**PCT** WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

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

| (51) Internationale Patentklassifikation 6 : | | (11) Internationale Veröffentlichungsnummer: WO 98/08189 |
|---|---|---|
| G06K 19/073, G07F 7/10 | A1 | (43) Internationales Veröffentlichungsdatum: 26. Februar 1998 (26.02.98) |

(21) Internationales Aktenzeichen: PCT/DE97/01457

(22) Internationales Anmeldedatum: 10. Juli 1997 (10.07.97)

(30) Prioritätsdaten:
196 34 133.7 23. August 1996 (23.08.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacher Platz 2, D-80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HUBER, Michael [DE/DE]; Peter-Rosegger-Strasse 17, D-93152 Nittendorf (DE). STAMPKA, Peter [DE/DE]; Klardorfer Strasse 41A, D-92421 Schwandorf (DE). HEITZER, Josef [DE/DE]; Alleestrasse 6, D-93090 Bach (DE).

(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

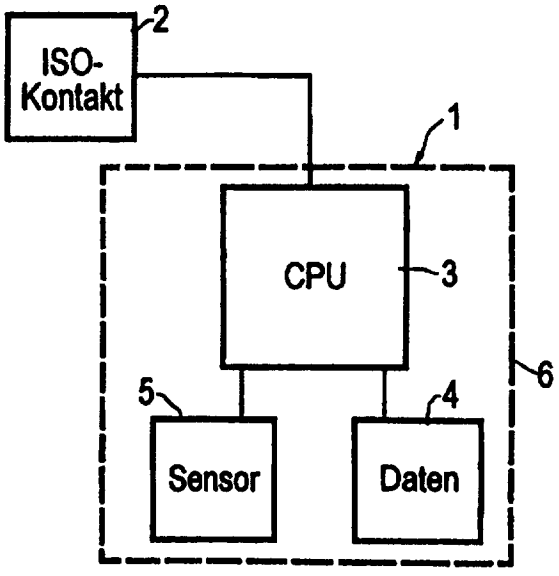
Veröffentlicht
*Mit internationalem Recherchenbericht.*

(54) Title: MICROPROCESSOR, PARTICULARLY FOR USE IN A CHIP CARD WITH A CONTROL UNIT AND A HOUSING SURROUNDING THE CONTROL UNIT

(54) Bezeichnung: MIKROPROZESSOR, INSBESONDERE ZUR VERWENDUNG IN EINER CHIPKARTE, MIT EINER STEUERUNGSEINHEIT UND MIT EINEM DIE STEUERUNGSEINHEIT UMGEBENDEN GEHÄUSE

(57) Abstract

This invention concerns a microprocessor with a control unit and a housing surrounding the control unit, as well as a chip card with such a microprocessor. Up until now, a significant weakness of the chip card systems has been that the microprocessor in the chip card which is surrounded by a housing, can be exposed for purposes of manipulation. Therefore, this invention aims to make a microprocessor and chip card available which are protected against manipulation. The invention achieves this task by providing the area of the housing of the microprocessor with at least one sensor which is linked to the control unit and indicates its environmental state. The control unit is constructed so that it can be set at an inactive state, if the sensor sends it one and/or no test signal which indicates a preset environmental state.




2...ISO CONTACT
4...DATA

(57) Zusammenfassung

Die Erfindung betrifft einen Mikroprozessor mit einer Steuerungseinheit und mit einem die Steuerungseinheit umgebenden Gehäuse sowie eine Chipkarte mit einem ebensolchen Mikroprozessor. Nach wie vor besteht ein erheblicher Schwachpunkt der bekannten Chipkartensysteme darin, daß der Mikroprozessor in der Chipkarte, der durch ein Gehäuse umgeben ist, zu Manipulationszwecken freigelegt werden kann. Es ist daher Aufgabe der Erfindung, ein Mikroprozessor sowie eine Chipkarte bereitzustellen, der bzw. die gegen Manipulationen geschützt ist. Diese Aufgabe wird gemäß der Erfindung dadurch gelöst, daß im Bereich des Gehäuses des Mikroprozessors mindestens ein Umweltzustände anzeigender, mit der Steuerungseinheit in Verbindung stehender Sensor vorgesehen ist, wobei die Steuerungseinheit so ausgebildet ist, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr vom Sensor ein und/oder kein Meßsignal zugeführt wird, das einen vorbestimmten Umweltzustand anzeigt.

