

(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
16. Februar 2006 (16.02.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/015573 A1

(51) Internationale Patentklassifikation⁷: **G06K 19/07**

(21) Internationales Aktenzeichen: PCT/DE2005/001293

(22) Internationales Anmeldedatum:
22. Juli 2005 (22.07.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 039 365.6 12. August 2004 (12.08.2004) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **WINCOR NIXDORF INTERNATIONAL GMBH**
[DE/DE]; Heinz-Nixdorf-Ring 1, 33106 Paderborn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): **HASSENBUERGER,**
Anneliese [DE/DE]; Am Damm 3-9, 33100 Paderborn

(DE). **REIMER, Bernd** [DE/DE]; Mentropstrasse 50,
33106 Paderborn (DE).

(74) Gemeinsamer Vertreter: **WINCOR NIXDORF IN-**
TERNATIONAL GMBH; Heinz-Nixdorf-Ring 1, 33106
Paderborn (DE).

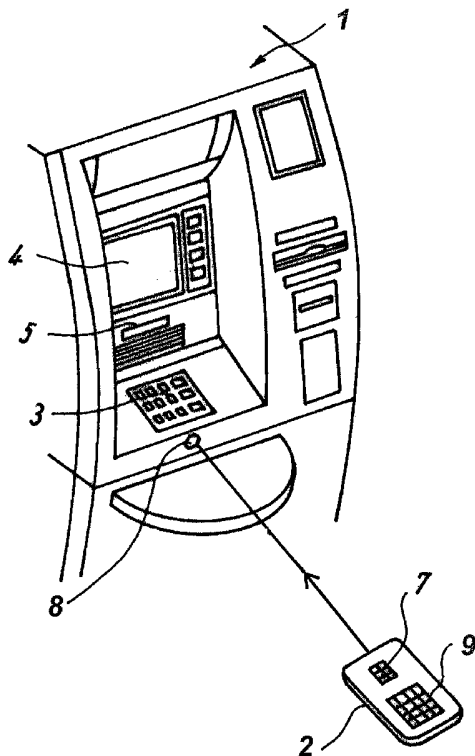
(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KP, KR, KZ, LC, LK, LR,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

[Fortsetzung auf der nächsten Seite]

(54) Title: DATA CARRIER FOR THE CONTACTLESS TRANSMISSION OF ENCRYPTED DATA SIGNALS

(54) Bezeichnung: DATENTRÄGER ZUR KONTAKTLOSEN ÜBERTRAGUNG VON VERSCHLÜSSELTEN DATENSIGNA-
LEN



(57) Abstract: The invention relates to a data carrier for the
secure transmission of data signals. Said data carrier com-
prises an RFID transponder (7) for storing and transmitting
data to a reader; an input device (9) for inputting data; at
least one encryption device (14) for encrypting data; a control
device (14) for processing data; and at least one circuit device
(13) for influencing the RFID transponder (7) and/or the input
and encrypted stored data.

(57) Zusammenfassung: Für die sichere Übertragung von
Datensignalen ist ein Datenträger vorgesehen mit: einem
RFID-Transponder (7) zum Speichern und Übertragen
von Daten an ein Lesegerät; einer Eingabeeinrichtung
(9) zur Eingabe von Daten; zumindest einer Verschlüsse-
lungseinrichtung (14) zum Verschlüsseln von Daten; einer
Steuerungseinrichtung (11) zur Verarbeitung von Daten; und
mindestens einer Schalteinrichtung (13) zur Beeinflussung
des RFIDTransponders (7) und/oder der eingegebenen und
verschlüsselten gespeicherten Daten.

WO 2006/015573 A1



GH, GM, KE, LS, MW, MZ, NA, 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, IS, IT, LT, LU, LV, 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).

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.

Veröffentlicht:

