

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
30 April 2009 (30.04.2009)

PCT

(10) International Publication Number
WO 2009/054807 A1

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/SG2007/000363

(22) International Filing Date: 26 October 2007 (26.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US):
NANYANG POLYTECHNIC [SG/SG]; 180 Ang
Mo Kio Avenue 8, Singapore 569830 (SG).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **TEO, Yong King**
[SG/SG]; 233 Paya Lebar Road, #16-06 Le Crescendo,
Singapore 409044 (SG).

(74) Agent: **LAWRENCE Y D HO & ASSOCIATES PTE
LTD**; 30 Bideford Road, #02-02, Thongsia Building, Sin-
gapore 229922 (SG).

(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.

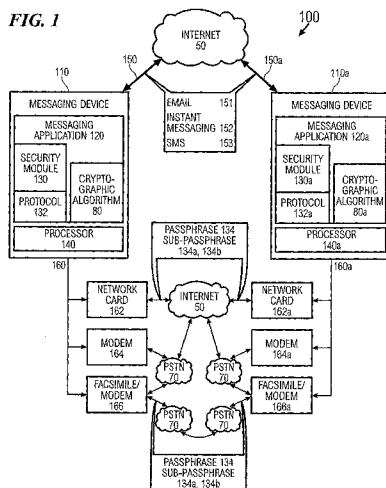
(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,
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

(54) Title: SECURE MESSAGING USING OUTBAND MODE AUTHENTICATION

FIG. 1



(57) Abstract: The present invention provides a secure messaging system (100) using outband mode authentication. The secure messaging system includes a security module (130, 130a) that is pluggable into a messaging application (120, 120a). The security module (130, 130a) has a protocol (132) for allowing a user to enter a passphrase (134) for use with a symmetric cryptographic algorithm (80). In another embodiment, the protocol (132) allows the passphrase (134) to be split into a predetermined number of sub-passphrases (134a, 134b, etc.); the passphrase (134) or at least one sub-passphrase (134a, 134b, etc.) is operable to be sent to a recipient through an out-of-band channel (160), which is separate from an I/O channel (150) for sending the secure message. Each mode of the out-of-band channel (160) enhances security of the message by increasing the difficulty of re-assembling the sub-passphrases; in addition, each out-of-band mode constitutes a form of authentication.