(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
8. Dezember 2005 (08.12.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/116834 A1

(51) Internationale Patentklassifikation[7]: G06F 01/00

(21) Internationales Aktenzeichen: PCT/EP2004/004666

(22) Internationales Anmeldedatum:
29. April 2004 (29.04.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT** [DE/DE]; Petuelring 130, 80909 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KUHLS, Burkhard** [DE/DE]; Elmer-Fryar-Ring 21, 86391 Stadtbergen (DE). **KIESSLING, Horst** [DE/DE]; Wettersteinring 24, 85354 Freising (DE).

(74) Gemeinsamer Vertreter: **BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT**; Patentabteilung AJ-3, 80788 München (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, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, 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, IT, LU, 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).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

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.

(54) **Title:** AUTHENTICATION OF CONTROL UNITS IN A VEHICLE

(54) **Bezeichnung:** AUTHENTISIERUNG VON STEUERGERÄTEN IN EINEM FAHRZEUG

(57) **Abstract:** The invention particularly relates to a method for authenticating control units in a bus system of a motor vehicle. In order to effectively and inexpensively prevent a sequence control system that is stored in a control unit from being manipulated, a first control unit transmits an authentication request to an authentication apparatus via the bus system, said authentication apparatus signs the authentication request using a first symmetric key and transmits the signed authentication request or exclusively the signature to the first control unit, the first control unit compares the transmitted signature of the authentication request to a signature which is determined by the first control unit by applying the symmetric key to the authentication request, and/or the first control unit decodes the transmitted signature of the authentication request using the first symmetric key and a first hash value is obtained, and the first control unit applies a hash algorithm to the authentication request, whereby a second hash value is obtained, and the first control unit is rendered operational if the comparison of the signatures and/or the hash values is positive or if the signatures and/or the hash values match.

(57) **Zusammenfassung:** Die Erfindung betrifft insbesondere ein Verfahren zur Authentisierung von Steuergeräten in einem Bussystem eines Kraftfahrzeugs. Um eine Manipulation einer in einem Steuergerät gespeicherten Ablaufsteuerung bei geringen Kosten wirksam zu verhindern wird vorgeschlagen, dass ein erstes Steuergerät über das Bussystem eine Authentisierungsanfrage an eine Authentisierungsvorrichtung übermittelt, dass die Authentisierungsvorrichtung die Authentisierungsanfrage unter Verwendung eines ersten symmetrischen Schlüssels signiert und die signierte Authentisierungsanfrage oder lediglich die Signatur an das erste Steuergerät übermittelt, dass das erste Steuergerät die übermittelte Signatur der Authentisierungsanfrage mit einer vom ersten Steuergerät, unter Anwendung des symmetrischen Schlüssels auf die Authentisierungsanfrage ermittelten Signatur vergleicht, und/oder dass das erste Steuergerät die übermittelte Signatur der Authentisierungsanfrage unter Verwendung des ersten symmetrischen Schlüssels entschlüsselt und ein erster Hash-Wert erhalten wird, und dass das erste Steuergerät einen Hash-Algorithmus auf die Authentisierungsanfrage anwendet, wodurch ein zweiter Hash-Wert erhalten wird, und dass das erste Steuergerät bei positivem Vergleich bzw. Obereinstimmung der Signaturen und/oder der Hash-Werte betriebsbereit gemacht wird.

WO 2005/116834 A1

Authentisierung von Steuergeräten in einem Fahrzeug

Die Erfindung betrifft insbesondere ein Verfahren zur Authentisierung von Steuergeräten in einem Bussystem eines Kraftfahrzeugs nach dem Oberbegriff des Anspruchs 1.

Zur Verhinderung von Manipulationen an der in den Steuergeräten gespeicherten Ablaufsteuerung bzw. der entsprechenden Software, die von einem oder mehreren in den Steuergeräten vorgesehenen Prozessoren ausgeführt wird, ist es wichtig, die Berechtigung des Zugriffs auf die Steuergeräte zu überwachen. Die Berechtigung kann durch kryptografische Maßnahmen überprüft werden.

