(19) Deutsches Patent- und Markenamt

(10) **DE 10 2011 119 441 A1** 2013.05.29

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2011 119 441.3**
(22) Anmeldetag: **25.11.2011**
(43) Offenlegungstag: **29.05.2013**

(51) Int Cl.: ***G06Q 20/32*** (2012.01)

(71) Anmelder:
Giesecke & Devrient GmbH, 81677, München, DE

(72) Erfinder:
Weiß, Dieter, 81825, München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

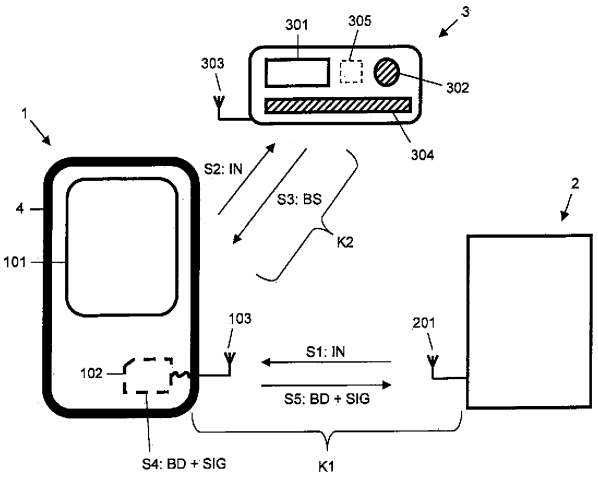
US	**2002 / 0 152 178**	**A1**
US	**2004 / 0 128 509**	**A1**
US	**2005 / 0 001 711**	**A1**
US	**2009 / 0 203 355**	**A1**
US	**2009 / 0 240 625**	**A1**
US	**2010 / 0 090 011**	**A1**
US	**2011 / 0 132 987**	**A1**
EP	**2 224 375**	**A1**

Rechercheantrag gemäß § 43 Abs. 1 Satz 1 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät und einem Terminal**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät (1) und einem Terminal (2). In dem erfindungsgemäßen Verfahren wird von dem Terminal (2) über eine erste kontaktlose Kommunikationsstrecke (K1) eine Information (IN), welche im Rahmen der elektronischen Transaktion durch einen Benutzer zu bestätigen ist, an das Endgerät (1) übermittelt. Die Information (IN) wird von dem Endgerät (1) über eine zweite kontaktlose Kommunikationsstrecke (K2) an einen tragbaren, am Endgerät (1) angebrachten Datenträger (3) umfassend eine Anzeigeeinheit (301) und eine von dem Benutzer betätigbare Eingabeeinheit (302) übermittelt. Diese Information (IN) wird dann auf der Anzeigeeinheit (301) des tragbaren Datenträgers (3) angezeigt, woraufhin der Bennutzer die Information (IN) über die Eingabeeinheit (302) bestätigen kann. Schließlich wird im Falle der Bestätigung der Information (IN) über die Eingabeeinheit (302) ein Bestätigungssignal (BS) von dem tragbaren Datenträger (3) über die zweite kontaktlose Kommunikationsstrecke (K2) an das Endgerät (1) übermittelt, woraufhin Bestätigungsdaten (BD) von dem Endgerät (2) über die erste kontaktlose Kommunikationsstrecke (K1) an das Terminal (2) übermittelt werden.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät und einem Terminal sowie ein entsprechendes System und einen tragbaren Datenträger, der zur Durchführung der elektronischen Transaktion verwendbar ist.

[0002] Im Rahmen der Durchführung von elektronischen Transaktionen zwischen einem mobilen Endgerät und einem Terminal ist es in der Regel erforderlich, dass eine entsprechende Information durch den Benutzer des Endgeräts bestätigt wird. Herkömmlicherweise wird zur Anzeige dieser Information bzw. zu deren Bestätigung das mobile Endgerät selbst verwendet, d. h. die Information wird auf dem Display des Endgeräts angezeigt und entsprechende Tasten des Endgeräts werden zur Bestätigung der Information verwendet. Es erweist sich dabei als nachteilhaft, dass dieser Vorgang für den Benutzer oftmals unkomfortabel ist, insbesondere wenn das mobile Endgerät von dem Benutzer erst aus einer entsprechenden Schutzhülle entnommen werden muss. Ferner ist die Verwendung des Displays und der Tasten des Endgeräts sicherheitskritisch, denn diese Komponenten können u. U. durch Angreifer manipuliert werden.

[0003] In der Druckschrift DE 10 2006 048 797 A1 ist ein Verfahren zum Ausführen einer Applikation beschrieben, welches beispielsweise für eine Homebanking-Anwendung verwendet werden kann. Dabei wird ein tragbarer Datenträger in der Form einer Chipkarte verwendet, welche Transaktionsdaten, die von einem Browser stammen und an einen Server weiterzuleiten sind, zunächst an ein Mobiltelefon übermittelt. Auf dem Mobiltelefon werden die Transaktionsdaten zur Anzeige gebracht und der Benutzer wird aufgefordert, die Transaktionsdaten freizugeben.

[0004] Die Druckschrift DE 103 16 771 A1 offenbart ein selbstklebendes Sicherheitslabel für Sicherheits- oder Wertdokumente, welches einen integrierten Schaltkreis und einen Transponder zur kontaktlosen Kommunikation umfasst. In dem integrierten Schaltkreis können z. B. benutzerindividuelle Daten gespeichert werden.

[0005] Aufgabe der Erfindung ist es, die Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät und einem Terminal sicher und für den Benutzer komfortabel auszugestalten.

[0006] Die Aufgabe der Erfindung wird durch die in den nebengeordneten unabhängigen Patentansprüchen beschriebenen Maßnahmen gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den jeweils abhängigen Ansprüchen beschrieben.

[0007] Das erfindungsgemäße Verfahren dient zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät und einem Terminal. Der Begriff des mobilen Endgeräts ist dabei weit zu verstehen und betrifft jede beliebige tragbare elektronische Vorrichtung, insbesondere ein Mobilfunktelefon und vorzugsweise ein Smartphone, ein PDA (PDA = Personal Digital Assistent), ein Laptop und dergleichen. Das Terminal stellt dabei eine Gegenstelle im Rahmen der elektronischen Transaktion dar und ist z. B. ein öffentlich zugängliches Terminal, über das entsprechende Transaktionen abgewickelt werden können.

[0008] Das Terminal stellt dabei beispielsweise eine Verbindung zu einem entfernten Server bereit, der sogenannte E-Services anbietet. Unter E-Services sind alle Dienste und Aktivitäten als Transaktionen zusammengefasst, die mittels Computern erstellt und über elektronische Medien interaktiv und/oder statisch angeboten und ausgeführt werden können. Der Begriff Server ist in dieser Anmeldung gleichbedeutend mit dem Begriff Anwendungsserver.

