

(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
23. März 2006 (23.03.2006)

PCT

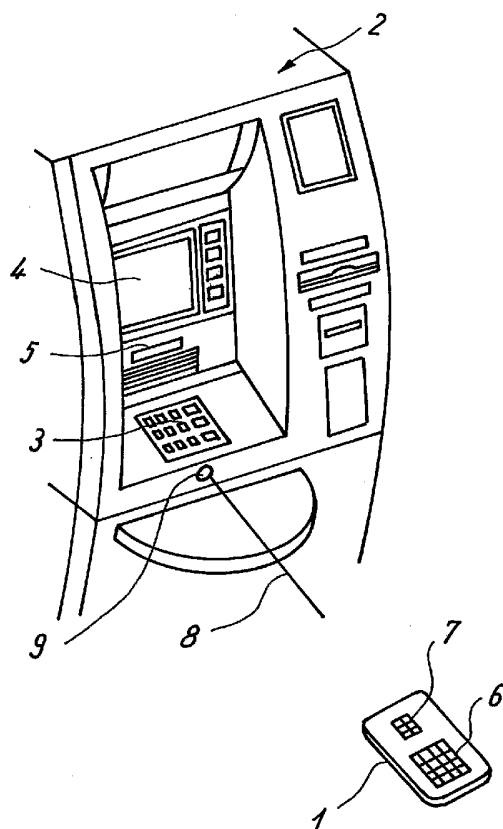
(10) Internationale Veröffentlichungsnummer
WO 2006/029596 A1

- (51) Internationale Patentklassifikation⁷: **G07F 7/10**, 19/00
- (21) Internationales Aktenzeichen: PCT/DE2005/001561
- (22) Internationales Anmeldedatum:
7. September 2005 (07.09.2005)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2004 044 914.7
14. September 2004 (14.09.2004) DE
10 2005 005 378.5 5. Februar 2005 (05.02.2005) 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): **OSTERHOLZ, Gerhard** [DE/DE]; Kleeweg 21, 33154 Salzkotten (DE).
SCHLIEBE, Dieter [DE/DE]; Am Südhang 53, 33181 Bad Wünnenberg (DE).
- (74) Gemeinsamer Vertreter: **WINCOR NIXDORF INTERNATIONAL 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,

[Fortsetzung auf der nächsten Seite]

(54) Title: DEVICE FOR ENTERING AND TRANSMITTING ENCRYPTED SIGNALS

(54) Bezeichnung: VORRICHTUNG ZUR EINGABE UND ÜBERTRAGUNG VON VERSCHLÜSSELTEN SIGNALEN



(57) Abstract: The invention relates to a device for transmitting encrypted data signals and to a method that uses said device. The method comprises the following steps: a) reading and storing of data values that have been input using an entry device (6); b) encryption of the read data values using an encryption device (16) and storing of the encrypted data values; c) release of the transmission device (13) within a predeterminable time period; d) transmission of the stored encrypted data signals; and e) deactivation of the transmission device (13) after the predeterminable interval.

(57) Zusammenfassung: Eine Vorrichtung sowie ein Verfahren zum Übertragen von verschlüsselten Datensignalen mit dieser Vorrichtung arbeiten nach folgenden Schritten: a) Einlesen und Speichern von mittels einer Eingabeeinrichtung (6) eingegebenen Datenwerten; b) Verschlüsseln dieser eingelesenen Datenwerte mittels einer Verschlüsselungseinrichtung (16) und Speichern der verschlüsselten Datenwerte; c) Freischalten der Übertragungseinrichtung (13) innerhalb eines vorgebbaren Zeitintervalls; d) Übertragen der gespeicherten verschlüsselten Datensignale; und e) Ausschalten der Übertragungseinrichtung (13) nach dem vorgebbaren Zeitintervall.

WO 2006/029596 A1



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.

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).

Veröffentlicht:

— mit internationalem Recherchenbericht

- (84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, 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,

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.

Vorrichtung zur Eingabe und Übertragung von verschlüsselten Signalen

- 5 Die Erfindung betrifft eine Vorrichtung zur Eingabe und Übertragung von verschlüsselten Signalen nach dem Oberbegriff des Anspruchs 1 und ein Verfahren zum Betreiben der Vorrichtung.

10 An bestimmten Selbstbedienungsgeräten, wie zum Beispiel Geldautomaten, Überweisungsterminals, Bezahlterminals im Einzelhandel und dergleichen, muss aus Sicherheitsgründen ein Passwort, das heißt eine persönliche Geheimzahl, eine so genannte PIN-Nummer, zur Autorisierung des Benutzers eingegeben werden. Nur so kann eine Auszahlung beziehungsweise eine Überweisung erfolgen. Diese PIN-Nummer wird üblicherweise innerhalb der Tastatur
15 des Selbstbedienungsgerätes verschlüsselt und gesichert weiter an einen übergeordneten Rechner übertragen. Solche Tastaturen werden als EPP (= Encrypted Pin Pad) bezeichnet.

