(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. Oktober 2004 (21.10.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/090800 A2

(51) Internationale Patentklassifikation[7]: G06K 19/00

(21) Internationales Aktenzeichen: PCT/EP2004/003880

(22) Internationales Anmeldedatum:
13. April 2004 (13.04.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 17 257.2 14. April 2003 (14.04.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 MÜNCHEN (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **GRAF, Hans** [DE/DE]; Hochgernstrasse 3, 83026 Rosenheim (DE). **FINKENZELLER, Klaus** [DE/DE]; Georg-Wopfner-Strasse 54, 80939 München (DE). **ROSSMADL, Alfred** [DE/DE]; Bessererstrasse 8, 87737 Boos (DE).

(74) Anwalt: **KLUNKER SCHMITT-NILSON HIRSCH**; Winzererstrasse 106, 80797 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) **Title:** CONTACTLESS DATA CARRIER

(54) **Bezeichnung:** KONTAKTLOSER DATENTRÄGER

(57) **Abstract:** The invention relates to a device and method for reliably determining the deliberate use of a contactless data carrier. In addition to an antenna-based data transmission channel, an optical data transmission channel can, according to the data to be transmitted, be used between the reading device and data carrier.

(57) **Zusammenfassung:** Die Erfindung betrifft eine Vorrichtung sowie ein Verfahren zur sicheren Feststellung der willentlichen Benutzung eines kontaktlosen Datenträgers. Neben einem antennenbasierten kann in Abhängigkeit von den zu übertragenen Daten zusätzlich ein optischer Datenübertragungskanal zwischen Lesegerät und Datenträger eingesetzt werden.

WO 2004/090800 A2

Kontaktloser Datenträger

Die vorliegende Erfindung betrifft eine Vorrichtung sowie ein Verfahren zur sicheren Feststellung der willentlichen Benutzung eines kontaktlosen Datenträgers.

Unter dem im Folgenden verwendeten Begriff „kontaktloser Datenträger" bzw. „Kontaktloskarte" werden alle Anordnungen verstanden, welche einen Mikrochip und eine mit diesem verbundene Antenne aufweisen und mit einem geeigneten Lesegerät Daten austauschen können. Hierzu zählen neben Chipkarten für Zahlungsanwendungen auch kontaktlos lesbare Identifikationsdokumente, wie Reisepässe und Personalausweise mit eingebautem Mikrochip sowie ferner RFID-Etiketten.

Kontaktlose Datenträger werden im Zahlungsverkehr heutzutage ausschließlich in geschlossenen Anwendungen, wie etwa zum Bezahlen in der Kantine, oder in öffentlichen Verkehrsmitteln eingesetzt. Der Grund hierfür ist, dass kontaktlose Karten aus Sicherheitsgründen in Deutschland bisher nicht für Zahlungsanwendungen wie z. B. als Geldkarte zugelassen sind. Ausschlaggebend hierfür ist die Befürchtung, dass vom Karteninhaber unbemerkt Dritte eine Geldkarte kontaktlos entladen könnten. Es wäre beispielsweise denkbar, dass mithilfe eines mobilen Terminals für kontaktlose Karten, welches durch Menschenansammlungen (z. B. Messen, Konzerte, U-Bahn, Bahnhof...) bewegt wird, unbemerkt „elektronisches" Geld aus den sich in der Nähe befindlichen Brieftaschen abgebucht werden kann. Bei kontaktbehafteten Karten tritt ein derartiges Problem nicht auf, da ein Zahlungsvorgang von dem Karteninhaber durch Einstecken der Karte in den Kartenleser erfolgt.

Neben der Verwendung als Zahlungsmittel können Kontaktloskarten auch als Datenträger in Wertdokumenten, wie z. B. Reisepässen eingesetzt wer-

den. Insbesondere bietet es sich an, kontaktlose Karten als Visa zu verwenden, die in das Reisedokument aufgenommen, beispielsweise aufgeklebt, werden können. Hierzu eignet sich z.B. das Coil-on-Chip-Verfahren (CoC), bei dem die Antenne auf dem Chip angeordnet ist. Es können aber auch herkömmliche Kontaktlosanordnungen verwendet werden, wie z. B. Folien mit darauf angeordnetem Chip und einer auf der Folie aufgedruckten Spule.

Auch bei der Verwendung von Kontaktloskarten in Wertdokumenten stellt sich das Problem, dass ein unbeabsichtiges Lesen durch Dritte verhindert werden soll. Gleiches gilt für das unberechtigte und unbemerkte Auslesen von Kontaktlostranspondern die zur Produktkennzeichnung eingesetzt werden.

Aufgabe der vorliegenden Erfindung ist daher die Bereitstellung einer Vorrichtung sowie eines Verfahrens zur sicheren Feststellung der willentlichen Benutzung eines kontaktlosen Datenträgers durch den Karteninhaber.

Die Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. In davon abhängigen Ansprüchen sind vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung angegeben.

Mithilfe des zusätzlichen Datenübertragungskanals werden auf optischem Weg Daten zwischen Lesegerät und Datenträger ausgetauscht, die geeignet sind, eine Authentifizierung zwischen Lesegerät und Kontaktloskarte durchzuführen. Die Authentifizierung über den zusätzlichen Datenübertragungskanal verhindert ein unbeabsichtigtes Betätigen der Kontaktloskarte, da die optische Information nicht mehr zur Verfügung steht, wenn der Datenträger für das Lesegerät optisch nicht mehr sichtbar ist, also z. B. in einer Tasche/Geldbörse getragen wird.

