

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
22 May 2020 (22.05.2020)



(10) International Publication Number
WO 2020/101567 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
H04L 9/30 (2006.01)

(21) International Application Number:
PCT/SG2019/050382

(22) International Filing Date:
31 July 2019 (31.07.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201810250P 16 November 2018 (16.11.2018) SG

(71) Applicant: MICROSEC PTE LTD [SG/SG]; 83B Rowell
Road, Singapore 208015 (SG).

(72) Inventors: MISHRA, Vishram; 446 Hougang Avenue 8,
#10-1623, Singapore 530446 (SG). IKRAM, Magzhan;
271 Tampines Street 21, #11-107, Singapore 520271 (SG).
KERRISON, Steven Paul; 83 Commonwealth Close,
#11-163, Singapore 140083 (SG). ZAINI, Shazina Binte;
33 Club Street, #10-18, Singapore 069415 (SG). SIDDIQI,
Ahnaf Aff; 770 Bedok Reservoir View, #15-179, Singapore
470770 (SG).

(74) Agent: VIERING, JENTSCHURA & PARTNER LLP;
P.O. Box 1088, Rochor Post Office, Rochor Road, Singa-
pore 911833 (SG).

(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,

(54) Title: METHOD AND ARCHITECTURE FOR SECURING AND MANAGING NETWORKS OF EMBEDDED SYSTEMS
WITH OPTIMISED PUBLIC KEY INFRASTRUCTURE

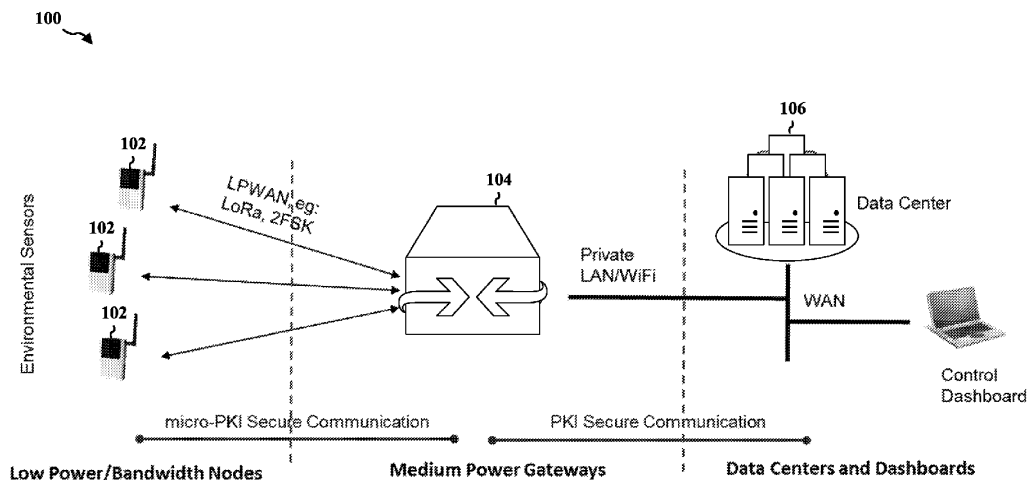


FIG. 1

(57) Abstract: Methods and apparatuses for data communication and cybersecurity are provided. An optimized way is built to handle the PKI over constrained devices with application over PAN/LP-WAN and other similar devices and networks. This significantly improves the security capabilities of such devices in terms of identity verification, encrypted communication, and device life-cycle management. The apparatus may authenticate a party of a data communication session using a micro certificate within a micro public key infrastructure that provides transport or application layer security. The micro public key infrastructure may be the combination of communication protocol, micro certificates, and a management platform. The apparatus may establish the data communication session using the micro certificate. The apparatus may perform secured data communication over the data communication session.

[Continued on next page]

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