20 Bei Manipulationsversuchen wird u.a. versucht, die vom Benutzer am Selbstbedienungsgerät eingeführte Magnetkarte zu kopieren und die dazugehörige PIN-Nummer auszuspähen. Dieses Ausspähen der PIN-Nummer bei ihrer Eingabe erfolgt beispielsweise auf die folgende Weise mit:

- einem vorzugsweise am Selbstbedienungsgerät oder über der Tastatur des Terminals installierten Spiegel,
- 25 - einer zusätzlichen Tastatur, die auf die Originaltastatur aufgesetzt wird, oder
- einer vorzugsweise am Selbstbedienungsgerät oder über der Tastatur des Terminals installierten Miniaturkamera mit Übertragungseinrichtung.

30 Ein seitlicher Sichtschutz am EPP hilft dagegen nur bedingt. Auch Hinweise an die Benutzer, mit der PIN-Nummer sorgfältig umzugehen und bei ihrer Eingabe zum Beispiel die andere Hand als Sichtschutz zu gebrauchen, werden in der Praxis zu wenig beachtet.

35 Es ist auch bekannt, die PIN-Nummer an einer separaten Vorrichtung einzugeben, so z.B. über ein Handy, mit dem die PIN-Nummer dann direkt und vorzugsweise drahtlos an das Selbstbedienungsgerät übertragen wird. Auch hier sollte die PIN-Nummer verschlüsselt übertragen werden.

Die Erfindung hat vor diesem Hintergrund die Aufgabe, eine Vorrichtung und ein Verfahren zum Betreiben der Vorrichtung zu schaffen, um Informationen, insbesondere eine Geheimnummer (PIN) in sicherer Weise an ein Selbstbedienungsgerät weiterzuleiten.

5

Die Lösung der Aufgabe erfolgt durch den Gegenstand des Anspruchs 1 und durch das Verfahren nach Anspruch 11.

10

Die Erfindung schafft eine Vorrichtung zur Eingabe und Übertragung von verschlüsselten Datensignalen mit einer Eingabeeinrichtung zur Eingabe von Zeichen; einer Verschlüsselungseinrichtung zum Verschlüsseln von Daten; einer Übertragungseinrichtung zum Übertragen von Daten; einer Steuerungseinrichtung zur Verarbeitung von Daten; sowie mit mindestens einer Schalteinrichtung zur Beeinflussung der Übertragungseinrichtung und der eingegebenen und verschlüsselten gespeicherten Daten und zum Freischalten der Übertragungseinrichtung innerhalb eines vorgebbaren Zeitintervalls.

15

Durch die vom Selbstbedienungsgerät unabhängige Vorrichtung ist es vorteilhaft möglich, dass der Benutzer seine Geheimnummer oder ein erforderliches Passwort zunächst in diese erfindungsgemäße Vorrichtung unabhängig vom Ort eines Selbstbedienungsgerätes oder dergleichen eingeben kann. Zweckmäßigerweise kann die Vorrichtung die eingegebene Geheimnummer in erforderlicher Weise verschlüsseln. Der Benutzer kann dann vor einem Selbstbedienungsgerät wie einem Geldautomaten die Übertragungseinrichtung der Vorrichtungen aktivieren und eine Übertragung des eingegebenen Codes zum Automaten veranlassen. Dabei lässt es sich vorteilhaft vorher festlegen, in welchem Zeitraum eine Übertragung der verschlüsselten Daten möglich ist. Nach Ablauf des Zeitraums wird die Vorrichtung automatisch deaktiviert, so dass eine weitere Übertragung der verschlüsselten Daten nicht mehr möglich ist. Eine Einschränkung auf eine einmalige Übertragung ist besonders vorteilhaft. Ein Verlust der Vorrichtung führt damit nicht automatisch zu einer Gefahr unbefugter Nutzung der Vorrichtung.

25

30

35

Weiterhin ist es zweckmäßig, dass die Schalteinrichtung auch zum Löschen von eingegebenen Daten nach dem Freischalten der Übertragung innerhalb eines vorgebbaren Zeitintervalls ausgebildet ist. Dadurch wird nach der Übertragung beziehungsweise nach dem Ablauf des vorher festgelegten Zeitintervalls auch ein gespeicherter Wert der Geheimzahl gelöscht, so dass ein missbräuchliches

Auslesen mittels besonderer Geräte nicht mehr möglich ist. Die Sicherheit wird somit vorteilhaft erhöht.

5 In einer weiteren bevorzugten Ausgestaltung ist die Übertragungseinrichtung der erfindungsgemäßen Vorrichtung zur Übertragung von Daten für eine drahtlose und/oder drahtgebundene Übertragungsstrecke ausgebildet. Zudem ist sie derart ausgebildet, dass sie für unterschiedliche Bautypen von Selbstbedienungsgeräten und Terminals eingesetzt werden kann.

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

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

20 Für eine vorteilhafte Kommunikation der erfindungsgemäßen Vorrichtung mit dem jeweiligen Selbstbedienungsgerät ist es zweckmäßig, dass die Übertragungseinrichtung für einen zweiseitigen Datenaustausch mit dem Selbstbedienungsgerät ausgebildet ist.

25 In einer weiteren bevorzugten Ausführungsform ist die erfindungsgemäße Vorrichtung als eine intelligente Chipkarte mit den Merkmalen zumindest des Anspruches 1 ausgebildet, insbesondere eine sogenannte Smart-Card. Hierdurch ist eine besonders vorteilhafte Gestaltung mit geringen Abmessungen erreicht, welche eine einfache und bequeme Handhabung ermöglicht.