Nach einer ersten Ausführungsform der Erfindung weist der Datenträger optisch lesbare Informationen auf, wie z. B. einen Strich- oder Matrixcode. Wird die Karte dem Lesegerät präsentiert, so wird diese Information mittels einer optischen Lesevorrichtung, z. B. einem Barcodescanner gelesen und ausgewertet. Die optisch gelesene Information kann anschließend von dem kontaktlosen Datenträger zur Authentifizierung mit dem kontaktlosen Lesegerät verwendet werden, um so die Berechtigung für eine anschließende Transaktion vorzuweisen.

Eine Erweiterung dieser ersten Ausgestaltung besteht darin, die optisch angezeigte Information durch den Chip auf eine Anzeigevorrichtung, z. B. einem LCD-Display auszugeben. Auf diese Weise ist ein einfaches Kopieren der Informationen nicht mehr möglich, da die Informationen auch zufällig generierte Datenstrukturen enthalten können.

Nach einer weiteren Ausgestaltung der Erfindung ist der kontaktlose Datenträger mit einem optischen Leuchtmittel ausgestattet, z. B. einer IR-Leuchtdiode oder einer Leuchtfolie. Dabei kann das Leuchtmittel über eine elektrische Verbindung mit dem Chip verfügen oder integraler Bestandteil des Chips sein. Sobald ein kontaktloses Lesegerät eine Transaktion mit dem Datenträger beabsichtigt, wird das Leuchtmittel verwendet, um zusätzlichen Daten vom Chip auf optischem Wege an das Lesegerät zu senden. Diese Daten können Bestandteil einer gegenseitigen Authentifizierung sein und werden erfindungsgemäß dazu verwendet, eine nachfolgende Transaktion freizugeben. Ohne Kenntnis der optisch übertragenen Daten im Lesegerät kann eine Transaktion mit dem Datenträger nicht durchgeführt werden.

Vorzugsweise lassen sich auf dem Datenträger Veränderungen der Umgebungsbedingungen detektieren, sobald diese für einen Bezahlvorgang aus der Tasche genommen wird. So kann beispielsweise mittels eines lichtempfindlichen optischen Bauteils (14) festgestellt werden, ob sich die Karte in einer Tasche oder ausserhalb befindet. Das lichtempfindliche Bauteil kann dabei über eine elektrische Verbindung mit dem Chip verfügen oder integraler Bestandteil des Chips sein. Sobald das lichtempfindliche Bauteil einer Mindesthelligkeit ausgesetzt ist, wird erfindungsgemäß ein Freigabesignal erzeugt, welches eine Transaktion des Chips mit dem kontaktlosen Lesegerät ermöglicht.

Der Vorteil dieser Variante besteht darin, dass keine speziellen kontaktlosen Terminals erforderlich sind, sondern die bisher schon vorhandene Infrastruktur (z. B. kontaktlose Terminals, wie sie bisher schon in geschlossenen Systemen, wie z. B. Kantine verwendet werden) weiter zu benutzen.

Eine Weiterbildung dieser Idee besteht darin, durch das Lesegerät selbst ein optisches Signal zu erzeugen. Zur Freigabe einer Transaktion mit dem Chip ist es denkbar, das optische Signal mit einer markanten Modulation, z. B. einem 1 kHz Signal zu versehen oder mittels des optischen Signals Daten an den Chip zu übertragen, welche zur Authentisierung zwischen Datenträger und Lesegerät verwendet werden.

Eine Kombination der vorgenannten Ausführungsformen besteht darin, auf der Karte sowohl ein optisches Leuchtmittel als auch ein optisches Empfangsmittel zur Verfügung zu stellen und mit dem Chip zu verbinden oder diese Mittel als integralen Bestandteil des Chips bereitzustellen. In diesem Falle wäre neben einer kontaktlosen bidirektionalen Datenübertragung zusätzlich eine bidirektionale optische Datenübertragung zwischen der Karte

und einem Lesegerät durchführbar. Erfindungsgemäß ist dabei vorgesehen, zwischen den unterschiedlichen Übertragungskanälen zu wechseln, wobei vorzugsweise jeder Übertragungskanal zumindest einmal für die Übertragung von Daten verwendet werden kann.

Ein weiterer Vorteil dieser Anordnung besteht darin, dass die Energie zum Betrieb der optischen Kommunikationsmittel aus dem kontaktlosen Übertragungskanal (z. B. magnetische oder kapazitive Kopplung) gewonnen wird. Es versteht sich darüber hinaus von selbst, dass für die optische Kommunikation neben sichtbarem Licht auch IR, UV oder eine Mischung (uplink vs. downlink) aus diesen Bereichen verwendet werden kann.

Analog zu optischer Information könnten alternativ oder zusätzlich auch akustische Informationen verwendet werden, z. B. in Form der Übertragung eines codierten akustischen Signals, welches z. B. mit einem in der Karte integrierten Lautsprecher (z. B. Piezolautsprecher) erzeugt werden kann.

