(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 101 04 409 B4** 2005.11.24

(12) # Patentschrift

(21) Aktenzeichen: **101 04 409.7**
(22) Anmeldetag: **01.02.2001**
(43) Offenlegungstag: **29.08.2002**
(45) Veröffentlichungstag
der Patenterteilung: **24.11.2005**

(51) Int Cl.[7]: **H04L 12/28**
H04L 29/12, H04M 1/737, H04Q 7/32

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten(§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 2 Patentkostengesetz).

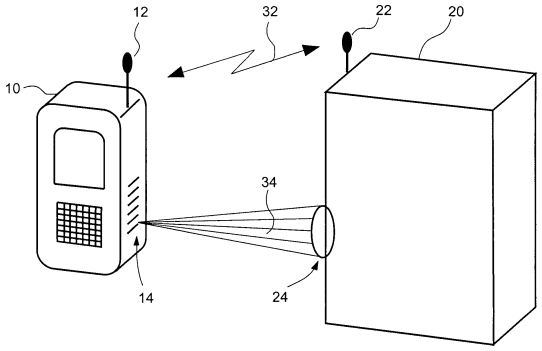
(73) Patentinhaber:
WINCOR NIXDORF International GmbH, 33106 Paderborn, DE

(72) Erfinder:
Kremer, Holger, 33175 Bad Lippspringe, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 100 25 017 A1
DE 6 92 22 911 T2
AOKI, Hisashi; MATSUSHITA, Soichiro: Balloon Tag:
(In)visible Marker Which Tells Who's Who, IEEE, 2000, S. 181-182;

(54) Bezeichnung: **Verbindungsauswahl über einen optischen Code**

(57) Hauptanspruch: Verfahren zum Aufbauen einer drahtlosen Verbindung zwischen einem Geldausgabeautomaten und einem Mobiltelefon, dadurch gekennzeichnet, daß der Geldausgabeautomat mittels einer Leseeinrichtung einen außen an dem Mobiltelefon sichtbaren optischen Code liest, daß der Code oder ein dem Code eindeutig zugeordneter Wert in dem Mobiltelefon elektronisch gespeichert ist, und beim Aufbau der Verbindung mittels dieses Codes die Identität der Teilnehmer der Verbindung gesichert wird, wobei für die drahtlose Verbindung ein Nahfeld-Funknetzwerk nach dem Bluetooth-Standard, verwendet wird.



Beschreibung

[0001] Die Erfindung betrifft eine Einrichtung, mit der beim Aufbau einer drahtlosen Verbindung die Identität der Teilnehmer gesichert wird.

Stand der Technik

[0002] Es wurde vorgeschlagen, bei einem Geldausgabeautomaten zumindest einen Teil der Interaktion mit dem Benutzer über ein mobiles Gerät abzuwickeln. Die Datenverbindung zu dem mobilen Gerät erfolgt bevorzugt über eine unter der Bezeichnung 'Bluetooth' bekannten Schnittstelle für drahtlose Funkübertragung. Im folgenden wird stellvertretend für ein mobiles Gerät mit Verarbeitungsfähigkeiten und einer Schnittstelle für drahtlose Datenübertragung ein Mobiltelefon mit Bluetooth-Transceiver angenommen.

[0003] Im Gegensatz zu der drahtlosen Verbindung nach dem IrDA-Standard, die mit Infrarotlicht arbeitet, ist eine Funkübertragung praktisch ungerichtet. Daher sieht die Bluetooth-Schnittstelle eine Geräte-Identifikation vor, so daß gezielt eine Verbindung zu einem Gerät der gewünschten Klasse erfolgen kann. Durch diese Methode ist an einem Arbeitsplatz oder im häuslichen Bereich das Problem der Geräte-Identifikation als gelöst anzusehen.

[0004] Bei mehreren gleichartigen Geräten jedoch sind weitere Maßnahmen notwendig.

[0005] Aus der DE 692 22 911 T2 ist ein Verfahren zwischen einer Mobilfernsprechstation und. einer fest verbundenen Fernsprechstelle beschrieben, bei dem die Fernsprechstellen mit einem Strichcode versehen sind. Wenn ein Benutzer der Mobilsprechstation wünscht, einen ankommenden Ruf zu einer nahegelegenen fest verbundenen Fernsprechstelle umzuleiten, liest der Benutzer den Strichcode des Telefons durch Aktivieren eines auf der Mobilfernsprechstation befindlichen Strichcodelesers. Hierdurch ist eine Identifikation der Fernsprechstelle möglich, jedoch kein Datenaustausch zwischen der Mobilfernsprechstation und der stationären Fernsprechstation.

