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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 May 2005 (19.05.2005)

PCT

(10) International Publication Number
WO 2005/045617 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US2004/035459

(22) International Filing Date: 26 October 2004 (26.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/514,760 27 October 2003 (27.10.2003) US
10/882,527 1 July 2004 (01.07.2004) US

(71) Applicant *(for all designated States except US)*: **JP MORGAN CHASE BANK** [US/US]; 270 Park Avenue, New York, NY 10172 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BENSON, Glenn, Stuart** [US/US]; 334 Alden Place, Newton, MA 02465 (US). **CALACETO, Joseph, R.** [US/US]; 645 Terhune Road, Ridgewood, NJ 07450 (US). **LOGAR, Russel, M.** [US/US]; 28 Pelham Walk, Breezy Point, NY 11697 (US).

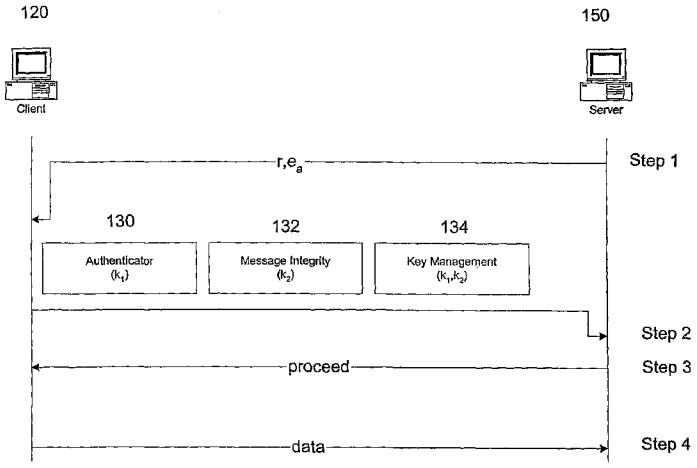
(74) Agent: **PETRUZZELLI, Justin, D.**; Lowenstein Sandler PC, 65 Livingston Avenue, Roseland, NJ 07068 (US).

(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, 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).

[Continued on next page]

(54) Title: PORTABLE SECURITY TRANSACTION PROTOCOL



(57) Abstract: A technique for providing message authenticity includes accepting transaction information, accepting a first data item used for authenticating an originating user, cryptographically processing the transaction information using only a second data item, wherein the entropy of the first data item is less than the entropy of the second data item, and authenticating the originating user using the first data item. The first data item can be a sequence of digits corresponding to those displayed on an external device, such as, for example, an RSA authorization token, credit card, *etc.* In general, the first data item will be a short alphanumeric string and the second data item will generally be much larger, *e.g.*, a 128 bit sequence to be used principally for data authentication. According to another aspect of the present invention, consequential evidence of the transaction may be secured to provide after-the-fact evidence of the transaction. This evidence can include a message written to a tamper-resistant log record, the message including the transaction information, the first data item, the second item, and an identifier for the originating user, as well as other information. At a subsequent point, the transaction can be shown to have been sent by the originating user and received by the intended recipient, by consulting the log record. Preferably, the validity of the transaction would be ascertained by an independent, mutually trusted third party.

WO 2005/045617 A2

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.