

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
19 September 2024 (19.09.2024)



(10) International Publication Number
WO 2024/191341 A1

- (51) **International Patent Classification:**
G06F 21/53 (2013.01) *H04L 9/00* (2022.01)
G06Q 20/00 (2012.01)
- (21) **International Application Number:**
PCT/SE2024/050245
- (22) **International Filing Date:**
18 March 2024 (18.03.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2350296-6 16 March 2023 (16.03.2023) SE
- (71) **Applicant: CRUNCHFISH DIGITAL CASH AB**
[SE/SE]; c/o Crunchfish AB, Stora Varvsgatan 6A 4TR, 211 19 MALMÖ (SE).
- (72) **Inventors: SAMUELSSON, Joachim;** Drottninggatan 77, lgh 1602, 254 33 HELSINGBORG (SE). **CRONHOLM, Paul;** c/o Crunchfish AB, Stora Varvsgatan 6A 4TR, 211 19 MALMÖ (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, 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,

(54) **Title:** PREVENTING FRAUDULENT ROLLBACK OF A TRUSTED APPLICATION

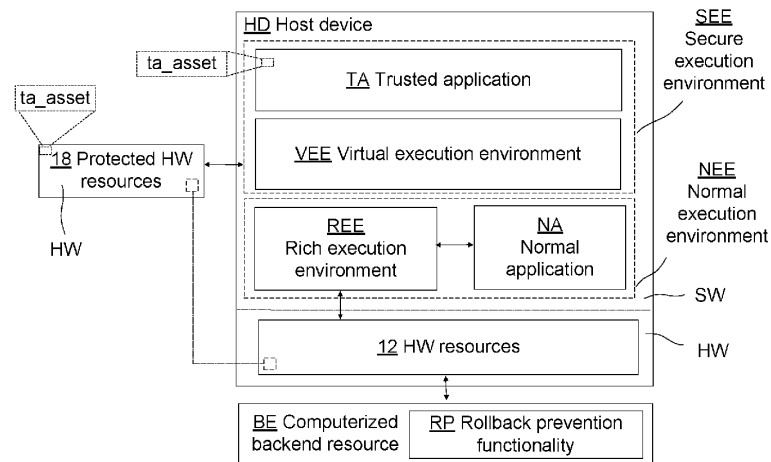


FIG. 1B

(57) **Abstract:** A method (500) of preventing fraudulent rollback of a trusted application (TA) involving repeatedly recording (510) an execution state of the trusted application (TA); repeatedly causing (520) recording of the execution state in an entity external to the trusted application (TA); upon occurrence of an event in the trusted application (TA), sending (530) a request (Sec Update Req, Issuer Update Req; Device SE Sign Req) to said external entity; receiving (540) a response (Issuer Update Resp; Device SE Sign Resp, Sec Update Resp) to said request including information which enables verification by the trusted application (TA) that a present execution state within the trusted application (TA) is not older than a most recent execution state as recorded by the external entity; and controlling (550) access to the protected asset (ta asset) depending on an outcome of the verification. The external entity signs the response (Issuer Update Resp; Device SE Sign Resp, Sec Update Resp) with a private cryptographic key (issuer _priv_key; device se priv key), and

[Continued on next page]

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))

the trusted application (TA) verifies the signature.