*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** | Aserbaidschan | **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 | | | **TR** | Türkei |
| **BG** | Bulgarien | **HU** | Ungarn | **ML** | Mali | **TT** | Trinidad und Tobago |
| **BJ** | Benin | **IE** | Irland | **MN** | Mongolei | **UA** | Ukraine |
| **BR** | Brasilien | **IL** | Israel | **MR** | Mauretanien | **UG** | Uganda |
| **BY** | Belarus | **IS** | Island | **MW** | Malawi | **US** | Vereinigte Staaten von Amerika |
| **CA** | Kanada | **IT** | Italien | **MX** | Mexiko | | |
| **CF** | Zentralafrikanische Republik | **JP** | Japan | **NE** | Niger | **UZ** | Usbekistan |
| **CG** | Kongo | **KE** | Kenia | **NL** | Niederlande | **VN** | Vietnam |
| **CH** | Schweiz | **KG** | Kirgisistan | **NO** | Norwegen | **YU** | Jugoslawien |
| **CI** | Côte d'Ivoire | **KP** | Demokratische Volksrepublik Korea | **NZ** | Neuseeland | **ZW** | Zimbabwe |
| **CM** | Kamerun | | | **PL** | Polen | | |
| **CN** | China | **KR** | Republik Korea | **PT** | Portugal | | |
| **CU** | Kuba | **KZ** | Kasachstan | **RO** | Rumänien | | |
| **CZ** | Tschechische Republik | **LC** | St. Lucia | **RU** | Russische Föderation | | |
| **DE** | Deutschland | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Dänemark | **LK** | Sri Lanka | **SE** | Schweden | | |
| **EE** | Estland | **LR** | Liberia | **SG** | Singapur | | |

Beschreibung

"Mikroprozessor, insbesondere zur Verwendung in einer Chipkarte, mit einer Steuerungseinheit und mit einem die Steuerungseinheit umgebenden Gehäuse"

Die Erfindung betrifft einen Mikroprozessor, insbesondere zur Verwendung in einer Chipkarte, mit einer Steuerungseinheit sowie mit einem die Steuerungseinheit umgebenden Gehäuse. Weiterhin betrifft die Erfindung eine Chipkarte mit einem ebensolchen Mikroprozessor.

In zunehmendem Maße werden Zahlungsvorgänge für kleinere Geldbeträge mit Hilfe eines Chipkartensystems abgewickelt. Eine Chipkarte hat dazu die Funktion eines "Geldspeichers", wobei auf einer Chipkarte eine Mikroprozessor vorgesehen ist, der eine Steuerungseinheit, einen Datenspeicher zur Aufnahme des auf der Chipkarte gespeicherten Geldbetrages, Schnittstellen insbesondere zur Eingabe und Ausgabe von für Zahlungen relevante Daten, eine Steuerungseinrichtung zur Steuerung des Verarbeitungsablaufes der im Zusammenhang mit der Chipkarte verarbeiteten Daten sowie einen Befehlsspeicher aufweist, der das Betriebsprogramm für die Steuerungseinrichtung aufnimmt. Derartige Chipkartensysteme werden im Kreditkarten-Bereich, bei
Pay-TV-Anwendungssystemen und auch bei Systemen zur Überwachung des Zutritts zu sicherheitsrelevanten Einrichtungen und Gebäuden verwendet.

Schon bald nach Einführung der ersten Chipkartensysteme wurden Versuche unternommen, Chipkarten zu manipulieren, um sich mit derartigen manipulierten Chipkarten unberechtigte Vorteile zu verschaffen. So wurde versucht, Chipkarten nachzubilden und deren Datenspeicher mit einem manipulierten Guthaben zu versehen.

Dem wurde dadurch entgegengewirkt, daß die im Datenspeicher der Chipkarte vorhandenen Daten so verschlüsselt werden, daß eine Nachbildung der Daten nicht mehr möglich ist. Dazu werden Algorithmen wie DES, FES, DAS, DEA und RSA angewendet.

Nach wie vor liegt jedoch ein erheblicher Schwachpunkt der bekannten Chipkartensysteme darin, daß der durch ein Gehäuse umgebene Mikroprozessor auf einfache Weise freigelegt werden kann. Dazu wird das Gehäuse des Mikroprozessors über einen gewissen Zeitraum hinweg einer aggressiven Substanz wie beispielsweise einer Säure ausgesetzt, so daß das Gehäuse weggeätzt wird und der Mikroprozessor freiliegt. Der freigelegte Mikroprozessor kann dann in seinem Strukturaufbau analysiert werden. Dazu können die Anschlüsse des Mikroprozessors mit unterschiedlichen Eingangssignalen beaufschlagt werden, so daß insbesondere Informationen über das im Befehlsspeicher vorhandene Programm zur Steuerung des Verarbeitungsablaufes gewonnen werden können. Damit können beispielsweise die Daten im Datenspeicher entschlüsselt werden.

