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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2025 (19.06.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/124748 A1

(51) International Patent Classification:
H04L 9/40 (2022.01) *G01D 4/00* (2006.01)
H04L 67/12 (2022.01) *H04L 67/56* (2022.01)
H04Q 9/00 (2006.01)

(21) International Application Number:
PCT/EP2024/062291

(22) International Filing Date:
03 May 2024 (03.05.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10 2023 135 321.7
15 December 2023 (15.12.2023) DE

(71) Applicant: **MARCHL METERING GMBH** [DE/DE]; Buchenstraße 18, 93426 Roding (DE).

(72) Inventor: **MARCHL, Julian F.**; Am Steinriegel 6, 93426 Roding (DE).

(74) Agent: **KEHL, ASCHERL, LIEBHOFF & ETTMAYR PATENTANWÄLTE * PARTNERSCHAFT MBB**; Emil-Riedel-Str. 18, 80538 Munich (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, CV, 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, MG, MK, MN, MU, 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.

WO 2025/124748 A1

(54) Title: COMMUNICATION SYSTEM

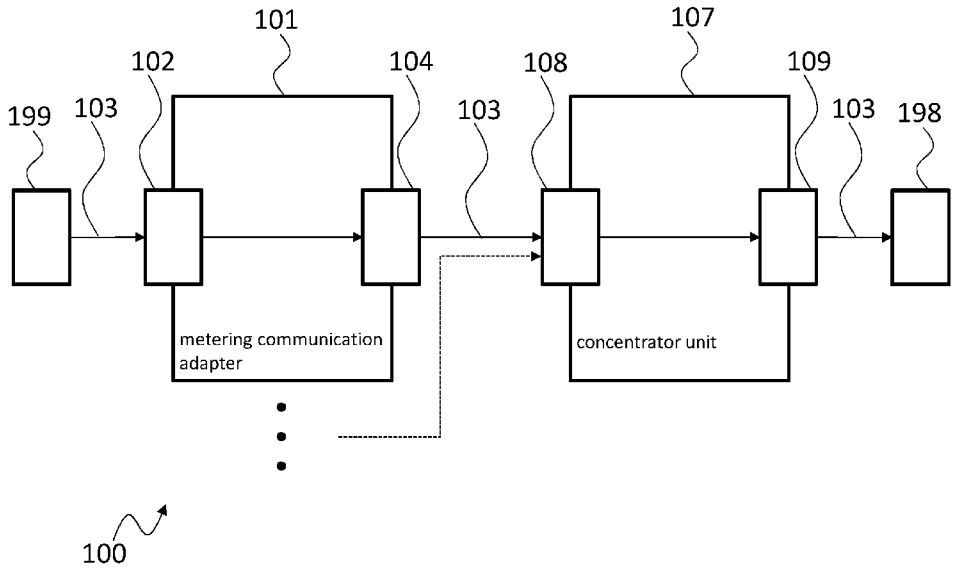


Fig. 1

(57) Abstract: The present disclosure provides a communication system comprising at least one metering communication adapter, the metering communication adapter comprising a local meter interface configured to communicatively couple to a metering element, and to receive metering data from the metering element, and comprising a first communication interface configured to output the metering data received from the metering element, and a concentrator unit comprising a second communication interface configured to receive the metering data output by the at least one metering communication adapter, and comprising a local interface configured to output the received metering data.

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))*
— *with amended claims (Art. 19(1))*

COMMUNICATION SYSTEM

TECHNICAL FIELD

[0001] The disclosure relates to a communication system.

BACKGROUND

[0002] Although applicable to any type of metering system, the present disclosure will mainly be described in conjunction with electrical power metering devices.

[0003] Electrical power consumption of electrical installations in industrial or residential buildings may be measured or metered locally and may then be documented by employees of electricity providers.

[0004] Alternatively, the local power meters may transmit the measured power consumption to a central server electronically via a respective network connection. However, such electronic data transmission makes strong security measures mandatory to prevent data falsification during the transmission of the measured power consumption to the central server.

[0005] Such communication networks are consequently difficult to set up.

[0006] Accordingly, there is a need for an improved metering system.

SUMMARY

[0007] The above-stated problem is solved by the features of the independent claims. It is understood, that independent claims of a claim category may be formed in analogy to the dependent claims of another claim category.

[0008] Accordingly, it is provided:

[0009] A communication system comprising at least one metering communication adapter, the metering communication adapter comprising a local meter interface configured to communicatively couple to a metering element, and to receive metering

data from the metering element, and comprising a first communication interface configured to output the metering data received from the metering element, and a concentrator unit comprising a second communication interface configured to receive the metering data output by the at least one metering communication adapter, and comprising a local interface configured to output the received metering data.

[0010] Further, it is provided:

[0011] A data communication method comprising receiving metering data from at least one metering element via a local meter interface, outputting the metering data received from the metering element via a first communication interface, receiving the metering data with a second communication interface, and outputting the received metering data via a local interface.

[0012] Further, it is provided:

[0013] A non-transitory data carrier comprising instructions that when executed by a processor, especially a processor of a metering communication adapter in a communication system according to the present disclosure, cause the processor to perform the functions of the metering communication adapter.

[0014] Further, it is provided:

[0015] A non-transitory data carrier comprising instructions that when executed by a processor, especially a processor of a concentrator unit in a communication system according to the present disclosure, cause the processor to perform the functions of the concentrator unit.

[0016] The present disclosure is based on the finding that local legal requirements may force electricity providers to install a secure communication device locally at every single power meter. For example, the German legal requirements require a so-called smart meter gateway, SMGw, to be installed at every single power meter (so-called mME, moderne Messeinrichtung) if the power meter readings are to be transmitted electronically to the electricity providers, e.g., for performing the invoicing. However, installing a single SMGw for every power meter increases the costs for the electricity providers. Such costs may not always be passed on to the customers.

[0017] German regulations regarding SMGws are, for example, provided in the standard document “Smart Meter Gateway PTB-A 50.8”.

[0018] The BSI guidelines are specified for smart meter gateways (SMGw) as the central interface to the Internet. (BSI TR-03109[-1])

[0019] Further, mMEs send data telegrams with values for instantaneous power, energy consumption, etc. at periodic intervals via a serial interface. Two interfaces are specified for this purpose: The INFO-DSS, which is accessible to the end customer (consumer), and the MSB-DSS. The MSB-DSS also serves as a configuration interface for configuring the mME. This interface is not specified for all manufacturers, meaning that a separate communication adapter is required for each meter type in order to be able to communicate with the mME. The INFO-DSS, on the other hand, is standardized across manufacturers and is always implemented on the front of the device, for example.

[0020] Currently, only the MSB interface is used for billing by the metering point operator, as the data provided by the mME in this way is already encrypted. In order to be able to transmit the data to an SMGw or another radio base station, the data transmitted by the interface of the mME must be translated into an LMN-compatible protocol in a so-called communication adapter. This communication adapter is specified in [PTB-A 50.8 of December 2014] and thus enables the connection of an mME to a local LMN. This means, for example, that all mMEs in an apartment building can be connected wirelessly to an SMGw. However, due to the short range of an LMN-compatible radio standard (e.g. 10m for wM-Bus), the number of mMEs that can be connected to an SMGw is severely limited. This means that e.g., only all mMEs on one floor can be connected to one SMGw.

[0021] However, since the connection and installation costs of an SMGw (or a radio base station in general) are very high, it should be possible to connect as many mMEs as possible to an SMGw in order to keep the costs for operation and meter reading low. However, this is not possible with the current technology.

[0022] The present disclosure, therefore, provides the communication system that may serve as a kind of intermediary between multiple power meters and a single SMGw.

[0023] To this end, the communication system comprises at least one, especially multiple, metering communication adapters that communicate with a single concentrator unit.

[0024] Each one of the metering communication adapters comprises a local meter interface. The local meter interface serves for communicatively coupling the respective metering communication adapter to a metering element. The metering element may be any kind of metering element, for example, a power meter. Other meters, like water meters or heat meters, are also possible.

[0025] In addition, each one of the metering communication adapters comprises a first communication interface that communicatively couples the metering communication adapters to the concentrator unit that comprises a respective second communication interface.

[0026] The number of metering communication adapters supported by the communication system is only limited by the capacity of the concentrator unit and the SMGw, and the communication interface between the single metering communication adapters, and the concentrator unit.

[0027] During the operation of the communication system, the metering communication adapters each receive metering data from the respective metering element via the local meter interface. The metering communication adapters then transmit the received metering data via their first communication interface to the concentrator unit.

[0028] The metering communication adapters may serve as a so-called “measurement system component communication adapter” (“Messsystemkomponente Kommunikationsadapter” as described in chapter 6 of the standard document “Smart Meter Gateway PTB-A 50.8” of December 2014. The metering communication adapters may, consequently, be registered in respective smart meter gateways as communication adapters prior to transmitting the metering data.

[0029] A single concentrator unit may receive the metering data from a plurality of metering communication adapters. Via the local interface, the concentrator unit may then provide the acquired metering data from the plurality of metering communication adapters to a single receiver, e.g., an SMGw.

[0030] Consequently, instead of installing a plurality of smart meter gateways, the electricity provider may install a single smart meter gateway for a plurality of power meters and use the communication system according to the present disclosure for coupling multiple power meters to a single smart meter gateway.

[0031] The communication between the metering communication adapters, and the concentrator unit is transparent to the metering element, and the receiver of the metering data e.g., the SMGw. In such a case, the communication system may be seen as a kind of range extension and accumulator for a local communication between the metering element and the SMG.

[0032] The communication system according to the present disclosure may be used to bridge large distances in the so called local metrological network, LMN, according to standard document “Smart Meter Gateway PTB-A 50.8” (also according to BSI TR03109-1 S. 49: Optionales unidirektionales Protokoll mit Crypto).

[0033] Further embodiments of the present disclosure are subject of the further dependent claims and of the following description, referring to the drawings.

[0034] It is a task of the present disclosure, as described above, to realize a communication adapter, herein called the communication system, especially by means of long-range radio in order to increase the radio range of mME and other meters and to drastically increase the number of mME per SMGw and thus reduce the costs of connection and installation to a minimum.

[0035] The aforementioned task is solved according to the disclosure by a communication adapter, also called the metering communication adapter herein, in particular for the smart connection of consumption meters by means of long-range radio, in particular LoRaWAN and mioty.

[0036] The invention comprises a communication adapter, in particular for the smart connection of consumption meters, also called metering units herein, by means of long-range radio, in particular LoRaWAN and mioty, wherein the range of the communication link between base station, also called concentrator unit herein, in particular with SMGw, and a consumption meter or smart meter (mME), also called metering unit herein, is increased by securely connecting a communication adapter

for consumption meters, in particular according to PTB, by means of long-range radio with network protocol.

[0037] This solution is particularly advantageous in that the communication adapter or system according to the invention increases the radio range of mME and other meters and drastically increases the number of mME per SMGw and minimizes the costs of connection and installation.

[0038] According to an embodiment of the present disclosure, a communication adapter or system is provided, wherein it is separated into two physical parts, meter side, also called metering communication adapter, and SMGw (LMN-side) or base station side, also called concentrator unit, and the security of the network protocol is improved by using an inner end-to-end encryption or signature in addition to the outer transport encryption.

[0039] According to a further embodiment of the present disclosure, the communication adapter or system is provided, wherein only the register values and not the register identifiers of a data telegram can be encrypted or signed in the internal encryption or signature in order to generate a compact and easily analyzable data telegram with undiminished security.

[0040] Furthermore, according to one embodiment of the present disclosure, the communication adapter or system is provided, whereby the communication adapter fulfills the functionality of a sub-metering and control unit, in particular according to BSI regulations, so that in addition to consumption meters, any other device can also be connected.

