



(51) Internationale Patentklassifikation ⁶ : G06K 19/07	A2	(11) Internationale Veröffentlichungsnummer: WO 99/08230 (43) Internationales Veröffentlichungsdatum: 18. Februar 1999 (18.02.99)
(21) Internationales Aktenzeichen: PCT/DE98/02147 (22) Internationales Anmeldedatum: 29. Juli 1998 (29.07.98) (30) Prioritätsdaten: 197 34 507.7 8. August 1997 (08.08.97) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): SEDLAK, Holger [DE/DE]; Neumünster 10A, D-85658 Eggenmating (DE). BRÜCKLMAYR, Franz-Josef [DE/DE]; Riedener Weg 38, D-87600 Kaufbeuren (DE). (74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D-80506 München (DE).		(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht <i>Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.</i>

(54) Title: METHOD FOR VERIFYING THE AUTHENTICITY OF A DATA MEDIUM

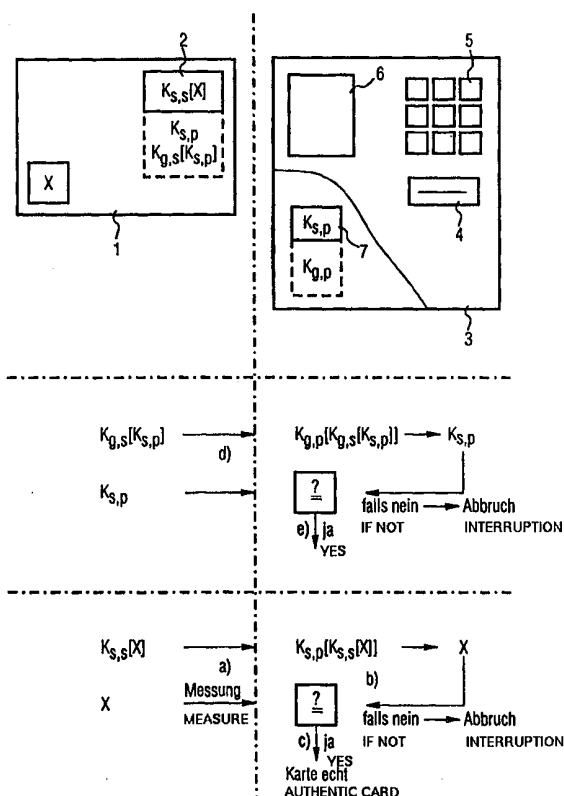
(54) Bezeichnung: VERFAHREN ZUR ECHTHEITSPRÜFUNG EINES DATENTRÄGERS

(57) Abstract

The invention concerns a method for verifying the authenticity of a data medium (1), in particular a chip card. The method is characterised in that the coded form of a physical characteristic (X) of the data medium (1) is stored in said medium. The coded form of said characteristic is transmitted to a terminal (3) which itself measures the physical characteristic (X). The latter (X) is coded with a secret code ($K_{s,s}$) and decoded with a known code ($K_{s,p}$) in the terminal (3). The authenticity is acknowledged when a coincidence is established after comparing the decoded characteristic with the measured characteristic. Said method ensures great security since the secret code ($K_{s,s}$) is contained neither in the medium (1) nor in the terminal (3).

(57) Zusammenfassung

Bei einem Verfahren zur Echtheitsprüfung eines Datenträgers (1), insbesondere einer Chipkarte, ist die verschlüsselte Form eines physikalischen Merkmals (X) des Datenträgers (1) in diesem gespeichert. Die verschlüsselte Form des Merkmals wird zu einem Terminal (3) übertragen, welches auch das physikalische Merkmal (X) selbst mißt. Das physikalische Merkmal (X) ist mit einem geheimen Schlüssel ($K_{s,s}$) verschlüsselt und wird mit einem öffentlichen Schlüssel ($K_{s,p}$) im Terminal (3) entschlüsselt. Bei einem Vergleich des entschlüsselten Merkmals und des gemessenen Merkmals wird bei Übereinstimmung die Echtheit festgestellt. Da der geheime Schlüssel ($K_{s,s}$) weder im Datenträger (1) noch im Terminal (3) enthalten ist, ist eine hohe Sicherheit gegeben.



