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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001629 A3

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2004/018048

(22) International Filing Date: 4 June 2004 (04.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/607,195 25 June 2003 (25.06.2003) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 10/607,195 (CON)
Filed on 25 June 2003 (25.06.2003)

(71) Applicant *(for all designated States except US)*: **VOLTAGE SECURITY, INC.** [US/US]; 1070 Arastradero Road, Suite 100, Palo Alto, CA 94304 (US).

(72) Inventors; and

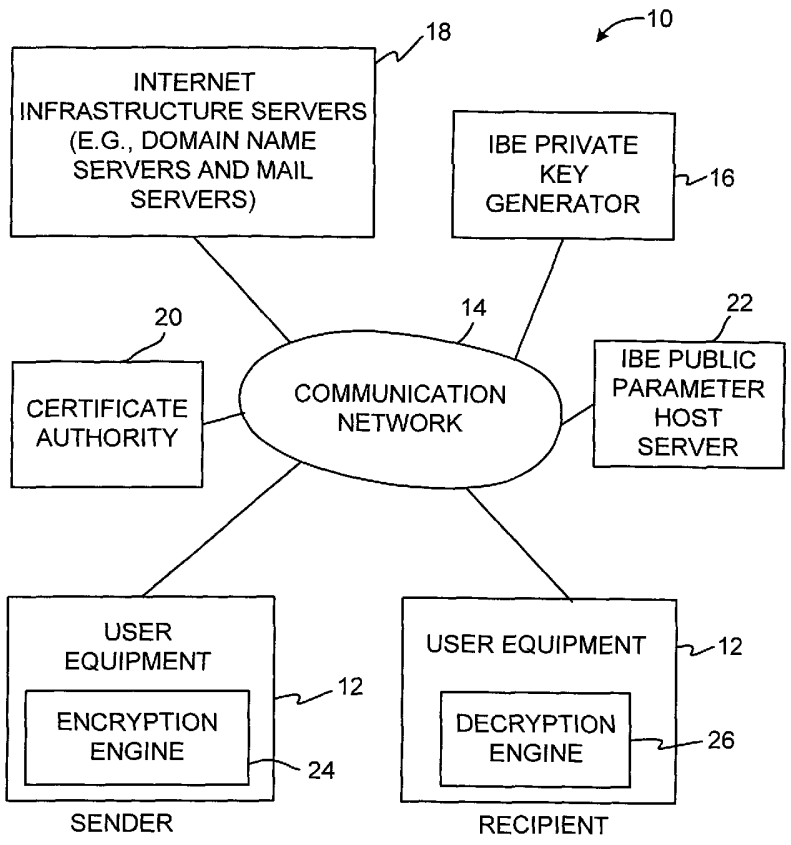
(75) Inventors/Applicants *(for US only)*: **SPIES, Terence** [US/US]; 826 Warfside Road, San Mateo, CA (US). **KACKER, Rishi, R.** [US/US]; 2128 Stockbridge Road, Woodside, CA 94062 (US). **APPENZELLER, Guido** [DE/US]; 1035 Noel Drive, Apt. F, Menlo Park, CA 94025 (US). **PAUKER, Matthew, J.** [US/US]; 15 Red Rock Way, N106, San Francisco, CA 94131 (US). **RESCORLA, Eric** [US/US]; 2064 Edgewood Drive, Palo Alto, CA 94303 (US).

(74) Agent: **TREYZ, Victor, G.**; Flood Building, Suite 984, 870 Market Street, San Francisco, CA 94102 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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,

[Continued on next page]

(54) Title: ENCRYPTION SYSTEM WITH PUBLIC PARAMETER HOST SERVERS



(57) Abstract: A system is provided that uses identity-based encryption (IBE) to support secure communications. Messages from a sender may be encrypted using an IBE public key and IBE public parameter information associated with a recipient. The recipient may decrypt IBE-encrypted messages from the sender using an IBE private key. A host having a service name may be used to store the IBE public parameter information. The sender may use a service name generation rule to generate the service name based on the IBE public key of the recipient. The sender may use the service name to obtain the IBE public parameter information from the host.

WO 2005/001629 A3

MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *with international search report*

(88) Date of publication of the international search report:
26 May 2005

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/US04/18048

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/200
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. : 713/200 713/156,175;380/21,49,277;709/206,225,238

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.
Y	THE HP TIME VAULT SERVICE: INNOVATING THE WAY CONFIDENTIAL INFORMATION IS DISCLOSED, AT THE RIGHT TIME (Marco Casassa Mont) 04 September 2002, see entire document.	1-24
Y	US 6,061,448 A (Smith) 09 May 2000, see entire document.	1-24
Y	US 2002/0188690 A1 (Lee) 12 December 2002, see entire document.	1-24
Y	US 2003/0081785 A1 (Boneh et al.) 01 May 2003, see entire document.	4
Y,P	US 2003/0163567 A1 (McMorris) 28 August 2003, see entire document.	10
Y,P	US 2003/0198348 A1 (Mont. et al.) 23 October 2003, see entire document.	18
Y	US 2002/0169857 A1 (Martija) 14 November 2002, see entire document.	23
A,P	US 2003/0182554 A1 (Gentry et al.) 25 September 2003.	1-24

☒ 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
15 January 2005 (15.01.2005)

Date of mailing of the international search report
15 FEB 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
BRIAN JOHNSON for James R. Matthews
Telephone No. (571) 272-3595

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/18048

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 2003/0179885 A1 (Gentry et al.) 25 September 2003.	1-24
A,P	US 2003/0120733 A1 (Forman) 26 June 2003.	1-24
A	US 6,396,830 B2 (Aravamudan et al.) 28 May 2002.	1-24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/18048

Continuation of B. FIELDS SEARCHED Item 3:
USPAT;US-PGPUB;EPO;JPO;DERWENT
host,authority,asymmetric,public,compute,identity,address,name,parameter