[0009] Eine Transaktion ist beispielsweise ein Informations- und Bildungsdienst, wie E-Education, E-Learning, E-Teaching, E-Publishing, E-Book und E-Catalog, um Beschaffungs-, Handels- und Bestelldienste wie E-Business, E-Commerce, E-Procurement, E-Cash, E-Shop, E-Intermediary, E-Auction, um kulturelle und administrative Dienste wie E-Culture, E-Government oder E-Vote, um Verbesserung der Dienstleistungen des Marketings, des Produktes oder der Kundenbeziehung, um elektronische Beratung wie E-Consult oder E-Advising.

[0010] Im Rahmen des erfindungsgemäßen Verfahrens wird von dem Terminal über eine erste kontaktlose Kommunikationsstrecke eine Information, welche im Rahmen der Transaktion durch einen Benutzer zu bestätigen ist, an das Endgerät übermittelt. Anschließend wird diese Information von dem Endgerät über eine zweite kontaktlose Kommunikationsstrecke an einen tragbaren, an dem mobilen Endgerät angebrachten Datenträger umfassend eine Anzeigeeinheit und eine von dem Benutzer betätigbare Eingabeeinheit übermittelt. Der tragbare Datenträger kann unmittelbar und insbesondere auch mittelbar am Endgerät befestigt sein. In einer besonders bevorzugten Ausführungsform ist der tragbare Datenträger an einer an dem Endgerät angebrachten Schutzhülle vorgesehen und vorzugsweise als Sticker (d. h. als flaches Element) ausgestaltet, der beispielsweise auf die Schutzhülle aufgeklebt ist. Der Datenträger ist insbesondere derart am Endgerät angebracht bzw. an der Schutzhülle vorgesehen, dass die Anzeigeeinheit vom Benutzer von außen wahrnehmbar ist und die Eingabeeinheit vom Benutzer von außen (z. B. über die Schutzhülle) betätigbar ist.

[0011] Der tragbare Datenträger ist insbesondere ein RFID-Transponder. Herkömmlich erfolgt sowohl die Energieversorgung eines RFID-Transponders in einem RFID-System als auch der Datenaustausch zwischen dem Transponder und dem Endgerät unter Verwendung magnetischer oder elektromagnetischer Felder. RFID-Transponder besitzen eine elektronische Schaltung und je nach Frequenzbereich eine Antennenspule (z. B. 13,56 MHz) oder eine elektromagnetische Antenne (z. B. 868 MHz). Über die Antenne kann dem Feld des Endgeräts die zum Betrieb des Transponders benötigte Energie entnommen sowie die Datenübertragung durchgeführt werden. Dazu stellt das Endgerät die entsprechende Energie bereit. Alternativ erfolgt die Energiebereitstellung von dem Terminal, an dem die Transaktion durchzuführen ist. Bis zu einem bestimmten Abstand zwischen Endgerät/Terminal und dem Transponder, welcher auch als Energiereichweitebezeichnet wird, kann der Transponder dem Feld des EndgerätsTerminals gerade noch ausreichend Energie zum Eigenbetrieb seiner Schaltung entnehmen. Typische Energiereichweiten solcher Systeme sind etwa 10 cm für ISO 14443 und bis zu 1 m für ISO 15693 kompatible Systeme.

[0012] Die Reichweite, innerhalb derer eine Kommunikation im System durch Datenübertragung möglich ist, kann erhöht werden durch Verwendung von aktiven Transpondern, also Transponder mit eigener Energieversorgung. Die Energieversorgung des aktiven Transponders, beispielsweise in Form einer Batterie oder eines Ladekondensators, betreibt dessen elektronische Schaltung. Herkömmliche Transponder ohne eigene Energieversorgung werden dagegen als passive Transponder bezeichnet.

[0013] RFID-Systeme, beispielsweise für verschiedene Kopplungsarten, sowie eine Lastmodulation unter Verwendung eines Hilfsträgers in induktiv gekoppelten RFID-Systemen werden insbesondere unter Kapitel 3.2 in dem ”RFID-Handbuch” von Klaus Finkenzeller beschrieben.

[0014] In Mobilfunkendgeräten wird die sogenannte Nahfeldkommunikationstechnik (NFC, Near Field Communication) integriert, um eine Kommunikation zwischen den Endgeräten oder mit dem Terminal zu ermöglichen. Die Kopplung der Geräte/Terminals findet über Spulen statt, wobei die Trägerfrequenz wie in RFID-Systemen 13,56 MHz beträgt. Wie in dem NFC-Standard ISO/IEC 18092 näher beschrieben, gibt es in NFC-Systemen einen aktiven Kommunikationsmodus und einen passiven Kommunikationsmodus. In dem aktiven Modus erzeugen zwei NFC-Einheiten abwechselnd ihr eigenes RF-Feld als Signalträger, schalten also wie in einem klassischen Mobilfunksystem, beide aufeinander abgestimmt, zwischen Sende- und Empfangsbetrieb hin und her. In dem passiven Modus müssen sich die beiden NFC-Einheiten dagegen einigen, welche Einheit als Lesegerät agiert und ein Feld erzeugt, das die andere Einheit dann mittels Lastmodulation beeinflussen kann.

[0015] Primär aufgrund der verwendeten kleinen Antennendurchmesser sind in NFC-Systemen – insbesondere im passiven Modus – nur geringe Kommunikationsreichweiten möglich. Die typische Reichweite von NFC-Endgeräten beträgt etwa 20 cm. Die eingesetzten Verfahren zur Datenübertragung sind denen kontaktloser Datenträger sehr ähnlich. NFC-Geräte sind daher auch in der Lage, mit kontaktlosen Datenträgern zu kommunizieren. Zur Realisierung der Kommunikation sind die Betriebsarten „Card Emulation”, „Reader Emulation” und „Peer to Peer” (P2P) möglich.

[0016] Im erfindungsgemäßen Verfahren wird die zu bestätigende Information auf der Anzeigeeinheit des tragbaren Datenträgers angezeigt, woraufhin der Benutzer die Information über die Eingabeeinheit bestätigen kann. Im Falle, dass der Benutzer diese Information über die Eingabeeinheit bestätigt, wird ein Bestätigungssignal von dem tragbaren Datenträger über die zweite kontaktlose Kommunikationsstrecke an das Endgerät übermittelt, woraufhin Bestätigungsdaten von dem Endgerät über die erste kontaktlose Kommunikationsstrecke an das Terminal übermittelt werden und hierdurch die Transaktion abgeschlossen wird.

[0017] Bei dem tragbaren Datenträger handelt es sich vorzugsweise um einen RFID-Sticker, der auf das Endgerät mechanisch lösbar angebracht werden kann. Insbesondere eine Klebeschicht auf dem Datenträger sorgt für die entsprechende Haftung zwischen Endgerät und Datenträger.

[0018] Alternativ ist der Datenträger mit Sicherheitsfunktionalitäten ausgestaltet und beispielsweise als Smart Card, Chipkarte, Token, Massenspeicherkarte, Multimediakarte oder elektronischen Identitätsdokument ausgestaltet.