Es ist daher Aufgabe der Erfindung, einen Mikroprozessor bzw. eine Chipkarte bereitzustellen, der bzw. die gegen eine Manipulierung geschützt ist.

Diese Aufgabe wird gemäß der Erfindung dadurch gelöst, daß im Bereich des Gehäuses des Mikroprozessors mindestens ein Umweltzustände anzeigender, mit der Steuerungseinheit in Verbindung stehender Sensor vorgesehen ist, wobei die Steuerungseinheit so ausgebildet ist, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr vom Sensor ein Meßsignal zugeführt wird, das ein vorbestimmten Umweltzustand anzeigt.

Alternativ dazu kann die Steuerungseinheit auch so ausgebildet sein, daß sie in einen inaktiven Zustand versetzbar ist,

wenn ihr vom Sensor kein Meßsignal zugeführt wird, das einen bestimmten Umweltzustand anzeigt.

Die Erfindung beruht auf dem Grundgedanken, daß eine Chipkarte mit einem Mikroprozessor vorgesehen wird, der ohne erhebliche Inaktivierung bzw. Zerstörung des Mikroprozessors selbst nicht mehr auf einfache Wiese durch chemische und/oder physikalische Methoden freigelegt werden kann. Dazu ist ein Sensor vorgesehen, der mit der Steuerungseinheit verbunden ist. Die Steuerungseinheit tastet dabei regelmäßig den Sensor ab und überprüft, ob der Sensor einen Umweltzustand anzeigt, der beispielsweise mit dem Umweltzustand bei der Fertigung des Mikroprozessors übereinstimmt. Wenn der Umweltzustand im Bereich des Sensors wie beispielsweise durch Anwenden einer Chemikalie verändert ist, verändert sich das vom Sensor ausgehende Signal, was von der Steuerungseinheit abgetastet und erkannt wird. In diesem Fall geht die Steuerungseinheit in einen inaktiven Zustand über, so daß selbst bei einem freigelegten Mikroprozessor dessen Funktion nicht mehr auf einfache Weise nachvollzogen werden kann. Im Hinblick auf das vorstehende ist der Begriff "Steuerungseinheit" weit auszulegen, das heißt es kann jegliche Komponente des Mikroprozessors oder der Chipkarte außer Betrieb gesetzt werden, solange dadurch gewährleistet ist, daß ein Zugriff auf die Daten oder die Struktur des Datenspeichers, des Programmspeichers oder der Steuerungseinheit verhindert oder erschwert wird.

Erfindungsgemäß ist es auch möglich, einen Sensor vorzusehen, der insbesondere das Vorhandensein typischer zum Freilegen von Mikroprozessoren verwendeter Chemikalien als "Umweltzustand" anzeigt. So können Sensoren zur Anwendung kommen, die auf Säuren ansprechen. Wenn ein derartiger Sensor das Vorhandensein einer Säure im Bereich des Gehäuses anzeigt, ist anzunehmen, daß ein Versuch vorliegt, dem Mikroprozessor zu manipulieren. Dies wird von der Steuerungsein-

heit abgetastet, worauf sie in einen inaktiven Zustand übergeht.

Gemäß der Erfindung sind auch beide Ausführungsformen zugleich möglich, wobei dann mindestens zwei Sensoren oder ein Sensor mit Doppelfunktion vorgesehen sind. Die Steuerungseinheit ist in diesen Fall so ausgebildet, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr der eine Sensor ein Meßsignal zuführt, das einen vorbestimmten "verdächtigen" Umweltzustand anzeigt und/oder wenn ihr der andere Sensor kein Meßsignal mehr zuführt, das einen vorbestimmten "normalen" Umweltzustand anzeigt. Die Steuerungseinrichtung wird dann in einen inaktiven Zustand versetzt, wenn wenigstens einer der Sensoren einen vom Normalzustand abweichenden Umweltzustand anzeigt.

Der erfindungsgemäße, einen vorbestimmten Umweltzustand_anzeigende Sensor ist dabei ausdrücklich nicht auf einen Sensor beschränkt, der das Vorliegen oder Nicht-Vorliegen einer Chemikalie anzeigt. Es sind auch physikalische Veränderungen anzeigende Sensoren denkbar, wobei insbesondere Drucksensoren oder mechanische Sensoren vorgesehen werden können. Solche mechanischen Sensoren können beispielsweise als feine Leitungsdrähte im Bereich des Gehäuses ausgeführt sein, die bei einen Freischaben des Mikroprozessors zwangsweise zerstört werden müssen.

