

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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
31. August 2006 (31.08.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/089584 A1

(51) Internationale Patentklassifikation:

H04L 29/06 (2006.01) *H04L 9/30* (2006.01)
H04L 9/08 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2005/014064

(22) Internationales Anmeldedatum:

21. Dezember 2005 (21.12.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:

10 2005 009 490.2

24. Februar 2005 (24.02.2005) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): VOLKSWAGEN AG [DE/DE]; 38436 Wolfsburg (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): CALISKAN, Murat

[DE/DE]; Rothenfelderstr. 38, 38440 Wolfsburg (DE).
AIJAZ, Amer [DE/DE]; Berliner Strasse 44, 38165 Lehre (DE). **RECH, Bernd** [DE/DE]; Bauernberg 10b, 38556 Bokendorf (DE). **LÜBKE, Andreas** [DE/DE]; Weidenkamp 12, 38442 Wolfsburg (DE).

(74) **Anwalt: EFFERT, BRESSEL UND KOLLEGEN;** Radickestrasse 48, 12489 Berlin (DE).

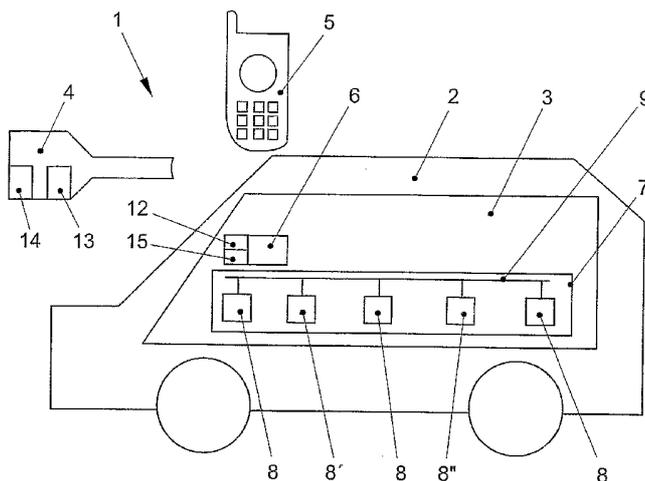
(81) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD, DEVICE, UNIT AND SYSTEM FOR PROTECTING A PRIVATE COMMUNICATIONS KEY IN A VEHICLE-ENVIRONMENT COMMUNICATION

(54) **Bezeichnung:** VERFAHREN, VORRICHTUNG, GERÄT UND SYSTEM ZUM SCHÜTZEN EINES PRIVATEN KOMMUNIKATIONSSCHLÜSSELS FÜR EINE FAHRZEUG-UMWELT-KOMMUNIKATION



(57) **Abstract:** The invention relates to a method, device (3), unit (4) and a system (1) for protecting a private communications key for a vehicle-environment communication. The invention relates to producing a pair of keys during the vehicle (2) operational phase, wherein said pair of keys consists of a private communications key and an associated public key. Said private communications key is divided into a key part and at least one vehicle part, wherein said at least one vehicle part of the private communication key is stored in at least one storage device (11) of the vehicle (2). The key part of the private communications key is transmitted to the unit (4) separated or separable from the vehicle (2) and can be stored in the other storage device (14) of the unit (4). Each representation of the key part of the private communications key in the vehicle (2) is thereby cleared.

[Fortsetzung auf der nächsten Seite]

WO 2006/089584 A1



GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— mit internationalem Recherchenbericht

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren, eine Vorrichtung (3), ein Gerät (4) und ein System (1) zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation. Es wird das Erzeugen eines Schlüsselpaars während einer Betriebsphase eines Fahrzeugs (2) vorgeschlagen, wobei das Schlüsselpaar den privaten Kommunikationsschlüssel und einen dazugehörigen öffentlichen Kommunikationsschlüssel umfasst. Der private Kommunikationsschlüssel wird in einen Schlüsselteil und mindestens einen Fahrzeugteil geteilt, wobei der mindestens eine Fahrzeugteil des privaten Kommunikationsschlüssels in mindestens einer Speichervorrichtung (11) des Fahrzeugs (2) gespeichert wird. Der Schlüsselteil des privaten Kommunikationsschlüssels wird zu einem von dem Fahrzeug (2) getrennten oder von dem Fahrzeug (2) trennbaren Gerät (4), insbesondere einem Fahrzeugschlüssel, übertragen und in einer weiteren Speichervorrichtung (14) des Geräts (4) gespeichert. Ferner wird jede Repräsentation des Schlüsselteils des privaten Kommunikationsschlüssels in dem Fahrzeug (2) gelöscht.

Verfahren, Vorrichtung, Gerät und System zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation

Die Erfindung betrifft ein Verfahren, eine Vorrichtung, ein Gerät und ein System zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation.

Bei einer Fahrzeug-Umwelt-Kommunikation werden Informationen und/oder Daten zwischen einem Fahrzeug und Kommunikationseinrichtungen in der Umgebung des Fahrzeugs ausgetauscht. Bei den Kommunikationseinrichtungen in der Umgebung des Fahrzeugs kann es sich um andere Fahrzeuge oder um ortsfeste Relais- und Sendestationen, Einrichtungen eines Verkehrsleitsystems, Erfassungseinrichtungen eines Mautsystems usw. handeln. Bei den Daten kann es sich z. B. um Daten zur Gewinnung von Verkehrsinformationen und zur dynamischen Routenoptimierung handeln. Beispiele für ein Kommunikationsnetz und für die Gewinnung von Verkehrsinformationen sind in den Druckschriften DE 102 066 98 A1 und EP 1 151 428 B1 beschrieben. Es können aber auch sicherheitsrelevante Informationen, z. B. Informationen über den Straßenzustand (beispielsweise Glatteis) zwischen Fahrzeugen ausgetauscht werden. Ferner können Informationen, die eine Identifikation des Fahrzeugs oder seiner Insassen oder seiner Ladung ermöglichen, beispielsweise an ein Mautsystem übertragen werden. Bei diesen sicherheitsrelevanten und personen- und fahrzeugbezogenen Daten ist es notwendig, diese vor einem unerwünschten Zugriff Dritter zu schützen. Daher wird die Kommunikation zwischen dem Fahrzeug und den anderen Kommunikationseinrichtungen verschlüsselt. Hierbei kommen vor allem asymmetrische Schlüsselverfahren zur Anwendung, die mit einem Schlüsselpaar, bestehend aus einem öffentlichen Kommunikationsschlüssel und einem privaten Kommunikationsschlüssel, arbeiten.

