



(51) International Patent Classification:

H04L 9/08 (2006.01) H04L 9/40 (2022.01)
H04L 9/32 (2006.01) G06F 21/30 (2013.01)
H04W 12/06 (2021.01)

(21) International Application Number:

PCT/EP2022/053090

(22) International Filing Date:

09 February 2022 (09.02.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

21161033.2 05 March 2021 (05.03.2021) EP

(71) Applicant: SEPIOR APS [DK/DK]; Inge Lehmanns Gade
10, etage 6, 8000 Aarhus C (DK).(72) Inventors: DAMGÅRD, Ivan, Bjerre; Johannes Ewalds
Vej 9, 8230 Åbyhøj (DK). JAKOBSEN, Thomas Pelle;
Obstrupvej 12K, 8320 Mårslet (DK). PAGTER, Jakob,
Illeborg; Fenrisvej 71, 8210 Aarhus V (DK). LAU-
RITZEN, Torben; c/o SEPIOR A/S, Inge Lehmanns Gade
10, etage 6, 8000 Aarhus C (DK).(74) Agent: INSPICOS P/S; Agern Allé 24, 2970 Hørsholm
(DK).

(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).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

(54) Title: A METHOD FOR AUTHENTICATING A USER TOWARDS A MULTI-NODE PARTY

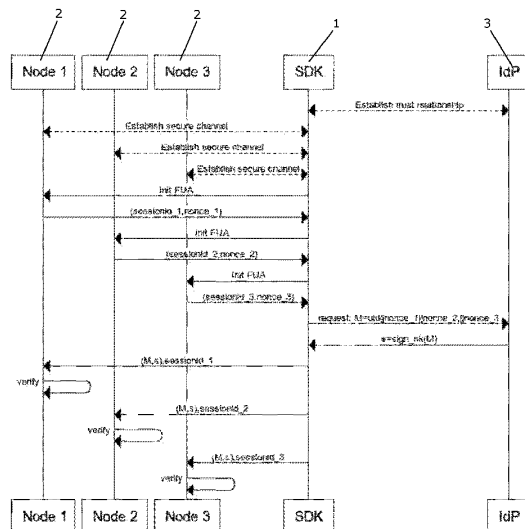


Fig. 1

(57) Abstract: A method for authentication of a user towards a multi-node party is disclosed, the multi-node party comprising at least two nodes. The user contacts the nodes of the multi-node party, via a user application, and each of the nodes of the multi-node party generates a nonce and returns the nonce to the user application. The user application requests authentication from an Identity Provider, based on the nonces received from the nodes of the multi-node party and on a unique identity of the user. The Identity Provider generates a message, based on the request for authentication, and provides the message to the user application. The user application provides the message in a secret form to each of the nodes of the multi-node party. The nodes of the multi-node party verify the message, based on the received secret form of the message and by means of a multi-party verifying operation, such as secure multi-party computation (MPC), and the user is authenticated based on the multi-party verifying operation.

[Continued on next page]

Published:

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