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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2001 (11.10.2001)

PCT

(10) International Publication Number
WO 01/075564 A3

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

(21) International Application Number: PCT/US01/08891

(22) International Filing Date: 21 March 2001 (21.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/541,108 31 March 2000 (31.03.2000) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and

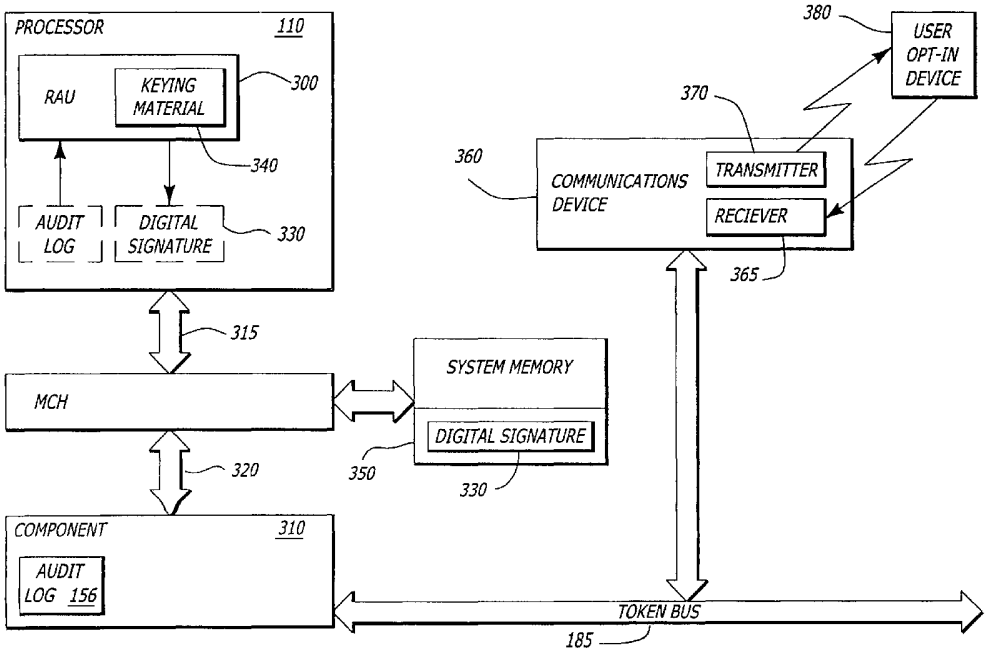
(75) Inventors/Applicants *(for US only)*: **HERBERT, Howard, C.** [US/US]; 16817 South 1st Drive, Phoenix, AZ 85045 (US). **GRAWROCK, David, W.** [US/US]; 8285 S.W. 184th Avenue, Aloha, OR 97007 (US). **ELLISON, Carl, M.** [US/US]; 181 N.W. 28th Avenue, Portland, OR 97210 (US). **GOLLIVER, Roger, A.** [US/US]; 16185 S.W. Night Hawk Drive, Beaverton, OR 97007 (US). **LIN, Derrick, C.** [US/US]; 1737 Oakwood Drive, San Mateo, CA 94403 (US). **MCKEEN, Francis, X.** [US/US]; 10612 N.W. LeMans Court, Portland, OR 97229 (US). **NEIGER, Gilbert** [US/US]; 2424 N.E. 11th Avenue, Portland, OR 97212 (US). **RENERIS, Ken** [US/US]; 8 Red Gap Road, Wilbraham, MA 01095 (US). **SUTTON, James, A.** [US/US]; 20205 N.W. Paulina Drive, Portland, OR 97229 (US). **THAKKAR, Shreekant, S.** [GB/US]; 150 S.W. Moonridge Place, Portland, OR 97225 (US). **MITTAL, Millind** [US/US]; 800 E. Charleston Road #29, Palo Alto, CA 94303 (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, 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,

[Continued on next page]

(54) Title: PLATFORM AND METHOD FOR REMOTE ATTESTATION OF A PLATFORM



(57) Abstract: In one embodiment, a method of remote attestation for a special mode of operation. The method comprises storing an audit log within protected memory of a platform. The audit log is a listing of data representing each of a plurality of IsoX software modules loaded into the platform. The audit log is retrieved from the protected memory in response to receiving a remote attestation request from a remotely located platform. Then, the retrieved audit log is digitally signed to produce a digital signature for transfer to the remotely located platform.

WO 01/075564 A3

MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, 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, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

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

Int ional Application No
PCT/US 01/08891

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

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)
WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	EP 1 030 237 A (HEWLETT PACKARD CO) 23 August 2000 (2000-08-23) column 1, line 46 -column 2, line 51 column 4, line 44 -column 6, line 32 column 7, line 9 - line 50 column 8, line 15 -column 9, line 35 figures 1,2,4,6 ---	1-4, 9-11, 15-17, 24,25
X	US 5 953 502 A (HELBIG SR WALTER A) 14 September 1999 (1999-09-14)	15
A	column 2, line 49 -column 3, line 67 column 8, line 28 - line 62 column 23, line 60 -column 25, line 36 figure 1 --- -/--	1-4,16, 17,24,25

[X] Further documents are listed in the continuation of box C.

[X] 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	Date of mailing of the international search report
31 July 2002	06/08/2002

Name and mailing address of the ISA	Authorized officer
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	Arbutina, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 01/08891

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 29567 A (GRESSEL CARMI ;GRANOT RAN (IL); FORTRESS U & T LTD (IL)) 14 August 1997 (1997-08-14) page 3, paragraphs 2,3 page 5, paragraphs 1,4 figure 1 -----	18,19, 21,22

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/US 01/08891

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1030237 A	23-08-2000	EP 1030237 A1	23-08-2000
		EP 1161714 A1	12-12-2001
		EP 1161715 A1	12-12-2001
		EP 1161716 A1	12-12-2001
		WO 0048061 A1	17-08-2000
		WO 0048062 A1	17-08-2000
		WO 0048063 A1	17-08-2000
US 5953502 A	14-09-1999	EP 1013023 A1	28-06-2000
		JP 2001524229 T	27-11-2001
		WO 9836517 A1	20-08-1998
		US 6038667 A	14-03-2000
		US 6311273 B1	30-10-2001
WO 9729567 A	14-08-1997	AU 1455897 A	28-08-1997
		WO 9729567 A1	14-08-1997
		US 6360321 B1	19-03-2002