(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2005 045 118 A1** 2007.03.29

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2005 045 118.7**
(22) Anmeldetag: **21.09.2005**
(43) Offenlegungstag: **29.03.2007**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
H04L 12/28 (2006.01)

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Fries, Steffen, 85598 Baldham, DE; Korenyi, Csaba, 85635 Höhenkirchen-Siegertsbrunn, DE; Montag, Michael, 81667 München, DE

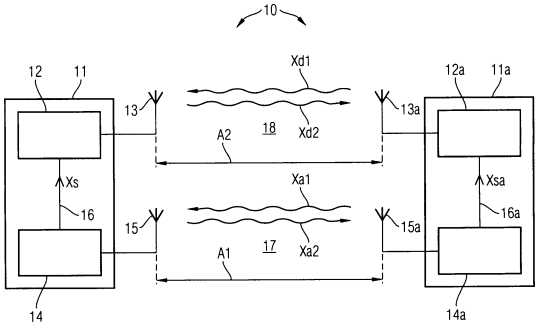
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2005/01 60 138 A1
US2005/01 32 193 A1
US2002/00 69 364 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Anmeldeverfahren zwischen Teilnehmern eines Kommunikationssystems und Teilnehmer**

(57) Zusammenfassung: Die Erfindung betrifft ein Anmeldeverfahren zwischen Teilnehmern eines drahtlos arbeitenden Kommunikationssystems (10), insbesondere eines nach dem Bluetooth-Standard arbeitenden Kommunikationssystems, bei dem für eine Schlüsseletablierung im Anmeldebetrieb zwischen an einer nachfolgenden Datenkommukation vorgesehenen Teilnehmern (11, 11a) hochfrequente elektromagnetische Schlüsseletablierungssignale (Xa1, Xa2) nach dem RFID-Standard ausgetauscht werden, welche eine gegenüber den Datensignalen (Xd1, Xd2) der Datenkommunikation (Xd1, Xd2) geringere Reichweite aufweisen. Die Erfindung betrifft ferner einen entsprechenden Teilnehmer, insbesondere einen Bluetooth-Teilnehmer.



Beschreibung

[0001] Die Erfindung betrifft ein Anmeldeverfahren zwischen Teilnehmern eines drahtlos arbeitenden Kommunikationssystems, insbesondere eines nach dem Bluetooth-Standard arbeitenden Kommunikationssystems. Die Erfindung betrifft ferner einen entsprechenden Teilnehmer, insbesondere einen Bluetooth-Teilnehmer.

Stand der Technik

[0002] In der jüngeren Vergangenheit wurden vermehrt Anstrengungen unternommen, die Kommunikation zwischen Geräten mittels Funkwellen über vergleichsweise kurze Distanzen zu Standardisieren. Ein Resultat dieser Bemühungen ist der unter dem Begriff "Bluetooth" bekannte und eingesetzte Standard. Obgleich prinzipiell bei beliebigen drahtlos arbeitenden Kommunikationssystemen anwendbar, wird die Erfindung sowie die ihr zugrunde liegende Problematik nachfolgend mit Bezug auf nach dem Bluetooth-Standard arbeitende Kommunikationssysteme sowie deren Teilnehmer erläutert, ohne jedoch die Erfindung dahingehend zu beschränken.

[0003] Der Bluetooth-Standard ist ein Kurzstrecken-Funk-Standard, der mit Trägerfrequenzen aus dem weltweit nicht lizenzierten Industrial, Scientific, Medical 2,4 GHz Band, kurz 2,4 GHz ISM-Band, arbeitet und auf den gültigen Funkvorschriften für Europa, Japan und Nordamerika basiert. Die für den Standard relevanten Informationen sind in der Spezifikation des Bluetooth-Systems unter der Internet-Adresse "www.bluetooth.com" erhältlich.

[0004] Ein wesentliches Merkmal des Bluetooth-Standards ist die Art und Weise der Datenübertragung zwischen dessen einzelnen Teilnehmern. Dabei können bis zu acht nach dem Bluetooth-Standard arbeitende Teilnehmer in einer – auch als Pico-Zelle bezeichneten – Funkzelle zu einem so genannten Pico-Netz zusammengeschlossen werden und miteinander kommunizieren. Jeder Teilnehmer in einem Pico-Netz kann dieses Pico-Netz initialisieren. Ein Teilnehmer, welcher ein Pico-Netz initialisiert hat, kontrolliert die restlichen Teilnehmer des Pico-Netzes und synchronisiert deren Zeitgeber und wird daher auch als "Master" bezeichnet, während die verbleibenden Teilnehmer des Pico-Netzes, die mit diesem Master in kommunikativer Verbindung stehen, als "Slaves" bezeichnet werden. Neben diesen bis zu acht Teilnehmern eines Pico-Netzes können eine praktisch beliebige Vielzahl weiterer Teilnehmer im Pico-Netz vorhanden sein, die nicht mit den acht Teilnehmern kommunizieren. Diese befinden sich in einem passiven, so genannten Parkmodus.

[0005] Für den Aufbau einer Kommunikationsverbindung muss sich ein jeweiliger Teilnehmer zunächst an dem Kommunikationssystem anmelden. Der Anmeldevorgang dient dem Zweck, zunächst eine zugelassen Verbindung aufzubauen und umfasst typischerweise eine Initialisierungsphase sowie eine sich daran anschließende so genannte Link-Key-Generation, bei der ein Schlüssel für die nachfolgende Datenkommunikation der drahtlosen Verbindung erzeugt wird. Dieser Anmeldevorgang wird im Bluetooth-Standard meist auch als "Pairing" bezeichnet. Für den Anmeldevorgang ist es erforderlich, dass eine eindeutige Anmeldung sichergestellt ist, um zu vermeiden, dass unberechtigte Teilnehmer ebenfalls an der Datenkommunikation teilnehmen.

[0006] Der herkömmliche Anmelde- und Verbindungsprozess der Bluetooth-Teilnehmer ist relativ kompliziert. Im Rahmen eines Anmeldeversuches eines Bluetooth-Teilnehmers findet im Allgemeinen zunächst eine Abfrage einer vorgegebenen Kennung (PIN, Passwort, etc.) statt. Erst nach erfolgreicher Abfrage dieser Kennung wird dieser Bluetooth-Teilnehmer als berechtigter Teilnehmer (entrusted device) betrachtet, woraufhin er uneingeschränkt mit den übrigen Bluetooth-Teilnehmern des Pico-Netzes kommunizieren kann. Das Anmeldeverfahren hängt im Wesentlichen von den Eigenschaften der an der Datenkommunikation teilnehmenden Bluetooth-Teilnehmer ab.

[0007] Bei vielen Bluetooth-Kommunikationssystemen erfolgt das Anmeldeverfahren durch eine eigens dafür vorgesehene Eingabevorrichtung, beispielsweise durch eine Tastatur, über die eine jeweilige Identifikation durch einen Benutzer vorgenommen wird, die von einem gegenüberliegenden Bluetooth-Teilnehmer entsprechend auf ihre Gültigkeit hin überprüft wird. Ein entsprechendes Verfahren ist in der US 2004/0192206 A1 beschrieben.

[0008] Bei modernen Bluetooth-Kommunikationssystemen kann das Anmeldeverfahren auch automatisch, also ohne unmittelbare Tastatureingabe, erfolgen.

[0009] Eine zunehmend wichtigere Anforderung besteht in der Sicherheit des Anmeldeverfahrens, um zu vermeiden, dass sich – bewusst oder unbewusst – unberechtigte Teilnehmer in dem Pico-Netz anmelden können. Aus diesem Grunde wird zur Sicherheit bei dem Anmeldeverfahren zunächst überprüft, ob es sich hier um einen berechtigten Teilnehmer handelt. Hierzu ist das Bluetooth-Anmeldeverfahren typischerweise in zwei Phasen aufgebaut, die Initialisierungsphase und die Phase zur Erzeugung eines Verbindungsschlüssels. Das Ziel bei der Initialisierungsphase besteht darin, einen Initialisierungsschlüssel zu erzeugen, welcher gewissermaßen ein gemeinsames Geheimnis (shared secret) der beiden Bluetooth-Teilnehmern bildet, welches also nur diese Teilnehmer kennen. Zur Erzeugung dieses Initialisie-

rungsschlüssels existieren verschiedene Verfahren, die hier allerdings nicht näher ausgeführt werden sollen. Im Anschluss wird daraus der Verbindungsschlüssel, der so genannte Link Key, erzeugt, der zwischen den Teilnehmern ausgetauscht und überprüft wird. Die Qualität des Verbindungsschlüssel hängt dabei im Wesentlichen von den an das Kommunikationssystem gestellten Sicherheitsanforderungen ab.

