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 | A3

(11) Internationale Veröffentlichungsnummer: WO 98/48389

(43) Internationales Veröffentlichungsdatum: 29. Oktober 1998 (29.10.98)

(21) Internationales Aktenzeichen: PCT/EP98/02231

(22) Internationales Anmeldedatum: 16. April 1998 (16.04.98)

(30) Prioritätsdaten:
197 16 111.1 17. April 1997 (17.04.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D–81677 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: FRÖHLICH, Hans–Hermann [DE/DE]; Josephsburgstrasse 5, D–81673 München (DE). GALL, Winfried [DE/DE]; Zirlweg 9, D–85652 Pliening (DE).

(74) Anwalt: KLUNKER, SCHMITT–NILSSON, HIRSCH; Winzererstrasse 106, D–80797 München (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, 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, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, 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, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 28. Januar 1999 (28.01.99)

(54) Title: METHOD FOR MUTUAL AUTHENTICATION BETWEEN TWO UNITS

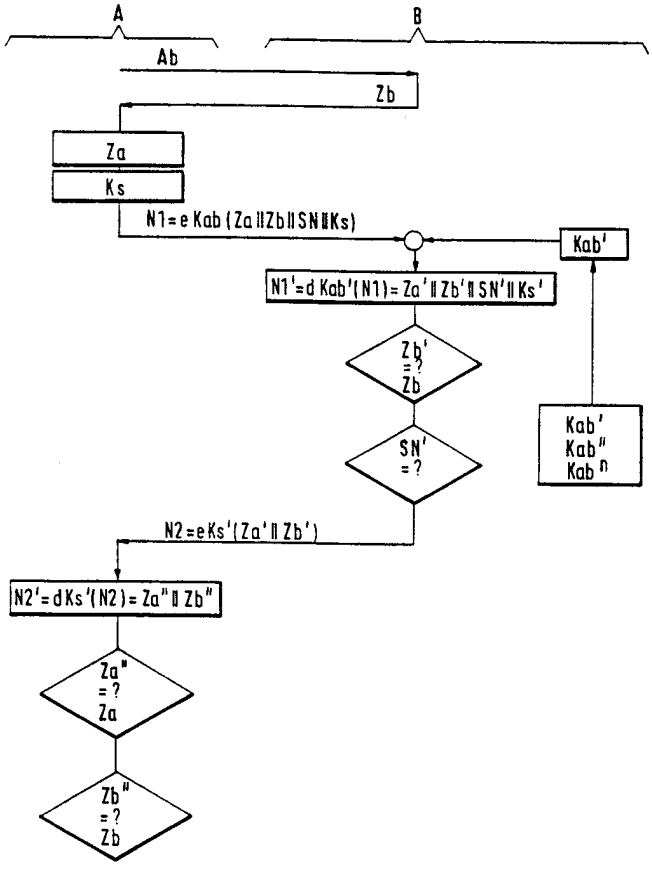
(54) Bezeichnung: VERFAHREN ZUR GEGENSEITIGEN AUTHENTIFIZIERUNG ZWEIER EINHEITEN

(57) Abstract

The invention relates to a method for mutual authentication between two units that communicate with each other. An encrypted message sent from unit A to unit B is transmitted along with a key differing from the one used to encrypt the message from unit A. Unit B then encrypts the message addressed to unit A using the key received from unit A, on the basis of which unit B is authenticated by unit A

(57) Zusammenfassung

Die Erfindung betrifft ein Vefahren zur gegenseitigen Authentifizierung zweier miteinander kommunizierender Einheiten, wobei in der von einer Einheit A an eine Einheit B in chiffrierter Form übermittelten Nachricht ein Schlüssel mitübertragen wird, der von dem zur Verschlüsselung der Nachricht von der Einheit A verwendeten Schlüssel verschieden ist. Die Einheit B verschlüsselt dann mit Hilfe des von der Einheit A empfangenen Schlüssels die für die Einheit A bestimmte Nachricht, anhand der die Enheit B von der Einheit A authentifiziert wird.