In Ausgestaltung der Erfindung ist im Bereich des Gehäuses eine von einem Sensor wahrnehmbare Substanz vorgesehen, wobei die Substanz auch wenigstens zwei Komponenten aufweisen kann, von denen wenigstens eine vom Sensor wahrnehmbar ist. Durch das Vorsehen einer derartigen Substanz ist es möglich, zum Zeitpunkt der Fertigung des Mikroprozessors einen definierten Umweltzustand herzustellen, wobei gerade bei der Ausführung der Substanz mit mehreren Komponenten durch das Verändern ih-

rer Mischungsverhältnisse eine Codierung eines Umweltzustandes vorgenommen werden kann. Bei einem quantitativ auf chemische Verbindungen reagierenden Sensor ist es so möglich, das Vorhandensein einer Substanz abzutasten, die eine bestimmte quantitative Zusammensetzung aufweist. Mit der letztgenannten Ausgestaltung kann auf besonders einfache Weise verhindert werden, daß bei einer Manipulation in einem ersten Schritt der Mikroprozessor freigelegt wird und daß im zweiten Schritt eine Substanz im Bereich des Sensors angebracht wird, um dem Mikroprozessor erneut zu aktivieren. Selbst bei Kenntnis der Bestandteile der Substanz ist es nahezu unmöglich, diese in der ursprünglichen Zusammensetzung nachzubilden. Durch eine derartige einfache Kodierung erhöht sich die Sicherheit des erfindungsgemäßen Mikroprozessors beträchtlich.

In einer weiteren Ausgestaltung der Erfindung ist der Sensor im Inneren des Gehäuses vorgesehen. Dabei ist es gemäß dieser Ausgestaltung der Erfindung besonders vorteilhaft, die Substanz, auf die der Sensor anspricht, bereits in die Abdeckmasse des Mikroprozessors bzw. in das Gehäusematerial einzulagern. Bei einem Ablösen des Gehäuses tastet dies der Sensor sofort ab, so daß die Steuerungseinheit in einen inaktiven Zustand versetzt wird, in dem ihre Eigenschaften nicht nachvollziehbar sind.

Gemäß einer besonders vorteilhaften Abwandlung der Erfindung ist der Sensor als Biosensor ausgebildet. Derartige Sensoren sind im Stand der Technik bereits bekannt und können zuverlässig, genau und besonders klein ausgestaltet werden, so daß sie für die Anwendung im Zusammenhang mit Mikroprozessoren prädestiniert sind. So sind zum Beispiel Sensoren zur Messung des menschlichen Blutzuckers bekannt, die einfach und vorteilhaft im Zusammenhang mit dem erfindungsgemäßen Mikroprozessor verwendet werden können. Derartige Biosensoren können sowohl die Existenz eines Stoffes als auch die Einzelkonzen-

trationen der Stoffe in einem Stoffgemisch schnell und einfach messen. Dadurch sind Biosensoren sowohl als qualitative Sensoren, die nur auf die Anwesenheit eines bestimmten Stoffs reagieren, als auch als quantitative Sensoren anwendbar, mit denen Konzentrationen von Substanzen erfaßt werden können.

Gemäß einer besonders einfachen Ausführung liefert der Sensor im erfindungsgemäßen Mikroprozessor ein digitales Ausgangssignal. Ein derartiger Sensor eignet sich besonders für quantitative Analysen. Dies kann zum Beispiel bei einem Sensor der Fall sein, der dafür bestimmt ist, die Anwendung von Säure auf das Gehäuse des Mikroprozessors abzutasten.

In Ausgestaltung des vorstehend beschriebenen Mikroprozessors kann der Sensor auch ein analoges Ausgangssignal liefern. Gerade im Zusammenhang mit einem von der Steuerungseinrichtung bzw. von dem Gehäuse des Mikroprozessors getrennt angeordneten Sensor ergibt eine derartige Ausgestaltung einen erhöhten Schutz gegen unerwünschte Manipulationen, und zwar insbesondere dann, wenn die für den Betrieb der Steuerungseinrichtung notwendigen, vom Sensor zu erfassenden Umweltzustände in der Steuerungseinheit oder im Datenspeicher des Mikroprozessors festgehalten sind. Die Daten, die den für den Betrieb der Steuerungseinheit notwendigen Umweltzustand kennzeichnen, können dann nämlich nur ausgelesen werden, wenn der Sensor die Steuerungseinheit in einen aktiven Zustand versetzt hält. Im Zuge einer Manipulation an dem Mikroprozessor tastet der Sensor jedoch die Manipulation ab und schaltet die Steuerungseinheit und damit den Zugriff auf die dem Sensor charakterisierenden Daten ab, bevor auf diese zugegriffen werden kann.

