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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number
WO 2004/114575 A3

(51) International Patent Classification[7]: H04L 9/30, 9/32

(21) International Application Number:
PCT/US2004/019437

(22) International Filing Date: 17 June 2004 (17.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/479,626 17 June 2003 (17.06.2003) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, CA 94128-8999 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SAHOTA, Jagdeep, Singh** [US/US]; 981 Coral Ridge Road, Rodeo, 94572 (US).

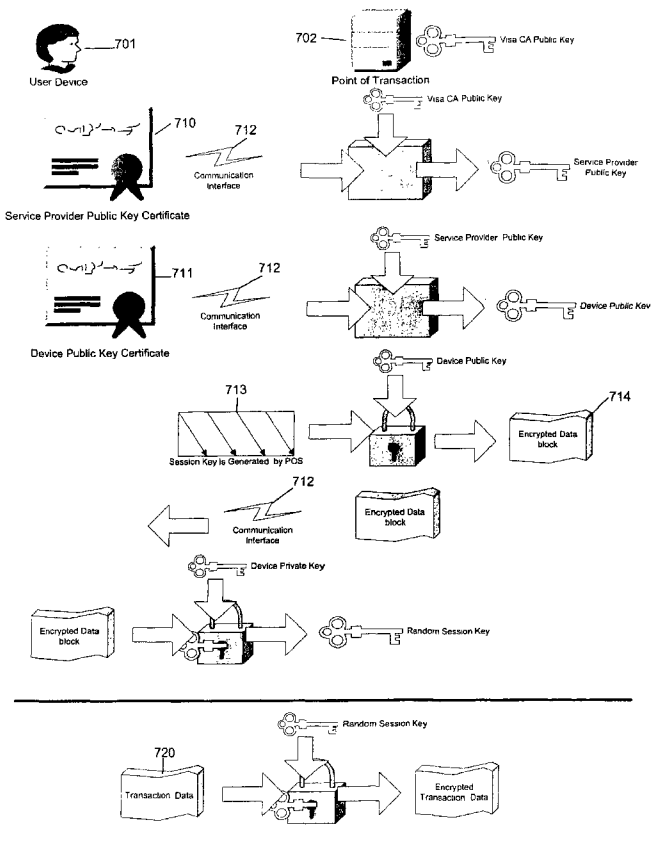
(74) Agent: **MELNIK, W., Joseph**; Pepper Hamilton LLP, One Mellon Center, 50th Floor, 500 Grant Street, Pittsburgh, PA 15219 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: 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, NA, 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, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

*[Continued on next page]*

(54) Title: METHOD AND SYSTEMS FOR SECURELY EXCHANGING DATA IN AN ELECTRONIC TRANSACTION




(57) Abstract: Methods and systems of encrypting and authenticating transaction data via the use of encryption and authentication algorithms are disclosed. Encryption and decryption algorithms are stored within a computer-readable storage medium and executed by a processor on a user device (701). These algorithms are used when a transaction is initiated by the user device (701) with a point of transaction terminal (702) across a communication interface (712) to establish a secure connection for the transmission of data. Data relating to the transaction is then sent across the communication interface (712) through the secure connection.

WO 2004/114575 A3

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, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— *with international search report*

**(88) Date of publication of the international search report:**
31 March 2005

*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.*