



(51) International Patent Classification:

H04L 9/32 (2006.01) G06F 21/60 (2013.01)
H04L 9/40 (2022.01) G06Q 20/38 (2012.01)
H04L 67/01 (2022.01)

(21) International Application Number:

PCT/IB2024/051131

(22) International Filing Date:

07 February 2024 (07.02.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2350116-6	07 February 2023 (07.02.2023)	SE
2350135-6	13 February 2023 (13.02.2023)	SE
2350200-8	21 February 2023 (21.02.2023)	SE
2350364-2	29 March 2023 (29.03.2023)	SE

(71) Applicant: **CRUNCHFISH DIGITAL CASH AB**
[SE/SE]; c/o Crunchfish AB, Stora Varvsgatan 6A 4TR, 211 19 MALMÖ (SE).

(72) Inventors: **CRONHOLM, Paul**; c/o Crunchfish AB, Stora Varvsgatan 6A 4TR, 211 19 MALMÖ (SE). **SAMUELSSON, Joachim**; Drottninggatan 77, lgh 1602, 254 33 HELSINGBORG (SE).

(74) Agent: **STRÖM & GULLIKSSON AB**; P.O. Box 4188, 203 13 Malmö (SE).

(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,

(54) Title: TRUSTED APPLICATION PROTOCOL-BASED COMMUNICATION

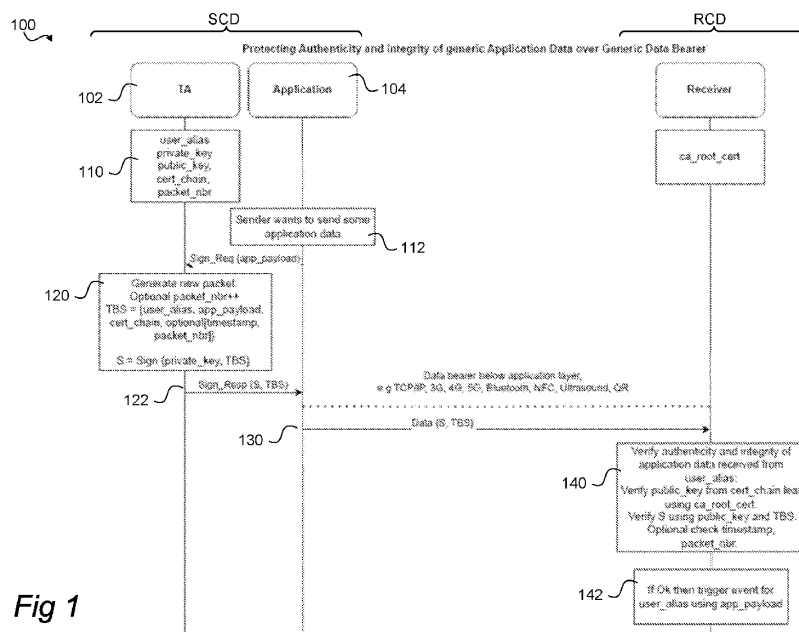


Fig 1

(57) Abstract: The claimed invention concerns a method (100) for building trust in communication application. The invention solves the problem of current methods requiring an exchange of cryptographic information in a handshake procedure. The problem is solved by an extension to a layered communication stack for the purpose of introducing trust at the application layer from a sending device. The added trusted application protocol layer provides trust to services regardless of the communication network and is implemented by running a trusted application (102) that keeps a private cryptographic key in a secure execution environment and keeping a digital certificate in the sending communication device, the digital certificate comprising a public cryptographic key corresponding to the private cryptographic key being signed by a certificate authority, wherein a second application in the sending device receives signed data and signature and generates (120) a header or tail with the signature and certificate and sends (130) this information to a receiving

[Continued on next page]

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, UZ, VC, VN, WS,
ZA, ZM, ZW.

(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))*

device for verification (140).