Ein Sensor, der ein analoges Ausgangssignal liefert, kann auch besonders einfach im Zusammenhang mit den bekannten Mikroprozessoren verwendet werden, da diese in aller Regel be-

reits Digital-Analog-Wandler aufweisen, die die Daten eines derartigen Sensors so umwandeln können, daß sie durch den Mikroprozessor verarbeitbar sind.

Ganz besonders vorteilhaft ist im Zusammenhang mit dem wie vorstehend ausgestalteten erfindungsgemäßen Mikroprozessor ein Sensor, der ein Meßsignal liefert, das hinsichtlich der wiederholten Abtastung eines wechselnden Umweltzustandes einen Hysterese-Charakter aufweist. Nach einem Freilegen des Sensors wird dadurch verhindert, daß der Mikroprozessor nach Wiederherstellen eines Umweltzustandes nach dem Freilegen des Sensors wieder im Betrieb gesetzt werden kann. Durch einen an sich bei Sensoren unerwünschten Hysterese-Charakter des Sensors liefert derselbe Sensor bei zeitlich versetzter, wiederholter Herstellung eines Umweltzustandes wie beispielsweise durch Entfernen und Wiederanfügen derselben charakteristischen Substanz im Bereich des Sensors nämlich jeweils unterschiedliche Ausgangssignale. Daher liegt beim Wiederanfügen einer identischen Substanz im Bereich des Sensors ein Ausgangssignal des Sensors vor, daß sich von demjenigen beispielsweise bei der Herstellung des erfindungsgemäßen Mikroprozessors unterscheidet. Die Steuerungseinrichtung ist dann vorteilhafterweise so eingerichtet, daß dieser Unterschied abgetastet und damit festgestellt werden kann, ob eine Manipulation im Bereich des Mikroprozessors vorliegt.

Schließlich ist der erfindungsgemäße Mikroprozessor vorteilhafterweise so ausgestaltet, daß ein ihm vom Sensor zugeführtes Signal dauerhaft abspeicherbar ist. Ein derartiges Abspeichern eines Signals, das dem Mikroprozessor von wenigstens einem Sensor zugeführt worden ist, kommt vor allem dann in Frage, wenn ein für den Zeitpunkt der Fertigung maßgeblicher Umweltzustand für den Vergleich mit einem Umweltzustand zu einem späteren Zeitpunkt festgehalten werden soll. Ein derartiges Abspeichern ist bei den im Stand der Technik be-

kannten Mikroprozessoren besonders einfach möglich, da diese bereits einen kleinen elektrisch programmierbaren Nur-Lese-Speicher (PROM) aufweisen, der bisher nur zum Abspeichern beispielsweise einer Seriennummer verwendet wird.

Die Erfindung betrifft ferner eine Chipkarte mit einem Mikroprozessor, der gemäß einem oder mehreren der Ansprüche 1 bis 10 ausgestaltet ist. Zwei der sich auf diese Weise aus den Ansprüchen 1 bis 10 ergebenden erfindungsgemäßen Ausgestaltungen sind in den unabhängigen Ansprüchen 11 und 12 festgelegt.

Die Erfindung wird anhand eines Ausführungsbeispiels mit Bezug auf die anliegenden Zeichnungen näher erläutert.

Figur 1 zeigt ein Blockdiagramm einer Schaltung in einer erfindungsgemäßen Chipkarte.

Figur 2 zeigt ein Diagramm eines Ausgangssignals eines typischen Sensors der erfindungsgemäßen Chipkarte.

Figur 3 zeigt ein Diagramm eines Ausgangssignals eines weiteren typischen Sensors der erfindungsgemäßen Chipkarte.

Figur 1 zeigt ein Blockschaltbild einer erfindungsgemäßen Chipkarte mit einem Mikroprozessor 1, der mit ISO-Kontakten 2 verbunden ist, die auf der Oberfläche der Chipkarte vorgesehen sind. Der Mikroprozessor 1 weist eine Steuerungseinheit 3 und einen Datenspeicher 4 auf. Weiterhin ist im Bereich der Steuerungseinheit 3 ein Sensor 5 vorgesehen. Die Steuerungseinheit 3, der Datenspeicher 4 und der Sensor 5 sind im Inneren eines Gehäuses 6 angeordnet. Das Gehäuse 6 besteht aus einer thermisch aushärtbaren Masse, in der eine nicht gezeigte Substanz eingelagert ist, auf die der Sensor 5 anspricht.