— mit internationalem Recherchenbericht

Datenträger zur kontaktlosen Übertragung von verschlüsselten Datensignalen

- 5 Die Erfindung betrifft einen Datenträger zur kontaktlosen Übertragung von verschlüsselten Datensignalen an ein Lesegerät, ein Verfahren zum Betreiben des Datenträgers sowie ein Selbstbedienungsgerät mit einem Lesegerät für den Datenträger.
- 10 An Selbstbedienungsgeräten wie zum Beispiel Geldautomaten, Überweisungsterminals, Bezahlterminals im Einzelhandel und dergleichen sind für die Durchführung einer Transaktion Kartenleser für das Lesen und Beschreiben von Datenträgern wie Magnetstreifenkarten oder Chipkarten vorgesehen. Aus
- 15 Sicherheitsgründen muss zudem oft noch ein Passwort, das heißt eine persönliche Geheimzahl, eine so genannte PIN-Nummer, zur Autorisierung des Benutzers eingegeben werden. Nur so kann beispielsweise eine Auszahlung oder eine Überweisung erfolgen. Diese PIN-Nummer wird üblicherweise innerhalb der Tastatur des
- 20 Selbstbedienungsgerätes verschlüsselt und gesichert weiter an einen übergeordneten Rechner übertragen. Solche Tastaturen werden als EPP (= Encrypted Pin Pad) bezeichnet.
- Bei Manipulationsversuchen wird versucht, den vom Benutzer am
- 25 Selbstbedienungsgerät eingeführten Datenträger zu kopieren und die dazugehörige PIN-Nummer auszuspähen. Das Kopieren der Magnet- oder Chipkarte erfolgt vorzugsweise durch Vorbauten am Kartenleser. Das Ausspähen der PIN-Nummer bei ihrer Eingabe erfolgt beispielsweise durch Einsatz einer an der Tastatur des Terminals
- 30 installierten Miniaturkamera mit Übertragungseinrichtung.

Die Erfindung hat daher die Aufgabe, ein Selbstbedienungsgerät zu schaffen, das eine erhöhte Sicherheit gegenüber Manipulationen bietet.

Die Lösung der Aufgabe erfolgt durch den Gegenstand des Anspruchs 1 und durch das Verfahren nach Anspruch 9.

Die Erfindung schafft einen Datenträger zur Eingabe und Übertragung
5 von verschlüsselten Datensignalen an ein Lesegerät mit einem RFID-
Transponder zum Speichern und Übertragen von Datensignalen, einer
Eingabeeinrichtung zur Eingabe von Daten, einer
Verschlüsselungseinrichtung zum Verschlüsseln von Daten, einer
Steuerungseinrichtung zur Verarbeitung von Daten, sowie mit
10 mindestens einer Schalteinrichtung zur Beeinflussung des RFID-
Transponders und/oder der eingegebenen und verschlüsselten
gespeicherten Daten.

Durch einen Datenträger mit einem RFID-Transponder ist eine
15 kontaktlose Übertragung von Datensignalen zwischen dem Datenträger
und dem Lesegerät, das vorzugsweise in einem Selbstbedienungsgerät
eingebaut ist, möglich. Die Datensignale zwischen dem Datenträger
und dem Lesegerät werden verschlüsselt mittels geheimer
kryptographischer Schlüssel übertragen. Manipulationsversuche wie an
20 herkömmlichen Kartenleser können somit nicht mehr auftreten.

Der Datenträger enthält eine Eingabevorrichtung zur Eingabe
alphanumerischer Zeichen wie einer PIN, um eine autorisierte
Benutzung des Datenträgers nur durch die berechtigte Person
25 sicherzustellen. Der Datenträger weist eine Verschlüsselungs-
vorrichtung auf, um die eingegebene Geheimnummer zu verschlüsseln.
Durch Eingabe einer PIN oder einer anderen Tastenkombination kann
eine Freischaltung des RFID-Transponders und somit die Übertragung
der gespeicherten Daten bewirkt werden. Der Benutzer kann somit vor
30 einem Selbstbedienungsgerät den Datenträger aktivieren. Dabei kann
vorgesehen werden, dass die Eingabe der PIN bereits für eine
Autorisierung der gewünschten Transaktion ausreichend ist, da im
Datenträger die eingegebene PIN oder der eingegebene Code mit
einem zuvor gespeicherten Code verglichen wird und nur bei einer
35 Übereinstimmung der RFID-Transponder aktiviert wird. Es ist jedoch

auch möglich, dass die PIN getrennt von den Daten des RFID-Transponders verschlüsselt an das Lesegerät des Selbstbedienungsgerätes gesendet werden und im Selbstbedienungsgerät die Autorisierung des Datenträgers vorgenommen wird. Kann keine gültige
5 Autorisierung festgestellt werden, so wird die Kommunikation zwischen dem Datenträger und dem Lesegerät abgebrochen.

Es ist in weiterer bevorzugter Ausführung zweckmäßig, dass die
10 Steuereinrichtung mindestens einen Prozessor, einen Speicher und eine Verschlüsselungseinrichtung aufweist, damit eine Be- und Verarbeitung der eingegebenen Daten wie an einem Selbstbedienungsgerät erfolgen kann.

In einer weiteren Ausgestaltung weist der erfindungsgemäße
15 Datenträger eine Sensorik zur Abtastung biometrischer Daten auf. Diese zusätzliche Sicherheit gewährleistet einerseits, dass nur der autorisierte Benutzer den Datenträger verwenden kann, und andererseits, dass bei einem Verlust eine vorteilhaft noch höhere Sicherheitsstufe vorhanden ist.