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

Int. ional Application No
PCT/EP 98/02231

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 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 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.
X	EP 0 548 967 A (GAO GES AUTOMATION ORG) 30 June 1993 see column 2, line 45 - column 5, line 58; figures 2,3	1,3
A	EP 0 440 800 A (NTT DATA TSUSHIN KK) 14 August 1991 see abstract see column 6, line 30 - column 7, line 26 see column 8, line 48 - column 9, line 13 see figure 5	1,3,4
A	FR 2 600 188 A (BULL CP8) 18 December 1987 see page 5, line 22 - page 11, line 22	1,2

-/--

[X] Further documents are listed in the continuation of box C.

[X] 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
27 October 1998	04/11/1998

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	Bocage, S

2

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

INTERNATIONAL SEARCH REPORT

Int .tional Application No
PCT/EP 98/02231

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 see abstract see page 3, line 27 - page 5, line 30 see figure 3 ---	4,5
A	EP 0 253 722 A (BULL CP8) 20 January 1988 see abstract see column 2, line 9 - line 57 -----	4

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/EP 98/02231

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0548967 A	30-06-1993	DE 4142964 A	01-07-1993
		JP 5274493 A	22-10-1993
		SG 43321 A	17-10-1997
		US 5317637 A	31-05-1994
EP 0440800 A	14-08-1991	JP 2731945 B	25-03-1998
		JP 3007399 A	14-01-1991
		WO 9014962 A	13-12-1990
FR 2600188 A	18-12-1987	NONE	
FR 2681165 A	12-03-1993	NONE	
EP 0253722 A	20-01-1988	FR 2601795 A	22-01-1988
		CA 1284223 A	14-05-1991
		DE 3783171 A	04-02-1993
		WO 8800744 A	28-01-1988
		HK 91995 A	16-06-1995
		JP 1500933 T	30-03-1989
		JP 2690923 B	17-12-1997
		US 4811393 A	07-03-1989

INTERNATIONALER RECHERCHENBERICHT

Int. ionales Aktenzeichen
PCT/EP 98/02231

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 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 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.
X	EP 0 548 967 A (GAO GES AUTOMATION ORG) 30. Juni 1993 siehe Spalte 2, Zeile 45 - Spalte 5, Zeile 58; Abbildungen 2,3 ---	1,3
A	EP 0 440 800 A (NTT DATA TSUSHIN KK) 14. August 1991 siehe Zusammenfassung siehe Spalte 6, Zeile 30 - Spalte 7, Zeile 26 siehe Spalte 8, Zeile 48 - Spalte 9, Zeile 13 siehe Abbildung 5 ---	1,3,4
A	FR 2 600 188 A (BULL CP8) 18. Dezember 1987 siehe Seite 5, Zeile 22 - Seite 11, Zeile 22 ---	1,2

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] 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
27. Oktober 1998	04/11/1998

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	Bocage, S

2

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

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/02231

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	FR 2 681 165 A (GEMPLUS CARD INT) 12. März 1993 siehe Zusammenfassung siehe Seite 3, Zeile 27 - Seite 5, Zeile 30 siehe Abbildung 3	4,5
A	EP 0 253 722 A (BULL CP8) 20. Januar 1988 siehe Zusammenfassung siehe Spalte 2, Zeile 9 - Zeile 57	4

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

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 98/02231

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0548967 A	30-06-1993	DE 4142964 A	01-07-1993
		JP 5274493 A	22-10-1993
		SG 43321 A	17-10-1997
		US 5317637 A	31-05-1994
EP 0440800 A	14-08-1991	JP 2731945 B	25-03-1998
		JP 3007399 A	14-01-1991
		WO 9014962 A	13-12-1990
FR 2600188 A	18-12-1987	KEINE	
FR 2681165 A	12-03-1993	KEINE	
EP 0253722 A	20-01-1988	FR 2601795 A	22-01-1988
		CA 1284223 A	14-05-1991
		DE 3783171 A	04-02-1993
		WO 8800744 A	28-01-1988
		HK 91995 A	16-06-1995
		JP 1500933 T	30-03-1989
		JP 2690923 B	17-12-1997
		US 4811393 A	07-03-1989