(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
26. April 2001 (26.04.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/29352 A1

(51) Internationale Patentklassifikation[7]: E05B 49/00

(21) Internationales Aktenzeichen: PCT/EP00/09276

(22) Internationales Anmeldedatum:
22. September 2000 (22.09.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 49 970.5 16. Oktober 1999 (16.10.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **VOLKSWAGEN AKTIENGESELLSCHAFT** [DE/DE]; 38436 Wolfsburg (DE). **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02 20, 70442 Stuttgart (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **MEIER, Michael** [DE/DE]; Thomas-Dehler Weg 13, 31141 Hildesheim (DE). **SCHMITZ, Stephan** [DE/DE]; Werderstrasse 24, 50672 Köln (DE). **TITZE, Andreas** [DE/DE]; Gabelsbergerstrasse 18, 38118 Braunschweig (DE). **NEMETSCHEK, Dominique** [DE/DE]; Am Kuhlacker 3, 38110 Braunschweig (DE).

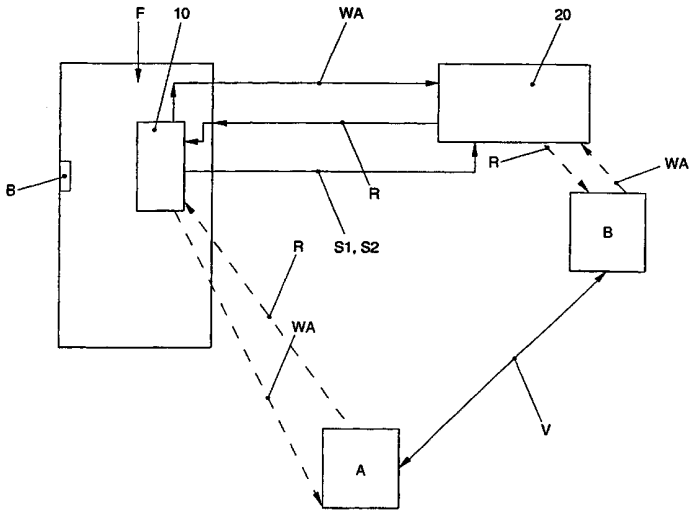
(74) Gemeinsamer Vertreter: **VOLKSWAGEN AKTIENGESELLSCHAFT**; Brieffach 1770, 38436 Wolfsburg (DE).

(81) Bestimmungsstaaten *(national)*: CN, IN, JP, KR, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR CONTROLLING ENTRY INTO A SECURED LOCATION, ESPECIALLY INTO A MOTOR VEHICLE

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ZUGANGSKONTROLLE ZU EINEM GESICHERTEN ORT, INSBESONDERE EINEM KRAFTFAHRZEUG



(57) Abstract: The invention relates to a method for controlling entry, in particular, into a motor vehicle (F), during which a key (20) and a base station (10) wirelessly exchange authentication data between one another in an active or a passive communication mode. At the beginning of this authentication process, the base station (10) transmits a call signal (WA) to the key (20) and the key replies to said call signal (WA) with a reply signal (R). The base station (10) verifies the received reply signal (R) of the key (20) in the communications mode in which said reply signal (R) was received. If the reply signal (R) of the key (20) was received in the active communications mode, the base station (10) transmits a first selection instruction (S1) to the key (20) thus causing the key (20) to carry out the subsequent communication in the active communications mode. If the reply signal (R) of the key (20) was received in the passive communications mode, the base station (10) transmits a second selection instruction (S2) to the key (20) thus causing the electronic key (20) to carry out the subsequent communication in the passive communications mode.

[Fortsetzung auf der nächsten Seite]

WO 01/29352 A1

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

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.