[0041] In order to make a rollout as flexible as possible, it should also be possible to use the INFO-DSS for the communication adapter in order to provide a manufacturer-independent solution. However, the data must be transmitted in encrypted form, which is another innovation.

[0042] Further embodiments of the present disclosure are subject of the further dependent claims and of the following description, referring to the drawings.

[0043] In the following, the dependent claims referring directly or indirectly to claim 1 are described in more detail. For the avoidance of doubt, the features of the

dependent claims relating to independent claim 1 can be combined in all variations with each other and the disclosure of the description is not limited to the claim dependencies as specified in the claim set. Further, the features of the dependent claims referring to independent claim 1 may be combined with any of the features of the other independent claims or the dependent claims relating to any one of the other independent claims. In a respective method, respective method steps may perform the function of the respective apparatus elements, and in a respective apparatus, respective apparatus elements may perform the respective method steps.

[0044] In an embodiment, which can be combined with all other embodiments mentioned above or below, the local meter interface may comprise at least one of an optical interface, an infrared optical interface, a character-based optical interface, a reed-switch-based interface, a wired interface, and a wireless interface.

[0045] A metering element may comprise at least one of multiple possible types of interfaces.

[0046] The local meter interface may comprise any adequate type of optical, wired or wireless interface for receiving the metering data from the metering element. An optical interface may comprise any visible or non-visible light data transmission interface, like an infrared interface.

[0047] Another type of optical interface may comprise a character-based optical interface. Such an interface may comprise a camera that acquires an image of a character-based metering data indicator of the metering element. The character-based optical interface may comprise an OCR function to convert the metering data provided in the image into digital data to be transferred to the concentrator unit.

[0048] A reed-switch-based interface may comprise a reed-switch that is cyclically closed by a magnet that is provided by the metering element or an electrical contact which is cyclically closed by another mechanical provision.

[0049] Other types of interface for coupling the metering communication adapters to the metering elements may comprise wired or wireless data interfaces.

[0050] In embodiments, the local meter interface may be adapted to communicatively couple to a metering element via a so-called INFO-DSS interface or via a so-

called MSB-DSS interface. The INFO-DSS interface, and the MSB-DSS interface in this context refer to protocol level interfaces. While they may use an infrared physical interface, any other physical interface may also be used.

[0051] The INFO-DSS interface is used by the metering element to periodically output a respective meter reading or respective metering data. The MSB-DSS interface may periodically output the same data, but may also be used to provide configuration data to the metering element.

[0052] While the INFO-DSS interface is a standardized interface (e.g., according to VDE FNN Lastenheft Basiszähler; and alos in: VDE FNN Lastenheft EDL: Elektronische Haushaltszähler: Funktionale Merkmale und Protokolle), the physical design MSB-DSS interface is not standardized. Every manufacturer of metering elements may define a respective MSB-DSS interface (e.g., an Ethernet port, wire terminals, etc.). As indicated above, the local meter interface may be adapted to communicate via any of such vendor-defined MSB-DSS interfaces.

[0053] In embodiments, the local meter interface may comprise multiple different physical interfaces. The local meter interface may e.g., comprise the main metering interface for reading or acquiring the metering data from a metering element. The local meter interface may comprise further interfaces, also called sub-metering interface, for acquiring data from other elements, also called sub-metering units.

[0054] The main metering interface may serve e.g., for acquiring the metering data from power meters, water meters, gas meters, and the like. The sub-metering interface may serve to acquire data from sub-ordinate metering elements, like power meters or heat meters in single apartments of a building.

[0055] In a further embodiment, which can be combined with all other embodiments mentioned above or below, the first communication interface and the second communication interface may comprise one of a wired data interface, a wireless data interface, a LoRaWAN interface, a mioty interface, a wireless sub-GHz interface, a WiFi interface, and a Bluetooth interface.

[0056] The first communication interface, and the second communication interface both server to bridge larger distances between the multiple metering communication adapters and the final receiver of the metering data e.g., a smart meter gateway.

[0057] While any type of physical interface may be used for the first communication interface, and the second communication interface, in embodiments, a wireless sub-GHz interface, like a LoRaWAN or a mioty interface, may be used to provide a low power consumption interface that may bridge large distances with minimal installation effort.

[0058] In another further embodiment, which can be combined with all other embodiments mentioned above or below, at least one metering communication adapter may further comprise a first cryptographic module coupled between the local meter interface and the first communication interface, wherein the first cryptographic module may be configured to cryptographically encrypt the received metering data and provide the cryptographically encrypted metering data to the first communication interface for transmission to the concentrator unit.

[0059] The metering data provided by the metering element may already be encrypted. This may e.g., be the case for the above-mentioned MSB-DSS interface, while the INFO-DSS interface may (but necessarily needs to) provide the metering data in an unencrypted form.

[0060] Improved security of the data transmission may especially be required if an interface, like the MSB-DSS interface, is also used for configuring the metering element. Further, such an improved security of the data transmission may also be required according to local legislation. In Germany, such an improved security is e.g., required according to the standard documents “PTB-A 50.8” from December 2014 and the “BSI TR-03109 series”.

[0061] If an improved security is required for the data transmission, the metering communication adapters may be provided with the first cryptographic module. The first cryptographic module may receive the metering data from the local meter interface, cryptographically encrypt the received metering data, and provide the encrypted

metering data back to the local meter interface or to the first communication interface for transmission to the concentrator unit.

[0062] It is understood, that the encryption may be performed such that a receiver of the encrypted metering data, that not necessarily needs to be the concentrator unit, may decrypt the metering data for further processing. The first cryptographic module may e.g., be configured to cryptographically encrypt the metering data such that only receiver that is provided with the metering data by the concentrator unit may decrypt the cryptographically encrypted metering data. The concentrator unit in such embodiments has no access to the cryptographically encrypted metering data.

[0063] The first cryptographic module may comprise any kind of adequate element, like module in a processor or controller that is already present in the local meter interface.

[0064] In a further embodiment, which can be combined with all other embodiments mentioned above or below, the local meter interface may be configured to receive data packages comprising meta data and measurement data, and the first cryptographic module may be configured to at least one of perform a single encryption of the measurement data and the meta data, or perform a first encryption of the measurement data, and a second encryption of the encrypted measurement data and the meta data.

[0065] The term “meta data” may refer to any data that allows to identify the nature of the measurement data, the source of the measurement data, or any other information regarding the measurement data. The term “measurement data”, in contrast, refers to the actual value measured by the metering element.

[0066] In embodiments, the measurement data in the data package may already be encrypted by the respective metering element. In such cases, no further encryption of the metering data is required.

[0067] In other cases, the metering data may be provided in an unencrypted form. In such embodiments, the first cryptographic module may first encrypt the measurement data, and then encrypt the encrypted measurement data together with the meta data.

[0068] In embodiments with double encryption, the fully encrypted data package may be decrypted in the receiver to retrieve the meta data. At the same time, the content of the measurement data will still be encrypted. This allows analyzing the meta data and processing the data package accordingly, without allowing the measurement data to be accessed. The meta data may e.g., allow to identify the nature of the measurement data, and to store the measurement data accordingly. For example, the meta data may identify the measurement data as power measurement of a specific power metering element. The respectively encrypted measurement data may then be stored accordingly in encrypted form.

[0069] The data e.g., keys, for decrypting the measurement data may e.g., only be available to respectively authorized entities.

[0070] In another further embodiment, which can be combined with all other embodiments mentioned above or below, the concentrator unit may further comprise a second cryptographic module coupled between the second communication interface and the local interface, wherein the second cryptographic module may be configured to cryptographically decrypt the received metering data and provide the cryptographically decrypted metering data to the local interface.

[0071] As explained above, improved security of the data transmission of the metering data may be required in applications. This requirement may in embodiments apply to the transmission of data between the metering communication adapters and the concentrator unit.

[0072] In such embodiments, the concentrator unit may comprise a second cryptographic module. The explanations provided above for the first cryptographic module apply mutatis mutandis to the second cryptographic module. The second cryptographic module may comprise any kind of adequate element, like a module in a processor or controller that is already present in the local meter interface.

[0073] If the first cryptographic module cryptographically encrypts the metering data such that the second cryptographic module may decrypt the cryptographically encrypted metering data, a kind of secure tunnel may be established between the metering communication adapters and the concentrator unit. If the metering data is

already cryptographically encrypted a first or inner encryption is present. The encryption performed by the first cryptographic module may be seen as a second or outer encryption in such embodiments.

[0074] In case of the first communication interface, and the second communication interface being provided as LoRaWAN interfaces, the encryption may be performed according to the LoRaWAN standard.

[0075] The first cryptographic module, and the second cryptographic module may perform any type of adequate encryption and decryption. Possible cryptographic algorithms comprise, but are not limited to, symmetrical cryptographic algorithms, like AES (Advanced Encryption Standard) algorithms, or asymmetric cryptographic algorithms, like a public/private key algorithm.

[0076] In a further embodiment, which can be combined with all other embodiments mentioned above or below, the second communication interface may be configured to receive data packages comprising measurement data encrypted with a first encryption, and meta data with the encrypted measurement data encrypted with a second encryption, wherein the second cryptographic module may be configured to at least one of perform a single decryption of the encrypted measurement data and the meta data, or perform a first decryption of the encrypted measurement data and the meta data, and a second decryption of the encrypted measurement data.

[0077] As explained above, the first cryptographic module may perform a single or double encryption. The second cryptographic module may be adapted to decrypt the single encryption, or the double encryption accordingly. The specific configuration of the second cryptographic module may depend on legislative requirements, or the requirements of the respective application.

[0078] Generally, the first encryption may e.g., comprise a AES-CMAC and -CBC authentication and encryption, or an ECC192 signature in conformance with BSI TR-03116-3 from December 2022.

[0079] In another further embodiment, which can be combined with all other embodiments mentioned above or below, the local meter interface, the first communication interface, the second communication interface, and the local interface may comprise bi-directional interfaces, wherein the local interface may configured to receive

configuration and control data and to provide the configuration and control data to the second communication interface, wherein the second communication interface may be configured to transmit the received configuration and control data to the first communication interface, wherein the first communication interface may be configured to transmit the received configuration and control data to the local meter interface, and wherein the local meter interface may be configured to output the received configuration and control data.

[0080] As explained above, different kinds of local meter interfaces are possible, while at least some of these local meter interfaces may allow bi-directional data communication between the metering communication adapter, and the metering element.

[0081] With such local meter interfaces, a data path from the concentrator unit to the single metering communication adapters may be provided by allowing the first communication interface, the second communication interface, the local meter interface, and the local interface to perform a bi-directional data communication.

[0082] This will allow e.g., a smart meter gateway coupled to the local interface to provide data e.g., the configuration or control data, to one of the metering elements or a group of metering elements.

[0083] The term configuration and control data in this regard refers to any type of data that may be provided from a sender e.g., the smart meter gateway, to the metering element. Such data may, but not necessarily needs to, refer to configuration of the metering element, or control of the metering element.

[0084] In embodiments with bidirectional data communication, the communication system according to the present disclosure may also be used to bridge large distances in the so-called home area network, HAN, according to standard document “PTB-A 50.8” or “BSI TR-03109-1”. Such a HAN may be used to control consumers e.g., electrical power consumers, like charging units for electric vehicles. Such consumers may also be called a controllable local system, CLS.

[0085] In a further embodiment, which can be combined with all other embodiments mentioned above or below, the second cryptographic module may be configured to cryptographically encode the configuration and control data, and to provide

the cryptographically encoded configuration and control data to the second communication interface, and the second communication interface may be configured to transmit the cryptographically encoded configuration and control data to the first communication interface.