Nachteilig ist, dass die Durchführung entsprechender kryptografischer Maßnahmen den oder die Prozessoren des Steuergeräts und weitere Hardware-Komponenten des Steuergeräts belastet bzw. leistungsfähigere und damit teurere Steuergeräte bedingt. Dies schlägt insbesondere bei einem millionenfach eingesetzten Produkt, wie bei dem Steuergerät eines Kraftfahrzeugs, zu Buche.

Aufgabe der vorliegenden Erfindung ist es insbesondere, ein Verfahren anzugeben, das eine Manipulation einer in einem Steuergerät gespeicherten Ablaufsteuerung bei geringen Kosten wirksam verhindert.

Diese Aufgabe wird durch die im Anspruch 1 angegebenen Maßnahmen verfahrensmäßig und durch den unabhängigen System-Anspruch vorrichtungsmäßig gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der abhängigen Patentansprüche.

Ein wesentlicher Aspekt des erfindungsgemäßen Verfahrens zur Authentisierung von Steuergeräten bzw. zur Prüfung, ob es sich um berechtigte Steuergeräte im Bussystem handelt, besteht in der Durchführung der folgenden Maßnahmen. In einem ersten Schritt übermittelt ein erstes Steuergerät einer Vielzahl von Steuergeräten des Kraftfahrzeugs über das Bussystem eine Authentisierungsanfrage an eine Authentisierungsvorrichtung.

Bei der Authentisierungsanfrage handelt es sich bevorzugt um eine von dem Steuergerät generierte Zufallszahl oder dgl., die lediglich einmalig erzeugt wird. Bei der Authentisierungsvorrichtung handelt es sich bevorzugt um ein zentrales Steuergerät, das Zugriff auf einen symmetrischen, kryptografischen Schlüssel hat und ein symmetrisches kryptografisches Verfahren ausführen kann.

Die Ausführung eines symmetrischen kryptografischen Verfahrens beansprucht die Ressourcen, insbesondere den Prozessor, des Steuergeräts bzw. der Authentisierungsvorrichtung deutlich weniger als ein asymmetrisches Verfahren, so dass Steuergeräte bei der Verwendung der Erfindung deutlich kostengünstiger gestaltet werden können.

Die Authentisierungsvorrichtung signiert die Authentisierungsanfrage unter Verwendung eines ersten symmetrischen Schlüssels und übermittelt die signierte Authentisierungsanfrage oder lediglich die Signatur an das erste Steuergerät. Das Signieren bzw. die Erzeugung der Signatur geschieht, indem ein Hash-Algorithmus auf die Authentisierungsanfrage bzw. Authentisierungsdaten angewandt wird. Der Hash-Algorithmus liefert einen Hash-Wert, der charakteristisch für die konkreten Authentisierungsdaten ist. Der Hash-Wert wird mit dem ersten symmetrischen Schlüssel verschlüsselt und der verschlüsselte Hash-Wert an die Authentisierungsanfrage bzw. an die Authentisierungsdaten angefügt und zusammen mit der Authentisierungsanfrage an das erste Steuergerät übermittelt. Alternativ kann auch lediglich die Signatur bzw. der verschlüsselte Hash-Wert an das erste Steuergerät übermittelt werden, weil dort ja die Authentisierungsanfrage erzeugt worden und damit bereits vorhanden ist.

Das erste Steuergerät vergleicht die übermittelte Signatur mit einer vom ersten Steuergerät unter Anwendung des symmetrischen Schlüssels auf die Authentisierungsanfrage ermittelten Signatur. Die Signatur kann vom ersten Steuergerät ermittelt werden, indem derselbe Hash-Algorithmus, der von der Authentisierungsvorrichtung auf die Authentisierungsanfrage zur Ermittlung der Signatur angewandt worden ist, auch von dem ersten Steuergerät auf die Authentisierungsanfrage angewandt wird. Wiederum ergibt sich ein Hash-Wert. Dieser Hash-Wert oder die auf der Basis

des Hash-Werts unter Verwendung des symmetrischen Schlüssels gebildete Signatur wird mit der übermittelten Signatur oder dem aus der übermittelten Signatur wiederum unter Verwendung des symmetrischen Schlüssels erhaltenen Hash-Werts verglichen.

