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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 September 2004 (10.09.2004)

PCT

(10) International Publication Number
WO 2004/077290 A1

(51) International Patent Classification[7]: G06F 9/00, H04L 9/00, 9/32

(21) International Application Number: PCT/US2003/019953

(22) International Filing Date: 25 June 2003 (25.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/449,068 20 February 2003 (20.02.2003) US
10/250,004 27 May 2003 (27.05.2003) US

(71) Applicant: SECURE DATA IN MOTION, INC. [US/US]; 1875 South Grant Street, Suite 500, San Mateo, CA 94402 (US).

(72) Inventors: MOREH, Jahanshah; 2122 Century Park Lane, Apt. 417, Los Angeles, CA 90067 (US). BRUNS, Logan, O'Sullivan; 127 Quarry Drive, Napa, CA 94559 (US).

(74) Agent: ROBERTS, Raymond E.; Intellectual Property Law Offices, 1901 South Bascom Avenue, Suite 660, Campbell, CA 95008 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

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.

(54) Title: SYSTEM FOR ON-LINE AND OFF-LINE DECRYPTION

(57) Abstract: A secure communication system wherein message decryption may be performed while off-line, or optionally while on-line. A sender encrypts a message based on the message key and sends it to the recipient. An envelope containing a message key is created by encrypting the message key based on a verifier, where the verifier is based on a secret of the recipient. The recipient is provided the envelope, along with the message or separately, from the sender or from another party, contemporaneous with receipt of the message or otherwise. The recipient can then open the envelope while off-line, based on their secret, and retrieve the message key from the envelope to decrypt the message. In the event the recipient cannot open the envelope, optional on-line access permits obtaining assistance that may include obtaining an alternate envelope that the recipient can open.

WO 2004/077290 A1