

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
27 May 2022 (27.05.2022)



(10) International Publication Number
WO 2022/109020 A1

(51) International Patent Classification:

H04L 9/32 (2006.01) H04L 9/40 (2022.01)
H04L 9/08 (2006.01)

(21) International Application Number:

PCT/US2021/059717

(22) International Filing Date:

17 November 2021 (17.11.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/115,475 18 November 2020 (18.11.2020) US
63/241,495 07 September 2021 (07.09.2021) US

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

(72) Inventors: **WAGNER, Kim**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **SULLIVAN, Brian**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **SLOAN, Dinah**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **NGO, Hao**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **WATSON, Gaven James**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **ARORA, Sunpreet Singh**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **BADRINARAYANAN, Saikrishna**; c/o Visa International Ser-

(54) Title: INTEGRATING IDENTITY TOKENS AND PRIVACY-PRESERVING IDENTITY ATTRIBUTE ATTESTATIONS INTO INTERACTIONS

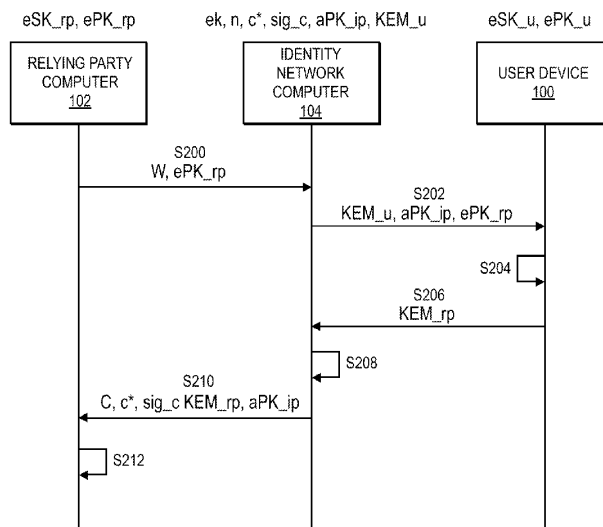


FIG. 2

(57) Abstract: A method is disclosed. The method comprises receiving, by an identity network computer, a query set including a plurality of test identity attributes. After receiving the query set, the identity network computer may retrieve derivatives of identity attributes associated with a user, and an encrypted trapdoor, then compute an obscured query set using the query set, and optionally the derivatives of identity attributes. The identity network computer may transmit the obscured query set (i) and the encrypted trapdoor to a user device associated with the user, which generates and transmits a first modified trapdoor and the obscured query set to a relying party computer, or (ii) and a second modified trapdoor to the relying party computer. The relying party computer may thereafter use the obscured query set, and the first modified trapdoor or the second modified trapdoor, to determine if the identity attributes is a member of the query set.

[Continued on next page]

vice Association, P.O. Box 8999, San Francisco, California 94128 (US). **RAGHURAMAN, Srinivasan**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US).

(74) **Agent: JEWIK, Patrick**; 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, 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))