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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 April 2006 (27.04.2006)

PCT

(10) International Publication Number
WO 2006/044717 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/037113

(22) International Filing Date: 17 October 2005 (17.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/618,600 15 October 2004 (15.10.2004) US

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

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **POPP, Nicolas** [US/US]; 196 Santa Monica Ave., Menlo Park, CA 94025 (US). **M'RAIHI, David** [US/US]; Mountain View, CA. **HART, Loren** [US/US]; Mountain View, CA.

(74) Agents: **ROSINI, James, E.** et al.; Kenyon & Kenyon, 1500 K Street, N.W., Suite 700, Washington, DC 20005 (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, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, 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, IS, IT, LT, LU, LV, 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:
— *without international search report and to be republished upon receipt of that 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.

WO 2006/044717 A2

(54) Title: ONE TIME PASSWORD

(57) Abstract: A token calculates a one time password by generating a HMAC-SHA-1 value based upon a key K and a counter value C, truncating the generated HMAC-SHA-1 value modulo 10^Digit, where Digit is the number of digits in the one time password. The one time password can be validated by a validation server that calculates its own version of the password using K and its own counter value C'. If there is an initial mismatch, the validation server compensate for a lack of synchronization between counters C and C' within a look-ahead window, whose size can be set by a parameter s.