[0019] Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass im Rahmen der Bestätigung von Informationen ein separater, nicht zum Endgerät gehöriger tragbarer Datenträger mit Anzeigeeinheit und Eingabeeinheit verwendet wird. Durch Anbringung dieses Datenträgers an dem Endgerät hat der Benutzer unmittelbar über sein Endgerät Zugriff auf den Datenträger. Er nutzt im Rahmen der Transaktion dabei nicht die Anzeigeeinheit bzw. die Tasten des Endgeräts, sondern die Anzeigeeinheit und die Eingabeeinheit des Datenträgers. Hierdurch werden Benutzerkomfort und Sicherheit erhöht. Insbesondere wenn der tragbare Datenträger an der Schutzhülle des Endgeräts vorgesehen ist, wird die Akzeptanz der Verwendung des Endgeräts bei der Durchführung der Transaktionen erhöht, denn ein Benutzer

muss zur Bestätigung entsprechender Informationen die Schutzhülle nicht mehr von dem Endgerät entfernen.

[0020] In einer besonders bevorzugten Ausführungsform basiert die erste und/oder die zweite Kommunikationsstrecke auf der mittlerweile weit verbreiteten Nahfeld- bzw. NFC-Kommunikation, mit der über kurze Reichweiten im Dezimeterbereich Informationen übertragen werden. Die Eingabeeinheit des tragbaren Datenträgers kann verschieden ausgestaltet sein. In einer Variante umfasst die Eingabeeinheit eine einzelne, durch den Benutzer betätigbare Taste, mit der die entsprechende, auf der Anzeigeeinheit dargestellte Information bestätigt werden kann. Gegebenenfalls kann die Eingabeeinheit auch mehrere Tasten zur Eingabe von komplexeren Bestätigungen nach Art einer PIN umfassen. Ebenso kann die Eingabeeinheit als Gesten-Erkennungs-Mittel bzw. als biometrischer Sensor zur Erkennung von biometrischen Merkmalen und insbesondere als Fingerabdrucksensor ausgestaltet sein.

[0021] Das erfindungsgemäße Verfahren kann zur Durchführung beliebiger elektronischer Transaktionen eingesetzt werden, bei denen eine Bestätigung durch einen Benutzer erforderlich ist. In einer besonders bevorzugten Ausführungsform wird das Verfahren zur Durchführung einer Bezahltransaktion verwendet, bei als Information, welche im Rahmen der elektronischen Transaktion durch den Benutzer zu bestätigen ist, ein an das Terminal zu zahlender Geldbetrag ist.

[0022] Um die Sicherheit des Verfahrens zu erhöhen, kommuniziert das Endgerät in einer besonders bevorzugten Ausführungsform mittels eines an sich bekannten Sicherheitselements (englisch: Secure Element) und/oder einer gesicherten Laufzeitumgebung, welche im Endgerät vorgesehen sind, über die erste und/oder die zweite kontaktlose Kommunikationsstrecke. Das Sicherheitselement ist dann insbesondere als Hardwarekomponente ausgestaltet und als ein fest integrierter Bestandteil im mobilen Endgerät angeordnet, wobei es entweder in der Form nicht vom mobilen Endgerät entnommen werden kann, beispielsweise als M2M Modul, Co-Prozessor bzw. Trusted Base oder als ein entnehmbares Modul mit Sicherheitsfunktionalität mit dem mobilen Endgerät verbunden ist, beispielsweise als Chipkarte, insbesondere einer Subscriber Identification Module, kurz SIM/USIM Karte, Smart Card, Massenspeicherkarte, USB-Token, Multimediakarte, Secure MicroSD-Karte, Mobilfunknetztoken, z. B. ein UMTS-Surfstick.

[0023] Alternativ ist das Sicherheitselement als eine Softwarekomponente als vertrauenswürdiger Teil des Betriebssystemkernels des mobilen Endgerätes bzw. als ein Sicherheitssoftware-Algorithmus ausgestaltet. Hierbei ist die Verwendung von gesicherten Laufzeitumgebungen zur Ausführung von Programmen bzw. Applikationen zu nennen. Insbesondere kann als gesicherte Laufzeitumgebung die an sich bekannte ARM TrustZone® eingesetzt werden, auf der z. B. das ebenfalls bekannte Betriebssystem MobiCore® läuft.

[0024] In einer weiteren, besonders bevorzugten Ausführungsform signiert das Sicherheitselement die über die erste kontaktlose Kommunikationsstrecke zu übermittelnden Bestätigungsdaten. Auf diese Weise wird es ermöglicht, dass am Terminal überprüft wird, dass die Bestätigungsdaten tatsächlich von dem Endgerät stammen, an das die zu bestätigende Information zuvor übermittelt wurde.

[0025] In einer weiteren bevorzugten Ausführungsform wird die Sicherheit des Verfahrens dadurch erhöht, dass sowohl eine gesicherte Laufzeitumgebung als auch ein Sicherheitselement im Endgerät vorgesehen sind, wobei die gesicherte Laufzeitumgebung den tragbaren Datenträger und das Sicherheitselement ansteuert. Durch die Ansteuerung des tragbaren Datenträgers durch die gesicherte Laufzeitumgebung wird eine manipulationsgeschützte Anzeige der Informationen auf der Anzeigeeinheit des Datenträgers erreicht. Durch die Ansteuerung des Sicherheitselements über die gesicherte Laufzeitumgebung können Manipulationen bei der Generierung bzw. Verarbeitung der an das Terminal zu übermittelnden Bestätigungsdaten vermieden werden.

[0026] In einer besonders bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird das Bestätigungssignal von dem tragbaren Datenträger an das Endgerät in der Form eines rollierenden Codes übermittelt, wobei sich der rollierende Code für jedes neu übermittelte Bestätigungssignal verändert und wobei der rollierende Code auf einem gemeinsamen Geheimnis zwischen tragbarem Datenträger und Endgerät oder zwischen tragbarem Datenträger und einer anderen (externen) Einheit basiert. Auf diese Weise werden Angriffe verhindert, bei denen ein Angreifer unbefugt versucht, das Bestätigungssignal zu simulieren und an das Endgerät zu übertragen.

[0027] In einer weiteren bevorzugten Ausführungsform ist das gemeinsame Geheimnis, das bei der Generierung des rollierenden Codes verwendet wird, durch eine manuelle, durch den Benutzer durchgeführte Paarung (englisch: Pairing) zwischen Endgerät und tragbarem Datenträger festgelegt. Die Paarung kann dabei auf einem Barcode basieren, der auf dem tragbaren Datenträger bzw. dessen Verpackung aufgebracht wird und bei der erstmaligen Verwendung des tragbaren Datenträgers z. B. über das Endgerät mittels eines geeigneten Lesers eingelesen wird. Hierdurch kann auf einfache Weise eine Zuordnung des tragbaren Datenträgers bei dessen Inbetriebnah-

me zu einem entsprechenden Endgerät erreicht werden.

[0028] In einer weiteren Variante des erfindungsgemäßen Verfahrens verifiziert das oben beschriebene Sicherheitselement den vom tragbaren Datenträger übermittelten rollierenden Code basierend auf dem gemeinsamen Geheimnis und generiert bei erfolgreicher Verifikation das Bestätigungssignal. Vorzugsweise signiert es dabei auch das Bestätigungssignal. Gegebenenfalls besteht auch die Möglichkeit, dass die oben beschriebene gesicherte Laufzeitumgebung den übermittelten rollierenden Code basierend auf dem gemeinsamen Geheimnis verifiziert und bei erfolgreicher Verifikation das Sicherheitselement dazu veranlasst, das Bestätigungssignal zu generieren und ggf. auch zu signieren.