[0006] In der DE 100 25 017 A1 ist ein Mobiltelefon beschrieben, das mit einem Barcodeleser ausgestattet ist. Hierdurch können Zeichen und Texte, die als Barcode verschlüsselt sind, vom Mobiltelefon eingelesen werden.

Aufgabenstellung

[0007] Gesucht ist jedoch ein Weg, für eine Datenverbindung zwischen einem Geldausgabeautomaten und einem Mobiltelefon schnell und eindeutig eine Zuordnung zwischen mobilem und stationärem Gerät zu bewirken

[0008] Die Erfindung verwendet hierzu eine außen auf dem mobilen Gerät sichtbare oder angezeigte optische Markierung, bevorzugt einen Strichcode, die von einer Leseeinrichtung an einem Geldautomaten gelesen werden kann.

[0009] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung, welche in Verbindung mit den beigefügten Zeichnungen die Erfindung an Hand eines Ausführungsbeispiels erläutert.

Kurzbeschreibung der Zeichnungen

[0010] Es zeigt

[0011] Fig. 1 symbolisch eine Anordnung, in der die Erfindung benutzt wird.

Ausführungsbeispiel

Beschreibung einer Ausführungsform der Erfindung

[0012] In Fig. 1 ist eine Anordnung symbolisiert, in der die Erfindung benutzt wird.

[0013] Ein mobiles Gerät, hier als Mobiltelefon **10** dargestellt, verfügt über eine Schnittstelle für eine drahtlose Verbindung, insbesondere ein Nahfeld-Funknetzwerk wie Bluetooth. Diese Einrichtung ist durch eine Antenne **12** symbolisiert. Bei einem Mobiltelefon sind demnach zwei drahtlose Verbindungen und zwei Antennen vorhanden; eine nicht gezeigte für die Verbindung für mobile Telefone und die gezeigte für das Funknetzwerk. Im übrigen ist bei modernen Funktelefonen keine der beiden Antennen als Stabantenne ausgeführt, so daß diese Symbolisierung angemessen erscheint.

[0014] Ferner ist an dem mobilen Gerät ein optischer Code angebracht, hier als Strichcode **14** an der Seite dargestellt.

[0015] Weiterhin ist ein stationäres Gerät **20** gezeigt, das gleichfalls über eine Schnittstelle für eine drahtlose Verbindung verfügt, die der von dem mobilen Gerät verwendeten entspricht und gleichfalls durch eine Antenne **22** symbolisiert ist.

[0016] Ferner verfügt das stationäre Gerät **20** über eine Abtasteinrichtung **24**, mit der, hier durch ein Strahlenbündel **34** symbolisiert, der Barcode **14** an dem mobilen Gerät **10** abgetastet wird.

[0017] Bei einer Ausführungsform der Erfindung stellt der Code auf dem mobilen Gerät die Netzwerkadresse des mobilen Geräts dar. In Netzwerksystemen ist es verbreitet, daß jeder Sende-Empfänger ('transceiver') eine eindeutige Adresse auf der untersten Ebene der Kommunikationsprotokolle, dem

'media access'-Layer, besitzt, die daher auch als MAC-Adresse bezeichnet wird. Ein geeignete Software im stationären Gerät wird daher nach dem Lesen des optischen Codes eine Verbindung zu genau dieser Adresse aufbauen und damit die Identität des mobilen Geräts sicherstellen. Um die Identität des stationären Geräts zu sichern, kann das mobile Gerät einen Verbindungaufbau darauf beschränken, daß dieser ohne vorherige Adressermittlung direkt mit der MAC-Adresse erfolgt.

[0018] Die Verwendung der MAC-Adresse hat insbesondere den Vorteil, daß dieser weltweit eindeutig ist und daher Kollisionen praktisch vollständig ausgeschlossen sind. Alternativ kann auch eine Netzwerkadresse aus anderen Schichten verwendet werden, insbesondere eine IP-Adresse, was mit Einführung von der Version 6 der Internetprotokolle wieder praktikabel wird.