[0086] As explained above, for the transmission of the metering data, the configuration and control data may also be transmitted cryptographically encrypted.

[0087] To this end, the second cryptographic module in the concentrator unit may be adapted to cryptographically encrypt the configuration and control data prior to transmission of the configuration and control data to the respective metering communication adapter.

[0088] In an embodiment, which can be combined with all other embodiments mentioned above or below, the first cryptographic module may be configured to cryptographically decode the received configuration and control data and to provide the cryptographically decoded configuration and control data to the local meter interface, and the local meter interface may be configured to output the cryptographically decoded configuration and control data.

[0089] In embodiments, the cryptographically encrypted configuration and control data may be decrypted by the metering element. However, in embodiments, the metering communication adapters may decrypt the cryptographically encrypted configuration and control data, and provide the originally, un-encrypted configuration and control data to the metering element.

[0090] In another further embodiment, which can be combined with all other embodiments mentioned above or below, at least one metering communication adapter may comprise a first module comprising the local meter interface and a first coupling interface coupled to the local meter interface, and a second module comprising a second coupling interface coupled to the first communication interface, wherein the first coupling interface may be configured to couple to the second coupling interface.

[0091] The metering communication adapters may be provided as modular units. Such metering communication adapters may comprise the first module that may be individually provided for specific types of metering elements. The second module, in contrast, may be a general module that may be used in all metering communication

adapters as a platform or base for accommodating the different possible first modules.

[0092] In the first module the local meter interface may be, directly or indirectly, coupled to the first coupling interface. The first coupling interface may be an electrical interface implemented with a respective connector. Of course, further mechanical means for fixing the first module to the second module may be provided. The first coupling interface may also serve to receive electrical supply power to power any of the elements provided on the first module.

[0093] The second module, as the base or carrier of the first module, comprises the second coupling interface. The second coupling interface may form the counterpart for the first coupling interface and provide a respective, direct or indirect, electrical connection from the second coupling interface to the first communication interface.

[0094] The term direct connection in this regard refers to the connection comprising no further elements than the respective electrical traces or connections. An indirect coupling refers to any other element being provided between the two endpoints of the connection.

[0095] In an embodiment, the first module may e.g., only comprise a respective interfacing element of the local meter interface, like an IR receiver, that may be directly coupled to the first coupling interface. Any other element required to drive the interfacing element and acquire data with the interfacing element may be provided on the second module. In other embodiments, at least a data decoding element may be provided on the first module with the interfacing element, and the data decoding element may decode the raw data received by the interfacing element, and provide a respective digital data package or stream to the second module.

[0096] In a further embodiment, which can be combined with all other embodiments mentioned above or below, the first cryptographic module may be arranged between the local meter interface, and the first coupling interface, or between the second coupling interface, and the first communication interface.

[0097] In embodiments, the first cryptographic module may be provided on the first module in order to cryptographically encrypt the metering data as soon as possible in the signal chain. In other embodiments, the first cryptographic module may be provided on the second module in order to reduce the complexity of the first module.

[0098] In an embodiment, which can be combined with all other embodiments mentioned above or below, the local interface may comprises a wired communication interface, especially an Ethernet-based communication interface.

[0099] The concentrator unit may be provided local to the receiver of the metering data. Especially in such embodiments, the local interface of the concentrator unit may comprise a wired interface, like an Ethernet-based communication interface. Such a wired interface allows for a simple connection of the concentrator unit to the receiving unit that does not leak any data, like a wireless interface.

[0100] The local interface may also comprise a wireless interface, especially a cellular network wireless interface, and the local interface may be configured to output the metering data to a remote receiver.

[0101] In further embodiments, the local interface may comprise a wireless interface. The wireless interface may serve for communication with the SMGw, or for transmitting the metering data to other receivers than the above-mentioned SMGw.

[0102] The wireless interface may e.g., comprise a GSM-based interface, a UMTS-based interface, an LTE-based interface, or any other cellular communication standard-based interface.

[0103] This allows transmitting the metering data to any receiver as required by the respective application.

[0104] It is understood, that in embodiments, the local interface may comprise multiple different types of interfaces, like the wired and the wireless interface, or multiple wired, and multiple wireless interfaces.

[0105] In an embodiment, which can be combined with all other embodiments mentioned above or below, the local interface may be configured to output the metering data to a local smart meter gateway.

[0106] Smart meter gateways, especially according to standard document “PTB-A 50.8” and “BSI TR-03109”, are required to communicate according to a predefined standard. The predefined standard as shown in chapter 3.3.5 of the standard document “PTB-A 50.8”, requires the SMGw to communicate via an EIA/RS 485 bidirectional physical interface, and/or via a wireless MBUS Mode (C), T unidirectional physical interface.

[0107] Therefore, the local interface of the concentrator unit may be adapted to support all required functions of the respective communication standard.

[0108] The metering communication adapters and the concentrator unit described herein may be implemented by any adequate combination of processors, interface controllers, sensors, actors and the like.

[0109] A respective processor may perform control of the single elements, and may comprise or integrate at least some of the elements. For example, such a processor may be provided as a microcontroller that comprises a respective processing core that is coupled to a respective local meter interface e.g., a IR sensor, and a respective first communication interface. The IR sensor may be directly coupled to such a microcontroller, and the microcontroller may decode the signals received via the IR sensor. A respective LoRaWAN interface may be provided as first communication interface. Such a LoRaWAN interface may be coupled to the microcontroller e.g., via a SPI-Bus interface. The microcontroller may also comprise a TPM or any other adequate module that may perform the function of the first cryptographic module.

[0110] Generally, a respective processor may comprise or may be provided in or as part of at least one of a dedicated processing element e.g., a processing unit, a microcontroller, a field programmable gate array, FPGA, a complex programmable logic device, CPLD, an application specific integrated circuit, ASIC, or the like. A respective program or configuration may be provided to implement the required functionality. The processor may at least in part also be provided as a non-transitory computer program product comprising computer readable instructions that may be executed by a processing element. In a further embodiment, the processor may be provided as an addition or additional function or method to the firmware or operating system of a processing element that is already present in the respective application as respective computer readable instructions. Such computer readable instructions

may be stored in a memory that is coupled to or integrated into the processing element. The processing element may load the computer readable instructions from the memory and execute them.

[0111] In addition, it is understood, that any required supporting or additional hardware may be provided like e.g., a power supply circuitry and clock generation circuitry.

[0112] Generally, any computer program or computer program product disclosed herein is to be understood as a non-transitory computer program product.

[0113] The above-provided explanations regarding the processor also apply mutatis mutandis to the concentrator unit.

BRIEF DESCRIPTION OF THE DRAWINGS

[0114] For a more complete understanding of the present disclosure and advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings. The disclosure is explained in more detail below using exemplary embodiments which are specified in the schematic figures of the drawings, in which:

[0115] Figure 1 shows a block diagram of an embodiment of a communication system according to the present disclosure;

[0116] Figure 2 shows a block diagram of an embodiment of a metering communication adapter according to the present disclosure;

[0117] Figure 3 shows a block diagram of an embodiment of a concentrator unit according to the present disclosure;

[0118] Figure 4 shows a block diagram of another embodiment of a metering communication adapter according to the present disclosure;

[0119] Figure 5 shows a block diagram of an embodiment of a second module for use in a metering communication adapter according to the present disclosure;

[0120] Figure 6 shows a block diagram of an embodiment of a first module for use in a metering communication adapter according to the present disclosure;

[0121] Figure 7 shows a block diagram of another embodiment of a metering communication adapter according to the present disclosure;

[0122] Figure 8 shows a block diagram of another embodiment of a metering communication adapter according to the present disclosure;

[0123] Figure 9 shows a block diagram of another embodiment of a second module for use in a metering communication adapter according to the present disclosure;

[0124] Figure 10 shows a block diagram of another embodiment of a second module for use in a metering communication adapter according to the present disclosure;

[0125] Figure 11 shows a block diagram of another embodiment of a concentrator unit according to the present disclosure;

[0126] Figure 12 shows a flow diagram of an embodiment of a method according to the present disclosure;

[0127] Figure 13 shows a flow diagram of another embodiment of a method according to the present disclosure;

[0128] Figure 14 shows a block diagram of an embodiment of possible data packets for use with the subject of the present disclosure; and

[0129] Figure 15 shows a flow diagram of another embodiment of a method according to the present disclosure.

[0130] In the figures like reference signs denote like elements unless stated otherwise.

DETAILED DESCRIPTION OF THE DRAWINGS

[0131] Figure 1 shows a block diagram of a communication system 100. The communication system 100 comprises a metering communication adapter 101, while more metering communication adapters are hinted at by three dots. The metering communication adapter 101 comprises a local meter interface 102 for communicatively coupling to a metering element 199, and receiving metering data 103 from the metering element 199. The metering communication adapter 101 further comprises a

first communication interface 104 for outputting the metering data 103. The communication system 100 further comprises a concentrator unit 107 comprising a second communication interface 108 for receiving the metering data 103 output by the metering communication adapter 101. Further, the concentrator unit 107 comprises a local interface 109 for output the received metering data 103 e.g., to a smart meter gateway 198. The explanations provided herein for any embodiment of the communication system apply mutatis mutandis to communication system 100.

[0132] In order to allow to couple the metering communication adapter 101 to a plurality of different metering elements 199, the local meter interface 102 may comprise at least one of an optical interface, especially an infrared optical interface, or a character-based optical interface, a reed-switch-based interface, a wired interface, and a wireless interface.

[0133] Further, in order to allow adapting the communication system 100 to different application requirements the first communication interface 104 and the second communication interface 108 may comprise at least one of a wired data interface, a wireless data interface, especially a wireless sub-GHz interface, more especially a LoRaWAN interface, or a mioty interface, a WiFi interface, and a Bluetooth interface.

[0134] The local interface109 may comprise any type of interface adequate for communicating with a receiving device 198 e.g., a smart meter gateway. Such an interface may comprise any type of interface as described above for the local meter interface 102, the first communication interface 104, and the second communication interface 108.

[0135] It is understood, that each one of the local meter interface 102, the first communication interface 104, the second communication interface 108, and the local interface109 may comprise more than a single physical interface, and may support any protocol that is required by a respective application.

[0136] In embodiments, the local meter interface 102, the first communication interface 104, the second communication interface 108, and the local interface 109 may comprise bi-directional interfaces. The local interface 109 may receive configuration and control data and provide the configuration and control data to the second communication interface 108. The second communication interface 108 may transmit

the received configuration and control data to the first communication interface 104. The first communication interface 104 may transmit the received configuration and control data to the local meter interface 102. The local meter interface 102 may output the received configuration and control data e.g., to a metering element 199, or may internally process the configuration and control data especially, if the configuration and control data is destined to the metering communication adapter 101.

[0137] Figure 2 shows a block diagram of a metering communication adapter 201 that may be used e.g., with a communication system 100 as shown in figure 1. The metering communication adapter 201 comprises a local meter interface 202, and a first communication interface 204, as already described with regard to figure 1. The explanations provided herein for any embodiment of the metering communication adapter apply mutatis mutandis to metering communication adapter 201.

[0138] The metering communication adapter 201 further comprises a first cryptographic module 215 coupled between the local meter interface 202 and the first communication interface 204. The first cryptographic module 215 cryptographically encrypts the received metering data 203 and provides the cryptographically encrypted metering data 216 to the first communication interface 204 for transmission to the concentrator unit. In embodiments, although not explicitly shown, a microcontroller or processor may be provided and coupled to the local meter interface 202, and the first communication interface 204. The first cryptographic module 215 may be provided as part of or in such a microcontroller or processor, or may be coupled to such a microcontroller or processor. Further, any supporting elements, like secure key memories may be provided.

