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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 March 2006 (09.03.2006)

PCT

(10) International Publication Number
WO 2006/025952 A3

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2005/024486

(22) International Filing Date: 8 July 2005 (08.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/892,265 14 July 2004 (14.07.2004) 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)*: **BRICKELL, Ernest** [US/US]; 3106 NW Luray Terrace, Portland, OR 87111 (US). **SUTTON, James, II** [US/US]; 20205 NW Paulina Drive, Portland, OR 97229 (US). **HALL, Clifford** [US/US]; 6940 Eastside Court, Orangevale, CA 95662 (US). **GRAWROCK, David** [US/US]; 8285 Southwest 184th Avenue, Aloha, OR 97007 (US).

(74) Agent: **VINCENT, Lester, J.**; Blakely Sokoloff Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (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, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

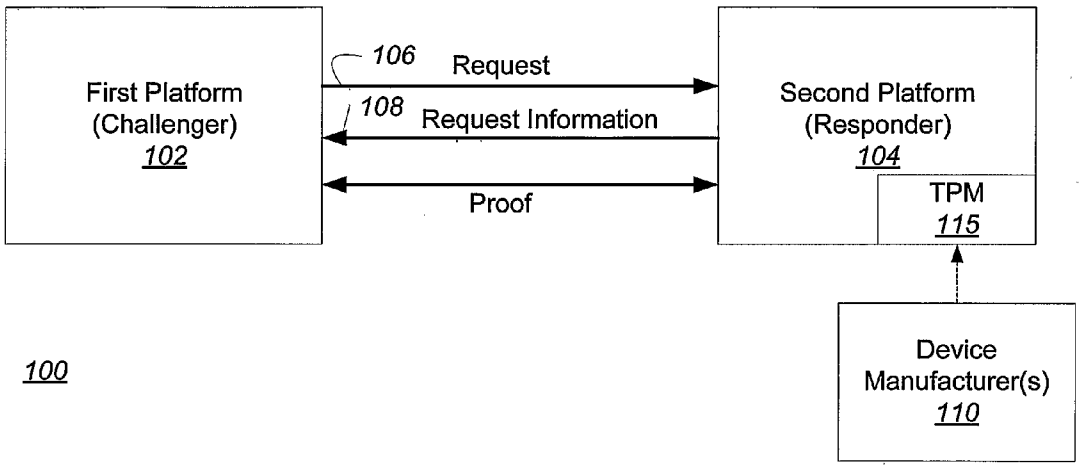
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

Published:
— *with international search report*

(88) Date of publication of the international search report:
1 February 2007

[Continued on next page]

(54) Title: METHOD OF DELIVERING DIRECT PROOF PRIVATE KEYS TO DEVICES USING A DISTRIBUTION CD



(57) Abstract: Delivering a Direct Proof private key to a device installed in a client computer system in the field may be accomplished in a secure manner without requiring significant non-volatile storage in the device. A unique pseudo-random value is generated and stored in the device at manufacturing time. The pseudorandom value is used to generate a symmetric key for encrypting a data structure holding a Direct Proof private key and a private key digest associated with the device. The resulting encrypted data structure is stored on a removable storage medium (such as a CD), and distributed to the owner of the client computer system. When the device is initialized on the client computer system, the system checks if a localized encrypted data structure is present in the system. If not, the system obtains the associated encrypted data structure from the removable storage medium. The device decrypts the encrypted data structure using a symmetric key regenerated from its stored pseudo-random value to obtain the Direct Proof private key. If the private key is valid, it may be used for subsequent authentication processing by the device in the client computer system.

WO 2006/025952 A3

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/US2005/024486

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/32

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)
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, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/103281 A1 (BRICKELL ERNIE F) 27 May 2004 (2004-05-27) cited in the application the whole document	1-39
Y	MENEZES, VANSTONE, OORSCHOT: 1997, CRC PRESS LLC , USA , XP002394263 page 321 - page 322 page 330 - page 331 page 388 - page 390 page 394 - page 395 page 397 - page 398 page 472 page 515 - page 516 page 548 - page 552	1-39

-/--

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

[X] 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 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
11 August 2006	18/09/2006

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	San Millán Maeso, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2005/024486

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 6 032 260 A (SASMAZEL ET AL) 29 February 2000 (2000-02-29) abstract column 2 - column 3	1-39

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2005/024486

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004103281 A1	27-05-2004	AU 2003287567 A1	23-06-2004
		CN 1717895 A	04-01-2006
		EP 1566011 A1	24-08-2005
		JP 2006508608 T	09-03-2006
		WO 2004051923 A1	17-06-2004
US 6032260 A	29-02-2000	NONE	