



(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/US2011/032271

(22) International Filing Date:
13 April 2011 (13.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/327,723 26 April 2010 (26.04.2010) US
13/081,067 6 April 2011 (06.04.2011) US

(71) Applicant (for all designated States except US): **HAWK AND SEAL, INC.** [US/US]; 8745 West Higgins Road, Suite 240, Chicago, Illinois 60631 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **GANESAN, Ravi** [US/US]; 701 South Olive, #1814, West Palm Beach, Florida 33401 (US).

(74) Agent: **STADNICKI, Alfred, A.**; Antonelli, Terry, Stout & Kraus, LLP, 1300 N. 17th Street, Suite 1800, Arlington, Virginia 22209 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SECURE AND EFFICIENT LOGIN AND TRANSACTION AUTHENTICATION USING IPHONES AND OTHER SMART MOBILE COMMUNICATION DEVICES

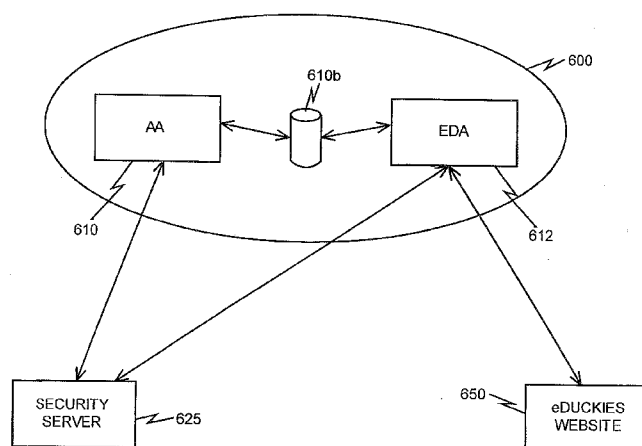


Figure 7

(57) Abstract: To authenticate a user of a mobile communication device for login or transaction authorization, a first application on the device directs transmission of a request for authentication of the user to a security server. A second application on the device receives the request for authentication from the security server and directs presentation of the received request for authentication to the user by the device. The second application receives a user input to the device indicating that the requested authentication should proceed and in response directs transmission of an indication that the requested authorization should proceed, to the security server. In response to this latter transmission, the second application receives a PIN from the authentication server. The first application directs transmission of the PIN received by the second application to the network site, which validates the transmitted PIN, in order to authenticate the user or the transaction to the network site.