[0010] Abhängig von der Sicherheitsstrategie erfolgt der Austausch eines Passworts zwischen den Teilnehmern eines Bluetooth-Kommunikationssystems über einer Funkstrecke, wobei für das Passwort abhängig von der Sicherheitsstrategie eine mehr oder weniger große Bitbreite eines digitalen Passwortes vorgesehen ist. Da der Austausch dieses Passwortes funkbasiert erfolgt, besteht hier die Gefahr, dass dieses Passwort bei einem Anmeldeverfahren von einem unberechtigten Teilnehmer abgehört und von diesem in der Folge für einen unberechtigten Anmeldevorgang genutzt wird. In diesem Falle könnte sich der unberechtigte Teilnehmer unerwünschter Weise Zugang zu dem Kommunikationssystem verschaffen, was es allerdings zu vermeiden gilt. Um dies zu vermeiden, existieren die verschiedensten Möglichkeiten, die Sicherheit bei einem Anmeldeverfahren zwischen Bluetooth-Teilnehmern zu gewährleisten.

[0011] Ein erstes Verfahren sieht vor, beispielsweise Einmal-Passwörter oder PINs zu verwenden, die also lediglich für einen einzigen Anmeldevorgang gültig sind. Problematisch ist hier allerdings, dass bei einer Vielzahl von Teilnehmern eines Kommunikationssystems eine entsprechende Komplexität der Vergabe der verschiedenen Passwörter bereitgestellt werden müsste, was unter Umständen sehr aufwändig sein könnte. Darüber hinaus ist diese Vorgehensweise auch speicheraufwändig und erfordert einen hohen Auswerteaufwand.

[0012] Eine weitere Möglichkeit ist in der US 2003/0050009 A1 beschrieben. Die Sende-/Empfangseinrichtung wird hier während eines Anmeldevorganges mit einer gegenüber einem normalen Betrieb geringeren Sendeleistung versorgt, wodurch die gesendeten Signale auch eine geringere Reichweite aufweisen. Durch Reduzierung der Reichweite kann eine höhere Sicherheit gewährleistet werden, da bei dieser Form des Anmeldeverfahrens die jeweiligen Teilnehmer näher aneinander positioniert werden müssen, was insgesamt die Sicherheit vergrößert.

Aufgabenstellung

[0013] Vor diesem Hintergrund liegt der vorliegenden Erfindung die Aufgabe zugrunde, das Anmeldeverfahren bei drahtlos arbeitenden Kommunikationssystemen und Teilnehmern und insbesondere bei Bluetooth-basierten Kommunikationssystemen und Teilnehmern weiter zu verbessern und vorzugsweise weiter zu vereinfachen.

[0014] Erfindungsgemäß wird zumindest eine dieser Aufgaben durch ein Anmeldeverfahren mit den Merkmalen des Patentanspruchs 1 und/oder durch einen Teilnehmer mit den Merkmalen des Patentanspruches 16 gelöst.

[0015] Demgemäß ist vorgesehen:
Ein Anmeldeverfahren zwischen Teilnehmern eines drahtlos arbeitenden Kommunikationssystems, bei dem für eine Schlüsseletablierung im Anmeldebetrieb zwischen an einer nachfolgenden Datenkommunikation vorgesehenen Teilnehmern hochfrequente elektromagnetische Schlüsseletablierungssignale nach dem RFID-Standard ausgetauscht werden, welche eine gegenüber den Datensignalen der Datenkommunikation geringere Reichweite aufweisen. (Patentanspruch 1)

[0016] Einen Teilnehmer für ein Kommunikationssystem,

– mit einem Kommunikations-Modul für eine Datenkommunikation, welches zum Senden und Empfangen von Datensignalen,
– mit einer programmgesteuerten Einrichtung, die zumindest die Steuerung der Datenkommunikation und die Auswertung der empfangenen Datensignale vornimmt,
– mit einem RFID-Modul für einen Anmeldebetrieb, das zum Senden und Empfangen von RFID-Schlüsseletablierungssignalen, welche eine gegenüber den Datensignalen geringere Reichweite aufweisen, ausgelegt ist. (Patentanspruch 16)

[0017] Vorzugsweise ist das drahtlos arbeitende Kommunikationssystem als ein nach dem Bluetooth-Standard arbeitendes Kommunikationssystem oder als ein WLAN-Kommunikationssystem ausgebildet. In diesem Falle ist der Teilnehmer als Bluetooth-Teilnehmer für ein nach dem Bluetooth-Standard arbeitendes Kommunikationssystem ausgebildet und das Kommunikations-Modul ist als Bluetooth-Modul für eine Datenkommunikation nach dem Bluetooth-Standard ausgelegt. Denkbar wären selbstverständlich auch andere drahtlose Kommunikationssysteme.

[0018] Die der vorliegenden Erfindung zugrunde liegende Idee besteht darin, den Anmeldevorgang bei einem beispielsweise auf dem Bluetooth-Standard basierenden Kommunikationsverfahren und -system, welches dort auch als Pairing bezeichnet wird, von der eigentlichen (Daten-)Kommunikation zu trennen. Insbesondere ist die Erkenntnis, dass dieser nachfolgend als Anmeldebetrieb bezeichnete Vorgang nicht notwendigerweise Bluetooth-basiert erfolgen und so-

mit unter Verwendung eines entsprechenden Bluetooth-Sende-/Empfangsmoduls durchgeführt werden muss. Die Idee besteht nun darin, im Anmeldebetrieb hochfrequente elektromagnetische Schlüsseletablierungssignale nach einem RFID-Standard zu erzeugen, die somit ausschließlich für die Schlüsseletablierung und somit für die Identifikation eines berechtigten Teilnehmers erzeugt werden. Unter einem berechtigten Teilnehmer ist ein solcher zu verstehen, der für eine Datenkommunikation innerhalb des (Bluetooth-basierten) Kommunikationssystems vorgesehen ist.

[0019] Die vorliegende Erfindung zeichnet sich im Vergleich zu bekannten Lösungen durch eine schaltungstechnisch sehr einfache Implementierung aus. Hierzu sind lediglich in den für die Datenkommunikation vorgesehenen, berechtigten Teilnehmern jeweilige RFID-Module zu implementieren, die allerdings sehr einfach und insbesondere außerordentlich kostengünstig herstellbar sind.

[0020] Der besondere Vorteil bei Verwendung von RFID-Schlüsseletablierungssignalen für den Anmeldeprozess besteht darin, dass die RFID-Datenkommunikation – abhängig von deren jeweiligen Auslegung – typischerweise auf sehr geringe Reichweiten ausgelegt ist, wohingegen die eigentliche (Bluetooth-)Datenkommunikation demgegenüber für sehr viel größere Reichweiten ausgelegt ist. Indem nun der Anmeldebetrieb unter Verwendung des RFID-Standards erfolgt, kann auf sehr einfache Weise eine Reduzierung der Reichweite und dadurch eine signifikante Erhöhung der Sicherheit beim Anmeldevorgang realisiert werden. Da ein Teilnehmer zunächst für eine anschließende (Bluetooth-)Datenkommunikation durch einen anderen Teilnehmer authentifiziert werden muss, ist es erforderlich, dass diese sehr eng aneinander angeordnet werden, damit überhaupt eine RFID-basierte Schlüsseletablierung vorgenommen werden kann. Durch die geringe Distanz bei der RFID-Schlüsseletablierung im Vergleich zu der eigentlichen (Bluetooth-)Datenkommunikation ergibt sich eine signifikant höhere Abhörsicherheit aufgrund der physikalischen Nähe, die durch die RFID-Technologie bedingt ist. Im Falle eines potenziellen Abhörens müsste eine entsprechende Sende-/Empfangseinrichtung eines unberechtigten Teilnehmers in unmittelbare Nähe der beiden berechtigten Teilnehmer, die gerade einen Anmeldevorgang durchführen, gebracht werden, was für einen Nutzer nicht ohne Weiteres unbemerkt bleiben würde.

[0021] Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung ergeben sich aus den weiteren Unteransprüchen sowie aus der Beschreibung in Zusammenschau mit der Zeichnung.