[0139] In embodiments, encryption of the configuration and control data may be performed with the first, and second cryptographic modules described herein, or with additional cryptographic modules.

[0140] In figure 2, the local meter interface 202 receives a data package 220 comprising meta data 221-1, 221-2 and measurement data 222-1, 222-2. The data package 220 comprises multiple sets of meta data 221-1, 221-2 with respective measurement data 222-1, 222-2, wherein one to multiple such sets may be provided in a single data package 220.

[0141] The first cryptographic module 215 may perform a single encryption of the measurement data 222-1, 222-2 and the meta data 221-1, 221-2. This will result in a fully encrypted data package 220. Alternatively, the first cryptographic module 215 may perform encryption only of the measurement data 222-1, 222-2 and leave the meta data 221-1, 221-2 unencrypted. This will allow to evaluate the meta data 221-1, 221-2 in the receiver, without a decryption step, and without publishing the actual measurement data 222-1, 222-2.

[0142] In a further alternative, the first cryptographic module 215 may perform a first encryption of the measurement data 222-1, 222-2, and a second encryption of the encrypted measurement data 222-1, 222-2 and the meta data 221-1, 221-2. This provides an additional layer of security during data transmission for the meta data 221-1, 221-2, and still allows evaluating the meta data 221-1, 221-2 in the receiver after a first decryption step without publishing the actual measurement data 222-1, 222-2. Of course, different encryption keys and/or encryption methods may be used for the first encryption and the second encryption.

[0143] Figure 3 shows a block diagram of a concentrator unit 307. The concentrator unit 307 comprises a second communication interface 308 and a local interface 309 as already explained with regard to figure 1. The explanations provided herein for any embodiment of the concentrator unit adapter apply mutatis mutandis to concentrator unit 307.

[0144] Further, the concentrator unit 307 comprises a second cryptographic module 325 that is coupled between the second communication interface 308 and the local interface 309. As in the metering communication adapter 201, in embodiments, although not explicitly shown, a microcontroller or processor may be provided and coupled to the second communication interface 308, and the local interface 309. The second cryptographic module 325 may be provided as part of or in such a microcontroller or processor, or may be coupled to such a microcontroller or processor. Further, any supporting elements, like secure key memories may be provided.

[0145] The second cryptographic module 325 may cryptographically decrypt the received metering data and provide the cryptographically decrypted metering data 303 to the local interface 309.

[0146] The second communication interface 308 may receive data packages comprising measurement data encrypted with a first encryption, and meta data that may optionally be encrypted with a second encryption together with the encrypted measurement data.

[0147] The second cryptographic module 325 may perform a single decryption of the encrypted measurement data and the meta data in order to at least access the meta data. Further, the second cryptographic module 325 may perform an optional first decryption of the encrypted measurement data and the meta data, and a second decryption of the encrypted measurement data in order to also access the measurement data.

[0148] Figure 4 shows a block diagram of another metering communication adapter 401. The metering communication adapter 401 is split in two parts, and comprises a first module 430 that comprises the local meter interface 402 and a first coupling interface 431 coupled to the local meter interface 402. The metering communication adapter 401 further comprises a second module 432 that comprises a second coupling interface 433 coupled to the first communication interface 404.

[0149] The first coupling interface 431 may electrically and, optionally, mechanically couple to the second coupling interface 433 for data transmission and fixation of the first module 430 to the second module 432.

[0150] In the metering communication adapter 401, the first cryptographic module 415 is exemplarily arranged between the second coupling interface 433, and the first communication interface 404. Alternatively, the first cryptographic module 415 may be installed between the local meter interface 402, and the first coupling interface 431. The explanations provided herein for other embodiments of the first cryptographic module apply mutatis mutandis to first cryptographic module 415.

[0151] Figure 5 shows a block diagram of an embodiment of a second module 532, also called base module, for use in a metering communication adapter.

[0152] In order to be able to connect any type of metering element, as many interfaces as possible must be able to be recorded by a reading terminal device e.g., the metering communication adapter as discussed herein. In order to keep product

costs and material consumption low, a modular design may be used for such metering communication adapters, as described herein with regard to the first module (also called interface module), and the second module (also called base module) e.g., with regard to figure 4.

[0153] The base module 532, shown in Fig. 5, comprises a circuit board 535 with several components: A central microcontroller 536 or SoC may comprise, among other things, a secure memory (secure key management) and a LoRaWAN transceiver (this can also be connected to the microcontroller 536 as a separate chip). The microcontroller 536 is powered by a power source 537, like a supply battery or rechargeable battery. In addition, or as alternative, the board 535 may be operated with an external power supply via external power input 538. The microcontroller 536 or a dedicated transceiver (not shown) may be connected to an antenna e.g., of the first communication interface 504.

[0154] The microcontroller 536 provides important interfaces (e.g. UART, digital and analog input) as well as the power supply for the interface module via second coupling interface 533 for the interface module.

[0155] Figure 6 shows a block diagram of a first module 630, also called interface module, for use in a metering communication adapter according to the present disclosure.

[0156] The interface module 630 is shown in Fig. 6 comprises of a circuit board 635 with first coupling interface 631 as counterpart to the second coupling interface 533 of the base module 532. The board may comprise circuits for signal processing e.g. a microcontroller 636 or SoC or DSP, but may also forward an unprocessed signal to the base module. A sensor 602, e.g. an INFO/MSB-DSS IR sensor, a pulse input, a reed switch, a CCD chip/CMOS camera etc. determines a digital signal from a variable to be measured e.g., the metering data 603 (analog: INFO/MSB-DSS on the counter side, pulse output, rotating magnet, counter reading) and transmits this to the signal processing 636 or directly to the base module e.g., via first coupling interface 631.

[0157] The interface module or first module 630 is coupled to the desired interface board and the corresponding housings (separately or together) are firmly connected to each other. The interface module or first module 630 may then be programmed with the appropriate software (e.g. INFO-DSS evaluation or pulse summation) to connect the desired metering element (mME with INFO-DSS or MSB-DSS, gas meter with rotating magnet, etc.) to the base station (also called concentrator unit herein) or transmit metering data from the respective metering element to the concentrator unit.

[0158] The modular terminal device i.e., the metering communication adapter, assembled as discussed in figures 5 and 6, therefore, functions as the "input-side part" of the "measuring system component communication adapter" from Chapter 6 of PTB Guideline PTB-A 50.8 from December 2014. The base station, therefore, represents the "second part" of this communication adapter, i.e. the "interface to the LMN". This communication adapter is thus physically separated into two parts that are securely connected to each other via e.g., a LoRaWAN with internal and external encryption, as explained in more detail below. In this way, the security chain required by the BSI is maintained.

[0159] Figure 7 shows a block diagram of another metering communication adapter 701, also called terminal device, for connecting to smart meters (digital electricity meter / mME) according to the present disclosure, and also illustrates the data flow and system structure for such a terminal device attached to a mME.

[0160] The terminal device 701 is attached to an interface (e.g. INFO- / MSB-DSS) 797 of a modern metering device or mME 799. The mME sends data telegrams 703 at periodic intervals with information on the meter reading, the phase voltages, etc. Such a telegram may contain, for example, the section {"1.8.0": 1257, "2.8.0": 960}, wherein "1.8.0", “2.8.0” my represent meta data, like a register designation, and 1257, 960 may represent actual readings. The sent telegram may be received by the IR receiver 702, also called the local meter interface, of the interface board and is transferred to the encryption module 715. The encrypted telegram is then sent to the base station, also called the concentrator unit, via LoRaWAN using a sub-GHz radio module or interface 704. It should be noted that the PowerTag i.e., the terminal device 701, may transmit several meter data sets in a combined radio telegram or several separate radio telegrams.

[0161] The terminal device can also be attached to the MSB-DSS. In this case, the internal encryption by encryption module 715 can be deactivated, as the user data is already signed on the meter side.

[0162] Analogously, a display of any meter can also be read by camera (CCD or CMOS) in order to obtain the required register values: Here, the terminal device 701 may be attached to the meter reading display 787 of a consumption meter. The consumption meter may show the meter reading via the display. The meter reading is e.g. {"1.8.0": 1257}. The camera 702 of the interface board 701 reads the meter reading and converts the recorded image into a decimal number (i.e. the digitized meter reading shown). The data telegram formed in this way is transferred to the encryption module 715. The encrypted telegram is then sent to the base station via LoRaWAN using a sub-GHz radio module 704. It should be noted that the camera can record several different meter readings (e.g. registers 1.8.0 and 2.8.0) in succession and transmit the end device either in a combined or several separate radio telegrams.

[0163] Similarly, a pulse interface 797 of a meter may also be used to determine metering data. Here, the terminal device 701 may be attached to a pulse interface 797 of a consumption meter. This can be either a pulse-generating element (e.g. a rotating magnet) or a digital pulse output (e.g. reed contact) of a meter, depending on the design of the interface board. The end device receives this pulse signal via an input or a sensor 702 and adds up the number of pulses over a defined time interval. The data telegram formed in this way is transferred to the encryption module 715. The encrypted telegram is then sent to the base station via LoRaWAN using a sub-GHz radio module 704.

[0164] In analogy, any other sensor values may also be sent. The interface board may have a sensor (e.g. temperature, CO2 etc.) 702 and read it out. The data telegram formed in this way is transferred to the encryption module 715. The encrypted telegram is then sent to the base station via LoRaWAN using a sub-GHz radio module 704.

[0165] Figure 8 shows a block diagram of a metering communication adapter 801, also called terminal device 801, according to the present disclosure. The terminal device 801 of figure 8 is integrated directly into a mME.

[0166] As described with regard to figure 7, the terminal device 801 is installed here in a modern metering device. Via an interface 897, the mME transmits data telegrams 803 with information on the meter reading, phase voltages, etc. at periodic intervals. Such a telegram may contain, for example, the section {"1.8.0": 1257, "2.8.0": 960}. The sent telegram is received by the interface 802 of the interface board and transferred to the encryption module 815. The encrypted telegram is then sent to the base station via LoRaWAN using a sub-GHz radio module 804, or first communication interface 804. The explanations, provided with regard to metering communication adapter 701 apply mutatis mutandis also to metering communication adapter 801.

[0167] If the terminal device already receives signed user data (see MSB-DSS) via 897, the internal encryption may be omitted.

[0168] Similar to Figure 7, the terminal device can also be integrated into the meter as shown in Figure 8. Here, the terminal device 801 is physically contained inside the mME 899. Via an internal data interface of the meter 897 (e.g. UART, M-Bus, etc.) the mME transmits data telegrams 803 with information on the meter reading, phase voltages, etc. at periodic intervals. Such a telegram may contain, for example, the section {"1.8.0": 1257, "2.8.0": 960}. The sent telegram is received by the interface 802 of the interface board and transferred to the encryption module 815. The encrypted telegram is then sent to the base station via LoRaWAN using a sub-GHz radio module 804, or first communication interface 804.

[0169] Figure 9 shows a block diagram of another second module 930 for use in a metering communication adapter according to the present disclosure. The interface module 930 may be coupled to a metering interface 997 of a metering unit. The second module 930 may be provided as INFO-DSS interface board that interfaces to the INFO-DSS interface 997.

[0170] The central task of the interface board 930 in conjunction with a main module or base module for mME is to receive the data telegrams sent by an mME. This requires duplication of the INFO-DSS interface 997 in order to be able to make this interface available to the customer even after the installation of a modular terminal device.

[0171] Figure 9 shows the structure of the plug-in interface board or second module 930 in variant 1. An mME has an INFO-DSS interface 997 consisting of a receiver 946 and transmitter 947. The terminal device or second module 930 is attached to the INFO-DSS. The terminal device or second module 930 has a tunnel 948-1 through the device (hole through the housing), which makes the receiver 946 of the INFO-DSS interface 946 available to the outside world without being affected. A similar tunnel 948-2 is also used for the transmitter 947. In this tunnel there is a semi-transparent mirror 949, which transmits part of the light to the outside world and directs the remaining part to the IR receiver of the interface board 950 (= sensor).

