

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
17 April 2008 (17.04.2008)

PCT

(10) International Publication Number
WO 2008/045773 A3

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

(74) Agent: BACHAND, Richard A.; 5775 Morehouse Drive,
San Diego, California 92121 (US).

(21) International Application Number:
PCT/US2007/080525

(22) International Filing Date: 5 October 2007 (05.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/850,882 10 October 2006 (10.10.2006) US
11/866,946 3 October 2007 (03.10.2007) US

(71) Applicant (for all designated States except US): QUAL-
COMM Incorporated [US/US]; Attn: International
Ip Administration, 5775 Morehouse Drive, San Diego,
California 92121 (US).

(72) Inventors; and

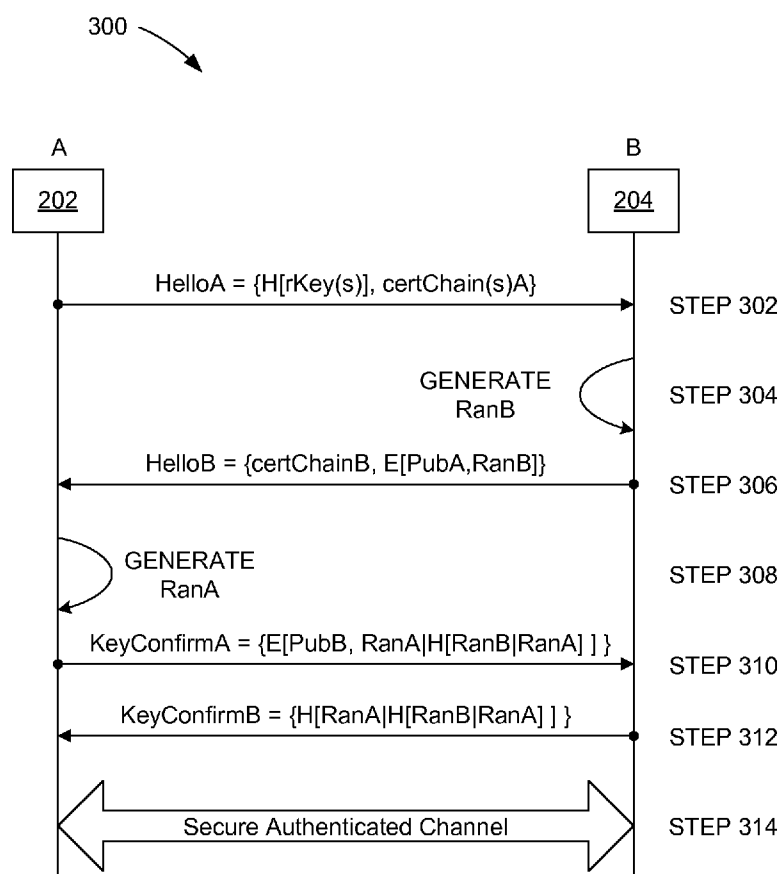
(75) Inventors/Applicants (for US only): PEREZ, Aram
[US/US]; 5775 Morehouse Drive, San Diego, California
92121 (US). DONDETI, Lakshminath Reddy [IN/US];
5775 Morehouse Drive, San Diego, California 92121 (US).

(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 MUTUAL AUTHENTICATION



(57) Abstract: Disclosed is a method for mutual authentication between a station, having a digital rights agent, and a secure removable media device. The digital rights agent initiates mutual authentication by sending a message to the secure removable media device. The secure removable media device encrypts a first random number using a public key associated with the digital rights agent. The digital rights agent decrypts the encrypted first random number, and encrypts a second hash based on at least the first random number. The secure removable media device decrypts the encrypted second random number and the first hash, verifies the first hash to authenticate the digital rights agent, and generates a second hash based on at least the second random number. The digital rights agent verifies the second hash to authenticate the secure removable media device.

WO 2008/045773 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*

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

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

12 June 2008