(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 April 2009 (02.04.2009)

(10) International Publication Number
WO 2009/041804 A8

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

(21) International Application Number:
PCT/MY2008/000114

(22) International Filing Date:
25 September 2008 (25.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20071621 26 September 2007 (26.09.2007) MY

(71) Applicant (for all designated States except US): MIMOS BERHAD [MY/MY]; Technology Park of Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and


(74) Agent: ABDULLAH, Mohd, Bustaman; Bustaman, Lot C9-3, Ialan Selaman 1, Dataran Palma, 68000 Ampang, Selangor (MY).


(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SA, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, [Continued on next page]

(54) Title: SECURE INSTANT MESSAGING

(57) Abstract: A setup for secure instant messaging allowing a user to use a smart card (32a) to authenticate its identification is described. A server (21) generates a random number and a network sends the random number to a user's client (31a). The smart card (32a) stores a unique private key for each user and encrypts the random number with a user's private key. A database (11) provides a public key. The server (21) decrypts the random number with the public key, compares the decrypted number with the random number, whereby same number validates the user's identity to establish a secure connection between validated user's client and server, allowing a user to log onto a secure instant messaging network. A user can also retrieve peer user's internet protocol and public key to establish a client-to-client connection, where the data communicated between them can be encrypted using the peer's public key and can only be decrypted using the user's private key stored in the user's smart card (32a). A breakdown detection feature is also described.
NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, Cl, 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(U))
— of inventorship (Rule 4.17(iv))

Published:
— with international search report

(88) Date of publication of the international search report: 22 May 2009

(48) Date of publication of this corrected version: 30 July 2009

(15) Information about Correction: see Notice of 30 July 2009