Weiterhin ist ein in der Karte befindlicher Lautsprecher auch dazu geeignet, um jede Zahlungstransaktion mit einem Signal zu quittieren, welches dem Karteninhaber signalisiert, dass momentan ein Zahlungsvorgang auf seiner Karte stattfindet. In dieser Ausgestaltung der Erfindung wäre es zwar immer noch möglich, unerlaubt Geld mit einem mobilen kontaktlosen Terminal von der Karte zu buchen, jedoch bliebe eine Transaktion nicht unbemerkt.

Anstelle eines Lautsprechers kann alternativ oder zusätzlich auch vorgesehen sein, den Datenträger mit einem Vibrationsalarm zu versehen.

Die Erfindung wird im folgenden anhand der in der Zeichnung dargestellten Ausführungsbeispiele näher erläutert.

Es zeigen:

Fig. 1 eine Ausführungsform der vorliegenden Erfindung, wobei auf dem Datenträger eine optische Information aufgebracht ist,

Fig. 2 eine weitere Ausführungsform der Erfindung mit einem auf dem Datenträger angeordneten Leuchtmittel,

Fig. 3 eine weitere Ausführungsform der Erfindung mit einem auf dem Datenträger angeordneten optischen Empfangsmittel,

Fig. 4 eine weitere Ausführungsform der Erfindung mit einem auf dem Datenträger angeordneten optischen Bauteil,

Fig. 5 ein Ausführungsbeispiel eines Verfahrens zur Ableitung eines kryptografischen Schlüssels, und

Fig. 6 ein Ausführungsbeispiel eines Authentifizierungsverfahrens.

Fig. 1 zeigt einen kontaktlosen Datenträger 1a, mit einer auf diesem angeordneten Antenne 2 und einem mit diesem elektrisch leitend verbundenen Chip 3. Ein Bereich des Datenträgers weist optische Informationen 4, beispielsweise einen Barcode oder auch einen Matrixcode auf, welche geeignet sind, über einen optischen Datenübertragungskanal 5 an das Lesegerät 1 übertragen zu werden. Der optische Datenübertragungskanal 5 wird zusätzlich zu dem antennenbasierten kontaktlosen Datenübertragungskanal 15 bereitgestellt.

In Fig. 2 wird ein kontaktloser Datenträger beschrieben, auf dem ein optisches Leuchtmittel 6 angeordnet ist. Das Leuchtmittel 6, welches als LED, OLED oder auch als Infrarot-Leuchtdiode (IR-LED) ausgestaltet werden kann, ist, wie durch den Pfeil 7 angedeutet, mit dem Chip 3 elektrisch leitend verbunden und wird durch diesen angesteuert. Auch hier erfolgt eine optische Datenübertragung über den Datenübertragungskanal 8.

Eine weitere Ausführungsform ist in Fig. 3 dargestellt, bei dem auf dem Datenträger 1a ein optisches Empfangsmittel 9 angeordnet ist, welches mit dem Chip 3 elektrisch leitend verbunden ist und eine bidirektionale optische Datenübertragung zwischen Lesegerät 1 und Datenträger 1a ermöglicht. Dabei kann der Chip 3 die Steuerung der Datenübertragung sowohl für die kontaktlose 15 als auch für die optische Datenübertragung 10 übernehmen. Beide Übertragungskanäle können im Wechsel oder auch gleichzeitig betrieben werden. Ferner können die Übertragungskanäle gleichberechtigt oder hierarchisch (Master-Slave) betrieben werden.

Mithilfe des in Fig. 4 dargestellten optischen Bauteils 14, welches eine elektrisch leitende Verbindung 11 mit dem Chip 3 aufweist, kann bei ausreichendem Lichteinfall 13 die Datenübertragung über die antennenbasierte kontaktlose Schnittstelle freigegeben werden (durch den Pfeil 12 angedeutet).

Das Verfahren zur Freigabe von im Datenträger 1a gespeicherten geheimen Informationen kann beispielsweise folgendermaßen ablaufen. Wie in Fig. 5 dargestellt, weist der Speicher 21 des Chips 3 mehrere Speicherbereiche 24 bzw. 22 auf, welche teilweise frei auslesbar sind und deren Inhalte teilweise mit Hilfe geeigneter Schlüssel gegen ein unberechtigtes Auslesen abgesichert sind. Der abgesicherte Speicherbereich 22 enthält mindestens einen Datensatz 23, der aus geheimzuhaltenen Informationen, wie z.B. Biometriedaten,

PIN etc. besteht. Der frei auslesbare Speicherbereich 24 enthält mindestens einen Datensatz 25, der dem jeweiligen Datensatz 23 eindeutig zugeordnet ist und einen Komprimierungswert, z.B. einen CRC, Hash, eine kryptografische Prüfsumme etc. darstellt. Ein Rückschluß von dem Inhalt des frei auslesbaren Datensatzes 25 auf den Inhalt des geheimen Datensatzes 23 ist ausgeschlossen.

Zum Auslesen eines der Datensätze 23 ist erfindungsgemäß vorgesehen, in einem ersten Verfahrensschritt den diesem zugeordneten Datensatz 25 über den antennenbasierten Datenübertragungskanal 15 sowie die optisch lesbaren Informationen 20, z.B. ein Barcode oder eine MRZ (machine readable zone), des Datenträgers 1a mit Hilfe des Lesegerätes 1 auszulesen.