[0019] Falls jedoch die Codierung der Netzwerkadresse nicht zweckmäßig ist, kann auch ein beliebiger anderer Code verwendet werden. Die Codierung der Netzwerkadresse kann insbesondere dann unzweckmäßig sein, wenn entweder die Netzwerksoftware deren Verwendung nicht oder schlecht unterstützt oder der Strichcode der Netzwerkadresse zu viel Platz auf einem kleinen Mobiltelefon beanspruchen würde oder eine Weitergabe dieses Codes aus anderen Gründen nicht erwünscht ist. Hierzu kann auch ein Code verwendet werden, der mittels einer Datenbank in die Netzwerkadresse umgewandelt wird.

[0020] Eine andere Alternative besteht darin, die Telefonnummer des Besitzers zu codieren. Auch dieser Code ist hinreichend eindeutig und weniger lang. Bei einem Mobiltelefon kann es ohnehin zweckmäßig sein, die relativ langen Nummern per Aufkleber maschinenlesbar zu machen.

[0021] In diesen Fällen, in denen der Code nicht eine Netzwerkadresse direkt darstellt, wird im Rahmen des Verbindungsaufbaus dieser Code übermittelt und überprüft. Dabei ist es unerheblich, welches Gerät den Code sendet und welches ihn vergleicht. Dies kann sowohl das die Verbindung initiierende Gerät als auch das gerufene Gerät, die Gegenstelle, sein. Der Code kann bereit mit dem Ruf übertragen oder in der Antwort des gerufenen Geräts enthalten sein.

[0022] Im Bluetooth-Netzwerk sind kryptographische Maßnahmen für die Sicherung des Datenverkehrs enthalten; das Schlüsselmanagement jedoch ist den Anwendungsschichten überlassen. Hier kann der Code in das Schlüsselmanagement integriert werden. Wird ein zufälliger Code verwendet, so kann dieser einfach zur Verschlüsslung der Kommunikation verwendet werden und so ohne weitere Maßnahmen bereits ein hohes Maß an Sicherheit gegen Abhören, Verfälschen und Vorspiegelung falscher Identität gewonnen werden. Obwohl dieser Sitzungsschlüssel nicht als sonderlich geheim anzusehen ist, erfordert ein gezielter Mißbrauch einen erheblichen Aufwand, der meist als prohibitiv hoch anzusehen ist. Selbstverständlich sollte ein solcher Code nicht zur Authentisierung einer Zahlung dienen.

[0023] Anstelle von einem zufälligen Code kann auch der öffentliche Schlüssel eines Schlüsselpaares bei asymmetrischer Verschlüsslung codiert sein, auch wenn dieser mit z.B. 1024 Bit oder 128 Byte länger als eine V6-Internet-Adresse ist. Dessen Verwendung rechtfertigt sich gegebenenfalls aus dem Zusatznutzen, daß einem Gesprächspartner auf einfach Art so der öffentliche Schlüssel für vertrauliche elektronische Kommunikation übergeben werden kann. Eine Variante benutzt eine Prüfsumme, üblicherweise als 'fingerprint' bezeichnet, eines öffentlichen Schlüssels, bzw. einen Teil davon und ermöglicht so die Verifizierung eines öffentlichen Schlüssels als Zusatznutzen.

[0024] Wird auf den Zusatznutzen verzichtet, so kann wegen der geringen Exposition und des relativ geringen Risikos auch ein speziell für diesen Fall gewähltes Schlüsselpaar mit geringer Bitlänge von z.B. 64 Bit entsprechend 22 Dezimalziffern gewählt werden, dessen privater Teil in dem mobilen Gerät gespeichert ist. Das stationäre Gerät verschüsselt einen neuen Sitzungsschlüssel mit dem gelesenen Code als öffentlichem Schlüssel und schickt das Ergebnis an das mobile Gerät, welches damit den Sitzungsschlüssel decodiert. Diese Hinweise sollen hier nur als Beispiel für die Integration des gelesenen Codes in das Schlüsselmanagement dienen.

[0025] Die Länge des Codes und der Grad seiner Zufälligkeit wird nach pragmatischen Gesichtspunkten oder normativen Vorgaben zu wählen sein. Lediglich vier Ziffern, insbesondere das Geburtsdatum ohne Jahr, dürfte wegen der Wahrscheinlichkeit einer Kollision, die beim Geburtsdatum ca. 1:30 beträgt, nicht ausreichend sein. Bevorzugt wird daher eine ohnehin eindeutige oder quasi-eindeutige Bezeichnung wie die Telefonnummer oder die Passnummer verwendet werden.

