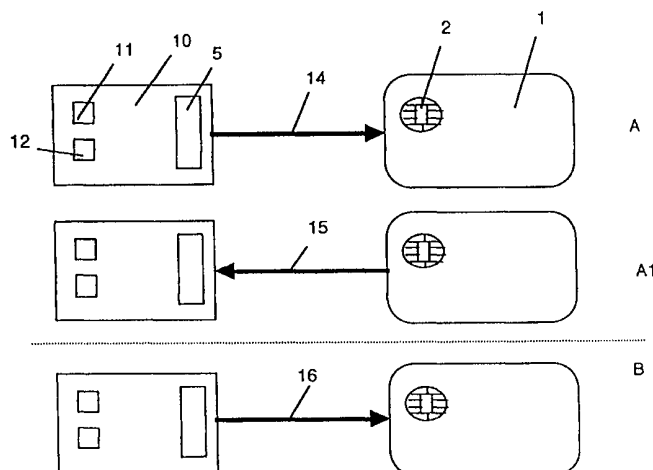


PCTWELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales BüroINTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation ⁷ : G07F 7/08	A1	(11) Internationale Veröffentlichungsnummer: WO 00/02170 (43) Internationales Veröffentlichungsdatum: 13. Januar 2000 (13.01.00)
(21) Internationales Aktenzeichen: PCT/IB99/01240 (22) Internationales Anmeldedatum: 5. Juli 1999 (05.07.99) (30) Prioritätsdaten: 98112441.5 6. Juli 1998 (06.07.98) EP (71) Anmelder (für alle Bestimmungsstaaten ausser US): EURO-PAY (SWITZERLAND) S.A. [CH/CH]; Hertistrasse 27, CH-8304 Wallisellen (CH). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): EBERLE, Adrian, Emil [CH/CH]; Hinterbergstrasse 22, CH-6318 Walchwil (CH). WOOLLVEN, Jack [GB/CH]; Bodenholzstrasse 30, CH-8340 Hadlikon (CH). (74) Anwalt: E. BLUM & CO.; Vorderberg 11, CH-8044 Zürich (CH).		(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Veröffentlicht <i>Mit internationalem Recherchenbericht.</i>

(54) Title: METHOD FOR PROTECTING DATA ON A DATA CARRIER AND CORRESPONDINGLY CONFIGURED CHIP CARD, READER AND CHIP SET

(54) Bezeichnung: VERFAHREN ZUM SCHUTZ VON DATEN AUF EINEM DATENTRÄGER SOWIE DAZU AUSGESTALTETE CHIPKARTE, LESEGERÄT UND CHIPSATZ



(57) Abstract

To prevent the unauthorized use of a credit card (1) a code (15) is generated after delivery of a blocking instruction (14) and transmitted to a code support (10), after which the card is blocked. The blockage can be reversed by returning the code (16) from the code support (10) to the card (10). In this way a card can be blocked and unblocked simply and without the use of a PIN code.

(57) Zusammenfassung

Zur Sperrung einer Wertkarte (1) gegen unberechtigten Gebrauch wird nach Abgabe eines Sperrbefehls (14) ein Code (15) erzeugt und an einen Codeträger (10) abgegeben. Danach geht die Karte in den Sperrzustand. Die Sperre kann durch Zurückgabe des Codes (16) vom Codeträger (10) an die Karte (1) aufgehoben werden. Dadurch ist eine Sperrung und Entsperrung auf einfache Weise, ohne Verwendung des PIN-Codes möglich.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

**Verfahren zum Schutz von Daten auf einem
Datenträger sowie dazu ausgestaltete Chipkarte, Lesegerät
und Chipsatz**

5

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum
10 Schutz von Daten gemäss Oberbegriff des Anspruchs 1.
Ferner betrifft die Erfindung einen Datenträger in Form
einer Karte gemäss Anspruch 9, ein Lesegerät gemäss
Anspruch 10 sowie einen Chipsatz für einen Datenträger
gemäss Anspruch 11.

15

Stand der Technik

Datenträger, insbesondere kartenförmige
Datenträger, welche einen Chipsatz beinhalten (sogenannte
20 "smart cards"), können grundsätzlich zur Speicherung
beliebiger Daten dienen. Bekannt ist die Funktion solcher
Karten zum Beispiel als Speicher für geldwerte Daten,
welche bei der Bezahlung einer Ware oder Dienstleistung
von der Karte abgebucht werden, so dass die Karte als
25 Ersatz für Geld in physischer Form, insbesondere als
Ersatz für Kleingeld, dienen kann ("Electronic purse",
Wertkarte). Der auf der Karte gespeicherte Betrag kann an
entsprechend ausgestatteten Terminals erhöht bzw. die
Karte wieder mit Geld aufgeladen werden; handelsübliche
30 Lesegeräte z.B. in der Form von Schlüsselanhängern,
erlauben das Lesen des noch auf der Karte gespeicherten
Betrages. Die Abbuchung von geldwerten Daten erfolgt an
speziellen Terminals an der Verkaufsstelle.

Eine Karte mit ungeschützter Chipfunktion
35 bzw. Wertfunktion aus der Hand zu geben, kann für den
Karteninhaber ein Risiko darstellen. Wenn der Inhaber
einer Kreditkarte mit Wertfunktion (z.B. EUROCARD mit

CASH-Chip) eine Kreditkarten-Imprinterzahlung durchführen will (z.B. im Restaurant), so muss er dazu seine Karte aus der Hand und oft auch aus seinem visuellen Überwachungsbereich geben. Es besteht dann die

5 Möglichkeit, dass der Kreditkarten-Vertragspartner, bzw. dessen Hilfspersonen (zum Beispiel Kellner), mit der Karte nicht nur den erwarteten Kreditkarten-Slip erstellt und zur Unterschrift zurückbringt, sondern ausserhalb des visuellen Überwachungsbereichs des Karteninhabers und

10 ohne dessen Zustimmung die ungeschützte Wertfunktion der Karte belastet (Diebstahl von elektronischem Wertkarten-Geld). Da der Karteninhaber bei Rückerhalt der Kreditkarte den Wertkartensaldo nicht unmittelbar einsehen wird, bemerkt er den Diebstahl erst später bzw.