(57) Zusammenfassung: Verfahren zur Zugangskontrolle insbesondere zu einem Kraftfahrzeug (F), bei dem zwischen einem Slüssel (20) und einer Basisstation (10) in einem aktiven oder einem passiven Kommunikationsmodus diese Einrichtungen (10, 20) drahtlos Authentifizierungsdaten austauschen, wobei zu Beginn dieses Authentifizierungsprozesses die Basisstation (10) an den Schlüssel (20) ein Aufrufsignal (WA) sendet und dieser auf das Aufrufsignal (WA) mit einem Antwortsignal (R) antwortet, und wobei die Basisstation (10) das von ihr empfangene Antwortsignal (R) des elektronischen Schlüssels (20) daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal (R) empfangen wurde, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im aktiven Kommunikationsmodus empfangen wurde, an den Schlüssel (20) einen ersten Selektionsbefehl (S1) sendet, welcher bewirkt, daß der (20) die darauffolgende Kommunikation im aktiven Kommunikationsmodus ausführt, und daß für den Fall, daß das Antwortsignal (R) des Schlüssels (20) im passiven Kommunikationsmodus empfangen wurde, die Basisstation (10) an den Schlüssel (10) einen zweiten Selektionsbefehl (S2) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die nachfolgende Kommunikation im passiven Kommunikationsmodus ausführt.

Verfahren und Vorrichtung zur Zugangskontrolle zu einem gesicherten Ort, insbesondere einem Kraftfahrzeug

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Zugangskontrolle zu einem gesicherten Ort, insbesondere zu einem Kraftfahrzeug, bei dem zwischen einem elektronischen Schlüssel und einer Basisstation in einem aktiven oder einem passiven Kommunikationsmodus diese Einrichtungen drahtlos Authentifizierungsdaten austauschen, wobei zu Beginn dieses Authentifizierungsprozesses die Basisstation an den elektronischen Schlüssel ein Aufrufsignal sendet und dieser auf das Aufrufsignal mit einem Antwortsignal antwortet, und wobei im aktiven Kommunikationsmodus eine Sicherungsprozedur gegen eine Funkstreckenverlängerung durchgeführt wird, sowie eine Vorrichtung zur Durchführung dieses Verfahrens.

Ein Verfahren und eine Vorrichtung der eingangs genannten Art sind in der älteren internationalen Patentanmeldung PCT/DE99/02178 beschrieben. Hierbei ist vorgesehen, daß die zwischen dem elektronischen Schlüssel und der Basisstation ablaufende Sicherungsprozedur derart erfolgt, daß im aktiven Betriebsmodus die Kommunikation zwischen dem elektronischem Schlüssel und der Basisstation über UHF-Frequenzen erfolgt, wobei die Reichweite der Übertragung zwischen dem elektronischen Schlüssel und der Basisstation begrenzt ist, um zu gewährleisten, daß die Kommunikationsverbindung unterbrochen wird, wenn sich die im Besitz des Schlüssels befindliche Person aus der unmittelbaren Nähe des gesicherten Ortes, z. B. des Kraftfahrzeugs, entfernt.

Um nun zu verhindern, daß ein derartiges passives Zugangskontrollsystem nicht dadurch außer Kraft gesetzt wird, daß ein unbefugter Angreifer das von der Basisstation ausgesandte Aufrufsignal an den elektronischen Schlüssel abfängt, das abgefangene Signal über eine Funkstreckenveränderung an einen weiteren Angreifer, der sich in der Nähe des elektronischen Schlüssels befindet, weitersendet und der weitere Angreifer dann das Antwortsignal des elektronischen Schlüssels auf das Aufrufsignal der Basisstation über die Funkstreckenverlängerung wieder zurück zum

ersten Angreifer und über diesen zurück zur Basisstation sendet, ist bei dem bekannten Verfahren vorgesehen, daß der elektronische Schlüssel der Basisstation ein Signal übermittelt, das von der Basisstation in spektrale Daten umgesetzt wird. Die Basisstation gewährt dann nur Zugang zu dem gesicherten Ort, wenn bei der Übertragung der Authentifizierungsdaten diese spektralen Daten mit einer in der Basisstation gespeicherten spektralen Signatur des elektronischen Schlüssels übereinstimmen. Hierbei ist vorgesehen, daß das von dem elektronischen Schlüssel ausgesandte Signal mindestens zwei Töne mit unterschiedlichen Frequenzen f_1 bzw. f_2 umfaßt, und daß die spektralen Daten Töne dritter Ordnung des übermittelten Signals darstellen, die von der Basisstation auf den Frequenzen $2f_1$-f_2 und $2f_2$-f_1 gemessen wird. Liegt die empfangene Signalstärke dieser Nebenlinien des vom elektronischen Schlüssel ausgesandten Signals über einem vordefinierten Wert, so interpretiert dies die Basisstation als sicheres Anzeichen dafür, daß eine Funkstreckenverlängerung durchgeführt wurde, und verweigert den Zugang zum gesicherten Ort.

