

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. November 2022 (10.11.2022)



(10) Internationale Veröffentlichungsnummer
WO 2022/233806 A1

(51) Internationale Patentklassifikation:

H04L 9/32 (2006.01) *H04W 4/70* (2018.01)
H04L 9/40 (2022.01) *H04W 12/06* (2021.01)

(21) Internationales Aktenzeichen: PCT/EP2022/061746

(22) Internationales Anmeldedatum:
03. Mai 2022 (03.05.2022)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2021 111 841.7
06. Mai 2021 (06.05.2021) DE

(71) Anmelder: **PERINET GMBH** [DE/DE]; Rudower Chaus-
see 29, 12489 Berlin (DE).

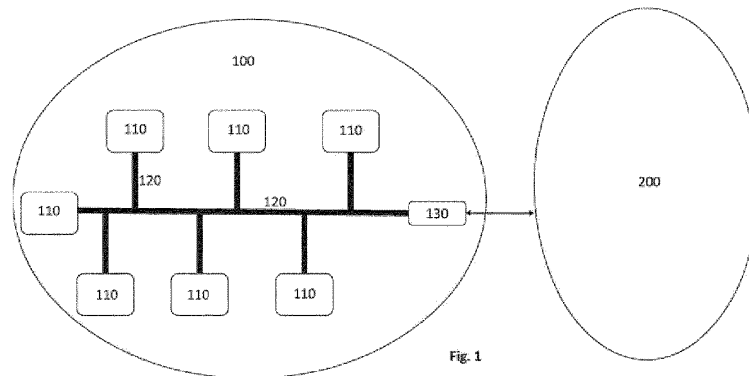
(72) Erfinder: **WALTHER, Karsten**; Dr.-Hans-Bredow-Stra-
ße 4, 15711 Königs Wusterhausen (DE).

(74) Anwalt: **EISENFÜHR SPEISER PATENTANWÄLTE
RECHTSANWÄLTE PARTGMBB** et al.; Postfach 10 60
78, 28060 Bremen (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): 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, IQ, IR, IS, IT, JM, 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,

(54) Title: COMMUNICATION METHOD FOR IOT NODES OR IOT DEVICES IN A LOCAL NETWORK

(54) Bezeichnung: VERFAHREN ZUR KOMMUNIKATION VON IOT KNOTEN ODER IOT GERÄTEN IN EINEM LOKALEN
NETZWERK



(57) **Abstract:** The invention relates to a communication method for IoT nodes (110) in a local network (100) which is connected to the Internet (200) solely via a computer (130). The local network (100) has an ethernet network or a single pair ethernet network. The IoT node is designed to be display-free and operating element-free and has a first interface for a communication with other IoT nodes in the local network (120). Each IoT node has a first public key and a first private key. The first private key is stored in advance or is generated by the IoT node itself. IoT nodes are authenticated by the process of transmitting a request for a root certificate to a root certificate server (210) by means of the computer, said root certificate server having at least one root certificate of the manufacturer of the IoT nodes, receiving and storing the root certificate, and checking whether the IoT nodes are original and unmodified devices using the received root certificate. The root certificate (Z) links the first public key of the IoT nodes to unique address information of the IoT node, said address information being valid solely in the local network. The computer checks whether the public key of the IoT node is signed by the manufacturer of the IoT node using the stored root certificate (Z), and the first key is checked on the basis of a cryptographic method.

(57) **Zusammenfassung:** Es wird ein Verfahren zur Kommunikation von IoT Knoten (110) in einem lokalen Netzwerk (100) vorgese-
hen, das nur über einen Computer (130) mit dem Internet (200) verbunden ist. Das lokale Netzwerk (100) weist ein Ethernet-Netzwerk
oder ein Single Pair Ethernet-Netzwerk auf. Der IoT Knoten ist Display-los und Bedienungselemente-frei ausgestaltet und weist eine
erste Schnittstelle zur Kommunikation in dem lokalen Netzwerk (120) mit anderen IoT Knoten auf. Jeder IoT Knoten weist einen ersten

[Fortsetzung auf der nächsten Seite]

WO 2022/233806 A1

SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, WS, ZA, ZM, ZW.

- (84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (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).

Veröffentlicht:

- mit internationalem Recherchenbericht (Artikel 21 Absatz 3)
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)

öffentlichen und einen ersten privaten Schlüssel auf. Der erste private Schlüssel ist vorab abgelegt oder von dem IoT Knoten selber erzeugt. Eine Authentifizierung von IoT Knoten erfolgt durch Senden einer Anfrage nach einem Root-Zertifikat durch den Computer an einen Root-Zertifikat-Server (210), der mindestens ein Root-Zertifikat eines Herstellers der IoT Knoten aufweist, durch Empfangen und Speichern des Root-Zertifikats und durch Überprüfen anhand des empfangenen Root-Zertifikat, ob die IoT Knoten originale und unveränderte Geräte sind. Das Root-Zertifikat (Z) verknüpft den ersten öffentlichen Schlüssel der IoT Knoten mit einer eindeutigen ausschließlich im lokalen Netz gültigen Adressinformation des IoT Knotens. Der Computer überprüft anhand des gespeicherten Root-Zertifikats (Z), ob der öffentliche Schlüssel des IoT Knotens durch den Hersteller des IoT Knotens signiert ist. Der erste Schlüssel wird basierend auf einem kryptografischen Verfahren überprüft.