Im Betrieb der Chipkarte tauscht der Mikroprozessor 1 über den ISO-Kontakt 2 Daten aus einem externen Speicher eines nicht dargestellten Lese/Schreib-Geräts mit Daten aus dem Datenspeicher 4 und umgekehrt aus. Bei jedem Verarbeitungsschritt überprüft die Steuerungseinheit 3, ob der Sensor 5 auf die im Gehäuse 6 vorgesehene Substanz anspricht. Solange der Sensor 5 auf die im Gehäuse 6 vorhandene Substanz anspricht, erhält die Steuerungseinheit 3 den Betrieb aufrecht. Sobald der Sensor 5 die im Gehäuse 6 vorgesehene Substanz nicht mehr abtastet, etwa weil diese anläßlich einer Manipulation entfernt und durch eine Substanz mit anderer Zusammensetzung ersetzt worden ist, schaltet sich die Steuerungseinheit 3 zwingend und unwiderruflich ab. Eine Analyse des Funktionsablaufes innerhalb des Mikroprozessors 1 ist so ausgeschlossen.

Figur 2 zeigt ein Betriebsdiagramm eines Sensors, der im erfindungsgemäßen Mikroprozessor 1 und in der erfindungsgemäßen Chipkarte angeordnet werden kann. Die Abzisse des Diagramms aus Figur 2 bezeichnet dabei die Konzentration der im Gehäuse 6 vorgesehenen Substanzen. Diese variiert von 0 bis 1. Die Ordinate gibt die normierte Ausgangsspannung des Sensors in Abhängigkeit von der Konzentration der Substanz im Gehäuse 6 an. So ergibt sich bei einer Konzentration x der Substanz im Gehäuse 6 eine normierte Ausgangspannung $U_x$. Anhand der Ausgangsspannung $U_x$ kann die Steuerungseinheit 3 feststellen, ob und in welcher Konzentration die Substanz in der Umgebung des Sensors vorliegt.

Figur 3 zeigt ein Betriebsdiagramm eines Sensors, der im wesentlichen demjenigen entspricht, dessen Diagramm in Figur 2 gezeigt ist. Der Sensor, dessen Betriebsdiagramm in Figur 3 dargestellt ist, weist jedoch eine ausgeprägte Hysterese-Charakteristik auf. Diese Charakteristik kann im Zusammenhang

mit der erfindungsgemäßen Chipkarte besonders vorteilhaft zum Schutz gegen unerwünschte Manipulationen eingesetzt werden, wie nachfolgend beschrieben wird.

Bei der Herstellung des Mikroprozessors 1 steigt die Ausgangsspannung $U_{OUT}$ des in Figur 3 dargestellten Sensors von "0" auf den Wert $\alpha$ an. Dieser Wert $\alpha$ wird nach Beendigung der Herstellung des Mikroprozessors 1 von der Steuereinheit 3 eingelesen und fest in einen PROM-Bereich des Datenspeichers 4 eingebrannt. Wird bei einer Manipulation an der Chipkarte die den Sensor 5 umgebene Substanz entfernt, nimmt die Ausgangsspannung des Sensors 5 auf den Wert $\beta$ ab, der im Bereich der Ordinate des in Figur 3 gezeigten Diagramms eingezeichnet ist. Dieser Wert $\beta$ ist aufgrund der Hysterese-Charakteristik des Sensors 5 größer als der Ausgangswert "0" vor der Herstellung des Mikroprozessors 1. Bei einem erneuten Anbringen der Substanz im Bereich des Sensors 5 steigt die Ausgangsspannung des Sensors 5 wieder an, und zwar auf einen Wert der größer als der sich nach der Herstellung des Mikroprozessors 1 einstellende Wert $\alpha$ ist. Dieser Unterschied beruht ebenfalls auf der Hysterese-Charakteristik des Sensors 5. Dieser Unterschied in der Ausgangsspannung ($\gamma$-$\alpha$) wird von der Steuerungseinheit 3 abgetastet, wobei sie auf eine Manipulation im Bereich des Mikroprozessors 1 schließt, wenn der Wert ($\gamma$-$\alpha$) eine gewisse Schranke überschreitet, die vorgesehen ist, um einen unerwünschten Ausfall der Chipkarte aufgrund eines Alterungseffekts des Sensors 5 zu kompensieren.

Patentansprüche

"Mikroprozessor, insbesondere zur Verwendung in einer Chipkarte, mit einer Steuerungseinheit und mit einem die Steuerungseinheit umgebenden Gehäuse"

1) Mikroprozessor, insbesondere zur Verwendung in einer Chipkarte, mit einer Steuerungseinheit und mit einem die Steuerungseinheit umgebenden Gehäuse, dadurch gekennzeichnet, daß im Bereich des Gehäuses (6) mindestens ein Umweltzustände anzeigender, mit der Steuerungseinheit (3) in Verbindung stehender Sensor (5) vorgesehen ist, wobei die Steuerungseinheit (3) so ausgebildet ist, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr vom Sensor (5) ein einen vorbestimmten Umweltzustand anzeigendes Meßsignal zugeführt wird.