Um beim Ausfall des aktiven Kommunikationsmodus im Rahmen eines sogenannten Back-up-Modus, also eines passiven Kommunikationsmodus, dem Benutzer der elektronischen Zugangskontrolle noch die Möglichkeit zu geben, den gesicherten Ort betreten zu können, ist vorgesehen, daß in diesem passiven Kommunikationsmodus eine Datenübertragung zwischen dem elektronischen Schlüssel und der Basisstation durch eine passive Modulation des von der Basisstation ausgesandten Erregerfeldes erfolgt: Der elektronische Schlüssel verstimmt entsprechend den zu sendenden Daten seinen Ressonanzkreis, was von der Basisstation als zusätzliche Belastung ihres Schwingkreises gemessen werden kann. Diese auf LF-Frequenzen erfolgende passive Kommunikation ist auf wenige Zentimeter beschränkt, was bedeutet, daß ein potentieller Angreifer seine entsprechende Antenne sehr nahe an die Sendeantenne der Basisstation plazieren muß, um in diesem Back-up-Modus zu arbeiten, wenn er versucht, die vom Schlüssel ausgesandten Datensignale auf einer LF-Frequenz im Back-up-Modus an die Basisstation zu senden. Das bekannte Verfahren sowie die nach diesem Verfahren arbeitenden bekannten Vorrichtungen besitzen den Nachteil, daß sie keinen wirksamen Schutz gegen einen auf diese vorgenannte Art und Weise erfolgenden Angriff bieten.

Es ist daher Aufgabe der Erfindung, ein Verfahren und eine Vorrichtung der eingangs genannten Art derart weiterzubilden, daß ein wirksamer Schutz gegen eine Funkstreckenverlängerung im passiven Kommunikationsmodus gegeben ist.

Diese Aufgabe wird durch das erfindungsgemäße Verfahren dadurch gelöst, daß die Basisstation das von ihr empfangene Antwortsignal des elektronischen Schlüssels daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal empfangen wurde, und daß die Basisstation für den Fall, daß das Antwortsignal des elektronischen Schlüssels im aktiven Kommunikationsmodus empfangen wurde, an den elektronischen Schlüssel einen ersten Selektionsbefehl sendet, welcher bewirkt, daß der elektronische Schlüssel die darauffolgende Kommunikation im aktiven Kommunikationsmodus ausführt, und daß für den Fall, daß das Antwortsignal des elektronischen Schlüssels im passiven Kommunikationsmodus empfangen wurde, die Basisstation an den elektronischen Schlüssel einen zweiten Selektionsbefehl sendet, welcher bewirkt, daß der elektronische Schlüssel die nachfolgende Kommunikation im passiven Kommunikationsmodus ausführt.

Durch das erfindungsgemäße Verfahren wird in vorteilhafter Art und Weise erreicht, daß auch im passiven Kommunikationsmodus zwischen dem elektronischen Schlüssel und der Basisstation ein entsprechender Angriff einer nicht authorisierten Person abgewehrt werden kann, indem die Basisstation aktiv auf die Kommunikationsart, in der sie das Antwortsignal des elektronischen Schlüssels empfängt, reagiert. Wenn das Antwortsignal im aktiven Kommunikationsmodus erfolgt, wird das weitere Authentifizierungsverfahren im aktiven Kommunikationsmodus durchgeführt und eine Funkstreckenverlängerung kann durch die bekannte Sicherungsprozedur ausgeschlossen werden. Wenn aber die Basisstation das Antwortsignal des elektronischen Schlüssels im passiven Kommunikationsmodus empfängt, verhindert sie bis zum Abschluß der Zugangsprozedur in vorteilhafter Art und Weise eine Kommunikation zwischen Basisstation und Schlüssel über den ersten, aktiven Kommunikationsmodus. Es ist somit nicht möglich, daß ein Angreifer über eine Frequenz des aktiven Kommunikationsmodus eine Funkstreckenverlängerung durchführt.

Vorteilhafte Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Weitere Einzelheiten und Vorteile der Erfindung sind dem Ausführungsbeispiel zu entnehmen, das im folgenden anhand der einzigen Figur beschrieben wird. Es zeigt:

Figur 1 eine Prinzipskizze eines Ausführungsbeispiels des des Verfahrens.