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	Aserbaidshjan	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						

Beschreibung

Verfahren zur Echtheitsprüfung eines Datenträgers

5

Die Erfindung betrifft ein Verfahren zur Echtheitsprüfung eines Datenträgers, insbesondere einer Chipkarte, der zumindest einen Speicher aufweist, wobei ein spezifisches, physikalisches Merkmal des Datenträgers in verschlüsselter Form in dem Speicher abgelegt ist.

10

Ein solches Verfahren ist aus der EP 0 112 461 A1 bekannt. Dort sind die Eigenschaften einer in einer Identitätskarte enthaltenen Antenne in verschlüsselter Form in der Karte gespeichert und werden mit den gemessenen Eigenschaften verglichen. Der Vergleich findet dort jedoch in der Karte statt, wobei das wesentliche Geheimnis der Verschlüsselungsalgorithmus ist.

15

Datenträger, die einem Echtheitsprüfungsverfahren unterzogen werden sollen, weisen meist einen Zähler auf, dessen Stand einen Geldwert repräsentiert und liefern daher einen Kopier- bzw. Nachbuanreiz. Aber auch bei der Verwendung solcher Datenträger bei Zutrittskontrollsystemen oder im Bereich der Sozialversicherungen ist ein solcher Anreiz gegeben.

20

Es ist möglich, einen Halbleiterchip identisch zu kopieren, so daß auch alle Geheimzahlen und verschlüsselten Daten wie das verschlüsselte physikalische Merkmal auf der Kopie enthalten sind, ohne den genauen Schaltungsaufbau verstanden zu haben, so daß hier ein großes Sicherheitsrisiko vorliegt. Die Durchführung einer Echtheitsprüfung mittels eines physikalischen Merkmals, das bei jedem Datenträger anders und möglichst kompliziert ist und somit sehr schwer nachzubauen ist, ist jedoch ein erster Schritt zu einer höheren Fälschungssicherheit, da ein Betrüger zwar einen Chip nachbauen kann aber

30

35

kaum eine dazu passende Karte mit dem richtigen physikalischen Merkmal.

Das bekannte Verfahren bringt hier allerdings noch keine zufriedenstellende Fälschungssicherheit. Da der Vergleich in der Karte bzw. im in der Karte enthaltenen Halbleiterchip stattfindet, ist es möglich, einen Chip oder eine Karte nachzubauen, der oder die immer ein positives Vergleichsergebnis an das Terminal meldet, unabhängig von einem tatsächlich durchgeführten Vergleich. Würde der Vergleich bei dem bekannten Verfahren jedoch im Terminal stattfinden, müßte in jedem Terminal der Verschlüsselungsalgorithmus sowie die geheim zu haltende Schlüsselzahl vorhanden sein, um entweder die gemessenen Daten ebenfalls zu verschlüsseln und die verschlüsselten Formen zu vergleichen oder die aus der Karte ausgelesene verschlüsselte Form der Daten zu entschlüsseln und die Originaldaten zu vergleichen. Dies birgt jedoch erhebliche Sicherheitsrisiken, da es einem Betrüger Anreize bietet, Terminals zu entwenden und zu analysieren.

Das der Erfindung zugrunde liegende Problem ist also, ein Verfahren zur Echtheitsprüfung von Datenträgern anzugeben, das ein hohes Maß an Sicherheit bietet und die oben genannten Nachteile vermeidet.

Das Problem wird durch ein Verfahren gemäß Anspruch 1 gelöst. Eine vorteilhafte Weiterbildung ist im Unteranspruch angegeben.

