PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, G07F 7/08

A3

(11) International Publication Number: **WO 97/45979**

(43) International Publication Date: 4 December 1997 (04.12.97)

(21) International Application Number: PCT/US97/08265

(22) International Filing Date: 16 May 1997 (16.05.97)

(30) Priority Data:
08/650,888 17 May 1996 (17.05.96) US

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

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ABRAHAM, Dennis, G. [US/US]; 5795 Gettysburg Drive, Concord, NC 28027 (US). HITE, Richard, K. [US/US]; 938 Buttercup Place, Manteca, CA 95336 (US).

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

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, 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).

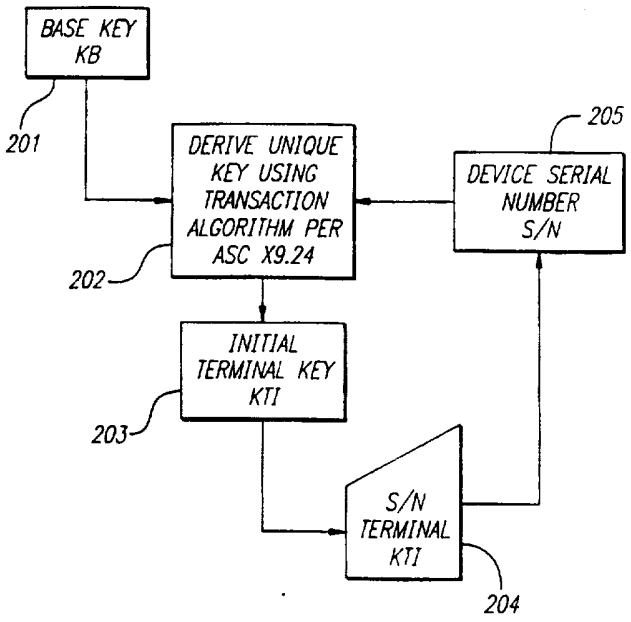
Published
With international search report.

(88) Date of publication of the international search report:
26 February 1998 (26.02.98)

(54) Title: METHOD AND APPARATUS FOR INITIALIZATION OF CRYPTOGRAPHIC TERMINAL

(57) Abstract

The present invention provides a method and apparatus for initializing cryptographic terminals in a cryptographic system. The invention provides a base key (201) that is common to all controllers produced by a manufacturer of cryptographic terminals in each controller prior to shipment of the controllers. The base key (201) is used only for the purposes of initialization of cryptographic terminals, and is not used for normal operations. Each cryptographic terminal that is to be used with any of the controllers containing the common base key (203) is derived from the particular terminal's serial number (205) and the common base key (201). The initial key (203) is only for initialization purposes and not for system operation. The terminal and controller establish communications in a normal manner using whatever communication protocol is appropriate for them. Upon installation, the controller and terminal enter into communications whereby the controller is able to securely determine the initial key (203) contained in the terminal since the controller contains the base key (201).



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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08265

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/32; G07F 7/08
US CL :380/24, 21, 25; 902/2

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)

U.S. : 380/24, 21, 25; 902/2

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 practicable, 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.
E, A	US 5,661,806 A (NEVOUX et al) 26 August 1997, col. 2, lines 25-33.	1-23
A	US 5,323,465 A (AVARNE) 21 June 1994, col. 3, lines 23-42.	1-23
A	US 5,249,230 A (MIHM, JR.) 28 September 1993, col. 6, line 48-col. 7, line 66.	1-23
A	US 5,150,412 A (MARU) 22 September 1992, col. 3, lines 1-3.	1-23
A	US 4,984,270 A (LABOUNTY) 08 January 1991, col. 3, lines 32-52.	1-23
A	US 4,912,762 A (LEE et al) 27 March 1990, col. 8, lines 5-19.	1-23

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 20 OCTOBER 1997	Date of mailing of the international search report 01 DEC 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRÓN JR. Telephone No. (703) 306-4177

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08265

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,630,201 A (WHITE) 16 December 1986, col. 6, lines 4-44.	1-23
A	US 4,578,530 A (ZEIDLER) 25 March 1986, col. 11, line 59-col. 12, line 68.	1-23
A	US 4,317,957 A (SENDROW) 02 March 1982, col. 6, lines 17-39.	1-23