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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2025 (18.09.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/193477 A1

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

(21) International Application Number:
PCT/US2025/018445

(22) International Filing Date:
05 March 2025 (05.03.2025)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
18/602,523 12 March 2024 (12.03.2024) US
19/022,285 15 January 2025 (15.01.2025) US

(71) Applicant: **CITIGROUP TECHNOLOGY, INC.** [US/US]; 388 Greenwich Street, New York, New York 10013 (US).

(72) Inventors: **MCMAHON, Alex**; 388 Greenwich Street, New York, New York 10013 (US). **CAREY, Paul**; 388 Greenwich Street, New York, New York 10013 (US). **IYER, Sudha**; 388 Greenwich Street, New York, New York 10013 (US).

(74) Agent: **SOPHIR, Eric** et al.; FOLEY & LARDNER LLP, 3000 K Street N.W., Washington, District of Columbia 20007 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, UY, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2025/193477 A1

(54) Title: SYSTEMS AND METHODS FOR ESTABLISHING DATA PROVENANCE BY GENERATING ONE-TIME SIGNATURES

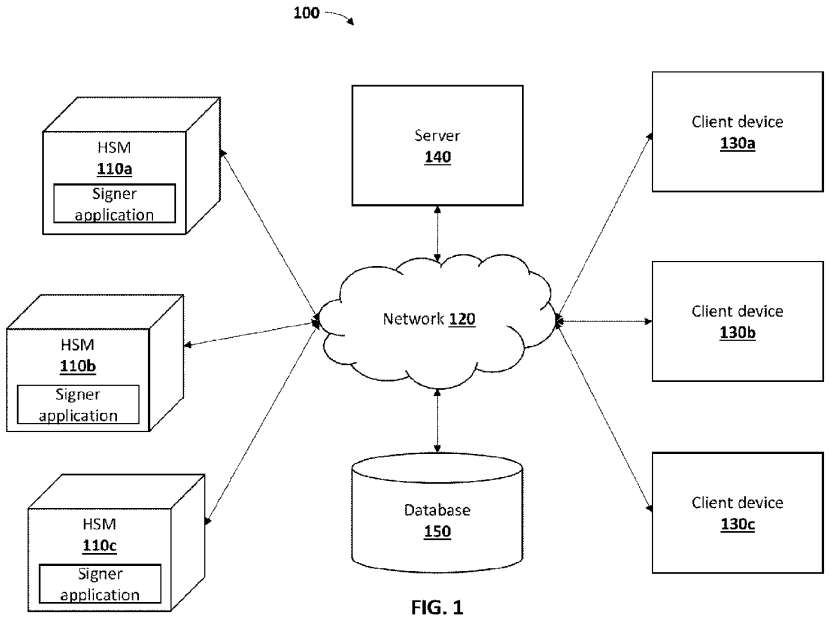


FIG. 1

(57) Abstract: Presented herein are system and methods for establishing data provenance by generating one- time signatures. A system may include one or more processors that receive, via an application programming interface (API) request, a request for a one-time signature and data associated with the request, provide a seed identifier and the data associated with the request to an HSM in a set of HSMs, and receive a response message from the HSM, the response message including a one-time signature. In examples, the response message and the one-time signature are provided to the device that transmitted the request for the one-time signature and the data associated with the request. Methods and non-transitory computer-readable mediums are also presented.

[Continued on next page]

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*