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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 October 2005 (13.10.2005)

PCT

(10) International Publication Number
WO 2005/096542 A1

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

(21) International Application Number:
PCT/CA2005/000466

(22) International Filing Date: 30 March 2005 (30.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/559,092 2 April 2004 (02.04.2004) US
60/559,646 5 April 2004 (05.04.2004) 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: **LITTLE, Herbert, A.**; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA). **BROWN, Michael, K.**; 8 Fernwood Place, Kitchener, Ontario N2M 2Z2 (CA).

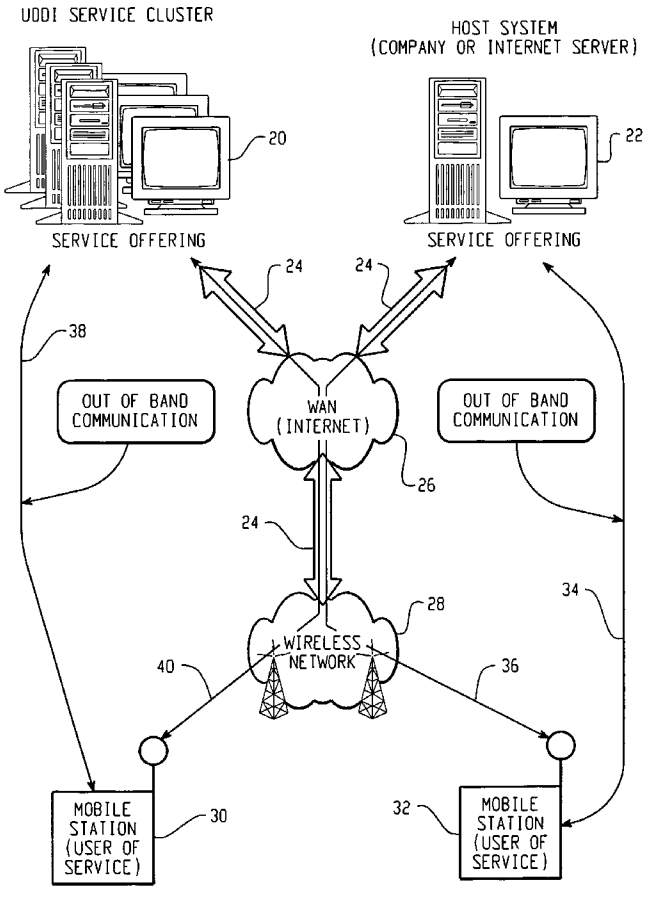
(74) Agents: **ANDRADE, Dilip, C.** et al.; Borden Ladner Gervais LLP, World Exchange Plaza, 100 Queen Street, Suite 1100, Ottawa, Ontario K1P 1J9 (CA).

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

[Continued on next page]

(54) Title: DEPLOYING AND PROVISIONING WIRELESS HANDHELD DEVICES



(57) Abstract: A method carried out by a first system for establishing a secure bidirectional communication path between the first system and a second system for an exchange of one or more messages is described. A first key pair having a first public key and a first private key is generated, and a second key pair having a second public key and a second private key is generated. The second public key is generated based upon a shared secret known to the first system and the second system. The second public key and the first public key are sent to the second system. A third public key and a fourth public key generated by the second system are received, wherein the fourth public key is generated based upon the shared secret. A master key is calculated based upon the first private key, the second private key, the third public key and the fourth public key, wherein the master key is configured to be used in encryption of one or more messages.

WO 2005/096542 A1

FR, GB, GR, HU, IE, IS, IT, LT, 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).

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.

Published:

— *with international search report*