20 Für eine vorteilhafte Kommunikation des erfindungsgemäßen Datenträgers mit dem jeweiligen Selbstbedienungsgerät ist es zweckmäßig, dass der RFID-Transponder zum Ein- und Auslesen und somit für einen zweiseitigen Datenaustausch mit dem Lesegerät
25 ausgebildet ist.

In einer weiteren bevorzugten Ausführungsform ist der erfindungsgemäße Datenträger als Chipkarte mit den Merkmalen
30 zumindest des Anspruches 1 ausgebildet. Hierdurch ist eine besonders vorteilhafte Gestaltung mit geringen Abmessungen erreicht, welche eine einfache und bequeme Handhabung ermöglicht.

Vorzugsweise ist die Vorrichtung schließlich mit einer Anzeigeeinrichtung zur Anzeige von Daten und/oder einem Energiespeicher zum autarken Betrieb versehen.

5 Die Erfindung schafft außerdem ein Verfahren zum Übertragen von verschlüsselten Datensignalen mit dem erfindungsgemäßen Datenträger zu einem Lesegerät mit folgenden Verfahrensschritten:

- (a) Einlesen von mittels einer Eingabeeinrichtung eingegebenen Daten;
- 10 (b) Verschlüsseln dieser eingelesenen Datenwerte mittels einer Verschlüsselungseinrichtung und Speichern der verschlüsselten Daten;
- (c) Durchführen einer Autorisierung des Datenträgers durch einen Vergleich zwischen den eingegebenen und verschlüsselten Datenwerten und bereits gespeicherten Datenwerten auf dem Datenträger und/oder zwischen dem
15 Datenträger und dem Lesegerät ;
- (d) Freischalten des RFID-Transponders;
- (e) Übertragen von gespeicherten Datensignalen des RFID-
20 Transponders und/oder der eingegebenen und verschlüsselten Datenwerte zum Lesegerät unter Verwendung eines geheimen Schlüssels.

25 Dieses Verfahren kann vorteilhaft in der Steuereinrichtung der erfindungsgemäßen Vorrichtung durch ein geeignetes Softwareprogramm von dem Prozessor ausgeführt werden. Dabei ist es ebenfalls von großem Vorteil, wenn in einer bevorzugten Ausgestaltung im Verfahrensschritt (a) ein vorgegebenes Passwort oder eine Geheimzahl eingegeben wird und/oder biometrische Daten des
30 Benutzers mittels einer Sensorik eingelesen werden, und dass bei falschen Eingabewerten nach einer vorgebbaren Anzahl von Wiederholungen die Vorrichtung deaktiviert wird.

In einer anderen, besonders vorteilhaften Ausführungsform kann im Verfahrensschritt (a) die Eingabe von Daten für einen vollständigen Bedienungsvorgang für ein Selbstbedienungsgerät durchgeführt werden, wie insbesondere auch die Eingabe des abzuhebenden Geldbetrages. Dadurch ist eine weitere hohe Sicherheitsstufe gegen Manipulationen gegeben, da der vollständige Eingabevorgang am Selbstbedienungsgerät vor Ort entfällt und vom Benutzer an einem von ihm gewählten sicheren Ort vorgenommen werden kann.

Die Sicherheit des Verfahrens ist insgesamt durch kryptografische Schlüssel und kryptografische Verfahren und die Verwendung von RFID-Transpondern gegeben.

Weitere vorteilhafte Ausführungsformen der Erfindung sind in den Unteransprüchen aufgeführt.

Die Erfindung wird nun mit Bezug auf die beigefügte Zeichnung anhand eines Ausführungsbeispiels erläutert. Hierbei zeigt:

Figur 1 eine perspektivische Ansicht eines Geldautomaten bei einer Anwendung; und

Figur 2 ein beispielhaftes Blockschaltbild eines erfindungsgemäßen Datenträgers in Form einer Chipkarte.

Ein Geldautomat 1 ist in Figur 1 als Beispiel für ein Selbstbedienungsgerät dargestellt. Vor dem Geldautomaten 1 ist ein als Chipkarte 2 ausgebildeter Datenträger während einer Datenübertragung zu dem Geldautomaten 1 dargestellt.