In einem zweiten Verfahrensschritt wird aus dem Datensatz 25 und den optisch lesbaren Informationen 20 ein kryptografischer Schlüssel 26 abgeleitet. Hierzu können beliebige Schlüsselableitungsverfahren eingesetzt werden, die aus dem Stand der Technik hinlänglich bekannt sind, wie z.B. Schlüsselableitung unter Verwendung eines Masterschlüssels, etc. Der für den Datenträger individuelle kryptografische Schlüssel, der aus dem geheimen Masterschlüssel abgeleitet ist, ist bereits auf dem Datenträger gespeichert. Der Masterschlüssel ist in dem Lesegerät abgelegt für die Ableitung des kryptografischen Schlüssels 26 mittels der optisch gelesenen Informationen 20 und dem kontaktlos gelesenen Datensatz 25.

Ein dritter Verfahrensschritt sieht vor, eine Authentifizierung 27 zwischen Lesegerät 1 und dem Chip 3 des Datenträgers 1a mittels des abgeleiteten kryptografischen Schlüssels durchzuführen. Hiermit wird überprüft, ob die jeweiligen dem Lesegerät 1 bekannten bzw. die im Datenträger 1a hinterlegten Schlüssel identisch sind. Ein bereits aus dem Stand der Technik bekann-

tes Authentifizierungsverfahren arbeitet nach dem „Challenge-Response-Prinzip", welches im Bereich der Chipkarten weite Verbreitung findet. Durch ein „GetChallenge"-Kommando erhält das Lesegerät 1 eine Zufallszahl von dem Chip 3, um sich anschließend durch die Daten eines „External Authenticate"-Kommando, die aus der Zufallszahl und dem Schlüssel abgeleitet sind, gegenüber dem Chip zu authentifizieren. Selbstverständlich können weitere Authentifizierungsschritte, beispielsweise zur gegenseitigen Authentifizierung, und andere Verfahren zur Authentifizierung verwendet werden.

In einem vereinfachten Verfahren soll sich das Lesegerät in dem dritten Verfahrensschritt lediglich als ein solches Authentifizieren, welches beide Datenübertragungskanäle benutzt, ohne dabei gleichzeitig die Kenntnis eines geheimen Schlüssels nachzuweisen. In dem zweiten Verfahrensschritt 26 wird dann beispielsweise ein Wert abgeleitet, der zwar als Schlüssel für den dritten Schritt 27 verwendet wird, aber nicht geheim bzw. aus einem Master-Schlüsel abgeleitet ist.

In einem optionalen letzten Verfahrensschritt wird aus dem ausgelesenen Datensatz 23 ein Komprimierungswert gebildet und dieser mit dem Inhalt des frei auslesbaren Datensatzes 25 verglichen (s. Fig. 5, Überprüfung 28). Unterscheiden sich beide Komprimierungswerte, so ist davon auszugehen, dass der Datensatz 23 unbefugt verändert wurde. Nach erfolgreicher Authentifizierung kann der Datensatz 23 ausgelesen werden.

Das in Fig. 6 beschriebene Verfahren sieht ebenfalls vor zumindest auf einen Teil, der im Transponder gespeicherten Daten, den Zugriff nur nach erfolgreicher Authentisierung zu ermöglichen. Das Verfahren arbeitet auch nach dem „Challenge-Response-Prinzip".

In einem ersten Schritt 30 fordert das Lesegerät 1 eine Zufallszahl vom Datenträger 1a über den antennenbasierten Übertragungskanal 15 an. In einer erfindungsgemäßen Ausführungsform wird eine vom Datenträger 1a generierte Zufallszahl über den optischen Datenübertragungskanal 5, beispielsweise einer (Infrarot-/UV-) LED, an das Lesegerät 1 übertragen (Schritt 31: „response"). Eine weitere Möglochkeit besteht darin, die Zufallszahl als Barcode, Pixelcode, MRZ (machine readable zone) auf einem Display 4 auf dem kontaktlosen Datenträger 1a aus zu geben. Auch kann gleichzeitig über den antennenbasierten Datenübertragungskanal 15 eine Antwort gesendet werden, welche sich inhaltlich von den auf optischem Wege übertragenen kontaktlosen Daten unterscheidet, aber einem Timeout auf dem Übertragungskanal, also insbesondere beim Lesegerät, vorbeugt. Einerseits kann ein potentieller Angreifer keine inhaltlichen Rückschlüsse beim Mithören des antennenbasierten Übertragungskanals 15 ziehen, andererseits ist aber auch keine besondere Behandlung einzelner Applikationskommandos erforderlich, so dass die Software des Lesegeräts 1 nicht verändert werden muss. Es bietet sich beispielsweise an, den Code „90 00" (Kommando erfolgreich ausgeführt) zu senden. Um eventuelle Angreifer irrezuführen, können auch falsche Daten übermittelt werden.

Es ist ebenfalls denkbar, die Zufallszahl über den optischen Datenübertragungskanal anzufordern und über den antennenbasierten Datenübertragungskanal zu übertragen.

Der Authentifizierungsalgorithmus läuft anschließend nach dem bekannten Verfahren zur einseitigen oder gegenseitigen Authentifizierung („external authenthicate", 32) ab. Wurde die Authentifizierung erfolgreich abgeschlos-

sen, so kann die eigentliche Kommunikation 33 beginnen und der Datensatz 23 ausgelesen werden.

Das in Bezug auf Fig. 6 beschriebene Verfahren kann in Kombination oder aber unabhängig von dem zu Fig. 5 beschriebenen Verfahren angewendet werden.