[0029] Wie oben erwähnt, kann das gemeinsame Geheimnis auch zwischen dem tragbaren Datenträger und einer anderen (externen) Einheit festgelegt sein. Vorzugsweise übermittelt dabei das Endgerät den rollierenden Code als Bestätigungsdaten oder zusammen mit den Bestätigungsdaten über die erste Kommunikationsstrecke an das Terminal, woraufhin das Terminal die Verifikation des rollierenden Codes veranlasst und nur bei erfolgreicher Verifikation die elektronische Transaktion abgeschlossen wird. Gegebenenfalls kann das Terminal die externe Einheit darstellen. Die externe Einheit kann jedoch auch ein externer Server eines Hintergrundsystems sein, an den der rollierende Code von dem Terminal zur Verifikation weitergeleitet wird.

[0030] Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein System zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät und einem Terminal. Das System umfasst dabei das mobile Endgerät und den Terminal sowie einen tragbaren Datenträger. Das System ist derart ausgestaltet, dass in dessen Betrieb das erfindungsgemäße Verfahren bzw. eine oder mehrere Varianten des erfindungsgemäßen Verfahrens durchführbar sind.

[0031] Die Erfindung betrifft darüber hinaus einen tragbaren Datenträger zur Verwendung in dem erfindungsgemäßen Verfahren bzw. in einer oder mehreren Varianten des erfindungsgemäßen Verfahrens. Er umfasst eine Anzeigeeinheit, eine kontaktlose Kommunikationsschnittstelle, insbesondere zur NFC-Kommunikation, und eine von einem Benutzer betätigbare Eingabeeinheit, welche derart ausgestaltet sind, dass der tragbare Datenträger im Betrieb eine Information, welche von dem Benutzer zu bestätigen ist, über die kontaktlose Kommunikationsschnittstelle von dem Endgerät empfängt und anschließend über die Anzeigeeinheit anzeigt, wobei der tragbare Datenträger nach einer anschließenden Bestätigung der Information über die Eingabeeinheit das Bestätigungssignal über die kontaktlose Kommunikationsschnittstelle zum Endgerät aussendet.

[0032] Der tragbare Datenträger ist vorzugsweise an einer Schutzhülle vorgesehen, welche an das Endgerät angebracht werden kann. Das Anbringen erfolgt insbesondere mechanisch lösbar, beispielsweise mittels einer Klebeschicht auf dem tragbaren Datenträger. In diesem Sinne betrifft die Erfindung auch eine Schutzhülle mit dem daran vorgesehenen tragbaren Datenträger.

[0033] Insbesondere ist der tragbare Datenträger in Kommunikationsreichweite mit dem Mobiltelefon angeordnet und wird anstelle des Endgeräts zur Bestätigung der Transaktion verwendet wird. Dabei führt das Mobiltelefon die Transaktion ohne Benutzerinteraktion durch. Benutzerinteraktion im Sinne der Erfindung bedeutet zum Einen, dass der Benutzer weder beim Aufbau noch bei der Durchführung der Transaktion eine Interaktion auf dem Mobiltelefon durchführen muss. Zusätzlich muss der Benutzer das Endgerät nicht aus seiner Aufbewahrung, beispielsweise einer Tasche des Benutzers entnehmen, um die Transaktion durchzuführen, da die Bestätigung vom Datenträger übernommen wird.

[0034] Nachfolgend wird anhand einer Figur die Erfindung bzw. deren Ausführungsformen und Vorteile der Erfindung näher erläutert, wobei die Figur lediglich Ausführungsbeispiele der Erfindung beschreiben. Gleiche Bestandteile in der Figur werden mit gleichen Bezugszeichen versehen. Die Figur ist nicht als maßstabsgetreu anzusehen, es können einzelne Elemente der Figur übertrieben groß bzw. übertrieben vereinfacht dargestellt sein.

[0035] Die Erfindung wird nachfolgend basierend auf einer elektronischen Transaktion in der Form einer Bezahltransaktion erläutert, welche zwischen einem mobilen Endgerät eines Benutzers und einem Bezahl-Terminal durchgeführt wird. Gemäß **Fig. 1** wird als mobiles Endgerät ein Mobiltelefon **1** verwendet, das drahtlos über eine NFC-Kommunikationsstrecke K1 mit einem Bezahl-Terminal **2** kommuniziert. Zur kontaktlosen Kommunikation umfasst das Bezahl-Terminal eine schematisch angedeutete kontaktlose NFC-Schnittstelle bzw. Antenne **201**, welche mit einer entsprechenden NFC-Schnittstelle bzw. Antenne **103** (ebenfalls schematisch dargestellt) des Mobiltelefons **1** kommuniziert. Das Mobiltelefon umfasst ferner ein Display **101** sowie ein an sich bekanntes Sicherheitselement **102** (englisch: Secure Element), welches in der dargestellten Variante über die USIM/SIM-Karte des Benutzers realisiert ist.

[0036] Im Rahmen des hier beschriebenen Verfahrens möchte ein Benutzer über sein Mobiltelefon **1** kontaktlos einen vorbestimmten Betrag bezahlen. Beispielsweise kann das Bezahl-Terminal **2** zur Aus-

gabe von Fahrkarten für öffentliche Verkehrsmittel vorgesehen sein, wobei die Bezahlung der Fahrkarte kontaktlos über die Kommunikationsstrecke K1 erfolgen soll. Im Rahmen des Bezahlvorgangs ist es erforderlich, dass der zu bezahlende Betrag dem Benutzer angezeigt wird und durch diesen bestätigt wird. In der hier beschriebenen Variante der Erfindung wird hierzu neben dem Mobiltelefon **1** ein tragbarer Datenträger **3** in der Form eines sog. Stickers eingesetzt. Dieser Sticker ist in einer Schutzhülle **4** vorgesehen, in welche das Mobiltelefon **1** gesteckt ist. Die Schutzhülle ist dabei durch einen dickeren Rand um das Mobiltelefon **1** angedeutet. Der Sticker **3** umfasst ein separates Display **301** sowie eine Taste **302** und wiederum eine NFC-Schnittstelle bzw. Antenne **303**, mittels der eine Kommunikation mit dem Mobiltelefon über dessen Antenne **103** basierend auf der kontaktlosen Kommunikationsstrecke K2 erfolgt. Darüber hinaus ist auf dem Sticker ein Barcode angebracht, der schematisch durch das Bezugszeichen **304** angedeutet ist. Durch die Anbringung des Stickers auf der Schutzhülle **4** kann auf einfache Weise eine Anzeige und Bestätigung des im Rahmen des Bezahlvorgangs zu bezahlenden Betrags über das Display **301** und die Taste **302** erreicht werden, wie im Folgenden noch näher erläutert wird.

