

(12)

Patentschrift

(21) Anmeldenummer: A 2060/2006

(51) Int. Cl.⁸: **G07C 9/00**
H04Q 7/38

(22) Anmeldetag: 2006-12-13

(43) Veröffentlicht am: 2009-05-15

(56) Entgegenhaltungen:

US 2005/0210283A1

WO 2002/039674A1

WO 2002/031778A1

WO 2001/023694A1 GB 2416964A

DE 10316307A1

(73) Patentanmelder:

CSANK CHRISTIAN

A-2840 GRIMMENSTEIN (AT)

(72) Erfinder:

CSANK CHRISTIAN

GRIMMENSTEIN (AT)

(54) VERFAHREN ZUR AUTHENTIFIZIERUNG EINES MOBILFUNKENDGERÄTES

(57) Die Erfindung betrifft ein Verfahren sowie eine Authentifizierungsvorrichtung (AVO) zur Authentifizierung eines Mobilfunkendgerätes (MFE), das durch Identifikationsmittel (IDM) eindeutig charakterisierbar ist, wobei die Authentifizierungsvorrichtung einen bestimmten Sende- und Empfangsbereich (SEB) abdeckt und die Identifikationsmittel des Mobilfunkendgeräts in zumindest einer Speichereinheit (SPE1, SPE2, SPE3) speichern kann, wobei die Authentifizierungsvorrichtung mit dem zumindest einen Mobilfunkendgerät einen Verbindungsaufbau initiiert, sobald das zumindest eine Mobilfunkendgerät sich in ihrem Sende- und Empfangsbereich befindet, und die Authentifizierungsvorrichtung weiters über Funk die Identifikationsmittel des zumindest einen Mobilfunkendgeräts abfragt und überprüft, ob sie mit den in der zumindest einen Speichereinheit gespeicherten Identifikationsmitteln identisch sind, wobei im Fall, dass sie identisch sind, die Authentifizierungsvorrichtung die Verbindung abbricht und eine Aktion ausführt, während im Fall, dass die Identifikationsmittel des zumindest einen Mobilfunkendgeräts nicht mit den in der zumindest einen Speichereinheit gespeicherten Identifikationsmitteln identisch sind, die Authentifizierungsvorrichtung die Verbindung abbricht und keine Aktion ausführt.

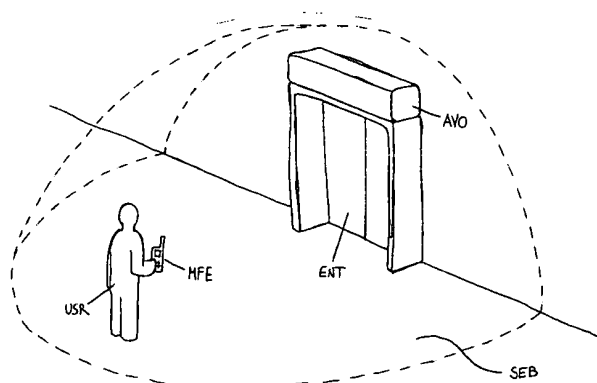


Fig. 1

Die Erfindung betrifft die Erfindung ein Verfahren zur Authentifizierung eines Mobilfunkendgerätes, das durch Identifikationsmittel eindeutig charakterisierbar ist, durch eine Authentifizierungsvorrichtung, die in einer Speichervorrichtung mit zumindest einer Speichereinheit die Identifikationsmittel des zumindest einen Mobilfunkendgeräts speichern kann und die einen bestimmten Sende- und Empfangsbereich abdeckt, wobei die Authentifizierungsvorrichtung mit dem zumindest einen Mobilfunkendgerät einen Verbindungsaufbau initiiert, sobald das zumindest eine Mobilfunkendgerät sich im Sende- und Empfangsbereich der Authentifizierungsvorrichtung befindet und die Authentifizierungsvorrichtung über Funk die Identifikationsmittel des zumindest einen Mobilfunkendgeräts abfragt und überprüft, ob sie mit den in der Speichervorrichtung mit zumindest einer Speichereinheit gespeicherten Identifikationsmitteln identisch sind.

Weiters betrifft die Erfindung eine Authentifizierungsvorrichtung die zur Authentifizierung von zumindest einem Mobilfunkendgerät, das mittels Identifikationsmitteln eindeutig charakterisierbar ist, zumindest ein Such-Modul für die Suche nach Mobilfunkendgeräten im Sende- und Empfangsbereich der Authentifizierungsvorrichtung sowie zumindest ein Verbindungs-Modul für den Verbindungsaufbau mit gefundenen Mobilfunkendgeräten aufweist, wobei weiters eine Speichervorrichtung mit zumindest einer Speichereinheit vorgesehen ist, in der die Identifikationsmittel der authentifizierten Mobilfunkendgeräte gespeichert sind, und die Authentifizierungsvorrichtung dazu eingerichtet ist, nach Initiierung eines Verbindungsaufbaus mittels des Verbindungs-Moduls über Funk die Identifikationsmittel des zumindest einen Mobilfunkendgeräts abzufragen und mit den in der Speichervorrichtung gespeicherten Identifikationsmitteln auf Identität zu überprüfen.

Es gibt unterschiedliche Verfahren zur Authentifizierung von Personen, beispielsweise um ein Fahrzeug in Betrieb zu nehmen, einen Computer zu verwenden oder Zutritt zu einem gesicherten Bereich zu gewähren, der mit einer Tür verschlossen ist. Häufig werden im letzten Fall Schlüssel verwendet, die den Nachteil haben, dass zum Öffnen unterschiedlicher Türen eine Vielzahl von Schlüsseln mitgeführt werden muss. Neben dem Nachteil, dass solche Türen durch geschicktes Hantieren auch ohne Schlüssel geöffnet werden können, kann der Schlüssel auch von Unbefugten verwendet werden, die so Zutritt zu gesicherten Bereichen erlangen. Ähnliche Probleme stellen sich bei der Verwendung von Schlössern, die mittels der Eingabe eines Codes über ein Tastenfeld geöffnet werden können.

In den letzten Jahren wurden zur Authentifizierung zunehmend beispielsweise Lesegeräte für Chip- oder Magnetkarten verwendet, mit denen nach Prüfung einer Zugangsberechtigung eine entsprechende Tür geöffnet wird. Das Problem dabei ist, dass bei häufiger Verwendung dieser Art von Authentifizierung eine Person beispielsweise Unmengen von Chipkarten bei sich tragen muss, um verschiedene Bereiche betreten zu können. Durch die Empfindlichkeit der Karten auf mechanische Einwirkung, aber auch elektrische oder magnetische Felder ist die Störanfälligkeit sehr hoch. Außerdem kann bei Verlust einer Karte auch unbefugten Personen der Zugang zu gesicherten Bereichen ermöglicht werden.

Die US 2005/0210283 zeigt ein System zum Öffnen von Türen mittels Bluetooth. Bei dem bekannten System kommuniziert ein Mobilfunktelefon, welches eine entsprechende Bluetooth Sende/Empfangseinheit aufweist, mit einer Authentifizierungseinheit, die ein Türschloss steuert. Bei dem bekannten Verfahren wird im Rahmen eines vorab durchzuführenden Setups in einem Speicher des Mobilfunktelefons ein Identifikationscode der Authentifizierungseinheit abgelegt. Befindet sich das Mobilfunktelefon in einem Empfangsbereich der Authentifizierungseinheit so kann von dem Benutzer über eine entsprechende Eingabe über das Mobilfunktelefon ein Verbindungsaufbau mit der Authentifizierungseinheit hergestellt werden. Nachteilig an dem bekannten Verfahren ist zum einen, dass ein aufwendiges Setup erforderlich ist, um den Identifikationscode der Authentifizierungseinheit in das Mobilfunktelefon zu laden. Zum anderen ist ein aufwendiger Umbau herkömmlicher bluetoothfähiger Mobilfunktelefone erforderlich, um einen aktiven Verbindungsaufbau einer Bluetooth-Verbindung initiieren zu können.

