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 : G07F 7/10, H04L 9/26

A3

(11) Internationale Veröffentlichungsnummer: **WO 97/46983**

(43) Internationales Veröffentlichungsdatum: 11. Dezember 1997 (11.12.97)

(21) Internationales Aktenzeichen: PCT/EP97/02894

(22) Internationales Anmeldedatum: 4. Juni 1997 (04.06.97)

(30) Prioritätsdaten:
196 22 533.7 5. Juni 1996 (05.06.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHAEFER-LORINSER, Frank [DE/DE]; Potsdamer Strasse 88, D-64372 Ober-Ramstadt (DE). SCHEERHORN, Alfred [DE/DE]; Ahornallee 3, D-49716 Meppen (DE).

(81) Bestimmungsstaaten: AU, BR, CA, CN, HU, JP, KR, MX, NO, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 26. Februar 1998 (26.02.98)

(54) Title: METHOD AND DEVICE FOR LOADING INPUT DATA INTO AN ALGORITHM DURING AUTHENTICATION

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM LADEN VON INPUTDATEN IN EINEN ALGORITHMUS BEI DER AUTHENTIKATION

(57) Abstract

The problem associated with data security during payment transactions using smart cards lies in the processes involved in loading input data into an algorithm during authentication. According to the invention, the security of the withdrawal and charging data is improved by dividing the data blocks and switching an additional feedback to the downstream counters on and off at pre-selected times (cycles). The invention can be used in all authentication processes involving smart cards.

(57) Zusammenfassung

Die Problematik der Datensicherheit beim Zahlungsverkehr mit Hilfe von Chipkarten liegt in den Vorgängen beim Laden von Inputdaten in einen Algorithmus bei der Authentikation begründet. Mit Hilfe einer Aufteilung der Datenblöcke und der Ein- und Ausschaltung einer zusätzlichen Rückkopplung nach den nachgeschalteten Zählern zu vorgewählten Zeiten (Takten) wird die Sicherheit der Ab- und Aufbuchungs-Daten verbessert. Die Anwendung der Erfindung ist bei allen Authentikationsvorgängen in Verbindung mit Chipkarten 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	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		

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/EP 97/02894

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 H04L9/26

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 G07F H04L

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.
A	DE 44 19 805 A (GIESECKE & DEVRIENDT) 7 December 1995 see abstract; claims; figures see column 5, line 63 - column 6, line 31	1,2,5,6, 9,13
A	EP 0 409 701 A (ETAT FRANCAIS) 23 January 1991	
A	FR 2 471 003 A (ELECTRONIQUE MARCEL DASSAULT) 12 June 1981	

☐ 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

1

Date of the actual completion of the international search	Date of mailing of the international search report
11 November 1997	05. 12. 97

Name and mailing address of the ISA	Authorized officer
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	David, J

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ›nal Application No
PCT/EP 97/02894

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4419805 A	07-12-95	AU 2787295 A	04-01-96
		CA 2168891 A	14-12-95
		CN 1131991 A	25-09-96
		WO 9534054 A	14-12-95
		EP 0712520 A	22-05-96
		JP 9501529 T	10-02-97
EP 0409701 A	23-01-91	FR 2650097 A	25-01-91
		DE 69012692 D	27-10-94
		DE 69012692 T	19-01-95
		JP 3141487 A	17-06-91
		US 5128997 A	07-07-92
FR 2471003 A	12-06-81	NONE	

INTERNATIONALER RECHERCHENBERICHT

Inte. onales Aktenzeichen
PCT/EP 97/02894

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10 H04L9/26

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F H04L

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.
A	DE 44 19 805 A (GIESECKE & DEVRIENDT) 7.Dezember 1995 siehe Zusammenfassung; Ansprüche; Abbildungen siehe Spalte 5, Zeile 63 - Spalte 6, Zeile 31 ---	1,2,5,6, 9,13
A	EP 0 409 701 A (ETAT FRANCAIS) 23.Januar 1991 ---	
A	FR 2 471 003 A (ELECTRONIQUE MARCEL DASSAULT) 12.Juni 1981 -----	

☐ 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
11.November 1997	05. 12. 97

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
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	David, J

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

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP 97/02894

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4419805 A	07-12-95	AU 2787295 A	04-01-96
		CA 2168891 A	14-12-95
		CN 1131991 A	25-09-96
		WO 9534054 A	14-12-95
		EP 0712520 A	22-05-96
		JP 9501529 T	10-02-97
EP 0409701 A	23-01-91	FR 2650097 A	25-01-91
		DE 69012692 D	27-10-94
		DE 69012692 T	19-01-95
		JP 3141487 A	17-06-91
		US 5128997 A	07-07-92
FR 2471003 A	12-06-81	KEINE	