[0037] Der in der hier beschriebenen Ausführungsform verwendete Sticker ist sehr einfach aufgebaut und umfasst vorzugsweise keine eigene Energieversorgung, d. h. er wird lediglich durch die über die NFC-Schnittstelle **303** empfangene Feldenergie im Rahmen einer kontaktlosen Kommunikation betrieben. Nichtsdestotrotz besteht gegebenenfalls auch die Möglichkeit, dass ein Pufferspeicher oder eine Batterie im Sticker vorgesehen sind, die je nach Anwendungsfall den Sticker zusätzlich oder vollständig mit Energie versorgen.

[0038] Im Folgenden wird der Ablauf des Bezahlvorgangs basierend auf den in Fig. 1 dargestellten Geräten erläutert. Im Rahmen des Bezahlvorgangs ist es erforderlich, dass der Benutzer den zu zahlenden Betrag in geeigneter Weise bestätigt. Deshalb wird in Schritt S1 eine Information IN über die kontaktlose Kommunikationsstrecke K1 von dem Terminal **2** übermittelt. Diese Information enthält den von dem Benutzer zu zahlenden Geldbetrag. Nach Empfang der Information IN im Mobiltelefon **1** bzw. Sicherheitselement **102** wird diese – im Unterschied zu bekannten Verfahren nicht auf dem Display **101** angezeigt, sondern im Schritt S2 über die kontaktlose Kommunikationsstrecke K2 an den Sticker **3** weitergeleitet. Da der Sticker in der Schutzhülle **4** des Mobiltelefons vorgesehen ist, ist auch sichergestellt, dass dieser in Kommunikationsreichweite zu dem Mobiltelefon **1** ist. Die im Sticker empfangene Information IN wird anschließend auf dem Display **301** des Stickers angezeigt. Der Benutzer kann den Betrag dann ablesen, ohne dass er die Schutzhülle **4** vom Mobiltelefon **1** entfernen muss. Sollte der Betrag dem Zahlbetrag entsprechen, der im Rahmen der Transaktion dem Benutzer zuvor (z. B. über ein Display auf dem Terminal) mitgeteilt wurde, kann der Benutzer nunmehr über die Betätigung der Taste **302** den Betrag bestätigen.

[0039] Nach dieser Bestätigung wird im Schritt S3 über die kontaktlose Kommunikationsstrecke K2 ein entsprechendes Bestätigungssignal BS vom Sticker **3** an das Mobiltelefon **1** übermittelt. Aus diesem Bestätigungssignal werden in Schritt S4 entsprechende Bestätigungsdaten BD generiert, die über das Sicherheitselement **102** mit einer Signatur SIG versehen werden. Die Bestätigungsdaten können dabei ggf. dem Bestätigungssignal entsprechen. Die signierten Bestätigungsdaten werden schließlich in Schritt S5 über die erste kontaktlose Kommunikationsstrecke K1 an das Terminal **2** übermittelt. Durch die empfangenen Bestätigungsdaten wird dem Terminal mitgeteilt, dass der Bezahlvorgang durch den Benutzer autorisiert wurde und der Transaktionsvorgang hiermit abgeschlossen ist. Über die Signatur der Bestätigungsdaten kann das Terminal ferner überprüfen, dass die Bestätigungsdaten auch tatsächlich von dem Mobiltelefon **1** des Benutzers stammen.

[0040] Im Allgemeinen werden zur Unterstützung von elektronischen Transaktionen entsprechende Applikationen bzw. Applets verwendet, welche in dem Sicherheitselement **102** des Endgeräts **1** integriert sind. In einer Variante der Erfindung unterstützt das Applet im Sicherheitselement bereits von sich aus die Einbindung des Stickers **3** in die Transaktion. Es sind jedoch auch Varianten denkbar, bei denen das Applet die Einbindung des Stickers nicht unterstützt. In diesem Fall ist ein zweites Sticker-Applet auf dem Endgerät **1** installiert, welches nicht unbedingt auf dem Sicherheitselement **102** hinterlegt sein muss. Dieses Applet übernimmt dann die Kommunikation zwischen dem Sicherheitselement bzw. dem Endgerat und dem Sticker. Es fängt dabei die Ausgabe des Bezahlapplets auf dem Endgerät bzw. an das mobile Endgerät ab und leitet die Information bezüglich des zu zahlenden Betrags an den Sticker weiter. Umgekehrt empfängt dieses Applet die Antwort vom Sticker und erzeugt daraus eine Antwort, die den Anforderungen des Bezahlapplets auf dem Sicherheitselement genügt.

[0041] Die Kommunikation zwischen dem Endgerät und dem Sticker sollte möglichst einfach sein. D. h., auf die Verwendung von komplexen kryptographischen Algorithmen sollte im Rahmen der Kommunikation verzichtet werden. In einer bevorzugten Ausführungsform der Erfindung wird deshalb die in Schritt S2 übermittelte Information IN bezüglich des Bezahlbetrags unverschlüsselt übertragen. Dies ist unproblematisch, denn würde dieser Betrag von einem Angreifer verfälscht, so würde der falsche Betrag für den

Benutzer auf dem Display **301** des Stickers **3** sichtbar und demzufolge von dem Benutzer nicht bestätigt werden. Zur Erhöhung der Sicherheit wird in Schritt S2 auch darauf verzichtet, weitere Informationen, wie z. B. die Identifikation des Endgeräts, zusammen mit der Information IN zu übermitteln.

[0042] Im Unterschied zur Kommunikation vom Endgerät **1** hin zum Sticker **3**, ist die umgekehrte Kommunikation vom Sticker **3** hin zum Endgerät **1** deutlich sicherheitskritischer. Insbesondere könnte ein Angreifer das beim Drücken der Taste **302** ausgesendete Bestätigungssignal BS nachstellen und an das Endgerät **1** senden, so dass unbemerkt Transaktionen von außen durchgeführt werden könnten. Um dies zu vermeiden, sind in einer bevorzugten Variante der Erfindung entsprechende Sicherheitsmechanismen vorgesehen, welche vorzugsweise möglichst einfach ausgestaltet sein sollten. Insbesondere können dabei sog. rollierende Codes zum Einsatz kommen, welche nach Art eines One-Time-Passworts immer nur einmalig bei der Betätigung der Taste **302** erzeugt werden und sich somit von Betätigung zu Betätigung verändern. D. h., der Sticker **3** sendet nach dem Anzeigen des zu zahlenden Betrags auf dem Display **301** und nach der zugehörigen Bestätigung des Benutzers über die Taste **302** bei jeder Bezahltransaktion einen anderen Code zurück an das Endgerät **1**. Hierfür ist es erforderlich, dass das Endgerät den Code in geeigneter Weise als Bestätigungssignal verifizieren kann. In einer bevorzugten Variante wird dies durch eine manuelle Paarung (englisch: Pairing) zwischen dem Endgerät **1** und dem Sticker **3** erreicht. Über diese Paarung wird sichergestellt, dass das Endgerät und der Sticker ein gemeinsames Geheimnis aufweisen, auf dem dann der entsprechende rollierende Code basiert. Einem Angreifer ist es dann nicht mehr möglich, die Ausgabe eines Bestätigungssignals gegenüber dem Endgerät vorzutäuschen.