Üblicherweise wird an einem Geldautomaten bei einer gewünschten Transaktion zunächst eine kontaktbehaftete Chipkarte mit einem Chip

und/oder einem Magnetstreifen in einen Kartenleser des Gerätes gesteckt. Auf dem Chip und/oder dem Magnetstreifen befinden sich Daten des Benutzers wie sein Name und seine Kontonummer. Nach dem Lesen der Chipkarte wird die Verbindung zu einem Host
5 aufgenommen, der die eingelesenen Daten mit abgespeicherten Daten vergleicht und eine Autorisierung der gewünschten Transaktion ermöglicht. Zusätzlich wird über eine Tastatur 3 ein Passwort oder eine Geheimzahl, ein so genannter PIN-Code eingegeben, damit ein bestimmter Vorgang, beispielsweise eine Auszahlung, vorgenommen
10 werden kann. Diese zusätzliche PIN dient der Sicherheit, so dass Dritte ohne Kenntnis der Geheimzahl keine Transaktionen am Geldautomaten durchführen können. Die Eingabeaufforderungen und Reaktionen des Selbstbedienungsgerätes werden an einem Bildschirm 4 zur Bedienerführung angezeigt. Beim Auszahlungsvorgang wird das
15 entsprechende Geld über eine Ein-/Ausgabereinrichtung 5 in bekannter Weise ausgegeben.

Anstelle der Eingabe einer Chipkarte in den Kartenleser sieht die Erfindung eine kontaktlose Übertragung der Daten vor. Hierzu ist ein
20 Datenträger vorgesehen, der vorteilhafterweise als Chipkarte 2 ausgebildet ist. Die Chipkarte 2 ist mit einem RFID-Transponder 7 bestehend aus einer Spule und einem integrierten Mikrochip als Datenspeicher versehen, wobei der Transponder 7 auslesbar und beschreibbar ist. Die Daten des RFID-Transponders 7 können von
25 einem RFID-Lesegerät 8 des Geldautomaten 1 ausgelesen werden. Zudem kann das RFID-Lesegerät 8 neue Daten zum Transponder 7 senden. Das Lesegerät 8 überträgt neben Daten auch Energie durch induktive Kopplung zur Chipkarte 2. Am Standort des Geldautomaten 1 wird, wie in Figur 1 dargestellt, die in dem RFID-Transponder 7
30 gespeicherten Daten über eine Übertragungsstrecke an das RFID-Lesegerät 8 des Geldautomaten 1 übertragen. Der Kunde muss die Karte 2 nicht mehr in den Kartenleser stecken, sondern hält ihn vor das RFID-Lesegerät 8. Falls über einen längeren Zeitraum Daten vom RFID-Transponder 7 ein- und ausgelesen werden, so ist der
35 Geldautomat 1 vorteilhafterweise mit einer Mulde oder sonstigen Ablagemöglichkeit versehen, so dass der Kunde sie aus der Hand nehmen und während der Transaktion ablegen kann.

Vorzugsweise werden RFID-Transponder 7 eingesetzt, die eine Reichweite von 10 – 20 cm aufweisen, damit ein Auslesen des RFID-Transponders 7 nur in der unmittelbaren Umgebung des Lesegerätes 8 erfolgen kann.

Um die Sicherheit der Datenübertragung sicherzustellen, ist ein Schreib- und Lesezugriff auf die Chipkarte 2 nur nach einer Autorisierung der Chipkarte 2 gegenüber dem Lesegerät 8 möglich. Der Datenträger 2 enthält eine Eingabevorrichtung 9 zur Eingabe alphanumerischer Zeichen wie einer PIN, um eine autorisierte Benutzung des Datenträgers nur durch die berechnigte Person sicherzustellen. Hierzu werden kryptographische Schlüssell zwischen der Chipkarte 2 und dem Lesegerät 8 ausgetauscht bzw. überprüft, ob kryptographische Schlüssell in der Chipkarte 2 und dem Lesegerät 8 gespeichert sind. Der nach der Autorisierung folgende Datenaustausch zwischen der Chipkarte 2 und dem Lesegerät 8 wird gleichfalls verschlüsselt, um ein Ausspähen der übertragenen Daten durch Abhören der Funkverbindung zwischen der Chipkarte 2 und dem Lesegerät 8 zu verhindern. Da die Datensignale kontaktlos übertragen werden und ein zweiseitiger Austausch zwischen dem Datenträger 2 und dem RFID-Lesegerät 8 möglich ist, ist eine kryptographisch sichere Datenübertragung möglich, die ein Ausspähen der übertragenen Daten erheblich erschwert. Somit ist ein wirksamer Schutz vor Manipulationen während der Datenübertragung erreicht. Die Sicherheit der Datenübertragung ist somit insgesamt durch kryptografische Schlüssell und kryptografische Verfahren und die Verwendung von RFID-Transpondern gegeben.

Während bei kontaktbehafteten Chipkarten es automatisch sichergestellt ist, dass im Lesegerät immer nur eine einzige Karte ausgelesen wird, muss bei kontaktlosen Karten verhindert werden, dass sich zur gleichen Zeit mehrere Karten im Ansprechbereich des Lesegerätes 8 befinden. Hierzu ist das Lesegerät 8 mit Antikollisionssoftware versehen, um die gezielte Kommunikation mit einer Chipkarte 2 sicherzustellen.