Aus der WO2002/039674 A1 ist beispielsweise ein Bluetooth Network Acces Point bekannt geworden, der zusätzliche Sender/Empfänger aufweist, um eine bessere Funktionsweise zu erzielen.

- 5 Die WO 2002/031778 A1 bezieht sich auf ein Verfahren zum Öffnen einer Tür mittels eines elektronischen Schlüssels, der über eine Funkverbindung mit einem Schloss Daten austauschen kann. Vor Öffnen der Tür wird von einer mit einem Schloss verbundenen Sende/Empfangseinheit ein zufälliges Signal an den Schlüssel gesendet, welcher dieses Signal verschlüsselt an die Sende/Empfangseinheit zurücksendet. Die Sende/Empfangseinheit ent-
10 schlüsselt hierauf das empfangene Signal und vergleicht dieses mit dem ursprünglich übermittelten. Bei Übereinstimmung des empfangenen Signals mit ursprünglich gesendeten wird das Schloss geöffnet. Bei dem bekannten Verfahren kommt ein Paar von Schlüsseln zum Einsatz, wie es beispielsweise beim PGP-System Verwendung findet, wobei der „Public Key“ in der mit dem Schloss verbundenen Sende/Empfangseinheit und der „Privat Key“ in dem elektronischen Schlüssel gespeichert ist. Nachteilig an diesem Verfahren sind vor allem der relativ hohe Rechenaufwand für die Ver/Entschlüsselung und die aufwendige Implementierung.

- Die WO 2001/023694 A1 bezieht sich auf ein System zur Zugangskontrolle, beispielsweise zum Öffnen einer Tür oder zur Benutzung eines Computers, mittels eines bluetoothfähigen Mobilfunkendgerätes. Bei dem bekannten System ist eine Authentifizierungsvorrichtung vorgesehen, welche nach erfolgtem Verbindungsaufbau mit dem Mobilfunkendgerät und gewährtem Zugriffsrecht permanent überprüft, ob dieses Gerät noch in einem Empfangsbereich vorhanden und aktiv ist. Wird diese Verbindung von Seiten des Mobilfunktelefons unterbrochen wird der weitere Zugriff verweigert. Weiters ist zum Öffnen einer Tür jedes Mal die Eingabe eines PIN Codes
25 zwingend erforderlich.

- Die GB2416 964 A offenbart ein System zum Öffnen einer Tür, bei welchem eine bluetoothfähige Vorrichtung zur Überprüfung, ob sich ein bluetoothfähige Mobilfunkendgerät in der Nähe der Tür befindet, verwendet wird. Gemäß der technischen Lehre dieses Dokuments wird die Identität der Mobilfunkendgeräte anhand einer Geräte-ID überprüft, wobei j bei einer Übereinstimmung der Geräte-ID mit einer gespeicherten ID eine Entfernungsmessung gestartet wird.

- Die DE 103 16 307 A1 zeigt ein System zum berührungslosen Öffnen einer Fahrzeugtür mittels einer Bluetooth Funkstrecke.

- 35 Durch die weltweite Verbreitung von Mobilfunkendgeräten in den letzten Jahren wurde auch die Verwendung dieser Geräte zur Authentifizierung in Erwägung gezogen. Unter einem Mobilfunkendgerät wird in diesem Dokument jedes Endgerät verstanden, welches über Funk mit einem anderen Endgerät Daten austauschen kann, beispielsweise Mobilfunktelefone und Personal Digital Assitants (PDAs).

Die große Anzahl an möglichen Funkstandards von GSM, WAP, UMTS über GPRS und Bluetooth bis hin zu W-LAN lässt eine Vielzahl von Anwendungen zu.

- 45 Vielen derartigen Anwendungen ist gemeinsam, dass dabei auf den verwendeten Mobilfunkendgeräten zusätzliche Software installiert werden muss. Zusätzlich haben gängige derartige Verfahren eine Vielzahl von weiteren Nachteilen.

- Es ist daher eine Aufgabe der Erfindung, ein einfaches und sicheres Verfahren für die Authentifizierung von Mobilfunkendgeräten, bzw. eine entsprechende Vorrichtung, zu ermöglichen.

- 55 Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art erfindungsgemäß dadurch gelöst, dass im Fall, dass die Identifikationsmittel identisch sind, die Authentifizierungsvorrichtung den Verbindungsaufbau abbricht und eine Aktion ausführt, während im Fall, dass die Identifikationsmittel des zumindest einen Mobilfunkendgeräts nicht mit den in der eine Spei-

chervorrichtung mit zumindest einer Speichereinheit gespeicherten Identifikationsmitteln identisch sind, die Authentifizierungsvorrichtung den Verbindungsaufbau abbricht und keine Aktion ausführt.

- 5 Die Identifikationsmittel umfassen dabei eine Identifikationsnummer, die eine herstellerseitig einmalig vergebene Gerätenummer ist. Diese Nummer ist eine gerätespezifische Nummer, die ein hohes Maß an Sicherheit gewährt, da sie weltweit nur ein einziges Mal vergeben wird.

10 In der Erfindung wird zur sicheren Authentifizierung der Mobilfunkeinheit der Paarbildungsprozeß des Bluetooth™-Funkstandards verwendet. Bluetooth™ ist ein in den 1990er Jahren entwickelter Industriestandard gemäß IEEE 802.15.1 für die drahtlose Funk-Vernetzung von Geräten über kurze Distanzen. Bluetooth™ benutzt eine drahtlose Schnittstelle, die im Großteil der heute verwendeten Mobilfunkendgeräte vorhanden ist und so die Verwendung des erfindungsgemäßen Verfahrens erleichtert. Außerdem umfasst Bluetooth™ unterschiedliche Sicherungsmechanismen, die ein hohes Maß an Sicherheit erlauben.

Bei Verwendung des Bluetooth™-Funkstandards beinhalten die Identifikationsmittel zusätzlich nach erfolgtem bluetooth™-spezifischen „Paarbildungsprozess“, der zwischen dem Mobilfunkendgerät und der Authentifizierungseinrichtung erfolgt, einen bei diesem „Paarbildungsprozess“ erzeugten bluetooth™-spezifischen Verbindungsschlüssel (auch: „Link Key“). Dieser Verbindungsschlüssel stellt üblicherweise einen 128 Bit-Schlüssel dar. Er bietet ein hohes Maß an Sicherheit, da er charakteristisch für die Verbindung zwischen zwei bestimmten Endgeräten ist. Außerdem erfolgt der Paarbildungsprozess und damit die Erzeugung des Verbindungsschlüssels erst dann, wenn die Verbindung von demjenigen Verbindungsteilnehmer, dem eine Verbindungsaufnahme angeboten wird, durch Eingabe eines PIN-Codes bestätigt wird, der zwischen 4 und 16 Byte lang sein kann. Um die Sicherheit zu erhöhen kann der PIN-Code optional auch nur einmalig gültig sein (One-Time-Code). Bei Verlust des Mobilfunkendgerätes muss auf Seiten der Authentifizierungsvorrichtung ein neuer PIN eingetragen werden, welcher dann ebenfalls nur einmal verwendet werden kann. So kann gewährleistet werden, daß die hohe Sicherheit des Link-Keys nicht mit der niedrigeren Sicherheit des PINs umgangen wird.