15 überhaupt nicht; zudem ist es kaum beweisbar, welcher Betrag vor der Weggabe der Karte gespeichert war.

Es ist bekannt, bei Wertkartenchips, bzw. bei mit solchen Chipsätzen bestückten Wertkarten, eine Sperrfunktion vorzusehen, welche auf dem persönlichen

20 Benutzercode des Karteninhabers (sogenannter PIN-Code) basiert und mit der sich die Wertfunktion schützen lässt. Dazu steckt der Karteninhaber die Wertkarte (bzw. Kreditkarte mit Wertfunktionschip) in ein kleines, taschenrechnerähnliches Gerät, das er immer mit sich

25 führen muss. Anschliessend drückt er die "Lock"-Taste. Das Gerät sendet dem Chip einen "Lock"-Befehl, worauf sich der Chip in einen Zustand versetzt, in dem keine Belastungen der Wertfunktion mehr möglich sind. (Die Lockfunktion ist bei diesem Gerät meist mit weiteren

30 Funktionen kombiniert, z.B. Anzeige des Wertkartensaldos, Anzeige der letzten Wertkartenzahlungen). Der Karteninhaber kann nun die Karte gefahrlos aus der Hand geben. Niemand kann den Wertkartensaldo belasten, sofern er den PIN-Code der Karte nicht kennt. Nach Rückerhalt

35 der Karte steckt der Karteninhaber die Karte wiederum in das Gerät und gibt auf der eingebauten Tastatur seinen PIN-Code ein. Das Gerät sendet dem Chip einen "unlock"-

Befehl zusammen mit dem PIN-Code. Falls der PIN-Code stimmt, entsperrt sich der Chip, und die Wertfunktion ist wieder normal benutzbar.

Obwohl im Prinzip tauglich, hat dieses
5 Verfahren Nachteile. Der Vorgang ist für den Karteninhaber relativ umständlich (Eingabe des PIN-Codes). Er müsste das Verfahren im Prinzip vor bzw. nach jeder Kreditkarten-Imprinterzahlung durchführen. Ferner ist das Zusatzgerät relativ gross und teuer, weil es eine
10 numerische Eingabetastatur haben muss. Weiter kann der PIN-Code von Umstehenden ausgespäht werden. Würde ein solcher "Späher" dem Karteninhaber anschliessend seine Kreditkarte stehlen, könnte er damit EFT/POS-Zahlungen, Bargeldbezüge bzw. Wertkartenladungen durchführen und
15 damit den Kreditkarteninhaber bzw. das Kreditkartenunternehmen schädigen.

Darstellung der Erfindung

20 Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zu schaffen, welches den Schutz der Daten auf dem Datenträger, insbesondere einer Kreditkarte mit Wertfunktion, für den Benutzer einfacher und sicherer macht.

25 Diese Aufgabe wird bei einem Verfahren der eingangs genannten Art durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst.

Dadurch, dass der zur Entsperrung dienende Code bei der Sperrung erzeugt und in einem vom
30 Schutzobjekt, insbesondere der Wertfunktionskarte, getrennten Speichermittel aufbewahrt wird, steht dieser Code zur nachfolgenden Entsperrung auf diesem Speichermittel zur Verfügung, und auf die Eingabe des PIN-Codes kann verzichtet werden, wodurch der
35 entsprechende Aufwand und das entsprechende Sicherheitsrisiko wegfällt.

Vorzugsweise wird der Code vom Schutzobjekt bzw. der Wertfunktionskarte selber erzeugt. In einer anderen Ausführungsform der Erfindung wird der Code von einem das Speichermittel enthaltenden Codeträger erzeugt und an die Karte abgegeben. Weiter ist es bevorzugt, wenn der Code bei jeder Sperrung neu erzeugt wird.

Der Erfindung liegt weiter die Aufgabe zugrunde, einen Datenträger vorzugsweise in Form einer Karte zu schaffen, bei welchem die genannten Nachteile nicht auftreten. Dies wird bei einem Datenträger der eingangs genannten Art mit den kennzeichnenden Merkmalen des Anspruchs 9 erreicht.

Ferner soll ein Lesegerät geschaffen werden, welches zur Durchführung des Verfahrens geeignet ist. Ein solches weist die kennzeichnenden Merkmale des Anspruchs 10 auf. Weiter ist ein Chipsatz zur Durchführung des Verfahrens durch die Merkmale des Anspruchs 11 gekennzeichnet.

Kurze Beschreibung der Zeichnungen

Im folgenden werden Ausführungsbeispiele der Erfindung anhand der Zeichnungen näher erläutert. Dabei zeigt

Figur 1 eine schematische Darstellung von Datenträger und Lesegerät zur Sperrung und Entsperrung nach Stand der Technik,

Figur 2 eine schematische Darstellung ähnlich Figur 1 einer ersten Ausführungsform der Erfindung,

Figur 3 eine schematische Darstellung ähnlich Figur 1 einer weiteren Ausführungsform der Erfindung und

Figur 4 ein vereinfachtes Blockschema eines Datenträgers und eines Lesegerätes.

