2006023873

07 APR 2006

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

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

162162

(43) International Publication Date
10 November 2005 (10.11.2005)

PCT

(10) International Publication Number
WO 2005/107140 A1

(51) International Patent Classification[7]: H04L 9/28, 9/30

(21) International Application Number:
PCT/CA2004/002043

(22) International Filing Date:
26 November 2004 (26.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/567,611 3 May 2004 (03.05.2004) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

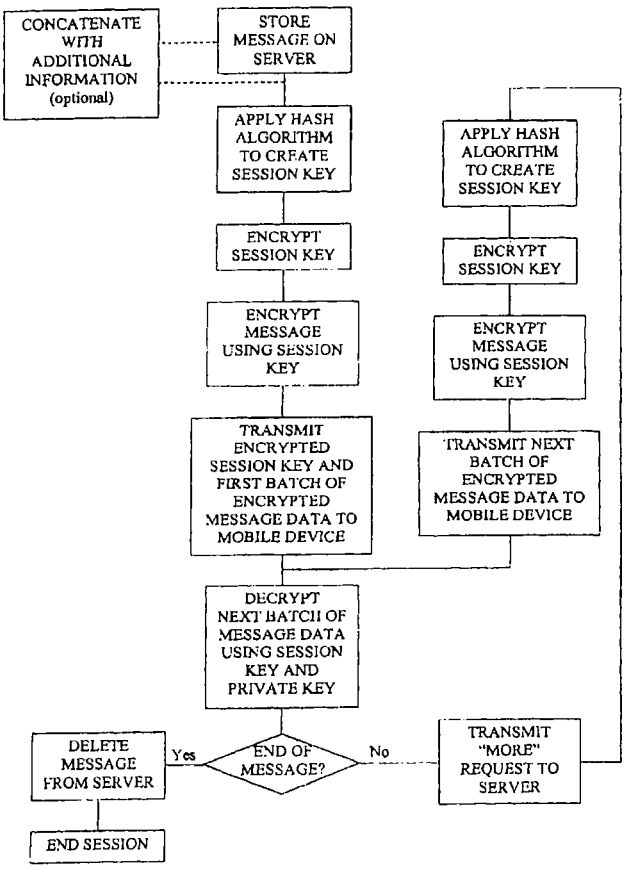
(75) Inventors/Applicants *(for US only)*: **BROWN, Michael, K.** [CA/CA]; 8 Fernwood Place, Kitchener, Ontario N2M 2Z2 (CA). **BROWN, Michael, S.** [CA/CA]; 350 University Downs Cres., Waterloo, Ontario N2K 4B1 (CA). **LITTLE, Herbert, A.** [CA/CA]; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA).

(74) Agents: **EISEN, Mark, B.** et al.; Dimock Stratton LLP, 20 Queen St. W., Suite 3202, Box 102, Toronto, Ontario M5H 3R3 (CA).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR GENERATING REPRODUCIBLE SESSION KEYS



(57) Abstract: A system and method for generating reproducible session keys in a wireless messaging system. The session key is generated based on a hash of a message itself, optionally concatenated with additional information. Since the local server stores the message, it can easily regenerate the same session key in response to each MORE request. The method of the invention can be implemented with the stored original message, a public key, and an algorithm for generating the session key based on a hash of the message.

WO 2005/107140 A1

ACTION

MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, LU, 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*

— *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 revised international search report:** 29 December 2005

(15) **Information about Correction:**
see PCT Gazette No. 52/2005 of 29 December 2005, Section II

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.