Gemäß einer vorteilhaften Variante der Erfindung sind die Identifikationsmittel von Mobilfunkendgeräten in zumindest einer internen Datenbank oder in zumindest einen externen Datenbank abgelegt, wobei, wenn die Authentifizierungsvorrichtung die Identifikationsmittel eines Mobilfunkendgeräts abfragt, das sich im Sende- und Empfangsbereich der Authentifizierungsvorrichtung befindet, überprüft wird, ob die Identifikationsmittel in der internen Datenbank oder in der externen Datenbank abgelegt sind, und bei einem Auffinden der Identifikationsmittel die Identifikationsmittel aus der internen Datenbank bzw. aus der externen Datenbank in die zumindest eine Speichereinheit übertragen werden und ein Verbindungsaufbau initiiert wird.

40 Die oben genannte Aufgabe lässt sich auch mit einer Authentifizierungsvorrichtung der eingangs erwähnten Art erfindungsgemäß dadurch lösen, dass die Authentifizierungsvorrichtung dazu eingerichtet ist, im Fall einer Identität der Identifikationsmittel den Verbindungsaufbau abubrechen und eine Aktion auszuführen, wobei die Authentifizierungsvorrichtung weiters dazu eingerichtet ist, im Fall fehlender Identität der Identifikationsmittel den Verbindungsaufbau abubrechen und keine Aktion auszuführen.

50 Eine vorteilhafte Variante des erfindungsgemäßen Systems lässt sich erzielen, indem die zumindest eine Speichereinheit direkt in dem zumindest einen Such-Modul angeordnet ist. Ein solches System lässt sich besonders platzsparend herstellen. Allerdings sind üblicherweise verwendete Speichereinheiten in ihrer Speicherfähigkeit begrenzt.

55 Besser ist es daher, wenn die Speichervorrichtung zumindest eine interne Datenbank umfasst, welche in der Authentifizierungsvorrichtung angeordnet ist. Dadurch kann die Anzahl der authentifizierbaren Mobilfunkendgeräte drastisch erhöht werden, da die interne Datenbank mit

einem größeren Speicher ausgestattet werden kann.

In einer weiteren Ausführungsform kann die Speichervorrichtung zumindest eine externe Datenbank umfassen, welche außerhalb der Authentifizierungsvorrichtung angeordnet ist. Durch die Anordnung außerhalb der Authentifizierungsvorrichtung kann die externe Datenbank auch von ihren physischen Abmessungen größer ausgestaltet werden, wodurch natürlich auch ein größerer Speicherplatz realisiert werden kann. Weiters kann die externe Datenbank von der Authentifizierungsvorrichtung entfernt angeordnet werden, beispielsweise auf einem zentralen Server.

Es ist weiters von Vorteil, wenn die Identifikationsmittel von Mobilfunkendgeräten in der zumindest einen internen Datenbank bzw. der zumindest einen externen Datenbank ablegbar und aus der zumindest einen Speichereinheit löscherbar sind. Dadurch kann verhindert werden, dass ein Verbindungsaufbau nicht möglich ist, weil der Speicherplatz der Speichereinheit aufgebraucht ist und keine weitere Verbindung mehr aufgebaut werden kann.

Bei dem zumindest einen Such-Modul sowie dem zumindest einen Verbindungs-Modul handelt es sich um Bluetooth™-Module. Es ist dadurch möglich, den Bluetooth™-Funkstandard zu verwenden, der weltweit als etabliert bezeichnet werden kann, da sehr viele heute in Gebrauch befindliche Mobilfunkendgeräte bereits bluetooth™-fähig sind.

Dabei können auch mehrere Such-Module vorgesehen sein. Es ist weiters von Vorteil, wenn diese mehreren Such-Module den Suchbetrieb zeitversetzt starten. Dadurch können Mobilfunkendgeräte, die sich im Sende- und Empfangsbereich der Authentifizierungsvorrichtung befinden, sehr viel schneller gefunden werden. Dies wird ermöglicht durch das so genannte 'asynchrone Suchen', das weiter unten noch genauer beschrieben ist.

Vorteilhafterweise kann die Reichweite des zumindest einen Such-Moduls und des zumindest einen Verbindungs-Moduls durch geräteinterne Dämpfung des Funksignals vermindert werden oder dadurch, dass man die Teile der Module, die das Funk-Signal abgeben und empfangen, mit einem dämpfenden Material umgibt. Ersteres kann beispielsweise mit einem Widerstand realisiert werden, zweiteres lässt sich durch Abschirmen der Antenne bzw. durch Einsatz von Richtfunkantennen erreichen. Wenn man die Reichweite der Module vermindert, kann man dadurch verhindern, dass man unbeabsichtigt mit der Authentifizierungsvorrichtung kommuniziert und ungewollt eine Aktion, z.B. das Öffnen einer Türe, auslöst.

Die Erfindung samt weiteren Vorteilen wird im Folgenden anhand einiger nicht einschränkender Ausführungsbeispiele näher erläutert, welche in der Zeichnung dargestellt sind. In dieser zeigen schematisch:

Fig. 1 eine schematische Darstellung der erfindungsgemäßen Vorrichtung,

Fig. 2 ein Mobilfunkendgerät,

Fig. 3a-b verschiedene Ausführungen einer erfindungsgemäßen Authentifizierungsvorrichtung und

Fig. 4 ein Blockdiagramm eines erfindungsgemäßen Verfahrens.

In Figur 1 ist beispielhaft eine Türe ENT dargestellt. Um diese Türe ENT öffnen zu können, muss ein Benutzer USB dafür authentifiziert werden. Bei erfolgter Authentifizierung öffnet sich die Tür. Zur Authentifizierung dient in diesem Fall ein Mobilfunkendgerät MFE, das mit der Authentifizierungsvorrichtung AVO über den Bluetooth™-Funkstandard kommuniziert. Der Vorteil an der Verwendung von Bluetooth™ liegt in seinen immanenten Sicherheitsmerkmalen und seiner begrenzten Reichweite. Je nach Sendeleistung kann Bluetooth™ über Strecken von bis zu 100 m verwendet werden. Im Beispiel von Figur 1 wird aber eine sehr viel geringere Leistung verwendet, sodass der Sende- und Empfangsbereich SEB sehr begrenzt ist. Neben verminderter Sendeleistung kann die Reichweite auch begrenzt werden, indem das Signal

gedämpft wird. Dabei ist es möglich, das Signal geräteintern, beispielsweise durch den Einbau eines Widerstandes, zu dämpfen, oder man verringert die Reichweite, indem man die Antenne mit dämpfenden Materialien abschirmt. Durch die geringe Reichweite wird unbeabsichtigte Kommunikation mit der Authentifizierungsvorrichtung AVO über große Distanzen verhindert.