Bester Weg zur Ausführung der Erfindung

Figur 1 zeigt schematisch eine Wertkarte 1 nach Stand der Technik, welche mit einer elektronischen Datenverarbeitungs- und Speichereinheit 2 ("Chip") ausgerüstet ist, welche in bekannter Weise mit Daten, insbesondere mit geldwerten Daten, beschreibbar ist. In dieser bekannten Form kann die Karte 1 als Zahlungsmittel verwendet werden, indem in am Verkaufspunkt angeordneten Terminals der jeweils zu entrichtende Geldwert von der Karte abgebucht wird. In entsprechend ausgerüsteten anderen Terminals kann die Karte mit geldwerten Daten wieder aufgeladen werden. Wie bereits erwähnt, ist es bekannt, die Wertfunktion solcher Karten zu sperren, wobei diese dazu in ein Lesegerät 3 mit einer Tastatur 4 so eingeführt werden, dass die Kontaktanordnungen der Einheit 2 mit nicht dargestellten Kontaktanordnungen des Lesegeräts 3 in Kontakt treten. In der Figur 1 ist dies nur durch eine Pfeilverbindung zwischen der Karte 1 und dem Lesegerät 3 dargestellt. In Wirklichkeit wird die Karte 1 zum Zweck der Kontaktaufnahme mindestens ein Stück weit in das Lesegerät 3 hineingeschoben, was indes in der Zeichnung zur besseren Darstellung nicht gezeigt ist. Das Lesegerät weist ferner auf bekannte Weise eine Anzeige 5 auf, auf welcher zum Beispiel die Information von der Karte 1 ablesbar ist, wieviele geldwerte Einheiten sich noch auf der Karte befinden. Zur Sperrung der Karte wird nun nach Stand der Technik so vorgegangen, dass durch Betätigen einer entsprechenden Taste auf der Tastatur 4 ein Sperrbefehl 6 an die Karte abgegeben wird. Auf den Empfang dieses Sperrbefehls 6 hin sperrt sich die Karte so ab, dass auf die Wertfunktionen nicht mehr zugegriffen werden kann, d.h. es können auch keine geldwerten Einheiten von der Karte 1 abgebucht werden. Dieser Sperrschritt ist als Schritt A oberhalb der unterbrochenen Linie dargestellt. Unterhalb der unterbrochenen Linie ist als Schritt B das Entsperren der

Karte 1 nach Stand der Technik dargestellt. Dazu wird auf der Tastatur 4 des Lesegerätes 3 der PIN-Code eingetippt und als Signal 7 an die Karte abgegeben. Auf den Empfang dieses PIN-Codes hin entsperrt sich die Karte 1 und kann
5 wieder als Wertfunktionskarte verwendet werden. Das beschriebene Verfahren hat die in der Einleitung bereits erwähnten Nachteile.

Anhand von Figur 2 wird nun eine erste Ausführungsform des erfindungsgemässen Verfahrens
10 erläutert. Dabei bezeichnen gleiche Bezugszeichen wie anhin gleiche Elemente, die Sperrschritte sind wiederum oberhalb der unterbrochenen Linie dargestellt und der Entsperrungsschritt B unterhalb der unterbrochenen Linie. Generell kann das erfindungsgemässe Verfahren so
15 umschrieben werden, dass das Schutzobjekt 1, auf den Anstoss hin, sich zu schützen, ein Geheimnis erzeugt, welches an einen Geheimnisträger 10 abgegeben wird und nur dem Schutzobjekt und dem Geheimnisträger bekannt ist. Nach der Abgabe dieses Geheimnisses sperrt sich das
20 Schutzobjekt 1. Zur Entsperrung des Schutzobjektes muss das Geheimnis vom Geheimnisträger 10 wieder zum Schutzobjekt 1 zurücktransferiert werden, was bei Übereinstimmung mit dem vorher abgegebenen Geheimnis zur Entsperrung führt. Die genauere Beschreibung des
25 Ausführungsbeispiels von Figur 2 zeigt wiederum eine Wertfunktionskarte 1 mit einer Einheit 2, welche wiederum mit einem Lesegerät 10 in Verbindung steht. Auch in der Figur 2 ist die galvanische Kontaktaufnahme zwischen dem Lesegerät 10 und der Wertkarte 1 nicht dargestellt und
30 der Austausch der elektrischen Signale wird nur durch die jeweiligen Pfeile 14 bis 16 symbolisiert. Auch hier wird davon ausgegangen, dass das Lesegerät 10 auf an sich bekannte Weise mit der Karte 1 in Kontakt tritt. Anstelle der an sich bekannten Kontaktnahme mit Kontaktstiften des
35 Lesegerätes 10, welche auf Kontaktfelder der Einheit 2 einwirken, kann natürlich auch eine beliebig ausgestaltete kontaktlose Datenverbindung zwischen der

Karte 1 und dem Lesegerät 10 bestehen, zum Beispiel auf induktiver oder kapazitiver Basis oder auch optischer Basis. Das Lesegerät 10 benötigt keine numerische Tastatur, mittels welcher ein PIN-Code eingegeben werden könnte, sondern z.B. in an sich bekannter Weise nur eine Taste 11, mittels welcher das Gerät ein- und ausgeschaltet werden kann. Bei eingeschaltetem Gerät werden beim Einführen der Karte sofort die Daten von der Karte 1 abgefragt und auf der Anzeigeeinheit 5 dargestellt, so insbesondere der Saldo der Karte. Es sind aber auch Lesegeräte bekannt, welche keine Taste 11 aufweisen und nur durch das Einführen der Karte aktiviert werden. Jedenfalls weist das Lesegerät nun eine Taste auf, im gezeigten Beispiel die Taste 12, mittels welcher ein Sperrbefehl 14 an die Karte abgegeben werden kann. Dies könnte z.B. aber auch durch mehrmaliges kurzes Betätigen der Taste 11 erfolgen. Der Anstoss zur Sperrung der Karte erfolgt somit durch den Inhaber der Karte, welcher diese in das Lesegerät 10 einführt und die entsprechende Taste betätigt. Dies wird zum Beispiel der Kreditkarteninhaber tun, bevor er die Kreditkarte 1 mit Wertkartenfunktion aus der Hand gibt. Bei Betätigung der Taste 12 sendet das Lesegerät 10 dem Wertfunktions-Chip einen Befehl 14. Beim Empfang des Sperrbefehls erzeugt die Einheit 2 einen Code 15, welcher ein Einmalpasswort zum Beispiel in Form einer bei jedem Anstoss neu berechneten Zufallszahl sein kann und speichert diesen Code auf dem Speicher der Karte 1 ab. Anschliessend gibt die Einheit 2 dieses Einmalpasswort an das Lesegerät ab, was mit dem Pfeil 15 in Figur 2 dargestellt wird. Das Passwort, bzw. der Code 15 wird im Lesegerät 10 in einem Speicher abgelegt. Nach der Abgabe des Codes 15 an das Lesegerät 10 sperrt sich die Karte 1 in an sich bekannter Weise so ab, dass auf die Wertfunktion nicht mehr zugegriffen werden kann. Der Kreditkarteninhaber kann nun die Karte aus der Hand geben, ohne dass deren gesperrte Funktionen einer Gefahr ausgesetzt sind, solange das

Lesegerät 10, welches als Codeträger dient, in seinen Händen verbleibt. Zur Entsperrung der Karte 1 nach Rückerhalt derselben steckt sie der Kreditkarteninhaber wiederum in das Gerät 10. Dieses sendet entweder
5 selbständig, oder nach erneutem Betätigen der Taste 12, den Code als Signal 16 wieder an die Karte 1 zurück. Diese prüft ob der von ihr empfangene Code 16 mit dem vormals als Code 15 ausgegebenen Code identisch ist und hebt, wenn dies der Fall ist, die Sperre auf, so dass die
10 Karte wieder normal als Wertkarte verwendet werden kann.