Im folgenden wird unter Bezugnahme auf Fig. 2 der Aufbau der Chipkarte 2 noch näher beschrieben. Da übliche RFID-Transponder passiv ausgebildet sind und ausgelesen werden, sobald sie in die Reichweite eines RFID-Lesegerätes kommen, ist die Chipkarte 2 mit einer Eingabevorrichtung 9 zur Eingabe eines Aktivierungssignals versehen, um die Übertragung der Daten von dem RFID-Transponder 7 an das Lesegerät 8 freizuschalten und somit eine zufällige Übertragung der Daten an das RFID-Lesegerät 8 zu verhindern. Um die Sicherheit der Karte 2 bei einem Verlust zu erhöhen, ist die Eingabevorrichtung 9 vorzugsweise als Eingabetastatur zur Eingabe einer Geheimzahl wie insbesondere einer PIN oder eines Codes ausgebildet. Die Eingabetastatur ist mit Tastenelementen 10 für die Eingabe von alphanumerischen Zeichen sowie auch von anderen Steuerzeichen versehen. Sie ist mit einer Steuereinrichtung 11 verbunden. Die Bedienerführung des Benutzers zur korrekten Eingabe in die Eingabetastatur 9 kann über eine Anzeigeeinrichtung 12 erfolgen. Die Anzeigeeinrichtung 12 ist in dieser Ausführung mit der Steuereinrichtung 11 verbunden. Sie kann jedoch auch einen eigenen Prozessor oder eine eigene Steuereinrichtung besitzen.

An die Steuereinrichtung 11 ist der RFID-Transponder 7 sowie eine Schalteinrichtung 13 angeschlossen. Diese Schalteinrichtung 13 aktiviert den RFID-Transponder 7 zur Übertragung der gespeicherten Daten an den Geldautomaten 1. In der Steuereinrichtung 11 befindet sich eine Verschlüsselungseinrichtung 14, ein Prozessor 15 und ein nicht dargestellter Speicher. Die Verschlüsselungseinrichtung 14 und der Speicher können ebenfalls außerhalb der Steuereinrichtung 11 angeordnet sein.

30

Die Chipkarte 2 weist in einer weiteren Ausgestaltung eine Sensorik 16 mit einem Kontaktfeld 17 auf, welches für die Abtastung biometrischer Daten vorgesehen ist, wie zum Beispiel ein Fingerabdrucksensor. Diese Sensorik 16 kann zusätzlich oder anstelle einer PIN-Eingabe zur Autorisierung des Benutzers verwendet werden.

35

Vorzugsweise ist die Chipkarte mit einem Energiespeicher 18 versehen, der die notwendige elektrische Energie zum Betrieb der Chipkarte zur Verfügung stellt. Es ist vorzugsweise eine
5 wiederaufladbare Batterie. Das Wiederaufladen kann durch Induktion drahtlos oder drahtgebunden über Kontaktfelder in einer entsprechenden, nicht dargestellten Einrichtung erfolgen. Da der Betrieb der Chipkarte 2 nur kurzfristig erfolgt, ist der Energiebedarf äußerst gering.

10

Im Weiteren wird der Betrieb der Chipkarte 2 näher erläutert. Die Chipkarte 2 wird über die Eingabeeinrichtung 9 eingeschaltet. Die Steuereinrichtung 11 gibt den Eingabeablauf über die Anzeigeeinrichtung 12 dem Benutzer vor. Der Benutzer wird
15 aufgefordert, seine PIN-Nummer und/oder ein Passwort einzugeben, welche/welches mit einem gespeicherten Referenzwert verglichen wird. Dieser gespeicherte Referenzwert kann von dem die Chipkarte 2 ausgebenden Geldinstitut gespeichert sein. Dabei kann vorgesehen werden, dass die Eingabe der PIN bereits für eine Autorisierung der
20 gewünschten Transaktion ausreichend ist, da im Datenträger 2 die eingegebene PIN oder der eingegebene Code mit einem zuvor gespeicherten Code verglichen wird und nur bei einer Übereinstimmung der RFID-Transponder 7 aktiviert wird.

25 Es ist jedoch auch möglich, dass die PIN getrennt von den Daten des RFID-Transponders 7 verschlüsselt an das Lesegerät 8 des Selbstbedienungsgerätes gesendet werden und im Selbstbedienungsgerät die Autorisierung des Datenträgers 2 vorgenommen wird. Kann keine gültige Autorisierung festgestellt
30 werden, so wird die Kommunikation zwischen dem Datenträger 2 und dem Lesegerät 8 abgebrochen. Für die Übertragung der verschlüsselten PIN kann im Datenträger 2 eine weitere Übertragungseinrichtung, die beispielsweise als Nahfunkverbindung wie Bluetooth ausgebildet ist, vorgesehen sein.