In Figur 1 ist nun die typische Konstellation dargestellt, die Ausgangspunkt des nachstehend beschriebenen Verfahrens zur Zugangskontrolle zu einem gesicherten Ort, hier zu einem Kraftfahrzeug F, ist. Im Kraftfahrzeug F ist eine Basisstation 10 angeordnet, welche drahtlos mit einem elektronischen Schlüssel 20 Authentifizierungsdaten austauscht, um zu gewährleisten, daß nur der Besitzer des elektronischen Schlüssels 20 Zugang zu dem gesicherten Ort erhalten kann. Hierzu ist vorgesehen, daß die Basisstation 10 in einem aktiven, ersten Kommunikationsmodus ein Aufrufsignal WA für den elektronischen Schlüssel 20 aussendet, wenn ein Betätigungsorgan B, z. B. ein Türgriff, am Kraftfahrzeug F betätigt wird. Der elektronische Schlüssel 20 antwortet daraufhin im aktiven Kommunikationsmodus mit einem entsprechenden Antwortsignal R, womit eine in dem aktiven Kommunikationsmodus ablaufende Kommunikationsverbindung zwischen dem elektronischen Schlüssel 20 und der Basisstation 10 hergestellt ist. Die zwischen dem elektronischen Schlüssel 20 und der Basisstation 10 übermittelten Daten werden durch ein an und für sich bekanntes und daher nicht mehr näher beschriebenes Kommunikationsprotokoll bestimmt, welches der elektronische Schlüssel 20 und die Basisstation 10 befolgen und die Übermittlung von Authentifizierungsdaten vom elektronischen Schlüssel 20 an die Basisstation 10 beinhaltet. Der Zugang zu dem gesicherten Kraftfahrzeug F wird von der Basissation 10 nur dann zugelassen, wenn die vom elektronischen Schlüssel 20 übermittelten Authentifizierungsdaten mit den von der Basisstation 10 gespeicherten Authentifizierungen übereinstimmen. Hierbei ist vorgesehen, daß die vom elektronischen Schlüssel 20 und/oder von der Basisstation 10 ausgesandten Signale nur eine begrenzte Reichweite aufweisen, um zu verhindern, daß von der Basisstation 10 Zugang zu dem gesicherten Kraftfahrzeug F auch dann gewährt wird, wenn sich der elektronische Schlüssel 20 nicht innerhalb einer definierten Umgebung - typischerweise einige wenige Meter - des Kraftfahrzeugs F befindet.

Um nun zu verhindern, daß sich Angreifer zu dem gesicherten Kraftfahrzeug F dadurch Zugang verschaffen, daß ein erster Angreifer A das von der Basisstation 10 im ersten, aktiven Kommunikationsmodus ausgesandte Aufrufsignal WA mittels einer