[0022] Ein bevorzugte Ausgestaltung des erfindungsgemäßen Verfahrens sieht zumindest zwei Betriebsmodi vor:

– einen Anmeldebetrieb, bei dem zunächst eine Schlüsseletablierung der an einer Datenkommunikation teilnehmenden Teilnehmer durch Austauschen von RFID-Schlüsseletablierungssignalen durchgeführt wird,

– einen sich daran anschließenden Normalbetrieb, bei dem nach durchgeführter und erfolgreicher Schlüsseletablierung die Datenkommunikation zum Austausch von Datensignalen zwischen den Teilnehmern nach dem für die eigentliche Datenkommunikation vorgesehenen Standard, beispielsweise nach dem Bluetooth-Standard, erfolgt.

[0023] In einer besonders bevorzugten Ausgestaltung ist eine maximale Distanz zwischen den Teilnehmern für die Schlüsseletablierung im Anmeldebetrieb signifikant geringer ist als für die Datenkommunikation im Normalbetrieb. Signifikant bedeutet hier mindestens um den Faktor 10 und vorzugsweise um den Faktor 100 oder sogar 1000. Insbesondere ist zum Beispiel die maximale Reichweite der Schlüsseletablierung im Anmeldebetrieb kleiner als 1,5 Meter, insbesondere kleiner als 0,5 Meter und vorzugsweise kleiner als 10 cm. Demgegenüber ist die maximale Reichweite der eigentlichen Datenkommunikation, wie beispielsweise der der Bluetooth-Kommunikation, im Normalbetrieb größer als 2 Meter und insbesondere größer als 10 Meter. Diese maximale Reichweite der eigentlichen (Bluetooth-)Kommunikation hängt im Wesentlichen von der Umgebung ab, das heißt die Reichweite ist umso größer, je weniger Gegenstände (Wände, Decken, etc.) sich innerhalb des Übertragungspfades befinden.

[0024] Typischerweise, jedoch nicht notwendigerweise, umfasst eine Schlüsseletablierung im Anmeldebetrieb eine Initialisierung sowie eine nachfolgende Link-Key-Erzeugung. Im Anschluss an die Schlüsseletablierung im Rahmen des Authentifikationsbetriebs wird vorzugsweise eine Authentifikation (oder Auswertung) der ausgetauschten RFID-Schlüsseletablierungssignale vorgenommen.

[0025] Vorzugsweise wird die Auswertung, dass heißt die Authentifikation der ausgetauschten RFID-Schlüsseletablierungssignale nach dem Bluetooth-Standard vorgenommen, dass heißt im RFID-Modul erfolgt dann lediglich die reine Übertragung der Schlüsseletablierungssignale, nicht aber deren Auswertung und Authentifikation. Diese Auswertung bzw. die Authentifikation erfolgt zum Beispiel in dem für die Datenkommunikation vorgesehenen Kommunikations- oder Bluetooth-Modul. Das RFID-Modul bzw. die RFID-Übertragung wird somit lediglich für die reine Anmeldung (also für die Übermittlung des Schlüssels/Bluetooth-Passkeys) verwendet, wobei hier die mit der geringe Reichweite einhergehende zwingende Nähe der an der Anmel-

dung beteiligten Teilnehmer ausgenutzt wird. In dem RFID-Modul erfolgt somit keine Auswertung der übermittelten kryptologischen Daten, dass heißt hier in diesem Falle ist auch keine entsprechende kryptologische Auswerteeinrichtung vorgesehen. Zusätzlich oder alternativ wäre es allerdings auch denkbar, dass die Auswertung bzw. die Authentifikation auch im RFID-Modul stattfindet.

[0026] Zur Erhöhung der Sicherheit ist es zweckmäßig, zu Beginn des Anmeldebetriebs zunächst ein Initialisierungsschlüssel zwischen den an der Anmeldung beteiligten Teilnehmern auszutauschen, auf dem die weitere Schlüsseletablierung basiert. Als Initialisierungsschlüssel im Anmeldebetrieb kann zum Beispiel ein Passwort und/oder eine PIN-Nummer übertragen werden. Zur Erzeugung des Initialisierungsschlüssels wird dafür zum Beispiel ein Schlüsseletablierungsprotokoll, insbesondere das Diffie Hellmann Protokoll, herangezogen. Zusätzlich oder alternativ kann auch vorgesehen sein, dass der Initialisierungsschlüssel mittels eines Random-Generators erzeugt wird.

[0027] In einer bevorzugten Ausgestaltung weisen die an einer Anmeldung beteiligten Teilnehmern jeweils ein gemeinsames Geheimnis auf, welches im Anmeldebetrieb zwischen diesen ausgetauscht wird.

[0028] Alternativ wäre natürlich auch denkbar und auch vorteilhaft, wenn für den Anmeldebetrieb keine Verschlüsselung vorgesehen ist. Da der Anmeldebetrieb durch eine sehr geringe Distanz der an der Anmeldung beteiligten Teilnehmer gekennzeichnet ist, sind häufig keine weitere Sicherheitsmaßnahmen erforderlich, was auch eine Reduzierung des für die Anmeldung erforderlichen Hardware- und Softwareaufwandes mit sich bringt.

[0029] Eine sehr bevorzugte Ausgestaltung sieht vor, dass der Anmeldebetrieb Teil des Protokolls der Datenkommunikation ist.

[0030] In einer besonders bevorzugten Ausgestaltung nimmt die programmgesteuerte Einrichtung zusätzlich auch die Steuerung des Anmeldebetriebs und/oder die Auswertung der empfangenen RFID-Schlüsseletablierungssignale vor. Damit kann auf eine eignes dafür vorgesehene Auswerteeinrichtung, beispielsweise innerhalb des RFID-Moduls, verzichtet werden.

[0031] Typischerweise ist die programmgesteuerte Einrichtung Bestandteil des Kommunikations-Moduls bzw. des Bluetooth-Moduls. Als programmgesteuerte Einrichtung kommt zum Beispiel ein Mikroprozessor, Mikrocontroller oder auch eine festverdrahtete Logikschaltung, beispielsweise ein FPGA oder ein PLD, in Betracht.

[0032] In einer typischen, jedoch nicht notwendigen Ausgestaltung weist das Kommunikations-Modul bzw. das Bluetooth-Modul eine mit einer ersten Sende-/Empfangsantenne verbundene erste Sende-/Empfangseinrichtung zum Senden und/oder Empfangen von Datensignalen, eine Codiereinrichtung zum Codieren der zu sendenden Datensignale, eine Decodiereinrichtung zum Decodieren der empfangenen Datensignale, eine Auswerteeinrichtung zum Auswerten der empfangenen Datensignale sowie einen Speicher zum Speichern von Programm-, Adress- und/oder empfangenen Daten auf.

[0033] In einer ebenfalls typischen, jedoch nicht notwendigen Ausgestaltung weist das RFID-Modul eine mit einer zweiten Sende-/Empfangsantenne verbundene zweite Sende-/Empfangseinrichtung zum Senden und/oder Empfangen von RFID-Schlüsseletablierungssignalen, eine Modulatoreinrichtung zum Modulieren der zu sendenden RFID-Schlüsseletablierungssignalen und eine Demodulatoreinrichtung zum Demodulieren der empfangenen RFID-Schlüsseletablierungssignale auf.

[0034] Eine besonders bevorzugte Ausgestaltung sieht vor, dass das RFID-Modul als Transponder (Tag) ausgebildet ist. Solche Transponder zur Verwendung als Authentifikation sind außerordentlich kostengünstig in der Herstellung. Zusätzlich oder alternativ kann ein RFID-Modul auch ein Lesegerät (Reader) aufweisen, welches mit einem Transponder eines anderen Teilnehmers zum Zwecke der Authentifikation in kommunikative Verbindung bringbar ist. Lesegeräte werden im Allgemeinen bei als Master vorgesehenen Teilnehmer implementiert, während Transponder vornehmlich bei als Slave vorgesehenen Teilnehmer implementiert sind. Da ein Teilnehmer unter Umständen sowohl als Master als auch als Slave fungieren kann, ist es in diesem Fall auch vorteilhaft, wenn dieser Teilnehmer sowohl ein Lesegerät als auch einen Transponder in dessen RFID-Modul aufweist.

[0035] Eine besonders bevorzugte Ausgestaltung sieht einen Schlüsseletablierungsgenerator vorzugsweise im RFID-Modul vor, der mit der zweiten Sende-/Empfangseinrichtung gekoppelt ist und der einen Initialisierungsschlüssel für die zu sendenden RFID-Schlüsseletablierungssignale erzeugt. Vorzugsweise ist ein Random-Schlüsselgenerator als Bestandteil des Schlüsseletablierungsgenerators zur Erzeugung eines Zufallschlüssels vorgesehen. Für die Schlüsseletablierung kann beispielsweise ein Diffie-Hellmann-Schlüsseletablierung vorgesehen sein.