[0043] Das manuelle Pairing zwischen dem Endgerät **1** und dem Sticker **3** kann auf verschiedene Weise vorgenommen werden. In der Ausführungsform der **Fig. 1** wird hierzu der auf dem Sticker **3** aufgedruckte Barcode **304** verwendet, der eindimensional oder zweidimensional sein kann. Der Barcode kann gegebenenfalls auch auf der Verpackung des Stickers aufgebracht sein, der nach dem Auspacken dann auf der Schutzhülle des Mobiltelefons, z. B. über eine entsprechende Klebefläche, befestigt wird. Der Barcode enthält den Teil des Geheimnisses, den das Endgerät zur Verifikation des rollierenden Codes benötigt. Im Rahmen der Durchführung des manuellen Pairings wird zur Inbetriebnahme des Stickers der entsprechende Barcode über einen Leser des Endgeräts eingelesen und anschließend dazu verwendet, um das Bezahlapplet auf dem Sicherheitselement bzw. das separate Sticker-Applet zu personalisieren. Das manuelle Pairing kann jedoch gegebenenfalls auch auf andere Weise ablaufen, z. B. über die Eingabe einer Zahlenfolge mittels der Tastatur des Endgeräts, ähnlich dem Pre-Shared Key bei WLAN. Die Zahlenfolge kann dabei wiederum auf dem Sticker bzw. dessen Verpackung aufgebracht sein.

[0044] Das im Vorangegangenen beschriebene erfindungsgemäße Verfahren kann verschiedenen Modifikationen unterliegen. Insbesondere kann der Sticker komplexer ausgestaltet sein, um die Transaktionssicherheit weiter zu erhöhen. Es kann beispielsweise zur Bestätigung des am Display **301** angezeigten Betrags die Eingabe einer Tastenkombination nach Art einer PIN vorgesehen sein. In diesem Fall sind auf dem Sticker weitere Tasten vorgesehen. Ferner kann die Bestätigung mittels einer Geste des Benutzers eingegeben werden, welche z. B. durch einen Dehnungsmessstreifen am Sticker erfasst werden kann. Ebenso besteht bei hochsicherheitskritischen Transaktionen die Möglichkeit, biometrische Merkmale des Benutzers über einen biometrischen Sensor am Sticker zu erfassen. Vorzugsweise wird hierzu ein Fingerabdrucksensor verwendet. Nur wenn ein über den Sensor erfasster Fingerabdruck mit einem im Sticker hinterlegten Abdruckmuster übereinstimmt, wird dann ein entsprechendes Bestätigungssignal BS ausgesendet.

[0045] In einer weiteren Variante können spezielle Sicherheitsmechanismen zur Prüfung der oben beschriebenen rollierenden Codes vorgesehen werden.

[0046] Vorzugsweise ist dabei auf dem Mikroprozessor des mobilen Endgeräts eine an sich bekannte Trustzone vorgesehen, innerhalb der die Verifikation der rollierenden Codes erfolgt. Die Trustzone stellt eine gesicherte Laufzeitumgebung dar und verwendet in einer bevorzugten Ausführungsform das an sich bekannte Betriebssystem MobiCore. In einer weiteren Ausführungsform wird die Ansteuerung des Stickers **3** und des Sicherheitselements **102** ausschließlich über eine Trustzone vorgenommen. Durch diese Ansteuerung ist das Sticker-Display **301** ein sog. sicheres Display, welches gegen Manipulationen geschützt ist. Der auf dem Display angezeigte Bezahlbetrag ist demzufolge vertrauenswürdig. Über die Trustzone wird auch die Prüfung eines empfangenen Bestätigungssignals und insbesondere eines entsprechenden rollierenden Codes durchgeführt. Erst bei positiver Verifikation des Signals steuert die TrustZone das Sicherheitselement **102** zur Signatur entsprechender Bestätigungsdaten an. Ggf. besteht auch die Möglichkeit, dass der rollierende Code durch das Sicherheitselement geprüft wird. Dabei kann der rollierende Code z. B. mit dem bestätigten Bezahlbetrag verknüpft sein, wodurch eine Art TAN geschaffen wird.

[0047] In den soeben beschriebenen Varianten der Erfindung wird immer ausgehend vom Endgerät die Richtigkeit der rollierenden Codes geprüft. Gegebe-

nenfalls ist es auch möglich, dass ein entfernter, vertrauenswürdiger Server, beispielsweise der Server des Anbieters des Bezahlsystems, die rollierenden Codes überprüft. Dabei wird der Code zusammen mit den Bestätigungsdaten BD über die Kommunikationsstrecken K1 von dem Endgerät **1** an das Terminal **2** gesendet. Das Terminal reicht den Code dann an den entfernten Server weiter, der diesen überprüft. Diese Variante der Erfindung hat den Vorteil, dass ein Trojaner-Angriff auf das Endgerät deutlich geringere Aussichten auf Erfolg hat. Dies Liegt daran, dass das Endgerät nun nicht mehr personalisiert ist und ein Trojaner somit keinen Zugriff auf das gemeinsame Geheimnis zwischen Sticker und Server hat. Ein Trojaner kann folglich auch keine verborgenen Transaktionen mehr auslösen, denn hierzu ist immer die Generierung eines entsprechenden Bestätigungssignals erforderlich, für das jedoch das gemeinsame Geheimnis benötigt wird.

[0048] Die im Vorangegangenen beschriebenen Ausführungsformen der Erfindung weisen eine Reihe von Vorteilen auf. Über die Verwendung eines am Endgerät angebrachten Stickers mit Display und Taster wird eine einfache und komfortable Abwicklung von Transaktionen mit geringen Zusatzkosten erreicht. Da der Sticker vorzugsweise in der Schutzhülle des Endgeräts vorgesehen ist, ist es nicht mehr erforderlich, dass zur Abwicklung der Transaktionen das Endgerät aus der Schutzhülle entfernt werden muss, was die Akzeptanz bei der Durchführung der Transaktionen beim Benutzer erhöht. Ferner wird die Gefahr reduziert, dass das Endgerät beim Entfernen aus der Schutzhülle herunterfällt und hierdurch beschädigt bzw. zerstört wird. Zur Realisierung der elektronischen Transaktionen sind ferner nur geringe Modifikationen im Vergleich zu herkömmlichen, ohne Zwischenschaltung eines Stickers durchgeführten Transaktionen erforderlich. Insbesondere muss nur die Software auf dem Endgerät angepasst werden. Somit kann das erfindungsgemäße Verfahren in bereits bestehende Bezahlsysteme problemlos integriert werden. Darüber hinaus ist es von Vorteil, dass zur Bestätigung der Transaktion ein separater tragbarer Datenträger verwendet wird, denn die Tastatur auf einem mobilen Endgerät gilt im Regelfall nicht als sicher.