Ein Vorteil der beschriebenen Verfahren besteht darin, dass durch die Verwendung zweier unterschiedlicher Datenübertragungskanäle - des optischen 5 sowie des antennenbasierten 15 - ein Verfälschen oder Austauschen der Daten erheblich erschwert wird. Es eignet sich daher insbesondere für den Austausch von sensiblen, wie z. B. personenbezogenen Daten. Eine einseitige Authentifizierung oder eine gegenseitige Authentifizierung werden verbessert durch den miteinander verbundenen Einsatz der beiden Datenübertragungskanäle.

Je nach Art der zu übertragenen Daten ist es aber auch denkbar, wahlweise nur einen Datenübertragungskanal zu verwenden. Der damit verbundene Verlust an Sicherheit ist in der Regel mit einem Zugewinn an Verarbeitungsgeschwindigkeit verbunden und kann bei Daten, wie sie beispielsweise für den Bereich der Logistik, des Warentransports und der Warenverwaltung benötigt werden, u.U. toleriert werden. Sollen mit Hilfe des gleichen Datenträgers 1a auch sensible Daten verarbeitet werden, kann hierfür zwingend vorgesehen sein, beide Datenübertragungskanäle beim Auslesen durch das Lesegerät zu nutzen. Die Umschaltung zwischen ein bzw. zwei Übertragungskanälen kann dabei nach Setzen eines Flags o.ä. automatisiert erfolgen.

Bei einem erfindungsgemäßen Lesegerät 1 handelt es sich um ein intelligentes Gerät, welches sowohl über antennenbasierte kontaktlose Lesemittel 2

wie auch über optische Lesemittel verfügt. In einer bevorzugten Ausführungsform ist das Lesegerät 1 als mobiles Endgerät, z.B. Mobiltelefon, PDA, Laptop o.ä. ausgebildet und weist eine Schnittstelle zur Kontaktloskommunikation, wie NFC (Near Field Communication) auf. Als optisches Kommunikationsmittel kann die in den meisten Geräten vorhandene IRDA-Schnittstelle eingesetzt werden. Als optisches Lesemittel kann eine Kamera vorgesehen sein. Vorzugsweise werden die optisch lesbaren Daten, wie z.B. die Seriennummer des Chips 3 auf dem Datenträger 1a in einer maschinenlesbaren Form dargestellt (Barcode, OCR-Daten). Ein derartiges Lesegerät 1 eignet sich besonders zur Kontrolle von Reisedokumenten durch Polizei oder Grenzschutzbeamte, wobei über eine eventuell zusätzlich vorhandene Onlineverbindung weitere Abfragen ausgeführt werden können.

Zur Erhöhung der Sicherheit kann vorgesehen sein, dass der Chip 3 des Datenträgers 1a zusätzlich eine Zufallszahl als Seriennummer generiert und über den antennenbasierten Datenübertragungskanal an das Lesegerät 1 überträgt. Die Verwendung derartiger Zufallsseriennummern wird beispielsweise in der ISO 14443 (Chapter 6.4.4, „UID contents and cascade levels") beschrieben. Die zur Abwicklung des Antikollisionsalgorithmus benötigte Seriennummer des Datenträgers 1a besteht dabei nicht wie üblich aus einer eindeutigen und unverwechselbaren Ziffer, sondern aus einer bei jeder Transaktion neu erzeugten Zufallszahl. Durch diese Maßnahme ist kein Rückschluß aus der verwendeten Seriennummer auf die Identität des Datenträgers mehr möglich. Ein eventueller (Replay-)Angriff durch Wiederholen einer einmal abgehörten Kommunikation zwischen Datenträger und Terminal kann somit besonders effektiv verhindert werden.

Auch die optisch lesbaren Daten können nicht-statisch auf dem Datenträger 1a verfügbar sein und z.B. mit Hilfe eines Displays o.ä. dynamisch verändert

werden. Es lassen sich derart auch Einmal-Passwörter, Zufallsseriennummern etc. generieren und darstellen. Ferner ist auch eine beliebige Kombination aus den dynamisch generierten und entweder antennenbasiert oder optisch übertragenen Daten denkbar.

Gemäß der vorliegenden Erfindung weist ein kontaktloser Datenträger eine Antenne und einen Chip auf, wobei der Datenträger Mittel zur Übertragung von Daten über einen optischen Datenübertragungskanal und Mittel zur Übertragung von Daten über einen antennenbasierten Datenübertragungskanal aufweist. Auf dem Datenträger sind Daten angeordnet, die über den optischen Datenübertragungskanal und/oder den antennenbasierten Datenübertragungskanal an ein Lesegerät übertragbar sind.

Patentansprüche:

1. Kontaktloser Datenträger mit einer Antenne und einem Chip, **dadurch gekennzeichnet, dass** auf dem Datenträger Daten angeordnet sind, die über einen optischen Datenübertragungskanal an ein Lesegerät übertragbar sind und Daten angeordnet sind, die über einen antennenbasierten Datenübertragungskanal an ein Lesegerät übertragbar sind.

2. Datenträger nach Anspruch 1, **dadurch gekennzeichnet, dass** der Chip Speicherbereiche aufweist, wobei mindestens ein Speicherbereich frei auslesbar und mindestens ein Speicherbereich nur nach einer Authentifizierung von Datenträger und Lesegerät auslesbar ist.