Das Mobilfunkendgerät MFE weist entsprechend Figur 2 Identifikationsmittel IDM auf, die zumindest eine Identifikationsnummer IDN umfassen, die eine herstellerseitig einmalig vergebene Gerätenummer ist. Diese Nummer besteht aus 6 Byte und wird weltweit nur ein einziges Mal vergeben. Bei der Produktion des Bluetooth™-Chips, der im vorliegenden Beispiel in dem Mobilfunkendgerät verwendet wird, wird diese Nummer bei der Produktion des Chips auf diesem hinterlegt. Die Darstellung der Nummer erfolgt in einer sechsstelligen Hexadezimalzahl. Die ersten drei Blöcke bilden sich aus dem Herstellercode, die restlichen werden zu einer internen Kodierung verwendet.

Ein weiteres Identifikationsmittel IDM des Mobilfunkendgeräts MFE ist laut Figur 2 der bluetooth™-spezifische Verbindungsschlüssel VBS (auch: 'Link Key'). Dieser Verbindungsschlüssel VBS wird bei der ersten Kontaktaufnahme zwischen zwei bluetooth™-fähigen Geräten generiert. Dabei erfolgt von Seiten des Geräts, das den Verbindungsaufbau intiiert, eine PIN-Abfrage an das andere Gerät. Der PIN-Code, der daraufhin eingegeben werden muss, kann zwischen 6 und 16 Bytes lang sein. Wird der PIN korrekt eingegeben, kommt es zu einem Verbindungsaufbau und es erfolgt eine so genannte 'Paarbildung' (auch: 'Pairing') zwischen den beiden Geräten. Dabei wird die Identifikationsnummer des jeweils anderen Geräts direkt in den Bluetooth™-Chips gespeichert. Zudem wird der Verbindungsschlüssel VBS berechnet und generiert. Es handelt sich dabei um einen 128 Bit-Schlüssel, der zur Erhöhung der Sicherheit ebenfalls in den Bluetooth™-Chips gespeichert wird. Bei jedem weiteren Verbindungsaufbau zwischen den beiden Geräten wird dann überprüft, ob dieser Verbindungsschlüssel korrekt ist. Ist der Verbindungsschlüssel VBS korrekt, muss dann in weiterer Folge kein PIN-Code mehr eingegeben werden.

Betreffend das beschriebene Beispiel der erfindungsgemäßen Vorrichtung bedeutet das, dass Mobilfunkendgeräte durch ihre Identifikationsnummer IDN, bei erstmaliger Kontaktaufnahme durch den PIN-Code und weiters durch den bei der ersten Kontaktaufnahme und dann bei jeder weiteren Kontaktaufnahme überprüften Verbindungsschlüssel VBS authentifiziert werden. Diese Nummern stellen die Identifikationsmittel IDM eines Mobilfunkendgeräts MFE dar.

Wenn diese Identifikationsmittel IDM vollständig in der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO gespeichert sind, erfolgt jede weitere Authentifizierung automatisch. Im vorliegenden Fall bedeutet das: Der Benutzer USR nähert sich mit einem authentifizierten Mobilfunkendgerät MFE, mit dem bereits eine erste Kontaktaufnahme mit der Authentifizierungsvorrichtung erfolgt ist, einer Tür ENT. Sobald er den Sende- und Empfangsbereich SEB der Authentifizierungsvorrichtung AVO betreten hat, nimmt die Authentifizierungsvorrichtung AVO Kontakt mit dem Mobilfunkendgerät MFE auf und überprüft, ob dessen Identifikationsmittel IDM in der Speichervorrichtung SPV gespeichert sind. Ist das der Fall, öffnet sich die Tür ENT. Sollte das Mobilfunkendgerät MFE nicht authentifiziert und daher seine Identifikationsmittel nicht in der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO gespeichert sein, erfolgt ein Abbruch der Kontaktaufnahme und die Tür ENT bleibt geschlossen.

In den Figuren 3a bis 3c sind verschiedene Ausführungen einer Authentifizierungsvorrichtung AVO dargestellt. Grundsätzlich umfasst sie zumindest ein Such-Modul SM1, SM2 oder SM3, ein Verbindungsmodul VBM und eine Speichervorrichtung SPV mit zumindest einer Speichereinheit SPE1, SPE2 und SPE3, wie in Figur 3a dargestellt ist. Weiters umfasst die Authentifizierungsvorrichtung AVO einen oder mehrere Eingänge ENG und einen oder mehrer Ausgänge AUG1 und AUG2.

Der Eingang ENG dient dazu, die Vorrichtung nicht nur mit dem Mobilfunkendgerät MFE,

sondern auch mit anderen Mitteln zu bedienen, beispielsweise mit einem herkömmlichen Wechselschalter. Im vorliegenden Fall würde das bedeuten, dass die Türe ENT aus Figur 1 nicht nur geöffnet werden kann, indem ein berechtigtes Mobilfunkendgerät MFE authentifiziert wird, sondern auch, indem einfach ein herkömmlicher Wechselschalter bedient wird, der über den Eingang ENG angeschlossen ist. Die Ausgänge AUG1 und AUG2 dienen dazu, dass die erforderliche Aktion, im vorliegenden Fall das Öffnen der Türe ENT, angesteuert werden kann, also beispielsweise ein elektrisches Schloss bedient wird. Weiters ist es durch Vorsehen von einem oder mehreren zusätzlichen Ausgängen auch möglich, über eine Authentifizierungsvorrichtung AVO verschiedene Tätigkeiten anzusteuern. Im vorliegenden Fall wäre denkbar, einerseits bei Authentifizierung die Türe ENT zu öffnen, andererseits aber beispielsweise einen Signalton abzugeben oder eine Warnmeldung zu versenden (beispielsweise, wenn sich ein Mobilfunkendgerät MFE nähert, dessen Identifikationsmittel IDM nicht in der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO gespeichert sind). Mobilfunkendgeräte könnten dann je nach Wunsch für die entsprechende Tätigkeit authentifiziert werden.

In der zumindest einen Speichereinheit SPE1, SPE2 oder SPE3 der Speichervorrichtung SPV wird eine Liste der Identifikationsmittel IDM der authentifizierten Mobilfunkendgeräte gespeichert. Diese Liste wird auch ‚Access Liste‘ genannt. Es ist jederzeit möglich, durch Hinzufügen oder Entfernen von Identifikationsmitteln Authentifizierungen zu vergeben oder zu entziehen. Dies kann von einem Server aus erfolgen. Maßgeblich sind hier die Zeitabstände, in denen sich der Server mit der Speichereinheit synchronisiert: Sie definieren die Intervalle, in denen die ‚Access Liste‘ aktualisiert wird.

Das Verbindungsmodul VBM ist für den Verbindungsaufbau zu gefundenen authentifizierten Mobilfunkendgeräten zuständig. Der Verbindungsaufbau erfolgt dabei auf einer tiefen Protokollschicht, um die Interoperabilität zu allen bluetooth™-fähigen Geräten sicherzustellen.

Die Such-Module SM1, SM2 und SM3 sind im beschriebenen Ausführungsbeispiel Bluetooth™-Module. Beispielhaft werden hier drei Suchmodule verwendet, es ist aber auch möglich, nur eines oder sehr viel mehr als drei zu verwenden. Das zumindest eine Suchmodul sucht permanent nach Mobilfunkendgeräten MFE innerhalb des Sende- und Empfangsbereichs SEB. Werden mehrere Suchmodule verwendet, kann durch die Methode des ‚asynchronen Suchens‘ die Zeit zum Auffinden eines Mobilfunkendgeräts MFE, das sich innerhalb des Sende- und Empfangsbereichs SEB befindet, stark verringert werden.