Bevorzugterweise wird bei der Sperrung im Schritt A 1 nicht nur der Code 15 an das Lesegerät 10 abgegeben, sondern auch eine Identifikation der Karte 1, zum Beispiel deren Kartenummer, welche in der Einheit 2
15 gespeichert ist. Das Lesegerät 10 speichert dann beide Angaben zusammen in einer Tabelle ab. Diese Tabelle ermöglicht es dem Gerät 10, die Einmalpassworte bzw. -codes mehrerer Chipkarten gleichzeitig zu speichern und sie den einzelnen Chipkarten zuzuordnen. Sofern die
20 Tabellengrösse überschritten wird, nimmt das Gerät keine weiteren Einträge entgegen, damit keine Einmalpassworte verloren gehen und somit bereits gesperrte Chipkarten nicht mehr entsperrt werden könnten. Weiter ist es bevorzugt, wenn das Gerät 10 bei der Sperrung der Karte 1
25 den fehlerfreien Erhalt und die korrekte Abspeicherung des Codes und allenfalls auch der Kartenidentifikation quittiert. Die Sperrfunktion der Karte 1 tritt dann nur im Falle einer positiven Quittierung in Funktion. Im Falle einer negativen Quittierung bricht die Karte 1 den
30 Sperrvorgang ab und sperrt keine ihrer Funktionen. Dadurch wird verhindert, dass zum Beispiel bei einem Verbindungsunterbruch die Chipkarte gesperrt, das Einmalpasswort aber verloren und die Karte 1 somit nicht mehr entsperrrbar ist. Weiter ist es bevorzugt, wenn die
35 Karte 1 ihre Sperrung an das Gerät 10 zurückmeldet, worauf das Gerät 10 dem Kreditkarteninhaber den gesperrten Zustand der Karte 1 bestätigen kann, zum

Beispiel über die Anzeige 5 oder über einen Signaltongenerator. Die Rückmeldung kann z.B. aus der Quittierung direkt abgeleitet werden.

In einer weiteren Ausführungsform kann die Karte 1 ferner so ausgestaltet sein, dass die Entsperrung zusätzlich auch über die Eingabe des PIN-Codes möglich ist, wie grundsätzlich aus dem Schritt B von Figur 1 bekannt. Damit kann sichergestellt werden, dass eine Entsperrung auch noch dann stattfinden kann, wenn das Gerät 10 verloren geht oder seinen Speicherinhalt verliert. Mit dieser zusätzlichen Funktion wird allerdings die Sperrung weniger sicher, da dann auch Unbefugte, die den PIN-Code kennen, die Karte jederzeit entsperren können.

Die gemäss der Erfindung gesperrte Karte kann von Unberechtigten ohne das Gerät 10 nicht mit ihrer Wertfunktion verwendet werden. Gegen Angriffe mit erschöpfender Suche nach dem zutreffenden Code kann sich die Karte 1 zum Beispiel durch einen entsprechend langen Code und/oder durch zeitliche Unterbrechungen zwischen zwei unkorrekten Code-Eingabeversuchen und/oder durch irreversible Sperrung nach einer gewissen Anzahl empfangener unkorrekter Code schützen.

Bei der korrekten Entsperrung quittiert bevorzugterweise die Karte 1 dem Lesegerät den korrekten Empfang des Codes und die erfolgreiche Verarbeitung desselben, woraufhin das Lesegerät 10 den Eintrag in der Tabelle löscht und dem Kreditkarteninhaber den entsperrten Zustand der Chipkarte anzeigt, was wiederum über die Anzeigeeinheit 5 oder einen Signaltongenerator erfolgen kann.

Der Code 15 wird bei dem gezeigten Beispiel von der Einheit 2 auf der Karte erzeugt. Dies kann zum Beispiel durch einen Zufallsgenerator auf der Karte erfolgen oder durch einen Zähler, welcher jeweils den zuvor benutzten Code um 1 oder mehr erhöht. Anstelle eines solchen, jeweils neu erzeugten Codes, kann

grundsätzlich auch ein fest eingegebener Code auf der Karte 1 vorhanden sein, der jedesmal als gleichlautender Code ausgegeben wird. Diese letztere Lösung ist indes weniger sicher als die bevorzugte Erzeugung eines neuen
5 Codes bei jeder Sperrung.

Figur 3 zeigt eine weitere Ausführungsform der Erfindung, wobei wiederum gleiche Bezugszeichen gleiche Elemente bezeichnen. Bei der Ausführungsform von Figur 3 wird ebenfalls zur Auslösung der Sperrung die
10 Taste 12 betätigt, und der Sperrbefehl 17 an die Karte 1 abgegeben. Im Gegensatz zu dem anhand von Figur 2 beschriebenen Verfahren wird indes beim Verfahren gemäss Figur 3 der Code nicht von der Karte 1 erzeugt, sondern vom Lesegerät 20. Dieses speichert den Code bei sich ab
15 und sendet ihn als Signal 18 an die Karte 1, wo der Code ebenfalls gespeichert wird. Danach geht die Karte 1 auf an sich bekannte Weise in die Sperre, in welcher nicht mehr auf die Karte 1 zugegriffen werden kann. Nach diesem Schritt A 2 ist die Sperrung abgeschlossen. Zur
20 Entsperrung B wird die Karte 1 wiederum in Kontakt mit dem Lesegerät 20 gebracht und dieses sendet den Code erneut als Signal 19 an die Karte. Empfängt die Karte 1 dadurch den korrekten Code, so entsperrt sie sich wieder.

