

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 March 2021 (11.03.2021)



(10) International Publication Number
WO 2021/044411 A1

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

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

(21) International Application Number:
PCT/IL2020/050949

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- of inventorship (Rule 4.17(iv))

(22) International Filing Date:
01 September 2020 (01.09.2020)

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))

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/559,693 04 September 2019 (04.09.2019) US

(71) Applicant: **PUZZZLE CYBERSECURITY LTD.**
[IL/IL]; 3 Israel Bak Street, 4th floor, 6701908 Tel Aviv (IL).

(72) Inventors: **SHAMAI, Shazar**; 6B Sokolov Street, 7644508 Rehovot (IL). **LAMESHI, Lior**; 13 Heil HaShiryon Street, 7570243 Rishon-LeZion (IL). **SHALTI, Tal**; 19 HaPalmach Street, 6706533 Tel-Aviv (IL). **ORLAND, Matan**; 18 Zichron Yaakov Street, 6299919 Tel-Aviv (IL).

(74) Agent: **EHRlich, Gal et al.**; G. E. EHRlich (1995) LTD., 11 Menachem Begin Road, 5268104 Ramat-Gan (IL).

(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,

(54) Title: SYSTEMS AND METHODS FOR SIGNING OF A MESSAGE

(57) Abstract: There is provided a requestor device for digital signing of a message, comprising: at least one hardware processor executing a code for: transmitting the message for signing thereof, in a single request session over the network to each one of a plurality of validator devices, wherein a beacon device computes and transmits over a network to each one of a plurality of validator devices a signature-data value computed and signed by the beacon device, receiving in a single response session from each one of the plurality of validator devices, a respective partial-open decrypted value computed for the signature-data value and the message, and aggregating the partial-opens decrypted values received from the plurality of validator devices to compute the digital signature of the message.



WO 2021/044411 A1