[0036] Eine besonders bevorzugte Ausgestaltung sieht vor, dass ein (Bluetooth-)Teilnehmer und vorzugsweise dessen (Bluetooth-)Modul einen Speicher aufweist, in dem Informationen über die empfangenen Schlüsseletablierungssignale und somit über die

von einem anderen Teilnehmer übermittelten Passwörter, PINs und dergleichen ablegbar sind. In dem Speicher sind somit Informationen über eine bereits aufgebaute Kommunikations-Verbindung mit jeweils anderen berechtigten Teilnehmern abgelegt. Wenn diese beiden berechtigten Teilnehmer zu einem späteren Zeitpunkt (nach Unterbrechung der entsprechenden Kommunikationsverbindung) wieder eine Kommunikationsverbindung zueinander aufbauen möchten, kann diese sehr viel schneller erfolgen, da die entsprechenden Informationen bereits in dem Speicher abgelegt sind und sehr einfach – ohne sie aufwändig entschlüsselt und erzeugt werden müssten – dort wieder abgerufen werden können.

Ausführungsbeispiel

[0037] Die Erfindung wird nachfolgend anhand der in den schematischen Figuren der Zeichnung angegebenen Ausführungsbeispiele näher erläutert. Es zeigen dabei:

[0038] Fig. 1 ein Blockschaltbild eines Bluetooth-basierten Kommunikationssystem mit zwei Teilnehmern zur Darstellung des erfindungsgemäßen Anmeldeverfahrens;

[0039] Fig. 2 ein Blockschaltbild für ein erstes Ausführungsbeispiel eines erfindungsgemäßen Bluetooth-Teilnehmers;

[0040] Fig. 3 ein Blockschaltbild für ein zweites Ausführungsbeispiel eines erfindungsgemäßen Bluetooth-Teilnehmers;

[0041] Fig. 4 ein Bluetooth-basiertes Kommunikationssystem mit einem als Master fungierenden Teilnehmer und mehreren als Slave fungierenden Teilnehmern.

[0042] In allen Figuren der Zeichnung sind gleiche und funktionsgleiche Elemente, Merkmale und Signale – sofern nichts Anderes angegeben ist – mit denselben Bezugszeichen versehen worden.

[0043] Fig. 1 zeigt ein Blockschaltbild eines Bluetooth-basierten Kommunikationssystems, welches hier mit Bezugszeichen **10** bezeichnet ist. Das Kommunikationssystem **10** weist zwei Bluetooth-Teilnehmer **11**, **11a** auf. Im vorliegenden Ausführungsbeispiel in Fig. 1 sei angenommen, dass beide Teilnehmer **11**, **11a** einen im Wesentlichen gleichen schaltungstechnischen Aufbau aufweisen. Es sei ferner angenommen, dass diese Teilnehmer **11**, **11a** für eine Datenkommunikation innerhalb des Kommunikationssystems **10** berechtigt sind.

[0044] In Fig. 1 sei angenommen, dass der Teilnehmer **11** als Master fungiert und der Teilnehmer **11a** als Slave fungiert. In entsprechender Weise weisen die Bezugszeichen aller Elemente des als Slave fungierenden Teilnehmers zusätzlich ein "a" auf.

[0045] Ein jeweiliger Bluetooth-Teilnehmer **11**, **11a** enthält ein Bluetooth-Modul **12**, **12a**, welches dazu ausgelegt ist, eine auf dem Bluetooth-Standard basierende Datenkommunikation mit einem entsprechend anderem Teilnehmer **11**, **11a** durchzuführen. Hierzu weist ein Bluetooth-Modul **12**, **12a** jeweils eine Sende-/Empfangsantenne **13**, **13a** auf. Der Aufbau eines Bluetooth-Moduls **12** ist in einer Vielzahl unterschiedlicher Ausführungsformen und Varianten allgemein bekannt, so dass nachfolgenden hierauf nicht näher eingegangen werden muss. Lediglich beispielsweise wurde in Fig. 3 der ungefähre Aufbau eines Bluetooth-Moduls **12**, **12a** beschrieben.

[0046] Erfindungsgemäß weist ein jeweiliger Teilnehmer **11**, **11a** ferner ein RFID-Modul **14**, **14a** auf. Das RFID-Modul **14**, **14a** ist dazu ausgelegt, eine Kommunikation mit einem entsprechenden RFID-Modul **14**, **14a** eines anderen Teilnehmers **11**, **11a** aufzubauen und durchzuführen. Das RFID-Modul **14**, **14a** enthält ebenfalls eine Sende-/Empfangsantenne **15**, **15a**. Das RFID-Modul **14**, **14a** ist über eine Steuerleitung **16**, **16a** mit dem jeweiligen Bluetooth-Modul **12**, **12a** verbunden.

[0047] Zumindest eines der RFID-Module **14**, **14a** kann Bestandteil eines Transponders oder ein Transponder selbst sein. Ein solcher Transponder kann als aktiver, passiver oder semipassiver Transponder ausgebildet sein. Aktive Transponder weisen über eine eigene Energieversorgung auf, während passive Transponder ihre Energieversorgung ausschließlich über die vom Lesegerät ausgesendeten elektromagnetischen Signale Xa1, Xa2 entnehmen. Umgekehrt kann auch in zumindest einem der RFID-Module **14**, **14a** ein Lesegerät angeordnet sein.

[0048] Die Schlüsseletablierungssignale Xa1, Xa2 können von den jeweiligen RFID-Modulen **14**, **14a** aktiv erzeugt und ausgesendet werden. Darüber hinaus existiert auch die Möglichkeit, diese Signale Xa1, Xa2 durch Rückstreuen der empfangenen, hochfrequenten Signale Xa1, Xa2 unter Ausnutzung des Rückstreuquerschnitts der Sende-/Empfangsantenne **15**, **15a** zu erzeugen.

[0049] Die miteinander im Anmeldebetrieb miteinander kommunizierenden RFID-Module **14**, **14a** bilden insgesamt ein RFID-System.

[0050] Solche RFID-Systeme sind allgemein bekannt. Lediglich zum allgemeinen Hintergrund von RFID-Systemen und deren Funktionsweise im Allgemeinen und deren Schlüsseletablierung und Authentifikation im Speziellen sei auf das Buch von Klaus Finkenzeller, RFID-Handbuch, dritte aktualisierte und erweiterte Auflage, Hansa-Verlag, 2002, verwiesen.

[0051] Ein RFID-System besteht dabei immer aus zwei Komponenten, einem Transponder, der an dem zu identifizierenden Objekt angebracht ist, und einem Erfassungs- oder Lesegerät, dem so genannten Reader, das je nach Ausführung und eingesetzter Technologie als bloßes Lese- oder als Schreib-/Leseeinheit ausgebildet ist. Ein solches Lesegerät beinhaltet typischerweise ein Hochfrequenzmodul (Sender und Empfänger), eine Steuereinheit sowie ein Koppelelement zum Transponder. Daneben sind viele Lesegeräte mit einer zusätzlichen Schnittstelle, beispielsweise einer RS 232- oder RS 485-Schnittstelle, ausgestattet, um die empfangenen Daten an ein anderes System, im vorliegenden Ausführungsbeispiel an das jeweilige Bluetooth-Modul **12**, **12a**, weiterzuleiten.

[0052] Der Transponder bildet den eigentlichen Datenträger eines RFID-Systems und besteht üblicherweise aus einem Koppelelement sowie einem einfachen elektronischen Mikrochip. Außerhalb des Ansprechbereiches des Lesegerätes verhält sich der Transponder typischerweise vollkommen passiv, sodass der Ansprechbereich des Transponders die maximale Reichweite der Datenkommunikation des RFID-Systems und somit der beiden RFID-Module **14**, **14a** bestimmt. Erst innerhalb des Ansprechbereiches des Lesegerätes und somit innerhalb der maximalen Reichweite A1 wird der Transponder aktiviert. Die maximale Reichweite A1 hängt im Wesentlichen von der Positioniergenauigkeit des Transponders bezüglich des Lese- Schreibgerätes und der Geschwindigkeit des Transponders im Ansprechbereich des Lesegerätes ab.