30 Eine andere Ausführung sieht vor, dass die Vorrichtung aus einer Chip-Card und einem Übertragungsgerät, vorzugsweise einem Funktelefon, besteht. So können Geräte, die aus dem täglichen Leben nicht mehr wegzudenken sind, für die erfindungsgemäße Vorrichtung vorteilhaft zur Anwendung kommen.

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

Die Erfindung schafft außerdem ein Verfahren zum Übertragen von verschlüsselten Daten mit der erfindungsgemäßen Vorrichtung mit folgenden Verfahrensschritten:

- 5 (a) Einlesen und Speichern von mittels einer Eingabeeinrichtung eingegebenen Daten;
 - (b) Verschlüsseln dieser eingelesenen Daten mittels einer Verschlüsselungseinrichtung und Speichern der verschlüsselten Daten;
 - (c) Freischalten der Übertragungseinrichtung innerhalb eines vorgebbaren
10 Zeitintervalls;
 - (d) Übertragen der gespeicherten verschlüsselten Daten; und
 - (e) Ausschalten der Übertragungseinrichtung nach dem vorgebbaren Zeitintervall.
- 15 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 Be-
20 nutzers mittels einer Sensorik eingelesen werden, und dass bei falschen Eingabewerten nach einer vorgebbaren Anzahl von Wiederholungen die Vorrichtung deaktiviert wird.

25 Besonders bevorzugt ist, dass im Verfahrensschritt (e) die in den Verfahrensschritten (a) und (b) gespeicherten Daten gelöscht werden, um somit eine hohe Sicherheitsstufe gegen Missbrauch zu erlangen.

Ein weiterer Vorteil besteht darin, dass in einer anderen bevorzugten Ausgestaltung im Verfahrensschritt (a) eine Eingabe eines vorgebbaren Zeitintervalls erfolgt, womit eine besondere Flexibilität erreicht wird. Der Benutzer kann das von ihm eingegebene Zeitintervall ganz individuell an seine Bedürfnisse anpassen, wenn beispielsweise der Weg von dem Ort seiner Eingabe zum Selbstbedienungsgerät besonders lang ist, und sich keine Gelegenheit mehr vorher zu einer
30 sicheren Eingabe bietet.

35 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 Ausspähen der Geheimnummer 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 durch kryptografische Schlüssel und kryptografische Verfahren und die Verwendung von Smart-Cards gegeben. Jede erfindungsgemäße Vorrichtung, die auch als ein persönlicher EPP (Encrypted Pin Pad) bezeichnet werden kann, kann außerdem durch eine weltweit einzigartige Seriennummer identifiziert werden.

Durch die erfindungsgemäße Vorrichtung mit einer zeitlichen Begrenzung der Gültigkeit der Eingaben, beispielsweise PIN-Nummer und/oder Geldbetrag, führt ein Verlust des persönlichen EPP außerhalb des vorher eingestellten Gültigkeitszeitraumes nicht zwangsläufig auch zu einem finanziellen Verlust des Kontoinhabers. Hieraus ergibt sich ein besonders wirtschaftlicher Sicherheitsvorteil.

Durch die sichere Verschlüsselung und die zeitliche Begrenzung kann das persönliche EPP zum Beispiel auch an andere Personen für einen ein- oder mehrmaligen zeitlich und/oder betragsmäßig limitierten Aus- oder Bezahlvorgang überlassen werden, ohne dass diesen Personen die Geheimzahl mitgeteilt werden muss.

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 einer beispielhaften Ausführungsform einer erfindungsgemäßen Vorrichtung bei einer Anwendung; und

Figur 2 ein beispielhaftes Blockschaltbild einer erfindungsgemäßen Vorrichtung.

Die Figur 1 zeigt eine perspektivische Ansicht einer beispielhaften Ausführungsform einer erfindungsgemäßen Vorrichtung 1 bei einer Anwendung einer Datenübertragung zu einem Selbstbedienungsgerät 2.

Üblicherweise wird an dem Selbstbedienungsgerät 2, welches in der Figur 1 ein Geldautomat ist, über eine Tastatur 3 ein Passwort oder eine Geheimzahl, ein so genannter PIN-Code eingegeben, damit ein bestimmter Vorgang, beispielsweise eine Auszahlung, vorgenommen werden kann. Die Eingabeaufforderungen und Reaktionen des Selbstbedienungsgerätes werden an einem Bildschirm 4 zur Bedienerführung angezeigt. Beim Auszahlungsvorgang wird das entsprechende Geld über eine Ein-/Ausgabereinrichtung 5 in bekannter Weise ausgegeben.

Anstelle der manuellen Eingabe mittels der Tastatur 3 ist zur Übertragung der Geheimzahl die erfindungsgemäße Vorrichtung 1 vorgesehen, welche vorzugsweise aus einer Smart-Card besteht. Die Smart-Card 1 weist eine Eingabetastatur 6 zur Eingabe der Geheimzahl und vorzugsweise eine Anzeige 7 zur Bedienerführung auf. Hiermit kann die Geheimzahl an einem für den Benutzer sicheren Ort unabhängig vom Standort des Selbstbedienungsgerätes 2 vorgenommen werden.

