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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 November 2004 (18.11.2004)

PCT

(10) International Publication Number
WO 2004/100439 A1

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

(21) International Application Number:
PCT/US2003/019954

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/249,717 2 May 2003 (02.05.2003) US

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

(72) Inventors: **OLKIN, Terry M.**; 104 Regent Drive, Los Gatos, CA 95032 (US). **MOREH, Jahanshah**; 2122 Century Park Lane, Apt. 417, Los Angeles, CA 90067 (US). **OLKIN, Jeffrey C.**; 1015 Mountain Home Road, Woodside, CA 94062 (US).

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

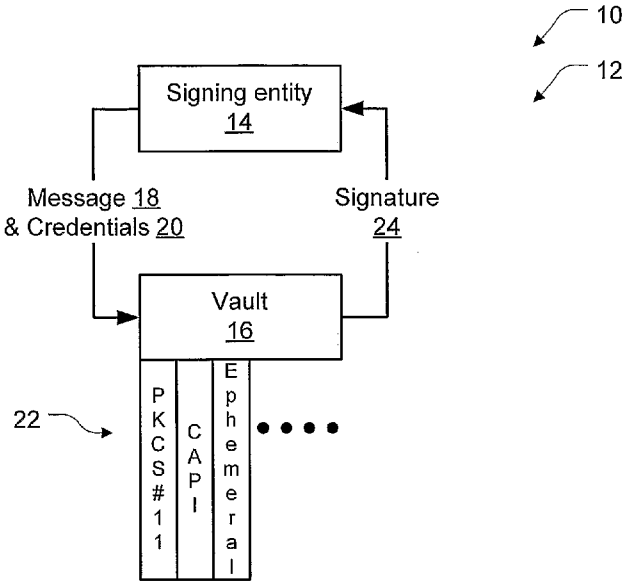
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, 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: DIGITAL SIGNATURE AND VERIFICATION SYSTEM FOR CONVERSATIONAL MESSAGES



(57) Abstract: A digital signature verification system wherein a signature system may sign a conversational message, as might be used in a chat, instant messaging or enterprise instant messaging dialog, and a verification system may then verify the signature. The signature system may include a signing entity (14) and a vault (16), wherein the signing entity provides the message and credentials and the vault creates the signature (24) based on a first hash of the message that is further encrypted with a signature key. The verification system may include a validating entity and a verifier, wherein the validating entity provides the message, the signature, and assertions to the verifier and the verifier then forms a second hash of the message, uses a verification key corresponding with the signature key to decrypt the signature and obtain the first hash, and compares the two hashes to determine a proper validation response.

WO 2004/100439 A1