[0172] In this case, the interface board is implemented as an IR receiver with signal processing.

[0173] Figure 10 shows a block diagram of another second module 1030 for use in a metering communication adapter according to the present disclosure. Figure 10 shows the structure of the plug-on interface board or first module 1030 in variant 2. An mME has an INFO-DSS interface 1097 consisting of a receiver 1046 and transmitter 1047. The terminal device is attached to the IR-INFO interface. The terminal device has a tunnel 1048 through the device (hole through the housing), which makes the receiver 1046 of the INFO-DSS available to the outside world without being affected. The signal from the transmitter 1047 is absorbed by the IR receiver 1050 of the interface board 1045. The signal is duplicated and transmitted to the outside world 1051.

[0174] Figure 11 shows a block diagram of a concentrator unit 1107, also called base station 1107. The hardware components of the base station 1107 are explained below.

[0175] Figure 11 shows the schematic structure of the hardware components of the base station 1107. The base station 1107 consists of a main board 1155 (with processor, memory, secure key memory, etc.) and several interfaces or slots.

[0176] The Ethernet interface 1109 is used in SMGw mode as a HAN connection for the CLS proxy and in stand-alone mode for connection to the LAN.

[0177] A slot for a 3G/4G/5G module 1156 is used for the mobile data connection as an alternative to the LAN in stand-alone mode (hereinafter 5G module).

[0178] A slot for a sub-GHz radio module (for wM-Bus) 1108 is used as an LMN interface in SMGw mode (hereinafter LMN radio module). An additional (optional) M-Bus connection 1157 is used as a second LMN interface in SMGw mode.

[0179] One or more slots for radio modules 1158 for simultaneous communication on different frequencies (e.g. 433 and 868 MHz) and modulations (e.g. for LoRaWAN, mioty etc.) are used for long-range radio connection (hereinafter: SubGHz module).

[0180] An additional (optional) configuration port 1159 (USB, UART etc.) is used to set important parameters.

[0181] Software for external encryption and the associated key management is installed on the base station (e.g. LoRaWAN Network Server).

[0182] The uplink of terminal devices is explained according to Figure 12 regarding the base station 1107.

[0183] Figure 12 shows the processes or method performed e.g., in the base station 1107, when a telegram is received via the SubGHz module (uplink). The SMGw mode of the base station was selected.

[0184] The telegram 1203 sent by a terminal device contains double-encrypted data, e.g. {Payload: 65abdc764} as well as metadata such as SNR and the DevEUI of the transmitting device. This telegram is received by the SubGHz module 1202 or second communication interface and an ACK message may be sent back to the device if required. First, the outer encryption/signature is decrypted S1201 so that the following telegram can be received, for example: {"1.8.0": 3qv9, "2.8.0": g4a}.

[0185] The base station has a securely stored database 1265 (e.g. SQL, JSON file, etc.) with all LMN devices (e.g. electricity, gas, water meters) whose telegrams are to be transmitted via the LMN interface. S1202 uses this database to check whether the transmitting device is an LMN device (e.g. based on the DevEUI of the transmitting end device). If this is the case, the meter ID (and possibly other data) assigned by the metering point operator is added to the data telegram in S1203 (which is also stored in a secure database) and sent by the LMN radio module 1209 to the

LMN radio module of an SMGw. This telegram then has the content {counter ID: 6548, "1.8.0": 3qv9, "2.8.0": g4a}, for example.

[0186] At the same time, the telegrams of the LMN devices are stored in a secure database 1266 in order to transmit them to the SMGw via the M-Bus port following a request from the SMGw received by the M-Bus port 1257. Due to these two inherently redundant transmission paths (wM-Bus and M-Bus) to the LMN of the SMGw, maximum reliability of the data transmission can be guaranteed. One of the two transmission paths can also be deactivated or not physically featured.

[0187] This process maps the second LMN-side part of the communication adapter according to PTB-A 50.8 and thus completes it.

[0188] If the transmitting device is not an LMN device, the internal encryption can be decrypted S1204 if the key for the internal encryption has been stored in the secure key memory of the base station 1267. The encrypted or decrypted telegram can be transmitted to other devices via a SubGHz module 1256. In addition, the telegram is converted into an MQTT (or similar) telegram and sent to the CLS proxy of an SMGw via the HAN connection 1268.

[0189] For added value purposes, the LMN data telegram from S1203 can also be transmitted via the CLS proxy: For this purpose, the data telegram is copied to S1204 and runs through the same process. If necessary, the telegram can be anonymized in step S1203, e.g. by removing or randomizing the meter ID.

[0190] This ensures the functions of the LMN communication adapter and the SME. If the stand-alone module is selected instead, the database of the LMN devices is empty so that the LMN radio module and the M-Bus interface remain unused. The M-Bus port is also deactivated. All data is then transmitted via the LAN connection or the 5G module.

[0191] The downlink of 5G/SMGw is explained according to Figure 13 regarding the base station of the present disclosure.

[0192] Figure 13 shows the processes in the base station e.g., in concentrator unit 1107, when a telegram is received via the HAN interface (downlink). The SMGw mode of the base station was selected.

[0193] The SMGw transmits a data telegram to the base station via the HAN interface (CLS proxy). This data packet 1370 is TLS-encrypted and has the content {data: 0572a6f01}, for example. The base station receives this command via the HAN interface 1368. First, the outer encryption (e.g. TLS) is decrypted S1301, allowing the type of control command to be read S1302.

[0194] If this is a control telegram (for controlling a terminal device, e.g. wallbox), the DevEUI (a device ID) of the target terminal device (i.e. the device that is to receive the control command) is also extracted. If the register values of the telegram are not encrypted and the secure key memory of the base station 1367 contains an internal key for the target terminal device, the telegram is encrypted with the internal encryption S1303. The telegram is then encrypted with the outer encryption S1304. The telegram then has the form {Payload: 8e9010}. This telegram is sent to the selected end device using the SubGHz module 1308.

[0195] If this is a management telegram (e.g. add new terminal device to the network), this command is evaluated on the base station and implemented S1305. Other mechanisms such as access to a database are included in the conversion.

[0196] If the stand-alone mode is selected instead, the command is received via the LAN port or the 5G module (instead of from the SMGw).

[0197] According to the invention, a communication adapter, also called communication system, is thus disclosed, in particular for the smart connection of consumption meters by means of long-range radio, in particular LoRaWAN and mioty, whereby the range of the communication link between base station, in particular with SMGw, and a consumption meter or smart meter (mME) is increased by the fact that a communication adapter for consumption meters, in particular according to PTB, is securely connected by means of long-range radio with network protocol.

[0198] Figure 14 shows a block diagram of a possible data packet 1520. In particular, figure 14 shows the schematic structure of a data telegram 1520 that comprises of several data records, which in turn contain the identifier of a register 1521-1, 1521-2, 1521-3 and the associated register values 1522-1, 1522-2, 1522-3. For the internal encryption or signature, the content of the register values is first encrypted or signed

with the internal key. The entire data telegram may then be encrypted/signed with a second outer key.

[0199] This encryption architecture makes it possible, for example, to store the individual encrypted register values in separate databases without having to decrypt the values for correct storage, as the register identifier is readable.

[0200] Depending on the programming, the inner key may be implemented as regular (or CBC) AES encryption or, for example, as an ECC192 signature in accordance with the FNN specification "EDL" (for BSI conformity).

[0201] This type of internal and external encryption is used by the MSB interface, for example. The OMS Group presents a similar implementation, e.g. in Technical Report 06 "OMS over LoRaWAN". However, the telegram structure described therein requires far more bytes (see p. 38 f.) than the procedure described herein and, therefore, limits the device density.

[0202] Note: If (legally) prescribed, the register identifiers can also be encrypted with the inner key.

[0203] Example: Representation of a reduced data telegram of an mME:

[0204] {
1.8.0: 56841020, register 1.8.0: Energy consumption in Wh
2.8.0: 3197930 Register 2.8.0: Energy supply in Wh
}

[0205] 1. internal encryption / signature: user data
{
1.8.0: a9b0973f,
2.8.0: 0dae71
}

[0206] 2. outer encryption: complete telegram

[0207] {data: 9e6f73100ae2078f}

[0208] Figure 15 shows a flow diagram of another embodiment of a method according to the present disclosure. Figure 15 shows the procedure for internal and external encryption, which is referred to as the encryption module for the data flow: A data telegram 1620 to be encrypted is passed to the encryption module. The device has a securely stored key (e.g. AES, ECC192) 1675. This key is used to encrypt or sign the user data of the telegram with the internal encryption S1601. This data telegram 1676 is then additionally encrypted with the outer key (e.g. AES, TLS or ECC192) S1602. The double-encrypted telegram 1677 is then returned to the device for further data flow.

[0209] The processes, methods, or algorithms disclosed herein can be deliverable to/implemented by a processing device, controller, or computer, which can include any existing programmable electronic control unit or dedicated electronic control unit. Similarly, the processes, methods, or algorithms can be stored as data and instructions executable by a controller or computer in many forms including, but not limited to, information permanently stored on non-writable storage media such as ROM devices and information alterably stored on writeable storage media such as floppy disks, magnetic tapes, CDs, RAM devices, and other magnetic and optical media. The processes, methods, or algorithms can also be implemented in a software executable object. Alternatively, the processes, methods, or algorithms can be embodied in whole or in part using suitable hardware components, such as Application Specific Integrated Circuits (ASICs), Field-Programmable Gate Arrays (FPGAs), state machines, controllers or other hardware components or devices, or a combination of hardware, software and firmware components.

[0210] While exemplary embodiments are described above, it is not intended that these embodiments describe all possible forms encompassed by the claims. The words used in the specification are words of description rather than limitation, and it is understood that various changes can be made without departing from the spirit and scope of the disclosure. As previously described, the features of various embodiments can be combined to form further embodiments of the invention that may not be explicitly described or illustrated. While various embodiments could have been described as providing advantages or being preferred over other embodiments or prior art implementations with respect to one or more desired characteristics, those of ordinary skill in the art recognize that one or more features or characteristics can be

compromised to achieve desired overall system attributes, which depend on the specific application and implementation. These attributes can include, but are not limited to cost, strength, durability, life cycle cost, marketability, appearance, packaging, size, serviceability, weight, manufacturability, ease of assembly, etc. As such, to the extent any embodiments are described as less desirable than other embodiments or prior art implementations with respect to one or more characteristics, these embodiments are not outside the scope of the disclosure and can be desirable for particular applications.

[0211] With regard to the processes, systems, methods, heuristics, etc. described herein, it should be understood that, although the steps of such processes, etc. have been described as occurring according to a certain ordered sequence, such processes could be practiced with the described steps performed in an order other than the order described herein. It further should be understood that certain steps could be performed simultaneously, that other steps could be added, or that certain steps described herein could be omitted. In other words, the descriptions of processes herein are provided for the purpose of illustrating certain embodiments, and should in no way be construed so as to limit the claims.

[0212] Accordingly, it is to be understood that the above description is intended to be illustrative and not restrictive. Many embodiments and applications other than the examples provided would be apparent upon reading the above description. The scope should be determined, not with reference to the above description, but should instead be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled. It is anticipated and intended that future developments will occur in the technologies discussed herein, and that the disclosed systems and methods will be incorporated into such future embodiments. In sum, it should be understood that the application is capable of modification and variation.

