



(51) International Patent Classification:

G06F 21/62 (2013.01) G06F 21/33 (2013.01)
G06F 21/60 (2013.01) H04L 9/32 (2006.01)
G06F 21/64 (2013.01) H04L 29/06 (2006.01)

(21) International Application Number:

PCT/US2021/041314

(22) International Filing Date:

12 July 2021 (12.07.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/928,367 14 July 2020 (14.07.2020) US

(71) Applicant: VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: WAGNER, Kim Ritter; P.O. Box 8999, San Francisco, California 94128 (US). ARORA, Sunpreet Singh; P.O. Box 8999, San Francisco, California 94128 (US). WATSON, Gaven James; P.O. Box 8999, San Francisco, California 94128 (US). CHRISTODORESCU, Mihai; P.O. Box 8999, San Francisco, California 94128 (US). AGRAWAL, Shashank; P.O. Box 8999, San Francisco, California 94128 (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,

(54) Title: PRIVACY-PRESERVING IDENTITY ATTRIBUTE VERIFICATION USING POLICY TOKENS

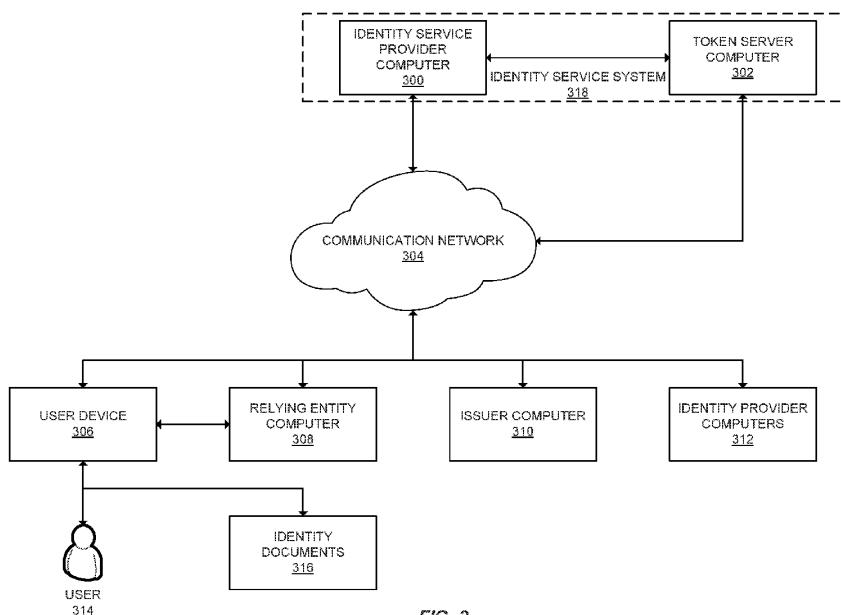


FIG. 3

(57) Abstract: Methods and systems for privacy-preserving identity attribute verification are presented. During an interaction between a relying entity and a user, a relying entity computer can transmit a policy token to a user device. The policy token may indicate the information needed by the relying entity in order to perform the interaction. The user device can verify the policy token, then use the policy token in conjunction with an identity token to generate a zero-knowledge proof. The user device may transmit the zero-knowledge proof to an identity service provider computer. The identity service provider computer may verify the zero-knowledge proof, then generate a verification message. The identity service provider computer may sign the verification message and transmit the signed verification message to the relying entity computer. The relying entity computer may verify the verification message and complete the interaction with the user.

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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, 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))