Bei positivem Vergleich bzw. bei einer Übereinstimmung gelten das erste Steuergerät und die Authentisierungsvorrichtung als wechselseitig authentisiert, d.h. für das Steuergerät gilt die Authentisierungsvorrichtung als echt bzw. berechtigt und umgekehrt. Entsprechend wird das erste Steuergerät bei positivem Vergleich bzw. Übereinstimmung vorzugsweise betriebsbereit gemacht. Alternativ oder ergänzend könnte der Authentisierungsvorrichtung ein Schreib- und/oder Lesezugriff auf einen elektronischen Speicher des ersten Steuergeräts eingeräumt werden.

Bei einem bevorzugten Ausführungsbeispiel der Erfindung ist vorgesehen, dass ein oder mehrere weitere Steuergeräte des Bussystems in der beschriebenen Weise eine Authentisierung mit der Authentisierungsvorrichtung durchführen. Durch diese Maßnahmen kann also überprüft werden, ob sich unberechtigte Steuergeräte oder eine unberechtigte Authentisierungsvorrichtung im Bussystem befinden.

Bei einem weiteren Ausführungsbeispiel der Erfindung wird die Authentisierung der Steuergeräte ggü. der Authentisierungsvorrichtung der Reihe nach durchgeführt. Dies verringert die erforderlichen Hardware-Ressourcen.

Bei einem Ausführungsbeispiel der Erfindung ist vorgesehen, dass das Kraftfahrzeug erst dann in Betrieb genommen werden kann, wenn weitgehend sämtliche Steuergeräte des Bussystems das Verfahren zur Authentisierung mit positivem Vergleichsergebnis durchgeführt haben. Hierdurch kann die Betriebssicherheit des Bussystems bzw. die Kompatibilität der Busteilnehmer gewährleistet werden. Ebenso erhöht diese Maßnahme den Diebstahlschutz des mit dem Bussystem der Erfindung ausgestatteten Kraftfahrzeugs, wenn eine Wegfahrsperre in dem Bussystem bzw. in den Steuergeräten integriert ist.

Bei einem anderen Ausführungsbeispiel der Erfindung ist vorgesehen, dass die Durchführung des Authentisierungsverfahrens jeweils vor dem Anlassen des Fahr-

zeugs vorgenommen wird, vorzugsweise nach dem Öffnen des Fahrzeugs. Durch diese Maßnahme wird die Betriebssicherheit, Kompatibilität etc. periodisch überprüft.

Bei einem Ausführungsbeispiel der Erfindung wird vor dem Anlassen des Fahrzeugs das erfindungsgemäße Authentisierungsverfahren weitgehend lediglich für diejenigen Steuergeräte durchgeführt, die beim Anlassen des Fahrzeugs zur Verfügung stehen müssen, um das Fahrzeug bei kurzer Vorlaufzeit – falls erforderlich - betriebsbereit zu haben. Das erfindungsgemäße Authentisierungsverfahren kann dann für die anderen Steuergeräte nach dem Startvorgang des Fahrzeugs, ohne Behinderung der Inbetriebnahme des Kraftfahrzeugs, durchgeführt werden.

Bei einem weiteren Ausführungsbeispiel der Erfindung ist vorgesehen, dass weitgehend sämtliche Steuergeräte denselben symmetrischen Schlüssel bei der Durchführung des Authentisierungsverfahrens verwenden. Diese Maßnahme macht die Schlüsselverwaltung einfach und hat zudem den Vorteil, dass die Steuergeräte des betreffenden Fahrzeugs hierdurch einander zugeordnet sind.

