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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 December 2003 (24.12.2003)

PCT

(10) International Publication Number
WO 2003/107151 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US2003/015359

(22) International Filing Date: 15 May 2003 (15.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/177,626 18 June 2002 (18.06.2002) US

(71) Applicant: INTEL CORPORATION [US/US]; (a Delaware Corporation), 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor: BRICKELL, Ernest; 3106 N.W. Luray Terrace, Portland, OR 87111 (US).

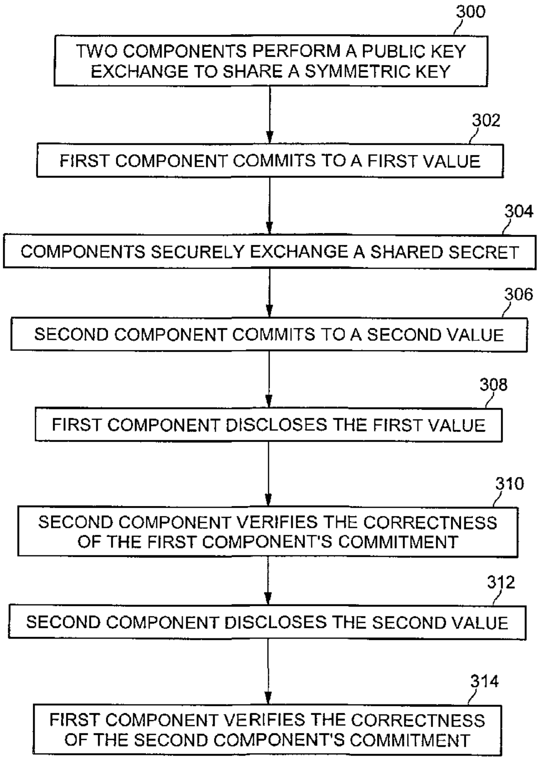
(74) Agents: MALLIE, Michael, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(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, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, 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, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD OF CONFIRMING A SECURE KEY EXCHANGE


300
TWO COMPONENTS PERFORM A PUBLIC KEY EXCHANGE TO SHARE A SYMMETRIC KEY
302
FIRST COMPONENT COMMITS TO A FIRST VALUE
304
COMPONENTS SECURELY EXCHANGE A SHARED SECRET
306
SECOND COMPONENT COMMITS TO A SECOND VALUE
308
FIRST COMPONENT DISCLOSES THE FIRST VALUE
310
SECOND COMPONENT VERIFIES THE CORRECTNESS OF THE FIRST COMPONENT'S COMMITMENT
312
SECOND COMPONENT DISCLOSES THE SECOND VALUE
314
FIRST COMPONENT VERIFIES THE CORRECTNESS OF THE SECOND COMPONENT'S COMMITMENT

(57) Abstract: A key exchange protocol can be performed between components of a system, such as between a computer program being executed by the processor of a PC (or other computer system) and a peripheral. A peripheral with a user input capability and a very limited display capability, such as a keyboard or a mouse, may be used to confirm a key exchange between the system components in a way that requires the user to enter only small amounts of input data (*e.g.*, keystrokes or mouse clicks). Security between components may be enhanced without having a negative impact on usability of the system. Embodiments of the present invention help to deter "man in the middle" attacks wherein an attacker gains control of a system component situated between certain communicating system components.

WO 2003/107151 A3

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
16 September 2004

INTERNATIONAL SEARCH REPORT

In onal Application No
PCT/US 03/15359

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

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 7 G06F H04L

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 practical, search terms used)

EPO-Internal, INSPEC, PAJ, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 892 521 A (HEWLETT PACKARD CO) 20 January 1999 (1999-01-20) column 5, line 51 - column 6, line 51 -----	1-12
X	SCHNEIER B: "Applied Cryptography, communications using symmetric cryptography" 1996, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, NY: JOHN WILEY & SONS, US, PAGE(S) 28-33,176-177,216-217,461-473,518--522 , XP002251738 ISBN: 0-471-12845-7 page 33, line 23 - line 38 ----- -/--	1,7

