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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2008 (17.07.2008)

PCT

(10) International Publication Number
WO 2008/085579 A3

(51) International Patent Classification:
H04L 9/14 (2006.01)

(21) International Application Number:
PCT/US2007/082564

(22) International Filing Date: 25 October 2007 (25.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/862,945 25 October 2006 (25.10.2006) US

(71) Applicant *(for all designated States except US)*: **SPYRUS, INC.** [US/US]; 1860 Hartog Drive, San Jose, CA 95131-2203 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JUENEMAN, Richard R.** [US/US]; 1276 Belbrook Way, Milipitas, CA 95035-3117 (US). **LINSENBARDT, Duane J.** [US/US]; 5532 Sweigert Road, San Jose, CA 95132-3402 (US). **YOUNG, John N.** [US/US]; 1467 Myrtle Avenue, San Jose, CA 95118-1143 (US). **CARLISLE, William Reid** [US/US]; 1728 Bright Waters NE, St. Petersburg, FL 33704-3816 (US).

(74) Agents: **ROSE, Robert J.** et al.; Sheldon Mak Rose & Anderson PC, 100 East Corson Street, Third Floor, Pasadena, CA 91103-3842 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, IS, IT, LT, LU, LV, MC, MT, 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).

Published:
— *with international search report*

(88) Date of publication of the international search report:
4 December 2008

(54) Title: METHOD AND SYSTEM FOR DEPLOYING ADVANCED CRYPTOGRAPHIC ALGORITHMS

(57) Abstract: A method and system for deploying a suite of cryptographic algorithms including: providing a legacy cryptographic interface associated with a legacy operating system and a legacy application, and supports a suite of legacy cryptographic algorithms; providing a suite of advanced cryptographic algorithms that includes one or more of an advanced asymmetric key algorithm, an advanced symmetric key algorithm, and/or an advanced hash function; providing an advanced cryptographic interface that is independent of the legacy operating system and the legacy application, backwards compatible with the legacy cryptographic interface, and capable of supporting the suite of advanced cryptographic algorithms; and transparently and automatically substituting the suite of advanced cryptographic algorithms for the legacy cryptographic algorithms through the invocation of the advanced cryptographic interface at the time of an initial performance of encrypting, hashing, digitally signing the hash of, decrypting, re-hashing, and/or validating the digital signature of an item.

WO 2008/085579 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/082564

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14(2006.01)i

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 8 H04L 9/14, H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility Models and applications for Utility Models since 1975
Japanese Utility Models and applications for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
e-KIPASS(KIPO internal): "cryptographic", "algorithm"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2006-0149962 A1 (THOMAS FOUNTAIN et al.) 06 July 2006 see the abstract and claim 1.	1-25
A	US2006-0133616 A1 (YUN-JOO KIM et al.) 22 June 2006 see the abstract and claim 10.	1-25
A	KR10-2003-0043451 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 02 June 2003 see the abstract and claim 1.	1-25
A	KR10-2004-0000925 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 07 January 2004 see the abstract and figures 4(a)-4(b).	1-25

☐ 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 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 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
17 SEPTEMBER 2008 (17.09.2008)	**17 SEPTEMBER 2008 (17.09.2008)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
IM, DAE SHIK
Telephone No. 82-42-481-5947

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2007/082564

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0149962 A1	06.07.2006	AU 2003-251853 A8	02.02.2004
		CN 1679066 A	05.10.2005
		EP 1540628 A2	15.06.2005
		JP 2005-533438 T2	04.11.2005
		KR 10-2005-0026478 A	15.03.2005
		US 2006-149962 AA	06.07.2006
		WO 2004-008676 A2	22.01.2004
		WO 2004-008676 A3	01.04.2004
US 2006-0133616 A1	22.06.2006	KR 10-2006-0071068 A	26.06.2006
KR 10-2003-0043451 A	02.06.2003	None	
KR 10-2004-0000925 A	07.01.2004	None	