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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 July 2004 (22.07.2004)

PCT

(10) International Publication Number
WO 2004/061668 A1

(51) International Patent Classification[7]: G06F 11/30, 12/14, H04L 9/00, 9/32

(21) International Application Number:
PCT/US2003/041662

(22) International Filing Date:
31 December 2003 (31.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/437,416 31 December 2002 (31.12.2002) US

(71) Applicant: **SYSTEMS RESEARCH & DEVELOPMENT** [US/US]; 6600 Bermuda Road, Suite A, Las Vegas, NV 89119 (US).

(72) Inventor: **JONAS, Jeffrey, James**; 9717 Winter Palace Drive, Las Vegas, NV 89145 (US).

(74) Agent: **BERGER, Jeffrey, K.**; Marshall, Gerstein & Borun LLP, 6300 Sears Tower, 233 South Wacker Drive, Chicago, IL 60606 (US).

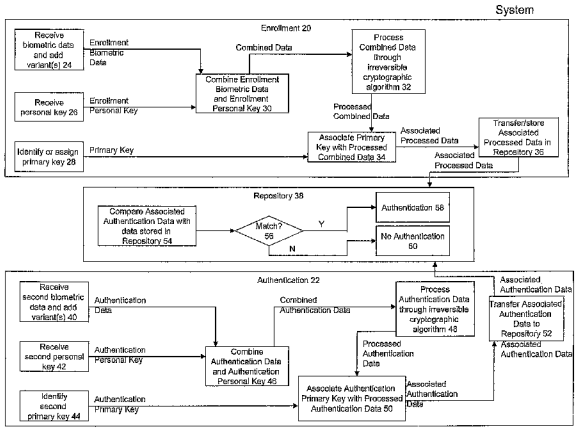
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, 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:**
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*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: AUTHORIZED ANONYMOUS AUTHENTICATION




(57) Abstract: A method, program and system for processing data is disclosed. The method, program and system comprising the steps of: (a) receiving (e.g., during an enrollment process) a first biometric data (24) and a first personal key (26), (b) processing the first biometric data and the first personal key through an irreversible cryptographic algorithm (32), sometimes after: (i) generating one or more variants from the first biometric data, (ii) processing the first personal key through a reversible cryptographic algorithm, and (iii) adding salt to the first biometric data (40) or first personal key, (c) receiving (e.g., during an authentication process) a second biometric data (40) and a second personal key (42), (d) processing the second biometric data and the second personal key through the irreversible cryptographic algorithm (48), (e) comparing the second processed data to the first processed data (54), and (f) generating a signal pertaining to the comparison of the second processed data to the first processed data, such as: (i) a confirmation (58) reflecting authentication when the second processed data matches the first processed data (sometimes allowing access to a facility or system) or (ii) a denial (60) reflecting no confirmation when the second processed data does not match the first processed data.

WO 2004/061668 A1