[0213] All terms used in the claims are intended to be given their broadest reasonable constructions and their ordinary meanings as understood by those knowledgeable in the technologies described herein unless an explicit indication to the contrary in made herein. In particular, use of the singular articles such as “a,” “the,” “said,” etc. should be read to recite one or more of the indicated elements unless a claim recites an explicit limitation to the contrary.

[0214] The abstract of the disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

[0215] While exemplary embodiments are described above, it is not intended that these embodiments describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention. Additionally, the features of various implementing embodiments may be combined to form further embodiments of the invention.

List of Abbreviations used in the description

- mME: moderne measurement euipment: digital power meter / Smart Meter
- INFO-DSS: Infrared Info Data Interface (unidirectional)
- MSB-DSS: Infrared Data Interface for the operator of the metering point (bidirectional)
- Useful data: Metering data to be protected, Control data and the like e.g., for inner encryption
- Smart Metering: Reading of main measuring points for electricity, water, gas, etc.
- Sub-metering: Reading of sub-metering points (apartment water meters, heat cost allocators, etc.)
- Control: Devices such as charging points, thermostats, etc.
- Automated control: control of devices without the internet
- SMGw: Smart meter gateway according to BSI (Bundesamt für Sicherheit in der Informationstechnik) standards for connecting domestic devices to the Internet
- EMT: external market participant (except grid operator, metering point operator) with access to the SMGw
- CLS proxy: Secure connection route between EMT and local device
- LMN: Network for the transmission of metering data from smart metering
- SE: Control unit for the SMGw
- SME: Sub-metering unit for the SMGw
- LoRaWAN: 868 MHz (long-range) radio with network protocol (MAC), also used herein as a synonym for other radio protocols such as mioty
- Base station: Base station/gateway for LoRaWAN to receive and send radio telegrams from end devices, interface between Internet/SMGw and LoRaWAN
- DevEUI: Unique device ID in the network (cf. IP or MAC address)

LIST OF REFERENCE SIGNS

100	communication system
101, 201, 401, 701, 801	metering communication adapter
102, 202, 402, 602, 702, 802, 1202	local meter interface
103, 203, 303, 603, 703, 803, 1203	metering data
104, 204, 404, 504, 704, 804	first communication interface
107, 307, 1107	concentrator unit
108, 308, 1108, 1308	second communication interface
109, 309, 1109, 1209	local interface
215, 415, 715, 815	first cryptographic module
216, 316	cryptographically encrypted metering data
220, 1520, 1620	data package
221-1, 221-2, 1521-1, 1521-2, 1522-3	meta data
222-1, 222-2, 1522-1, 1522-2, 1522-3	measurement data
325	second cryptographic module
430, 630, 930, 1030	first module
431, 631	first coupling interface
432, 532	second module
433, 533	second coupling interface
535, 635	board
536, 636	microcontroller
537	power source
538	external power input
945, 1045	housing
946, 1046	receiver
947, 1047	sender
948-1, 948-2, 1048	tunnel

949	semi-transparent mirror
950	receiver
1050	controller
1051	sender
1155	board
1156, 1256	communication interface
1157, 1257	M-Bus communication interface
1158	wireless communication interface
1159	configuration interface
1265	database
1266	secure database
1267, 1367	key database
1268, 1368	HAN communication interface
1370	data packet
1675	cryptographic key
1676	single encrypted data package
1677	double encrypted data package
199, 299, 799, 899	metering element
198, 398	smart meter gateway
797, 897, 997, 1097	metering interface
S1201, S1202, S1203, S1204	method steps
S1301, S1302, S1303, S1304, S1305	method steps
S1501, S1502	method steps
S1601, S1602	method steps

CLAIMS

1. Communication system (100) comprising:

at least one metering communication adapter (101, 201, 401, 701, 801), the metering communication adapter (101, 201, 401, 701, 801) comprising a local meter interface (102, 202, 402, 602, 702, 802, 1202) configured to communicatively couple to a metering element (199, 299, 799, 899), and to receive metering data (103, 203, 303, 603, 703, 803, 1203) from the metering element (199, 299, 799, 899), and comprising a first communication interface (104, 204, 404, 504, 704, 804) configured to output the metering data (103, 203, 303, 603, 703, 803, 1203) received from the metering element (199, 299, 799, 899); and

a concentrator unit (107, 307, 1107) comprising a second communication interface (108, 308, 1108, 1308) configured to receive the metering data (103, 203, 303, 603, 703, 803, 1203) output by the at least one metering communication adapter (101, 201, 401, 701, 801), and comprising a local interface (109, 309, 1109, 1209) configured to output the received metering data (103, 203, 303, 603, 703, 803, 1203);

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) comprises at least one of:

an optical interface;

an infrared optical interface;

a character-based optical interface; and

a reed-switch-based interface; and

wherein the first communication interface (104, 204, 404, 504, 704, 804) and the second communication interface (108, 308, 1108, 1308) comprise at least one of:

a LoRaWAN interface; and

a mioty interface.

2. Communication system (100) according to any one of the preceding claims, wherein the at least one metering communication adapter (101, 201, 401, 701, 801)

further comprises a first cryptographic module (215, 415, 715, 815) coupled between the local meter interface (102, 202, 402, 602, 702, 802, 1202) and the first communication interface (104, 204, 404, 504, 704, 804);

wherein the first cryptographic module (215, 415, 715, 815) is configured to cryptographically encrypt the received metering data (103, 203, 303, 603, 703, 803, 1203) and provide the cryptographically encrypted metering data (216, 316) to the first communication interface (104, 204, 404, 504, 704, 804) for transmission to the concentrator unit (107, 307, 1107).

3. Communication system (100) according to claim 2, wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) is configured to receive data packages (220, 1520, 1620) comprising meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3) and measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3); and

wherein the first cryptographic module (215, 415, 715, 815) is configured to at least one of:

perform a single encryption of the measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3); and

perform a first encryption of the measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) , and a second encryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3).

4. Communication system (100) according to any one of the preceding claims, wherein the concentrator unit (107, 307, 1107) further comprises a second cryptographic module (325) coupled between the second communication interface (108, 308, 1108, 1308) and the local interface (109, 309, 1109, 1209);

wherein the second cryptographic module (325) is configured to cryptographically decrypt the received metering data and provide the cryptographically decrypted metering data (103, 203, 303, 603, 703, 803, 1203) to the local interface (109, 309, 1109, 1209).

5. Communication system (100) according to claim 4, wherein the second communication interface (108, 308, 1108, 1308) is configured to receive data packages

(220, 1520, 1620) comprising measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) encrypted with a first encryption, and meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3) with the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) encrypted with a second encryption; and

wherein the second cryptographic module (325) is configured to at least one of:

perform a single decryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3); and

perform a first decryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3), and a second decryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3).

6. Communication system (100) according to any one of the preceding claims, wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202), the first communication interface (104, 204, 404, 504, 704, 804), the second communication interface (108, 308, 1108, 1308), and the local interface (109, 309, 1109, 1209) comprise bi-directional interfaces;

wherein the local interface (109, 309, 1109, 1209) is configured to receive configuration and control data and to provide the configuration and control data to the second communication interface (108, 308, 1108, 1308);

wherein the second communication interface (108, 308, 1108, 1308) is configured to transmit the received configuration and control data to the first communication interface (104, 204, 404, 504, 704, 804);

wherein the first communication interface (104, 204, 404, 504, 704, 804) is configured to transmit the received configuration and control data to the local meter interface (102, 202, 402, 602, 702, 802, 1202); and

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) is configured to output the received configuration and control data.

7. Communication system (100) according to the preceding claims 4 and 6, wherein the second cryptographic module (325) is configured to cryptographically encode the configuration and control data, and to provide the cryptographically encoded configuration and control data to the second communication interface (108, 308, 1108, 1308); and

wherein the second communication interface (108, 308, 1108, 1308) is configured to transmit the cryptographically encoded configuration and control data to the first communication interface (104, 204, 404, 504, 704, 804).

8. Communication system (100) according to the preceding claims 2 and 5, wherein the first cryptographic module (215, 415, 715, 815) is configured to cryptographically decode the received configuration and control data and to provide the cryptographically decoded configuration and control data to the local meter interface (102, 202, 402, 602, 702, 802, 1202); and

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) is configured to output the cryptographically decoded configuration and control data.

9. Communication system (100) according to any one of the preceding claims, wherein the at least one metering communication adapter (101, 201, 401, 701, 801) comprises:

a first module (430, 630, 930, 1030) comprising the local meter interface (102, 202, 402, 602, 702, 802, 1202) and a first coupling interface (431, 631) coupled to the local meter interface (102, 202, 402, 602, 702, 802, 1202); and

a second module (432, 532) comprising a second coupling interface (433, 533) coupled to the first communication interface (104, 204, 404, 504, 704, 804);

wherein the first coupling interface (431, 631) is configured to couple to the second coupling interface (433, 533).

10. Communication system (100) according to the preceding claims 2 and 9, wherein the first cryptographic module (215, 415, 715, 815) is arranged:

between the local meter interface (102, 202, 402, 602, 702, 802, 1202), and the first coupling interface (431, 631); or

between the second coupling interface (433, 533), and the first communication interface (104, 204, 404, 504, 704, 804).

11. Communication system (100) according to any one of the preceding claims, wherein the local interface (109, 309, 1109, 1209) comprises a wired communication interface, especially an Ethernet-based communication interface.

12. Communication system (100) according to any one of the preceding claims, wherein the local interface (109, 309, 1109, 1209) comprises a wireless interface, especially a cellular network wireless interface, and wherein the local interface (109, 309, 1109, 1209) is configured to output the metering data (103, 203, 303, 603, 703, 803, 1203) to a remote receiver.

13. Communication system (100) according any one of claims 11 and 12, wherein the local interface (109, 309, 1109, 1209) is configured to output the metering data (103, 203, 303, 603, 703, 803, 1203) to a local smart meter gateway (198, 398).

AMENDED CLAIMS
received by the International Bureau on 14 April 2025 (14.04.2025)

1. Communication system (100) comprising:

at least one metering communication adapter (101, 201, 401, 701, 801), the metering communication adapter (101, 201, 401, 701, 801) comprising a local meter interface (102, 202, 402, 602, 702, 802, 1202) configured to communicatively couple to a metering element (199, 299, 799, 899), and to receive metering data (103, 203, 303, 603, 703, 803, 1203) from the metering element (199, 299, 799, 899), and comprising a first communication interface (104, 204, 404, 504, 704, 804) configured to output the metering data (103, 203, 303, 603, 703, 803, 1203) received from the metering element (199, 299, 799, 899); and

a concentrator unit (107, 307, 1107) comprising a second communication interface (108, 308, 1108, 1308) configured to receive the metering data (103, 203, 303, 603, 703, 803, 1203) output by the at least one metering communication adapter (101, 201, 401, 701, 801), and comprising a local interface (109, 309, 1109, 1209) configured to output the received metering data (103, 203, 303, 603, 703, 803, 1203);

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) comprises at least one of:

an optical interface;

an infrared optical interface;

a character-based optical interface; and

a reed-switch-based interface; and

wherein the first communication interface (104, 204, 404, 504, 704, 804) and the second communication interface (108, 308, 1108, 1308) comprise at least one of:

a LoRaWAN interface; and

a mioty interface;

wherein the at least one metering communication adapter (101, 201, 401, 701, 801) further comprises a first cryptographic module (215, 415, 715, 815) coupled between

the local meter interface (102, 202, 402, 602, 702, 802, 1202) and the first communication interface (104, 204, 404, 504, 704, 804);

wherein the first cryptographic module (215, 415, 715, 815) is configured to cryptographically encrypt the received metering data (103, 203, 303, 603, 703, 803, 1203) and provide the cryptographically encrypted metering data (216, 316) to the first communication interface (104, 204, 404, 504, 704, 804) for transmission to the concentrator unit (107, 307, 1107);

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) is configured to receive data packages (220, 1520, 1620) comprising meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3) and measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3); and

wherein the first cryptographic module (215, 415, 715, 815) is configured to

perform a first encryption of the measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) , and a second encryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3);

wherein the concentrator unit (107, 307, 1107) further comprises a second cryptographic module (325) coupled between the second communication interface (108, 308, 1108, 1308) and the local interface (109, 309, 1109, 1209); and

wherein the second cryptographic module (325) is configured to cryptographically decrypt the received metering data and provide the cryptographically decrypted metering data (103, 203, 303, 603, 703, 803, 1203) to the local interface (109, 309, 1109, 1209).