Beim asynchronen Suchen werden die Suchmodule zeitversetzt mit Spannung versorgt. Dadurch werden zu jedem Zeitpunkt unterschiedliche Frequenzbereiche des Bluetooth™-Frequenzbandes abgesucht, was die Dauer der Suche nach einem Mobilfunkendgerät drastisch verkürzen kann.

Sobald die Suchmodule ein Mobilfunkendgerät MFE gefunden haben, wird überprüft, ob die vom Mobilfunkendgerät MFE übermittelten Identifikationsmittel IDM ident sind mit denen, die in der zumindest einen Speichereinheit SPE1, SPE2 oder SPE3 der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO gespeichert sind. Ist dies der Fall, erfolgt ein Verbindungsaufbau.

Um nun eine Person USR für den Zutritt zu einem gesicherten Bereich zu authentifizieren, müssen die Identifikationsmittel IDM des Mobilfunkendgeräts MFE der betreffenden Person USR in der zumindest einen Speichereinheit SPE1, SPE2 oder SPE3 der Speichervorrichtung SPV hinterlegt werden. Weiters muss der Person USR ein PIN-Code mitgeteilt werden, der bei der ersten Kontaktaufnahme der Such-Module mit dem Mobilfunkendgerät MFE eingegeben werden muss. Dieser PIN-Code wird ebenfalls in der zumindest einen Speichereinheit der Authentifizierungsvorrichtung hinterlegt.

Es ist auch denkbar, dass die Eingabe des PIN-Codes automatisch durch eine Software erfolgt,

die auf dem Mobilfunkendgerät MFE installiert werden muss. In diesem Fall ist keinerlei Handlung vom Benutzer des Mobilfunkendgeräts erforderlich, um sich zu authentifizieren. Nachteilig daran ist aber, dass eben auf allen Mobilfunkendgeräten, die authentifiziert werden sollen, eine entsprechende Software installiert werden muss. Denkbar ist aber auch, dass der PIN-Code sowohl automatisch und unbemerkt vom Benutzer über Software als auch vom Benutzer selber eingegeben werden kann.

Da handelsübliche Bluetooth™-Chips nur begrenzte Speicherfähigkeit für Identifikationsmittel IDM haben, kann die Speichervorrichtung SPV neben der zumindest einen Speichereinheit SPE1, SPE2 und SPE3 durch eine Datenbank erweitert werden. Dadurch können sehr viel mehr Mobilfunkendgeräte authentifiziert werden, die einzige Begrenzung liegt hier in der Größe der Datenbank. Es kann entweder eine interne Datenbank IDB wie in Figur 3b oder eine externe Datenbank EDB wie in Figur 3c verwendet werden.

Wird nun bei Verwendung einer Datenbank von der Authentifizierungsvorrichtung AVO ein Mobilfunkendgerät MFE gefunden, wird überprüft, ob dessen Identifikationsmittel IDM sich in der Datenbank befinden. Wenn dem so ist, werden die Identifikationsmittel aus der Datenbank in die zumindest eine Speichereinheit SPE1, SPE2 oder SPE3 kopiert, und es erfolgt ein Verbindungsaufbau wie oben beschrieben.

In Figur 4 ist ein Blockdiagramm dargestellt, dass einen beispielhaften, nicht einschränkenden Ablauf des erfindungsgemäßen Verfahrens zeigt, beispielsweise bei der Verwendung des Bluetooth™-Funkstandards. Ziel des Verfahrens ist es hier, eine Tür zu öffnen.

Mit dem Start beginnt ein Suchvorgang, ab der Verwendung von zwei oder mehr Suchmodulen ist es möglich, asynchrones Suchen durchzuführen. Es wird dabei ein spezielles Verfahren verwendet, um sicherzustellen, dass wirklich alle Mobilfunkendgeräte MFE im Sende- und Empfangsbereich SEB der Authentifizierungsvorrichtung AVO gefunden werden. Dieser Suchvorgang erfolgt in einer Endlosschleife.

Wird nun ein Mobilfunkendgerät MFE gefunden, wird überprüft, ob sich die Identifikationsnummer IDN, in diesem Fall als MAC-Adresse (Media Access Control) bezeichnet, die das Mobilfunkgerät in weiterer Folge überträgt, in der Liste der authentifizierten Nummern, der 'Access-Liste', befindet. Wenn dem nicht so ist, wird der Vorgang abgebrochen. Befindet sich die Nummer in der 'Access-Liste', wird überprüft, ob die entsprechende Anwendung, die durch den Authentifizierungsprozess ausgelöst wird (Türe öffnen) aktiviert ist. Wenn dem nicht so ist, wird der Vorgang abgebrochen. Ist die Anwendung aktiviert, werden die Verbindungsschlüssel (auch: 'Link Key') aus der zumindest einen Speichereinheit SPE1, SPE2 oder SPE3 der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO ausgelesen.

Handelt es sich um die erste Verbindungsaufnahme (hier: 1. Connect) zwischen Authentifizierungsvorrichtung AVO und Mobilfunkendgerät MFE, wird im Rahmen des Paarbildungsprozesses (hier: Pairing) die Eingabe eines PIN-Codes verlangt. Wird ein falscher PIN-Code eingegeben, wird der Vorgang abgebrochen. Bei der korrekten Eingabe wird der Paarbildungsprozess fortgesetzt, im Zuge dessen ein Verbindungsschlüssel VBS (hier: 'Link Key') generiert wird, der dann in der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO gespeichert wird. Der Verbindungsschlüssel VBS kann dabei je nach verwendeter Variante direkt in die zumindest eine Speichereinheit SPE1, SPE2 oder SPE3 oder in der internen Datenbank IDB oder der externen Datenbank EDB gespeichert werden. Danach wird die Tür geöffnet.

Ist die erste Verbindungsaufnahme schon in der Vergangenheit erfolgt, wird der Verbindungsschlüssel VBS (hier: 'Link Key'), der in der 'Access-Liste' gespeichert ist, die je nach verwendeter Variante auf der internen Datenbank IDB oder der externen Datenbank EDB gespeichert ist, in die zumindest eine Speichereinheit SPE1, SPE2 oder SPE3 eingetragen. Wenn die Variante verwendet wird, in der die Identifikationsmittel IDM direkt in der zumindest einen Speichereinheit

SPE1, SPE2 oder SPE3 gespeichert sind, kann dieser Schritt entfallen.

Weiters wird dann überprüft, ob der Verbindungsschlüssel VBS (hier: „Link Key“), der in der Speichervorrichtung SPV der Authentifizierungsvorrichtung AVO unter der, von dem Mobilfunkendgerät MFE übertragenen Identifikationsnummer IDN gespeichert ist, mit dem von dem Mobilfunkendgerät MFE übertragenen Verbindungsschlüssel VBS übereinstimmt. Ist das nicht der Fall, wird der Vorgang abgebrochen. Stimmen gespeicherte und übertragene Identifikationsmittel IDM überein, ist das gefundene Mobilfunkendgerät MFE authentifiziert, und die Türe wird geöffnet.

