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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 December 2009 (30.12.2009)

PCT

(10) International Publication Number
WO 2009/158086 A3

(51) International Patent Classification:
G06F 21/24 (2006.01) *H04L 9/00* (2006.01)
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2009/044780

(22) International Filing Date:
21 May 2009 (21.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/146,520 26 June 2008 (26.06.2008) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, WA 98052-6399 (US).

(72) Inventors: **HSU, Wen-Pin, Scott**; c/o Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 (US). **SOULAMI, Tarik**; c/o Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 (US). **ZAGORSKI, Mark**; c/o Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 (US). **ZHANG, Mark**; c/o Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 (US). **PERLMAN, Brian**; c/o Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, 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, ST, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, 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))*

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

[Continued on next page]

(54) Title: TECHNIQUES FOR ENSURING AUTHENTICATION AND INTEGRITY OF COMMUNICATIONS

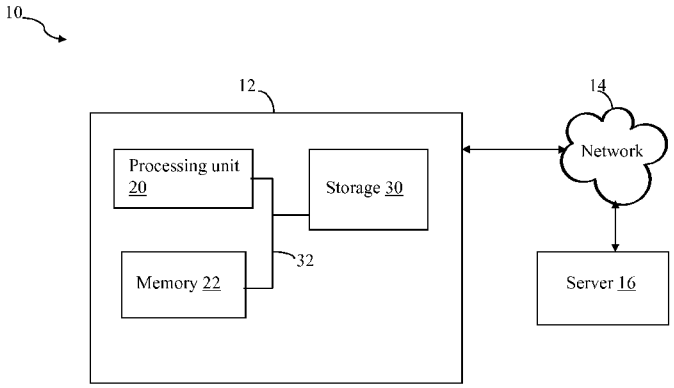

FIG. 1

(57) Abstract: Techniques are described for ensuring data integrity and authentication of received messages. One technique includes sending a request from a first module to a second module in which the request includes a first portion that is a shared secret encrypted with a public key, obtaining by the second module a private key from a secure and trusted information store, such as a license information store, including license information or other application specific information for the first module, using the private key to decrypt the first portion and obtain the shared secret, sending a response from the second module to the first module in which the response includes authentication data and at least one data item used with the shared secret to determine the authentication data, and performing by the first module verification processing to verify the authentication data included in the response.

WO 2009/158086 A3

WO 2009/158086 A3

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:
25 February 2010

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/044780

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/24(2006.01)i, G06F 21/00(2006.01)i, H04L 9/00(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: G06F, H04L

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)
eKOMPASS(KIPO internal) "authentication, asymmetric, authorization, private, key, encryp*"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006-0200857 A1 (YOKOTA) 07 September 2006 See the abstract and pages 4-5.	1, 13, 17
A	US 2008-0091957 A1 (EVERETT et al.) 17 April 2008 See the abstract, figure 1A and claim 1.	1, 13, 17
A	US 2007-0277038 A1 (HARDY et al.) 29 November 2007 See the abstract, figure 3 and pages 3-4.	1, 13, 17
A	US 2003-0217275 A1 (BENTLEY et al.) 20 November 2003 See the abstract, figures 1-2 and claim 1.	1, 13, 17

☐ 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
15 DECEMBER 2009 (15.12.2009)	**16 DECEMBER 2009 (16.12.2009)**

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
SOHN, Hyun-Woong
Telephone No. 82-42-481-5973

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2009/044780

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0200857 A1	07.09.2006	CN 1838593 A	27.09.2006
		JP 2006-246272 A	14.09.2006
US 2008-0091957 A1	17.04.2008	AU 736325 B2	26.07.2001
		AU 1998-62996 B2	19.02.1998
		CA 2281576 C	30.11.2004
		CA 2281576 A1	27.08.1998
		EP 0963580 B1	06.05.2004
		EP 0976114 A2	02.02.2000
		EP 0981805 A1	01.03.2000
		EP 0976114 B1	14.08.2002
		EP 0963580 A1	15.12.1999
		EP 0981805 B1	09.04.2003
		EP 0985204 B1	13.12.2006
		EP 0985204 A1	15.03.2000
		EP 0985203 B1	12.04.2006
		EP 0985203 A1	15.03.2000
		EP 0985202 B1	13.09.2006
		EP 0985202 A1	15.03.2000
		EP 0981807 B1	06.08.2008
		EP 0981807 A2	01.03.2000
		JP 04-127862 B2	30.07.2008
		JP 04-129063 B2	30.07.2008
		JP 04-181641 B2	19.11.2008
		JP 04-251667 B2	08.04.2009
		JP 2002-512715 A	23.04.2002
		JP 2001-527675 A	25.12.2001
		JP 2009-003945 A	08.01.2009
		JP 2001-525958 A	11.12.2001
		JP 2001-525957 A	11.12.2001
		JP 2001-525956 A	11.12.2001
		JP 2001-513231 A	28.08.2001
		JP 04-327261 B2	19.06.2009
		JP 2001-527674 A	25.12.2001
		US 2007-180276 A1	02.08.2007
		US 06164549 A	26.12.2000
		US 06220510 B1	24.04.2001
		US 06230267 B1	08.05.2001
		US 06317832 B1	13.11.2001
		US 06328217 B1	11.12.2001
		US 06385723 B1	07.05.2002
		US 06575372 B1	10.06.2003
		US 06659354 B2	09.12.2003
		US 07469339 B2	23.12.2008
		US 07584358 B2	01.09.2009
		US 2001-0056536 A1	27.12.2001
		US 2002-0050528 A1	02.05.2002
		US 2007-0143616 A1	21.06.2007
		US 2007-0255955 A1	01.11.2007

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/044780

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 2008-0010470 A1	10.01.2008
		US 2008-0052515 A1	28.02.2008
		US 2008-0059812 A1	06.03.2008
		US 2008-0091956 A1	17.04.2008
		US 2008-0091958 A1	17.04.2008
		US 2008-0137842 A1	12.06.2008
		WO 1998-037526 A1	27.08.1998
		WO 1998-052153 A2	19.11.1998
		WO 1998-052158 A2	19.11.1998
		WO 1998-052163 A2	19.11.1998
		WO 1998-052161 A2	19.11.1998
		WO 1998-052162 A2	19.11.1998
		WO 1998-052159 A2	19.11.1998
US 2007-277038 A1	29.11.2007	None	
US 2003-0217275 A1	20.11.2003	US 2008-0159527 A1	03.07.2008