Das Fahrzeug teilt seinen öffentlichen Kommunikationsschlüssel anderen Kommunikationsteilnehmern mit. Die anderen Kommunikationsteilnehmer verschlüsseln Nachrichten an das Fahrzeug mit dem öffentlichen Kommunikationsschlüssel. In dem Fahrzeug können die verschlüsselten Nachrichten mittels des privaten Kommunikationsschlüssels entschlüsselt werden. Der private Kommunikationsschlüssel

kann ferner verwendet werden, um Nachrichten zu signieren. Hierbei kann ein Empfänger einer signierten Nachricht mittels des öffentlichen Kommunikationsschlüssels überprüfen, ob die Signatur authentisch ist.

Der private Kommunikationsschlüssel stellt bei einem asymmetrischen Verschlüsselungsverfahren eine besonders zu schützende Information dar.

Wenn eine nicht berechtigte Person den privaten Kommunikationsschlüssel einer anderen Person bzw. eines Fahrzeugs erlangt, kann diese Person mit dem privaten Kommunikationsschlüssel auf unterschiedlichste Art Schäden verursachen. Beispielsweise kann sich diese Person für die Person bzw. das Fahrzeug ausgeben (Identitätsdiebstahl) oder verschlüsselte Daten dekodieren, die für die Person oder das Fahrzeug bestimmt sind, deren oder dessen privater Kommunikationsschlüssel entwendet wurde. In der Druckschrift DE 101 41 737 C1 ist eine Kommunikationseinrichtung für ein Fahrzeug (On-Board-Unit) beschrieben, die als ein Trust Center betrieben wird und in der der private Kommunikationsschlüssel abgespeichert ist. Die On-Board-Unit stellt eine definierte Schwachstelle dieses Systems dar. Mit dem Diebstahl oder einem unbemerkten Austausch der On-Board-Unit können sich Dritte Kenntnis von dem privaten Kommunikationsschlüssel verschaffen, der in der On-Board-Unit gespeichert ist.

Die Fahrzeug-Umwelt-Kommunikation findet in der Regel über Funksignale statt, die mittels elektromagnetischer Wellen in bestimmten Frequenzbereichen übertragen werden. Geeignet ist z. B. eine Kommunikation mit Eigenschaften eines W-LAN (Wireless Lokal Area Network).

Die Kommunikationseinrichtung (On-Board-Unit) in einem Fahrzeug dient heute häufig als Zugangspunkt (Accesspoint) für Laptops und andere elektronische Geräte, die Daten über die Kommunikationseinrichtung des Fahrzeugs austauschen. Insbesondere wegen ihrer Eigenschaft, als Accesspoint eines W-LAN zu dienen, ist die Kommunikationseinrichtung besonders anfällig gegenüber einem Ausspionieren durch Dritte, da in der Netzwerkprotokollsoftware, die den Zugriff auf den Accesspoint steuert, häufig unentdeckte Sicherheitslücken sind, die einen unberechtigten Zugriff auf die Kommunikationseinrichtung durch Dritte gestatten.

Der Erfindung liegt das technische Problem zugrunde, ein Verfahren, eine Vorrichtung, ein Gerät und ein System zum Schützen eines privaten Kommunikationsschlüssels für

eine Fahrzeug-Umwelt-Kommunikation zu schaffen, bei denen der private Kommunikationsschlüssel gegenüber einem Zugriff durch unbefugte Dritte besser geschützt ist.

Das technische Problem wird durch ein Verfahren mit den Merkmalen des Patentanspruchs 1, eine Vorrichtung mit den Merkmalen des Patentanspruchs 10, ein Gerät mit den Merkmalen des Patentanspruchs 19 und ein System mit den Merkmalen des Patentanspruchs 23 gelöst. Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

Der Erfindung liegt der Gedanke zugrunde, dass der private Schlüssel zur Aufbewahrung in mindestens zwei Teile, einen Fahrzeugteil und einen so genannten Schlüsselteil, aufgeteilt wird. Der Schlüsselteil des privaten Kommunikationsschlüssels wird auf ein von dem Fahrzeug getrenntes oder von dem Fahrzeug trennbares Gerät übertragen und anschließend in dem Fahrzeug gelöscht. Hierdurch ist es selbst bei einem Zugriff auf das Fahrzeug durch einen Dritten nicht möglich, Kenntnis von dem privaten Kommunikationsschlüssel zu erlangen. Da in dem Gerät nur der Schlüsselteil gespeichert ist, kann sich eine dritte Person durch einen gezielten Diebstahl des Geräts oder bei einem Verlust des Geräts ebenfalls keine Kenntnis von dem privaten Kommunikationsschlüssel verschaffen. In einem solchen Fall fehlt der Fahrzeugteil des privaten Kommunikationsschlüssels.