Patentansprüche:

1. Verfahren zur Authentifizierung eines Mobilfunkendgerätes (MFE), das durch Identifikationsmittel (IDM) eindeutig charakterisierbar ist, durch eine Authentifizierungsvorrichtung (AVO), die in einer Speichervorrichtung (SPV) mit zumindest einer Speichereinheit (SPE1, SPE2, SPE3) die Identifikationsmittel (IDM) des zumindest einen Mobilfunkendgeräts (MFE) speichern kann und die einen bestimmten Sende- und Empfangsbereich (SEB) abdeckt, wobei die Authentifizierungsvorrichtung (AVO) mit dem zumindest einen Mobilfunkendgerät (MFE) einen Verbindungsaufbau initiiert, sobald das zumindest eine Mobilfunkendgerät (MFE) sich im Sende- und Empfangsbereich (SEB) der Authentifizierungsvorrichtung (AVO) befindet und die Authentifizierungsvorrichtung (AVO) über Funk die Identifikationsmittel (IDM) des zumindest einen Mobilfunkendgeräts (MFE) abfragt und überprüft, ob sie mit den in der Speichervorrichtung (SPV) mit zumindest einer Speichereinheit (SPE1, SPE2, SPE3) gespeicherten Identifikationsmitteln (IDM) identisch sind,
dadurch gekennzeichnet, dass
*) im Fall, dass die Identifikationsmittel (IDM) identisch sind, die Authentifizierungsvorrichtung (AVO) den Verbindungsaufbau abbricht und eine Aktion ausführt, während
*) im Fall, dass die Identifikationsmittel (IDM) des zumindest einen Mobilfunkendgeräts (MFE) nicht mit den in der eine Speichervorrichtung (SPV) mit zumindest einer Speichereinheit (SPE1, SPE2, SPE3) gespeicherten Identifikationsmitteln (IDM) identisch sind, die Authentifizierungsvorrichtung den Verbindungsaufbau abbricht und keine Aktion ausführt.
2. Verfahren nach Anspruch 1, *dadurch gekennzeichnet, dass* die Identifikationsmittel eine Identifikationsnummer (IDN) umfassen, die eine herstellerseitig einmalig vergebene Gerätenummer ist.
3. Verfahren nach einem der Ansprüche 1 oder 2, *dadurch gekennzeichnet, dass* zur Durchführung des Verfahrens der Bluetooth™-Funkstandard verwendet wird.
4. Verfahren nach Anspruch 3, *dadurch gekennzeichnet, dass* die Identifikationsmittel (IDM) zusätzlich nach erfolgtem bluetooth™-spezifischen „Paarbildungsprozess“, der zwischen Mobilfunkendgerät (MFE) und Authentifizierungseinrichtung (AVO) erfolgt, einen, bei diesem „Paarbildungsprozess“ erzeugten, bluetooth™-spezifischen Verbindungsschlüssel (VBS) beinhalten.
5. Verfahren nach einem der Ansprüche 1 bis 4, *dadurch gekennzeichnet, dass* die Identifikationsmittel (IDM) von Mobilfunkendgeräten in zumindest einer internen Datenbank (IDB) oder in zumindest einer externen Datenbank (EDB) abgelegt sind, und wenn die Authentifizierungsvorrichtung (AVO) die Identifikationsmittel (IDM) eines Mobilfunkendgeräts (MFE) abfragt, das sich im Sende- und Empfangsbereich (SEB) der Authentifizierungsvorrichtung (AVO) befindet, überprüft wird, ob die Identifikationsmittel (IDM) in der internen Datenbank (IDB) oder in der externen Datenbank (EDB) abgelegt sind, und bei einem Auffinden der Identifikationsmittel (IDM) die Identifikationsmittel (IDM) aus der internen Datenbank (IDB)

bzw. aus der externen Datenbank (EDB) in die zumindest eine Speichereinheit (SPE1, SPE2, SPE3) übertragen werden und ein Verbindungsaufbau initiiert wird.

6. Authentifizierungsvorrichtung (AVO) zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 5, wobei die Authentifizierungsvorrichtung (AVO) zur Authentifizierung von zumindest einem Mobilfunkendgerät (MFE), das mittels Identifikationsmitteln (IDM) eindeutig charakterisierbar ist, zumindest ein Such-Modul (SM1, SM2, SM3) für die Suche nach Mobilfunkendgeräten (MFE) im Sende- und Empfangsbereich (SEB) der Authentifizierungsvorrichtung (AVO) sowie zumindest ein Verbindungs-Modul (VBM) für den Verbindungsaufbau mit gefundenen Mobilfunkendgeräten (MFE) aufweist, wobei weiters eine Speichervorrichtung (SPV) mit zumindest einer Speichereinheit (SPE1, SPE2, SPE3) vorgesehen ist, in der die Identifikationsmittel (IDM) der authentifizierten Mobilfunkendgeräte gespeichert sind, und die Authentifizierungsvorrichtung (AVO) dazu eingerichtet ist, nach Initiierung eines Verbindungsaufbaus mittels des Verbindungs-Moduls (VBM) über Funk die Identifikationsmittel (IDM) des zumindest einen Mobilfunkendgeräts (MFE) abzufragen und mit den in der Speichervorrichtung (SPV) gespeicherten Identifikationsmitteln (IDM) auf Identität zu überprüfen, *dadurch gekennzeichnet*, dass die Authentifizierungsvorrichtung (AVO) dazu eingerichtet ist, im Fall einer Identität der Identifikationsmittel (IDM) den Verbindungsaufbau abubrechen und eine Aktion auszuführen, wobei die Authentifizierungsvorrichtung (AVO) weiters dazu eingerichtet ist, im Fall fehlender Identität der Identifikationsmittel (IDM) den Verbindungsaufbau abubrechen und keine Aktion auszuführen.
7. Authentifizierungsvorrichtung (AVO) nach Anspruch 6, *dadurch gekennzeichnet*, dass die zumindest eine Speichereinheit (SPE1, SPE2, SPE3) direkt in dem zumindest einen Such-Modul (SM1, SM2, SM3) angeordnet ist.
8. Authentifizierungsvorrichtung (AVO) nach Anspruch 6 oder Anspruch 7, *dadurch gekennzeichnet*, dass die Speichervorrichtung (SPV) zumindest eine interne Datenbank (IDB) umfasst, welche in der Authentifizierungsvorrichtung (AVO) angeordnet ist.
9. Authentifizierungsvorrichtung (AVO) nach einem der Ansprüche 6 bis 8, *dadurch gekennzeichnet*, dass die Speichervorrichtung (SPV) zumindest eine externe Datenbank (EDB) umfasst, welche außerhalb der Authentifizierungsvorrichtung (AVO) angeordnet ist.
10. Authentifizierungsvorrichtung (AVO) nach einem der Ansprüche 8 oder 9, *dadurch gekennzeichnet*, dass die Identifikationsmittel (IDM) von Mobilfunkendgeräten in der zumindest einen internen Datenbank (IDB) oder der zumindest einen externen Datenbank (EDB) ablegbar und aus der zumindest einen Speichereinheit (SPE1, SPE2, SPE3) löscherbar sind.
11. Authentifizierungsvorrichtung (AVO) nach einem der Ansprüche 6 bis 10, *dadurch gekennzeichnet*, dass es sich bei dem zumindest einen Such-Modul (SM1, SM2, SM3) sowie dem zumindest einen Verbindungs-Modul (VBM) um Bluetooth™-Module handelt.
12. Authentifizierungsvorrichtung (AVO) nach Anspruch 11, *dadurch gekennzeichnet*, dass mehrere Such-Bluetooth™-Module (SM1, SM2, SM3) vorgesehen sind.
13. Authentifizierungsvorrichtung (AVO) nach Anspruch 12, *dadurch gekennzeichnet*, dass die Such-Bluetooth™-Module (SM1, SM2, SM3) den Suchbetrieb zeitversetzt starten.
14. Authentifizierungsvorrichtung (AVO) nach einem der Ansprüche 6 bis 13, *dadurch gekennzeichnet*, dass die Reichweite des zumindest einen Such-Moduls (SM1, SM2, SM3) und des zumindest einen Verbindungs-Moduls (VBM) durch geräteinterne Dämpfung des Funksignals vermindert wird.
15. Authentifizierungsvorrichtung (AVO) nach einem der Ansprüche 6 bis 14, *dadurch gekennzeichnet*

zeichnet, dass die Reichweite des zumindest einen Such-Moduls (SM1, SM2, SM3) und des zumindest einen Verbindungsmoduls (VBM) vermindert wird, indem die Teile, die das Funk-Signal abgeben und empfangen, mit einem dämpfenden Material umgeben werden.