[0049] In einer alternativen Ausgestaltung ist der Datenträger **3** nicht notwendigerweise auf der Schutzhülle **4** des Mobiltelefons **1** angebracht sein. Vielmehr kann der Datenträger **3** auch als ein kostengünstiges Endgerät dienen, welches das Hantieren mit dem Mobiltelefon **1** überflüssig macht. In diesem Fall hatte der Datenträger **3** die Form einer ID-**1**-Chipkarte.

[0050] Der beschriebene Ablauf der Transaktion ändert sich dabei nicht. Der Kunde/Benutzer zieht nur noch die Karte aus der Tasche und bestätigt die Transaktion. Da die Kommunikationsreichweite zwischen Datenträger **3** du Endgerät **1** wie üblich in RFID- und NFC-Systemen bis zu 20 cm beträgt ist eine derartige Ausgestaltung prinzipiell möglich. Attraktiver für den Benutzer ist allerdings eine größere Kommunikationsreichweite für die Datenübertragung.

[0051] Dafür wird zur Kommunikation zwischen Endgerät **1** und Datenträger **3** ein RFID-System zur Übertragung im Ultra High Frequency, kurz UHF-Bereich eingesetzt, sodass eine größere Kommunikationsreichweite zur Übertragung der Daten vom Endgerät **1** zum Datenträger **3** ermöglicht wird. Der Datenträger **1** weist insbesondere eine Energieversorugn **305** in Form einer Battere auf. Alternativ werden die Daten vor dem Herausziehen des Datenträgers **3** aus einer Tasche des Benutzers von dem Endgerät **1** an den Datenträger **3** übertragen. Nach dem Einstecken in die Tasche wird die Bestätigung vom Datenträger **3** zurück an das Endgerät **1** gesendet.

[0052] Durch dieses alternative Verfahren wird das Hantieren mit den durchaus empfindlichen Mobiltelefonen **1**, beispielsweise das Herunterfallen oder der Diebstahl komplett vermieden. Wenn der Datenträger **1** eine Chipkarte ist, kann deren enorme Robustheit gegen Umwelteinflüsse genutzt werden. Gleichzeitig ist ein Verlust/Diebstahl der Chipkarte kein Problem, da eine erfindungsgemäße Transaktion ohne die Energiebereitstellung und die Datenübertragung mit dem Endgerät **1** nicht möglich ist. Die Karte kann demnach an einem viel unsichereren Platz, beispielsweise einer Hosen- oder Hemdtasche des Benutzers verwahrt werden, was die Handhabung für den Kunden/Benutzer deutlich erleichtert.

Bezugszeichenliste

1	mobiles Endgerät
101	Display
102	Sicherheitselement
103	NFC-Schnittstelle
2	Terminal
201	NFC-Schnittstelle
3	tragbarer Datenträger
301	Display
302	Taste
303	NFC-Schnittstelle
304	Barcode
305	Energieversorgung
4	Schutzhülle
S1, S2, S3, S4, S5	Schritte
IN	Information zur Bestätigung durch den Benutzer
BS	Bestätigungssignal
BD	Bestätigungsdaten
SIG	Signatur

K1	erste kontaktlose Kommunikationsstrecke
K2	zweite kontaktlose Kommunikationsstrecke

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102006048797 A1 [**0003**]
- DE 10316771 A1 [**0004**]

Zitierte Nicht-Patentliteratur

- ISO 14443 [**0011**]
- ISO 15693 [**0011**]
- Kapitel 3.2 in dem ”RFID-Handbuch” von Klaus Finkenzeller [**0013**]
- NFC-Standard ISO/IEC 18092 [**0014**]

Patentansprüche

1. Verfahren zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät (**1**) und einem Terminal (**2**), bei dem:
– von dem Terminal (**2**) über eine erste kontaktlose Kommunikationsstrecke (K1) eine Information (IN), welche im Rahmen der elektronischen Transaktion durch einen Benutzer zu bestätigen ist, an das Endgerät (**1**) übermittelt wird;
– die Information (IN) von dem Endgerät (**1**) über eine zweite kontaktlose Kommunikationsstrecke (K2) an einen tragbaren, am Endgerät (**1**) angebrachten Datenträger (**3**) umfassend eine Anzeigeeinheit (**301**) und eine von dem Benutzer betätigbares Eingabeeinheit (**302**) übermittelt wird;
– die Information (IN) auf der Anzeigeeinheit (**301**) des tragbaren Datenträgers (**3**) angezeigt wird, woraufhin der Benutzer die Information (IN) über die Eingabeeinheit (**302**) bestätigen kann;
– im Falle der Bestätigung der Information (IN) über die Eingabeeinheit (**302**) ein Bestätigungssignal (BS) von dem tragbaren Datenträger (**3**) über die zweite kontaktlose Kommunikationsstrecke (K2) an das Endgerät (**1**) übermittelt wird, woraufhin Bestätigungsdaten (BD) von dem Endgerät (**2**) über die erste kontaktlose Kommunikationsstrecke (K1) an das Terminal (**2**) übermittelt werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der tragbare Datenträger (**3**) an einer an dem Endgerät (**1**) angebrachten Schutzhülle (**4**) vorgesehen ist und insbesondere als Sticker ausgestaltet ist.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die erste und/oder zweite Kommunikationsstrecke (K1, K2) auf NFC-Kommunikation basiert und/oder die Eingabeeinheit (**302**) des tragbaren Datenträgers eine oder mehrere Tasten und/oder ein Gesten-Erkennungs-Mittel und/oder einen Sensor zur Erkennung von biometrischen Merkmalen umfasst.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die elektronische Transaktion eine Bezahltransaktion ist, bei der als Information (IN), welche im Rahmen der elektronischen Transaktion durch den Benutzer zu bestätigen ist, ein an das Terminal (**2**) zu zahlender Geldbetrag ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Endgerät (**2**) mittels eines Sicherheitselements (**102**) und/oder einer gesicherten Laufzeitumgebung, welche im Endgerät (**1**) vorgesehen sind, über die erste und/oder zweite kontaktlose Kommunikationsstrecke (K1, K2) kommuniziert.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass das Sicherheitselement (**102**) die über die erste kontaktlose Kommunikationsstrecke (K1) zu übermittelnden Bestätigungsdaten (BD) signiert.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass die gesicherte Laufzeitumgebung den tragbaren Datenträger und das Sicherheitselement ansteuert.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Betätigungssignal (BS) von dem tragbaren Datenträger (**3**) an das Endgerät (**2**) in der Form eines rollierenden Codes übermittelt wird, wobei sich der rollierende Code für jedes neu übermittelte Bestätigungssignal (BS) verändert und wobei der rollierende Code auf einem gemeinsamen Geheimnis zwischen tragbarem Datenträger (**3**) und Endgerät (**1**) oder zwischen tragbarem Datenträger (**3**) und einer anderen Einheit basiert.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass das gemeinsame Geheimnis über eine manuelle, durch den Benutzer durchgeführte Paarung zwischen Endgerät (**2**) und tragbarem Datenträger (**3**) festgelegt wird.

10. Verfahren nach Anspruch 8 oder 9 in Kombination mit einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass das Sicherheitselement (**102**) den übermittelten rollierenden Code basierend auf dem gemeinsamen Geheimnis verifiziert und bei erfolgreicher Verifikation das Bestätigungssignal (BS) generiert und/oder dass die gesicherte Laufzeitumgebung den übermittelten rollierenden Code basierend auf dem gemeinsamen Geheimnis verifiziert und bei erfolgreicher Verifikation das Sicherheitselement (**102**) dazu veranlasst, das Bestätigungssignal (BS) zu generieren.

11. Verfahren nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass das Endgerät (**1**) den rollierenden Code als Bestätigungsdaten (BD) oder zusammen mit den Bestätigungsdaten (BD) über die erste Kommunikationsstrecke (K1) an das Terminal (**2**) übermittelt, woraufhin das Terminal (**2**) die Verifikation des rollierenden Codes veranlasst und nur bei erfolgreicher Verifikation die elektronische Transaktion abgeschlossen wird.

12. System zur Durchführung einer elektronischen Transaktion zwischen einem mobilen Endgerät (**1**) und einem Terminal (**2**), wobei das System derart ausgestaltet ist, dass in dessen Betrieb:
– von dem Terminal (**2**) über eine erste kontaktlose Kommunikationsstrecke (K1) eine Information (IN), welche im Rahmen der elektronischen Transaktion durch einen Benutzer zu bestätigen ist, an das Endgerät (**1**) übermittelt wird

– die Information (IN) von dem Endgerät (**1**) über eine zweite kontaktlose Kommunikationsstrecke (K2) an einen tragbaren, am Endgerät (**1**) angebrachten Datenträger (**3**) umfassend ein Anzeigeeinheit (**301**) und eine von dem Benutzer betätigbare Eingabeeinheit (**302**) übermittelt wird;
– die Information (IN) auf der Anzeigeeinheit (**301**) des tragbaren Datenträgers (**3**) angezeigt wird, woraufhin der Benutzer die Information (IN) über die Eingabeeinheit (**302**) bestätigen kann;
– im Falle der Bestätigung der Information (IN) über die Eingabeeinheit (**302**) ein Bestätigungssignal (BS) von dem tragbaren Datenträger (**3**) über die zweite kontaktlose Kommunikationsstrecke (K2) an das Endgerät (**1**) übermittelt wird, woraufhin Bestätigungsdaten (BD) von dem Endgerät (**2**) über die erste kontaktlose Kommunikationsstrecke (K1) an das Terminal (**2**) übermittelt werden.

13. System nach Anspruch 12, dadurch gekennzeichnet, dass das System zur Durchführung eines Verfahrens nach einem der Ansprüche 2 bis 11 ausgestaltet ist.

14. Tragbarer Datenträger zur Verwendung in einem Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass der tragbare Datenträger (**3**) eine Anzeigeeinheit (**301**), eine kontaktlose Kommunikationsschnittstelle (**303**) und eine vom einem Benutzer betätigbare Eingabeeinheit (**302**) umfasst, welche derart ausgestaltet sind, dass der tragbare Datenträger (**3**) im Betrieb eine Information, welche von dem Benutzer zu bestätigen ist, über die kontaktlose Kommunikationsschnittstelle (**303**) von dem Endgerät (**1**) empfängt und anschließend über die Anzeigeeinheit (**301**) anzeigt, wobei der tragbare Datenträger (**3**) nach einer anschließenden Bestätigung der Information über die Eingabeeinheit (**302**) ein Bestätigungssignal (BS) über die kontaktlose Kommunikationsschnittstelle (**303**) zum Endgerät (**1**) aussendet.

15. Tragbarer Datenträger nach Anspruch 14, dadurch gekennzeichnet, dass der tragbare Datenträger an einer Schutzhülle (**4**) angebracht ist, wobei die Schutzhülle (**4**) an das Endgerät (**1**) angebracht werden kann.

16. Tragbarer Datenträger nach Anspruch 14, dadurch gekennzeichnet, dass der tragbare Datenträger (**3**) in Kommunikationsreichweite mit dem Mobiltelefon (**3**) angeordnet ist und anstelle des Endgeräts (**1**) zur Bestätigung der Transaktion verwendet wird und wobei das Mobiltelefon (**1**) ohne Benutzerinteraktion die Transaktion durchführt.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

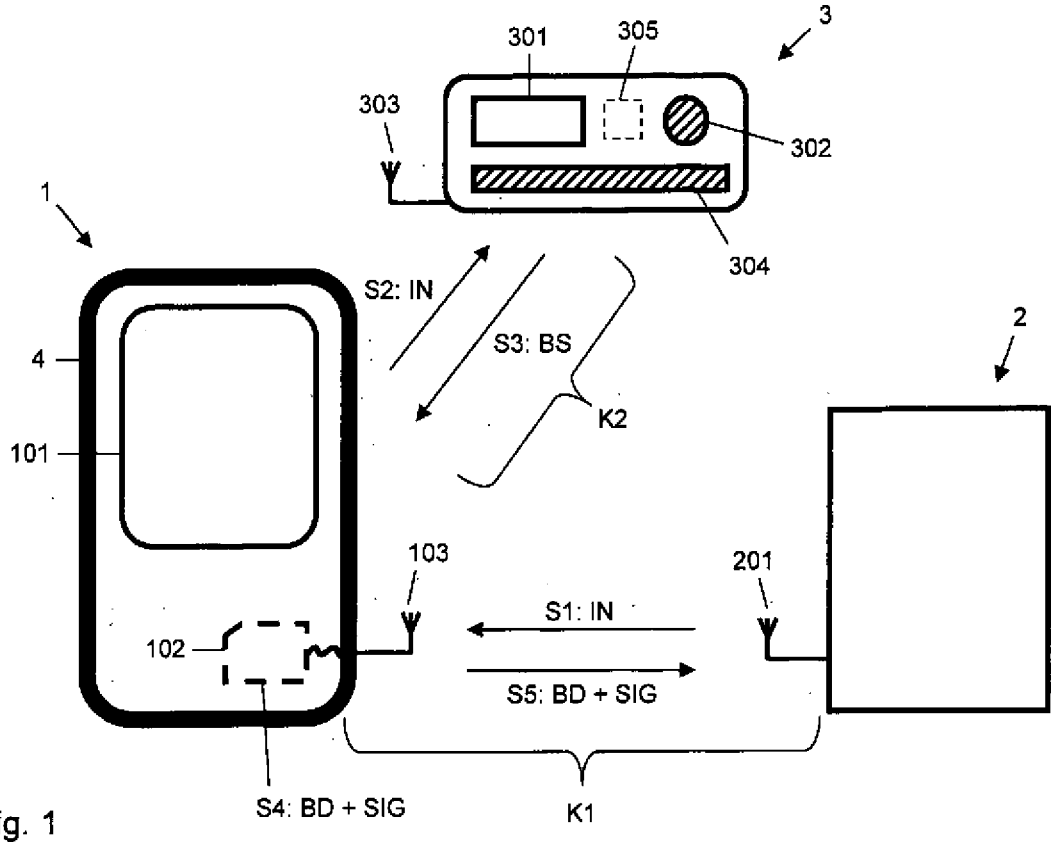


Fig. 1