Funkstreckenverlängerung V zu einem zweiten Angreifer B leitet, dieser daraufhin das Aufrufsignal WA der Basisstation 10 an den sich außerhalb der Reichweite der Basisstation 10 befindliche elektronische Schlüssel 20 leitet, das Antwortsignal R des elektronischen Schlüssels 20 auffängt, über die Funkstreckenverlängerung V dem ersten Angreifer A weiterleitet und dieser dann das Antwortsignal R des elektronischen Schlüssels 20 an die Basisstation 10 weiterleitet, ist vorgesehen, daß die zwischen dem elektronischen Schlüssel 20 und der Basisstation 10 im ersten, aktiven Kommunikationsmodus stattfindenden Kommunikation auch eine Sicherheitsprozedur aufweist, welche es gestattet, eine derartige Funkstreckenverlängerung V der entsprechenden Signale WA, R zu erkennen und gegebenenfalls daraufhin die Kommunikation abzubrechen. Eine derartige Sicherheitsprozedur ist z. B. in der älteren internationalen Patentanmeldung PCT/DE99/02178 beschrieben, auf die zur Vermeidung von Wiederholungen bezug genommen wird und deren Offenbarung durch diese Bezugnahme explizit zum Gegenstand der hier vorliegenden technischen Lehre gemacht wird. Sie wird dort dadurch realisiert, daß der elektronische Schlüssel 20 im Rahmen seines als Reaktion auf das Aufrufsignal WA der Basisstation 10 generierten Antwortsignals R ein Kennungssignal übermittelt, das die Basisstation 10 in spektrale Daten umsetzt und nur dann die Kommunikation mit dem elektronischen Schlüssel 20 fortsetzt, wenn die von ihr empfangenen spektralen Daten mit der spektralen Signatur des elektronischen Schlüssels 20, die in der Basisstation 10 gespeichert ist, übereinstimmt. Insbesondere ist hierbei vorgesehen, daß der elektronische Schlüssel 20 zwei Töne mit der Frequenz f_1 bzw. f_2 aussendet, die nachher von der Basisstation 10 gemessen werden. Es werden aber nicht nur die beiden Töne f_1 und f_2, sondern auch Mischungen der beiden Grundtöne höherer Ordnung empfangen, welche in von den Grundtönen frequenzmäßig separierten Freqenzkanälen empfangen werden. Wenn nun die empfangene Signalstärke insbesondere der Nebenlinien dritter Ordnung über einem vordefinierten Wert liegt, ist das ein sicheres Indiz dafür, daß das empfangene Signal des elektronischen Schlüssels 20 über eine Funkstreckenverlängerung V geleitet wurde. In diesem Fall bricht dann die Basisstation 10 die Kommunikation mit dem elektronischen Schlüssel 20 ab und sperrt den Zugang zu dem gesicherten Kraftfahrzeug F.

Da aber üblicherweise vorgesehen ist, daß der elektronische Schlüssel 20 mit der Basisstation 10 nicht nur über im vorstehend beschriebenen aktiven Kommunikationsmodus, sondern auch im sogenannten Back-up-Modus in einem

zweiten, passiven Kommunikationsmodus miteinander zu kommunizieren in der Lage sein sollen, ist es erforderlich, auch in diesem passiven Kommunikationsmodus, in dem die Sicherungsprozedur des aktiven Kommunikationsmodus nicht funktioniert, eine weitere Sicherungsprozedur für eben diesen passiven Kommunikationsmodus vorzusehen.

Dies wird in vorteilhafter Art und Weise dadurch erreicht, daß die Basisstation 10 nicht nur den Informationsgehalt der ihr zugeführten Signale, insbesondere des Antwortsignals R des Schlüssels 20 auswertet, sondern auch untersucht, ob die ihr zugeführten Signale des elektronischen Schlüssels 20 im ersten, aktiven Kommunikationsmodus oder im zweiten, passiven Kommunikationsmodus empfangen werden. Empfängt die Basisstation 10 das als Reaktion auf einen von ihr ausgesandten Aufrufbefehl WA vom elektronischen Schlüssel 20 generierte Antwortsignal R im ersten, aktiven Kommunikationsmodus, so sendet sie als Reaktion auf das im aktiven Kommunikationsmodus erhaltene Antwortsignal R des elektronischen Schlüssels 20 an diesen ein erstes Selektionssignal S1, welches - neben den üblichen Funktionen eines Selektionssignals - bewirkt, daß zumindest die sicherheitsrelevante und vorzugsweise die gesamte weitere Kommunikation zwischen dem elektronischen Schlüssel 20 und der Basisstation 10 ausschließlich im ersten, aktiven Kommunikationsmodus durchgeführt wird und die Durchführung des verbleibenden Authentifizierungsprozesses im passiven Kommunikationsmodus unterbunden wird. Dies hat den Vorteil, daß eine Funkstreckenverlängerung V durch die Sicherungsprozedur des aktiven Kommunikationsmodus detektierbar ist und gegebenenfalls entsprechende Maßnahmen gegen einen Angriff einer nicht-authorisierten Person vorgenommen werden können.

Empfängt jedoch die Basisstation 10 des Kraftfahrzeugs F das Antwortsignal R des elektronischen Schlüssels 20 im zweiten, passiven Kommunikationsmodus, so sendet sie als Reaktion darauf an den elektronischen Schlüssel 20 ein zweites Selektionssignal S2, welches in entsprechender Art und Weise bewirkt, daß die Kommunikation des weiteren Authentifizierungsvorgangs im zweiten, passiven Kommunikationsmodus durchgeführt wird, und eine Durchführung des verbleibenden Authentifizierungsvorgangs im ersten Kommunikationsmodus unterbunden wird. Es ist somit einem eine im aktiven Kommunikationsmodus arbeitende

Funkstreckenverlängerung V verwendenden Angreifer nicht mehr möglich, diese erfolgreich einzusetzen.