5

Hiezu 4 Blatt Zeichnungen

10

15

20

25

30

35

40

45

50

55

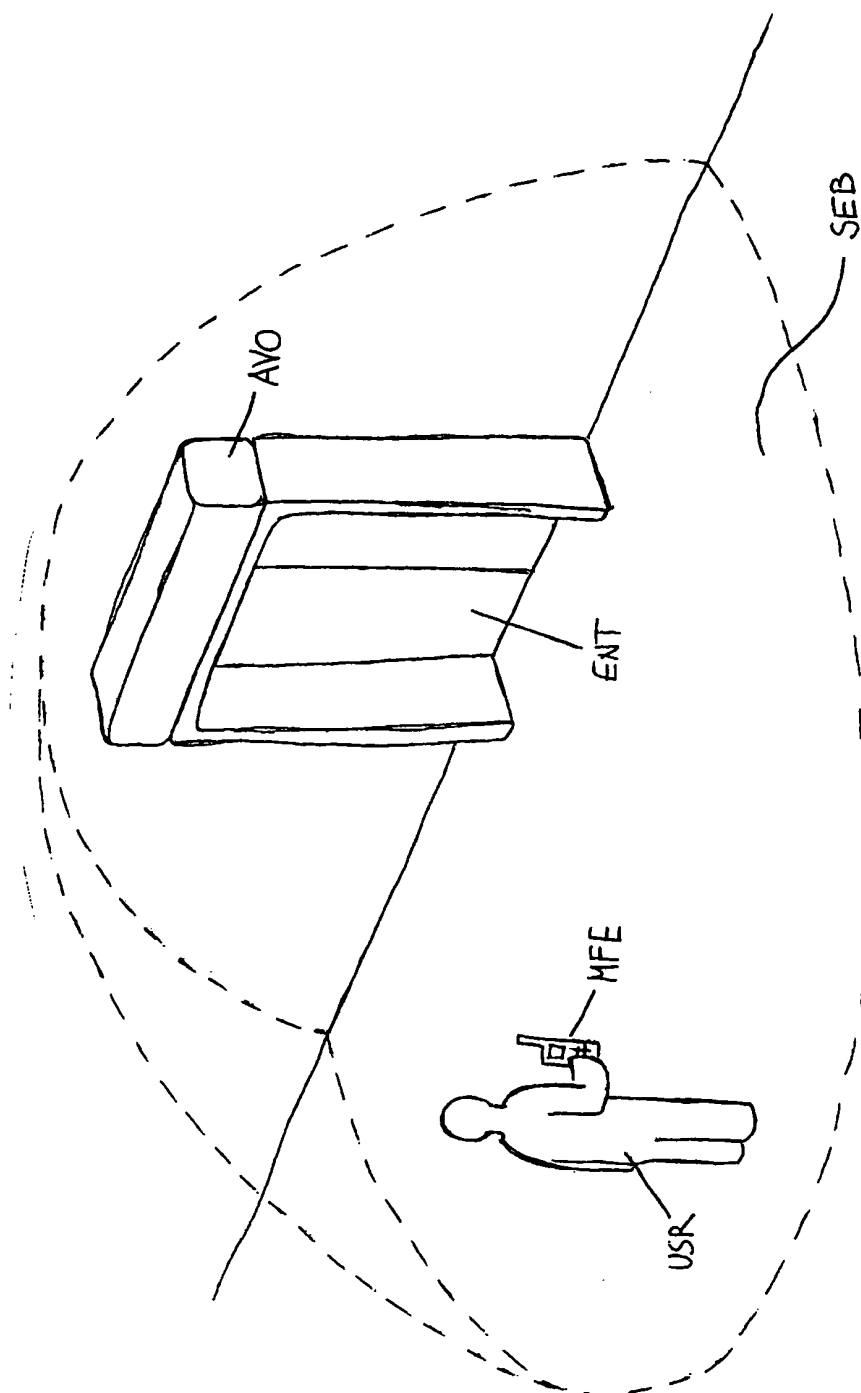


Fig. 1

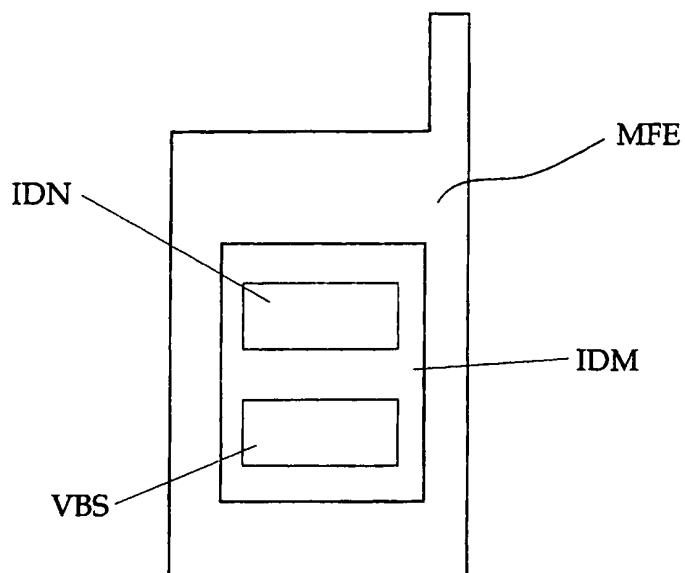


Fig. 2