Am Standort des Selbstbedienungsgerätes 2 wird wie in Figur 1 dargestellt, die in der Smart-Card 1 gespeicherte Geheimzahl über eine Übertragungsstrecke 8 an eine Empfangseinrichtung 9 des Selbstbedienungsgerätes 2 übertragen. Die Übertragungsstrecke 8 kann eine bekannte Ausführung einer drahtlosen Signalstrecke sein, beispielsweise Infrarot- oder Nahfeldfunkübertragung wie Bluetooth. Ebenso ist eine Induktionsschleife möglich. Auch eine drahtgebundene Übertragung kann ausgeführt werden, indem die Übertragungsstrecke 8 als Kabel ausgeführt ist, welches von der Smart-Card 1 an das Selbstbedienungsgerät 2 angeschlossen wird.

Im Folgenden wird der Aufbau der Smart-Card 1 beschrieben. Diese Beschreibung erfolgt mit Bezugnahme auf Figur 2, die ein beispielhaftes Blockschaltbild darstellt.

Die Eingabetastatur 6 mit Tastenelementen 10 ist für die Eingabe von alphanumerischen Zeichen sowie auch von anderen Steuerzeichen vorgesehen. Sie ist mit einer Steuereinrichtung 11 verbunden. Die Bedienerführung des Benutzers zur korrekten Eingabe in die Eingabetastatur 6 kann über die Anzeigeeinrichtung 7 erfolgen. Die Anzeigeeinrichtung 7 ist in dieser Ausführung mit der Steuereinrichtung 11 verbunden. Sie kann jedoch auch einen eigenen Prozessor oder eine eigene Steuereinrichtung besitzen.

Weiterhin weist die Smartkarte 1 eine Übertragungseinrichtung 13 auf, die mit der Steuereinrichtung 11 verbunden ist. Die Übertragungseinrichtung 13 kann außerdem ein erstes Kontaktfeld 14 für eine drahtgebundene Übertragung
5 beinhalten.

An die Steuereinrichtung 11 ist weiterhin eine Schalteinrichtung 15 angeschlossen. Diese Schalteinrichtung 15 aktiviert die Übertragungseinrichtung 13 zur Übertragung der eingegebenen Daten an das Selbstbedienungsgerät 2. In der
10 Steuereinrichtung 11 befindet sich eine Verschlüsselungseinrichtung 16, ein Prozessor 17 und ein nicht dargestellter Speicher. Die Verschlüsselungseinrichtung 16 und der Speicher können ebenfalls außerhalb der Steuereinrichtung 11 angeordnet sein.

15 Die Smartkarte 1 weist in einer weiteren Ausgestaltung eine Sensorik 18 mit einem zweiten Kontaktfeld 19 auf, welche für die Abtastung biometrischer Daten vorgesehen ist, wie zum Beispiel ein Fingerabdrucksensor.

Ein Energiespeicher 20 stellt die notwendige elektrische Energie zum Betrieb
20 der Smartkarte zur Verfügung. Es ist vorzugsweise eine wiederaufladbare Batterie, wobei es sich auch um eine Solaraufladung handeln kann. Das Wiederaufladen kann durch Induktion drahtlos oder drahtgebunden über das erste oder auch zweite Kontaktfeld 14, 19 in einer entsprechenden, nicht dargestellten
Einrichtung erfolgen. Da der Betrieb der Smartkarte 1 nur kurzfristig erfolgt, ist
25 der Energiebedarf äußerst gering.

Im Weiteren wird der Betrieb der Smartkarte 1 näher erläutert. Die Smartkarte 1 wird über die Eingabeeinrichtung 6 eingeschaltet. Die Steuereinrichtung 11 gibt den Eingabeablauf über die Anzeigeeinrichtung 7 dem Benutzer vor. Der Benutzer
30 wird aufgefordert, seine PIN-Nummer und/oder ein Passwort einzugeben, welche/welches mit einem gespeicherten Referenzwert verglichen wird. Dieser gespeicherte Referenzwert kann von dem die Smartkarte 1 ausgebenden Geldinstitut eingespeichert sein. Es ist aber auch möglich, dass in einer anderen Ausführung der Smartkarte 1 eine solche Überprüfung nicht erfolgt.

35 Der so geprüfte beziehungsweise eingegebene Datenwert wird mittels der Steuereinrichtung 11 gespeichert und mit der Verschlüsselungseinrichtung 16 verschlüsselt und gespeichert. Das erste Speichern kann auch unterbleiben.

Nun erfolgt ein Freischalten der Smartkarte 1 mittels der Schalteinrichtung 15 während eines vorgegebenen Zeitintervalls, welches entweder gespeichert vom Geldinstitut veränderbar oder fest vorgegeben ist, oder auch vom Benutzer auf Anforderung durch die Steuereinrichtung 11 vorgegeben werden kann. Der Benutzer muss daraufhin innerhalb dieses Zeitintervalls einen Übertragungsvorgang seiner auf der Smartkarte 1 eingegebenen Daten durchführen.