[0026] Die Erfindung wurde am einem Beispiel dargestellt, bei dem ein mobiles Gerät die optische Markierung trägt und ein stationäres Gerät den Leser für die Markierung umfaßt. Dies ist meistens dann sinnvoll, wenn die Anzahl der mobilen Geräte wesentlich größer als die der stationären Geräte ist. Zudem ist die Energieversorgung bei einem stationären Gerät einfacher. Die Erfindung umfaßt jedoch auch den umgekehrten Fall, bei dem die Markierung auf dem stationären Gerät angebracht und der optische Leser in dem mobilen Gerät vorgesehen ist. Da beispielsweise Selbstbedienungsgeräte, z.B. Geldautomaten,

normalerweise nicht über einen Barcode-Scanner verfügen, wird hier das mobile Gerät den Leser umfassen. Ein Barcode kann an einem Automaten dieser Art problemlos angebracht und ggf. erneuert werden.

[0027] Auch kann es für die Akzeptanz sinnvoll sein, daß das mobile Gerät die Adresse liest und von sich aus die Verbindung aufbaut. Im Falle der Bezahlung an einer Kasse ist es damit dem Ladeninhaber überlassen, daß die durch diesen Code veranlaßten Zahlung den richtigen Empfänger erreicht. Hier kann der Code auch besonders kurz sein, da nur eine kleine Zahl von stationären Geräten unterschieden werden muß.

[0028] Bei dem oben beschriebenen Fall eines speziell für diesen Fall bereitgestellten Schlüssels für asymmetrische Verschüsslung, dessen öffentlicher Teil auf dem mobilen Gerät codiert ist, liegt die Sicherung der Identität darin, daß das stationäre Gerät sicher sein kann, daß das mobile Gerät dasjenige ist, dessen Code gelesen wurde. Im Falle eines Geldautomaten und aus Sicht seiner Betreiber ist diese Variante vorzuziehen. In dem zuletzt dargestellten Fall, in dem die Leseeinrichtung an dem mobilen Gerät vorgesehen ist, ist daher umgekehrt die Identität des stationären Geräts gesichert. Dies könnte bei Kassen die bevorzugte Ausprägung sein.

[0029] Passende Strichcode-Leser geringer Leistungsaufnahme sind allgemein bekannt, insbesondere von Fernbedienungen für Videorecorder.

[0030] Der Anschaulichkeit halber wurde die Erfindung an Hand von Strichcodes als bevorzugter optischer Codierung beschrieben. Selbstverständlich sind andere Codes, z.B. OCR-Zeichen, gleichfalls verwendbar.

Patentansprüche

1. Verfahren zum Aufbauen einer drahtlosen Verbindung zwischen einem Geldausgabeautomaten und einem Mobiltelefon, **dadurch gekennzeichnet**, daß der Geldausgabeautomat mittels einer Leseeinrichtung einen außen an dem Mobiltelefon sichtbaren optischen Code liest, daß der Code oder ein dem Code eindeutig zugeordneter Wert in dem Mobiltelefon elektronisch gespeichert ist, und beim Aufbau der Verbindung mittels dieses Codes die Identität der Teilnehmer der Verbindung gesichert wird, wobei für die drahtlose Verbindung ein Nahfeld-Funknetzwerk nach dem Bluetooth-Standard, verwendet wird.

2. Verfahren nach Anspruch 1, wobei der gelesene Code die Netzwerkadresse des Mobiltelefons ist oder letztere über eine Datenbank aus dem gelesenen Code bestimmt wird.

3. Verfahren nach Anspruch 2, wobei als Code eine einer Person zugeordnete Nummer, wie zum Beispiel eine Telefonnummer, eine Passnummer oder ein Geburtsdatum, oder ein Teil davon, ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Code für das Schlüsselmanagement einer verschlüsselten Verbindung verwendet wird.

5. Verfahren nach Anspruch 4, wobei der an dem Mobiltelefon sichtbare Code den öffentlichen Teil eines Schlüsselpaares für asymmetrische Verschlüsslung bereitstellt und dessen geheimer Teil im Geldausgabeautomaten gespeichert ist.