2) Mikroprozessor, insbesondere zur Verwendung in einer Chipkarte, mit einer Steuerungseinheit und mit einem die Steuerungseinheit umgebenden Gehäuse, dadurch gekennzeichnet, daß im Bereich des Gehäuses mindestens ein Umweltzustände anzeigender, mit der Steuerungseinheit in Verbindung stehender Sensor vorgesehen ist, wobei die Steuerungseinheit so ausgebildet ist, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr vom Sensor kein einen vorbestimmten Umweltzustand anzeigendes Meßsignal zugeführt wird.

3) Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß im Bereich des Gehäuses (6) eine vom Sensor wahrnehmbare Substanz vorgesehen ist.

4) Mikroprozessor nach Anspruch 3, dadurch gekennzeichnet, daß die Substanz wenigstens zwei Komponenten aufweist, wobei wenigstens eine der Komponenten vom Sensor wahrnehmbar ist.

5) Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Sensor (5) im Inneren des Gehäuses vorgesehen ist.

6) Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Sensor als Biosensor ausgebildet ist.

7) Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Sensor ein digitales Ausgangssignal liefert.

8) Mikroprozessor nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß der Sensor ein analoges Ausgangssignal liefert.

9) Mikroprozessor nach Anspruch 8, dadurch gekennzeichnet, daß der Sensor so ausgebildet ist, daß er ein Meßsignal liefert, das hinsichtlich einer wiederholten Abtastung eines wechselnden Umweltzustandes einen Hysterese-Charakter aufweist.

10) Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Mikroprozessor (1) so ausgebildet ist, daß ein ihm von wenigstens einem Sensor zugeführtes Signal dauerhaft abspeicherbar ist.

11) Chipkarte mit einem Mikroprozessor, der eine Steuerungseinheit und eine die Steuerungseinheit umgebendes Gehäuse aufweist, dadurch gekennzeichnet, daß im Bereich des Gehäuses (6) mindestens ein Umweltzustände anzeigender, mit der Steuerungseinheit in Verbindung stehender Sensor (5) vorgesehen ist, wobei die Steuerungseinheit (3) so ausgebildet ist, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr vom Sensor (5) ein einen vorbestimmten Umweltzustand anzeigendes Meßsignal zugeführt wird.

12) Chipkarte mit einem Mikroprozessor, der eine Steuerungseinheit und eine die Steuerungseinheit umgebendes Gehäuse aufweist, dadurch gekennzeichnet, daß im Bereich des Gehäuses mindestens ein Umweltzustände anzeigender, mit der Steuerungseinheit in Verbindung stehender Sensor vorgesehen ist, wobei die Steuerungseinheit so ausgebildet ist, daß sie in einen inaktiven Zustand versetzbar ist, wenn ihr vom Sensor kein einen vorbestimmten Umweltzustand anzeigendes Meßsignal zugeführt wird.