[0053] Das RFID-System, bestehend aus den RFID-Modulen **14**, **14a** in Fig. 1, arbeitet typischerweise in einem Frequenzbereich von etwa 100 KHz bis etwa 30 MHz mittels induktiver Kopplung. Das Bluetooth-System bestehend aus den Bluetooth-Modulen **12**, **12a** arbeitet demgegenüber bei einer Arbeitsfrequenz von 2,4 GHz, die durch den Bluetooth-Standard vorgegeben ist.

[0054] Nachfolgend sei das erfindungsgemäße Anmeldeverfahren anhand des Blockschaltbildes in Fig. 1 kurz erläutert:
Bevor die beiden Teilnehmer **11**, **11a** aus Fig. 1 eine Datenkommunikation zum Zwecke des Austauschens von Daten aufbauen können, muss sich zunächst einer dieser Teilnehmer **11**, **11a**, beispielsweise der als Slave fungierende Teilnehmer **11a**, bei dem jeweils anderen, als Master fungierenden Teilnehmer **11** anmelder. Dieser Vorgang wird nachfolgend als Anmeldebetrieb oder als Pairing bezeichnet. Im Anmeldebetrieb werden die beiden Teilnehmer **11**, **11a** in einen maximalen Abstand A1 zueinander gebracht. Dieser maximale Abstand A1 bezeichnet die maximale Reichweite für eine RFID-Kommunikation. Sind die beiden Teilnehmer **11**, **11a** in einem Abstand zueinander angeordnet, der geringer ist als der maximale Abstand A1, dann kann sich der Teilnehmer **11a** bei dem anderen Teilnehmer **11** anmelden.

[0055] Hierzu sendet das RFID-Modul **14a** des Teilnehmers **11a** Schlüsseletablierungssignale Xa1 an das jeweilige RFID-Modul **14** des anderen Teilnehmers **11**. Der andere Teilnehmer **11** wertet diese Schlüsseletablierungssignale Xa1 aus und sendet seinerseits entsprechende Schlüsseletablierungssignale Xa2 an das RFID-Modul **14a** des Teilnehmers **11a** zurück. Dort werden diese Schlüsseletablierungssignale Xa2 ebenfalls ausgewertet. Ergibt die Authentifikation in beiden RFID-Modulen **14**, **14a**, dass es sich jeweils um berechtigte Teilnehmer **11**, **11a** handelt, dann sind diese Teilnehmer **11**, **11a** für eine anschließende Datenkommunikation freigegeben. Die jeweiligen RFID-Module **14**, **14a** signalisieren dies dem Bluetooth-Modul **12**, **12a** über jeweilige Steuersignale XS, XSa. Die Bluetooth-Module **12**, **12a** können nun eine datenkommunikative Verbindung mit dem jeweiligen Bluetooth-Modul **12a** des soeben authentifizierten Teilnehmers **11a** durchführen.

[0056] Für diese Datenkommunikation, der nachfolgend auch als Normalbetrieb bezeichnet wird, können die beiden Teilnehmer **11**, **11a** in einen größeren Abstand A2 gebracht werden. Der Abstand A2 definiert die maximale Reichweite zwischen den beiden Teilnehmern **11**, **11a**, innerhalb der eine Bluetooth-Datenkommunikation noch zuverlässig und erfolgreich durchgeführt werden kann. Typischerweise ist diese maximale Reichweite A2 signifikant größer als die maximale Reichweite A1 für die RFID-basierte Schlüsseletablierung.

[0057] Sowohl die Schlüsseletablierung über einen Schlüsseletablierungspfad **17** wie auch die Datenkommunikation über einen Datenkommunikationspfad **18** können unidirektional, das heißt von einem Teilnehmer **11**, **11a** lediglich zu dem gegenüberliegenden anderen Teilnehmer **11**, **11a**, oder auch bidirektional, das heißt von jeweils einem Teilnehmer **11**, **11a** zu dem anderen und wieder zurück, erfolgen. Denkbar ist für beide Betriebsmodi auch ein Multiplexverfahren.

[0058] Zur Erhöhung der Sicherheit erfolgt im Anmeldebetrieb eine gegenseitige Authentifizierung zwischen Lesegerät und Transponder dadurch, dass beide zugehörige Teilnehmer **11**, **11a** gegenseitig die Kenntnis eines beiden Teilnehmern **11**, **11a** bekannten, so genannten geteilten Geheimnisses überprüfen. Ein solches geteiltes Geheimnis wird typischerweise in Form eines geheimen kryptographischen Schlüssels in die jeweiligen RFID-Modulen **14**, **14a** implementiert. Die Auswertung dieser Schlüsseletablierungssignale Xa1, Xa2 und somit der in diesen Signalen Xa1, Xa2 enthaltenen Authentifizierungsinfor-

mationen kann entweder im RFID-Modul **14**, **14a** selbst und somit innerhalb des Lesegerätes bzw. des Transponders erfolgen oder auch in dem eigentlichen Bluetooth-Modul **12**, **12a**. Für die Authentifizierung sind dabei verschiedene, mehr oder weniger komplexe Schlüsseletablierungsprotokolle vorhanden, die hier allerdings nicht näher beschrieben werden sollen. Diese sind insbesondere im Zusammenhang mit der RFID-Technologie beispielsweise aus dem oben genannten Buch von Klaus Finkenzeller allgemein bekannt und bedürfen daher nachfolgend keiner näheren Erläuterung.

[0059] Fig. 2 zeigt einen Bluetooth-Teilnehmer **11**, wie er in einem Kommunikationssystem **10** aus Fig. 1 verwendbar ist. In Fig. 2 enthält das RFID-Modul **14** eine Sende-/Empfangseinrichtung **20** sowie eine Auswerteeinrichtung **21**. Die Sende-/Empfangseinrichtung **20** ist einerseits mit der Sende-/Empfangsantenne **15** und andererseits mit der Auswerteeinrichtung **21** verbunden. In Fig. 2 ist im Empfangspfad **22** ferner eine Dekodiereinrichtung **24** vorgesehen, die dem Dekodieren der empfangenen Schlüsseletablierungssignale Xa1' dient. Ferner ist im Sendepfad **23** eine Kodiereinrichtung **25** zur Kodierung der zu sendenden Schlüsseletablierungssignale Xa2' vorgesehen.

[0060] Im Falle einer positiven Authentifikation, also für den Fall, dass ein empfangenes Schlüsseletablierungssignal Xa1 einem berechtigten Teilnehmer zugeordnet wird, dann erzeugt die Auswerteeinrichtung **21** ein Steuersignal Xs, welches an das Bluetooth-Modul **12** weitergeleitet wird. Dieses Steuersignal Xs zeigt dem Bluetooth-Modul **12** an, dass die eigentliche Datenkommunikation mit dem soeben authentifizierten, berechtigten Teilnehmer begonnen werden kann.

[0061] Fig. 3 zeigt ein zweites Ausführungsbeispiel eines erfindungsgemäßen Bluetooth-Teilnehmers **11**. Im Unterschied zu dem Ausführungsbeispiel in Fig. 2 umfasst das RFID-Modul **14** hier lediglich die Sende-/Empfangseinrichtung **20**. Diese Sende-/Empfangseinrichtung **20** ist dazu ausgelegt, elektromagnetische Schlüsseletablierungssignale Xa1 aufzunehmen und entsprechende Schlüsseletablierungssignale Xa2 über die Sende-/Empfangsantenne **15** auszusenden. Die Steuerung des Anmeldebetriebs sowie die Auswertung der empfangenen Schlüsseletablierungssignale Xa1' erfolgt hier in dem eigentlichen Bluetooth-Modul **12**.

[0062] Das Bluetooth-Modul **12** weist neben einer Sende-/Empfangseinrichtung **30** zu diesem Zwecke eine programmgesteuerte Einrichtung **31** auf, die mit der Sende-/Empfangseinrichtung **30** gekoppelt ist. Ferner kann in dem Bluetooth-Modul **12** ein Speicher **32** vorgesehen sein, beispielsweise ein Programmspeicher, Datenspeicher und/oder Adressspeicher, der mit der programmgesteuerten Einrichtung **31** verbunden ist. Die programmgesteuerte Einrichtung **31** ist dazu ausgelegt, die eigentliche Datenkommunikation mit anderen Bluetooth-Teilnehmern zu steuern und die bei dieser Datenkommunikation ausgetauschten Schlüsseletablierungssignale Xa1, Xa2 auszuwerten. Hierzu weist das Bluetooth-Modul **12** eine Kodier-/Dekodiereinrichtung **33** auf, die zwischen der Sende-/Empfangseinrichtung **30** und der programmgesteuerten Einrichtung **31** angeordnet ist. In der Kodier-/Dekodiereinrichtung **33** erfolgt das Kodieren der zu übertragenden Datensignale Xs2 bzw. das Dekodieren der empfangenen Datensignale Xs1.