Insbesondere wird vorgeschlagen: ein Verfahren zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation umfassend die Schritte:

- Erzeugen eines Schlüsselpaares während einer Betriebsphase eines Fahrzeugs, wobei das Schlüsselpaar den privaten Kommunikationsschlüssel und einen dazugehörigen öffentlichen Kommunikationsschlüssel umfasst,

wobei

- der private Kommunikationsschlüssel in einen Schlüsselteil und mindestens einen Fahrzeugteil geteilt wird, wobei der Fahrzeugteil des privaten Kommunikationsschlüssels in einer Speichervorrichtung des Fahrzeugs gespeichert wird,

- der Schlüsselteil des privaten Kommunikationsschlüssels zu einem von dem Fahrzeug getrennten oder von dem Fahrzeug trennbaren Gerät, insbesondere einem Fahrzeugschlüssel, übertragen wird und in einer weiteren Speichervorrichtung des Geräts gespeichert wird,
- jede Repräsentation des Schlüsselteils des privaten Kommunikationsschlüssels in dem Fahrzeug gelöscht wird.

Ferner ist vorteilhafterweise vorgesehen, dass der Schlüsselteil am Beginn einer nachfolgenden Betriebsphase des Fahrzeugs von dem Gerät zu dem Fahrzeug übertragen wird, der Schlüsselteil mit dem in der Speichervorrichtung des Fahrzeugs abgespeicherten mindestens einen Fahrzeugteil zu dem privaten Kommunikationsschlüssel zusammengesetzt wird und der zusammengesetzte private Kommunikationsschlüssel mittels des öffentlichen Kommunikationsschlüssels authentifiziert wird. Hierzu kann beispielsweise eine Information mittels des öffentlichen Kommunikationsschlüssels kodiert werden. Zur Authentifizierung des privaten Kommunikationsschlüssels wird überprüft, ob die kodierte Information mittels des zusammengesetzten privaten Kommunikationsschlüssels dekodiert werden kann. Ist dies der Fall, so ist der private Kommunikationsschlüssel authentifiziert. Ist dies nicht der Fall, so gehört der von dem Gerät übertragene Schlüsselteil nicht zu dem in dem Fahrzeug gespeicherten Fahrzeugteil des privaten Kommunikationsschlüssels. Handelt es sich bei dem Gerät vorteilhafterweise um einen Fahrzeugschlüssel, so kann der Schlüsselteil des privaten Kommunikationsschlüssels zusätzlich eine Schließfunktion gemeinsam mit der beschriebenen Authentifizierung übernehmen.

Die Kommunikationssicherheit für die Fahrzeug-Umwelt-Kommunikation kann weiter gesteigert werden, wenn der private Kommunikationsschlüssel nur für eine Betriebsphase des Fahrzeugs gültig ist. Eine besondere Ausgestaltung der Erfindung sieht daher vor, dass der private Kommunikationsschlüssel nur in einer Betriebsphase des Fahrzeugs gültig ist, die auf die Betriebsphase folgt, in der der private Kommunikationsschlüssel erzeugt worden ist, wobei in jeder Betriebsphase ein neues Schlüsselpaar erzeugt wird. Der besondere Vorteil dieser Ausführungsform liegt darin, dass der private Kommunikationsschlüssel der in einer Betriebsphase erzeugt wurde, sofort am Beginn der nachfolgenden Betriebsphase verwendet werden kann, um eine verschlüsselte Fahrzeug-Umwelt-Kommunikation durchzuführen. Es muss nicht die Zeit abgewartet werden, die zum Erzeugen eines

Schlüsselpaars benötigt wird. So kann beispielsweise das Fahrzeug am Anfang der nachfolgenden Betriebsphase automatisch das Öffnen eines Garagentors über eine Fahrzeug-Umwelt-Kommunikation anfordern.

Um eine Manipulation oder Ausspähung des privaten Kommunikationsschlüssels bereits während der Erzeugung des Schlüsselpaars zu erschweren, ist vorgesehen, dass das Fahrzeug eine Kommunikationseinrichtung und eine Gruppe von Steuergeräten mit jeweils einer Recheneinheit umfasst, wobei die Steuergeräte und die Kommunikationseinrichtung miteinander kommunizieren können, und wobei jedes der Steuergeräte einen Teil eines verteilten Algorithmus zum Erzeugen des privaten Kommunikationsschlüssels umfasst und der private Kommunikationsschlüssel mittels eines oder mehrerer Steuergeräte aus der Gruppe der Steuergeräte erzeugt wird. Die Erzeugung des privaten Kommunikationsschlüssels findet nicht in der Kommunikationseinrichtung statt, die besonders leicht von außen ausgespäht werden kann, wenn sie z. B. als Accesspoint in einem W-LAN arbeitet und die Protokollsoftware, die den Zugriff auf den Accesspoint steuert, unentdeckte Fehler enthält, die Dritten einen unbemerkten und/oder unberechtigten Zugriff auf Daten der Kommunikationseinrichtung gestatten. Bei den Steuergeräten kann es sich um beliebige Komponenten eines Fahrzeugs handeln, die über eine Recheneinheit verfügen, um einen Kommunikationsschlüssel oder Teile eines Kommunikationsschlüssels berechnen zu können. Die Teile des verteilten Algorithmus auf den verschiedenen Steuergeräten müssen nicht identisch sein. In der Regel wird jedes Steuergerät, welches an der Berechnung eines Schlüsselpaars beteiligt ist, nur einen Teilschlüssel erzeugen. Hierdurch wird ein Ausspähen des privaten Kommunikationsschlüssels, indem einzelne Steuergeräte des Fahrzeugs unbemerkt ausgetauscht werden, wenn dieses abgestellt ist, unmöglich gemacht.

Um eine Vorhersage zu erschweren, welches oder welche der mehreren Steuergeräte aus der Gruppe der Steuergeräte einen neuen privaten Kommunikationsschlüssel erzeugen werden, ist vorgesehen, dass das eine oder die mehreren Steuergeräte aus der Gruppe der Steuergeräte nach einem Zufallsprinzip jeweils vor dem Erzeugen des privaten Kommunikationsschlüssels und/oder des neuen privaten Kommunikationsschlüssels ausgewählt werden.