Auch bei dem Verfahren gemäss Figur 3 können
25 natürlich die oben beschriebenen Quittierungsmeldungen, die Meldungen an den Karteninhaber und die verschiedenen Arten der Erzeugung des Codes verwendet werden.

Figur 4 zeigt in grobschematischer Form die Daten- und Speichereinheit 2 der Karte 1 sowie die
30 Datenverarbeitungs- und Speichereinheit des Gerätes 10. Die Karte 1 weist dabei in an sich bekannter Weise eine Zentraleinheit 21 auf, welche über ein Interface 23 mit der Aussenwelt Daten austauschen kann und mit einem Speicher 22 verbunden ist. Der Speicher kann insbesondere
35 ein Register 25 für die Kartenummer enthalten. Die Zentraleinheit 21 kann den Codegenerator 24 bilden, welcher zum Beispiel als Zufallszahlengenerator jeweils

den Code erzeugt. Die Codeerzeugung kann indes auch durch einen Zähler erfolgen, welcher den jeweils vorher benutzten Code um einen gewissen Wert erhöht. Im Speicher kann in einer weiteren Ausführungsform auch ein Register für einen festen Code vorgesehen sein, der anstelle des jeweils neu erzeugten Codes verwendet wird, so dass das Element 24 nicht benötigt wird. Im Speicher 22 wird jeweils der erzeugte Code abgelegt und bei der Entsperrung mit dem über das Interface 23 zurückempfungenen Code verglichen. Das Lesegerät 10 weist im gezeigten Beispiel nur ein Interface 39 und einen Speicher auf, welche zusammen die Datenverarbeitung und Speicherung bilden. Natürlich könnte im Lesegerät 10 ebenfalls eine Zentraleinheit vorgesehen sein, welche dem Gerät allenfalls die Ausführung noch weiterer Funktionen ermöglichen würde. Neben den erwähnten Elementen sind eine Stromversorgung 37 in der Form einer Batterie, mindestens eine Taste 38 und die Anzeigeeinheit 5 vorgesehen. Der Speicher 30 beinhaltet die Tabelle mit dem jeweiligen Code 31 und der zugehörigen Kartenummer 32 bzw. den Code 33 und der Kartenummer 34 und allenfalls noch einen weiteren Code 35 und der zugehörigen Karte 36. Der entsprechende Chipsatz zur Bildung der Einheit 2 für die Karte 1 weist in diesem Beispiel also die Fähigkeit zur Erzeugung eines Codes auf und zum Vergleich dieses erzeugten Codes mit einem empfangenen Code zur Entsperrung der Karte. Bei einer anderen Ausführungsform, gemäss Figur 3, bei welcher der Code in dem Lesegerät erzeugt wird, weist der Chipsatz der Einheit 2 die entsprechende Fähigkeit zum Empfang eines Codes und Abspeicherung desselben vor der Sperrung der Karte auf sowie zum Vergleich eines nachher empfangenen Codes mit dem abgespeicherten Code. Der vom Lesegerät erzeugte und an die Karte 1 abgegebene Code wird dabei nur temporär im Register 25 der Karte gespeichert und spätestens bei der nächsten Sperrung durch den neuen Entsperrcode überschrieben.

Anstelle der beschriebenen, als Karten ausgeführten, Datenträger können natürlich auch andere Datenträger, die mit einer Datenverarbeitungs- und Speichereinheit versehen sind, auf die beschriebene Weise
5 gegen unberechtigten vollen oder teilweisen Zugriff auf die gespeicherten Daten geschützt werden. Zu denken ist dabei insbesondere an auswechselbare Halbleiterspeicher (z.B. Flash-Memories) bei Computern. Die geschützten Daten sind natürlich nicht auf geldwerte Daten
10 beschränkt, auch nicht bei der Ausgestaltung des Datenträgers als Kreditkarte. So könnten auf der Kreditkarte auch weitere schützenswerte Informationen gespeichert sein, so zum Beispiel Adress- und Telefoninformationen. Auch für diesen Fall kann es
15 wichtig sein, diese Daten vor einer Weitergabe der Karte gegen unberechtigten Zugriff zu sperren.

Das beschriebene Verfahren ist besser als das nach Stand der Technik bekannte Sperrverfahren. Die Bedienung ist bequemer und schneller, und das verwendete
20 Gerät ist einfacher, kompakter und preisgünstiger. Falls bevorzugterweise als Geheimnis ein Einmalpasswort, zum Beispiel eine Zufallszahl, anstelle eines statischen Wertes, insbesondere des PIN-Codes verwendet wird, kann das Geheimnis nicht gestohlen und später missbräuchlich
25 eingesetzt werden. Es besteht insbesondere keine Gefahr, dass der PIN-Code des Karteninhabers ausgespäht werden kann. Das Schutzverfahren funktioniert insbesondere auch dann, wenn der Chipkarte gar kein PIN-Code zugeordnet ist. Natürlich können die Geräte 10, 20 neben der
30 beschriebenen Schutzfunktion auch noch andere Funktionen ausführen, zum Beispiel auf bekannte Weise die Anzeige des Wertkartensaldos, der letzten Wertkartenzahlungen oder der Gültigkeitsdauer der Wertkarte.

Patentansprüche

1. Verfahren zum Schutz von Daten, die auf einem mit einem Speicher versehenen Schutzobjekt (1) gespeichert sind, welches auf einen Sperrbefehl hin den Zugriff auf die Daten sperren kann, und welches die Sperrung nach Empfang eines Codes aufheben kann, dadurch gekennzeichnet, dass der zur Entsperrung dienende Code bei der Sperrung erzeugt oder ein vorgängig erzeugter Code abgerufen wird, und dass der Code im Schutzobjekt und in einem vom Schutzobjekt (1) getrennten Speichermittel (30 - 36) gespeichert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass bei der Sperrung der Code vom Schutzobjekt (1) selber erzeugt oder abgerufen wird und an einen das Speichermittel (30 - 36) enthaltenden Codeträger (10) übermittelt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass bei der Sperrung der Code von einem das Speichermittel enthaltenden Codeträger (20) erzeugt oder abgerufen und an das Schutzobjekt (1) übermittelt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass bei jedem Sperrvorgang ein neuer Code erzeugt wird, insbesondere in der Form einer Zufallszahl.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zusammen mit dem Code eine Identifikation des Schutzobjektes gespeichert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Sperrung erst nach einer Quittierung der Speicherung erfolgt.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Schutzobjekt eine Kreditkarte mit Wertkartenfunktion oder eine Wertkarte ist.

