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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 September 2002 (19.09.2002)

PCT

(10) International Publication Number
WO 02/073861 A3

(51) International Patent Classification[7]: H04L 9/00, 9/32, G06F 11/30, 12/14

(21) International Application Number: PCT/US02/07392

(22) International Filing Date: 11 March 2002 (11.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/274,457 9 March 2001 (09.03.2001) US
10/093,881 8 March 2002 (08.03.2002) US

(71) Applicant: **ARCOT SYSTEMS, INC.** [US/US]; 3200 Patrick Henry Drive, Suite 200, Santa Clara, CA 95054 (US).

(72) Inventors: **ALLEN, Robert**; 64 Roosevelt Circle, Palo Alto, CA 94306 (US). **JERDONEK, Robert, A.**; 454-C Costa Mesa Terrace, Sunnyvale, CA 94085 (US). **WANG, John**; 1265 Lakeside Drive #1175, Sunnyvale, CA 94085 (US). **WU, Tom**; 842 North Rengstorff Avenue, Apt. E, Mountain View, CA 94043 (US).

(74) Agents: **ALBERT, Philip, H.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), 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 (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

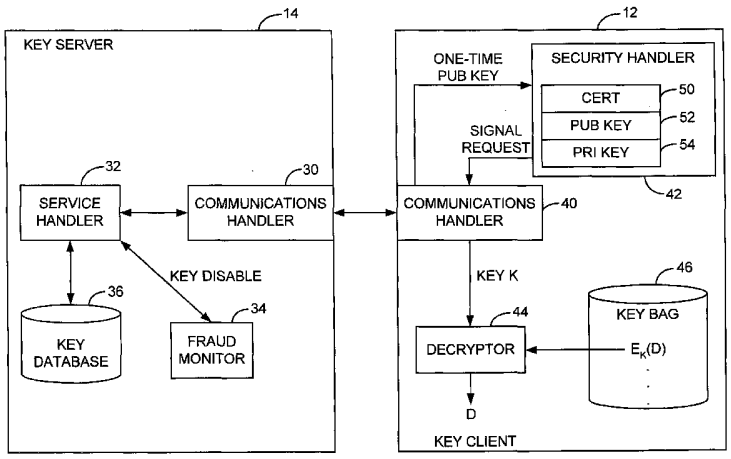
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,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

Published:
— *with international search report*

(88) Date of publication of the international search report:
30 October 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: METHOD AND APPARATUS FOR CRYPTOGRAPHIC KEY STORAGE WHEREIN KEY SERVERS ARE AUTHENTICATED BY POSSESSION AND SECURE DISTRIBUTION OF STORED KEYS



(57) Abstract: A key management system includes secured data stored on a first system secured by a control key stored securely on a key server. The secured data is secured against attacks such as unauthorized use, modification or access, where authorization to access the secured data is determined by knowledge of an access private key of an access key pair. When an authorized user is to access the secured data, the first system generates a request to the key server, signed with the access private key, wherein the request is for a decryption control key and the request includes a one-time public key of a key pair generated by the first system for the request. The first system can decrypt the decryption control key from the response, using a one-time private key. The first system can then decrypt the secured data with the decryption control key remaining secured in transport.

WO 02/073861 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/07392

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00, 9/32; G06F 11/30, 12/14

US CL :Please See Extra Sheet.

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. : 713/150, 168, 176, 189, 193, 200, 201; 380/277, 278, 279, 281, 282

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)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,606,617 A (BRANDS) 25 FEBRUARY 1997, SEE ENTIRE DOCURMENT	1-7
A,P	US 2002/0026582 A1 (FUTAMURA ET AL) 28 FEBRUARY 2002, SEE ENTIRE DOCUMENT	1-7
A,P	US 2002/0016913 A1 (WHEELER ET AL) 07 FEBRUARY 2002, SEE ENTIRE DOCUMENT	1-7

☐ 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 03 JUNE 2002	Date of mailing of the international search report 20 JUN 2002
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 GAIL HAYES Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/07392

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

713/150, 168, 176, 189, 193, 200, 201; 380/277, 278, 279, 281, 282

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS (files: USPAT, DERWENT, JPO, EPO, IBM TDB'S, US PGPUBS), DIALOG (files: COMPSCI, ELECTRON, SOFTWARE)

search terms: one, time, onetime, key, public, private, server, provider, vendor, source, sign, signed, signing, signature, secure, secured, securing, security, protect, protected, protective, protection, protecting, sensitive, classified, classify, classification, classifying