Als besonders vorteilhaft wird eine Ausführungsform angesehen, bei der der private Kommunikationsschlüssel nur auf einem nach dem Zufallsprinzip oder einem

anderen Zufallsprinzip ausgewählten Steuergerät der mehreren Steuergeräte zusammengesetzt, während der Betriebsphase und/oder der nachfolgenden Betriebsphase zwischengespeichert und gegebenenfalls in den Fahrzeugteil und den Schlüsselteil geteilt wird. Die Auswahl des Steuergeräts, welches als einziges Kenntnis von dem vollständigen privaten Kommunikationsschlüssel erlangt, kann anhand von Zufallszahlen erfolgen.

Um die Identität des Steuergeräts, welches den privaten Kommunikationsschlüssel speichert, zu verdecken, ist vorgesehen, dass die Kommunikation zwischen den Steuergeräten und/oder der Kommunikationseinrichtung und/oder dem Gerät mittels temporärer ID-Nummern erfolgt, auf die ID-Nummern der Steuergeräte und/oder der Kommunikationseinrichtung und/oder des Geräts abgebildet werden.

Um ein Abhören der Kommunikation zwischen dem Gerät und dem Fahrzeug sowie innerhalb des Fahrzeugs zu erschweren, kann die Kommunikation, einschließlich des Übertragens des privaten Kommunikationsschlüssels, des Fahrzeugteils und des Schlüsselteils des privaten Kommunikationsschlüssels, zwischen dem Gerät und dem Fahrzeug sowie innerhalb des Fahrzeugs über verschlüsselte, insbesondere symmetrisch verschlüsselte, Kommunikationsverbindungen erfolgen.

Für ein weiteres von dem Fahrzeug getrenntes oder trennbares Gerät, welches mit dem Fahrzeug kommunizieren kann, wird analog zu dem privaten Kommunikationsschlüssel ein weiterer privater Kommunikationsschlüssel erzeugt und verwendet. Bei dem weiteren Gerät kann es sich beispielsweise um einen zweiten Fahrzeugschlüssel oder ein Handy oder ein Laptop handeln, die die Accesspoint-Funktion der Kommunikationseinrichtung nutzen wollen.

Es wird ferner eine Vorrichtung zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation vorgeschlagen, die umfasst:

- eine Schlüsselerzeugungseinrichtung zum Erzeugen eines Schlüsselpaars während einer Betriebsphase eines Fahrzeugs, wobei das Schlüsselpaar den privaten Kommunikationsschlüssel und einen dazugehörigen öffentlichen Kommunikationsschlüssel umfasst,
- Teilungsmittel zum Teilen des privaten Kommunikationsschlüssels in einen Schlüsselteil und mindestens einen Fahrzeugteil, mindestens eine

Speichervorrichtung des Fahrzeugs zum Speichern des mindestens einen Fahrzeugteils des privaten Kommunikationsschlüssels,

- eine Kommunikationseinrichtung zum Übertragen des Schlüsselteils des privaten Kommunikationsschlüssels zu einem von dem Fahrzeug getrennten oder von dem Fahrzeug trennbaren Gerät, insbesondere einem Fahrzeugschlüssel, für ein Speichern des Schlüsselteils in einer weiteren Speichervorrichtung des Geräts,
- Mittel zum Löschen jeder Repräsentation des Schlüsselteils des privaten Kommunikationsschlüssels in dem Fahrzeug.

Weiterbildungen der Vorrichtung sind in den Unteransprüchen beschrieben, wobei die Merkmale dieselben Vorteile wie die entsprechenden Merkmale des erfindungsgemäßen Verfahrens aufweisen.

Weiter wird ein Gerät zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation vorgeschlagen, das ausgestaltet ist, um mit einer beschriebenen Vorrichtung zum Schützen eines privaten Kommunikationsschlüssels zusammenzuwirken. Das Gerät umfasst Kommunikationsmittel zum Austauschen eines Schlüsselteils des privaten Kommunikationsschlüssels mit dem Fahrzeug und eine weitere Speichervorrichtung zum Speichern des Schlüsselteils des privaten Kommunikationsschlüssels.

Um sicherzustellen, dass in dem Gerät jeweils nur der zuletzt von dem Fahrzeug übertragene Fahrzeugteil des privaten Kommunikationsschlüssels abgespeichert ist, ist bei einer vorteilhaften Weiterbildung vorgesehen, dass ein Fahrzeugteil des privaten Kommunikationsschlüssels beim Empfangen eines neuen Fahrzeugteils eines privaten Kommunikationsschlüssels in der weiteren Speichervorrichtung überschreibbar ist.

Für eine sichere Kommunikation mit dem Fahrzeug umfasst das Gerät weitere Verschlüsselungsmittel, so dass die Kommunikation mit dem Fahrzeug über eine verschlüsselte, insbesondere symmetrisch verschlüsselte Kommunikationsverbindung erfolgen kann.

Vorteilhafterweise ist das Gerät als Fahrzeugschlüssel ausgebildet.

Zusätzlich wird ein System zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation vorgeschlagen, das eine beschriebene Vorrichtung sowie mindestens ein beschriebenes Gerät umfasst.

Die Erfindung wird im Folgenden anhand eines bevorzugten Ausführungsbeispiels unter Bezugnahme auf eine Zeichnung näher erläutert. Hierbei zeigen:

Fig. 1 eine schematische Ansicht eines Systems zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation; und

Fig. 2 eine schematische Ansicht eines Steuergeräts.

In Fig. 1 ist schematisch ein System 1 zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation dargestellt. Ein Fahrzeug 2 umfasst eine Vorrichtung 3 zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation. Die Vorrichtung 3 wirkt mit einem Gerät 4 zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation und/oder einem weiteren Gerät 5 zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation zusammen. Das Gerät 4 ist vorzugsweise als Fahrzeugschlüssel ausgebildet. Das weitere Gerät 5 kann beispielsweise ein Handy, ein Laptop usw. sein.