8. Verfahren nach einem der Ansprüche 2 bis 7, dadurch gekennzeichnet, dass der Codeträger ein tragbares Lesegerät zum Lesen von Daten des Schutzobjektes ist, insbesondere ein tragbares Lesegerät für Wertkarten.

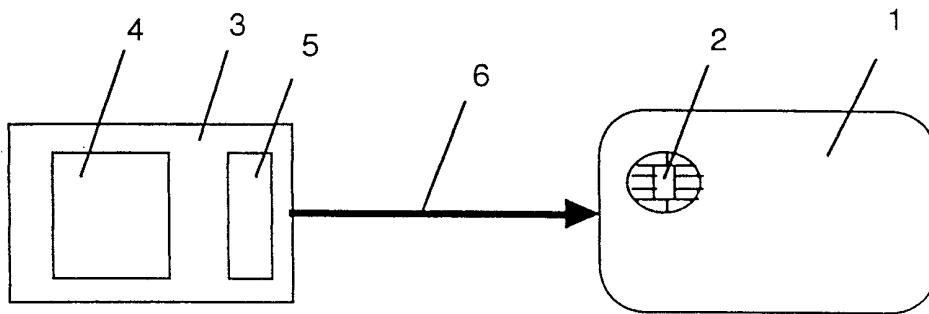
9. Datenträger, vorzugsweise in Form einer Karte (1), insbesondere Kreditkarte mit Wertkartenfunktion oder Wertkarte, mit einem auf Befehlseingabe sperrbaren Speicher (22), dessen Sperrung durch Eingabe eines Codes (16, 19) aufhebbar ist, dadurch gekennzeichnet, dass der Datenträger (1) zur Erzeugung, Speicherung und Ausgabe des Codes ausgestaltet ist, oder dass der Datenträger zum Empfang und zur temporären Speicherung des Codes ausgestaltet ist.

10. Lesegerät (10, 20), insbesondere als Schlüsselanhänger ausgestaltetes tragbares Lesegerät zur Datenkommunikation mit einem Datenträger in Form einer Karte, dadurch gekennzeichnet, dass das Lesegerät (10, 20) zur Abgabe eines Sperrbefehls (14) an die Karte, zur Speicherung eines von der Karte erzeugten Codes (15) und zur Übermittlung des gespeicherten Codes als Entsperrungscode (16) an die Karte ausgestaltet ist, oder dass das Lesegerät zur Abgabe eines Sperrbefehls (17) und zur Erzeugung und zur Abgabe eines Codes (18) an die Karte und zur Abgabe des Codes als Entsperrungscode (19) an die Karte ausgestaltet ist.

11. Chipsatz für einen Datenträger, insbesondere einen Datenträger in Form einer Karte, dadurch gekennzeichnet, dass der Chipsatz eine Speicher- und Datenverarbeitungselektronik (2) bildet, mittels welcher ein Code erzeugbar und ausgebbar ist, welcher bei erneutem Empfang als Entsperrungscode erkennbar ist.

1/2

FIG. 1



A
B

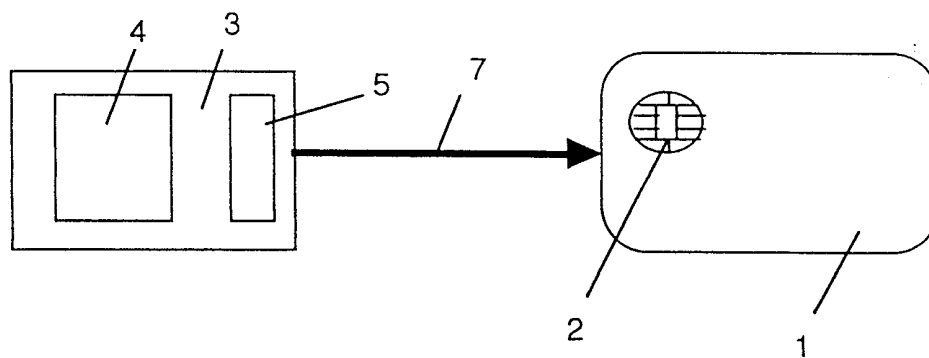
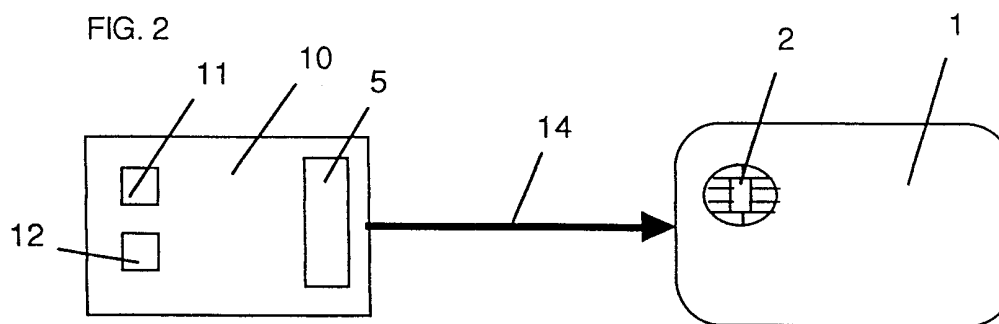
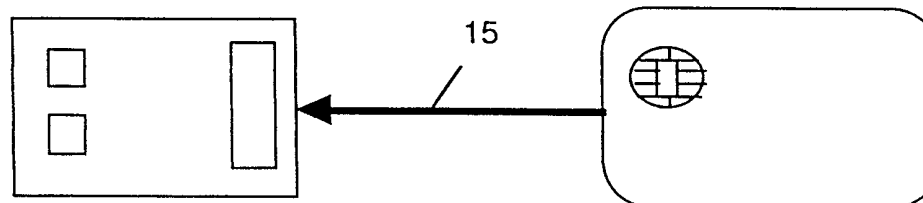