3. Datenträger nach Anspruch 2, **dadurch gekennzeichnet, dass** der nur nach einer Authentifizierung auslesbare zweite Speicherbereich mindestens einen ersten Datensatz aufweist und der frei auslesbare Speicherbereich wenigstens einen zweiten Datensatz aufweist, der dem ersten Datensatz eindeutig zugeordnet ist und aus dem ersten Datensatz ableitbar ist.

4. Datenträger nach einem der Ansprüche 2 oder 3, **dadurch gekennzeichnet, dass** die gespeicherten Datensätze als mit einem kryptografischen Schlüssel verschlüsselte Datensätze gespeichert sind.

5. Datenträger nach Anspruch 3 oder 4, **dadurch gekennzeichnet, dass** der zweite Datensatz einen Komprimierungswert des ersten Datensatzes bildet.

6. Datenträger nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** auf dem Datenträger ein lichtempfindliches Bauteil angeordnet ist,

welches die Funktion des Chips in Abhängigkeit von der Helligkeit steuert.

7. Datenträger nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** auf dem Datenträger optisch lesbare Informationen aufgebracht sind.

8. Datenträger nach Anspruch 7, **dadurch gekennzeichnet, dass** auf dem Datenträger ein Matrixcode aufgebracht ist.

9. Datenträger nach Anspruch 7, **dadurch gekennzeichnet, dass** auf dem Datenträger ein Barcode aufgebracht ist.

10. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** auf dem Datenträger ein Display zur Darstellung optischer Daten angeordnet ist.

11. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** auf dem Datenträger ein Leuchtmittel zum Senden von optischen Signalen angeordnet ist.

12. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** auf dem Datenträger ein optisches Empfangsmittel zum Empfangen von optischen Signalen angeordnet ist.

13. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** auf dem Datenträger ein Lautsprecher angeordnet ist.

14. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** auf dem Datenträger ein Vibrationsmelder angeordnet ist.

15. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** eine Authentifizierung die Verwendung beider Datenübertragungskanäle erfordert.

16. Verfahren zur sicheren Feststellung der willentlichen Benutzung eines kontaktlosen Datenträgers, **dadurch gekennzeichnet, dass** in Abhängigkeit von den zwischen Datenträger und Lesegerät auszutauschenden Daten zusätzlich zu einer antennenbasierten kontaktlosen Datenübertragung eine optische Datenübertragung mithilfe von auf dem Datenträger angeordneten Daten erfolgen kann.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, dass** die Datenübertragung bidirektional erfolgt.

18. Verfahren nach Anspruch 16 oder 17, **dadurch gekennzeichnet, dass** zwischen der optischen und der antennenbasierten Datenübertragung beliebig umgeschaltet werden kann.

19. Verfahren nach einem der Ansprüche 16 bis 18, **dadurch gekennzeichnet, dass** eine zumindest einseitige Authentifizierung (27, 32) zwischen dem Lesegerät und dem Datenträger erfolgt.

20. Verfahren nach Anspruch 19, **dadurch gekennzeichnet, dass** durch die optische Datenübertragung die Authentifizierung erfolgt.

21. Verfahren nach Anspruch 19 oder 20, **dadurch gekennzeichnet, dass** die Authentifizierung (27,32) so erfolgt, daß sie die Verwendung beider Datenübertragungskanäle erfordert.

22. Verfahren nach einem der Ansprüche 16 bis 21, **dadurch gekennzeichnet, dass** eine Zufallszahl über einen der beiden optischen bzw. antennenbasierten Datenübertragungskanäle angefordert wird und über den jeweils anderen Datenübertragungskanal übertragen wird.

23. Verfahren nach einem der Ansprüche 16 bis 22, **dadurch gekennzeichnet, dass** für ein Auslesen eines ersten Datensatzes (23) in einem ersten Verfahrensschritt das Lesegerät einen zweiten Datensatz (25), der dem ersten Datensatz zugeordnet ist, und optisch auf dem Datenträger dargestellte Daten (20) ausliest.

24. Verfahren nach Anspruch 23, **dadurch gekennzeichnet, dass**
in einem zweiten Verfahrensschritt (26) das Lesegerät aus den ausgelesenen Daten und einem geheimen Schlüssel einen abgeleiteten Wert bildet, dass
in einem dritten Verfahrensschritt auf der Grundlage des abgeleiteten Werts die Authentifizierung (27) zwischen Lesegerät und Datenträger erfolgt und dass
in einem vierten Verfahrensschritt der erste Datensatz (23) durch das Lesegerät ausgelesen wird.

25. Verfahren nach Anspruch 23 oder 24, **dadurch gekennzeichnet, dass** in einem fünften Verfahrensschritt aus dem ersten Datensatz ein Komprimierungswert gebildet wird und in einem weiteren Verfahrensschritt ein Vergleich des derart gebildeten Komprimierungswertes mit dem zweiten Datensatz erfolgt.

26. Verfahren nach einem der Ansprüche 19 bis 25, **dadurch gekennzeichnet, dass** die Authentifizierung (27,32) nach Art eines challenge-response-Verfahrens durchgeführt wird.

27. Lesegerät zum Lesen eines kontaktlosen Datenträgers, **dadurch gekennzeichnet, dass** es Mittel zum Lesen von optischen Daten aufweist.