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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 document 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 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 6 July 2004	Date of mailing of the international search report 16/07/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Chabot, P

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SCHNEIER: "APPLIED CRYPTOGRAPHY" 1996, APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, PAGE(S) 47-52 , XP002939871 ISBN: 0-471-11709-9 page 48, line 7 - page 49, line 24 page 51, line 1 - line 18 -----	1,3,7,9
X	SCHNEIER: "APPLIED CRYPTOGRAPHY" 1996, APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, PAGE(S) 56-65 , XP002138607 ISBN: 0-471-11709-9 page 56, line 35 - page 59, line 27 -----	1-12
X	MENEZES ET AL: "HANDBOOK OF APPLIED CRYPTOGRAPHY" 1997, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, PAGE(S) 403-405,506-515,570 , XP002165287 ISBN: 0-8493-8523-7 * 12.5.2 Protocols combining PK encryption and signatures - 12.5.3 Hybrid key transport protocols using PK encryption * -----	1-12
A	BRUCE SCHNEIER: "Applied Cryptography, second edition" 1996, APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, PAGE(S) 169-187 , XP002111449 ISBN: 0-471-11709-9 page 173, line 17 - page 174, line 9 -----	3-6,9-12
A	US 6 061 794 A (DRISCOLL DAN J ET AL) 9 May 2000 (2000-05-09) column 6, line 65 - column 7, line 38 -----	13-41
A	US 5 345 506 A (OOHASHI MASAYOSHI ET AL) 6 September 1994 (1994-09-06) column 3, line 35 - column 4, line 33 -----	13-41
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 April 1993 (1993-04-07) page 8, line 46 - page 10, line 16 -----	13-41
A	US 5 440 635 A (BELLOVIN STEVEN M ET AL) 8 August 1995 (1995-08-08) column 1, line 60 - column 3, line 32 ----- -/--	13-41

INTERNATIONAL SEARCH REPORT

In onal Application No
PCT/US 03/15359

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 173 400 B1 (HANNA STEPHEN R ET AL) 9 January 2001 (2001-01-09) column 8, line 24 - column 9, line 9 -----	13-41

national application No.
PCT/US 03/15359

INTERNATIONAL SEARCH REPORT

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. □ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. □ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. □ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. □ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

□ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-12

   Method for symmetric key exchange by using public key cryptography and a defined value based on a random value, a public key, a symmetric key and a shared secret.

   ---

2. claims: 13-41

   Method for symmetric key exchange by using public key cryptography and two nonces, a hash value and a public key. Additionally displaying part of the nonces and accepting the input this part of the nonce.

INTERNATIONAL SEARCH REPORT

In onal Application No
PCT/US 03/15359

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 0892521	A	20-01-1999	US	6584565	B1	24-06-2003
			DE	69810394	D1	06-02-2003
			DE	69810394	T2	30-10-2003
			EP	0892521	A2	20-01-1999
			JP	11119650	A	30-04-1999
US 6061794	A	09-05-2000	NONE			
US 5345506	A	06-09-1994	JP	2883243	B2	19-04-1999
			JP	5344117	A	24-12-1993
EP 0535863	A	07-04-1993	US	5241599	A	31-08-1993
			AU	648433	B2	21-04-1994
			AU	2351392	A	08-04-1993
			CA	2076252	A1	03-04-1993
			DE	69232369	D1	14-03-2002
			DE	69232369	T2	23-01-2003
			EP	1104959	A2	06-06-2001
			EP	0535863	A2	07-04-1993
			JP	2599871	B2	16-04-1997
			JP	6169306	A	14-06-1994
			NO	923740	A	05-04-1993
US 5440635	A	08-08-1995	NONE			
US 6173400	B1	09-01-2001	AU	5135499	A	21-02-2000
			EP	1101318	A1	23-05-2001
			JP	2002521962	T	16-07-2002
			WO	0007326	A1	10-02-2000