PATENTANSPRÜCHE

1. Verfahren zur Zugangskontrolle zu einem gesicherten Ort, insbesondere zu einem Kraftfahrzeug (F), bei dem zwischen einem elektronischen Schlüssel (20) und einer Basisstation (10) in einem aktiven oder einem passiven Kommunikationsmodus diese Einrichtungen (10, 20) drahtlos Authentifizierungsdaten austauschen, wobei zu Beginn dieses Authentifizierungsprozesses die Basisstation (10) an den elektronischen Schlüssel (20) ein Aufrufsignal (WA) sendet und dieser auf das Aufrufsignal (WA) mit einem Antwortsignal (R) antwortet, und wobei im aktiven Kommunikationsmodus eine Sicherungsprozedur gegen eine Funkstreckenverlängerung (V) durchgeführt wird, **dadurch gekennzeichnet,** daß die Basisstation (10) das von ihr empfangene Antwortsignal (R) des elektronischen Schlüssels (20) daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal (R) empfangen wurde, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im aktiven Kommunikationsmodus empfangen wurde, an den elektronischen Schlüssel (20) einen ersten Selektionsbefehl (S1) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die darauffolgende Kommunikation im aktiven Kommunikationsmodus ausführt, und daß für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im passiven Kommunikationsmodus empfangen wurde, die Basisstation (10) an den elektronischen Schlüssel (10) einen zweiten Selektionsbefehl (S2) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die nachfolgende Kommunikation im passiven Kommunikationsmodus ausführt.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß die Sicherungsprozedur des aktiven Kommunikationsmodus dadurch ausgeführt wird, daß der elektronische Schlüssel (20) im Rahmen seines als Reaktion auf das Aufrufsignal (WA) der Basisstation (10) generierten Antwortsignals (R) eine

Kennung an die Basisstation (10) übermittelt, welche die Basisstation (10) in spektrale Daten umsetzt und nur dann die Kommunikation mit dem elektronischen Schlüssel (20) fortsetzt, wenn die von ihr empfangenen spektralen Daten mit einer spektralen Signatur des elektronischen Schlüssels (20), die in der Basisstation (10) gespeichert ist, übereinstimmt.

3. Vorrichtung zur Zugangskontrolle zu einem gesicherten Ort (F), die eine Basisstation (10) und einen elektronischen Schlüssel (20) aufweist, wobei zwischen der Basisstation (10) und dem elektronischen Schlüssel (20) in einem aktiven oder passiven Kommunikationsmodus Authentifizierungsdaten ausgetauscht werden, wobei im aktiven Kommunikationsmodus die Basisstation (10) einer Sicherungsprozedur gegen eine Funkstreckenverlängerung (V) durchführt, **dadurch gekennzeichnet,** daß die Basisstation (10) ein von ihr empfangenes Antwortsignal (R) des elektronischen Schlüssels (20) daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal (R) empfangen wurde, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) empfangen wird, einen ersten Selektionsbefehl (S1) erzeugt und an den elektronischen Schlüssel (20) sendet, wobei der erste Selektionsbefehl (S1) bewirkt, daß der elektronische Schlüssel (20) die darauffolgende Kommunikation mit der Basisstation (10) im aktiven Kommunikationsmodus ausführt, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im passiven Kommunikationsmodus empfangen wurde, die Basisstation (10) einen zweiten Selektionsbefehl (S2) erzeugt und an den elektronischen Schlüssel (20) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die nachfolgende Kommunikation mit der Basisstation (10) im passiven Kommunikationsmodus ausführt.

4. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,** daß nach dem Empfang eines Selektionsbefehls (S1, S2) durch den elektronischen Schlüssel (20) dieser wenigstens die sicherheitsrelevanten Daten des Authentifizierungsprozesses in dem die empfangene Selektionsbefehle (S1, S2) entsprechenden Kommunikationsmodus durchführt.

5. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,** daß nach dem Empfang eines Selektionsbefehls (S1, S2) durch den elektronischen Schlüssel (20) dieser wenigstens den gesamten darauffolgenden Authentifizierungsprozess in dem die empfangene Selektionsbefehle (S1, S2) entsprechenden Kommunikationsmodus durchführt.

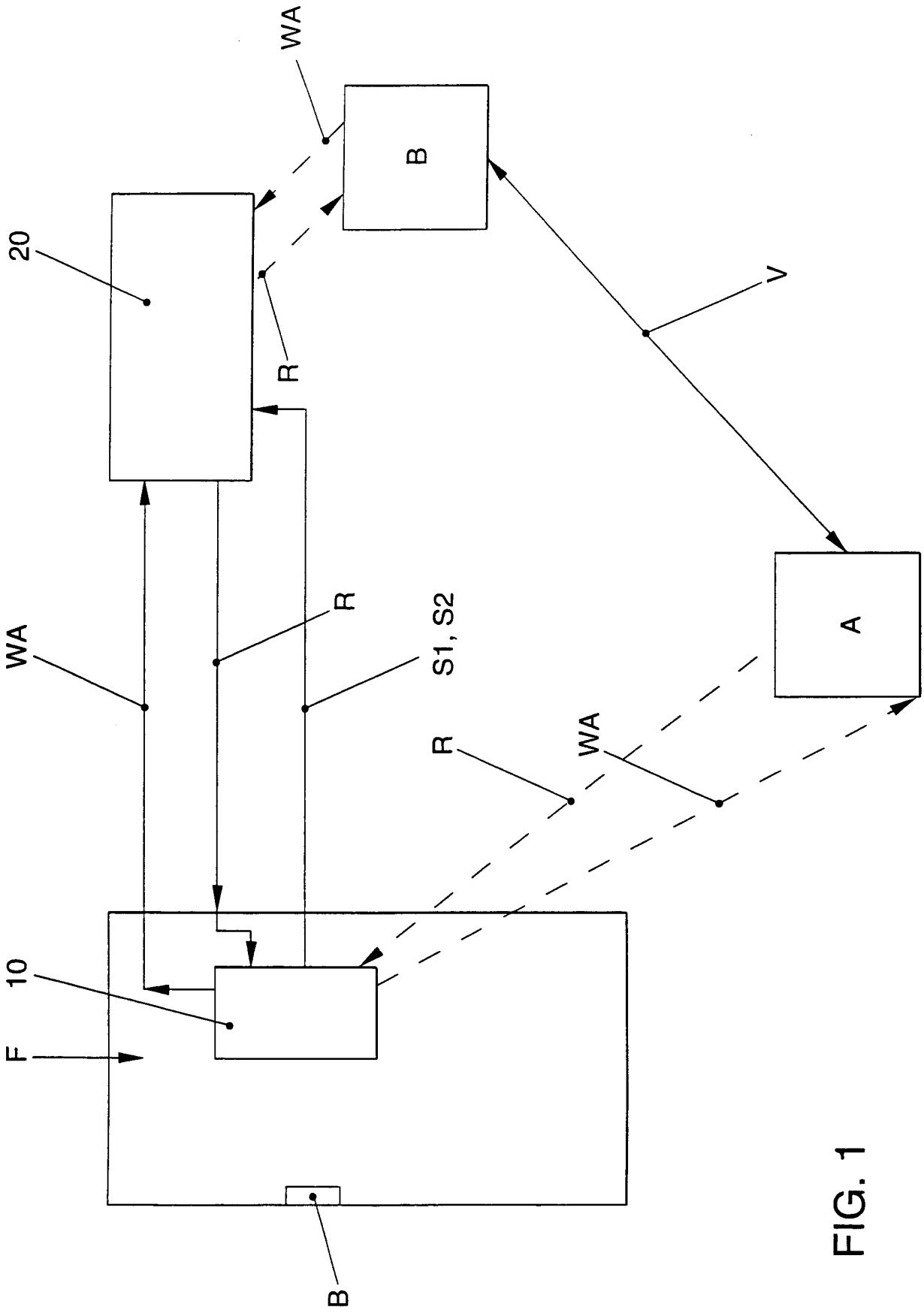


FIG. 1

INTERNATIONAL SEARCH REPORT

Inter ›nal Application No
PCT/EP 00/09276

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00

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 E05B B60R

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.
A	DE 43 29 697 A (SIEMENS AG) 9 March 1995 (1995-03-09) abstract; figures column 1, line 47 -column 2, line 10 column 3, line 31 - line 41 column 3, line 58 -column 4, line 2 column 6, line 44 - line 65 ---	1,3
A	EP 0 848 123 A (TEXAS INSTRUMENTS DEUTSCHLAND) 17 June 1998 (1998-06-17) abstract; figure 1 column 1, line 54 -column 2, line 49 column 5, line 5 -column 5, line 19 column 6, line 20 - line 53 column 9, line 48 - line 57 column 10, line 4 -column 11, line 15 --- -/--	1,3

[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
17 January 2001	24/01/2001

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	Buron, E

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/EP 00/09276

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 195 39 851 A (DAIMLER BENZ AG) 5 June 1997 (1997-06-05) abstract; figure column 4, line 16 -column 5, line 16 ---	1,3
A	DE 40 20 445 A (BAYERISCHE MOTOREN WERKE AG) 2 January 1992 (1992-01-02) abstract; figure column 1, line 40 - line 55 column 2, line 60 -column 3, line 10 -----	1,3

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/EP 00/09276

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4329697 A	09-03-1995	FR 2709512 A	10-03-1995
		GB 2282252 A,B	29-03-1995
		US 5552641 A	03-09-1996
EP 0848123 A	17-06-1998	JP 11177464 A	02-07-1999
DE 19539851 A	05-06-1997	FR 2740413 A	30-04-1997
		GB 2306573 A,B	07-05-1997
		IT RM960724 A	23-04-1998