Die Vorrichtung 3 zum Schützen eines privaten Kommunikationsschlüssels umfasst eine Kommunikationseinrichtung 6, über die das Fahrzeug 2 die Fahrzeug-Umwelt-Kommunikation durchführt. Kommunikationspartner des Fahrzeugs 2 können andere Fahrzeuge, Verkehrsleitsysteme, Mauterfassungssysteme usw. sein. Bei der Fahrzeug-Umwelt-Kommunikation werden zum Teil sensible Daten übertragen, die beispielsweise Auskunft über eine Identität eines Fahrers oder eine Ladung des Fahrzeugs 2 geben.

Um diese Daten zu schützen, wird die Fahrzeug-Umwelt-Kommunikation mittels eines asymmetrischen Schlüsselverfahrens verschlüsselt. Für das asymmetrische Verschlüsselungsverfahren wird ein Schlüsselpaar benötigt, das einen öffentlichen Kommunikationsschlüssel und einen privaten Kommunikationsschlüssel umfasst.

Die Vorrichtung 3 zum Schützen des privaten Kommunikationsschlüssels umfasst eine Schlüsselerzeugungseinrichtung 7. Die Schlüsselerzeugungseinrichtung 7 umfasst mehrere Steuergeräte 8. Die Steuergeräte 8 und die Kommunikationseinrichtung 6 sind

über einen Fahrzeugbus 9 miteinander verbunden. Bei dem Fahrzeugbus 9 kann es sich beispielsweise um einen CAN-, einen FlexRay- oder TTP-Bus handeln. Jedes Steuergerät 8, von denen eines schematisch in Fig. 2 dargestellt ist, umfasst eine Recheneinheit 10 und eine Speichervorrichtung 11.

Die Erzeugung des Schlüsselpaars erfolgt mittels eines verteilten Algorithmus, wobei jedes Steuergerät 8 einen Teil des verteilten Algorithmus umfasst. Die einzelnen Teile des Algorithmus können auf den Steuergeräten 8 parallel ausgeführt werden. Der verteilte Algorithmus ist so ausgestaltet, dass vor dem Erzeugen eines Schlüsselpaars nach einem Zufallsprinzip, welches bevorzugt Zufallszahlen verarbeitet, festgelegt wird, welches oder welche der Steuergeräte 8 am Erzeugen des privaten Kommunikationsschlüssels beteiligt werden. Vorzugsweise werden nicht alle Steuergeräte 8 an dem Erzeugungsprozess beteiligt. Jedes der ausgewählten Steuergeräte 8 erzeugt einen Teil des zu erzeugenden privaten Kommunikationsschlüssels. Per Zufallsauswahlmittel, die in dem verteilten Algorithmus enthalten sind, wird eines der Steuergeräte 8 bestimmt, auf dem die verschiedenen Teile des privaten Kommunikationsschlüssels zu dem privaten Kommunikationsschlüssel zusammengesetzt werden. Dieses bestimmte Steuergerät 8' teilt der Kommunikationseinrichtung 6 mit, dass es in Besitz des privaten Kommunikationsschlüssels ist. Das bestimmte Steuergerät 8' umfasst Teilungsmittel zum Teilen des privaten Kommunikationsschlüssels in einen Schlüsselteil und mindestens einen Fahrzeugteil. Bevorzugt wird der private Kommunikationsschlüssel in den Schlüsselteil und mehrere Fahrzeugteile geteilt. Der mindestens eine Fahrzeugteil bzw. die mehreren Fahrzeugteile werden verteilt in den Speichervorrichtungen 11 der Steuergeräte 8 gespeichert. Der Schlüsselteil des privaten Kommunikationsschlüssels wird über einen Sender 12 zu dem Gerät 4 übertragen. Anschließend wird jegliche Repräsentation des Schlüsselteils des privaten Kommunikationsschlüssels in dem Fahrzeug 2 gelöscht. Der Schlüsselteil des privaten Kommunikationsschlüssels wird von Kommunikationsmitteln 13 des Geräts 4 zum Schützen des privaten Kommunikationsschlüssels empfangen und in einer weiteren Speichervorrichtung 14 des Geräts 4 abgespeichert.

Am Beginn einer nachfolgenden Betriebsphase des Fahrzeugs 2, beispielsweise wenn das Fahrzeug mittels des als Fahrzeugschlüssel ausgestalteten Geräts 4 aufgeschlossen wird oder der Fahrzeugschlüssel in ein Zündschloss eingeführt wird, wird der Schlüsselteil des privaten Kommunikationsschlüssels von dem Gerät 4 zum

Schützen des privaten Kommunikationsschlüssels über die Kommunikationsmittel 13 zu einem Empfänger 15 des Fahrzeugs 2 übertragen. Anhand der Zufallsauswahlmittel wird von den Steuergeräten 8 eines festgelegt, welches den Schlüsselteil und den mindestens einen Fahrzeugteil bzw. die mehreren Fahrzeugteile des privaten Kommunikationsschlüssels zusammensetzt. Das festgelegte Steuergerät 8" authentifiziert anschließend den privaten Kommunikationsschlüssel mit Hilfe des zugehörigen öffentlichen Kommunikationsschlüssels. Hierzu wird beispielsweise eine Nachricht mittels des öffentlichen Kommunikationsschlüssels verschlüsselt und anschließend mittels des privaten Kommunikationsschlüssels entschlüsselt. Ist die Entschlüsselung erfolgreich, so ist der private Kommunikationsschlüssel authentifiziert. Das festgelegte Steuergerät 8" teilt der Kommunikationseinrichtung 6 mit, dass es im Besitz eines authentifizierten privaten Kommunikationsschlüssels ist. Während dieser dem Erzeugen des Kommunikationsschlüssels nachfolgenden Betriebsphase ist das festgelegte Steuergerät 8" für die Entschlüsselung eingehender verschlüsselter Nachrichten zuständig. Auf der Kommunikationseinrichtung 6 ist der private Kommunikationsschlüssel zu keiner Zeit gespeichert. Verwaltungsmittel (nicht dargestellt), die vorzugsweise in Software ausgeführt sind, stoßen am Beginn einer jeden Betriebsphase des Fahrzeugs 2 das Erzeugen eines neuen Schlüsselpaares an. Am Ende einer jeden Betriebsphase werden der aktuell gültige private Kommunikationsschlüssel und der dazugehörige öffentliche Kommunikationsschlüssel für ungültig erklärt und gegebenenfalls gelöscht. In einer auf die nachfolgende Betriebsphase folgenden Betriebsphase des Fahrzeugs 2 wird der neue Kommunikationsschlüssel, der in der nachfolgenden Betriebsphase erzeugt wurde, der für die Entschlüsselung verwendete private Kommunikationsschlüssel.