[0063] Die programmgesteuerte Einrichtung **31** ist hier zusätzlich dazu ausgelegt, die Schlüsseletablierung und damit den Anmeldebetrieb zu steuern. Hierzu ist die Sende-/Empfangseinrichtung **20** über eine Dekodiereinrichtung **34** mit der programmgesteuerten Einrichtung **31** verbunden. Die programmgesteuerte Einrichtung **31** ist somit dazu ausgelegt, zusätzlich die empfangenen und dekodierten Schlüsseletablierungssignale Xa1' auszuwerten. Das Bluetooth-Modul **12** enthält ferner eine Kodiereinrichtung **35**, welche der programmgesteuerten Einrichtung **31** nachgeschaltet ist und über welche von der programmgesteuerten Einrichtung **31** erzeugte Schlüsseletablierungssignale Xa2' kodiert werden.

[0064] Statt der Verwendung einer programmgesteuerten Einrichtung **31** und eines Kodierers **35** kann zur Erzeugung der Schlüsseletablierungssignale Xa2 auch ein Zufallsgenerator **36** vorgesehen sein, der gesteuert über die programmgesteuerte Einrichtung **31** ausgangsseitig Zufallssignale Xa2' erzeugt, welche zur Erzeugung des zu sendenden Schlüsseletablierungssignals Xa2 herangezogen werden.

[0065] Fig. 4 zeigt anhand eines Blockschaltbildes eine bevorzugte Anwendung des erfindungsgemäßen Anmeldeverfahrens in einem Bluetooth-basierten Kommunikationssystem. Das Bluetooth-basierte Kommunikationssystem kann beispielsweise in Ergänzung oder anstatt eines DECT-Systems (DECT = Digital Enhanced Cordless Telecommunications) vorgesehen sein. Der Bluetooth- wie auch der DECT-Standard bezeichnen eine so genannte picozellulare Telephonie, welche innerhalb von Gebäuden verwendet werden können, wobei innerhalb des Gebäudes eine Reichweite bzw. ein Zellradius von etwa 25–50 Metern und außerhalb davon von über 100 Metern erreicht werden können.

[0066] Das Bluetooth-Kommunikationssystem **10** in Fig. 4 enthält eine Basisstation **40** sowie drei mobile Telefon-Endgeräte **41**. Die Basisstation **40** fungiert als Master, während die Telefon-Endgeräte **41** als Slave fungieren. Die Basisstation **40** entspricht somit dem Teilnehmer **11** in Fig. 1, während die Telefon-Endgeräte **41** dem Teilnehmer **11a** entsprechen.

Möchte sich ein zusätzliches Telefon-Endgerät **42** an der Datenkommunikation beteiligen, dann muss es sich zunächst mittels eines erfindungsgemäßen Anmeldeverfahrens, wie dies anhand von Fig. 1 beschrieben wurde, bei der als Master fungierenden Basisstation **40** anmelden. Hierzu muss das Telefon-Endgerät **42** innerhalb eines Abstands A1 zu dieser Basisstation gebracht werden, sodass mittels RFID-Technologie der erfindungsgemäße Anmeldevorgang stattfinden kann. Nach erfolgreichem Anmelden, bei dem der zusätzliche Teilnehmer **42** als berechtigter Teilnehmer authentifiziert wurde, kann auch mit diesem Teilnehmer **42** eine Datenkommunikationsverbindung zu der Basisstation **40** und somit zu den übrigen Teilnehmern **41** aufgebaut werden.

[0067] Obgleich die vorliegende Erfindung vorstehend anhand bevorzugter Ausführungsbeispiele beschrieben wurde, sei sie nicht darauf beschränkt, sondern lässt sich auf mannigfaltige Art und Weise modifizieren.

[0068] So ist die Erfindung nicht notwendigerweise für ein DECT-basiertes Kommunikationssystem, wie es in Fig. 4 beschrieben wurde, beschränkt, sondern lässt sich auf beliebige, Bluetooth-basierte Kommunikationssysteme erweitern. Auch ist die Erfindung nicht notwendigerweise auf den exakten Aufbau von Bluetooth-Teilnehmern entsprechend den Fig. 2 und Fig. 3 beschränkt. Vielmehr wäre auch denkbar, dass der schaltungstechnische Aufbau dieser Teilnehmer, insbesondere hinsichtlich deren Kodier- und/oder Dekodiereinrichtungen, programmgesteuerter Einrichtungen, Sende-/Empfangseinrichtungen, Auswerteeinrichtungen, etc., beliebig anders ausgebildet sein kann, sofern dies von der jeweiligen Applikation gestützt wird.

[0069] Auch wurde der Anmeldevorgang vorstehend lediglich durch eine einfache Schlüsseletablierung, bei der die Schlüsseletablierungssignale quasi ungeschützt, also mehr oder weniger unverschlüsselt, zwischen den Teilnehmern ausgetauscht wurde, beschrieben. Selbstverständlich wäre auch denkbar, zur Erhöhung der Sicherheit diese Schlüsseletablierungssignale zusätzlich zu verschlüsseln. Hierzu sind verschiedene Verschlüsselungsprotokolle bekannt, die allerdings allgemein bekannt sind, sodass im Rahmen der vorliegenden Patentanmeldung nicht näher darauf eingegangen wurde. Für die Frage der Verschlüsselung und Schlüsseletablierung und somit für die Frage der Sicherheit des Anmeldevorgangs gilt jeweils, je höher die Sicherheit gewünscht ist, desto höher sind die Anforderungen an die Schlüsseletablierung und an die Verschlüsselung zu stellen.

[0070] Auch sei die Erfindung nicht auf ein Bluetooth-basiertes Kommunikationssystem und entsprechende Teilnehmer beschränkt, sondern lässt sich auf beliebige Kommunikationssysteme und deren Teilnehmer erweitern, deren Reichweite der Datenkommunikation zumindest größer und insbesondere signifikant größer ist als die der RFID-Kommunikation.

Patentansprüche

1. Anmeldeverfahren zwischen Teilnehmern (**11**, **11a**) eines drahtlos arbeitenden Kommunikationssystems (**10**), bei dem für eine Schlüsseletablierung im Anmeldebetrieb zwischen an einer nachfolgenden Datenkommunikation vorgesehenen Teilnehmern (**11**, **11a**) hochfrequente elektromagnetische Schlüsseletablierungssignale (Xa1, Xa2) nach dem RFID-Standard ausgetauscht werden, welche eine gegenüber den Datensignalen (Xd1, Xd2) der Datenkommunikation (Xd1, Xd2) geringere Reichweite aufweisen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das drahtlos arbeitende Kommunikationssystem als ein nach dem Bluetooth-Standard arbeitendes Kommunikationssystem (**10**) oder als ein WLAN-Kommunikationssystem ausgebildet ist.

3. Verfahren nach wenigstens einem der vorstehenden Ansprüche,
dadurch gekennzeichnet,
dass das Verfahren zumindest zwei Betriebsmodi umfasst:
– einen Anmeldebetrieb, bei dem zunächst eine Schlüsseletablierung der an einer Datenkommunikation teilnehmenden Teilnehmer (**11**, **11a**) durch Austauschen von RFID-Schlüsseletablierungssignalen (Xa1, Xa2) durchgeführt wird,
– einen sich daran anschließenden Normalbetrieb, bei dem nach durchgeführter und erfolgreicher Schlüsseletablierung die Datenkommunikation zum Austausch von Datensignalen (Xd1, Xd2) zwischen den Teilnehmern (**11**, **11a**) erfolgt.

4. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass eine maximale Distanz (A1, A2) zwischen den Teilnehmern (**11**, **11a**) für die Schlüsseletablierung im Anmeldebetrieb geringer ist als für die Datenkommunikation im Normalbetrieb.

5. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die maximale Reichweite (A1) der Schlüsseletablierung im Anmeldebetrieb kleiner ist als 1,5 Meter, insbesondere kleiner ist als 0,5 Meter und vorzugsweise kleiner ist als 10 cm, und dass die maximale Reichweite (A2) der Datenkommunikation im Normalbetrieb größer ist als 2 Meter und insbesondere größer ist als 10 Meter.

6. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass

eine Schlüsseletablierung im Anmeldebetrieb eine Initialisierung sowie eine nachfolgende Link-Key-Erzeugung umfasst.

7. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass im Anschluss an eine Schlüsseletablierung im Rahmen eines Authentifikationsbetriebs eine Authentifikation der ausgetauschten RFID-Schlüsseletablierungssignale (Xa1, Xa2) vorgenommen wird.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass die Authentifikation der ausgetauschten RFID-Schlüsseletablierungssignale (Xa1, Xa2) nach dem Bluetooth-Standard erfolgt.

9. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass zu Beginn des Anmeldebetriebs zunächst ein Initialisierungsschlüssel zwischen den an der Anmeldung beteiligten Teilnehmern (**11**, **11a**) ausgetauscht wird, auf dem die weitere Schlüsseletablierung basiert.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass als Initialisierungsschlüssel im Anmeldebetrieb ein Passwort und/oder eine PIN-Nummer übertragen wird.

11. Verfahren nach einem der Ansprüche 9 oder 10, dadurch gekennzeichnet, dass zur Erzeugung des Initialisierungsschlüssel ein Schlüsseletablierungsprotokoll, insbesondere das Diffie Hellmann Protokoll, herangezogen wird.

12. Verfahren nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, dass für die Schlüsseletablierung ein Random-Generator (**36**) herangezogen wird.

13. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die an einer Anmeldung beteiligten Teilnehmern (**11**, **11a**) jeweils ein gemeinsames Geheimnis aufweisen, welches im Anmeldebetrieb zwischen diesen ausgetauscht wird.

14. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass im Anmeldebetrieb keine Verschlüsselung vorgesehen ist.

15. Verfahren nach wenigstens einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der Anmeldebetrieb Teil des Protokolls der Datenkommunikation ist.

16. Teilnehmer (**11**, **11a**) für ein Kommunikationssystem (**10**), insbesondere zum Betreiben eines Verfahrens nach wenigstens einem der vorstehenden Ansprüche,

– mit einem Kommunikations-Modul (**12**, **12a**) für eine Datenkommunikation, welches zum Senden und Empfangen von Datensignalen (Xd1, Xd2),
– mit einer programmgesteuerten Einrichtung (**31**), die zumindest die Steuerung der Datenkommunikation und die Auswertung der empfangenen Datensignale (Xd1, Xd2) vornimmt,
– mit einem RFID-Modul (**14**, **14a**) für einen Anmeldebetrieb, das zum Senden und Empfangen von RFID-Schlüsseletablierungssignalen (Xa1, Xa2), welche eine gegenüber den Datensignalen (Xd1, Xd2) geringere Reichweite aufweisen, ausgelegt ist.

17. Teilnehmer nach Anspruch 16, dadurch gekennzeichnet, dass der Teilnehmer (**11**, **11a**) als Bluetooth-Teilnehmer (**11**, **11a**) für ein nach dem Bluetooth-Standard arbeitendes Kommunikationssystem (**10**) ausgebildet ist und dass das Kommunikations-Modul (**12**, **12a**) als Bluetooth-Modul (**12**, **12a**) für eine Datenkommunikation nach dem Bluetooth-Standard ausgelegt ist.

18. Teilnehmer nach wenigstens einem der Ansprüche 16 oder 17, dadurch gekennzeichnet, dass die programmgesteuerte Einrichtung (**31**) zusätzlich auch die Steuerung des Anmeldebetriebs und/oder die Auswertung der RFID-Schlüsseletablierungssignale (Xa1, Xa2) vornimmt.

19. Teilnehmer nach wenigstens einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, dass die programmgesteuerte Einrichtung Bestandteil des Kommunikations-Moduls (**12**, **12a**) ist.

20. Teilnehmer nach wenigstens einem der Ansprüche 16 bis 19, dadurch gekennzeichnet, dass das Kommunikations-Modul (**12**, **12a**) eine mit einer ersten Sende-/Empfangsantenne (**13**, **13a**) verbundene erste Sende-/Empfangseinrichtung (**30**, **30a**) zum Senden und/oder Empfangen von Datensignalen (Xd1, Xd2), eine Codiereinrichtung (**33**) zum Codieren der zu sendenden Datensignale, eine Decodiereinrichtung (**33**) zum Decodieren der empfangenen Datensignale, eine Auswerteeinrichtung (**31**) zum Auswerten der empfangenen Datensignale sowie einen Speicher (**32**) zum Speichern von Programm-, Adress- und/oder empfangenen Daten aufweist.

21. Teilnehmer nach wenigstens einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, dass das RFID-Modul (**14**, **14a**) eine mit einer zweiten Sende-/Empfangsantenne (**15**, **15a**) verbundene zweite Sende-/Empfangseinrichtung (**20**, **20a**) zum Senden und/oder Empfangen von RFID-Schlüsseletablierungssignalen (Xa1, Xa2), eine Modulatoreinrichtung zum Modulieren der zu sendenden RFID-Schlüsseletablierungssignalen (Xa2) und eine Demodulatoreinrichtung zum Demodulieren der empfangenen RFID-Schlüsseletablierungssignale

(Xa1) aufweist.

22. Teilnehmer nach wenigstens einem der Ansprüche 16 oder 21, dadurch gekennzeichnet, dass das RFID-Modul (**14**, **14a**) einen Transponder und/oder ein Schreib-/Lesegerät aufweist.

23. Teilnehmer nach wenigstens einem der Ansprüche 16 bis 22, dadurch gekennzeichnet, dass ein Schlüsseletablierungsgenerator (**36**) vorgesehen ist, der mit der zweiten Sende-/Empfangseinrichtung (**20**, **20a**) gekoppelt ist und der einen Schlüssel für die zu sendenden RFID-Schlüsseletablierungssignale erzeugt.

24. Teilnehmer nach Anspruch 23, dadurch gekennzeichnet, dass ein Random-Schlüsselgenerator (**36**) als Bestandteil des Schlüsseletablierungsgenerators (**36**) zur Erzeugung eines Zufallschlüssels vorgesehen ist.

25. Teilnehmer nach wenigstens einem der Ansprüche 16 bis 24, dadurch gekennzeichnet, dass ein Speicher (**32**) vorgesehen ist, in dem Informationen über die empfangenen Schlüsseletablierungssignale (Xa1, Xa2) ablegbar sind.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

