

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
05 December 2019 (05.12.2019)



(10) International Publication Number
WO 2019/229257 A1

- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *G06F 21/60* (2013.01)
- (21) **International Application Number:**
PCT/EP2019/064227
- (22) **International Filing Date:**
31 May 2019 (31.05.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
18175515.8 01 June 2018 (01.06.2018) EP
15/996,336 01 June 2018 (01.06.2018) US
- (72) **Inventor; and**
- (71) **Applicant: TEGEDER, Roland** [GB/GB]; 5th Floor,
Nuffield House, 41-46 Piccadilly, London W1J 0DS (GB).
- (72) **Inventor: SHARP, Richard**; 5th Floor, Nuffield House,
41-46 Piccadilly, London W1J 0DS (GB).

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))

- (74) **Agent: SMALL, Gary James et al.**; Carpmacels & Ransford LLP, One Southampton Row, London WC1B 5HA (GB).
- (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,

(54) **Title:** SYSTEM AND METHOD FOR PROVIDING AN AUTHORISED THIRD PARTY WITH OVERT LEDGER SECURED KEY ESCROW ACCESS TO A SECRET

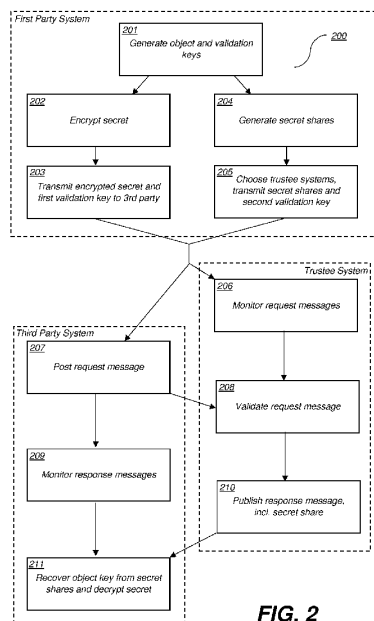


FIG. 2

(57) **Abstract:** The present invention relates to a cryptographic protocol, and a system for implementing said protocol, for providing overt ledger secured key escrow access to encrypted data. The invention uses a plurality of trustee systems, each holding a secret share of a secret, to validate requests for the secret from authorised third parties. When a valid request is made, each trustee system publishes its secret share to a ledger. The secret shares can be combined to reveal the encryption key only by the authorised third party. Requests for the encryption key, and the responses by the trustee systems, can be accessed by the owner of the encryption key to identify the requesting third party and to have proof that the key has been revealed to the third party.

WO 2019/229257 A1