Dieser Übertragungsvorgang erfolgt, indem der Benutzer die Smartkarte 1 am Standort des Selbstbedienungsgerätes 2 entweder selbst durch eine Tastenkombination an der Eingabeeinrichtung 6 aktiviert, oder indem die Smartkarte 1 von der Empfangseinrichtung 9 des Selbstbedienungsgerätes 2 drahtlos aktiviert wird, nachdem der Benutzer sich am Selbstbedienungsgerät 2 angemeldet hat. Diese Anmeldung kann auch automatisch über die Übertragungseinrichtung 13 der Smartkarte 1 erfolgen.

Wenn der Benutzer vom Selbstbedienungsgerät 2 aufgefordert wird, seine PIN-Nummer einzugeben, führt er dieses mit der Smartkarte 1 aus, indem er eine entsprechende Tastenkombination der Eingabeeinrichtung 6 betätigt, oder die Smartkarte 1 in dem Empfangsbereich der Empfangseinrichtung 9 des Selbstbedienungsgerätes 2 bringt. Es kann auch ein Einführen der Smartkarte 1 in einen bekannten Kartenleser des Selbstbedienungsgerätes 2 erfolgen, wobei dann die Übertragung der verschlüsselten Daten von der Übertragungseinrichtung 13 der Smartkarte 1 über das erste Kontaktfeld 14 vorgenommen wird.

Nach Ablauf des vorgebbaren Zeitintervalls, oder nach Beendigung des Übertragungsvorgangs der verschlüsselten Daten, oder nach Tastenbetätigung der Eingabeeinrichtung 6 der Smartkarte 1 wird die Übertragungseinrichtung 13 der Smartkarte 1 von der Schalteinrichtung 15 ausgeschaltet, so dass kein weiterer Übertragungsvorgang mehr stattfinden kann. In einer bevorzugten Ausführungsform wird gleichzeitig der gespeicherte Datenwert der verschlüsselten und unverschlüsselten Dateneingabe auf der Smartkarte 1 unwiderruflich gelöscht. Die Smartkarte 1 muss für einen neuen Übertragungsvorgang erneut aktiviert werden, das heißt, es ist eine weitere Eingabeprozedur erforderlich. Somit ist eine vorteilhafte Sicherheit gegen Missbrauch gewährleistet, beispielsweise im Fall einer verlorenen Smartkarte 1.

Die Erfindung ist nicht auf das oben beschriebene Ausführungsbeispiel beschränkt.

So ist es denkbar, dass die Smartkarte 1 oder eine Chip-Karte in Kombination mit einem Funktelefon verwendet werden kann, wobei die drahtlose Übertragungsstrecke 8 vom Funktelefon betrieben wird und die Übertragungseinrichtung 13 der Smartkarte 1 mit dem Funktelefon drahtgebunden über das erste Kontaktfeld 14 kommuniziert.

Weiterhin kann die Steuereinrichtung 11 der Smartkarte 1 eine solche Software aufweisen, mit welcher der gesamte Bedienerführungsvorgang des Selbstbedienungsgerätes 2 vorab an einem für den Benutzer sicheren Ort durchgeführt werden kann. Das bedeutet, dass der Benutzer am Standort des Selbstbedienungsgerätes 2 nur noch dieses aktivieren muss, die verschlüsselten Daten mit seiner Smartkarte 1 überträgt und so der gesamte Vorgang, beispielsweise der Dateneingabe zur Geldausgabe, von der Datenübertragung der Smartkarte 1 übernommen wird. Dazu ist es vorteilhaft, dass die Übertragungsstrecke 8 und die Übertragungseinrichtung 13 der Smartkarte 1 bidirektional ausgebildet ist.

Es ist auch denkbar, dass die erfindungsgemäße Vorrichtung vollständig mit den Funktionen der Smartkarte 1 in einem Funktelefon oder umgekehrt integriert ist. Dieses kann als Aufsteckmodul ähnlich einer aufsteckbaren Kamera ausgeführt sein. Die Datenübertragung kann beispielsweise mittels einer Infrarotstrecke oder einer so genannten drahtlosen „Bluetooth“-Funkverbindung erfolgen.

Ebenfalls kann die Smartkarte 1 für eine begrenzte Zeit und auf einen bestimmten Geldbetrag voreingestellt werden, so dass sie auch beispielsweise für das Abheben einer bestimmten Geldmenge für dritte Personen geeignet ist, wobei ein Missbrauch durch die Schalteinrichtung 15 gänzlich ausgeschlossen ist.