FIG 1

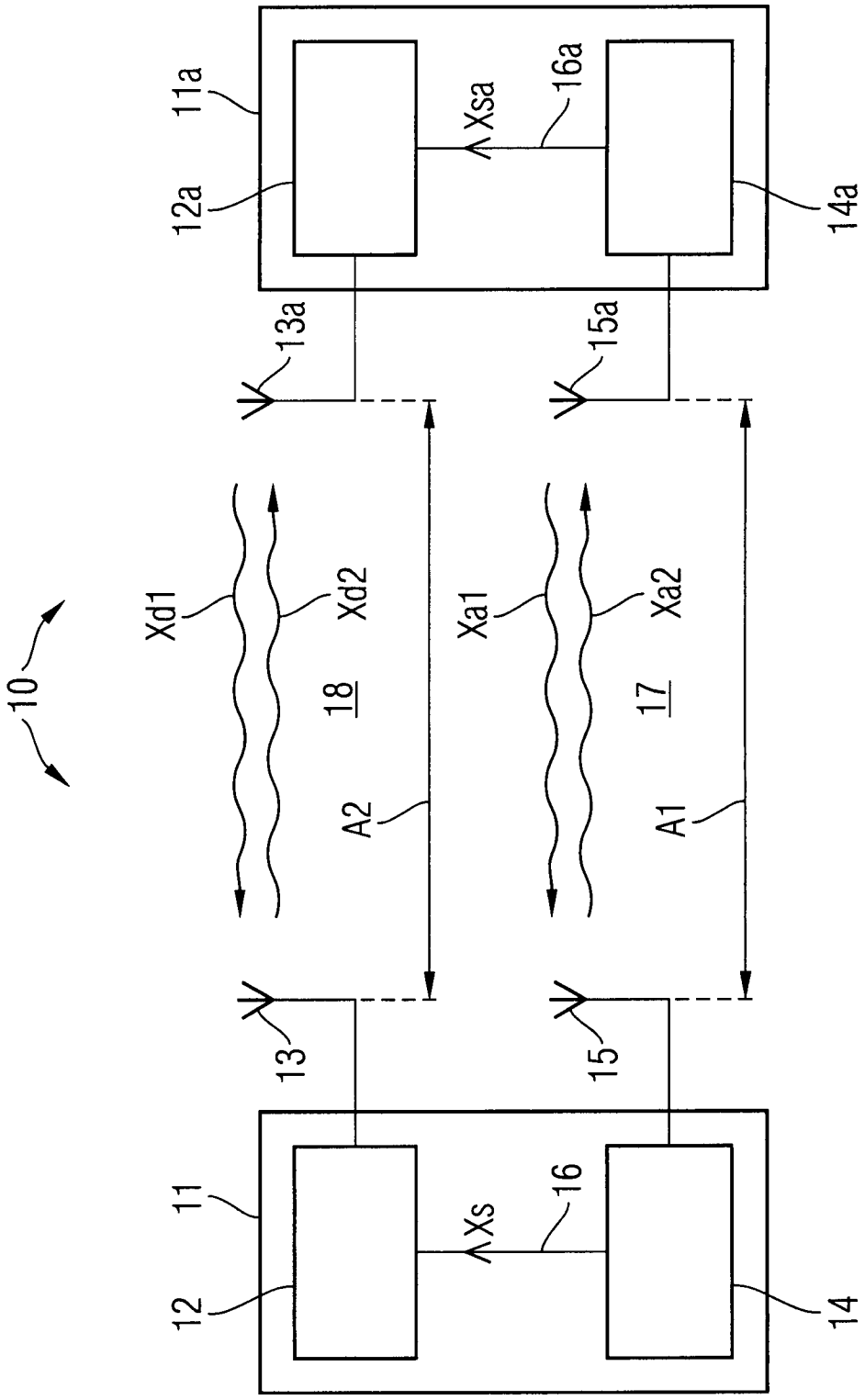


FIG 2

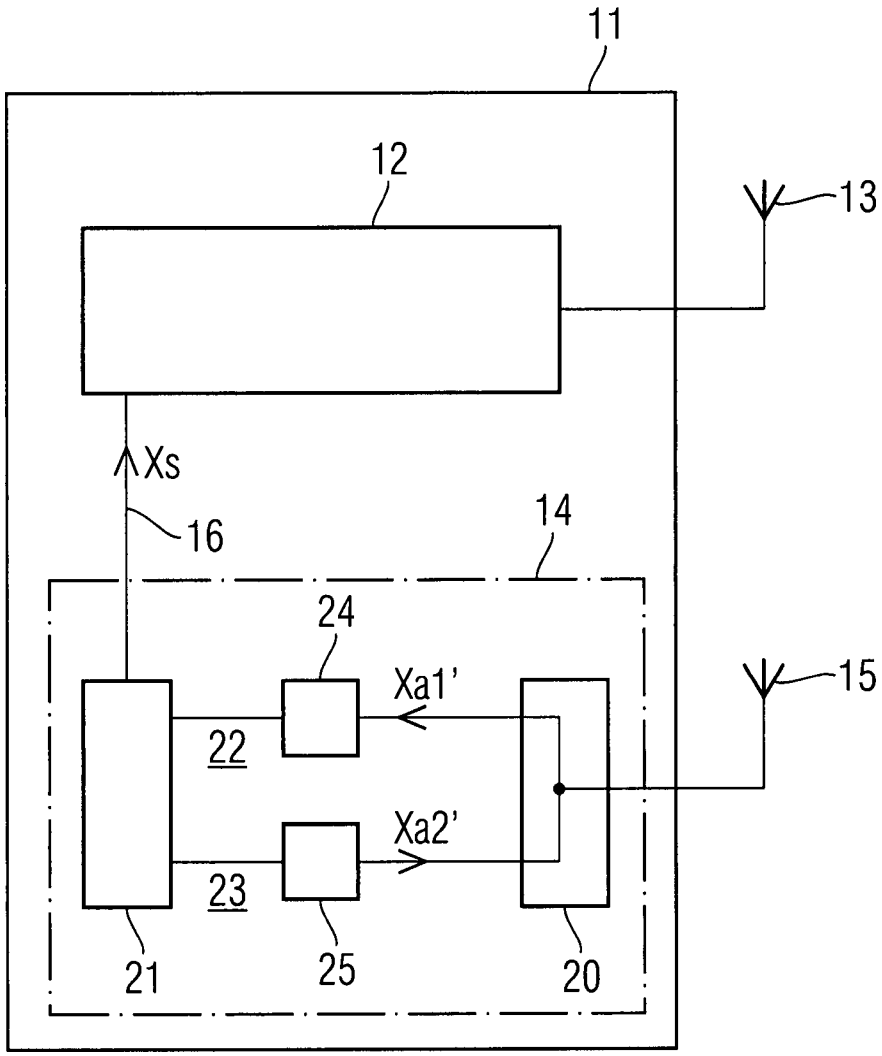


FIG 3

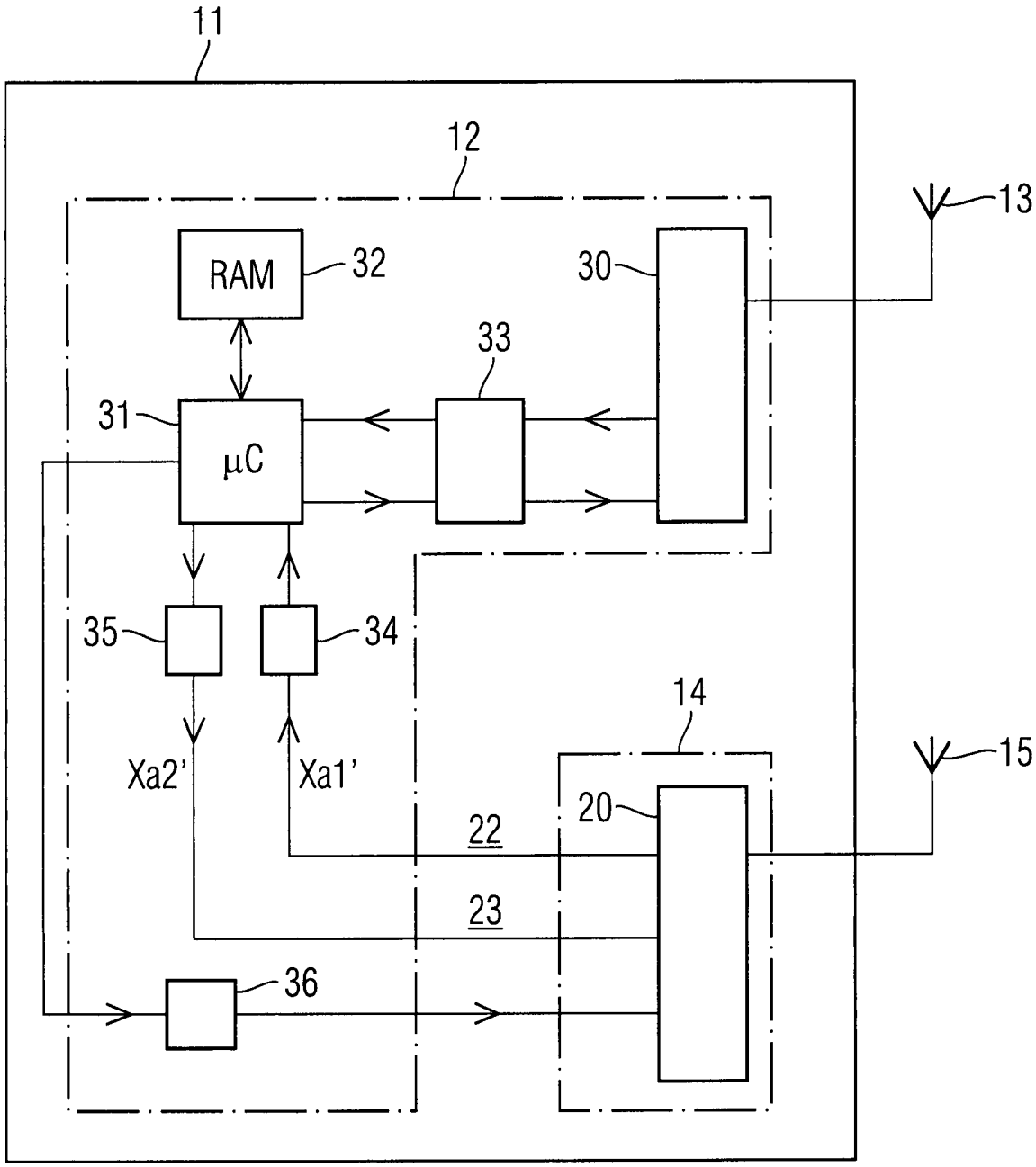


FIG 4