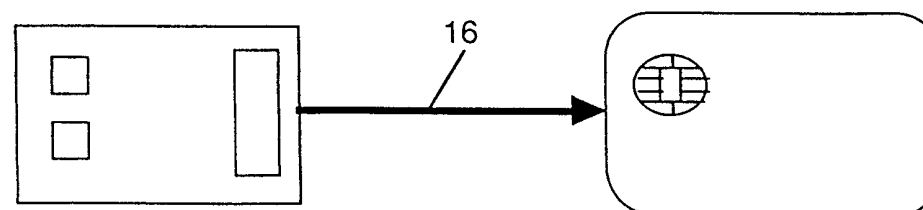
FIG. 2



A



A1



B

2/2

FIG. 3

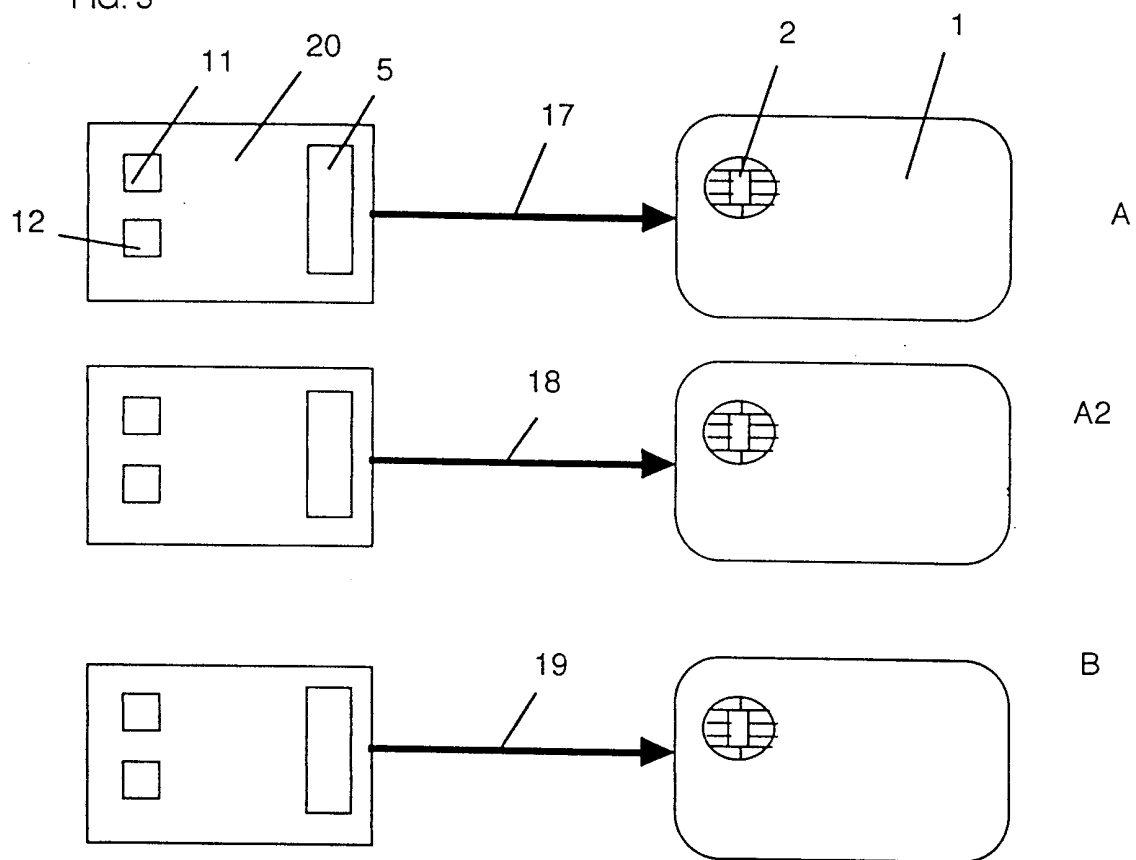
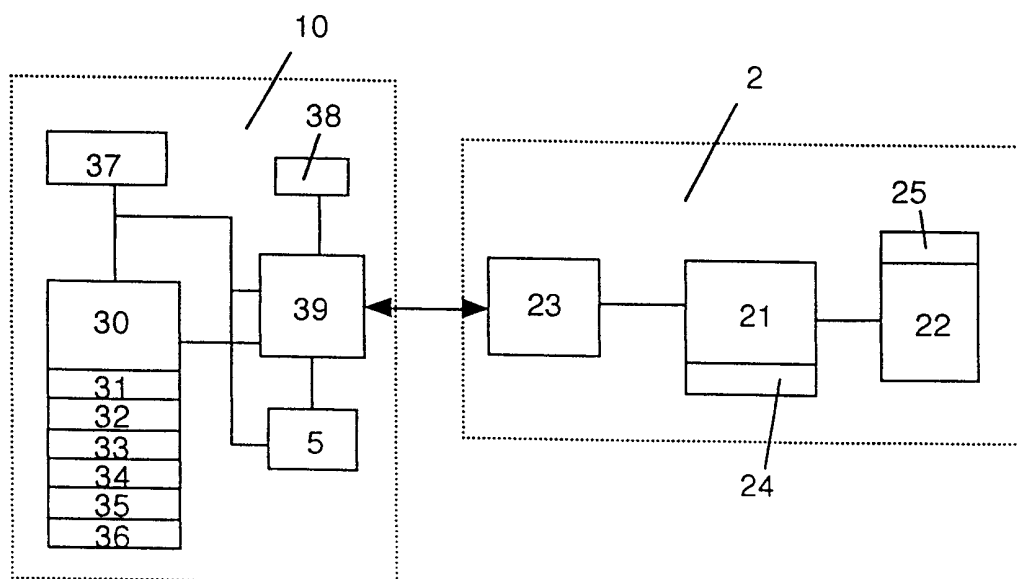


