

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
10 November 2022 (10.11.2022)



(10) International Publication Number
WO 2022/234137 A3

(51) International Patent Classification:

H04L 9/40 (2022.01) *G06F 21/33* (2013.01)
H04L 9/32 (2006.01) *H04L 67/146* (2022.01)

(21) International Application Number:

PCT/EP2022/062379

(22) International Filing Date:

06 May 2022 (06.05.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/185,687 07 May 2021 (07.05.2021) US

(71) Applicant: **DFINITY STIFTUNG** [CH/CH]; Genferstrasse 11, 8002 Zürich (CH).

(72) Inventors: **BREITNER, Joachim**; c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH). **CAMENISCH, Jan**;

c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH). **TACKMANN, Björn**; c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH). **WILLIAMS, Dominic**; c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH).

(74) Agent: **E. BLUM & CO. AG**; Vorderberg 11, 8044 Zürich (CH).

(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, IQ, IR, IS, IT, JM, 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,

(54) Title: IDENTITY SERVICES AND AUTHENTICATION IN DISTRIBUTED NETWORKS

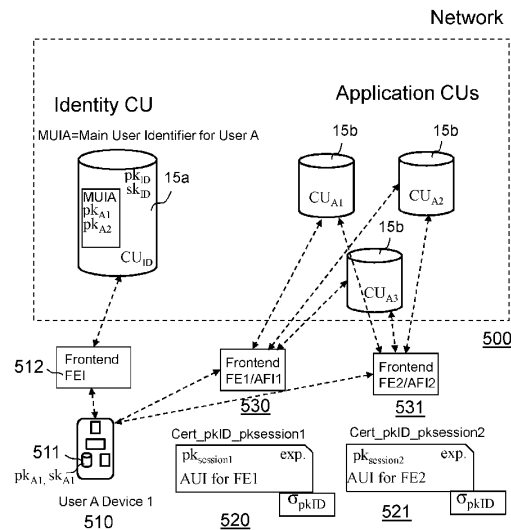


FIG. 5a

(57) Abstract: According to an embodiment of an aspect of the invention, there is a computer-implemented method for authenticating users of a network. The method comprises steps of maintaining, by an identity service, user accounts under a main user identifier, wherein the user accounts support a method of authentication by the user. The method further comprises generating, by an application frontend, a session public key of a public key verification scheme and providing, by the application frontend, the session public key to the identity service. Further steps include obtaining, by the application frontend, a certification from the identity service, the certification comprising the session public key and an application user identifier. The application user identifier is derived from the main user identifier and an application frontend identifier.

[Continued on next page]

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))*
- *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))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

(88) Date of publication of the international search report:

22 December 2022 (22.12.2022)