Bei einem Ausführungsbeispiel der Erfindung ist vorgesehen, dass der symmetrische Schlüssel von Fahrzeug zu Fahrzeug variiert und ein Steuergerät eines ersten Fahrzeugs bei der Durchführung des erfindungsgemäßen Authentisierungsverfahrens auf einen ersten symmetrischen Schlüssel und das gleiche Steuergerät eines zweiten Fahrzeugs bei der Durchführung des Verfahrens auf einen zweiten symmetrischen Schlüssel zugreift.

Der symmetrische Schlüssel ist bevorzugt derart in dem Bussystem „untergebracht", dass er lediglich von der Authentisierungsvorrichtung und von den am Verfahren beteiligten Steuergeräten gelesen werden kann, d.h. geheim bleibt und nicht unberechtigt verändert werden kann. Bei einer Ausgestaltung der Erfindung ist der symmetrische Schlüssel jeweils im nicht extern auslesbaren oder veränderbaren Boot-Bereich jeden Steuergeräts und im entsprechenden Bereich der Authentisierungsvorrichtung gespeichert.

Dadurch, dass der symmetrische Schlüssel von Fahrzeug zu Fahrzeug variiert, ist das Ausspähen des symmetrischen Schlüssels eines konkreten Fahrzeugs vergleichsweise unschädlich. Dies wäre beim Ausspähen eines symmetrischen Schlüssels aus einem Fahrzeug, der auf sämtliche Fahrzeuge desselben Typs „passt" selbstverständlich völlig anders.

Bei einem Ausführungsbeispiel der Erfindung ist vorgesehen, dass das erfindungsgemäße Verfahren in umgekehrter Richtung abläuft, d.h. dass die Authentisierungsvorrichtung eine Authentisierungsanfrage an das erste Steuergerät übermittelt, das erste Steuergerät die Authentisierungsanfrage mit dem ersten symmetrischen Schlüssel signiert und die signierte Authentisierungsanfrage an die Authentisierungsvorrichtung übermittelt.

Hierbei wird der Vergleich vom Steuergerät auf die Authentisierungsvorrichtung verlagert. Dies geht mit einer Ressourcen-Entlastung jeden Steuergeräts und einer Ressourcen-Belastung der Authentisierungsvorrichtung einher. Die vielfache Ressourcen-Entlastung ggü. einer einzigen Ressourcen-Belastung führt zur Einsparung von Hardware-Kosten.

Bei einem Ausführungsbeispiel der Erfindung ist vorgesehen, dass die Authentisierungsvorrichtung eine weitere Authentisierungsprüfung unter Durchführung eines asymmetrischen Verschlüsselungsverfahrens mit einer fahrzeugexternen Vorrichtung vornimmt, insbesondere ein Public-Key-Verfahren.

Bei einem Ausführungsbeispiel der Erfindung ist vorgesehen, dass die Authentisierungsvorrichtung eine Authentisierungsanfrage bzw. Authentisierungsdaten an die fahrzeugexterne Vorrichtung übermittelt. Die fahrzeugexterne Vorrichtung wendet auf die Authentisierungsanfrage bzw. die Authentisierungsdaten einen Hash-Algorithmus an, wodurch ein Hash-Wert erhalten wird. Der Hash-Wert wird mit einem geheimen persönlichen Schlüssel verschlüsselt und der verschlüsselte Hash-Wert wird an die Authentisierungsanfrage bzw. an die Authentisierungsdaten angefügt, d. h. die Authentisierungsanfrage wird signiert, und die signierte Authentisierungsanfrage oder lediglich die Signatur, d. h. der mit dem geheimen Schlüssel verschlüsselte Hash-Wert, wird an die Authentisierungsvorrichtung übermittelt. Die Au-

