

(19) World Intellectual Property Organization
International Bureau



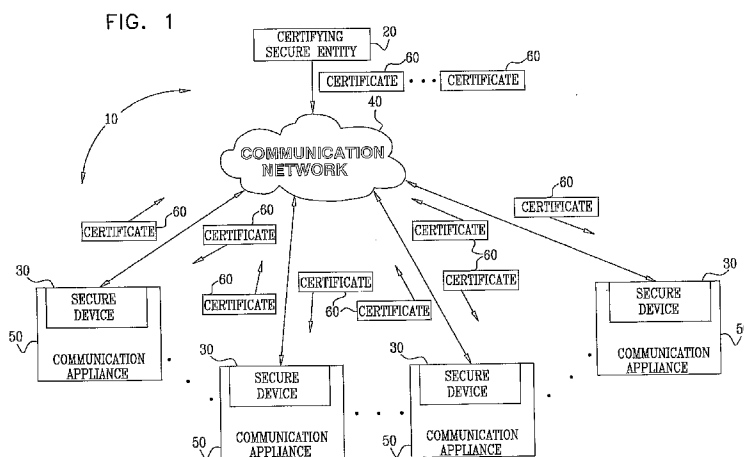
(43) International Publication Date
11 October 2007 (11.10.2007)

PCT

(10) International Publication Number
WO 2007/113787 A3

- (51) International Patent Classification:
H04L 9/00 (2006.01) H04K 1/02 (2006.01)
H04K 1/00 (2006.01)
 - (21) International Application Number:
PCT/IL2007/000092
 - (22) International Filing Date: 25 January 2007 (25.01.2007)
 - (25) Filing Language: English
 - (26) Publication Language: English
 - (30) Priority Data:
174706 31 March 2006 (31.03.2006) IL
 - (71) Applicant (for all designated States except US): NDS LIMITED [GB/GB]; One Heathrow Boulevard, 286 Bath Road, West Drayton Middlesex UB7 0DQ (GB).
 - (72) Inventors; and
 - (75) Inventors/Applicants (for US only): BELENKY, Yaa-cov [IL/IL]; 27/2 Hakinor Street, 98371 Maaleh Adumim (IL). SHEN-ORR, Chaim [IL/IL]; 16 Kiryat Sefer Street, 34676 Haifa (IL).
 - (74) Agents: SANFORD T. COLB & CO. et al.; P.O. Box 2273, 76122 Rehovot (IL).
 - (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, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, 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, 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:
22 May 2009

(54) Title: CERTIFICATE IMPLEMENTATION SYSTEM



(57) Abstract: A certificate for use in a secure communication system that employs a public-key infrastructure (PKI) scheme is disclosed. The certificate includes: a certificate field including an indication of identity of a secure device to which the certificate pertains, a certificate field including a public key, and at least one of the following certificate fields: a certificate field including a level of security of a timer used in the secure communication system, a certificate field including a level of security of a non-volatile memory (NVM) of the secure device, a certificate field including a level of implementation of export to another secure communication system, a certificate field including an identification of at least one encryption mode supported by the secure device, and a certificate field including a rendering type specification. Related apparatus and methods are also disclosed.

WO 2007/113787 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL07/00092

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 9/00(2006.01);H04K 1/00(2006.01),1/02(2006.01)**

USPC: 713/156,157,175,176;380/255,259

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)
U.S. : 713/156,157,175,176; 380/255,259

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 practicable, search terms used)
EAST (USPGPUB, USPAT, USOCR, JPO, EPO, DERWENT, IBM_TDB)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,772,331 (HIND ET AL.) 21, MAY 1999 (21.5.1999) col. 9 lines 16-61, col. 12 lines 20-67, col. 13 lines 1-44, Fig. 1A, 2, 3, 4, 5A, 5B, 6	1, 2, 4- 20, 26, 27
Y	US 20040139312 (MEDVINSKY) 14 JAN 2003 (14.1.2003) paragraph 0039, 0040, 0050,0055,0056 Tables I-V	1, 2, 4-14, 18, 19, 21-25
Y	US 20040025010 (AZENA ET AL.) 14 JUL. 2003 (14.7.2003) paragraph 0101 Fig. 10	3

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	"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
"E" earlier application or patent published on or after the international filing date	"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
"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)	"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
"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	"&"	document member of the same patent family

Date of the actual completion of the international search
12 May 2008 (12.05.2008)

Date of mailing of the international search report
27 MAY 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
Nirav Patel
Telephone No. 703-305-9600

DEBORAH A. THOMAS
PARALEGAL SPECIALIST

