(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 January 2003 (09.01.2003)

PCT

(10) International Publication Number
WO 03/003171 A3

(51) International Patent Classification[7]: H04L 9/32, G07F 7/10

(21) International Application Number: PCT/EP02/06674

(22) International Filing Date: 17 June 2002 (17.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/892,904 28 June 2001 (28.06.2001) US

(71) Applicant: **ACTIVCARD** [FR/FR]; -, 24-28 avenue du Général de Gaulle, F-92156 Suresnes Cedex (FR).

(72) Inventors: **AUDEBERT, Yves, Louis, Gabriel**; -, 237 Forrester Road, Los Gatos, CA 95032 (US). **LE SAINT, Eric, F.**; -, 1161 Chopin Terrace # 300, Freemont, CA 94538 (US).

(74) Agent: **CABINET JP COLAS**; -, 37 avenue Franklin D. Roosevelt, F-75008 Paris (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

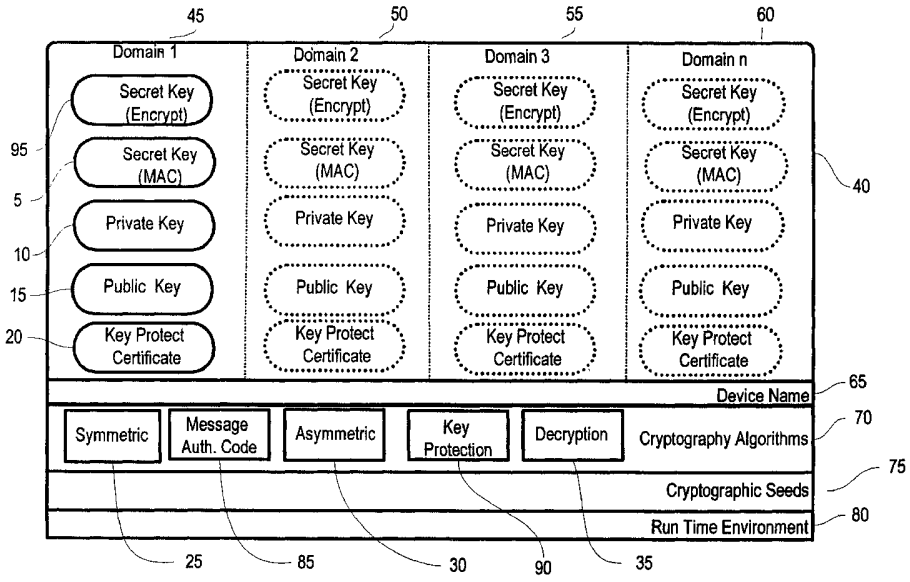
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
17 April 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD AND SYSTEM FOR GENERATING AND VERIFYING A KEY PROTECTION CERTIFICATE.



(57) Abstract: A data processing method and system for generating and verifying a key protection certificate. The data processing system comprises a Personal Security Device (40) including a unique device name (65), cryptography means, data processing means, data storage means and communications means. The cryptography means includes an asymmetric key pair generating algorithm (30), a first securely shared secret key, a second securely shared secret key, symmetric cryptography means, a concatenation algorithm, a message authentication code algorithm, cryptographic seed information (75), a key protection certificate algorithm (90) and a signing algorithm.

WO 03/003171 A3

INTERNATIONAL SEARCH REPORT

Interr hal Application No
PCT/EP 02/06674

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 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 7 H04L G07F

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)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MENEZES A J ET AL: "HANDBOOK OF APPLIED CRYPTOGRAPHY, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, page 552, 560, 564 XP002224033 ISBN: 0-8493-8523-7 page 33 page 552; figure 13.4 page 560, line 12 - line 25 page 564; figures 13.7,A ---	1-29
Y	EP 0 807 911 A (RSA DATA SECURITY INC) 19 November 1997 (1997-11-19) column 1, line 1 - line 20 column 13, line 24 -column 15, line 9 --- -/--	1-29

[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
11 December 2002	10/01/2003

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	Carnerero Álvaro, F

3

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

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DATABASE INSPEC 'Online! THE INSTITUTION OF ELECTRICAL ENGINEERS, STEVENAGE, GB; March 2000 (2000-03) STUHLMULLER R: "User identity: the key to safe authentication LAN/WAN security" Database accession no. 6574108 XP002224034 abstract ----	1-29

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/EP 02/06674

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0807911 A	19-11-1997	US 6085320 A	04-07-2000
		EP 0807911 A2	19-11-1997
		JP 11003033 A	06-01-1999
		US 6189098 B1	13-02-2001