thentisierungsvorrichtung wendet ebenfalls den Hash-Algorithmus auf die Authentisierungsanfrage an, das Ergebnis ist ein zweiter Hash-Wert. Ferner entschlüsselt die Authentisierungsvorrichtung den von der fahrzeugexternen Vorrichtung erhaltenen verschlüsselten Hash-Wert mit dem zum persönlichen, geheimen Schlüssel komplementären öffentlichen Schlüssel und vergleicht den ersten mit dem zweiten Hash-Wert. Ist der Vergleich positiv, d.h. stimmen beide Hash-Werte überein, so hat sich die fahrzeugexterne Vorrichtung ggü. der Authentisierungsvorrichtung im Fahrzeug erfolgreich authentisiert. Auf dieser Basis kann der fahrzeugexternen Vorrichtung unter der Kontrolle der Authentisierungsvorrichtung ein Schreib- und/oder Lese-Zugriff auf einen oder mehrere Speicher einer oder mehrerer Steuergeräte eingeräumt werden.

Bei einer bevorzugten Ausführungsform der Erfindung, wird der fahrzeugexternen Vorrichtung ermöglicht, den Speicher eines oder mehrerer Steuergeräte mit einer neuen Ablaufsteuerung bzw. Software und/oder mit einem Freischaltcode zu versehen. Bei der neuen Ablaufsteuerung kann es sich insbesondere um eine Ablaufsteuerung handeln, die ggü. der früheren Ablaufsteuerung aktualisiert worden ist, die Software-Probleme beseitigt, und/oder zusätzliche Funktionen des Steuergeräts bereitstellt. Bei der neuen Ablaufsteuerung kann es sich um eine Ergänzung zur bereits im Steuergerät gespeicherten Ablaufsteuerung handeln, die insbesondere zusätzliche Funktionen des Steuergeräts bereitstellt.

Bei dem Freischaltcode kann es sich insbesondere um Daten handeln, der eine in dem Steuergerät oder an anderer Stelle im Fahrzeug ablaufbereit gehaltene Ablaufsteuerung bzw. Software, insbesondere zeitlich befristet, freischaltet. D. h. die bereits im Fahrzeug gespeicherte Ablaufsteuerung bzw. Software kann erst nach der Bereitstellung des Freischaltcodes im Fahrzeug ausgeführt werden.

Die Erfindung ermöglicht ein Bussystem eines Kraftfahrzeugs mit Steuergeräten, bei dem in dem Bussystem eine Authentisierungsvorrichtung vorgesehen ist und in dem Bussystem ein erfindungsgemäßes Verfahren ausgeführt wird. Ferner ermöglicht die Erfindung ein Computer-Programm-Produkt zur Authentisierung von Steuergeräten in einem Bussystem eines Kraftfahrzeugs, das ein Verfahren nach einem oder mehreren der vorstehenden Verfahrensansprüche ablaufen lässt.

Patentansprüche

1. Verfahren zur Authentisierung von Steuergeräten in einem Bussystem eines Kraftfahrzeugs, dadurch gekennzeichnet, dass
   - ein erstes Steuergerät über das Bussystem eine Authentisierungsanfrage an eine Authentisierungsvorrichtung übermittelt,
   - die Authentisierungsvorrichtung die Authentisierungsanfrage unter Verwendung eines ersten symmetrischen Schlüssels signiert und die signierte Authentisierungsanfrage oder lediglich die Signatur an das erste Steuergerät übermittelt,
   - das erste Steuergerät die übermittelte Signatur der Authentisierungsanfrage mit einer vom ersten Steuergerät unter Anwendung des symmetrischen Schlüssels auf die Authentisierungsanfrage ermittelten Signatur vergleicht, und/oder
   - das erste Steuergerät die übermittelte Signatur der Authentisierungsanfrage unter Verwendung des ersten symmetrischen Schlüssels entschlüsselt und ein erster Hash-Wert erhalten wird, und das erste Steuergerät einen Hash-Algorithmus auf die Authentisierungsanfrage anwendet, wodurch ein zweiter Hash-Wert erhalten wird, und
   - das erste Steuergerät bei positivem Vergleich bzw. Übereinstimmung der Signaturen und/oder der Hash-Werte betriebsbereit gemacht wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass ein oder mehrere weitere Steuergeräte des Bussystems das Verfahren zur Authentisierung nach Anspruch 1 durchführen.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass Kraftfahrzeug erst dann in Betrieb genommen werden kann, wenn weitgehend sämtliche Steuergeräte des Bussystems das Verfahren zur Authentisierung nach Anspruch 1 mit positivem Vergleichsergebnis durchgeführt haben.

4. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Durchführung des Authentisierungsverfahren jeweils vor dem Anlassen des Fahrzeugs vorgenommen wird, vorzugsweise nach dem Öffnen des Fahrzeugs.

5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass weitgehend sämtliche Steuergeräte denselben symmetrischen Schlüssel bei der Durchführung des Authentisierungsverfahrens nach Anspruch 1 verwenden.

6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der symmetrische Schlüssel von Fahrzeug zu Fahrzeug variiert und ein Steuergerät eines ersten Fahrzeugs bei der Durchführung des Verfahrens nach Anspruch 1 auf einen ersten symmetrischen Schlüssel und das gleiche Steuergerät eines zweiten Fahrzeugs bei der Durchführung des Verfahrens nach Anspruch 1 auf einen zweiten symmetrischen Schlüssel zugreift.

7. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass das Verfahren nach Anspruch 1 in umgekehrter Richtung abläuft, d. h. dass die Authentisierungsvorrichtung eine Authentisierungsanfrage an das erste Steuergerät übermittelt, das erste Steuergerät die Authentisierungsanfrage mit dem ersten symmetrischen Schlüssel signiert und die signierte Authentisierungsanfrage an die Authentisierungsvorrichtung übermittelt.

8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Authentisierungsvorrichtung eine weitere Authentisierungsprüfung unter Durchführung eines asymmetrischen Verschlüsselungsverfahrens mit einer fahrzeugexternen Vorrichtung vornimmt, insbesondere ein Public-Key-Verfahren.

9. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Authentisierungsvorrichtung eine Authentisierungsanfrage an die fahrzeugexterne Vorrichtung übermittelt, die fahrzeugexterne Vorrichtung die

Authentisierungsanfrage mit einem geheimen Schlüssel eines asymmetrischen Schlüssel-Paars, insbesondere ein Public-Key-Schlüssel-Paar, signiert und die signierte Authentisierungsanfrage oder lediglich die Signatur an die Authentisierungsvorrichtung übermittelt, die Authentisierungsvorrichtung die Authentisierungsanfrage unter Verwendung desselben Algorithmus wie die fahrzeugexterne Vorrichtung eine Signatur der Authentisierungsanfrage ermittelt, die von der fahrzeugexternen Vorrichtung übermittelte Signatur unter Verwendung des zum geheimen Schlüssel komplementären öffentlichen Schlüssels entschlüsselt und die ermittelte mit der übermittelten Signatur vergleicht.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass bei positivem Vergleich die fahrzeugexterne Vorrichtung durch die Authentisierungsvorrichtung Schreib- und/oder Lese-Zugriff auf einen Speicher des ersten Steuergeräts erhält.

11. Bussystem eines Kraftfahrzeugs mit Steuergeräten, dadurch gekennzeichnet, dass in dem Bussystem eine Authentisierungsvorrichtung vorgesehen ist und in dem Bussystem ein Verfahren nach einem der vorstehenden Verfahrensansprüche ausgeführt wird.

12. Computer-Programm-Produkt zur Authentisierung von Steuergeräten in einem Bussystem eines Kraftfahrzeugs, dadurch gekennzeichnet, dass das Computer-Programm-Produkt ein Verfahren nach einem oder mehreren der vorstehenden Verfahrensansprüche ablaufen lässt.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/004666

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F01/00

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)
IPC 7 G06F

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	DE 101 48 323 A (DAIMLER CHRYSLER AG) 10 April 2003 (2003-04-10) paragraphs '0004!, '0006!, '0014!	1-12
Y	MENEZES ET AL: "Handbook of applied cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 400-405, XP002143934 ISBN: 0-8493-8523-7 page 401 - page 402	1-12
Y	US 6 526 460 B1 (DAUNER OSKAR ET AL) 25 February 2003 (2003-02-25) abstract	1-12

