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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 August 2003 (14.08.2003)

PCT

(10) International Publication Number
WO 03/067809 A1

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

(21) International Application Number: PCT/US03/03099

(22) International Filing Date: 3 February 2003 (03.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/062,551 5 February 2002 (05.02.2002) US

(71) Applicant: **SURETY, INC.** [US/US]; 12950 Worldgate Drive, Suite 150, Herndon, VA 20170 (US).

(72) Inventors: **ANDIVAHIS, Dimitrios, Emmanouil**; 2312 Rosedown Drive, Reston, VA 20191 (US). **CARNELL, Shawn, Michael, Edwards**; 554 Lewisville Road, Berryville, VA 22611 (US). **FISCHER, Addison, McElroy**; P.O. Box 7189, Naples, FL 34101-7189 (US). **WETTLAUFER, Albert, John**; 12116 Walnut Branch Road, Reston, VA 20194 (US).

(74) Agents: **ALAPATI, Nanda, K.** et al.; Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036 (US).

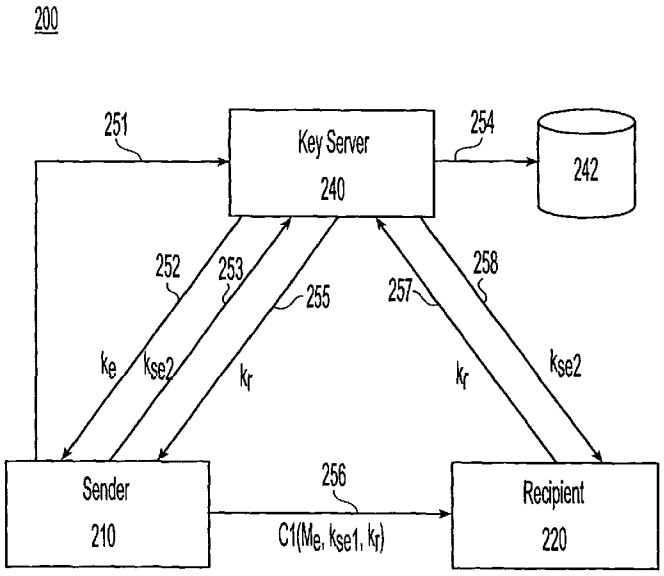
(81) Designated States *(national)*: AU, CA, CN, IN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

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: SECURE ELECTONIC MESSQGING SYSTEM REQUIRING KEY RETRIEVAL FOR DERIVING DECRYPTION KEYS



(57) Abstract: A secure electronic messaging system permits communication between registered users, with the assistance of a key server (240). The system requires a recipient (220) to submit key retrieval information to a key server (240), and obtain decryption key information. The decryption key information is necessary for the recipient (220) to form the decryption key which is used to read a message encrypted by the sender (210). The decryption key information may be an encrypted version of a decryption key, or portions thereof, or may be portions of an unencrypted version of a decryption key, among others. Typically, the key retrieval information may either be sent to the recipient (220) by the sender (210), or may be generated by the recipient (220), based on information sent by the sender (210).

WO 03/067809 A1