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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2002 (30.05.2002)

PCT

(10) International Publication Number
WO 02/043309 A3

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

(21) International Application Number: PCT/US01/46290

(22) International Filing Date: 19 October 2001 (19.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/242,083 20 October 2000 (20.10.2000) US
60/246,843 8 November 2000 (08.11.2000) US

(71) Applicant: WAVE SYSTEMS CORPORATION [US/US]; 480 Pleasant Street, Suite B200, Lee, MA 01238 (US).

(72) Inventor: KRAVITZ, David, W.; 3910 Ridgelea Drive, Fairfax, VA 22031 (US).

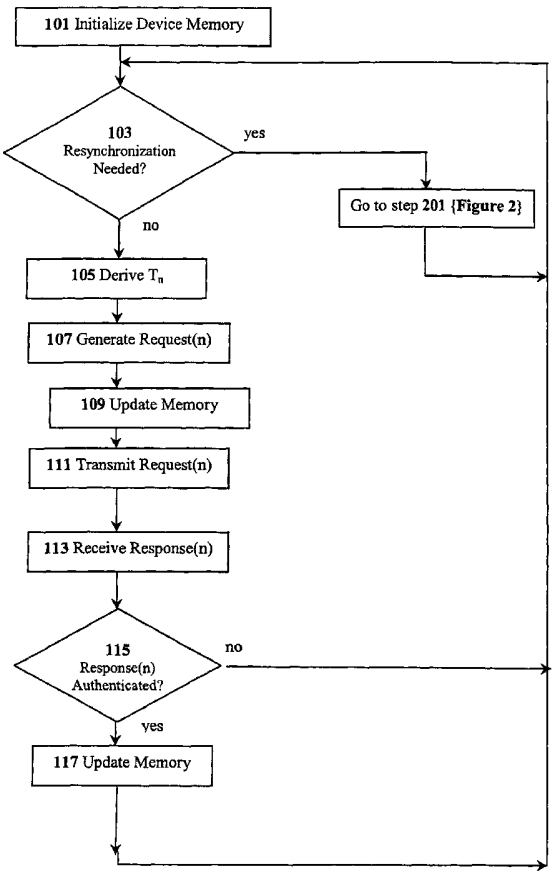
(74) Agents: BUTTER, Gary, M. et al.; Baker Botts, LLP, 30 Rockefeller Plaza, New York, NY 10112-0228 (US).

(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, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, 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,

[Continued on next page]

(54) Title: CRYPTOGRAPHIC DATA SECURITY SYSTEM AND METHOD



(57) Abstract: A method for communicating between a computer device and a trusted server is disclosed. According to the method of the invention, a one-time password for use in communication from the device (105) to the server is generated. The device (105) generates at least one on-time request-authentication datum (107) that includes a function of at least a portion of a previous response (113) from the server to previous message from the device (105). The server then generates at least one on-time response authentication datum (113) that includes a function of at least a portion of at least one-time password.

WO 02/043309 A3

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:
6 February 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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/46290

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/32
US CL : 713/202
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. : 380/21,23,25,37, 43, 49,50

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 Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,841,871 B1 (PINKAS) 24 November 1998 (24.11.1998), abstract, column 4, lines 1-67, column 9, column 5, lines 9-20, column 9, lines 34-65, Fig. 1-2. Column 9, lines 13-34, column 12, line30-45	1-10 ---------- 11-36
Y, P	US 6,148,404 A (YATSUKAWA) 14 November 2000 (14.11.2000), abstract, column 15, lines 20-64, lines 65-67 through column 16, lines 1-2, lines 33-67, column 17, lines 1-35, lines 65-67 through column 18, lines 1-9, Fig.16, column 19, lines 46-67, column 23, lines 26-47, column 24, lines 38-65.	11-36
Y	US 5,661,807 A (GUSKI et al) 26 August 1997 (26.08.1997), the entire document.	1-36
Y	5,241,599 A (BELLOVIN et al.) 31 August 1993 (31.08.1993), the enitire document.	1-36

☐ Further documents are listed in the continuation of Box C. ☐ See patent family 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 application or patent 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
01 June 2002 (01.06.2002)

Date of mailing of the international search report
09 JUL 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 O Hayes Peggy Harrod
Telephone No. (703) 305-4274

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

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/46290

Continuation of B. FIELDS SEARCHED Item 3:
WEST, Dialog, ProQuest, Dogpile. Search Terms: one time password and authentication, kerberos password and one time password, password and authentication, client/server session key.