



(51) International Patent Classification:

G06F 7/04 (2006.01) G11C 7/00 (2006.01)
G06F 12/00 (2006.01)

(21) International Application Number:

PCT/US2012/032840

(22) International Filing Date:

10 April 2012 (10.04.2012)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

13/089,430 19 April 2011 (19.04.2011) US

(71) Applicant (for all designated States except US): AU-
THENTIFY INC. [US/US]; 8745 W. Higgins Road, Suite
240, Chicago, Illinois 60631 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): Ravi, Ganesan
[US/US]; 701 South Olive, #1814, West Palm Beach, Flor-
ida 33401 (US).

(74) Agent: STADNICKI, Alfred, A.; Antonelli, Terry, Stout
& Kraus, LLP, 1300 North 17th Street, Suite 1800, Arling-
ton, Virginia 22209 (US).

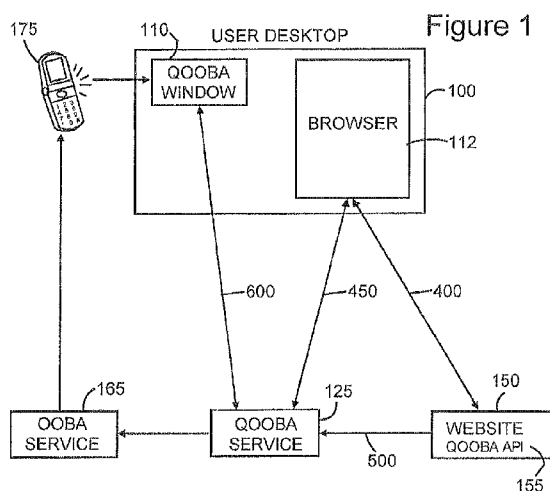
(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IS, JP, KE, KG, 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, QA, RO, RS, RU, RW, 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, RW, 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: KEY MANAGEMENT USING QUASI OUT OF BAND AUTHENTICATION ARCHITECTURE



(57) Abstract: To provide key management layered on a quasi-out-of-band authentication system, a security server receives a request for activation of a user interface window for a particular user from a network device via a communication channel. It then transmits an activation PIN to an out of band authentication system for forwarding to the user's telephone via a voice or text message. It next receives the previously transmitted PIN from the network device via the communication channel, and authenticates the user based on the received PIN. After authenticating the user, it establishes a secure, independent, encrypted communication channel between the user interface window and the security server on top of the original communication channel. It then generates and transmits to the user interface window and/or receives from the user interface window via the secure communication channel, key material and certificate material for public key and/or symmetric key cryptography based operations.