

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 June 2020 (11.06.2020)



(10) International Publication Number
WO 2020/114377 A1

- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/CN2019/122605
- (22) **International Filing Date:**
03 December 2019 (03.12.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
18115417.3 03 December 2018 (03.12.2018) HK
- (71) **Applicant: FORIS LIMITED** [CN/CN]; Unit 1506-07, 15/F, Pacific Plaza, 418 Des Voeux Road West, Sai Wan, Hong Kong (CN).
- (72) **Inventors: NG, Ming Sum Sam**; Unit 1506-07, 15/F, Pacific Plaza, 418 Des Voeux Road West, Sai Wan, Hong Kong (CN). **CHAN, Marthew David**; Unit 1506-07, 15/F, Pacific Plaza, 418 Des Voeux Road West, Sai Wan, Hong Kong (CN). **LAU, Wai King Jason**; Unit 1506-07, 15/F, Pacific Plaza, 418 Des Voeux Road West, Sai Wan, Hong Kong (CN). **KUNG, Siu Kei Thomas**; Unit 1506-07, 15/F, Pacific Plaza, 418 Des Voeux Road West, Sai Wan, Hong Kong (CN).

(74) **Agent: RUNPING & PARTNERS**; Suite 515, Yingu Mansion, No. 9 Beisihuanxilu, Haidian District, Beijing 100190 (CN).

(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, 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).

(54) **Title:** SECURE DISTRIBUTED KEY MANAGEMENT SYSTEM

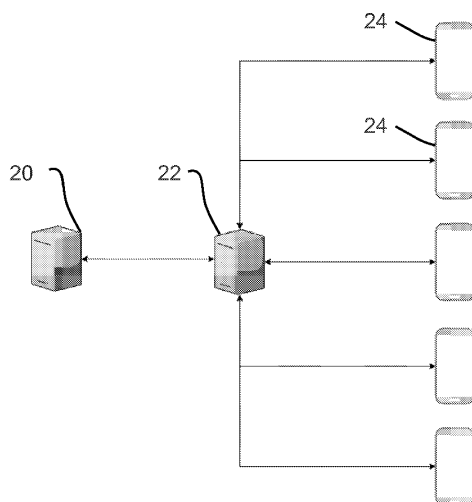


Fig.1

(57) **Abstract:** A distributed key management system, which contains a server, a plurality of key-holding devices adapted to communicate with the server; and a key-requesting device adapted to communicate with the server. Each one of the plurality of key-holding devices is adapted to hold a different fragment of a private key. The server is adapted to reconstruct the private key based on the fragments received from the plurality of key-holding devices. The key-requesting device is adapted to obtain the private key from the server. The systems according to the invention provide a zero-trust model key management scheme and would eliminate the risk of key leakage to unauthorized person while providing flexibility of authorizing devices.

[Continued on next page]

Published:

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