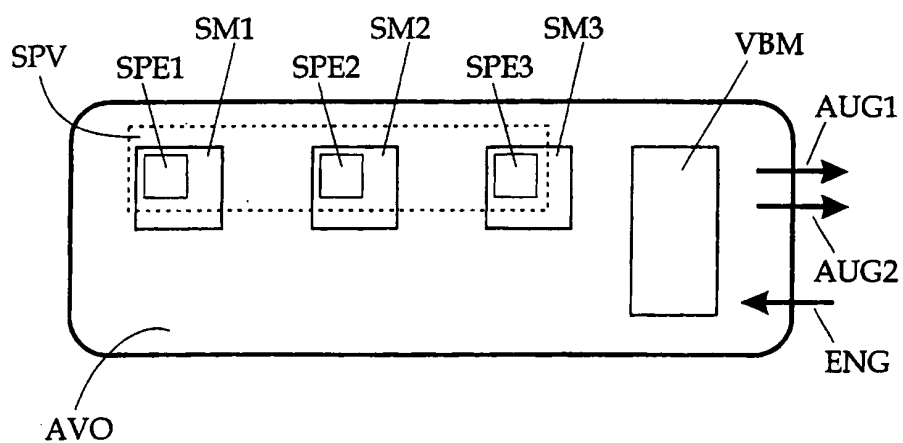


Fig. 3a

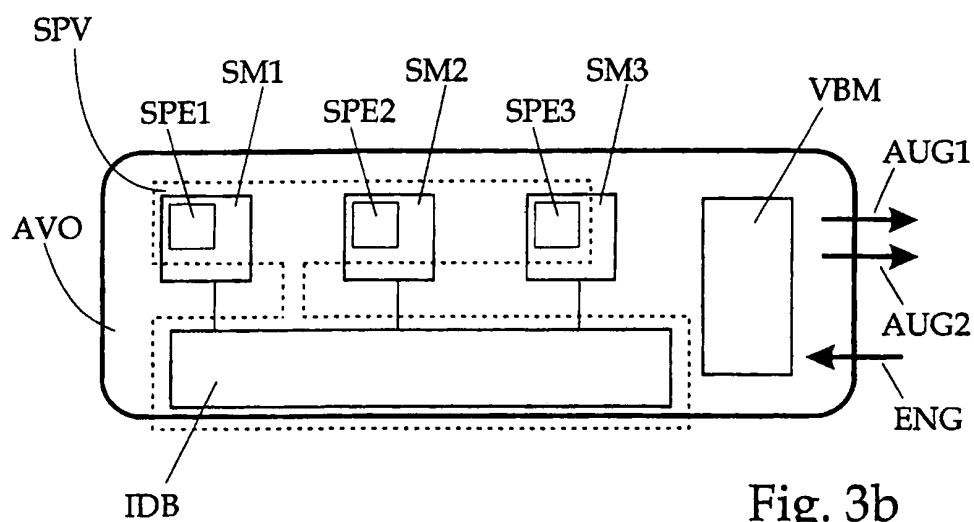


Fig. 3b

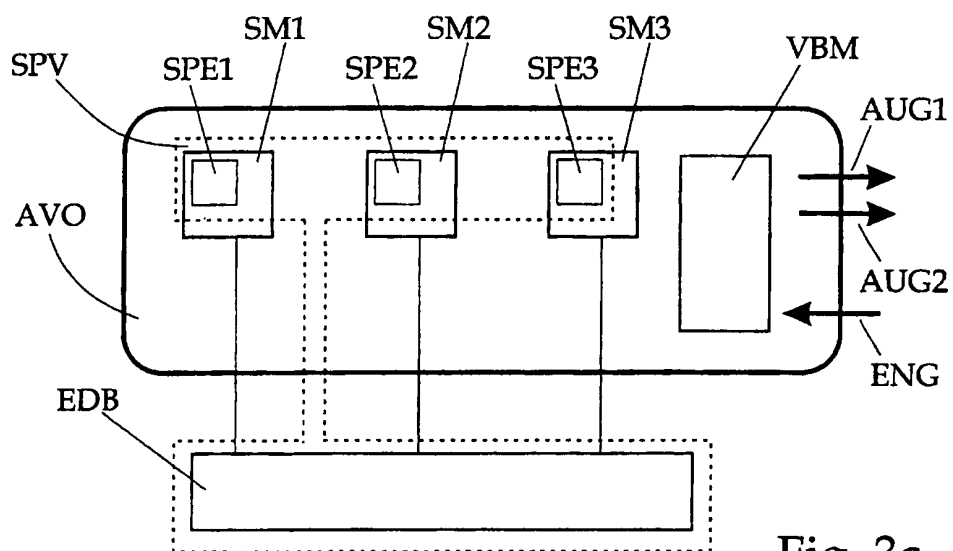


Fig. 3c

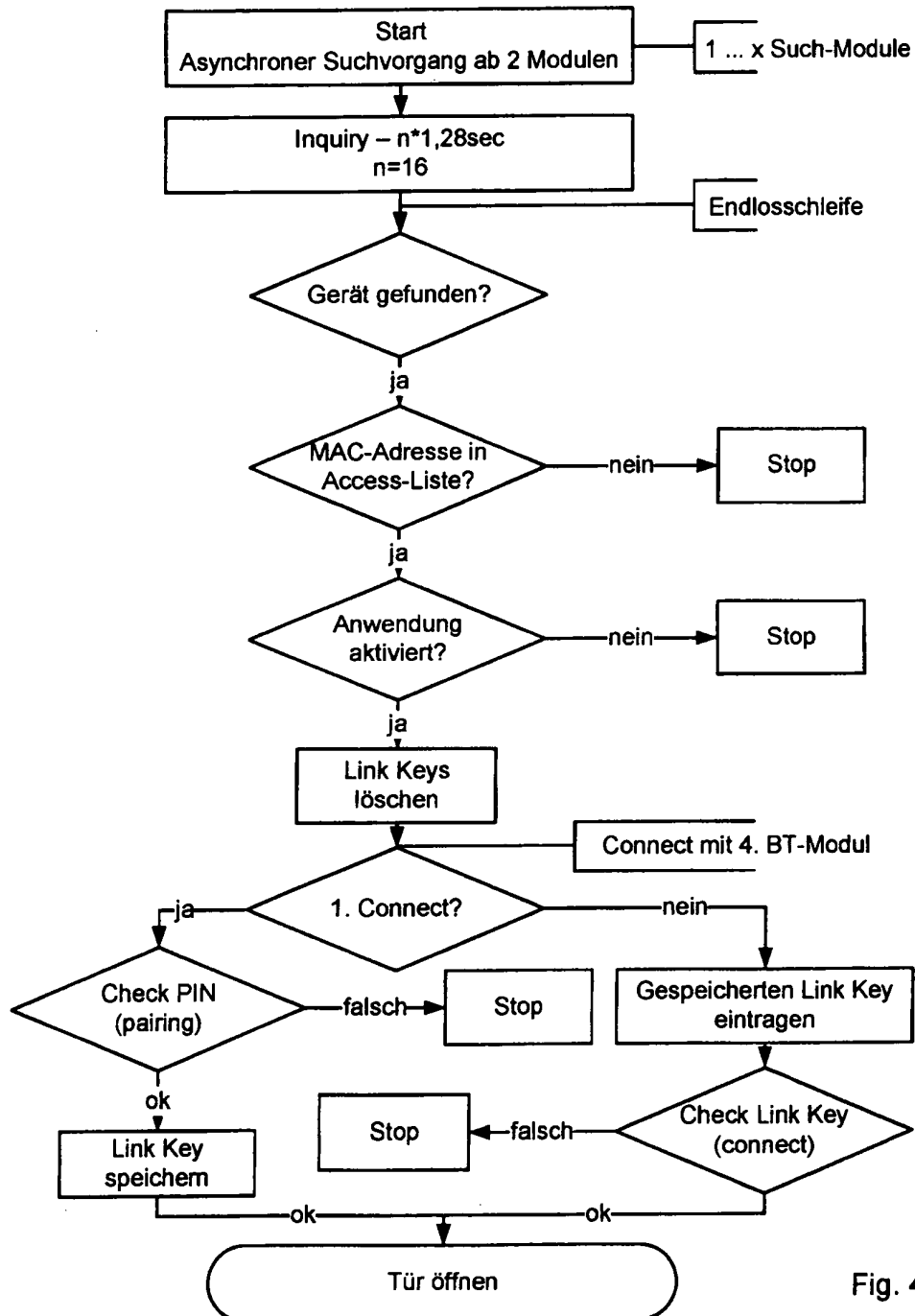


Fig. 4