Analog wird ein weiterer privater Kommunikationsschlüssel für das weitere Gerät 5 gebildet und verwaltet, um zum einen eine Kommunikation des weiteren Gerätes 5 mit der Umwelt über die Kommunikationseinrichtung 6 zu ermöglichen und/oder das weitere Gerät 5 zu authentifizieren. Ist das weitere Gerät 5 als zweiter Fahrzeugschlüssel ausgebildet, so wird der weitere private Kommunikationsschlüssel für die Fahrzeug-Umwelt-Kommunikation verwendet, wenn das Fahrzeug mittels des weiteren Geräts 5, d. h. des zweiten Fahrzeugschlüssels, geöffnet und gestartet wird.

Bei der hier beschriebenen Ausführungsform besitzt ein Schlüsselpaar jeweils nur in der Betriebsphase des Fahrzeugs 2 Gültigkeit, die auf die Betriebsphase folgt, in der das Schlüsselpaar erzeugt wurde. Ein Schlüsselpaar ist somit jeweils nur für eine

Betriebsphase gültig. In einer einfachen Ausführungsform kann jedoch ein Schlüsselpaar auch für mehrere Betriebsphasen als gültiges Schlüsselpaar verwendet werden. In jedem Fall wird der Schlüsselteil des privaten Kommunikationsschlüssels am Ende der Betriebsphase in dem Fahrzeug 2 gelöscht.

Die Kommunikation zwischen den Steuergeräten 8 und der Kommunikationseinrichtung 6 sowie dem Gerät 4 kann mittels versteckter Identitäten ausgeführt werden. Hierbei werden eine Identitätsnummer (ID-Nummer) auf einen bestimmten Wert abgebildet (Hash-Wert) und eine temporäre ID-Nummer für die Steuergeräte 8, die Kommunikationseinrichtung 6 und das Gerät 4 für die Kommunikation erzeugt. Die Kommunikation wird des Weiteren mittels eines hinreichend sicheren symmetrischen Verschlüsselungsverfahrens gesichert. Hierfür sind in der Vorrichtung 3 zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation Verschlüsselungsmittel (nicht dargestellt) und in dem Gerät 4 und dem weiteren Gerät 5 weitere Verschlüsselungsmittel (nicht dargestellt) vorgesehen.

Bei den beschriebenen bevorzugten Ausführungsformen ist die Kommunikationseinrichtung nicht an der Erzeugung und/oder Zwischenspeicherung des privaten Kommunikationsschlüssels beteiligt. Andere Ausführungsformen können dies jedoch vorsehen. Ebenso kann bei einer Ausführungsform vorgesehen sein, dass die Kommunikationseinrichtung ein Steuergerät im oben beschriebenen Sinne ist.

Patentansprüche

1. Verfahren zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation umfassend die Schritte:
 - a. Erzeugen eines Schlüsselpaars während einer Betriebsphase eines Fahrzeugs (2), wobei das Schlüsselpaar den privaten Kommunikationsschlüssel und einen dazugehörigen öffentlichen Kommunikationsschlüssel umfasst,

dadurch gekennzeichnet, dass
 - b. der privaten Kommunikationsschlüssel in einen Schlüsselteil und mindestens einen Fahrzeugteil geteilt wird, wobei der mindestens eine Fahrzeugteil des privaten Kommunikationsschlüssels in mindestens einer Speichervorrichtung (11) des Fahrzeugs (2) gespeichert wird,
 - c. der Schlüsselteil des privaten Kommunikationsschlüssels zu einem von dem Fahrzeug (2) getrennten oder von dem Fahrzeug (2) trennbaren Gerät (4), insbesondere einem Fahrzeugschlüssel, übertragen wird und in einer weiteren Speichervorrichtung (14) des Geräts (4) gespeichert wird,
 - d. jede Repräsentation des Schlüsselteils des privaten Kommunikationsschlüssels in dem Fahrzeug (2) gelöscht wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schlüsselteil am Beginn einer nachfolgenden Betriebsphase des Fahrzeugs (2) von dem Gerät (4) zu dem Fahrzeug (2) übertragen wird, der Schlüsselteil mit dem in der mindestens einen Speichervorrichtung (11) des Fahrzeugs (2) abgespeicherten mindestens einen Fahrzeugteil zu dem privaten Kommunikationsschlüssel zusammengesetzt wird und der zusammengesetzte private Kommunikationsschlüssel mittels des öffentlichen Kommunikationsschlüssels authentifiziert wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der private Kommunikationsschlüssel nur in einer Betriebsphase des Fahrzeugs (2) gültig ist, die auf die Betriebsphase folgt, in der der private Kommunikationsschlüssel