Bezugszeichen

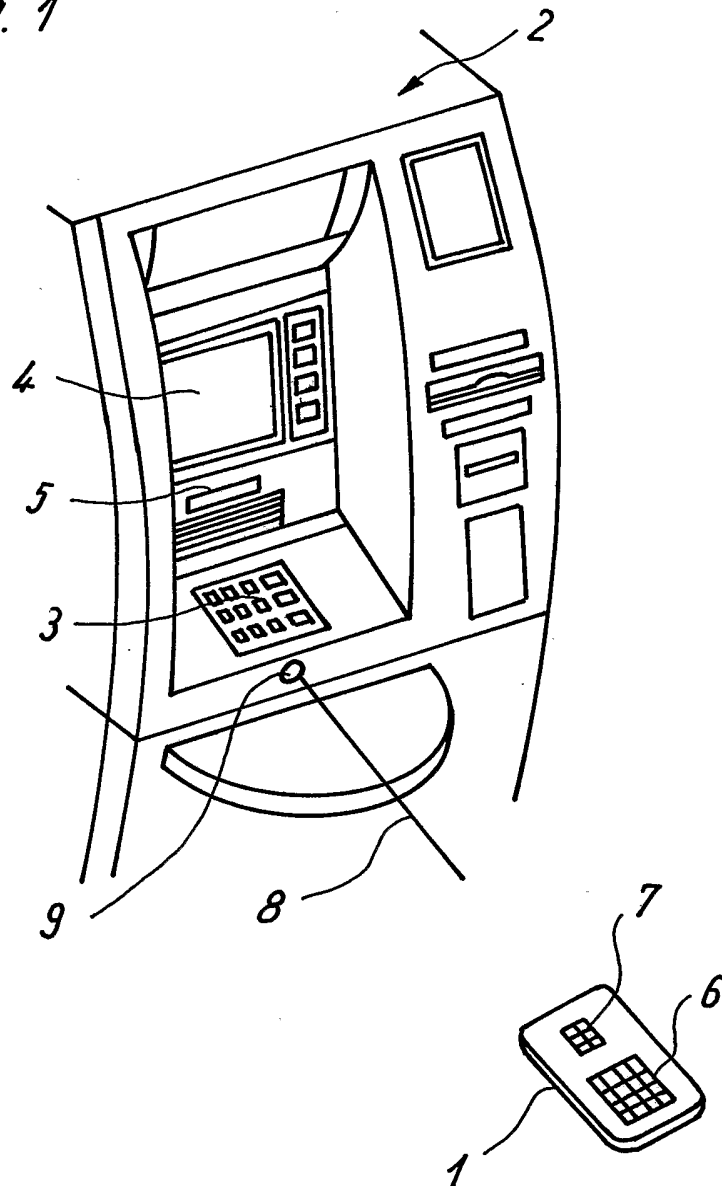
	1	Vorrichtung
	2	Selbstbedienungsgerät
5	3	Tastatur
	4	Bildschirm
	5	Ein-/Ausgabeeinrichtung
	6	Eingabetastatur
	7	Anzeige
10	8	Übertragungsstrecke
	9	Empfangseinrichtung
	10	Tastenelemente
	11	Steuereinrichtung
	13	Übertragungseinrichtung
15	14	erstes Kontaktfeld
	15	Schalteinrichtung
	16	Verschlüsselungseinheit
	17	Prozessor
	18	Sensorik
20	19	zweites Kontaktfeld
	20	Energiespeicher

PATENTANSPRÜCHE

- 5 1. Vorrichtung zur Eingabe von Informationen und zur Übertragung von verschlüsselten Datensignalen an ein Selbstbedienungsgerät (2), welche folgendes aufweist:
- a) eine Eingabeeinrichtung (6) zur Eingabe von Zeichen;
 - b) eine Verschlüsselungseinrichtung (16) zum Verschlüsseln von Daten;
 - 10 c) eine Übertragungseinrichtung (13) zum Übertragen von Daten an das Selbstbedienungsgerät;
 - d) eine Steuerungseinrichtung (11) zur Verarbeitung von Daten; und
 - e) mindestens eine Schalteinrichtung (15) zur Beeinflussung der Übertragungseinrichtung (13) und der eingegebenen und verschlüsselten gespeicherten Daten aufweist, welche zum Freischalten der Übertragungseinrichtung (13) innerhalb eines vorgebbaren Zeitintervalls ausgebildet ist.
 - 15
2. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Schalteinrichtung (15) zum Löschen von eingegebenen Daten nach dem Freischalten der Übertragungseinrichtung (13) innerhalb eines vorgebbaren Zeitintervalls ausgebildet ist.
- 20
3. Vorrichtung nach einem der vorstehenden Ansprüche, gekennzeichnet durch einen Energiespeicher (20).
- 25
4. Vorrichtung nach einem der vorstehenden Ansprüche, gekennzeichnet durch eine Anzeigeeinrichtung (7) zur Anzeige von Daten.
5. Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragungseinrichtung (13) zur Übertragung von Daten für eine drahtlose und/oder drahtgebundene Übertragungsstrecke (8) ausgebildet ist.
- 30
6. Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Steuereinrichtung (11) mindestens einen Prozessor (17) und eine Verschlüsselungseinrichtung (16) aufweist.
- 35
7. Vorrichtung nach einem der vorstehenden Ansprüche, gekennzeichnet durch eine Sensorik (18) zur Abtastung biometrischer Daten.

8. Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragungseinrichtung (13) für einen bidirektionalen Datenaustausch mit der Übertragungsstrecke (8) ausgebildet ist.
- 5
9. Vorrichtung nach einem der Ansprüche 1- 8, dadurch gekennzeichnet, dass die Vorrichtung eine Smartkarte (1) ist.
10. Vorrichtung nach einem der Ansprüche 1-8, dadurch gekennzeichnet, dass die Vorrichtung aus einer Chipkarte und einem Übertragungsgerät , vorzugsweise Funktelefon, besteht.
- 10
11. Verfahren zum Betreiben einer Vorrichtung nach einem der vorstehenden Ansprüche, gekennzeichnet durch folgende Schritte:
- 15
- (a) Einlesen und Speichern von mittels einer Eingabeeinrichtung (6) eingegebenen Datenwerten;
 - (b) Verschlüsseln dieser eingelesenen Datenwerte mittels einer Verschlüsselungseinrichtung (16) und Speichern der verschlüsselten Datenwerte;
 - 20 (c) Freischalten der Übertragungseinrichtung (13) innerhalb eines vorgebbaren Zeitintervalls;
 - (d) Übertragen der gespeicherten verschlüsselten Datensignale; und
 - (e) Ausschalten der Übertragungseinrichtung (13) nach dem vorgebbaren Zeitintervall.
- 25
12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass im Verfahrensschritt (a) „Einlesen“ ein Passwort oder eine Geheimzahl angefordert wird und/oder biometrische Daten des Benutzers mittels einer Sensorik (18) eingelesen werden, und dass bei falschen Eingabewerten nach einer vorgebbaren Anzahl von Wiederholungen die Vorrichtung deaktiviert wird.
- 30
13. Verfahren nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass im Verfahrensschritt (e) „Ausschalten“ die in den Verfahrensschritten (a) und (b) gespeicherten Daten gelöscht werden.
- 35
14. Verfahren nach einem der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass im Verfahrensschritt (a) „Einlesen“ eine Eingabe eines vorgebbaren Zeitintervalls erfolgt.

15. Verfahren nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, dass im Verfahrensschritt (a) „Einlesen“ die Eingabe von Daten für einen vollständigen Bedienungsvorgang für ein Selbstbedienungsgerät (2) durchgeführt wird.

Fig. 1

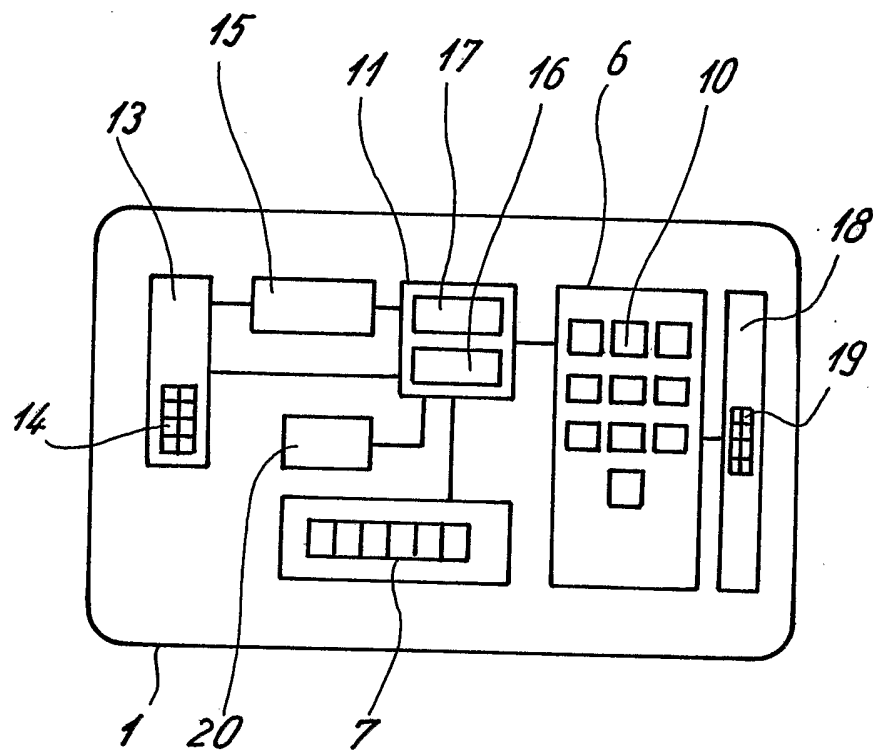


Fig 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE2005/001561

A. CLASSIFICATION OF SUBJECT MATTER G07F7/10 G07F19/00		
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) G07F		
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		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/25371 A (WANG, YNJIUN) 11 June 1998 (1998-06-11) abstract page 3, lines 5-11 page 6, line 3 - page 7, line 7 page 8, lines 14-25 page 9, lines 4-24 page 10, line 13 - page 11, line 30 page 12, lines 19-29 page 13, lines 7-18 page 14, line 3 - page 15, line 8 figures ----- -/--	1-15
☒ 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 21 November 2005		Date of mailing of the international search report 30/11/2005
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 Breugelmans, J

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE2005/001561

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 933 733 A (CITICORP DEVELOPMENT CENTER, INC) 4 August 1999 (1999-08-04) abstract paragraphs '0012! - '0016!, '0021! - '0024! figures -----	1-15
X	DE 102 45 347 A1 (GIESECKE & DEVRIENT GMBH) 8 April 2004 (2004-04-08) abstract paragraphs '0010! - '0016!, '0021! - '0024!, '0028! - '0031! figures -----	1-15
X	US 5 841 118 A (EAST ET AL) 24 November 1998 (1998-11-24) abstract column 4, line 1 - column 5, line 15 figure 1 -----	1-15
A	WO 01/03086 A (NCR INTERNATIONAL, INC; SAVAGE, JOHN, GERARD; GROSSI, MARK, MICHAEL; C) 11 January 2001 (2001-01-11) abstract page 1, paragraph 4 page 10, paragraph 5 - page 12, paragraph 2 page 16, paragraph 2 figures -----	1-15
A	WO 01/54084 A (WINCOR NIXDORF GMBH & CO. KG; MOLITOR, DIETMAR) 26 July 2001 (2001-07-26) abstract page 2, line 15 - page 3, line 2 page 8, line 4 - page 9, line 12 figures -----	1-15
A	EP 1 209 639 A (FUJITSU LIMITED) 29 May 2002 (2002-05-29) abstract paragraphs '0021!, '0027! - '0029!, '0031!, '0032!, '0034!, '0036!, '0045! figures -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE2005/001561