Beim erfindungsgemäßen Verfahren wird der Vergleich im Terminal durchgeführt, ohne daß der geheime Schlüssel im Terminal vorhanden sein muß, da eine asymmetrische Verschlüsselung verwendet wird. Asymmetrische Verschlüsselung bedeutet, daß zum Verschlüsseln ein anderer Schlüssel verwendet wird als zum Entschlüsseln und selbst bei Kenntnis des jeweils anderen keiner der beiden Schlüssel berechnet werden kann. Der Entschlüsselungsschlüssel kann allgemein bekannt sein und wird

in der Regel jedermann zugänglichen Dateien - beispielsweise aus dem Internet - entnehmbar sein.

Der öffentliche Schlüssel ist hierbei einem bestimmten speziellen Kartensystembetreiber, wie Kreditkartengesellschaften oder Banken und Versicherungen zugeordnet. Wesentlich beim erfindungsgemäßen Verfahren ist, daß der geheime, nur dem Systembetreiber bekannte Schlüssel nicht aus dem öffentlichen Schlüssel berechnet werden kann. Als Beispiel für ein asymmetrisches Verschlüsselungsverfahren wird das RSA-Verfahren genannt.

Wenn lediglich das verschlüsselte Merkmal zum Terminal übertragen wird, ist es nötig, daß im Terminal die öffentlichen Schlüssel sämtlicher Systembetreiber gespeichert oder über beispielsweise einen Intranetanschluß zugreifbar sind, die sich dieses Terminals bedienen wollen. Um diesen Nachteil zu vermeiden, ist in Weiterbildung der Erfindung der öffentliche, spezielle Schlüssel in verschlüsselter Form in der Karte abgespeichert, wobei zu dessen Verschlüsselung ein geheimer, globaler Schlüssel verwendet wurde. Dieser geheime, globale Schlüssel ist beispielsweise nur Zentralbanken oder sonstigen hoheitlichen Institutionen bekannt. Er wird für die Verschlüsselung jedes öffentlichen, speziellen Schlüssels verwendet. In der Karte ist außerdem der unverschlüsselte, öffentliche, spezielle Schlüssel gespeichert.

Im Terminal ist dann lediglich der zum geheimen, globalen Schlüssel gehörende öffentliche, globale Schlüssel enthalten, mittels dem die verschlüsselte Form des öffentlichen, speziellen Schlüssels entschlüsselt und mit dem Originalschlüssel, der ja ebenfalls gespeichert ist, verglichen wird. Eine Übereinstimmung zeigt dann, daß zum Verschlüsseln des öffentlichen, speziellen Schlüssels der richtige geheime, globale Schlüssel verwendet wurde und bedeutet eine Zertifizierung beispielsweise der Zentralbank, die somit dafür bürgt, daß

der öffentliche, spezielle Schlüssel korrekt ist und zum Entschlüsseln des physikalischen Merkmals verwendet werden kann.

Als physikalisches Merkmal kann bei kontaktlosen Datenträgern
5 eine Antenneneigenschaft wie beispielsweise die Güte oder
auch Kombinationen solcher Eigenschaften verwendet werden.
Weitere Möglichkeiten für physikalische Merkmale sind in der
EP 0 676 073 B1 und der EP 0 602 643 A2 angegeben. Dort wer-
den ein einstellbares Widerstandsnetzwerk bzw. die Eigen-
10 schaften einer EEPROM-Zelle als kartenspezifisches, physika-
lisches Merkmal vorgeschlagen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbei-
spiels mit Hilfe einer Figur näher beschrieben. Die Figur
15 zeigt dabei in schematischer Weise eine Chipkarte und ein Le-
se/Schreib-Terminal sowie ein Ablaufdiagramm des erfindungs-
gemäßen Verfahrens.

Die Figur zeigt eine Chipkarte 1, die einen Speicher 2, der
20 beispielsweise in einem Halbleiterchip realisiert sein kann,
sowie ein physikalisches Merkmal X aufweist.

Trotz der Darstellung einer Chipkarte ist die Erfindung kei-
neswegs auf eine solche Ausgestaltung eingeschränkt, sondern
25 kann bei beliebigen Formen von Datenträgern angewendet wer-
den.