- erzeugt worden ist, wobei in jeder Betriebsphase ein neues Schlüsselpaar erzeugt wird.
4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Fahrzeug (2) eine Kommunikationseinrichtung (6) und eine Gruppe von Steuergeräten (8) mit jeweils einer Recheneinheit (10) umfasst, wobei die Steuergeräte (8) und die Kommunikationseinrichtung (6) miteinander kommunizieren können und wobei jedes der Steuergeräte (8) einen Teil eines verteilten Algorithmus zum Erzeugen des privaten Kommunikationsschlüssels umfasst und der private Kommunikationsschlüssel mittels eines oder mehrerer Steuergeräte (8) aus der Gruppe der Steuergeräte (8) erzeugt wird.
 5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass das eine oder die mehreren Steuergeräte (8) aus der Gruppe der Steuergeräte (8) nach einem Zufallsprinzip jeweils vor dem Erzeugen des privaten Kommunikationsschlüssels und/oder des neuen privaten Kommunikationsschlüssels ausgewählt werden.
 6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der private Kommunikationsschlüssel auf nur einem nach dem Zufallsprinzip oder einem anderen Zufallsprinzip ausgewählten Steuergerät (8', 8'') der mehreren Steuergeräte (8) zusammengesetzt, während der Betriebsphase und/oder der nachfolgenden Betriebsphase zwischengespeichert und gegebenenfalls in den mindestens einen Fahrzeugteil und den Schlüsselteil geteilt wird.
 7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Kommunikation zwischen den Steuergeräten (8) und/oder der Kommunikationseinrichtung (6) und/oder dem Gerät (4) mittels temporärer ID-Nummern erfolgt, auf die ID-Nummern der Steuergeräte (8) und/oder der Kommunikationseinrichtung (6) und/oder des Geräts (4) abgebildet werden.
 8. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Kommunikation, einschließlich des Übertragens des privaten Kommunikationsschlüssels, des mindestens einen Fahrzeugteils und des Schlüsselteils des privaten Kommunikationsschlüssels, zwischen dem Gerät (4) und dem Fahrzeug (2) sowie innerhalb des Fahrzeugs (2) über verschlüsselte, insbesondere symmetrisch verschlüsselte, Kommunikationsverbindungen erfolgt.

9. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass für ein weiteres von dem Fahrzeug (2) getrenntes oder trennbares Gerät (5), welches mit dem Fahrzeug (2) kommunizieren kann, analog zu dem privaten Kommunikationsschlüssel ein weiterer privater Kommunikationsschlüssel erzeugt und verwendet wird.
10. Vorrichtung (3) zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation umfassend:
 - a. eine Schlüsselerzeugungseinrichtung (7) zum Erzeugen eines Schlüsselpaars während einer Betriebsphase eines Fahrzeugs (2), wobei das Schlüsselpaar den privaten Kommunikationsschlüssel und einen dazugehörigen öffentlichen Kommunikationsschlüssel umfasst, gekennzeichnet durch
 - b. Teilungsmittel zum Teilen des privaten Kommunikationsschlüssels in einen Schlüsselteil und mindestens einen Fahrzeugteil,
 - c. mindestens eine Speichervorrichtung (11) des Fahrzeugs (2) zum Speichern des mindestens einen Fahrzeugteils des privaten Kommunikationsschlüssels,
 - d. eine Kommunikationseinrichtung (6) zum Übertragen der Schlüsselteil des privaten Kommunikationsschlüssels zu einem von dem Fahrzeug (2) getrennten oder von dem Fahrzeug (2) trennbaren Gerät (4), insbesondere einem Fahrzeugschlüssel, für ein Speichern des Schlüsselteils in einer weiteren Speichervorrichtung (14) des Geräts (4),
 - e. Mittel zum Löschen jeder Repräsentation des Schlüsselteils des privaten Kommunikationsschlüssels in dem Fahrzeug (2).
11. Vorrichtung (3) nach Anspruch 10, dadurch gekennzeichnet, dass die Kommunikationseinrichtung Empfangsmittel (15) zum Empfangen des Schlüsselteils am Beginn einer nachfolgenden Betriebsphase des Fahrzeugs (2) von dem Gerät (4) umfasst und mittels einer Authentifizierungseinrichtung der Schlüsselteil mit dem in der mindestens einen Speichervorrichtung (11) des Fahrzeugs (2) abgespeicherten mindestens einen Fahrzeugteil zum dem privaten

- Kommunikationsschlüssel zusammensetzbar ist und der zusammengesetzte private Kommunikationsschlüssel mittels des öffentlichen Kommunikationsschlüssels authentifizierbar ist.
12. Vorrichtung (3) nach Anspruch 10 oder 11, gekennzeichnet durch Verwaltungsmittel zum Löschen und/oder Ungültigerklären des privaten Kommunikationsschlüssels am Ende einer Betriebsphase des Fahrzeugs (2), die auf die Betriebsphase folgt, in der der private Kommunikationsschlüssel erzeugt worden ist, und zum Einleiten des Erzeugens ein neues Schlüsselpaar in jeder Betriebsphase.
 13. Vorrichtung (3) nach einem der Ansprüche 10 bis 12, gekennzeichnet durch eine Gruppe von Steuergeräten (8) mit einer Recheneinheit (10), wobei die Steuergeräte (8) und die Kommunikationseinrichtung (6) untereinander kommunizieren können und wobei jedes der Steuergeräte (8) einen Teil eines verteilten Algorithmus zum Erzeugen des privaten Kommunikationsschlüssels umfasst und der private Kommunikationsschlüssel mittels eines oder mehrerer Steuergeräte (8) aus der Gruppe der Steuergeräte (8) erzeugbar ist.
 14. Vorrichtung (3) nach Anspruch 13, gekennzeichnet durch Zufallsauswahlmittel, mittels derer das eine oder die mehreren Steuergeräte (8) aus der Gruppe der Steuergeräte (8) nach einem Zufallsprinzip anhand von Zufallszahlen jeweils vor dem Erzeugen des privaten Kommunikationsschlüssels und/oder des neuen privaten Kommunikationsschlüssels auswählbar sind.
 15. Vorrichtung (3) nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, dass mittels der Zufallsauswahlmittel nach dem Zufallsprinzip oder einem anderen Zufallsprinzip eines der mehreren Steuergeräte (8) auswählbar ist, auf dem der private Kommunikationsschlüssel zusammensetzt, während der Betriebsphase und/oder der nachfolgenden Betriebsphase in der mindestens einen Speichervorrichtung (11) zwischengespeichert und gegebenenfalls in den mindestens einen Fahrzeugteil und den Schlüsselteil geteilt wird.
 16. Vorrichtung (3) nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, dass die Kommunikation zwischen den Steuergeräten (8) und/oder der Kommunikationseinrichtung (6) und/oder dem Gerät (4) mittels temporärer ID-