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9825371	A	11-06-1998	AU 5383198 A	29-06-1998
			TW 565786 B	11-12-2003
			US 6282656 B1	28-08-2001
			US 6594759 B1	15-07-2003
			US 5917913 A	29-06-1999
EP 0933733	A	04-08-1999	NONE	
DE 10245347	A1	08-04-2004	AU 2003271641 A1	23-04-2004
			WO 2004032414 A1	15-04-2004
US 5841118	A	24-11-1998	NONE	
WO 0103086	A	11-01-2001	AU 4937200 A	22-01-2001
			DE 60001661 D1	17-04-2003
			DE 60001661 T2	18-12-2003
			EP 1194905 A1	10-04-2002
			ES 2191626 T3	16-09-2003
			JP 2003504741 T	04-02-2003
WO 0154084	A	26-07-2001	AU 3534501 A	31-07-2001
			DE 20001117 U1	07-06-2001
EP 1209639	A	29-05-2002	JP 2002157632 A	31-05-2002
			US 2002062257 A1	23-05-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2005/001561

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
G07F7/10 G07F19/00

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G07F

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 98/25371 A (WANG, YNJIUN) 11. Juni 1998 (1998-06-11) Zusammenfassung Seite 3, Zeilen 5-11 Seite 6, Zeile 3 - Seite 7, Zeile 7 Seite 8, Zeilen 14-25 Seite 9, Zeilen 4-24 Seite 10, Zeile 13 - Seite 11, Zeile 30 Seite 12, Zeilen 19-29 Seite 13, Zeilen 7-18 Seite 14, Zeile 3 - Seite 15, Zeile 8 Abbildungen	1-15
X	EP 0 933 733 A (CITICORP DEVELOPMENT CENTER, INC) 4. August 1999 (1999-08-04) Zusammenfassung Absätze '0012! - '0016!, '0021! - '0024! Abbildungen	1-15
	----- -/--	

☒ 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

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

21. November 2005

Absendedatum des internationalen Recherchenberichts

30/11/2005

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

Breugelmans, J

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2005/001561

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 102 45 347 A1 (GIESECKE & DEVRIENT GMBH) 8. April 2004 (2004-04-08) Zusammenfassung Absätze '0010! - '0016!, '0021! - '0024!, '0028! - '0031! Abbildungen -----	1-15
X	US 5 841 118 A (EAST ET AL) 24. November 1998 (1998-11-24) Zusammenfassung Spalte 4, Zeile 1 - Spalte 5, Zeile 15 Abbildung 1 -----	1-15
A	WO 01/03086 A (NCR INTERNATIONAL, INC; SAVAGE, JOHN, GERARD; GROSSI, MARK, MICHAEL; C) 11. Januar 2001 (2001-01-11) Zusammenfassung Seite 1, Absatz 4 Seite 10, Absatz 5 - Seite 12, Absatz 2 Seite 16, Absatz 2 Abbildungen -----	1-15
A	WO 01/54084 A (WINCOR NIXDORF GMBH & CO. KG; MOLITOR, DIETMAR) 26. Juli 2001 (2001-07-26) Zusammenfassung Seite 2, Zeile 15 - Seite 3, Zeile 2 Seite 8, Zeile 4 - Seite 9, Zeile 12 Abbildungen -----	1-15
A	EP 1 209 639 A (FUJITSU LIMITED) 29. Mai 2002 (2002-05-29) Zusammenfassung Absätze '0021!, '0027! - '0029!, '0031!, '0032!, '0034!, '0036!, '0045! Abbildungen -----	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE2005/001561

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9825371	A	11-06-1998	AU	5383198 A	29-06-1998
			TW	565786 B	11-12-2003
			US	6282656 B1	28-08-2001
			US	6594759 B1	15-07-2003
			US	5917913 A	29-06-1999
EP 0933733	A	04-08-1999	KEINE		
DE 10245347	A1	08-04-2004	AU	2003271641 A1	23-04-2004
			WO	2004032414 A1	15-04-2004
US 5841118	A	24-11-1998	KEINE		
WO 0103086	A	11-01-2001	AU	4937200 A	22-01-2001
			DE	60001661 D1	17-04-2003
			DE	60001661 T2	18-12-2003
			EP	1194905 A1	10-04-2002
			ES	2191626 T3	16-09-2003
			JP	2003504741 T	04-02-2003
WO 0154084	A	26-07-2001	AU	3534501 A	31-07-2001
			DE	20001117 U1	07-06-2001
EP 1209639	A	29-05-2002	JP	2002157632 A	31-05-2002
			US	2002062257 A1	23-05-2002