35

Der so geprüfte beziehungsweise eingegebene Datenwert wird mittels der Steuereinrichtung 11 gespeichert und mit der Verschlüsselungseinrichtung 14 verschlüsselt und gespeichert. Das erste Speichern kann auch unterbleiben. Nach erfolgreicher
5 Autorisierung erfolgt ein Freischalten der Chipkarte 2 mittels der Schalteinrichtung 13 und die Daten können von dem RFID-Transponder 7 ausgelesen werden. Dieser Übertragungsvorgang erfolgt automatisch nach Eingabe der PIN oder indem der Benutzer die Chipkarte 2 am Standort des Selbstbedienungsgerätes 1 durch eine
10 Tastenkombination an der Eingabeeinrichtung 9 aktiviert.

Es ist auch möglich, dass der Benutzer zunächst die Chipkarte 2 aktiviert und erste Daten übertragen werden und der Benutzer dann vom Selbstbedienungsgerät 1 aufgefordert wird, seine PIN-Nummer
15 einzugeben. Der Benutzer gibt dann auf der Chipkarte 2 eine entsprechende Tastenkombination ein und bringt dann die Chipkarte 2 in den Empfangsbereich des Lesegerätes 8 des Selbstbedienungsgerätes 1.

20 Weiterhin kann die Steuereinrichtung 11 der Chipkarte 2 eine solche Software aufweisen, mit welcher der gesamte Bedienerführungsvorgang des Selbstbedienungsgerätes 1 vorab an einem für den Benutzer sicheren Ort durchgeführt werden kann. Das bedeutet, dass der Benutzer am Standort des Selbstbedienungs-
25 gerätes 1 nur noch dieses aktivieren muss, die verschlüsselten Daten mit seiner Chipkarte 2 überträgt und so der gesamte Vorgang, beispielsweise der Dateneingabe zur Geldausgabe, von der Datenübertragung der Chipkarte 2 übernommen wird.

PATENTANSPRÜCHE

- 5 1. Datenträger zur Übertragung von verschlüsselten Datensignalen
 an ein Lesegerät (8) mit:
- a) einem RFID-Transponder (7) zum Speichern und Übertragen
 von Daten an ein Lesegerät;
- 10 b) einer Eingabeeinrichtung (9) zur Eingabe von Daten;
- c) zumindest einer Verschlüsselungseinrichtung (1) zum
 Verschlüsseln von Daten;
- d) einer Steuerungseinrichtung (11) zur Verarbeitung von
 Daten; und
- 15 e) mindestens einer Schalteinrichtung (13) zur Beeinflussung
 des RFID-Transponders (7) und/oder der eingegebenen und
 verschlüsselten gespeicherten Daten.
- 20 2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, dass
 der RFID-Transponder (7) einen integrierten Mikrochip aufweist
 und zum Ein- und Auslesen von Daten geeignet ist.
3. Datenträger nach Anspruch 1 oder 2, gekennzeichnet durch
 einen Energiespeicher (18).
- 25 4. Datenträger nach einem der vorhergehenden Ansprüche,
 gekennzeichnet durch eine Anzeigeeinrichtung (12) zur Anzeige
 von Daten.
- 30 5. Datenträger nach einem der vorstehenden Ansprüche,
 gekennzeichnet durch eine weitere Übertragungseinrichtung zur
 Übertragung von eingegebenen und verschlüsselten Daten.
6. Datenträger nach einem der vorstehenden Ansprüche, dadurch
 gekennzeichnet, dass die Steuereinrichtung (11) mindestens

einen Prozessor (15) und eine Verschlüsselungseinrichtung (14) aufweist.

