



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

(21) International Application Number:
PCT/IB2021/051090

(22) International Filing Date:
10 February 2021 (10.02.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/818,534 13 March 2020 (13.03.2020) US

(71) Applicant: **INTERNATIONAL BUSINESS
MACHINES CORPORATION** [US/US]; New Orchard
Road, Armonk, New York 10504 (US).

(71) Applicants (*for MG only*): **IBM (CHINA) INVEST-
MENT COMPANY LTD.** [CN/CN]; 25/F, Pangu Plaza,
No. 27, Central North 4th Ring Road, Chaoyang District,
Beijing, Beijing 100101 (CN). **IBM DEUTSCHLAND
GMBH** [DE/DE]; IBM-Allee 1, 71139 Ehningen (DE).

(72) Inventors: **BECK, Michael**; c/o IBM Deutschland Re-
search & Development GmbH, Schoenaicher Strasse 220,
71032 Boeblingen (DE). **SMOLNY, Martin**; c/o IBM
Deutschland Research & Development GmbH, Schoenaich-
er Strasse 220, 71032 Boeblingen (DE). **DUERR, Thomas**;
c/o IBM Deutschland Research & Development GmbH,
Schoenaicher Strasse 220, 71032 Boeblingen (DE). **OCHS,
Georg**; c/o IBM Deutschland Research & Development
GmbH, Schoenaicher Strasse 220, 71032 Boeblingen (DE).
MCBREARTY, Gerald; c/o IBM Research - Austin,
11501 Burnet Rd, Austin, Texas 78758 (US). **SOOHOO,**

(54) Title: SECURE PRIVATE KEY DISTRIBUTION BETWEEN ENDPOINT INSTANCES

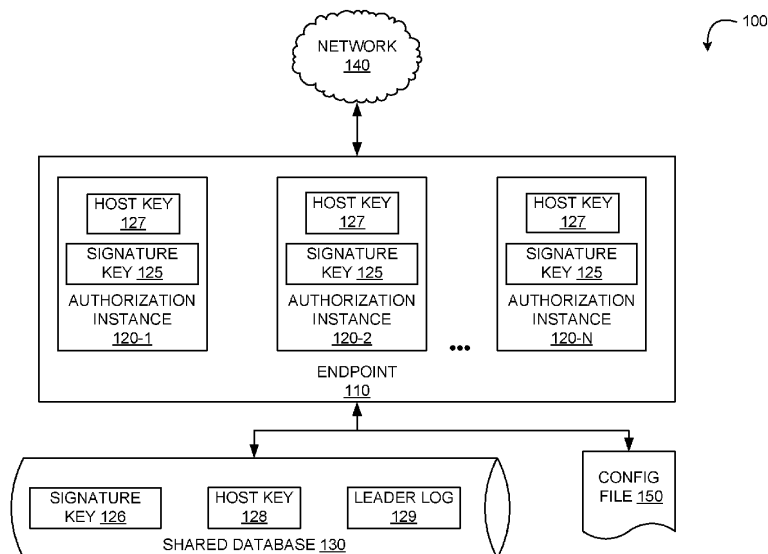


FIG. 1

(57) Abstract: A method, a computer program product, and a system for distributing a private signature key between authorization instances. The method includes registering a plurality of authorization instances in a configuration file and generating host instance key pairs by each of the authorization instances. The method also includes storing the public host keys in the shared database and electing one of the authorization instances to be a signature key leader instance. The method includes generating, by the signature key leader instance, a signature key pair. The signature key pair includes a public signature key and a private signature key. The method also includes storing the public signature key in the shared database and transmitting an encrypted private signature key to a requesting authorization instance of the authorization instances. The method further includes decrypting the encrypted private signature key using the private host key generated by the requesting authorization instance.

Stephen; c/o IBM Research - Austin, 11501 Burnet Rd,
Austin, Texas 78758 (US).

(74) **Agent: KLETT, Peter;** c/o IBM Deutschland GmbH,
Patentwesen und Urheberrecht, IBM Allee 1, 71139 Ehningen (DE).

(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, 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))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE