



(10) **DE 10 2012 108 645 A1** 2014.03.20

(12)

Offenlegungsschrift

(21) Aktenzeichen: **10 2012 108 645.1**

(22) Anmeldetag: **14.09.2012**

(43) Offenlegungstag: **20.03.2014**

(51) Int Cl.: **H04L 9/32 (2006.01)**

(71) Anmelder:

**Papagrigoriou, Paschalis, Dr., 90482, Nürnberg,
DE**

(72) Erfinder:

gleich Anmelder

(74) Vertreter:

**2K Patentanwälte Blasberg Kewitz & Reichel,
Partnerschaft, 60325, Frankfurt, DE**

(56) Ermittelter Stand der Technik:

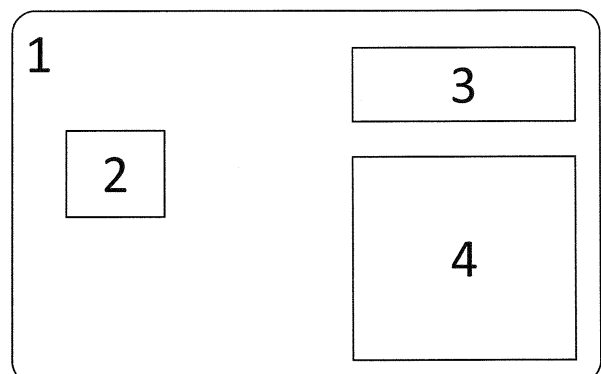
DE	10 2008 007 367	B4
US	2012 / 0 154 290	A1
EP	1 855 231	A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Vorrichtung zur Absicherung elektronischer Transaktionen mit sicheren elektronischen Signaturen**

(57) Zusammenfassung: Chipkarte für eine elektronische Transaktion umfassend eine Anzeige, eine Tastatur, eine Netzwerkschnittstelle, eine Verarbeitungseinheit, einen Micro-Controller und einen Speicherbereich für Signaturinformationen und/oder Schlüsselmaterial, gekennzeichnet durch eine Einrichtung, die es der Chipkarte erlaubt, sich mit einem Wirtssystem über die Netzwerkschnittstelle zu verbinden, um sich gegenüber diesem Wirtssystem als integriertes Kartenlesegerät mit eingeschobener Chipkarte darzustellen, wobei die Transaktionsdaten zu der Chipkarte über die Netzwerkschnittstelle vom Wirtssystem empfangen werden, um auf dem Display dargestellt zu werden, um durch eine Tasteingabe auf der Tastatur diese Transaktionsdaten bestätigen zu können, um diese Transaktionsdaten mit der Signatur zu versehen und um diese dann an den PC zu senden.



Beschreibung

[0001] Die Erfindung betrifft eine Vorrichtung zur signaturgestützten Absicherung elektronischer Transaktionen, die insbesondere von bankfachlichen Anwendungen auf persönlichen mobilen Endgeräten oder sonstigen Geld- oder Bezahlsystemen ausgeführt werden und die Integrität der digital signierten Informationen sowie die Identifikation des Urhebers dieser Informationen zweifelsfrei voraussetzen.

Gebiet der Erfindung:

[0002] Elektronische Signaturen kommen immer dann zum Einsatz, wenn es darum geht, den Ersteller oder Sender eines elektronischen Dokuments oder Datensatzes ohne Zweifel zu identifizieren und die Integrität der signierten elektronischen Informationen zu gewährleisten. Ein Beispiel für einen sicherheitskritischen Bereich, der im alltäglichen Leben zunehmend an Bedeutung gewinnt, sind bankfachliche Anwendungen wie Home-Banking oder Mobile-Banking. Es ist unmittelbar einsichtig, was passieren könnte, wenn sich ein böswilliger Dritter als Inhaber eines Bankkontos ausgeben könnte, das ihm nicht gehört.

[0003] Mit dem Einsatz mobiler Systeme sowohl im privaten als auch im betrieblichen Bereich, wie auch im Bereich des Gesundheitswesens oder der öffentlichen Verwaltung vervielfältigen sich die Gefahren, die sich daraus ergeben, wenn die Integrität der übermittelten Informationen nicht garantiert werden kann, oder wenn die Identität des Erstellers nicht zweifelsfrei festgestellt werden kann.

[0004] Ein wichtiges Kriterium bei der Auswahl eines elektronischen Sicherheitsverfahrens ist neben den Kosten auch die Benutzerfreundlichkeit, da es besonders im privaten Bereich sehr schwierig sein dürfte, Akzeptanz für ein zwar sicheres aber aufwendiges Sicherheitsverfahren zu erwarten, sei es aus mangelndem technischen Verständnis, oder sei es wegen der Umständlichkeit des Verfahrens. Im Zusammenhang mit mobilen Endgeräten wird die Akzeptanz ohne Zweifel auch davon abhängen, ob zusätzliche Geräte (z. B. Kartenleser/Chipkartenlesegerät) mit oder ohne Verkabelung nötig sind. Bereits vorhandene und auf dem Markt befindliche Lösungen, die weiter unten unter „Stand der Technik“ aufgeführt und beschrieben sind, sind deshalb nicht nur unter sicherheitsrelevanten Aspekten zu beurteilen, sondern auch was ihre Benutzerfreundlichkeit betrifft.

[0005] Die Anpassung der Sicherheitslösungen konnte bisher mit der rasanten Entwicklung im Bereich der mobilen Endgeräte (Smartphones, Tablets, etc.) nicht in angemessener Weise Schritt halten. So haben einige dieser Verfahren, die in Kombination mit mobilen Endgeräten angewendet werden könnten, in der Praxis für den Benutzer mehr oder weniger

vierende Nachteile hinsichtlich der Handhabbarkeit oder Bedienbarkeit, was sie für einen weitgestreuten Einsatz ungeeignet macht. Im Gegensatz dazu erfüllt die erfindungsgemäße Lösung die höchsten Sicherheitsanforderungen und kann dabei dennoch optimal und benutzerfreundlich mit mobilen Endgeräten verwendet werden.

Stand der Technik

[0006] Die relevanten Verfahren, anhand derer der Stand der Technik im Folgenden beschrieben wird, kommen aus den Bereichen der Sicherheit im Zahlungsverkehr, der Online-Banking-Sicherheit und der Chiptechnologie. Allein die Anzahl der Sicherheitsverfahren im Internet, welche in den letzten zehn Jahren entwickelt wurden, zeigt, wie wichtig es ist, die Sicherheit und Zuverlässigkeit der Kommunikation im Internet zu gewährleisten. Verfahren, welche sich zur Sicherung einer Transaktion auf die Verwendung von TAN-Listen stützen, gelten mittlerweile nicht mehr als sicher und wurden von anderen Verfahren abgelöst.

[0007] Die Chipkarte steht nunmehr im Mittelpunkt aller ernst zu nehmenden Sicherheitsverfahren. Sie gilt technisch als sicherer Träger geheimer Schlüsselinformationen, sie ist immer beim Kunden (Besitzkomponente) und stellt zudem mittlerweile für jeden Nutzer ein wertvolles und sicheres Medium dar, auf welches er besonders achtet und dessen etwaigen Verlust er umgehend dem Herausgeber (z. B. seiner Bank) meldet. Somit kann beispielsweise ein Kreditinstitut immer darauf vertrauen, dass die Chipkarte bei seinem Kunden ist, und dass dieser tatsächlich die Person ist, die die Transaktionen ausführt, denn bei Verlust der Chipkarte würde dieser sofort gemeldet werden. Synonym zur Chipkarte wird auch der Begriff Smartcard verwendet. Letzterer wird in dieser Schrift ebenfalls benutzt, insbesondere wenn es um den Crypto-Micro-Controller einer Chipkarte geht, den eigentlichen Baustein für kryptographische Operationen.

[0008] Noch heute wird häufig für die Nutzung einer TAN (Transaktionsnummer) in einer Transaktion ein sogenannter TAN-Generator verwendet. Dafür hat der Nutzer ein externes Gerät, an das keine besonderen Anforderungen hinsichtlich Sicherheit gestellt werden müssen, sowie seine persönliche Chipkarte.

[0009] Mehr Sicherheit sollte in der zweiten Hälfte des letzten Jahrzehntes das sogenannte indizierte TAN-Verfahren (iTAN-Verfahren) bringen. Hierbei handelt es sich um eine Bestätigung der Rückfrage eines Kreditinstitutes, bei der der Bankkunde eine bestimmte TAN aus einer Liste auszuwählen hat. Somit spricht man von einem „Zwei-Schritt-Verfahren“, bei dem nicht die Transaktion selbst, sondern die Rückfrage des Kreditinstitutes mit einer explizit angefor-

der TAN bestätigt wird. Auch bei diesem Verfahren haben sich große Schwächen gezeigt, denn weder der Benutzer kann feststellen, an wen er die Daten übergibt, noch das Kreditinstitut, ob die Daten tatsächlich von seinem Kunden oder einem unbekanntem Angreifer kommen.

[0010] Schnell wurden die Möglichkeiten des „Zwei-Schritt-Verfahrens“ erkannt und weitere Sicherheitsverfahren darauf aufbauend entwickelt, die für den „zweiten Schritt“ einen völlig anderen Kommunikationskanal verwenden. Im Rahmen des weiterentwickelten Zwei-Schritt-Verfahrens werden Daten, die von einem Server stammen, außerhalb des stationären oder mobilen Endgeräts (z. B. PC oder Smartphone), mit dem Transaktionen abgewickelt werden, dem Benutzer auf dem Display eines externen Chipkartenlesers angezeigt. Die Übertragung dieser Daten erfolgt an der Bildschirmoberfläche des PCs oder Smartphones über optische Detektoren des externen Chipkartenlesers, welcher einen flackernden Code aufnimmt (künftig auch akustisch möglich). Nachdem der Nutzer eine Reihe von Daten (Kontonummer, Betrag etc.) einzeln bestätigt hat, wird eine TAN mit Hilfe der Chipkarte des Kunden auf diesem Chipkartenleser und somit ebenfalls außerhalb des PCs oder Smartphones berechnet. Die mit Hilfe der Chipkarte des Benutzers auf diesem Gerät generierte und auf seinem externen Display angezeigte TAN muss dann explizit vom Benutzer auf die Anwendungsumgebung des Bankings (web- oder clientbasiert) übertragen werden. Der Vorgang ist als chipTAN-Verfahren bekannt.

[0011] Zu den Nachteilen des Verfahrens zählen die manuelle Übertragung der Transaktionsnummer (TAN) durch den Nutzer, die unpraktische Verwendung eines Zusatzgerätes durch den Nutzer, die unkomfortable Nutzung in Kombination mit Smartphones und die reduzierte Informationsanzeige und Informationsbestätigung bei Sammelüberweisungen.

[0012] Parallel zum chipTAN-Verfahren gehört auch das mTAN-Verfahren (auch SMS-TAN-Verfahren genannt) zum Stand der Technik. Auch hier handelt es sich um ein Zwei-Schritt-Verfahren. Der Nutzer hinterlegt bei seiner Bank vorab seine Handy-Nummer. Während einer Banktransaktion wird dem Nutzer eine SMS zugestellt, welche eine gültige TAN enthält. Der Nutzer muss diese dann im Rahmen seiner aktuellen Session mit der Bank übertragen. Angriffe über Handy-Trojaner zeigen, dass auch dieses Verfahren nicht sicher ist. Die Verbreitung solcher Trojaner steht uns noch bevor.

[0013] Für eine Erhöhung der Sicherheit sorgt auch das Verfahren mit der Patentnummer DE 10 2008 007 367 B4 2010.09.30. Basierend auf dem Zwei-Schritt-Verfahren werden Daten, die von einem Server stammen, unabhängig von dem PC,

auf dem die Transaktion abgewickelt wird, sicher auf einem Display angezeigt und durch den Benutzer bestätigt. Eine weitere Ausführungsform des Verfahrens besteht darin, dass ebenfalls eine TAN in sicherer Umgebung mit der Chipkarte erzeugt und angezeigt wird, ähnlich wie beim ChipTAN- oder mTAN-Verfahren.

[0014] Im Rahmen der einsetzbaren Verfahren im bankfachlichen Bereich sei hier auch die Secoder-Spezifikation [1] erwähnt, welche im Gegensatz zu den bisher vorgestellten Verfahren auch Implementierungsmöglichkeiten auf Basis des sogenannten „Ein-Schritt-Verfahrens“ bietet. In der Secoder-Spezifikation wird ein multifunktionaler IC card reader (Chipkartenleser) mit Display und Tastatur definiert. Seine Funktionalität ist durch eine Menge von Befehlen beschrieben, die innerhalb dieses Chipkartenlesers auf seiner eigenen CPU ausführbar sind. Besonders wichtig am Secoder ist einerseits die Verwendung einer für den Benutzer vertrauenswürdigen Ein- und Ausgabeeinheit, welche die Authentizität und Integrität der Daten garantiert, und andererseits die Nutzung des „Ein-Schritt-Verfahrens“, bei dem die Auftrags- bzw. Transaktionsdaten zuerst lokal durch den Benutzer im Banking-Client eingegeben werden, und, bevor diese dann in einem Schritt an den Bankserver übermittelt werden, auf einem Secoder-Chipkartenleser extern bestätigt und signiert werden.

[0015] Chipkartenleser sind Geräte, die Chipkarten ansteuern. Dabei werden nicht nur Daten gelesen, sondern auch geschrieben, oder Applikationen auf der Chipkarte angesteuert; daher spricht man auch von einem Chipkartenterminal [4]. Es gibt vier Sicherheitsklassen für Chipkartenleser, die bei der DK (Deutsche Kreditwirtschaft) spezifiziert wurden. Sicherheitsklasse 1 und 2 sind für ein ernsthaftes Sicherheitsniveau uninteressant. Chipkartenleser der Sicherheitsklasse 3 besitzen ein Display und eine Tastatur sowie Zusatzfunktionen, mit denen das Bezahlen mit der Geldkarte im Internet möglich ist. Chipkartenleser der Sicherheitsklasse 4 verfügen zusätzlich zu den Merkmalen der Klasse 3 auch über eine eigene manipulationssichere Identität. Dies wird mit einer zusätzlichen Chipkarte möglich. Wird ein Chipkartenleser mit einem PC über USB oder eine serielle Schnittstelle verbunden, so wird dieser über proprietäre oder standardisierte Software-Schnittstellen erkannt und kann mit einer Anwendung kommunizieren. Als Standard für solche Schnittstellen gilt heute PC/SC [5], wofür es sowohl Windows- als auch Linux-Implementierungen gibt. Die Secoder-Spezifikation [1] geht über die Merkmale der Sicherheitsklasse 3 hinaus. Ein nach dieser Spezifikation gebauter Chipkartenleser enthält eine Firewall, welche vor möglichen Manipulationen schützt, während das Gerät mit dem Nutzer über Display und Tastatur interagiert (z. B. PIN-Eingabe) oder Daten für den Signaturvorgang mit einer Chipkarte verarbeitet.

[0016] Des Weiteren sind beim Smartphone mit einem Blackberry- oder Android-OS Lösungen mit Chipkarten in speziellen Formfaktoren (z. B. microSD mit integrierter Chipkarte) denkbar. Da es jedoch in so einem Fall keine unabhängige sichere Ein- und Ausgabemöglichkeit gibt, können erhöhte Sicherheitsanforderungen kaum erfüllt werden, so dass sich eine nähere Betrachtung an dieser Stelle erübrigt.

[0017] Es wird erwartet, dass nahezu alle künftigen Smartphones mit gewissen Einschränkungen Bluetooth- [2] und NFC-fähig [3] sind. Es gibt Geräte, wie z. B. das iPhone, die Stand heute keine integrierte NFC-Schnittstelle aufweisen. In solchen Fällen kann für die Kommunikation mit einer Chipkarte über einen Chipkartenleser ein dafür verfügbares externes Zubehör verwendet werden oder ein anderes Kommunikationsprotokoll eingesetzt werden. Eine Möglichkeit für letzteres bietet der Bluetooth-Standard.

[0018] Diese drahtlosen Schnittstellen schaffen die Voraussetzungen, um z. B. auch Chipkartenleser kabellos mit einem PC oder Smartphone verbinden zu können. Erste solche Chipkartenleser sind bereits auf dem Markt. Sollte heute ein Chipkartenleser nach dem Secoder-Standard [1] in Zusammenspiel mit einem mobilen Gerät verwendet werden, so müsste Stand heute Zusatzverkabelung vorgenommen werden, ggf. Umkonfigurierung des Smartphones und Installation von Zusatzsoftware erfolgen, falls dies überhaupt auf einem marktüblichen Mobilegerät machbar ist. Alternativ müssten solche Chipkartenleser auf kabellose Kommunikation umgestellt werden, was zumindest heute bereits technisch machbar wäre. Beispielsweise ist dies bei einigen wenigen marktüblichen Chipkartenlesern über Bluetooth realisiert.

[0019] Die Integration eines Displays und einer in der Regel numerischen Tastatur direkt auf einer nach ISO 7810, ID-1 physikalisch dimensionierten Chipkarte gehört ebenfalls zum Stand der Technik. Solche Chipkarten werden heute lediglich im Authentifizierungsbereich für die Verfahren „one-time-password“ bzw. „challenge-response“ eingesetzt.

NFC Technologie

[0020] http://de.wikipedia.org/wiki/Near_Field_Communication
(Wikipedia): Near Field Communication (zu Deutsch „Nahfeld-Kommunikation“, Abkürzung NFC) ist ein internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten über kurze Strecken von bis zu 4 cm. Die Übertragung erfolgt entweder verbindungslos (mit passiven HF-RFID-Tags nach ISO 14443 oder ISO 15693) oder verbindungsbehaftet (zwischen gleichwertigen aktiven Transmittern). Bisher kommt diese Technologie vor allem in Lösungen

für Micropayment – bargeldlose Zahlungen kleiner Beträge – zum Einsatz. In Deutschland wird die Technik beispielsweise von den Sparkassen zur Zahlung von Summen bis zu 20 Euro angeboten und von der Deutschen Bahn in ihrem Touch&Travel-System eingesetzt. Es wird erwartet, dass nahezu alle künftigen Smartphones NFC-fähig sind.

BT (heute gültige Version 4.0)

[0021] http://de.wikipedia.org/wiki/Bluetooth#Aktueller_Standard:_Bluetooth_4.0
(Wikipedia): Die Spezifikation 4.0 wurde am 17. Dezember 2009 verabschiedet. Mit diesem Standard wurde erstmals der Protokollstapel Low Energy verfügbar [1] und neue Profile zu Low Energy kamen seitdem laufend hinzu. Entsprechende Chips waren in kleinen Stückzahlen bereits ab dem 4. Quartal 2010 verfügbar, weitere Hinweise ließen mit Bluetooth 4.0 ausgestattete Mobiltelefone ab dem 1. Quartal 2011 erwarten. Im Juni 2011 schließlich waren Bluetooth-4.0-konforme Chips bereits von Athoros, CSR, Nordic Semiconductor, [2] Texas Instruments sowie Toshiba verfügbar.

[0022] Im einzelnen betrifft die Erfindung eine Chipkarte für eine elektronische Transaktion, umfassend eine Anzeige, eine Tastatur, eine Netzwerkschnittstelle, eine Verarbeitungseinheit, einen Crypto-Micro-Controller und einen Speicherbereich für Signaturinformationen und/oder Schlüsselmaterial, gekennzeichnet durch eine Einrichtung, die es der Chipkarte erlaubt, sich mit einem Wirtssystem über die Netzwerkschnittstelle zu verbinden, um sich gegenüber diesem Wirtssystem als integriertes Kartenlesegerät mit eingeschobener Chipkarte darzustellen, wobei die Transaktionsdaten zu der Chipkarte über die Netzwerkschnittstelle vom Wirtssystem empfangen werden, um auf dem Display dargestellt zu werden, um durch eine Tastatureingabe auf der Tastatur diese Transaktionsdaten bestätigen zu können, um diese Transaktionsdaten mit der Signatur zu versehen, und um diese dann an den Wirtssystem zu senden. In einer vorteilhaften Ausführungsform wird die Chipkarte über ihre Netzwerkschnittstelle mit dem Wirtssystem verbunden und teilt diesem abhängig von der Kommunikationsart mit, welches Gerät sie ist. Erfolgt diese Kommunikationsverbindung über Bluetooth, zeigt der Prozessor der Chipkarte ein standardmäßiges Chipkartenlesegerät mit eingeschobener Chipkarte an, die dem Wirtssystem über die Netzwerkschnittstelle zur Verfügung stehen. Hierbei erkennt der Gerätetreiber des Hostgerätes ein zulässiges Chipkartenlesegerät und initialisiert entsprechend die Verbindung. Erfolgt die Kommunikation über NFC, so kommt die Verbindung in einem der bei NFC geltenden und spezifizierten Modi zustande. Handelt es sich bei der NFC-Schnittstelle des Wirtsystems um einen NFC-Chipkartenleser, so baut der NFC-Baustein der Chipkarte mit dem NFC-Chip-

kartenleser des Wirtsystems die Verbindung auf und zeigt dabei eine Chipkarte an (NFC-Modus „Cord Emulation“). Handelt es sich bei der NFC-Schnittstelle des Wirtsystems um eine NFC-Chipkarte, so baut der NFC-Baustein der Chipkarte mit der NFC-Chipkarte des Wirtsystems die Verbindung auf und zeigt dabei einen NFC-Chipkartenleser an (NFC-Modus „Read/Write“). Ferner gibt es noch den Modus peer-to-peer, bei dem beide Seiten (Netzwerkschnittstelle des Wirtsystems und NFC-Schnittstelle der Chipkarte) als gleichberechtigte Kommunikationsinstanzen auftreten, und wo die eine sendet und die andere empfängt. In allen drei NFC-Kommunikationsverbindungen handelt es sich um eine reine Übertragungsverbindung für Transaktionsdaten, welche im Display der Einrichtung manipulationssicher angezeigt werden, über die Tastatur der Einrichtung manipulationssicher bestätigt werden können, und mit den Signaturinformationen im Crypto-Micro-Controller signiert werden. Unabhängig davon, welche Art von Chipkartenleser im Wirtsystem nach dem Aufbau der Netzwerkverbindung initialisiert und bekannt wird, steht für alle sicherheitsrelevanten Anwendungen im Wirtsystem auch die Information bereit, dass eine Chipkarte über einen zulässigen Chipkartenleser mit Anzeige und Tastatur erreicht werden kann. Im Fall Bluetooth geschieht dies über die installierten Chipkartenleser-Treiber für die Einrichtung. Im Falle NFC-Card-Emulation erfolgt dies über den NFC-Chipkartenlesertreiber im Wirtsystem, indem die Anwendung des Wirtsystems zuvor die Befehle für den Chipkartenleser der Einrichtung als Daten innerhalb von Befehlen für die Smartcard der Einrichtung bereitstellt, welche wiederum von der NFC-Cord-Emulation der Einrichtung übergeben und dort ordnungsgemäß ausgeführt werden. In ähnlicher Weise werden Befehle für den Chipkartenleser der Einrichtung auch dann verpackt, wenn im Falle Bluetooth die vorinstallierten oder allgemeinen Chipkartenlesertreiber im Wirtsystem nicht in der Lage sind, die Chipkartenleserfunktionen der Einrichtung zu erkennen. Bei den anderen Arten der Kommunikationsverbindung handelt es sich um Spezialfälle, die weiter unten beschrieben werden. Das manipulationssichere Anzeigen, die sichere Verwendung der Tastatur, und der Signaturvorgang alles ohne externes Eingreifen in der Einrichtung kann ähnlich der Firewall-Technik des Secoder-Chipkartenlesers [1] erfolgen.

[0023] In einer weiteren Ausführungsform ist die Chipkarte durch eine physikalische Dimension nach einem Chipkartenstandard, insbesondere ISO 7810, vorzugsweise ID-1 definiert. Es handelt sich dabei vorzugsweise um den Formfaktor, welcher beispielsweise von Kreditinstituten bei speziellen Plastikkarten mit eingebautem integriertem Schaltkreis (Chip) verwendet wird.

[0024] In einer weiteren Ausführungsform ist die Chipkarte durch physikalische Kontakte und Schaltungen gekennzeichnet, die einen Betrieb in Standard Kartenlesegeräten erlaubt, um eine Transaktion durchzuführen. Durch diese Ausbildung kann die Karte auch verwendet werden, wenn das Hostsystem keine Verbindung über die Netzwerkschnittstelle der Einrichtung zulässt. Die physikalischen Kontakte sind die typischen Goldkontakte des Chipkartenmoduls oder Magnetstreifen, so dass die Chipkarte in bisher üblichen Kartenlesern oder Terminals verwendet werden kann.

[0025] In einer weiteren Ausführungsform ist die Chipkarte durch einen sicheren Speicherbereich, der vorzugsweise durch einen Crypto-Micro-Controller verwaltet wird oder in einem solchen integriert ist, gekennzeichnet. Micro-Controller für kryptographische Operationen werden bereits so hergestellt, dass sie sichere Speicherbausteine verwenden und in der Regel integrieren sowie deren Inhalte verwalten und als sehr vertrauenswürdig gelten. Sie führen in ihrer spezifischen Betriebssystemumgebung Anwendungen und Crypto-Operationen aus.

[0026] In einer weiteren Ausführungsform sind im Speicherbereich Signaturinformationen und Schlüsselmaterial insbesondere Signaturschlüssel abgelegt, um die Transaktionsdaten zu signieren, die Identität des Nutzers der Chipkarte zu prüfen oder die Identität des Chip-Kartenlesers gegenüber einer Anwendung des Wirtsystems auszuweisen. Das Schlüssel- und Signaturmaterial, welches üblicherweise bei der Herausgabe der Chipkarte oder nachträglich im Speicherbereich abgelegt wird, wird vom Crypto-Micro-Controller verwendet, um die angezeigten und über die Tastatur bestätigten Transaktionsdaten zu signieren. Mit der Möglichkeit der sicheren Eingabe einer persönlichen Identifikationsnummer über die Tastatur der Einrichtung und ihrer Verifikation vom Crypto-Micro-Controller, kann der Nutzer der Chipkarte identifiziert werden. Schließlich ist es auch möglich, die Identität des Chipkartenlesers oder einzelner Bausteine zu prüfen, wenn eine Anwendung dies erfordert.

[0027] In einer weiteren Ausführungsform ist die Chipkarte durch eine Tastatur, insbesondere Folientastatur oder berührungsempfindlichem Bildschirm, die so ausgebildet ist, dass die physikalischen Dimensionen nach einem Chipkarten-Standard eingehalten werden, gekennzeichnet durch die Anzahl und den Mix von alphanumerischen oder sonstigen Tastenzeichen oder Größen, die für das jeweilige Anwendungsgebiet vorgeschrieben werden. Z. B. beim sicheren online Banking mit einem Secoder-Chipkartenleser gemäß der Secoder-Spezifikation.

[0028] In einer weiteren Ausführungsform ist die Chipkarte durch einen integrierten Flachbildschirm,

der so ausgebildet ist, dass die physikalischen Dimensionen nach einem Chipkarten-Standard eingehalten werden, gekennzeichnet durch die Displaygrößen, die für das jeweilige Anwendungsgebiet vorgeschrieben werden. Z. B. beim sicheren online Banking mit einem Secoder-Chipkartenleser gemäß der Secoder-Spezifikation.

[0029] In einer weiteren Ausführungsform ist das Wirtssystem ein Kassensystem oder ein PC-System, Smartphone, Geldautomat oder Bezahlterminal. In all diesen Computersystemen ist es erforderlich oder auch zwingend notwendig, sicherheitsrelevante Anwendungen laufen zu lassen, die für ein hohes Sicherheitsniveau eine Chipkarte über einen angeschlossenen Chipkartenleser voraussetzen.

[0030] In einer weiteren Ausführungsform ist die Chipkarte ausgebildet, um in Abhängigkeit der Netzwerkverbindung sich gegenüber dem Wirtssystem als Chip-Kartenlesegerät oder während des Etablierens der Kommunikationsverbindung mit dem Wirtssystem sich als eine Chipkarte darzustellen, um sich jedoch einer Anwendung des Wirtsystems als Chipkartenleser mit eingeschobener Chipkarte darzustellen. Es ist über die Tastatur und das Display der Einrichtung möglich, festzulegen oder zu konfigurieren, welche Kommunikationsverbindungen über die Netzwerkschnittstelle der Einrichtung erlaubt oder möglich sein sollen. Wie weiter oben erläutert, kann immer in der jeweiligen Kommunikationsverbindung das Ziel der Einrichtung erfüllt werden, die Chipkartenfunktionen mit den integrierten vertrauenswürdigen Chipkartenleserfunktionen zu verwenden.

[0031] In einer weiteren Ausführungsform werden dem Nutzer die von ihm auf dem Bildschirm des Wirtsystems eingegebenen Daten zur Sicherstellung der Authentizität erneut anzeigt, und diese sind vom Nutzer dort explizit bestätigbar. Während der Vorbereitung einer Transaktion mit einer Anwendung auf dem Wirtssystem, wird der Nutzer aufgefordert, Daten einzugeben. Um sicherzustellen, dass bei der weiteren bzw. späteren Verwendung dieser Daten, diese nicht manipuliert worden sind, werden sie an die Chipkarte gesendet, um sie dort zu signieren. Vor der Signatur werden diese dem Benutzer noch einmal angezeigt. Sowohl die Anzeige als auch die Tastatur der Einrichtung gelten als vertrauenswürdig, weil die Einrichtung hierfür bekannte Verfahren nutzt, wie beispielsweise eine Firewall. Ähnliche Mechanismen werden heute beispielsweise auch bei Verwendung eines Secoder-Chipkartenlesers mit eingeschobener Chipkarte verwendet.

[0032] In einer weiteren Ausführungsform werden von der Chipkarte die Daten mit Schlüsselmaterial signiert, so dass die Daten nur von einem bestimmten Empfänger dieser signierten Daten sinnvoll und gültig verwendbar sind. Dies ermöglichen die asym-

metrischen oder symmetrischen Kryptosysteme, welche bei der Konzeption und Verteilung des Schlüsselmaterials dafür sorgen, dass nur diejenigen Stellen (Personen oder Maschinen), die behandelten Daten richtig und sinnvoll verwenden können, welche über die richtigen Schlüsselkomponenten verfügen. In einer weiteren Ausführungsform laufen auf der Verarbeitungseinheit weitere Anwendungen, umfassend einen funktionalen Teil eines oder mehrerer Anwendungsbereiche, wie Home-, Mobile- oder Online Banking, aber auch funktionale Blöcke der Anwendungsbereiche – VPN-Client, Email-Client, elektronische Pässe und Ausweise, oder auch Zeiterfassung und Türöffnung, welche vom Nutzer erwarten, dass er seine Chipkarte für Authentifizierungszwecke oder elektronische Signaturen einsetzt. Auf der Verarbeitungseinheit der Einrichtung können mehrere Anwendungen laufen, die vom jeweiligen Anwendungsgebiet bestimmt sind. Das Anwendungsgebiet und die Anwendung auf der Verarbeitungseinheit bestimmen die jeweiligen Informationen, welche während der Transaktion dem Nutzer angezeigt werden.

[0033] In einer weiteren Ausführungsform enthält die Chipkarte mehrere Crypto-Micro-Controller und/oder es werden mehrere Typen von Chip-Kartenlesegeräten emuliert. Dies ist nötig, um ein möglichst breites Spektrum an Anwendungen bedienen zu können. Möglich wird eine solche Ausführungsform durch die vorgeschaltete Verarbeitungseinheit, da sie abhängig von der Anwendung und dem Wirtssystem steuern kann, welcher Crypto-Micro-Controller benötigt wird und/oder welche Art Chipkartenlesertyp simuliert werden soll.

[0034] Ferner wird vorzugsweise eine Energiequelle zur Stromversorgung bereitgestellt, wobei diese über NFC-Induktion aufladbar, oder auch ein Solarmodul sein kann. Unterschiedliche Anwendungen auf der Chipkarte und unterschiedliche kryptographische Operationen oder Display-Anzeigen haben unterschiedlichen Strombedarf. Es besteht zwar die Möglichkeit, über die NFC-Induktion Strom zu beziehen, dieser wird jedoch nicht in allen Fällen ausreichend sein. Um die Einrichtung in Hinblick auf den Strombedarf möglichst lange verwenden zu können, sollte die Energiequelle aufladbar sein. Dies sowohl über die NFC-Induktion als auch als Solarmodul.

Beschreibung der Figuren

[0035] Es werden folgende Figuren präsentiert:

[0036] Fig. 1. mit der Nutzersicht der erfindungsgemäßen Vorrichtung

[0037] Fig. 2. mit der technischen Anordnung der erfindungsgemäßen Vorrichtung

[0038] Fig. 3a. mit der Ausführungsform: die Netzwerkschnittstelle ist auf NFC-Basis realisiert.

[0039] Fig. 3b. mit der Ausführungsform: die Netzwerkschnittstelle ist auf NFC-Basis realisiert. Die Vorrichtung enthält keine Energiequelle.

[0040] Fig. 3c. mit der Ausführungsform: die Netzwerkschnittstelle ist auf Bluetooth-Basis realisiert.

[0041] Fig. 3d. mit der Ausführungsform: es ist sowohl eine Netzwerkschnittstelle auf Bluetooth-Basis als auch eine auf NFC-Basis vorhanden.

[0042] Fig. 4. mit einer Kurzbeschreibung des erfindungsgemäßen Verfahrens

Beschreibung der Erfindung
und der Ausführungsformen

[0043] Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren.

[0044] Die Hauptaufgabe der Vorrichtung der vorliegenden Erfindung ist, mit einer einzigen Konstruktion aus vereinigten Sicherheitsmerkmalen und Sicherheitskomponenten die Ausführung von Sicherheitsfunktionen einer marktüblichen Chipkarte und die eines marktüblichen Chipkartenlesers [5] bei gleichzeitiger Erfüllung von strengen Sicherheitsanforderungen hinsichtlich der vertrauenswürdigen Anzeige und Eingabe oder Bestätigung von Transaktionsdaten, folgend beispielsweise dem Secoder-Prinzip der Deutschen Kreditwirtschaft [1], zu ermöglichen. Selbstverständlich kann die Vorrichtung ihre Funktionen auch einzeln oder teilweise ausführen. So kann die erfindungsgemäße Vorrichtung auch nur als Chipkarte arbeiten oder in anderen Fällen auch als Chipkarte mit integriertem Chipkartenleser, der nicht notwendigerweise die hohen Sicherheitsanforderungen hinsichtlich einer vertrauenswürdigen Ein- und Ausgabereinheit zu erfüllen braucht oder diese nur teilweise benötigt, wie beispielsweise nur für eine sichere PIN-Eingabe.

[0045] Ziel dieser Erfindung ist, den sicherheitskritischen Anwendungen in Terminalumgebungen, wie den PC, den Kassen- und Geldautomaten oder anderen Bezahlterminals, aber vor allem in der stark wachsenden Welt der Smartphones und Tablets-PC, mit nur einem einzigen Zusatzgerät in Form einer ISO-ID1-Chipkarte (ähnlich der heutigen EC-Karte) das hohe Sicherheitsniveau einer Chipkarte unter Verwendung eines integrierten Chipkartenlesegerätes mit vertrauenswürdiger Anzeige- und Tastatureinheit für alle wichtigen Sicherheitsoperationen bereitzustellen.

[0046] Bei der erfindungsgemäßen Vorrichtung handelt es sich um eine Chipkarte mit den physikalischen

Dimensionen ID-1 nach ISO 7810, welche nicht nur die kryptographischen Funktionen des Crypto-Micro-Controllers z. B. für digitale Signaturen bereitstellt, sondern zusätzlich die Funktionen eines Chipkartenlesers bietet. Zudem enthält sie eine vertrauenswürdige Anzeige- und Tastatureinheit, und ermöglicht aufgrund der ebenfalls integrierten NFC- und/oder Bluetooth-Funktionalität eine kabellose Kommunikation mit modernen mobilen Endgeräten wie Smartphones oder Tablets, aber auch mit PCs oder Bezahlterminals. Damit erfüllt die Vorrichtung alle Voraussetzungen für eine gute Akzeptanz durch die potentiellen Nutzer, da sie Sicherheit nach dem letzten Stand der Technik (Chipkarte und mindestens Chipkartenleser der Sicherheitsklasse **3**) mit komfortabler Bedienbarkeit vereint, optimal mit modernen mobilen Endgeräten kommuniziert, dabei jedoch nicht auf Rückwärtskompatibilität verzichtet (z. B. Verwendung der goldenen Kontaktfläche des Chipkartenmoduls weiterhin möglich), und zudem hohe Kosten für teure Chipkartenleser einspart.

[0047] Im Aufbau einer ISO-Chipkarte mit den physikalischen Dimensionen ID-1 nach ISO 7810 [Fig. 1, Ziffer 1] vereint die erfindungsgemäße Vorrichtung wichtige Funktionen eines Chipkartenlesers und einer Chipkarte. Für den Nutzer sichtbar sind die typische goldene Kontaktfläche des Chipkartenmoduls einer Chipkarte [siehe Fig. 1, Ziffer 2], eine Tastatur [siehe Fig. 4, Ziffer 4] und eine Anzeigeeinheit [siehe Fig. 1, Ziffer 3] für vertrauenswürdige Ein- und Ausgaben.

[0048] Die Fig. 2 zeigt eine ISO-ID1-Chipkarte **1** als Ganzes. Der Crypto-Micro-Controller **2** ist eine vollwertige Prozessor-Chipkarte mit kryptographischen Fähigkeiten. Die erfindungsgemäße Vorrichtung kann mehrere dieser Chipkarten-Elemente haben. Ferner ist eine zentrale Verarbeitungseinheit, CPU, **3** vorhanden, die die Verarbeitung vornimmt. Auf der Display-Einheit **4** werden manipulationssicher die Transaktionsdetails angezeigt. Die Tastatureinheit **5** dient zur Eingabe von Daten durch den Nutzer, insbesondere von PINs. Eine Energiequelle **6** (falls erforderlich z. B. bei BT) wird zur Stromversorgung der Einheit bereitgestellt. Diese kann über NFC aufladbar oder auch ein Solarmodul sein. Die Netzwerkschnittstelle(n) (**7a**, **7b**, **7c**), dienen zur Kommunikation. Die erfindungsgemäße Vorrichtung enthält mindestens eine Netzwerkschnittstelle. Diese kann aus heutiger Sicht nach der NFC- **7a** oder der Bluetooth-Technologie **7b** oder auch einer anderen kontaktlosen Technologie **7c**, wie wireless-USB realisiert sein.

[0049] Im Falle einer NFC-Schnittstelle kann der NFC-Baustein auch direkt mit einem der Crypto-Micro-Controller der Vorrichtung verbunden sein. Alternativ kann die Vorrichtung auch einen Crypto-Micro-Controller mit integrierter NFC-Funktionalität haben.

[0050] Ferner ist ein Wirtssystem **8** mit einer sicherheitskritischen Anwendung notwendig, die für ihre Transaktionsabsicherung eine Chipkarte voraussetzt.

[0051] Das Wirtssystem kann ein klassischer PC (Windows, LINUX), ein Smartphone oder Tablet-PC (iPhone, Android, WindowsPhone7, Blackberry/10 etc.), sowie heutige Kassensysteme, Geldautomaten oder Bezahlterminals sein.

[0052] Die erfindungsgemäße Vorrichtung mit der integrierten NFC-Funktionalität **7a** macht es möglich, diese in allen bei NFC definierten und standardisierten Modi zu verwenden. Diese sind „card emulation“ (Rolle einer Chipkarte), „Read/Write“ (Rolle eines Chipkartenlesers) und „Peer-2-Peer“ (gleichberechtigte aktive Kommunikationseinheit für den Datenaustausch).

[0053] Als erstes soll der Fall „Cord Emulation“ erläutert werden. Im Fokus dieser Erfindung stehen Anwendungen, die auf einem Wirtssystem **8** laufen und den Einsatz einer Chipkarte voraussetzen. Solche Anwendungen können Home-, Mobile- oder Online Banking-Applikationen sein, aber auch VPN-Clients und auch Email-Clients, welche vom Nutzer erwarten, dass er seine Chipkarte für Authentifizierungszwecke oder elektronische Signaturen einsetzt. Wenn nun die erfindungsgemäße Vorrichtung mit solchen Anwendungen genutzt werden soll, und diese auf NFC-fähigen Endgeräten bzw. Wirtssystemen **8** laufen (z. B. Android-Smartphones oder – Tablets), so übernimmt die erfindungsgemäße Vorrichtung gegenüber dem Wirtssystem **8** im Falle „Cord-Emulation“ die Rolle einer Chipkarte. Das Wirtssystem **8** kann auch ein PC sein, der bereits einen externen oder integrierten NFC-fähigen Chipkartenleser hat. D. h. das Wirtssystem **8** ist im NFC-Sinne der Chipkartenleser und die erfindungsgemäße Vorrichtung im Modus „Cord-Emulation“ die Chipkarte. Kommt die Koppelung dieser zwei Geräte zu Stande, so wird diese Kommunikationsverbindung rein für die Datenübertragung verwendet. In der Regel verwendet eine Anwendung die jeweiligen Gerätetreiber eines Chipkartenlesers mittelbar oder unmittelbar, um über diese an die angeschlossene Chipkarte zu gelangen. Solche Gerätetreiber sind grundsätzlich entweder vorinstalliert oder müssen nachträglich im Wirtssystem installiert werden. Im Falle der erfindungsgemäßen Vorrichtung, die ebenfalls einen Chipkartenleser enthält, welcher im Rahmen der erfindungsgemäßen Verfahren verwendet werden soll, besteht die Aufgabe darin, den vorhandenen vorgeschalteten NFC-Chipkartenleser des Wirtsystems (extern oder integriert) zu umgehen. Für ein hohes Niveau an Sicherheit werden von der Anwendung grundsätzlich nicht nur reine Chipkartenbefehle gesendet, sondern auch solche, die sowohl Chipkartenleser und Chipkarte betreffen, oder solche nur für Chipkartenleser.

Zum einen würden Befehle zur Verwendung einer Anzeige oder einer Tastatur an einen Chipkartenleser ohne Display und Tastatur nichts nutzen. Zum anderen würde der vorgeschaltete NFC-Chipkartenleser solche Befehle höchstens ignorieren oder abweisen. Die Aufgabe kann gelöst werden, indem über die Anwendung oder auch mittelbar über eine zwischengeschaltete Zusatzsoftware spezielle Chipkartenbefehle an die Chipkarte (Crypto-Micro-Controller **2**) adressiert werden. Eine ähnliche Methode findet in heutigen Chipkartenlesern nach der Secoder-Spezifikation statt. Der an einem PC üblicherweise über USB angeschlossene Secoder-Chipkartenleser wird zwar von diesem PC als USB-Gerät erkannt, die installierten Standard-PC-Gerätetreiber (PC/SC) wissen jedoch nicht unbedingt, dass es sich um einen Secoder-Chipkartenleser handeln kann. Da aber die sicherheitsrelevante Anwendung auf dem PC nur mit einem Secoder-Chipkartenleser und einer Chipkarte, die in einem solchen Chipkartenleser steckt, kommunizieren darf, übernimmt sie die Aufgabe, die Befehle für den Chipkartenleser mit Hilfe von Chipkartenbefehlen in Form von Daten abzusetzen. Der vorgeschaltete Chipkartenleser des Wirtsystems erkennt anhand des empfangenen Befehls, dass dieser für die Chipkarte adressiert ist und leitet diese ordnungsgemäß an die gekoppelte Chipkarte (erfindungsgemäße Vorrichtung im „Cord-Emulation“-Modus) zur Verarbeitung weiter. Die gekoppelte erfindungsgemäße Vorrichtung befindet sich im NFC-Modus „Cord-Emulation“ und empfängt solche Befehle. Die CPU **3** der erfindungsgemäßen Vorrichtung kann diese als Chipkartenleserbefehle erkennen, interpretieren und ausführen. In der Regel handelt sich hierbei um Daten, die ein Chipkartenleser mit besonderen Anforderungen zuerst dem Nutzer auf dem vertrauenswürdigen Display anzeigt, diese vom Nutzer mit Hilfe der Tastatur bestätigen lässt, und sie dann mit Hilfe des Crypto-Micro-Controllers **2** signieren lässt. In der Folge gelangen diese signierten Daten als Antwort zurück zur Anwendung im Wirtssystem. Zuerst wird durch die CPU **3** der Vorrichtung die Antwort bzw. das Ergebnis eines ausgeführten Chipkartenbefehls vorbereitet und dann an den Chipkartenleser des Wirtsystems übergeben, welcher wiederum diese Daten der Anwendung über die Gerätetreiber zur Verfügung stellt. Die Anwendung kann durchaus auch Chipkartenbefehle senden, welche nicht nur für den Chipkartenleser der Vorrichtung gedacht sind. In einem solchen Fall wird der Befehl mit den Daten an die Chipkarte oder, konkret gesagt, an den Crypto-Micro-Controller **2** der erfindungsgemäßen Vorrichtung weitergeleitet und dort ordnungsgemäß ausgeführt. Das Ergebnis dieser Operation empfängt zuerst die CPU **3**, die es entsprechend über die Kommunikationsschnittstelle an das Wirtssystem weiterleitet. Wie oben beschrieben, stehen die Daten anschließend für die Anwendung bereit.

[0054] Die anderen NFC-Modi sind je nach Einsatzszenario ebenfalls denkbar. Beispielsweise kann der Peer2Peer-Modus im Rahmen eines Software-Updates der Vorrichtung zum Einsatz kommen. Ist die erfindungsgemäße Vorrichtung im NFC-Read/Write-Modus eingestellt, d. h. die Vorrichtung hat die Rolle eines Chipkartenlesers, so ist es möglich, die erfindungsgemäße Vorrichtung nicht nur mit einem PC kontaktlos zu verwenden, sondern auch mit einer anderen kontaktlosen Smartcard/Chipkarte. Letztere kann sowohl eine echte ISO-Chipkarte (z. B. Bankkarte) sein als auch eine Chipkarte/Smartcard als NFC-„card emulation“, wie z. B. ein weiteres NFC-fähiges Android-Smartphone, das sich wie eine Chipkarte verhält (d. h. im NFC-Mode card-emulation arbeitet). In diesem Fall wird beispielsweise das Smartphone als Wirtssystem **8** mit der erfindungsgemäßen Vorrichtung verbunden, die sich dann gegenüber diesem Wirtssystem **8** als Chipkartenleser ausgibt. Einer der in der erfindungsgemäßen Vorrichtung enthaltenen Crypto-Micro-Controller **2** kann in diesem Szenario die erfindungsgemäße Vorrichtung zu einem Chipkartenleser der Sicherheitsklasse **4** machen.

[0055] Welchen Modus die erfindungsgemäße Vorrichtung einnehmen soll oder über welche Netzwerkschnittstelle diese verbunden werden soll, kann vom Nutzer an dieser voreingestellt werden oder nach dem Einschalten über die Tastatur eingestellt werden, oder die Vorrichtung soll, wenn möglich, das passende Kommunikationsprotokoll oder den richtigen NFC-Modus selbst erkennen.

[0056] Kommuniziert die erfindungsgemäße Vorrichtung nach außen mit einem Wirtssystem **8** über den Bluetooth-Standard **7b**, so wird diese vom Wirtssystem, ggf. mit Hilfe zusätzlicher Treiber-Software auf dem Wirtssystem, als vollwertiger Chipkartenleser erkannt. Als Chipkarte oder Smartcard kommt in diesem Szenario die in der Vorrichtung integrierte Chipkarte bzw. der Crypto-Micro-Controller **2** zum Einsatz. In der Regel, wie beim Bluetooth-Standard üblich, sind beide Geräte gepaart oder müssen noch standard-konform gekoppelt werden. Über diese Kommunikationsschnittstelle zeigt die erfindungskonforme Vorrichtung dem Wirtssystem **8** an, dass sie ein Standard-Chipkartenleser (ebenfalls standard-konform) sei. Die Erkennung des Chipkartenlesers erfolgt entweder über die im Wirtssystem vorinstallierten Gerätetreiber (PC/SC) oder ggf. über nachträglich auf dem Wirtssystem zu installierenden Treibern, soweit dies möglich ist. Die Information, dass ein Chipkartenleser an dem Wirtssystem angeschlossen ist, steht im Normalfall jeder Anwendung, die eine Chipkarte benötigt, zur Verfügung, denn es handelt sich aus der Sicht des Wirtssystems um einen Standard-Chipkartenleser.

[0057] Die in der erfindungsgemäßen Vorrichtung integrierte CPU **3** schafft die Voraussetzungen für

die Ausführung von Programmcode, mit dessen Hilfe bestimmte Verfahren und Algorithmen zur Steuerung der gesamten sicheren Umgebung unter Berücksichtigung der Ein- und Ausgabe-Einheiten implementiert werden. Anwendungsszenarien hierfür sind Geschäftsvorfälle und Transaktionen, welche eine Anwendung auf einem Wirtssystem steuert oder ausführt, die eine an diesem Wirtssystem angebundene Chipkarte für das sichere Signieren von Daten erwartet. Je nach Anwendungsgebiet ist es somit möglich, auf der CPU **3** der erfindungsgemäßen Vorrichtung mehrere spezielle Anwendungen laufen zu lassen, welche die Fähigkeiten der gesamten Vorrichtung nutzen können. Diese können vorinstalliert sein oder nachgeladen werden. Damit kann die erfindungsgemäße Vorrichtung mit ihrem Verfahren zusätzlich und ohne Aufwand durch den Nutzer auch für mehrere Anwendungsgebiete zum Einsatz kommen.

[0058] Die **Fig. 4** zeigt die vier Schritte des erfindungsgemäßen Verfahrens. Beginnend mit Schritt **100** erfolgt das drahtlose Koppeln zwischen Wirtssystem und erfindungsgemäßer Vorrichtung. Mit Schritt **200** werden die zu signierenden Transaktionsdaten der erfindungsgemäßen Vorrichtung übergeben. Das erneute Anzeigen dieser Daten, deren Bestätigung durch den Nutzer über die Tastatur und deren Signatur erfolgen in Schritt **300**. Mit Schritt **400** werden die signierten Daten zurück an das Wirtssystem übertragen. Im Folgenden werden die vier Schritte des Verfahrens detaillierter beschrieben.

[0059] Der erste Schritt **100** des erfindungsgemäßen Verfahrens basierend vorzugsweise auf der o. g. Vorrichtung ist, dass die erfindungsgemäße Vorrichtung (z. B. über NFC oder Bluetooth) mit einem Wirtssystem (PC, Smartphone, Kassen-, Geldautomat oder einem anderen Bezahlterminal) verbunden wird, welches eine Anwendung zur Steuerung von Transaktionen ausführen kann. Bei den Transaktionen handelt es sich in der Regel um Finanztransaktionen, wie der bargeldlosen Zahlung/Überweisung von Geld. In der Regel sind solche Wirtssysteme mit einem Hintergrundsystem einer Bank oder einem anderen Server verbunden, welches oder welcher in der Lage ist, die Transaktionsdaten entgegenzunehmen und zu verarbeiten. Zuvor sind auf dem PC, dem Smartphone oder der Bezahlstation, und abhängig von den Möglichkeiten der jeweiligen Betriebssystemumgebung, für die erfindungsgemäße Vorrichtung spezifische Programminformationen gespeichert oder dafür geeignete Treiber installiert worden. Dass beim Wirtssystem die Netzwerkschnittstellen NFC oder Bluetooth aktiv sind und der standardmäßige Erkennungsmechanismus für externe Chipkartenleser aktiviert ist, wird vorausgesetzt.

[0060] Aus der Sicht der vorliegenden Erfindung ist es für die Erfüllung der Hauptaufgabe beim Etablieren der Kommunikation zwischen Wirtssystem und der

erfindungsgemäßen Vorrichtung unerheblich, ob diese über Bluetooth oder NFC stattfindet, oder ob das Wirtssystem bereits einen angeschlossenen externen oder integrierten Chipkartenleser besitzt. Wird die erfindungsgemäße Vorrichtung beispielsweise über NFC als externe Chipkarte (card emulation) verwendet, so kann dennoch, wenn dies benötigt wird, der Chipkartenleser der erfindungsgemäßen Vorrichtung verwendet werden und nicht der Chipkartenleser des Wirtssystems. Denn nur dieser gilt aus verständlichen Gründen als vertrauenswürdig und nicht beispielsweise die Umgebung eines Android-Smartphones.

[0061] Der zweite Schritt **200** des erfindungsgemäßen Verfahrens besteht darin, während einer Transaktionsabwicklung beispielsweise innerhalb einer Banking-Anwendung – unabhängig davon, ob diese browser-basierend als Webanwendung oder als Client-Anwendung auf dem Wirtssystem installiert ist –, dem Nutzer die von ihm auf dem Bildschirm des Wirtssystems eingegebenen Daten (z. B. Überweisungsbetrag, Empfängerkonto) zur Sicherstellung der Authentizität erneut in der sicheren Umgebung der erfindungsgemäßen Vorrichtung anzuzeigen und diese von ihm dort explizit bestätigen zu lassen. Im Einzelnen werden diese Daten zunächst durch die Anwendung in geeigneter Weise aufbereitet. Anschließend werden sie an die/eine erfindungsgemäße Vorrichtung über dafür vorgesehenen Programmkomponenten übertragen. Im dritten Schritt **300** des Verfahrens werden diese auf der vertrauenswürdigen Display-Einheit **4** manipulationssicher angezeigt, vom Benutzer über die sichere Tastatur-Einheit **5** bestätigt und unter Verwendung des in der Chipkarte enthaltenen und dem jeweiligen Nutzer eindeutig zugeordneten Schlüsselmaterials, das sicher im Crypto-Micro-Controller **2** abgelegt ist, signiert. Der Ablauf dieses Vorgangs ist bekannt oder standardisiert. Die Anwendung kommuniziert mit der erwarteten Chipkarte, welche in einem erwarteten sicheren Chipkartenleser steckt. Dies auch dann, wenn die tatsächliche kontaktlose Datenübertragung, wie im Falle von NFC, auf Basis eines anderen vorhandenen und unsicheren Chipkartenlesers stattfindet. Diese so auf der erfindungsgemäßen Vorrichtung signierten Daten empfängt sodann die Anwendung auf dem Wirtssystem im letzten und vierten Schritt **400** des erfindungsgemäßen Verfahrens und überträgt sodann diese gegebenenfalls an einen dafür vorgesehenen Empfänger. Dieser Ablauf kann während einer Transaktion bzw. Sitzung je nach Geschäftsvorfall gänzlich oder partiell mehrfach wiederholt werden. Geeignet ist die erfindungsgemäße Vorrichtung auch für Verschlüsselungsoperationen, da sie im Schlüsselspeicher auch Schlüssel für eine Verschlüsselung der Daten halten kann.

[0062] Die erfindungsgemäßen Verfahren und die erfindungsgemäße Vorrichtung erfüllen höchste Sicherheitsansprüche. Die PIN-Eingabe des Besitzers

der Chipkarte erfolgt je nach Geschäftsvorfall bei Bedarf oder Verlangen auf der sicheren erfindungsgemäßen Vorrichtung und wird außerhalb jeglicher potentieller Gefahren eines Wirtssystems verifiziert. Die zu signierenden Daten werden dabei auf einer sicheren Anzeige außerhalb und frei von Manipulationsmöglichkeiten visualisiert und vom Nutzer bestätigt. Die Tatsache, dass diese Daten der erfindungsgemäßen Vorrichtung von einer gefährdeten Umgebung wie der eines Wirtssystems stammen, ist nicht weiter kritisch. Die mit dem auf der Chipkarte befindlichen Schlüsselmaterial signierten Daten können nur von einem bestimmten Empfänger dieser signierten Daten sinnvoll und gültig verwendet werden. Die Erklärung dafür liefern die verwendeten kryptographischen Systeme. Asymmetrische oder symmetrische Kryptosysteme verwenden für das Signieren von Daten Schlüssel, die sich in der Regel im Crypto-Micro-Controller **2** der erfindungsgemäßen Chipkarte befinden. Diese verlassen nie den Crypto-Micro-Controller und seinen sicheren Speicher und sind nicht vom Wirtssystem erreichbar oder in sonstiger Weise zugänglich. Jede kryptographische Signaturoperation erfordert eine „Gegenoperation“. Wenn beispielsweise im Crypto-Micro-Controller **2** der erfindungsgemäßen Chipkarte auf Basis eines asymmetrischen Kryptosystems eine Signatur erzeugt wurde, so wurde dafür ein privater Schlüssel der Chipkarte verwendet. Die Verifikation dieses Schlüssels findet beim bestimmten Empfänger statt, der eine so signierte Nachricht bekommt. Ähnliches gilt auch bei Verwendung eines symmetrischen Kryptosystems. Nur Nutzer und Empfänger können prinzipiell den geheimen Schlüssel besitzen, mit dem eine Nachricht signiert wurde.

[0063] Die Vorteile der erfindungsgemäßen Anordnung und des erfindungsgemäßen Verfahrens liegen einerseits in der Tatsache, dass moderne mobile Endgeräte mit ihren integrierten kontaktlosen Kommunikationsschnittstellen (Bluetooth, NFC) optimal genutzt werden können, um dem Nutzer ein Höchstmaß an Sicherheit, Bedienbarkeit und Komfort anzubieten, wobei andererseits für die Herausgeber (z. B. Kreditinstitute) enorme Kosteneinsparungen durch den Wegfall eigener Chipkartenleser zu erwarten sind. Weitere Vorteile bestehen darin, dass die erfindungsgemäße Vorrichtung ein hohes Maß an Rückwärtskompatibilität bietet, und zwar weil sie wie eine herkömmliche ISO-Chipkarte verwendet werden kann. Darüber hinaus ist es natürlich auch möglich, einen Magnetstreifen auf der Rückseite der Vorrichtung anzubringen. Dahingegen ist die Verwendung von z. B. in Smartphones integrierten Chipkartenlesern aus Vertrauensgründen nicht zu empfehlen.

Literaturverweise

- [1] Deutsche Kreditwirtschaft (DK) Secoder, Connected mode, Reader Applications", Version 2.2
- [2] Wikipedia, Bluetooth, http://de.wikipedia.org/wiki/Bluetooth#Aktueller_Standard:_Bluetooth_4.0
- [3] Wikipedia, NFC, http://de.wikipedia.org/wiki/Near_Field_Communication
- [4] Wikipedia, Chipkartenleser, Kartenlese Chip-Kartenlesergerät, <http://de.wikipedia.org/wiki/Kartenleseger%C3%A4t>
- [5] Wikipedia, PC/SC Workgroup, www.pcscworkgroup.com/

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 102008007367 B4 [0013]

Zitierte Nicht-Patentliteratur

- ISO 7810 [0019]
- http://de.wikipedia.org/wiki/Near_Field_Communication [0020]
- ISO 14443 [0020]
- ISO 15693 [0020]
- http://de.wikipedia.org/wiki/Bluetooth#Aktueller_Standard:_Bluetooth_4.0 [0021]
- ISO 7810 [0023]
- ISO 7810 [0046]
- ISO 7810 [0047]

Patentansprüche

1. Chipkarte für eine elektronische Transaktion umfassend eine Anzeige, eine Tastatur, eine Netzwerkschnittstelle, eine Verarbeitungseinheit, einen Micro-Controller und einen Speicherbereich für Signaturinformationen und/oder Schlüsselmaterial, gekennzeichnet durch eine Einrichtung, die es der Chipkarte erlaubt, sich mit einem Wirtssystem über die Netzwerkschnittstelle zu verbinden, um sich gegenüber diesem Wirtssystem als integriertes Kartenlesegerät mit eingeschobener Chipkarte darzustellen, wobei die Transaktionsdaten zu der Chipkarte über die Netzwerkschnittstelle vom Wirtssystem empfangen werden, um auf dem Display dargestellt zu werden, um durch eine Tastatureingabe auf der Tastatur diese Transaktionsdaten bestätigen zu können, um diese Transaktionsdaten mit der Signatur zu versehen und um diese dann an den PC zu senden.

2. Chipkarte nach dem vorhergehenden Anspruch gekennzeichnet, durch eine physikalische Dimension nach einem Chipkartenstandard, insbesondere ISO 7810, vorzugsweise ID-1.

3. Chipkarte gekennzeichnet nach einem oder mehreren der vorhergehenden Ansprüche, gekennzeichnet durch physikalische Kontakte und Schaltungen, die einen Betrieb in Standard Kartenlesegeräten erlaubt, um eine Transaktion durchzuführen.

4. Chipkarte gekennzeichnet nach einem oder mehreren der vorhergehenden Ansprüche, gekennzeichnet durch einen sicheren Speicherbereich, der vorzugsweise durch einen Crypto-Micro-Kontroller verwaltet wird oder in einem solchen integriert ist.

5. Chipkarte gekennzeichnet nach einem oder mehreren der vorhergehenden Ansprüche, wobei im Speicherbereich Signaturinformationen und Schlüsselmaterial insbesondere Signaturschlüssel abgelegt sind, um die Transaktionsdaten zu signieren, die Identität des Nutzers der Chipkarte zu prüfen oder die Identität des Chip-Kartenlesers gegenüber einer Anwendung des Wirtssystems auszuweisen.

6. Chipkarte gekennzeichnet nach einem oder mehreren der vorhergehenden Ansprüche, gekennzeichnet durch eine Tastatur, insbesondere Folientastatur oder berührungsempfindlichem Bildschirm, die so ausgebildet ist, dass die physikalischen Dimensionen nach einem Chipkarten-Standard eingehalten werden.

7. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, gekennzeichnet durch einen integrierten Flachbildschirm, der so ausgebildet ist, dass die physikalischen Dimensionen nach einem Chipkarten-Standard eingehalten werden.

8. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, wobei das Wirtssystem ein Kassensystem oder ein PC-System, Smartphone, Geldautomat oder Bezahlterminal ist.

9. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, ausgebildet um in Abhängigkeit der Netzwerkverbindung sich gegenüber dem Wirtssystem als Chip-Kartenlesegerät oder während des Etablierens der Kommunikationsverbindung mit dem Wirtssystem sich als eine Chipkarte darzustellen, um sich jedoch einer Anwendung des Wirtssystems als Chipkartenleser mit eingeschobener Chipkarte darzustellen.

10. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, wobei dem Nutzer die von ihm auf dem Bildschirm des Wirtssystems eingegebenen Daten zur Sicherstellung der Authentizität erneut anzeigbar sind, und diese vom Nutzer dort explizit bestätigbar sind.

11. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, wobei die mit Schlüsselmaterial signierten Daten nur von einem bestimmten Empfänger dieser signierten Daten sinnvoll und gültig verwendbar sind.

12. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, wobei auf der Verarbeitungseinheit weitere Anwendungen laufen, umfassend einen funktionalen Teil eines oder mehrerer Anwendungsbereiche wie Home-, Mobile- oder Online Banking, aber auch funktionale Blöcke der Anwendungsbereiche – VPN-Client, Email-Client, elektronische Pässe und Ausweise, oder auch Zeiterfassung und Türöffnung, welche vom Nutzer erwarten, dass er seine Chipkarte für Authentifizierungszwecke oder elektronische Signaturen einsetzt.

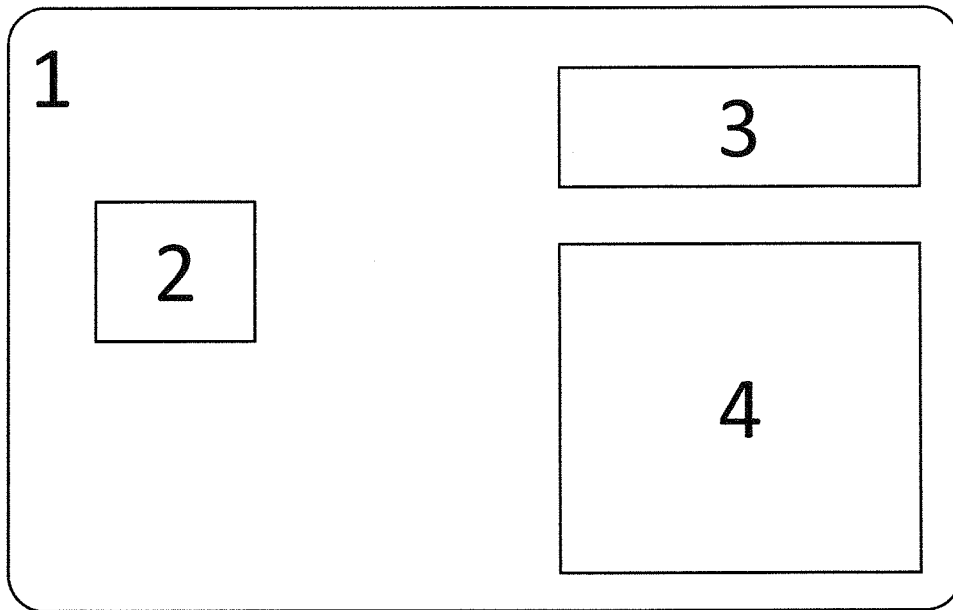
13. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, wobei ein oder mehrere Crypto-Micro-Controller enthalten sind und/oder mehrere Typen von Chip-Kartenlesegeräten emuliert werden.

14. Chipkarte nach einem oder mehreren der vorhergehenden Ansprüche, wobei eine Energiequelle zur Stromversorgung bereitgestellt wird, wobei diese über NFC Induktion aufladbar sein kann, oder auch ein Solarmodul sein kann.

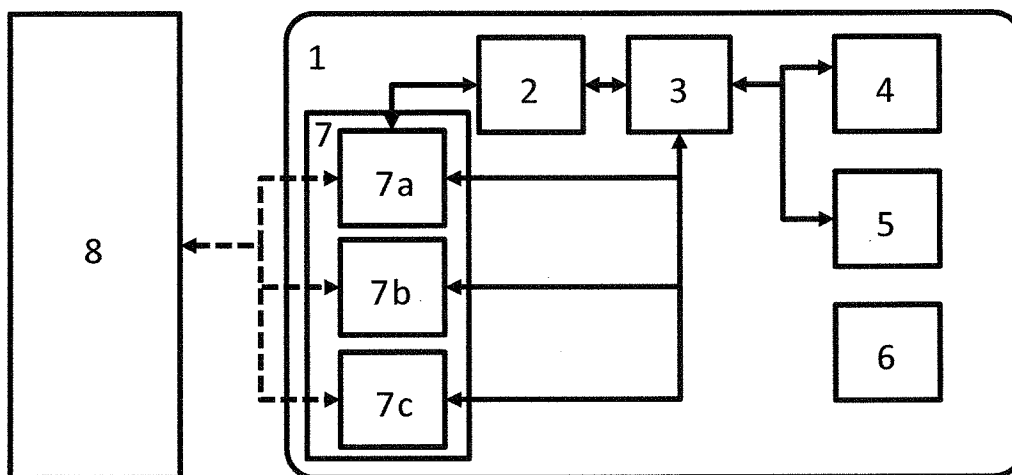
Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

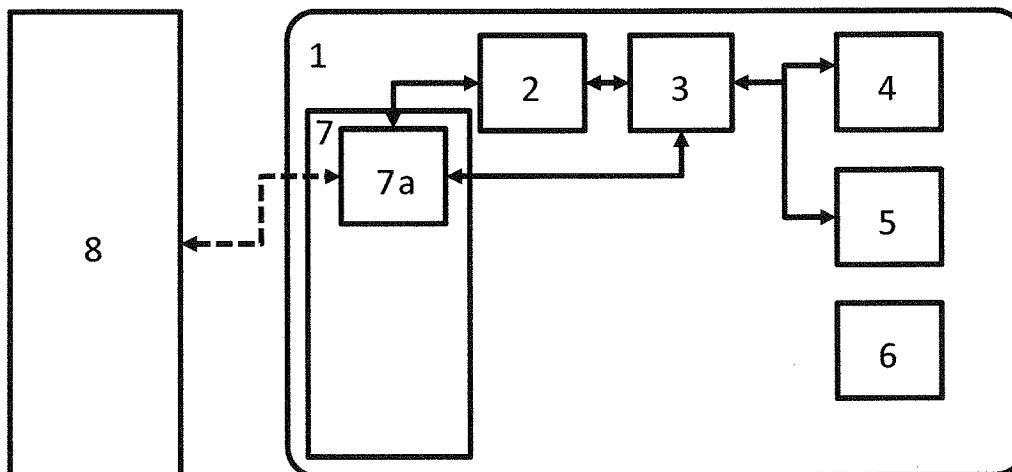
Zeichnungen



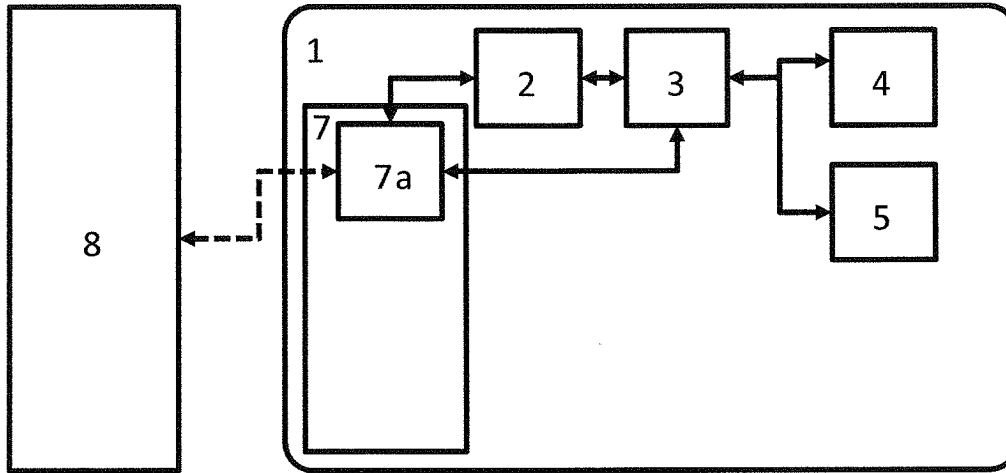
Figur 1.



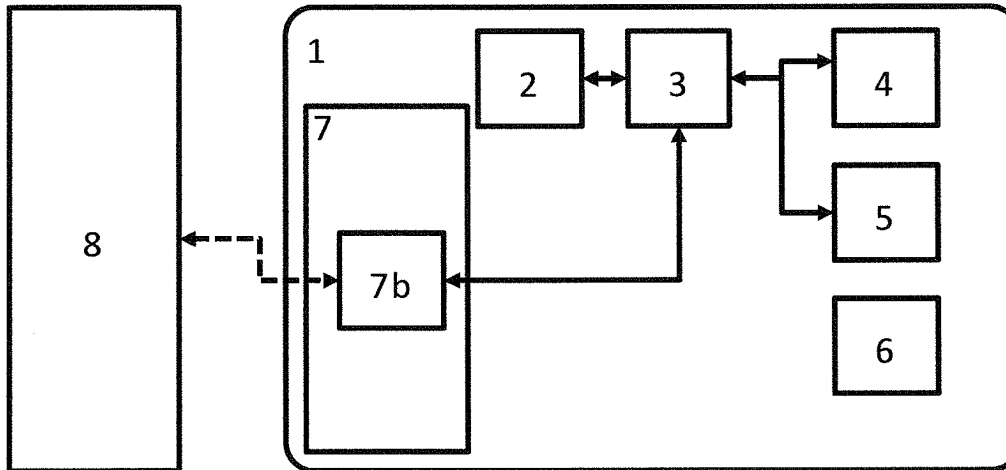
Figur 2.



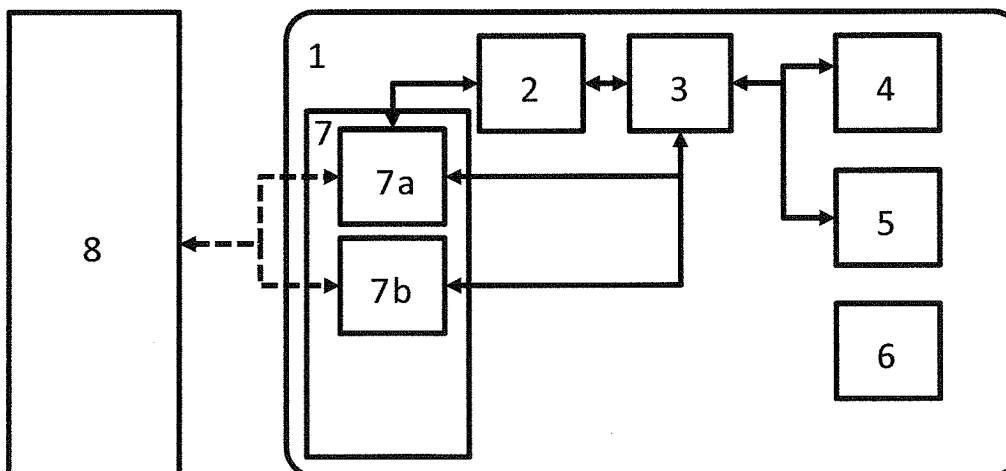
Figur 3a



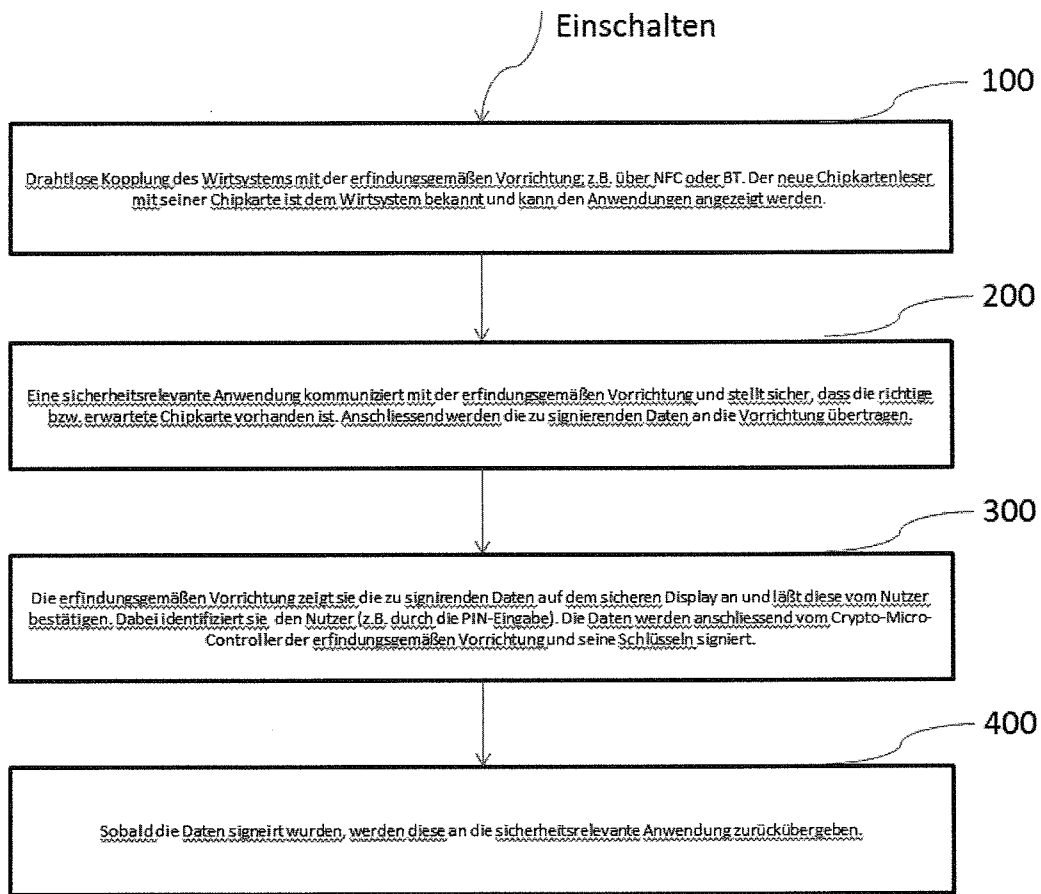
Figur 3b.



Figur 3c



Figur 3d



Figur 4