Im Speicher 2 ist zumindest die mit einem ersten geheimen,
speziellen Schlüssel $K_{s,s}$ verschlüsselte Form $K_{s,s}[X]$ des Merk-
30 mals X enthalten. Wie durch eine strichliert dargestellte
Vergrößerung des Speichers 2 angedeutet ist, kann in Weiter-
bildung der Erfindung außerdem ein zweiter öffentlicher, spe-
zieller Schlüssel $K_{s,p}$ sowie die verschlüsselte Form dieses
zweiten Schlüssels $K_{g,s}[K_{s,p}]$ enthalten sein. Zum Verschlüsseln
35 des zweiten Schlüssels $K_{s,p}$ wurde ein dritter geheimer, globa-
ler Schlüssel $K_{g,s}$ verwendet.

Durch eine senkrechte, strichlierte Linie von der Chipkarte 1 getrennt ist ein Terminal 3 dargestellt. Dieses weist einen Aufnahmeschacht 4 für die Chipkarte 1 auf sowie eine Tastatur 5 und ein Display 6. Das Terminal 3 weist außerdem einen Speicher 7 auf, in dem wenigstens temporär der zweite öffentliche, spezielle Schlüssel $K_{s,p}$ gespeichert ist. Das Terminal 3 kann diesen Schlüssel einerseits permanent gespeichert haben, aber auch für jede Echtheitsprüfung über eine Datenleitung von einer Zentrale oder aus einem Datennetz holen. Da es sich bei dem zweiten Schlüssel $K_{s,p}$ um einen speziellen Schlüssel handelt, der einem bestimmten Systembetreiber, wie beispielsweise einer Kreditkartenfirma zugeordnet ist, das Terminal 3 jedoch möglicherweise für Karten unterschiedlicher Systembetreiber anwendbar sein soll, wäre es nötig, verschiedene zweite öffentliche, spezielle Schlüssel gespeichert zu halten. Stattdessen kann in Weiterbildung der Erfindung ein vierter öffentlicher, globaler Schlüssel $K_{g,p}$ gespeichert sein, was durch eine strichlierte Erweiterung des Speichers 7 angedeutet ist.

Sowohl die Chipkarte 1 als auch das Terminal 3 können weitere Einrichtungen, wie Mikroprozessoren oder Kryptoprocessoren enthalten. Die Übertragung von der Chipkarte 1 zum Terminal 3 kann sowohl in kontaktbehafter Weise als auch kontaktlos, beispielsweise über induktive Kopplung erfolgen. Das Terminal 3 weist außerdem eine Meßeinrichtung auf, um das physikalische Merkmal X der Chipkarte 1 ermitteln zu können. All diese Details sind nicht in der Figur dargestellt, da sie bereits aus dem Stand der Technik bekannt sind und im Detail nicht zur Erfindung beitragen.

In der Figur ist unter der Darstellung der Chipkarte 1 und des Terminals 3 der Ablauf des erfindungsgemäßen Verfahrens dargestellt. Zwischen horizontalen strichlierten Linien ist die Weiterbildung der Erfindung dargestellt, falls im Terminal 3 lediglich ein öffentlicher, globaler Schlüssel enthalten ist. In diesem Fall wird in einem Verfahrensschritt d)

die verschlüsselte Form des öffentlichen, speziellen Schlüssels sowie der öffentliche, spezielle Schlüssel selbst von der Chipkarte 1 zum Terminal 3 übertragen, im Terminal 3 mittels des öffentlichen, globalen Schlüssels der öffentliche, spezielle Schlüssel berechnet und mit dem übertragenen öffentlichen, speziellen Schlüssel im Verfahrensschritt e) verglichen. Falls keine Übereinstimmung gegeben ist erfolgt ein Abbruch des Verfahrens.

- 10 Bei Übereinstimmung wird im Verfahrensschritt a) die verschlüsselte Form des physikalischen Merkmals von der Chipkarte 1 zum Terminal 3 übertragen sowie das physikalische Merkmal selbst vom Terminal 3 gemessen. Im Terminal wird dann mittels des zuvor übertragenen und als richtig erkannten öffentlichen, speziellen Schlüssels $K_{s,p}$ das verschlüsselte physikalische Merkmal entschlüsselt und mit dem gemessenen verglichen.