- Nummern durchführbar ist, auf die ID-Nummern der Steuergeräte (8) und/oder der Kommunikationseinrichtung (6) und/oder des Geräts (4) abbildbar sind.
17. Vorrichtung (3) nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, dass die Steuergeräte (8) und die Kommunikationseinrichtung (6) Verschlüsselungsmittel umfassen, so dass die Kommunikation, einschließlich des Übertragens des privaten Kommunikationsschlüssels, des mindestens einen Fahrzeugteils und des Schlüsselteils des privaten Kommunikationsschlüssels, zwischen dem Gerät (4) und dem Fahrzeug (2) sowie innerhalb des Fahrzeugs (2) über verschlüsselte, insbesondere symmetrisch verschlüsselte, Kommunikationsverbindungen erfolgen kann.
 18. Vorrichtung (3) nach einem der Ansprüche 10 bis 17, dadurch gekennzeichnet, dass für ein weiteres von dem Fahrzeug (2) trennbares Gerät (5), welches mit dem Fahrzeug (2) kommunizieren kann, analog zu dem privaten Kommunikationsschlüssel ein weiterer privater Kommunikationsschlüssel erzeugbar und verwendbar ist.
 19. Gerät (4) zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation, das ausgestaltet ist, um mit einer Vorrichtung (3) zum Schützen eines privaten Kommunikationsschlüssels nach den Ansprüchen 10 bis 18 zusammenzuwirken, mit Kommunikationsmitteln (13) zum Austauschen eines Fahrzeugteils des privaten Kommunikationsschlüssels mit dem Fahrzeug (2) und einer weiteren Speichervorrichtung (14) zum Speichern des Schlüsselteils des privaten Kommunikationsschlüssels.
 20. Gerät (4) nach Anspruch 19, dadurch gekennzeichnet, dass der Schlüsselteil des privaten Kommunikationsschlüssels beim Empfangen eines neuen Schlüsselteils eines neuen privaten Kommunikationsschlüssels in der weiteren Speichervorrichtung (14) überschreibbar ist.
 21. Gerät (4) nach Anspruch 19 oder 20, gekennzeichnet durch weitere Verschlüsselungsmittel, so dass die Kommunikation mit dem Fahrzeug (2) über eine verschlüsselte, insbesondere symmetrisch verschlüsselte, Kommunikationsverbindung erfolgen kann.
 22. Gerät (4) nach einem der Ansprüche 19 bis 21, dadurch gekennzeichnet, dass es als Fahrzeugschlüssel ausgebildet ist.

23. System (1) zum Schützen eines privaten Kommunikationsschlüssels für eine Fahrzeug-Umwelt-Kommunikation, welches eine Vorrichtung (3) nach einem der Ansprüche 10 bis 18 und mindestens ein Gerät (4) nach einem der Ansprüche 19 bis 22 umfasst.

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2005/014064

A. CLASSIFICATION OF SUBJECT MATTER H04L29/06 H04L9/08 H04L9/30		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/003230 A1 (PUHL LARRY C ET AL) 1 January 2004 (2004-01-01) paragraphs [0045], [0046], [0049], [0052], [0056], [0057], [0064] - [0069]	1-23
Y	US 2002/013772 A1 (PEINADO MARCUS) 31 January 2002 (2002-01-31) paragraphs [0173], [0174]	1-23
A	WO 02/46861 A (CERTIA INC; MEFFERT, GREGORY, J; HASTINGS, PAUL, R., II; KURT, MARK, C) 13 June 2002 (2002-06-13) page 2, line 32 - page 3, line 21 page 37, line 17 - line 24	1-23
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family		
Date of the actual completion of the international search 16 March 2006		Date of mailing of the international search report 23/03/2006
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Veenv, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2005/014064

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004003230 A1	01-01-2004	AU 2003251578 A1 WO 2004003857 A2	19-01-2004 08-01-2004
US 2002013772 A1	31-01-2002	US 2005216743 A1	29-09-2005
WO 0246861 A	13-06-2002	AU 4151402 A	18-06-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2005/014064

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES H04L29/06 H04L9/08 H04L9/30		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
B. RECHERCHIERTE GEBIETE		
Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) H04L		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 2004/003230 A1 (PUHL LARRY C ET AL) 1. Januar 2004 (2004-01-01) Absätze [0045], [0046], [0049], [0052], [0056], [0057], [0064] - [0069]	1-23
Y	US 2002/013772 A1 (PEINADO MARCUS) 31. Januar 2002 (2002-01-31) Absätze [0173], [0174]	1-23
A	WO 02/46861 A (CERTIA INC; MEFFERT, GREGORY, J; HASTINGS, PAUL, R., II; KURT, MARK, C) 13. Juni 2002 (2002-06-13) Seite 2, Zeile 32 - Seite 3, Zeile 21 Seite 37, Zeile 17 - Zeile 24	1-23
<input type="checkbox"/> Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen <input checked="" type="checkbox"/> Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist *X* Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden *Y* Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist *&* Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der Internationalen Recherche 16. März 2006		Absenddatum des internationalen Recherchenberichts 23/03/2006
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Veen, G

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2005/014064

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2004003230 A1	01-01-2004	AU 2003251578 A1 WO 2004003857 A2	19-01-2004 08-01-2004
US 2002013772 A1	31-01-2002	US 2005216743 A1	29-09-2005
WO 0246861 A	13-06-2002	AU 4151402 A	18-06-2002