

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
26 July 2007 (26.07.2007)

PCT

(10) International Publication Number
WO 2007/084863 A3

(51) International Patent Classification:

H04L 9/08 (2006.01) **H04L 29/06** (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/US2007/060519

(22) International Filing Date: 12 January 2007 (12.01.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/758,971	13 January 2006 (13.01.2006)	US
60/762,771	27 January 2006 (27.01.2006)	US
11/621,916	10 January 2007 (10.01.2007)	US

(71) Applicant (for all designated States except US): **QUALCOMM INCORPORATED** [US/US]; ATTN: INTERNATIONAL IP ADMINISTRATION, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ESCOTT, Adrian**

[GB/US]; 2575 Fenton Parkway, #311, San Diego, California 92108 (US). **SEMPLE, James** [CA/GB]; 7 Queensgate Place, Flat 4, London, South Wales SW7 5NU (GB).

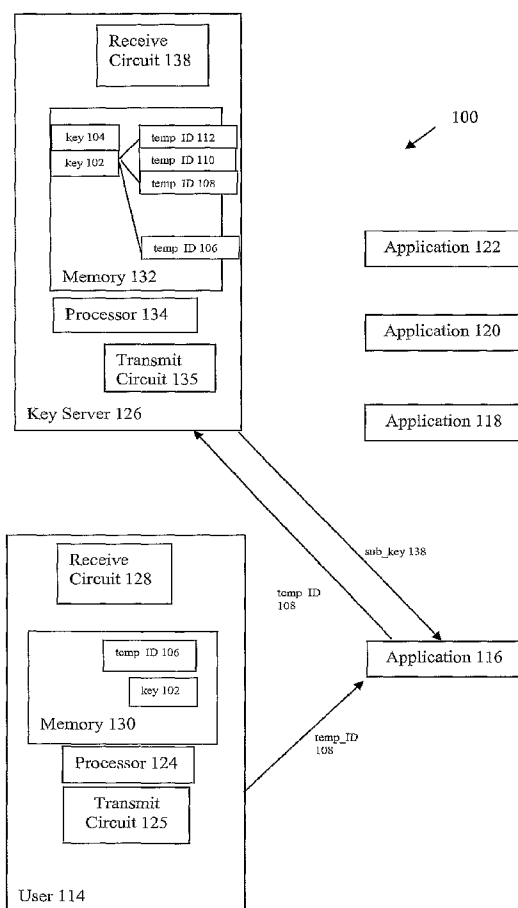
(74) Agents: **OGROD, Gregory D.** et al.; ATTN: INTERNATIONAL IP ADMINISTRATION, 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, 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),

[Continued on next page]

(54) Title: PRIVACY PROTECTION IN COMMUNICATION SYSTEMS



(57) Abstract: Methods and apparatus for protecting user privacy in a shared key system (100). According to one aspect, a user (114) generates a derived identity (108) based on a key (102) and a session variable, and sends the derived identity to an application (116). In one embodiment, a key server (126) may be used to receive the derived identity from the application, and return a sub-key (138) to the application to use for encrypting communications with the user.



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).

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))*

Published:

- *with international search report*

(88) Date of publication of the international search report:
20 September 2007

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.