- 5 7. Datenträger nach einem der vorstehenden Ansprüche, gekennzeichnet durch eine Sensorik (16) zur Abtastung biometrischer Daten.
8. Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der Datenträger eine Chipkarte (2) ist.
- 10 9. Verfahren zum Übertragen von verschlüsselten Daten mit dem erfindungsgemäßen Datenträger nach einem oder mehreren der Ansprüche 1-8, gekennzeichnet durch folgende Schritte:
- 15 (a) Einlesen von mittels einer Eingabeeinrichtung (9) eingegebenen Daten;
- (b) Verschlüsseln dieser eingelesenen Datenwerte mittels einer Verschlüsselungseinrichtung (14) und Speichern der verschlüsselten Daten;
- 20 (c) Durchführen einer Autorisierung des Datenträgers durch einen Vergleich zwischen den eingegebenen und verschlüsselten Datenwerten und bereits gespeicherten Datenwerten auf dem Datenträger und/oder zwischen dem Datenträger und dem Lesegerät (8);
- (d) Freischalten des RFID-Transponders (7);
- 25 (e) Übertragen von gespeicherten Datensignalen des RFID-Transponders (7) und/oder der eingegebenen und verschlüsselten Datenwerte zum Lesegerät (8) unter Verwendung eines geheimen Schlüssels.
- 30 10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass im Verfahrensschritt (a) „Einlesen“ ein Passwort oder eine Geheimzahl angefordert wird und/oder biometrische Daten des Benutzers mittels einer Sensorik (16) eingelesen werden, und dass bei falschen Eingabewerten nach einer vorgebbaren Anzahl von Wiederholungen die Vorrichtung deaktiviert wird.

11. Verfahren nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass im Verfahrensschritt (a) „Einlesen“ die Eingabe von Daten für einen vollständigen Bedienungsvorgang für ein Selbstbedienungsgerät (2) durchgeführt wird.
- 5 12. Selbstbedienungsgerät wie ein Geldautomat, ein Kioskterminal, ein Multifunktionsterminal, ein Bezahlterminal im Einzelhandel mit einem RFID-Leserät (8) für einen Datenträger (2) nach einem oder mehreren der Ansprüche 1 bis 8.

