



(51) International Patent Classification:

H04L 9/08 (2006.01) H04L 9/06 (2006.01)
H04L 9/14 (2006.01) H04L 9/32 (2006.01)

(21) International Application Number:

PCT/US2020/021824

(22) International Filing Date:

10 March 2020 (10.03.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/374,905 04 April 2019 (04.04.2019) US

(71) Applicant: MICRON TECHNOLOGY, INC. [US/US];
8000 South Federal Way, Boise, Idaho 83707 (US).(72) Inventor: DUVAL, Olivier; 308 Magellan Drive, Pacifica,
California 94044 (US).(74) Agent: WARD, John P. et al.; Greenberg Traurig, LLP,
77 West Wacker Drive, Suite 3100, Chicago, Illinois 60601
(US).(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, 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))

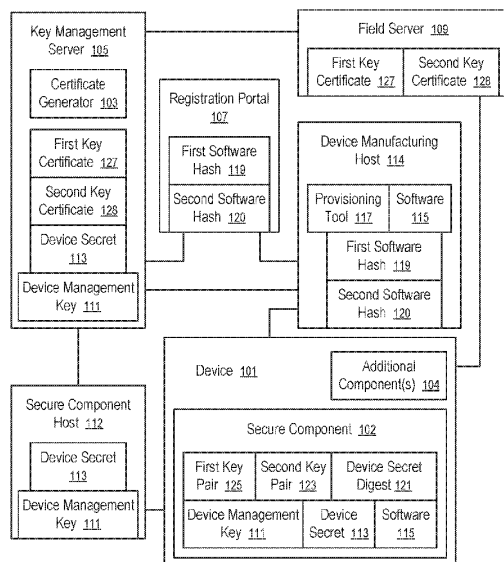
(54) Title: ONBOARDING SOFTWARE ON SECURE DEVICES TO GENERATE DEVICE IDENTITIES FOR AUTHENTI-
CATION WITH REMOTE SERVERS

FIG. 1

(57) Abstract: Systems, methods and apparatuses to configure a computing device for identification and authentication are described. For example, a key management server (KMS) has a certificate generator and is coupled to a registration portal. A copy of secret implemented into a secure component during its manufacture in a factory is stored in the KMS. After leaving the factory, the component can be assembled into the device. The portal receives registration of the component and a hash of software of the device. The certificate generator generates, independent of the device, public keys of the device, using the copy of the secret stored in the KMS and hashes of the software received via the registration portal, and then sign a digital certificate of the public key of the device. Authentication of the device can then be performed via the private key of the device and the certified public key.