FIG 1

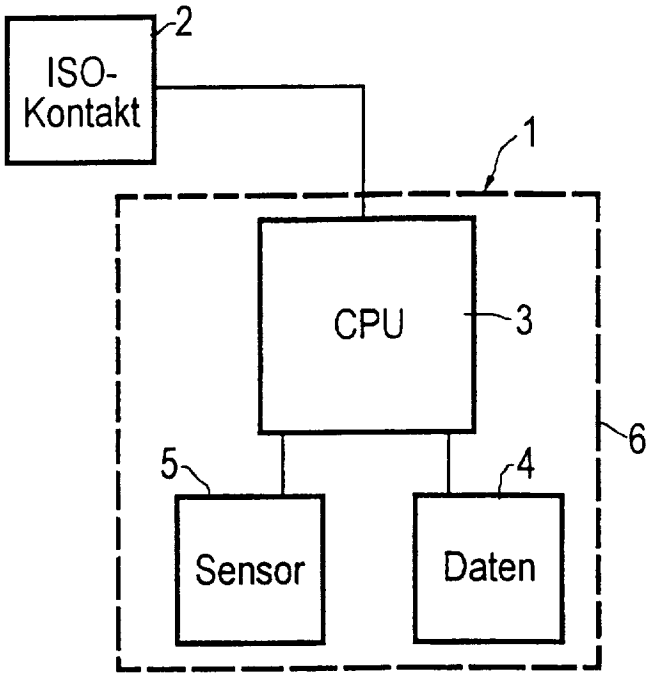



FIG 2

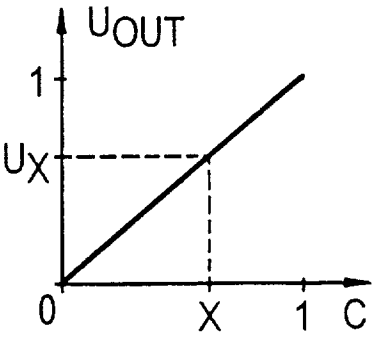
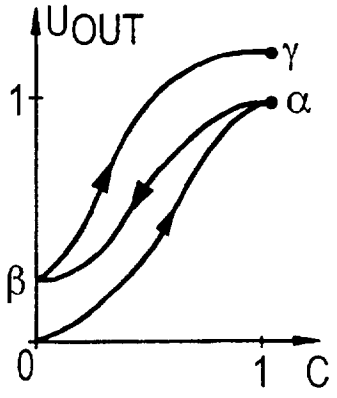



FIG 3



# INTERNATIONAL SEARCH REPORT

Intern. al Application No
PCT/DE 97/01457

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K19/073 G07F7/10

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 6 G06K 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. |
|---|---|---|
| X | EP 0 481 881 A (GEMPLUS CARD INTERNATIONAL) 22 April 1992 | 1,5,10, 11 |
| A | see abstract; claims; figures | 2,7,8,12 |
| | --- | |
| A | EP 0 565 480 A (ANGEWANDTE DIGITAL ELEKTRONIK) 13 October 1993 | 1-3,5,7, 9-12 |
| | see abstract; claims | |
| | see column 2, line 41 - line 57 | |
| | --- | |
| A | EP 0 718 794 A (SGS-THOMSON MICROELECTRONICS) 26 June 1996 | |
| | --- | |
| A | DE 40 18 688 A (SIEMENS) 10 January 1991 | |
| | --- | |
| A | FR 2 580 834 A (M. GRANDMOUGIN) 24 October 1986 | |
| | ----- | |

☐ 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 | Date of mailing of the international search report |
|---|---|
| 17 October 1997 | 31/10/97 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | David, J |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern: al Application No
PCT/DE 97/01457

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0481881 A | 22-04-92 | FR 2668274 A | 24-04-92 |
| | | CA 2053741 A,C | 20-04-92 |
| | | JP 1994511 C | 22-11-95 |
| | | JP 4264643 A | 21-09-92 |
| | | JP 7019231 B | 06-03-95 |
| | | US 5465349 A | 07-11-95 |
| EP 0565480 A | 13-10-93 | DE 4212111 A | 14-10-93 |
| EP 0718794 A | 26-06-96 | FR 2728369 A | 21-06-96 |
| | | JP 8249239 A | 27-09-96 |
| DE 4018688 A | 10-01-91 | NONE | |
| FR 2580834 A | 24-10-86 | NONE | |

# INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen
PCT/DE 97/01457

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06K19/073 G07F7/10

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
IPK 6 G06K 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. |
|---|---|---|
| X<br>A | EP 0 481 881 A (GEMPLUS CARD INTERNATIONAL) 22.April 1992<br>siehe Zusammenfassung; Ansprüche; Abbildungen | 1,5,10, 11<br>2,7,8,12 |
| A | EP 0 565 480 A (ANGEWANDTE DIGITAL ELEKTRONIK) 13.Oktober 1993<br>siehe Zusammenfassung; Ansprüche<br>siehe Spalte 2, Zeile 41 - Zeile 57 | 1-3,5,7, 9-12 |
| A | EP 0 718 794 A (SGS-THOMSON MICROELECTRONICS) 26.Juni 1996 | |
| A | DE 40 18 688 A (SIEMENS) 10.Januar 1991 | |
| A | FR 2 580 834 A (M. GRANDMOUGIN) 24.Oktober 1986 | |

☐ 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 | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 17.Oktober 1997 | 31/10/97 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | David, J |

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interne Aktenzeichen
PCT/DE 97/01457

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| EP 0481881 A | 22-04-92 | FR 2668274 A | 24-04-92 |
| | | CA 2053741 A,C | 20-04-92 |
| | | JP 1994511 C | 22-11-95 |
| | | JP 4264643 A | 21-09-92 |
| | | JP 7019231 B | 06-03-95 |
| | | US 5465349 A | 07-11-95 |
| EP 0565480 A | 13-10-93 | DE 4212111 A | 14-10-93 |
| EP 0718794 A | 26-06-96 | FR 2728369 A | 21-06-96 |
| | | JP 8249239 A | 27-09-96 |
| DE 4018688 A | 10-01-91 | KEINE | |
| FR 2580834 A | 24-10-86 | KEINE | |