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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 June 2004 (10.06.2004)

PCT

(10) International Publication Number
WO 2004/049137 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/037954

(22) International Filing Date:
26 November 2003 (26.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/305,726	26 November 2002 (26.11.2002)	US
10/707,190	25 November 2003 (25.11.2003)	US
10/707,191	25 November 2003 (25.11.2003)	US

(71) Applicant: SECURE DATA IN MOTION, INC. [US/US]; 1875 South Grant Street, 10th Floor, 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).

(74) Agents: ROBERTS, Raymond, E. et al.; IPLO Intellectual Property Law Offices, 1901 South Bascom Ave., Suite 660, Campbell, CA 95008 (US).

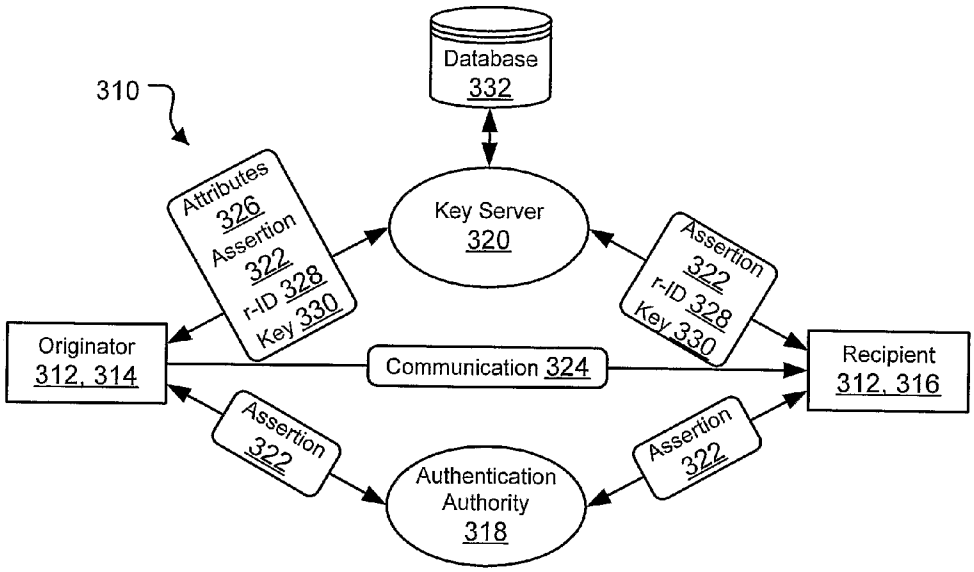
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, 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:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: KEY SERVER FOR SECURITY AND IMPLEMENTING PROCESSES WITH NONREPUDIATION AND AUDIT



(57) Abstract: Key server (216, 320, 420) based systems (210, 310, 410) permitting sender and recipient participants (212, 312, 412) to securely exchange communications (218, 324, 424). The key server (216, 320, 420) creates, stores, and releases keys that the participants use to protect the message. The participants employ keys (220, 330, 430), typically provided by the key server, to exchange the communications in encrypted form. Assertions (322, 422) from an authentication authority (318, 418) can be used to establish identities of the participants. Positive and negative events (342, 344) can be determined based on controlling events (340) and if, when, how often requests for a key for decryption occur. The key server can also store information from assertions in association with a transaction ID, to establish senders and recipients of communications in a manner that cannot plausibly be repudiated and can easily be audited.

WO 2004/049137 A2

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.