

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
16 January 2020 (16.01.2020)



(10) International Publication Number
WO 2020/013928 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/US2019/035420

(22) International Filing Date:
04 June 2019 (04.06.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/035,480 13 July 2018 (13.07.2018) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventor: **CHUMBLEY, Robert**; 4421 Pasada Lane, Round Rock, Texas 78681 (US).

(74) Agent: **JEWIK, Patrick** et al.; KILPATRICK TOWNSEND & STOCKTON LLP, Mailstop: IP Docketing - 22, 1100 Peachtree Street, Suite 2800, Atlanta, Georgia 30309 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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.

(54) Title: PUBLIC-PRIVATE KEY PAIR ACCOUNT LOGIN AND KEY MANAGER

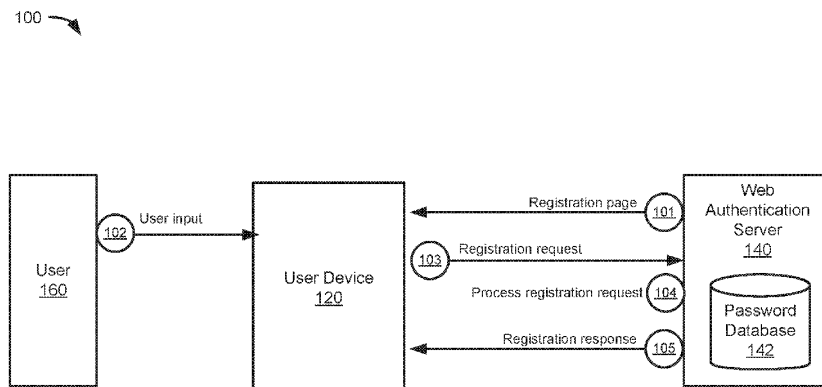


FIG. 1

(57) Abstract: Embodiments of the invention provide improved account authentication using public-private key cryptography instead of passwords. Instead of registering a password and using that password to login to an account, an authentication server of an account provider registers a public key received from a user device. To authenticate the user device for logging into an account, the authentication server generates a challenge and encrypts using the registered public key. The encrypted challenge is sent to the user device, which can decrypt the challenge using the private key corresponding to the registered public key. The decrypted challenge is used for authentication instead of using a password. The private key corresponding to the public key is securely stored and not revealed to the authentication server.

[Continued on next page]

WO 2020/013928 A1

(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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

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