FIG. 4



INTERNATIONAL SEARCH REPORT

International Application No

PC1/IB 99/01240

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07F7/08

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 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 197 11 210 A (P. TILS)	1,9-11
A	20 May 1998 (1998-05-20) abstract; claims; figures	2,4,5,7, 8
Y	US 5 065 155 A (Y. OOGITA)	1,9-11
A	14 May 1991 (1991-05-14) abstract; claims; figures	
A	EP 0 574 219 A (RACAL-DATACOM)	1,2,4,5, 7,9-11
	15 December 1993 (1993-12-15) the whole document	
A	EP 0 668 579 A (AT & T)	
	23 August 1995 (1995-08-23)	
A	EP 0 486 960 A (ANGEWANDTE DIGITAL ELEKTRONIK) 27 May 1992 (1992-05-27)	
	--- -/--	



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

30 September 1999

Date of mailing of the international search report

07/10/1999

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

David, J

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 99/01240

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 557 934 A (ANGEWANDTE DIGITAL ELEKTRONIK) 1 September 1993 (1993-09-01) ---	
A	EP 0 671 703 A (SOLAIC) 13 September 1995 (1995-09-13) ---	
A	WO 91 10971 A (UTVECKLING AB JONIC) 25 July 1991 (1991-07-25) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 99/01240

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19711210 A	20-05-1998	AU 7303798 A WO 9822916 A DE 19726451 A	10-06-1998 28-05-1998 20-05-1998
US 5065155 A	12-11-1991	JP 1903902 C JP 2120921 A JP 6030040 B JP 2128210 A	08-02-1995 08-05-1990 20-04-1994 16-05-1990
EP 0574219 A	15-12-1993	AU 663190 B CA 2097998 A GB 2267769 A, B NZ 247755 A US 5323465 A	28-09-1995 11-12-1993 15-12-1993 26-09-1995 21-06-1994
EP 0668579 A	23-08-1995	US 5461217 A BR 9500433 A CA 2138829 A CN 1120203 A JP 7319982 A JP 7319983 A US H1794 H	24-10-1995 17-10-1995 09-08-1995 10-04-1996 08-12-1995 08-12-1995 06-04-1999
EP 0486960 A	27-05-1992	DE 4036765 A DE 59108023 D US 5288979 A	21-05-1992 29-08-1996 22-02-1994
EP 0557934 A	01-09-1993	DE 4205556 A DE 4305571 A	26-08-1993 25-08-1994
EP 0671703 A	13-09-1995	FR 2716280 A JP 8036624 A US 5644638 A	18-08-1995 06-02-1996 01-07-1997
WO 9110971 A	25-07-1991	CA 2073449 A, C AU 639443 B AU 5104990 A DE 69032858 D DE 69032858 T EP 0511204 A ES 2129021 T JP 5503380 T NO 305149 B US 5350907 A	16-07-1991 29-07-1993 05-08-1991 04-02-1999 05-08-1999 04-11-1992 01-06-1999 03-06-1993 06-04-1999 27-09-1994

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/IB 99/01240

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G07F7/08

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 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)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	DE 197 11 210 A (P. TILS)	1,9-11
A	20. Mai 1998 (1998-05-20) Zusammenfassung; Ansprüche; Abbildungen	2,4,5,7,8
Y	US 5 065 155 A (Y. OOGITA)	1,9-11
A	14. Mai 1991 (1991-05-14) Zusammenfassung; Ansprüche; Abbildungen	
A	EP 0 574 219 A (RACAL-DATACOM)	1,2,4,5,7,9-11
A	15. Dezember 1993 (1993-12-15) das ganze Dokument	
A	EP 0 668 579 A (AT & T)	
A	23. August 1995 (1995-08-23) EP 0 486 960 A (ANGEWANDTE DIGITAL ELEKTRONIK) 27. Mai 1992 (1992-05-27)	
	--- -/--	



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

30. September 1999

Absenddatum des internationalen Recherchenberichts

07/10/1999

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

David, J

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT, IB 99/01240

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 557 934 A (ANGEWANDTE DIGITAL ELEKTRONIK) 1. September 1993 (1993-09-01) ---	
A	EP 0 671 703 A (SOLAIC) 13. September 1995 (1995-09-13) ---	
A	WO 91 10971 A (UTVECKLINGS AB JONIC) 25. Juli 1991 (1991-07-25) -----	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichung: Angaben, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/IB 99/01240

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19711210 A	20-05-1998	AU 7303798 A WO 9822916 A DE 19726451 A	10-06-1998 28-05-1998 20-05-1998
US 5065155 A	12-11-1991	JP 1903902 C JP 2120921 A JP 6030040 B JP 2128210 A	08-02-1995 08-05-1990 20-04-1994 16-05-1990
EP 0574219 A	15-12-1993	AU 663190 B CA 2097998 A GB 2267769 A,B NZ 247755 A US 5323465 A	28-09-1995 11-12-1993 15-12-1993 26-09-1995 21-06-1994
EP 0668579 A	23-08-1995	US 5461217 A BR 9500433 A CA 2138829 A CN 1120203 A JP 7319982 A JP 7319983 A US H1794 H	24-10-1995 17-10-1995 09-08-1995 10-04-1996 08-12-1995 08-12-1995 06-04-1999
EP 0486960 A	27-05-1992	DE 4036765 A DE 59108023 D US 5288979 A	21-05-1992 29-08-1996 22-02-1994
EP 0557934 A	01-09-1993	DE 4205556 A DE 4305571 A	26-08-1993 25-08-1994
EP 0671703 A	13-09-1995	FR 2716280 A JP 8036624 A US 5644638 A	18-08-1995 06-02-1996 01-07-1997
WO 9110971 A	25-07-1991	CA 2073449 A,C AU 639443 B AU 5104990 A DE 69032858 D DE 69032858 T EP 0511204 A ES 2129021 T JP 5503380 T NO 305149 B US 5350907 A	16-07-1991 29-07-1993 05-08-1991 04-02-1999 05-08-1999 04-11-1992 01-06-1999 03-06-1993 06-04-1999 27-09-1994