- 20 Falls eine Übereinstimmung gegeben ist, wird die Karte im Verfahrensschritt c) als echt erkannt. Falls keine Übereinstimmung gegeben ist, erfolgt ein Abbruch des Verfahrens.

- Bei Anwendung des erfindungsgemäßen Verfahrens brauchen in der Chipkarte 1 lediglich die verschlüsselten Formen des Merkmals X sowie des öffentlichen, speziellen Schlüssels und der öffentliche, spezielle Schlüssel selbst gespeichert sein. Der geheime, spezielle und der geheime, globale Schlüssel brauchen in der Chipkarte 1 nicht vorhanden zu sein, sondern müssen lediglich dem Systembetreiber bzw. der zertifizierenden Stelle bekannt sein. Da die geheimen Schlüssel jedoch eindeutig den zugehörigen öffentlichen Schlüsseln zugeordnet sind, ist es nicht möglich, eine Karte nachzubauen, die die korrekten verschlüsselten Formen der zur Echtheitsprüfung benötigten Daten enthalten.

- 35 Auch eine Entwendung und Analyse eines Terminals 3 seitens eines Betrügers führt nicht zum gewünschten Erfolg, da auch

dort lediglich die öffentlichen und somit auch andersweitig
erhaltbaren Schlüssel gespeichert sind. Sowohl im Datenträger
als auch im Terminal können die geheimen, speziellen und der
geheime, globale Schlüssel enthalten sein, obwohl dies nicht
5 nötig ist, allerdings würde dies zu einem Sicherheitsverlust
führen.

Patentansprüche

1. Verfahren zur Echtheitsprüfung eines Datenträgers (1), insbesondere einer Chipkarte,
- 5 der zumindest einen Speicher (2) aufweist, wobei ein spezifisches, physikalisches Merkmal (X) des Datenträgers (1) in verschlüsselter Form ($K_{s,s}[X]$) in dem Speicher (2) abgelegt ist,
- dadurch gekennzeichnet,
- 10 daß das Merkmal (X) mit einem ersten geheimen, speziellen Schlüssel ($K_{s,s}$) verschlüsselt ist,
- daß ein zum ersten geheimen Schlüssel ($K_{s,s}$) gehörender zweiter spezieller, öffentlicher Schlüssel ($K_{s,p}$) in einem Lese/Schreib-Terminal (3) vorhanden ist,
- 15 daß die folgenden Schritte ausgeführt werden:
- a) das Lese/Schreib-Terminal (3) liest das verschlüsselte Merkmal ($K_{s,s}[X]$) aus dem Speicher (2) des Datenträgers (1) und ermittelt das physikalische Merkmal (X) durch Messung,
- b) das Lese/Schreib-Terminal (3) errechnet mit dem zweiten
- 20 Schlüssel ($K_{s,p}$) das Merkmal ($X=K_{s,p}[K_{s,s}[X]]$) und vergleicht es mit dem gemessenen Merkmal (X)
- c) bei Übereinstimmung wird die Echtheit des Datenträgers (1) festgestellt.
- 25 2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, daß im Datenträger (1) zusätzlich der zweite spezielle, öffentliche Schlüssel ($K_{s,p}$) und die mit einem dritten globalen, geheimen Schlüssel ($K_{g,s}$) verschlüsselte Form des zweiten Schlüssels ($K_{g,s}[K_{s,p}]$) gespeichert ist,
- 30 daß folgende Schritte ausgeführt werden
- d) das Terminal (3) liest diese Daten und errechnet mit einem im Terminal (3) vorhandenen vierten globalen, öffentlichen Schlüssel ($K_{g,p}$) den zweiten Schlüssel ($K_{s,p}=K_{g,p}[K_{g,s}[K_{s,p}]]$) und vergleicht diesen mit dem gelesenen zweiten Schlüssel,
- 35 e) bei Übereinstimmung werden die Verfahrensschritte a) bis c) ausgeführt.

1/1