28. Lesegerät nach Anspruch 27, **dadurch gekennzeichnet, dass** es Mittel zum Senden eines optischen Signals aufweist.

29. Lesegerät nach Anspruch 28, **dadurch gekennzeichnet, dass** es Mittel zum Modulieren des optischen Signals aufweist.

30. Lesegerät nach Anspruch 28, **dadurch gekennzeichnet, dass** es eine Infrarot-Schnittstelle aufweist.

31. Lesegerät nach einem der Ansprüche 27 bis 30, **dadurch gekennzeichnet, dass** es als mobiles Endgerät ausgebildet ist.

32. Lesegerät nach einem der Ansprüche 27 bis 31, **dadurch gekennzeichnet, dass** es eine Schnittstelle für die Nahbereichskommunikation aufweist.

33. Lesegerät nach einem der Ansprüche 27 bis 32 **dadurch gekennzeichnet, dass** es angepaßt ist zum Lesen eines kontaktlosen Datenträgers nach einem der Ansprüche 1 bis 16.

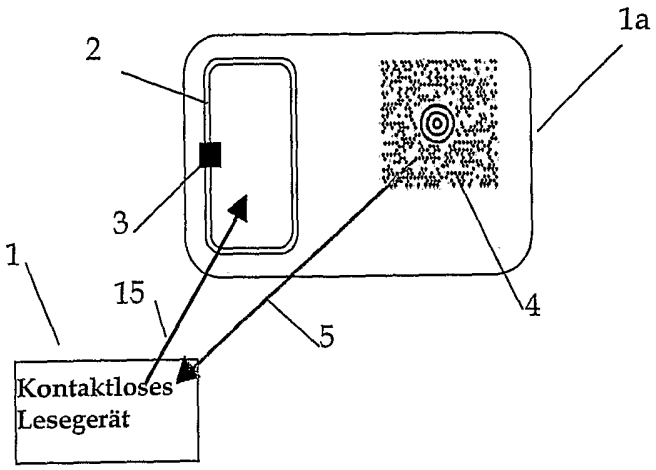

2
1a
3
1
15
4
5
Kontaktloses
Lesegerät

Fig. 1

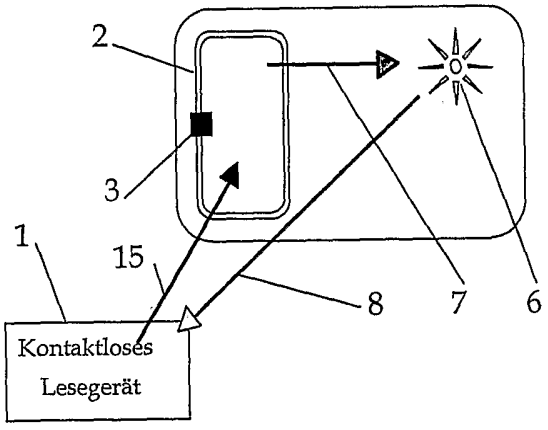

2
3
1
15
8
7
6
Kontaktloses
Lesegerät

Fig. 2

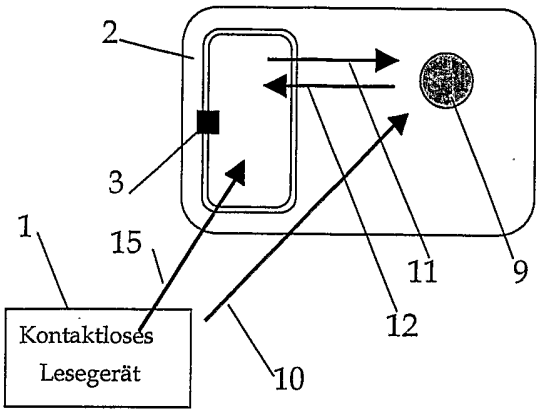

2
3
1
15
11
9
12
Kontaktloses
Lesegerät
10

Fig. 3

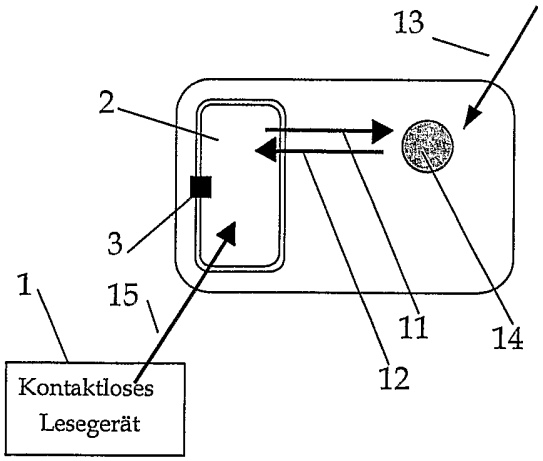

13
2
3
1
15
11
14
12
Kontaktloses
Lesegerät

Fig. 4

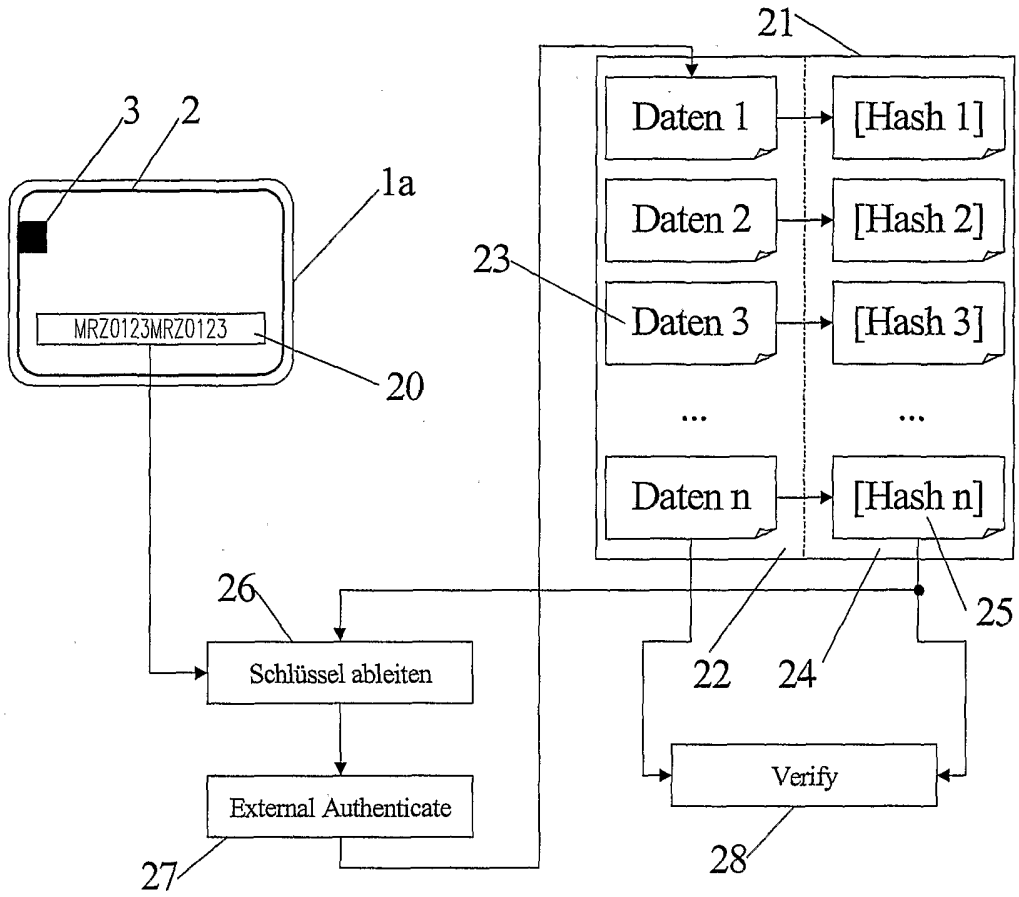

21
3
2
1a
MRZ0123MRZ0123
20
23
Daten 1
[Hash 1]
Daten 2
[Hash 2]
Daten 3
[Hash 3]
...
...
Daten n
[Hash n]
26
25
22
24
Schlüssel ableiten
External Authenticate
Verify
27
28

Fig. 5

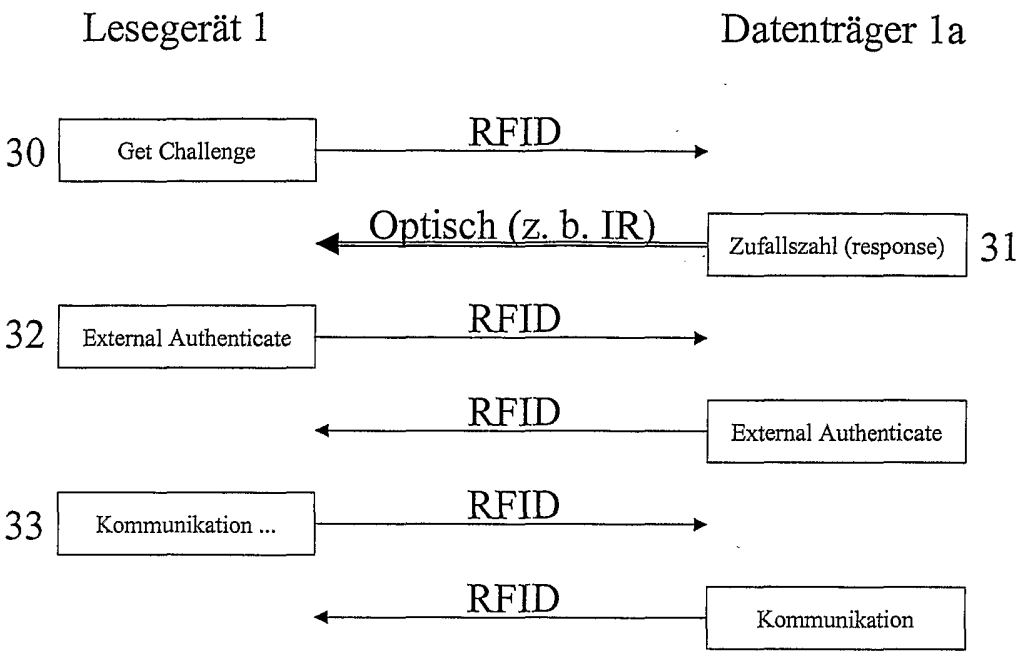

Lesegerät 1
Datenträger 1a
30
Get Challenge
RFID
Optisch (z. b. IR)
Zufallszahl (response)
31
32
External Authenticate
RFID
RFID
External Authenticate
33
Kommunikation ...
RFID
RFID
Kommunikation

Fig. 6