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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	Date of mailing of the international search report
7 September 2004	13/10/2004

Name and mailing address of the ISA	Authorized officer
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	Mezödi, S

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/004666

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 225 510 A (BAYERISCHE MOTOREN WERKE AG) 24 July 2002 (2002-07-24) abstract	1-12
A	US 6 032 257 A (ANGELO MICHAEL F ET AL) 29 February 2000 (2000-02-29) column 3, lines 31-34	
A	DE 101 41 737 C (DAIMLER CHRYSLER AG) 3 April 2003 (2003-04-03) abstract	
A	US 2002/152398 A1 (KRUMREIN RAINER) 17 October 2002 (2002-10-17) abstract	
A	DE 102 38 093 A (AUDI NSU AUTO UNION AG) 11 March 2004 (2004-03-11) abstract	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/004666

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 10148323	A	10-04-2003	DE	10148323 A1	10-04-2003
US 6526460	B1	25-02-2003	DE	19839354 A1	02-03-2000
			EP	0982700 A2	01-03-2000
			JP	2000165422 A	16-06-2000
EP 1225510	A	24-07-2002	DE	10102642 A1	25-07-2002
			EP	1225510 A2	24-07-2002
US 6032257	A	29-02-2000	NONE		
DE 10141737	C	03-04-2003	DE	10141737 C1	03-04-2003
US 2002152398	A1	17-10-2002	DE	10112699 A1	02-10-2002
			EP	1241061 A2	18-09-2002
DE 10238093	A	11-03-2004	DE	10238093 A1	11-03-2004
			WO	2004027587 A2	01-04-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/004666

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F01/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

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	DE 101 48 323 A (DAIMLER CHRYSLER AG) 10. April 2003 (2003-04-10) Absätze '0004!, '0006!, '0014!	1-12
Y	MENEZES ET AL: "Handbook of applied cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, Seiten 400-405, XP002143934 ISBN: 0-8493-8523-7 Seite 401 - Seite 402	1-12
Y	US 6 526 460 B1 (DAUNER OSKAR ET AL) 25. Februar 2003 (2003-02-25) Zusammenfassung	1-12

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] 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 naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
7. September 2004	13/10/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
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	Mezödi, S

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/004666

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 1 225 510 A (BAYERISCHE MOTOREN WERKE AG) 24. Juli 2002 (2002-07-24) Zusammenfassung	1-12
A	US 6 032 257 A (ANGELO MICHAEL F ET AL) 29. Februar 2000 (2000-02-29) Spalte 3, Zeilen 31-34	
A	DE 101 41 737 C (DAIMLER CHRYSLER AG) 3. April 2003 (2003-04-03) Zusammenfassung	
A	US 2002/152398 A1 (KRUMREIN RAINER) 17. Oktober 2002 (2002-10-17) Zusammenfassung	
A	DE 102 38 093 A (AUDI NSU AUTO UNION AG) 11. März 2004 (2004-03-11) Zusammenfassung	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2004/004666

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 10148323 A	10-04-2003	DE 10148323 A1	10-04-2003
US 6526460 B1	25-02-2003	DE 19839354 A1	02-03-2000
		EP 0982700 A2	01-03-2000
		JP 2000165422 A	16-06-2000
EP 1225510 A	24-07-2002	DE 10102642 A1	25-07-2002
		EP 1225510 A2	24-07-2002
US 6032257 A	29-02-2000	KEINE	
DE 10141737 C	03-04-2003	DE 10141737 C1	03-04-2003
US 2002152398 A1	17-10-2002	DE 10112699 A1	02-10-2002
		EP 1241061 A2	18-09-2002
DE 10238093 A	11-03-2004	DE 10238093 A1	11-03-2004
		WO 2004027587 A2	01-04-2004