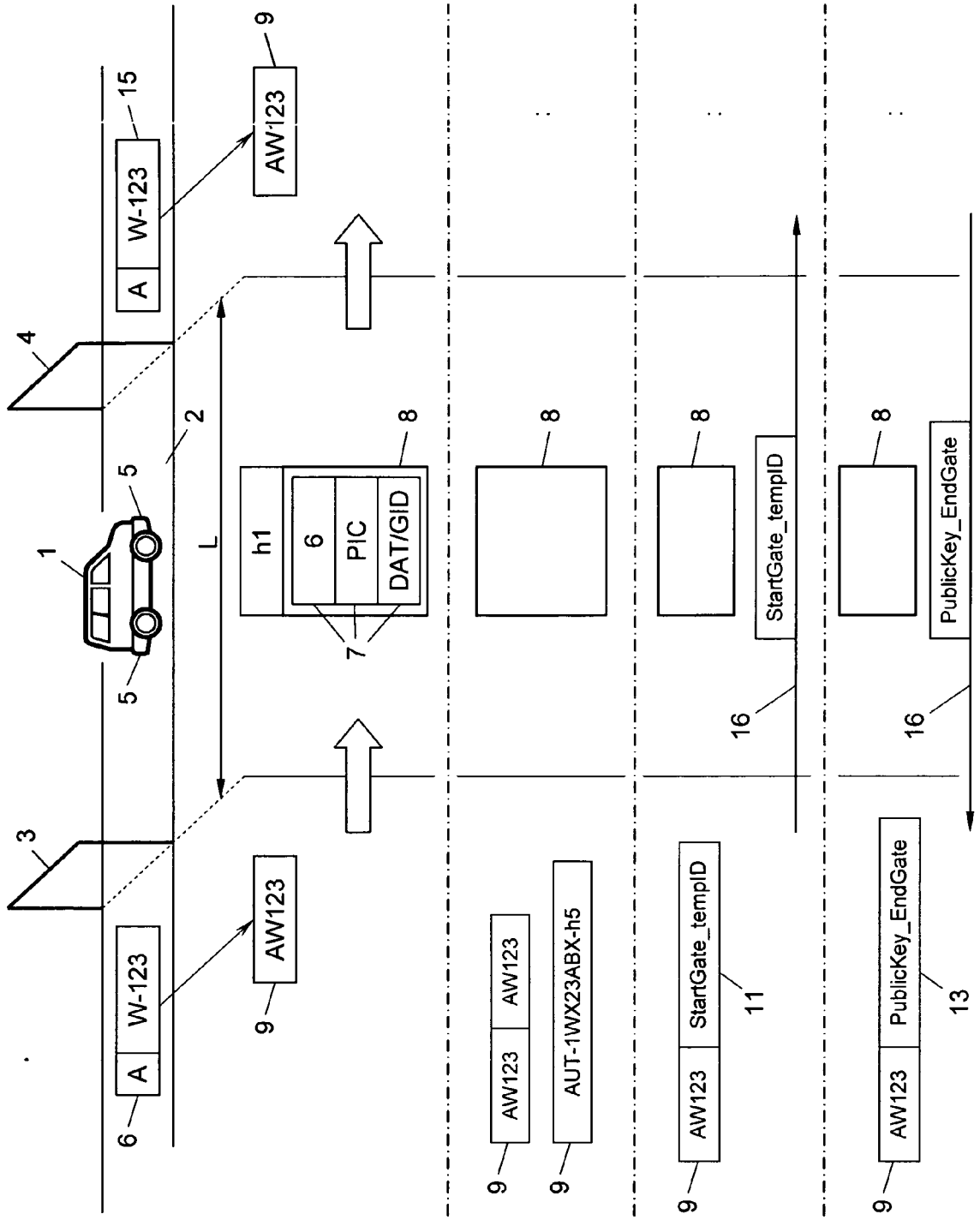


Fig. 1a

Fig. 1b

Fig. 1c

Fig. 1d

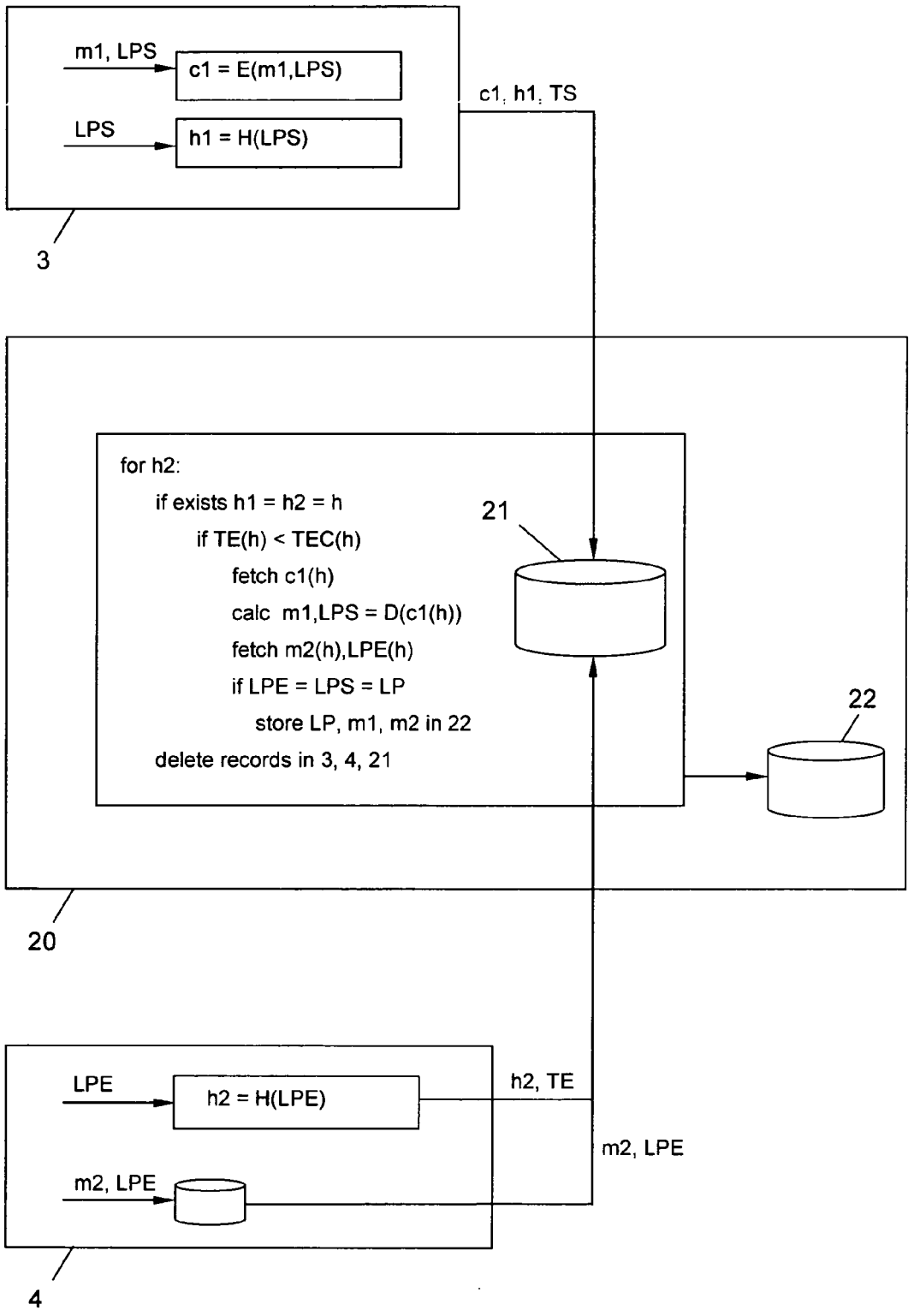

m1, LPS
c1 = E(m1,LPS)
LPS
h1 = H(LPS)
c1, h1, TS
3
for h2:
if exists h1 = h2 = h
if TE(h) < TEC(h)
fetch c1(h)
calc m1,LPS = D(c1(h))
fetch m2(h),LPE(h)
if LPE = LPS = LP
store LP, m1, m2 in 22
delete records in 3, 4, 21
21
22
20
LPE
h2 = H(LPE)
h2, TE
m2, LPE
m2, LPE
4

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 10 45 0005

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	DE 10 2007 059346 A1 (SIEMENS AG [DE]) 18. Juni 2009 (2009-06-18) * Zusammenfassung; Ansprüche; Abbildung * * Absätze [0001], [0002], [0007] - [0014], [0016] - [0026], [0030], [0037], [0041], [0042] - [0046], [0048] - [0054] * -----	1-14	INV. G07B15/02 G08G1/017 G08G1/054
A	DE 10 2005 036562 A1 (SIEMENS AG [DE]) 15. Februar 2007 (2007-02-15) * Zusammenfassung; Anspruch 1; Abbildung * * Absätze [0007] - [0013], [0016] - [0025] * -----	1-14	
A	EP 0 978 811 A2 (SIEMENS AG [DE]) 9. Februar 2000 (2000-02-09) * Zusammenfassung; Ansprüche 1,2,3,4,6; Abbildungen 1,2 * * Absätze [0017] - [0025] * -----	1-14	
A	US 6 081 206 A (KIELLAND PETER J [CA]) 27. Juni 2000 (2000-06-27) * das ganze Dokument * -----	1	RECHERCHIERTE SACHGEBIETE (IPC) G07B G08G
A	AT 8 939 U1 (SIEMENS AG OESTERREICH [AT]) 15. Februar 2007 (2007-02-15) * Seiten 2-6; Anspruch 1; Abbildung 1 * -----	1	

1 Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	29. März 2010	Rother, Stefan

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)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.

EP 10 45 0005

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.

29-03-2010

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102007059346 A1	18-06-2009	WO 2009074436 A1	18-06-2009
DE 102005036562 A1	15-02-2007	KEINE	
EP 0978811 A2	09-02-2000	KEINE	
US 6081206 A	27-06-2000	AU 6287498 A	12-10-1998
		CA 2199999 A1	14-09-1998
		WO 9841953 A1	24-09-1998
AT 8939 U1	15-02-2007	KEINE	

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

- **F. ALBRECHT.** Section Control in Deutschland. *Straßenverkehrsrecht,* 2009 **[0004]**