		JP 2906042 B	14-06-1999
		JP 9175332 A	08-07-1997
		US 5869908 A	09-02-1999
DE 4020445 A	02-01-1992	DE 4003280 A	08-08-1991
		DE 59009066 D	14-06-1995
		EP 0440974 A	14-08-1991
		ES 2071738 T	01-07-1995

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/09276

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B B60R

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.
A	DE 43 29 697 A (SIEMENS AG) 9. März 1995 (1995-03-09) Zusammenfassung; Abbildungen Spalte 1, Zeile 47 -Spalte 2, Zeile 10 Spalte 3, Zeile 31 - Zeile 41 Spalte 3, Zeile 58 -Spalte 4, Zeile 2 Spalte 6, Zeile 44 - Zeile 65 ---	1,3
A	EP 0 848 123 A (TEXAS INSTRUMENTS DEUTSCHLAND) 17. Juni 1998 (1998-06-17) Zusammenfassung; Abbildung 1 Spalte 1, Zeile 54 -Spalte 2, Zeile 49 Spalte 5, Zeile 5 -Spalte 5, Zeile 19 Spalte 6, Zeile 20 - Zeile 53 Spalte 9, Zeile 48 - Zeile 57 Spalte 10, Zeile 4 -Spalte 11, Zeile 15 --- -/--	1,3

[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
17. Januar 2001	24/01/2001

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	Buron, E

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/09276

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 195 39 851 A (DAIMLER BENZ AG) 5. Juni 1997 (1997-06-05) Zusammenfassung; Abbildung Spalte 4, Zeile 16 -Spalte 5, Zeile 16	1,3
A	DE 40 20 445 A (BAYERISCHE MOTOREN WERKE AG) 2. Januar 1992 (1992-01-02) Zusammenfassung; Abbildung Spalte 1, Zeile 40 - Zeile 55 Spalte 2, Zeile 60 -Spalte 3, Zeile 10	1,3

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP 00/09276

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4329697 A	09-03-1995	FR 2709512 A	10-03-1995
		GB 2282252 A,B	29-03-1995
		US 5552641 A	03-09-1996
EP 0848123 A	17-06-1998	JP 11177464 A	02-07-1999
DE 19539851 A	05-06-1997	FR 2740413 A	30-04-1997
		GB 2306573 A,B	07-05-1997
		IT RM960724 A	23-04-1998
		JP 2906042 B	14-06-1999
		JP 9175332 A	08-07-1997
		US 5869908 A	09-02-1999
DE 4020445 A	02-01-1992	DE 4003280 A	08-08-1991
		DE 59009066 D	14-06-1995
		EP 0440974 A	14-08-1991
		ES 2071738 T	01-07-1995