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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023713 A1

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

(21) International Application Number:
PCT/US2003/027342

(22) International Filing Date:
2 September 2003 (02.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/232,624 3 September 2002 (03.09.2002) US

(71) Applicant: **VERISIGN, INC.** [US/US]; 487 East Middlefield Road, Mountain View, CA 94043 (US).

(72) Inventors: **ANDREWS, Richard, F.**; 279 Leland Avenue, Menlo Park, CA 94025 (US). **HUANG, Zhiyong**; 1000 Escalon Avenue, #D1027, Sunnyvale, CA 94085 (US). **RUAN, Tom Qi Xion**; 6447 Ivy Lane, San Jose, CA 95129 (US).

(74) Agents: **ROSINI, James, E.** et al.; Kenyon & Kenyon, 1500 K Street, N.W., Suite 700, Washington, DC 20005 (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, SY, 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*
— *with amended claims*

Date of publication of the amended claims: 10 June 2004

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: METHOD AND SYSTEM OF SECURELY ESCROWING PRIVATE KEYS IN A PUBLIC KEY INFRASTRUCTURE

(57) Abstract: A method of restricting access to private keys in a public key infrastructure provides for storage of an encrypted private key at a primary site. A masked session key is stored at a secondary site, where the masked session key enables recovery of the private key. By using distributed storage architecture for recovery data, simplification can be achieved without sacrificing security.

WO 2004/023713 A1