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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/082778 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2007/083562

(22) International Filing Date:
5 November 2007 (05.11.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/616,348 27 December 2006 (27.12.2006) US

(71) Applicant *(for all designated States except US)*: **GENERAL INSTRUMENT CORPORATION** [US/US]; 101 Tournament Drive, Horsham, Pennsylvania 19044 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **QIU, Xin** [US/US]; 10529 Harvest View, San Diego, CA 92128 (US). **PETERKA, Petr** [US/US]; 5126 Caminito Vista Lujo, San Diego, CA 92130 (US). **SPRUNK, Eric, J.** [US/US]; 7309 Bolero Street, Carlsbad, CA 92009 (US).

(74) Agent: **CULLEN, Lawrence, T.**; 101 Tournament Drive, MD: PA06/1-3032, Horsham, Pennsylvania 19044, (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,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR DISTRIBUTING ROOT CERTIFICATES

(57) Abstract: An apparatus and method for providing at least one root certificate are disclosed. Specifically, a plurality of root certificates is received and stored. Afterwards, a request is received from a first endpoint device for a desired root certificate, where the desired root certificate is used by the first endpoint device to verify an identity of a second endpoint device. Furthermore, the first endpoint device and the second endpoint device are associated with different certificate hierarchies. The desired root certificate is then sent to at least the first endpoint device.

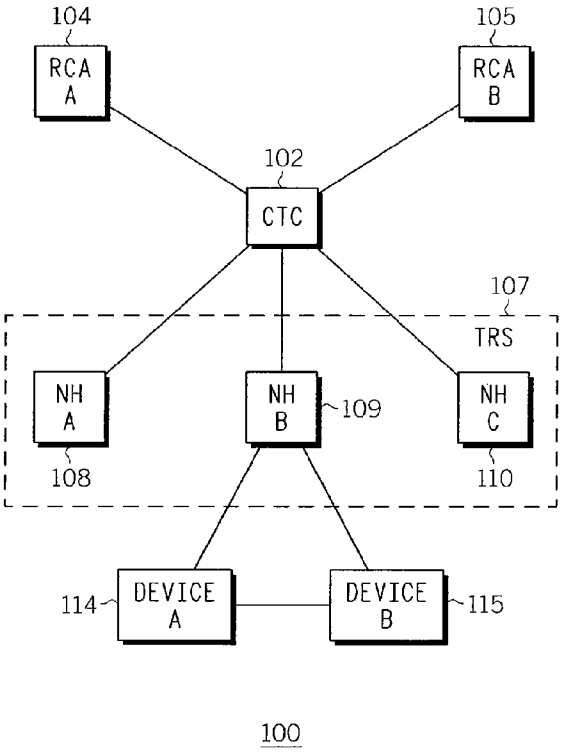

FIG. 1

WO 2008/082778 A3

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*

— *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:
21 August 2008

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/83562

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/00 (2008.04)
USPC - 713/157
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)
USPC: 713/157

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/150, 155, 166, 175 (view text search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
pubWEST(PGPB,USPT,EPAB,JPAB; PLUR=YES); DialogPRO(Engineering); Google Scholar; Text search terms: cryptography, public network, Secure distribution trust, root certificate, root certificate received stored, request received endpoint device desired root certificate, root certificate used endpoint device verify identity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X – Y	US 2006/0143700 A1 (HERRMANN) 29 June 2006 (29.06.2006) entire document, especially Abstract, FIG.5 and para [0021], [0071], [0077]-[0078] and [0088]	1, 4, 7, 9, 12, 15, 17, 20 ---------- 2-3, 5-6, 8, 10-11, 13-14, 16, 18-19, 21-23
Y	US 2006/0233363 A1 (GRAUNKE) 19 October 2006 (19.10.2006) entire document, especially Abstract and para [0023] and [0062]	2-3, 5-6, 10-11, 13-14, 18 -19, 21-23
Y	US 2004/0049675 A1 (MICALI, et al.) 11 March 2004 (11.03.2004) entire document, especially Abstract and para [0220]	8, 16
A	MARCHESINI, John et al. 'Virtual Hierarchies - An Architecture for Building and Maintaining Efficient and Resilient Trust Chains'. In the Proceedings of the 7th Nordic Workshop on Secure IT Systems---NORDSEC 2002. Published May 17, 2002. [retrieved on 2008-06-01]. Retrieved from the Internet: <URL: http://www.cs.dartmouth.edu/~sws/pubs/ms02.pdf >	1-23

☐ Further documents are listed in the continuation of Box C. ☐

* 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 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
01 June 2008 (01.06.2008)	13 JUN 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)