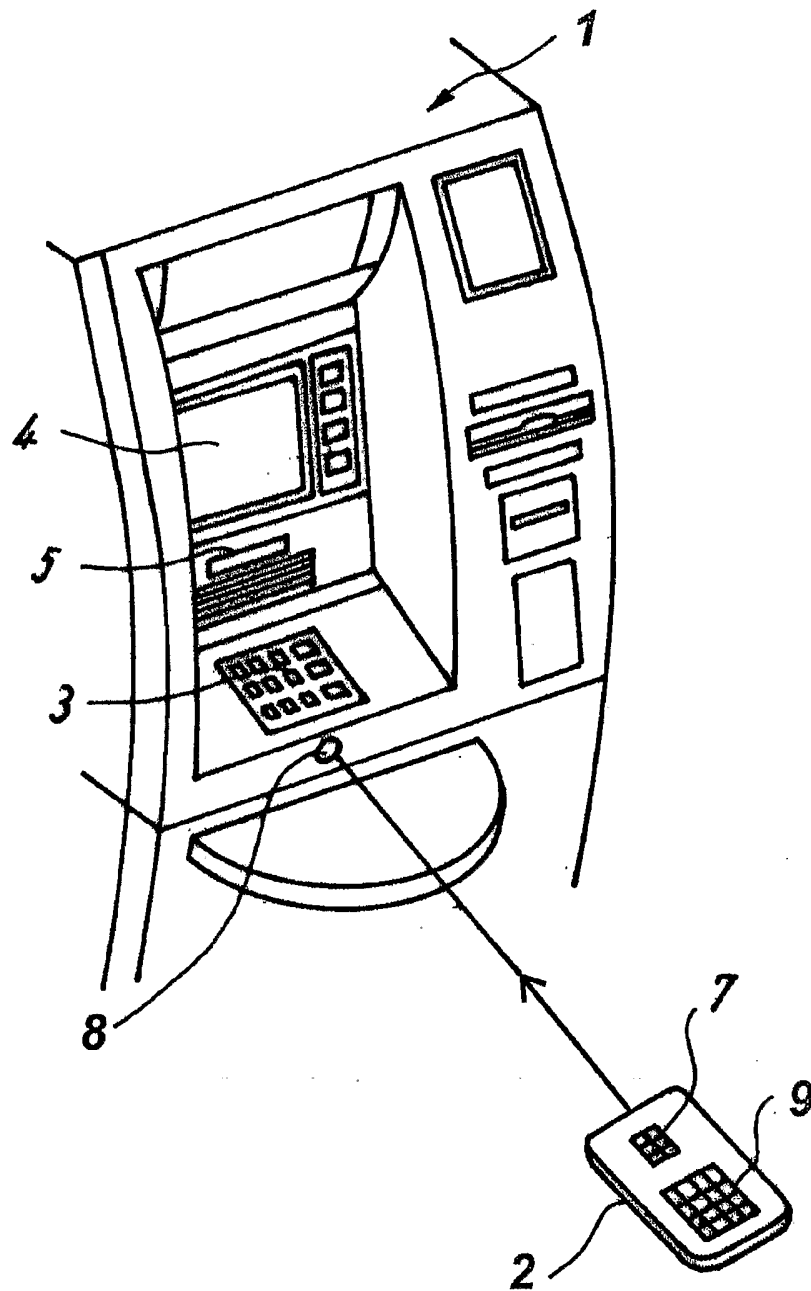


Fig. 1

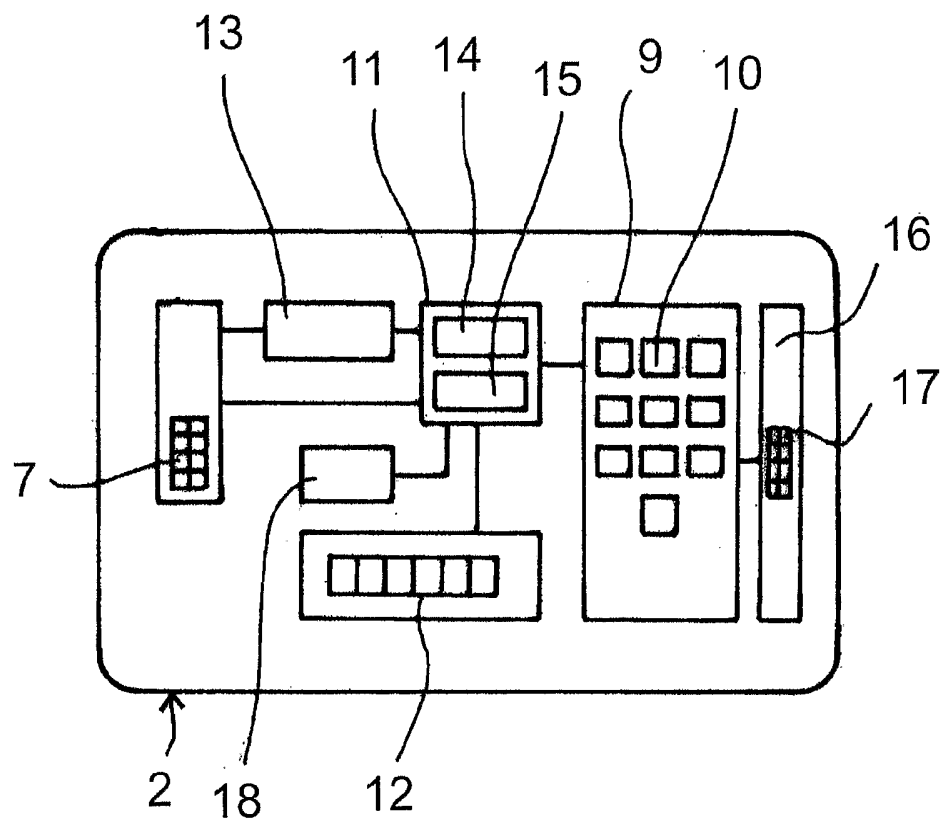


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No

PCT/DE2005/001293

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06K19/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/167207 A1 (BERARDI MICHAEL J ET AL) 4 September 2003 (2003-09-04) paragraphs '0063! - '0067!, '0070!, '0140! - '0142!; figures 2,3,9	1-12
X	US 5 748 737 A (DAGGAR ET AL) 5 May 1998 (1998-05-05) column 10, line 5 - line 64; figure 2A	1-8
X	US 6 257 486 B1 (TEICHER MORDECHAI ET AL) 10 July 2001 (2001-07-10) column 16, line 51 - line 58; figure 15B	1-8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

28 September 2005

Date of mailing of the international search report

26/10/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fichter, U

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE2005/001293

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2003167207	A1	04-09-2003	NONE	
US 5748737	A	05-05-1998	NONE	
US 6257486	B1	10-07-2001	EP 1004980 A2	31-05-2000

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE2005/001293

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G06K19/07

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2003/167207 A1 (BERARDI MICHAEL J ET AL) 4. September 2003 (2003-09-04) Absätze '0063! - '0067!, '0070!, '0140! - '0142!; Abbildungen 2,3,9	1-12
X	US 5 748 737 A (DAGGAR ET AL) 5. Mai 1998 (1998-05-05) Spalte 10, Zeile 5 - Zeile 64; Abbildung 2A	1-8
X	US 6 257 486 B1 (TEICHER MORDECHAI ET AL) 10. Juli 2001 (2001-07-10) Spalte 16, Zeile 51 - Zeile 58; Abbildung 15B	1-8



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

28. September 2005

Absenddatum des internationalen Recherchenberichts

26/10/2005

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Fichter, U

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE2005/001293

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2003167207 A1	04-09-2003	KEINE	
US 5748737 A	05-05-1998	KEINE	
US 6257486 B1	10-07-2001	EP 1004980 A2	31-05-2000