6. Verfahren nach Anspruch 5, wobei der Geldausgabeautomat einen zufälligen Sitzungsschlüssel mit dem gelesenen Code verschlüsselt, an das Mobiltelefon sendet und dieses den Sitzungsschlüssel mittels des gespeicherten geheimen Teils rekonstruiert.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Code als Strichcode dargestellt ist.

8. Geldausgabeautomat mit einer Schnittstelle für eine drahtlose Verbindung, dadurch gekennzeichnet, daß der Geldautomat eine optische Leseeinrichtung umfaßt und Mittel enthält, um mit der optischen Leseeinrichtung einen Code zu lesen und mittels dieses Codes die Identität einer Gegenstelle der Verbindung zu sichern, wobei für die drahtlose Verbindung ein Nahfeld-Funknetzwerk nach dem Bluetooth-Standard verwendet wird.

9. Geldausgabeautomat nach Anspruch 8, dadurch gekennzeichnet, daß der gelesene Code die Netzwerkadresse der Gegenstelle ist oder letztere über eine Datenbank aus dem gelesenen Code bestimmt wird.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

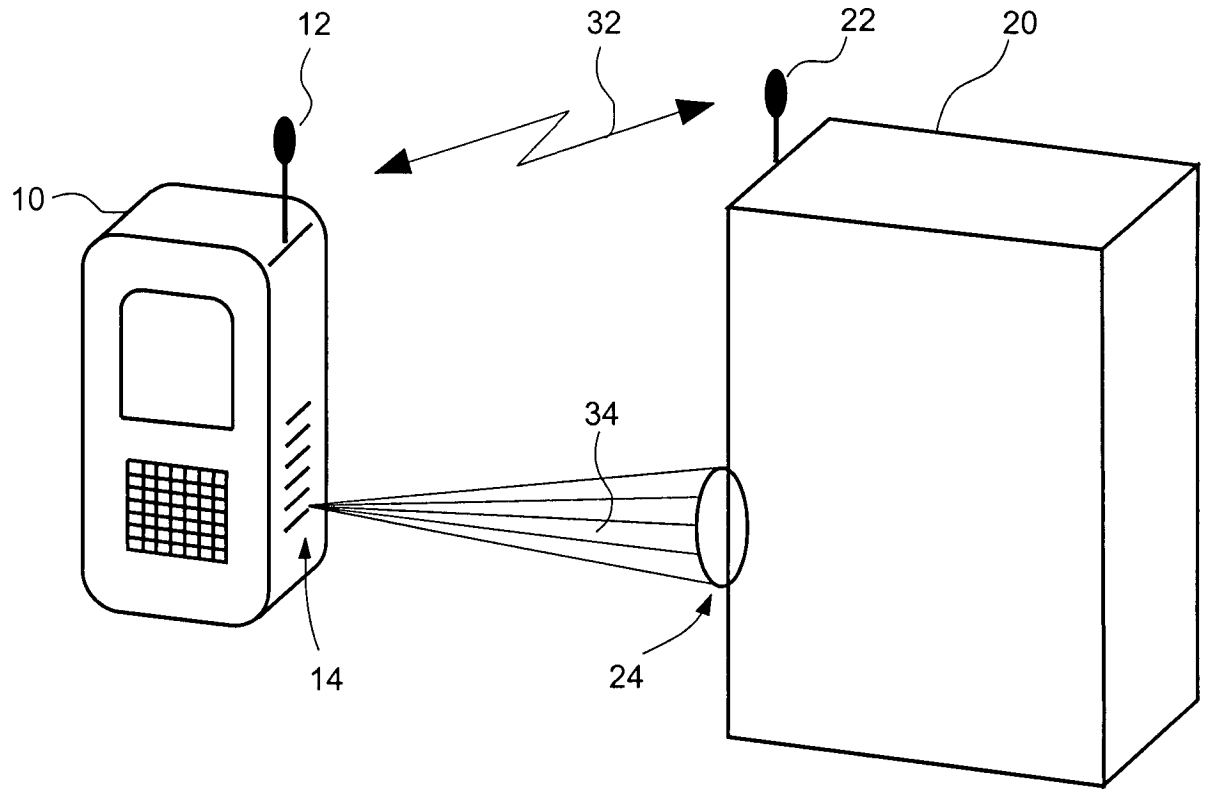


Fig. 1