PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10, H04L 9/08

A3

(11) International Publication Number: **WO 99/16031**

(43) International Publication Date: 1 April 1999 (01.04.99)

(21) International Application Number: PCT/US98/19756

(22) International Filing Date: 22 September 1998 (22.09.98)

(30) Priority Data:
08/934,838 22 September 1997 (22.09.97) US

(71) Applicant *(for all designated States except US)*: VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; 900 Metro Center Boulevard, MS M1-11A, Foster City, CA 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: DENNO, Rodney, G. [US/US]; 3371 Muscat Court, Pleasanton, CA 94566 (US). JOHNSON, Lance, J. [US/US]; 1029 Rossi Way, San Mateo, CA 94403 (US).

(74) Agent: MASCHOFF, Kurt, M.; Visa International Service Association, 900 Metro Center Boulevard, MS M1-11A, Foster City, CA 94404 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, 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), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European 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).

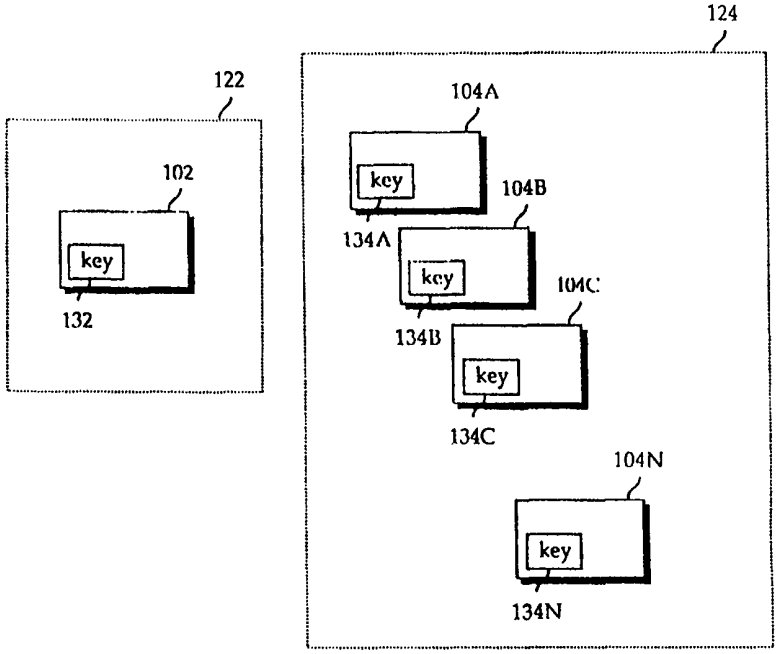
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
8 July 1999 (08.07.99)

(54) Title: METHOD AND APPARATUS FOR ASYMMETRIC KEY MANAGEMENT IN A CRYPTOGRAPHIC SYSTEM

(57) Abstract

A method and apparatus for asymmetrical key management in a cryptographic system is provided. Embodiments of the invention implement varying levels of diversification to manage the encryption keys. In one embodiment, a unique key per device approach is used that minimizes the risks due to unauthorized key access. In yet another embodiment, a unique key per device per transaction is used. The keys generated in embodiments of the invention can be used to authenticate one device with another. An authenticating device generates a current key that is initially unknown to an unauthenticated device. The authenticating device sends information to an unauthenticated device to assist it in determining the value of the current key. The unauthenticated device uses the determined value of the current key to derive the authenticating device's authentication value. Each device generates an authentication value that must be correctly determined by an unauthenticated device for successful authentication. Authentication is performed between two devices such that each device is authenticated with the other device. Computing devices of a system can be grouped. In one embodiment devices are grouped such that one group includes devices that have a master key and another group includes devices that have a key that is derived from the master key. Another embodiment includes groups whose devices have the group's master key and a key derived from each of the master keys of the other group(s). In this embodiment, a dual authentication process can be used to authenticate two devices from different groups.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/US 98/19756

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 H04L9/08

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 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 A	EP 0 253 722 A (BULL CP8) 20 January 1988 see abstract; claims; figures see column 3, line 24 - column 5, line 26	1,42 7-10, 44-46
A	EP 0 548 967 A (GAO) 30 June 1993 see the whole document	11,17, 20-24, 28-31, 35-41
A	US 4 605 820 A (C.M. CAMPBELL) 12 August 1986 see abstract; claims; figures 1,2,8	1-4, 12-16, 18,19, 32-34, 42,43

-/--

[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
12 May 1999	21/05/1999

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

1

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

INTERNATIONAL SEARCH REPORT

Intern. al Application No
PCT/US 98/19756

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 0 440 800 A (NTT DATA COMMUNICATIONS SYSTEMS) 14 August 1991 see abstract; claims; figures 1,2,5,6 see column 1, line 55 - column 2, line 41	1,9-11, 16-23, 28-31, 37,39, 42,44-46
A	FR 2 681 165 A (GEMPLUS CARD INTERNATIONAL) 12 March 1993	
A	FR 2 600 190 A (BULL CP8) 18 December 1987	
A	EP 0 552 392 A (SIEMENS NIXDORF INFORMATIONSSYSTEME) 28 July 1993	
A	US 3 764 742 A (G.F. ABBOTT) 9 October 1973	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna al Application No
PCT/US 98/19756

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0253722 A	20-01-1988	FR 2601795 A	22-01-1988
		AT 83869 T	15-01-1993
		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
EP 0548967 A	30-06-1993	DE 4142964 A	01-07-1993
		AT 172565 T	15-11-1998
		DE 59209537 D	26-11-1998
		ES 2121811 T	16-12-1998
		JP 5274493 A	22-10-1993
		SG 43321 A	17-10-1997
		US 5317637 A	31-05-1994
US 4605820 A	12-08-1986	NONE	
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 2681165 A	12-03-1993	NONE	
FR 2600190 A	18-12-1987	NONE	
EP 0552392 A	28-07-1993	AT 136139 T	15-04-1996
		DE 59205856 D	02-05-1996
		ES 2084846 T	16-05-1996
US 3764742 A	09-10-1973	CA 957948 A	19-11-1974
		DE 2253275 A	05-07-1973
		FR 2164939 A	03-08-1973
		GB 1399020 A	25-06-1975