2. Communication system (100) according to claim 1, wherein the first cryptographic module (215, 415, 715, 815) is further configured to perform a single encryption of the measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3).

3. Communication system (100) according to any one of the preceding claims, wherein the second communication interface (108, 308, 1108, 1308) is configured to receive data packages (220, 1520, 1620) comprising measurement data (222-1, 222-

2, 1522-1, 1522-2, 1522-3) encrypted with a first encryption, and meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3) with the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) encrypted with a second encryption; and

wherein the second cryptographic module (325) is configured to at least one of:

perform a single decryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3); and

perform a first decryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3) and the meta data (221-1, 221-2, 1521-1, 1521-2, 1522-3), and a second decryption of the encrypted measurement data (222-1, 222-2, 1522-1, 1522-2, 1522-3).

4. Communication system (100) according to any one of the preceding claims, wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202), the first communication interface (104, 204, 404, 504, 704, 804), the second communication interface (108, 308, 1108, 1308), and the local interface (109, 309, 1109, 1209) comprise bi-directional interfaces;

wherein the local interface (109, 309, 1109, 1209) is configured to receive configuration and control data and to provide the configuration and control data to the second communication interface (108, 308, 1108, 1308);

wherein the second communication interface (108, 308, 1108, 1308) is configured to transmit the received configuration and control data to the first communication interface (104, 204, 404, 504, 704, 804);

wherein the first communication interface (104, 204, 404, 504, 704, 804) is configured to transmit the received configuration and control data to the local meter interface (102, 202, 402, 602, 702, 802, 1202); and

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) is configured to output the received configuration and control data.

5. Communication system (100) according to the preceding claim 4, wherein the second cryptographic module (325) is configured to cryptographically encode the configuration and control data, and to provide the cryptographically encoded

configuration and control data to the second communication interface (108, 308, 1108, 1308); and

wherein the second communication interface (108, 308, 1108, 1308) is configured to transmit the cryptographically encoded configuration and control data to the first communication interface (104, 204, 404, 504, 704, 804).

6. Communication system (100) according to the preceding claim 3, wherein the first cryptographic module (215, 415, 715, 815) is configured to cryptographically decode the received configuration and control data and to provide the cryptographically decoded configuration and control data to the local meter interface (102, 202, 402, 602, 702, 802, 1202); and

wherein the local meter interface (102, 202, 402, 602, 702, 802, 1202) is configured to output the cryptographically decoded configuration and control data.

7. Communication system (100) according to any one of the preceding claims, wherein the at least one metering communication adapter (101, 201, 401, 701, 801) comprises:

a first module (430, 630, 930, 1030) comprising the local meter interface (102, 202, 402, 602, 702, 802, 1202) and a first coupling interface (431, 631) coupled to the local meter interface (102, 202, 402, 602, 702, 802, 1202); and

a second module (432, 532) comprising a second coupling interface (433, 533) coupled to the first communication interface (104, 204, 404, 504, 704, 804);

wherein the first coupling interface (431, 631) is configured to couple to the second coupling interface (433, 533).

8. Communication system (100) according to the preceding claim 7, wherein the first cryptographic module (215, 415, 715, 815) is arranged:

between the local meter interface (102, 202, 402, 602, 702, 802, 1202), and the first coupling interface (431, 631); or

between the second coupling interface (433, 533), and the first communication interface (104, 204, 404, 504, 704, 804).

9. Communication system (100) according to any one of the preceding claims, wherein the local interface (109, 309, 1109, 1209) comprises a wired communication interface, especially an Ethernet-based communication interface.

10. Communication system (100) according to any one of the preceding claims, wherein the local interface (109, 309, 1109, 1209) comprises a wireless interface, especially a cellular network wireless interface, and wherein the local interface (109, 309, 1109, 1209) is configured to output the metering data (103, 203, 303, 603, 703, 803, 1203) to a remote receiver.

11. Communication system (100) according any one of claims 9 and 10, wherein the local interface (109, 309, 1109, 1209) is configured to output the metering data (103, 203, 303, 603, 703, 803, 1203) to a local smart meter gateway (198, 398).

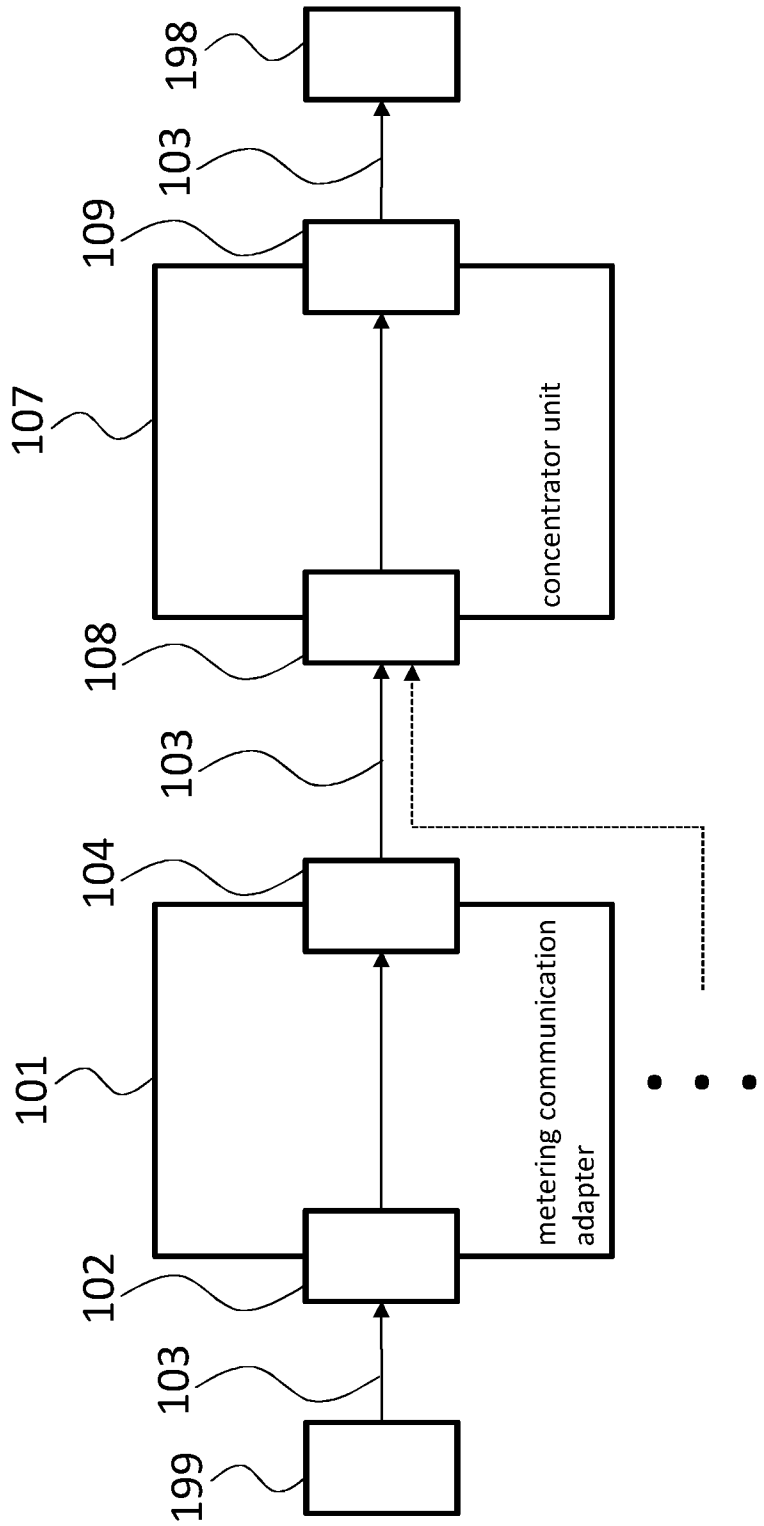

198
103
109
107
concentrator unit
108
103
104
101
metering communication adapter
102
103
199
100

Fig. 1

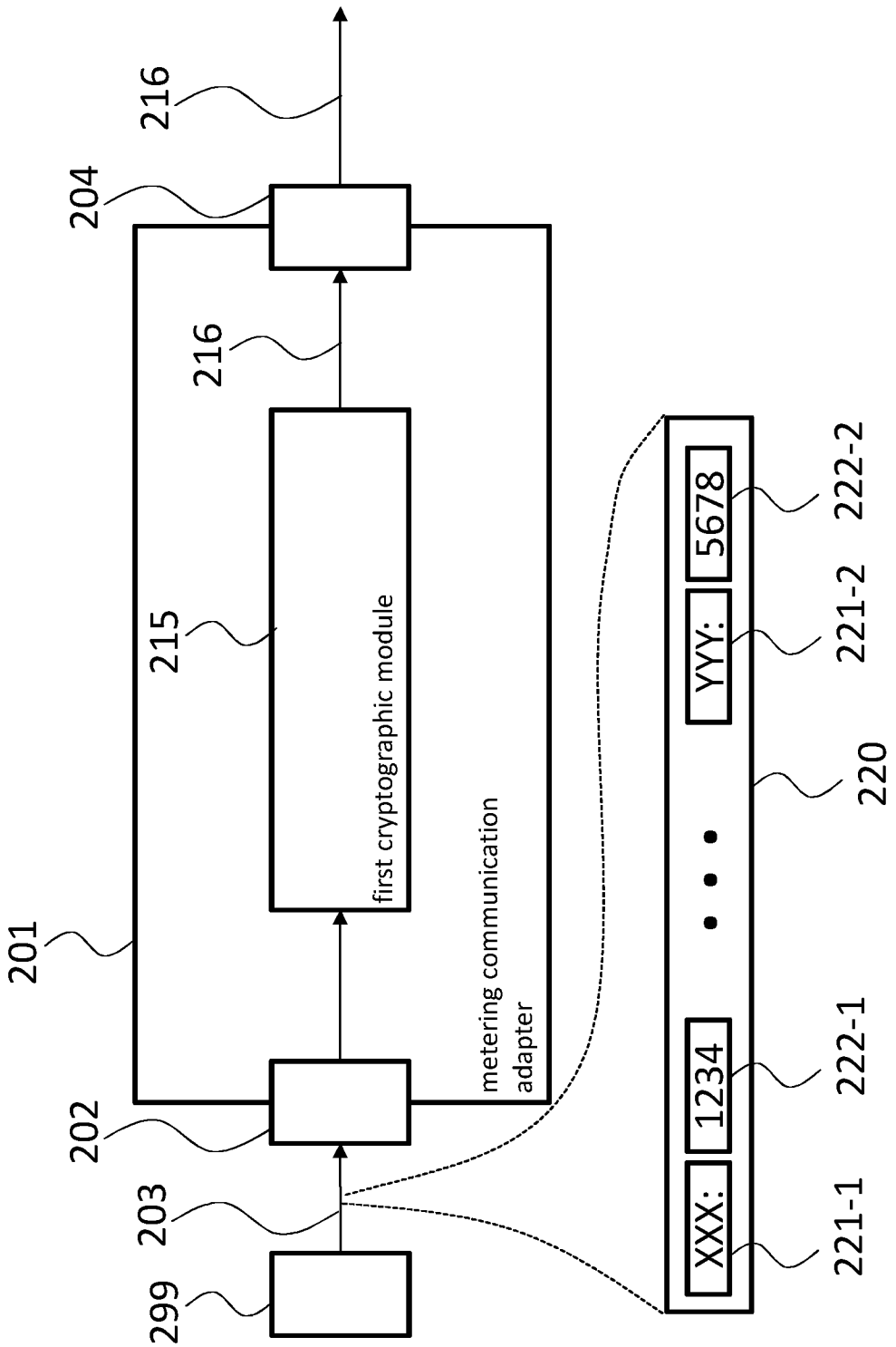

216
204
216
215
first cryptographic module
metering communication adapter
201
202
203
299
220
222-2
221-2
222-1
221-1
5678
YYY:
1234
XXX:

Fig. 2

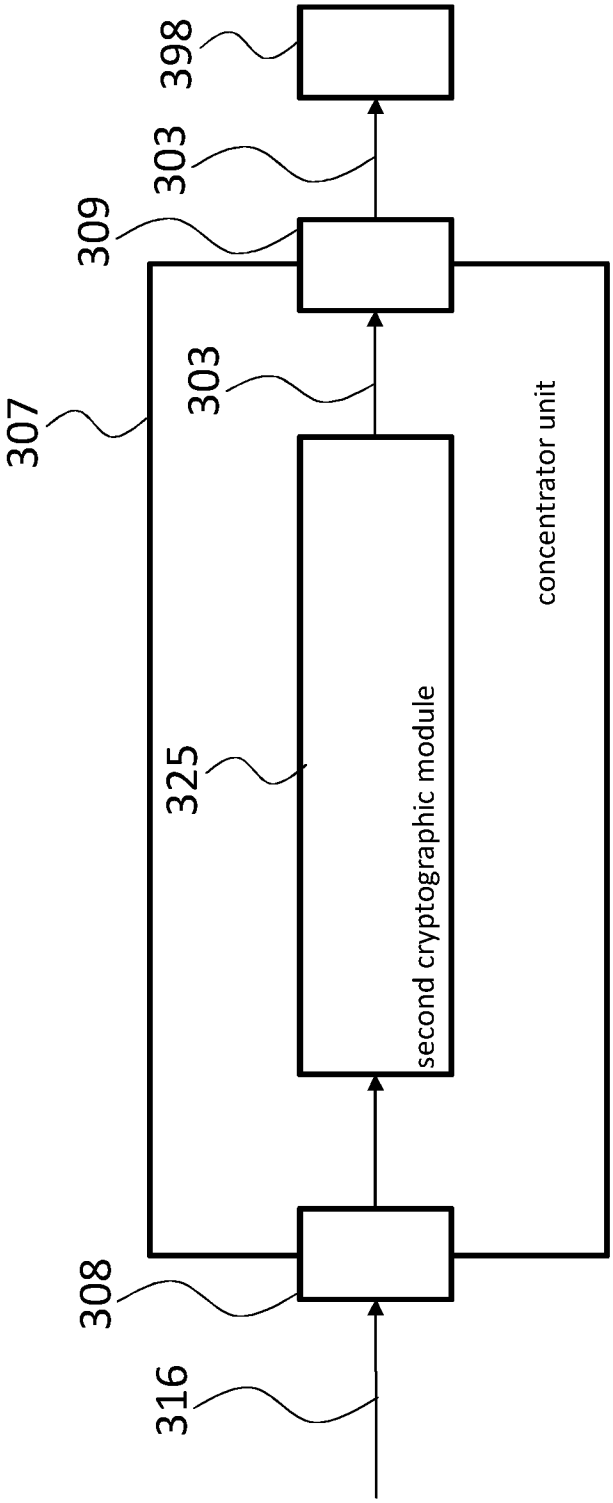

398
303
309
303
307
concentrator unit
second cryptographic module
325
308
316

Fig. 3

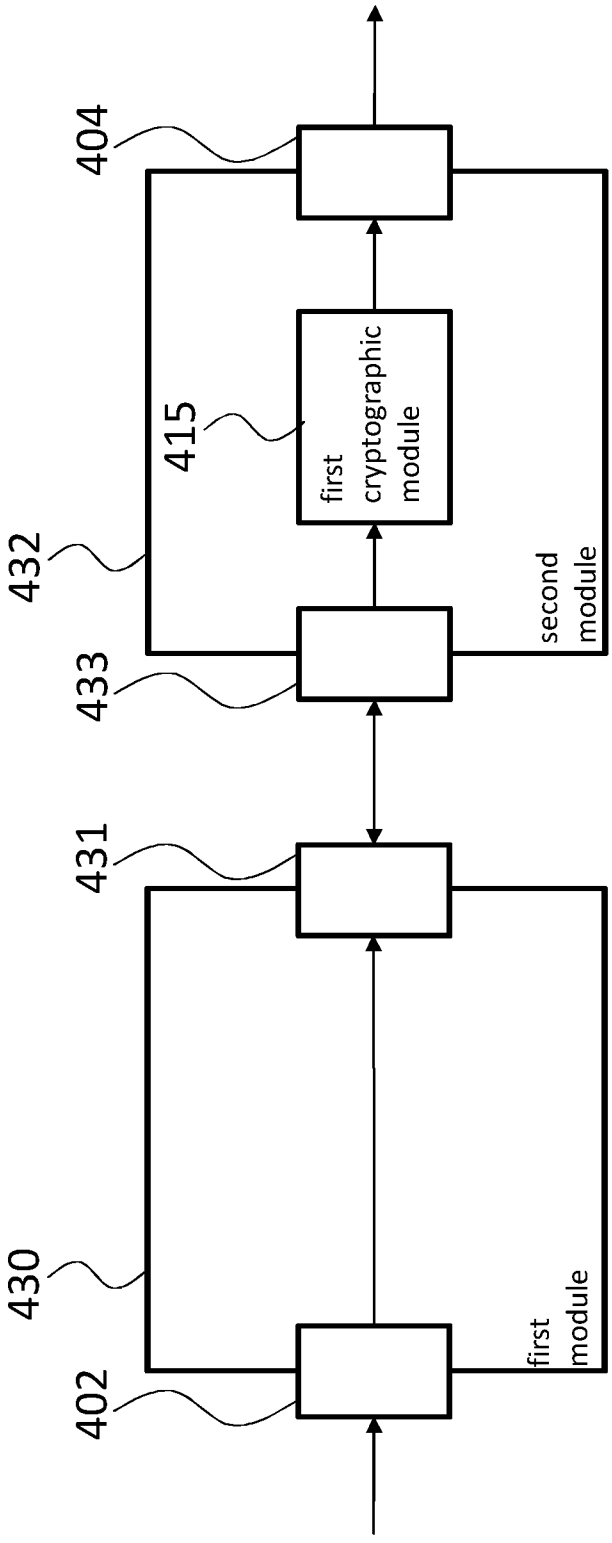

404
415
first cryptographic module
432
second module
433
431
430
first module
402
401

Fig. 4

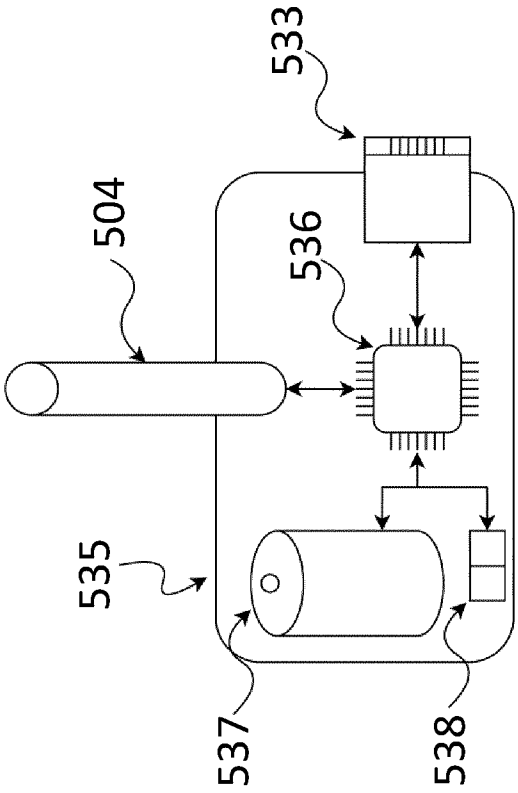


Fig. 5

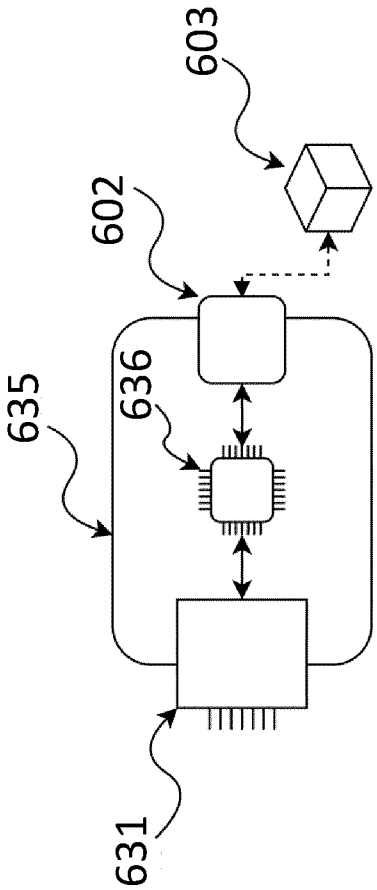


Fig. 6

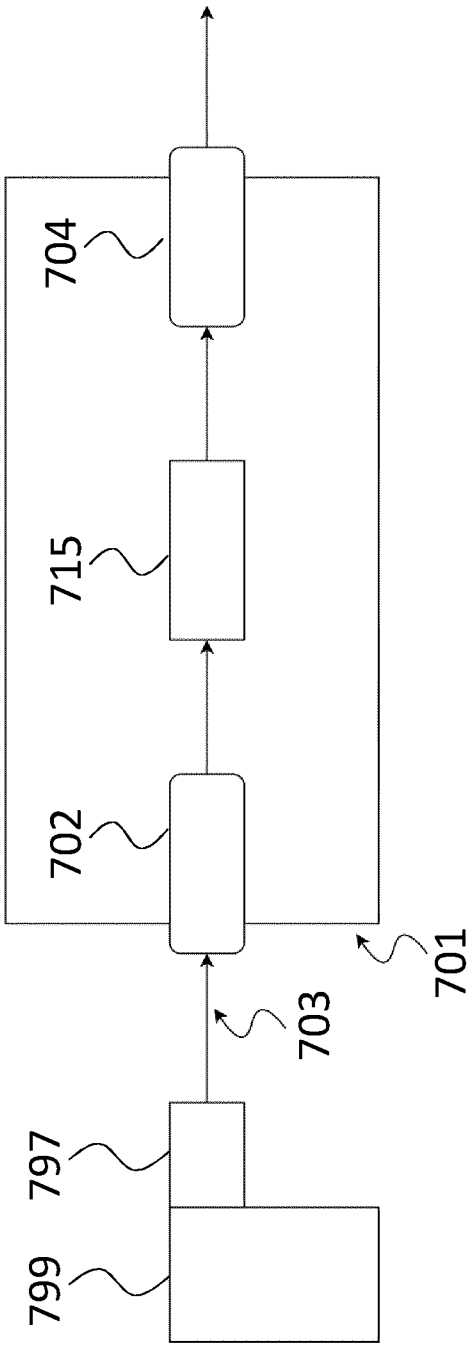


Fig. 7

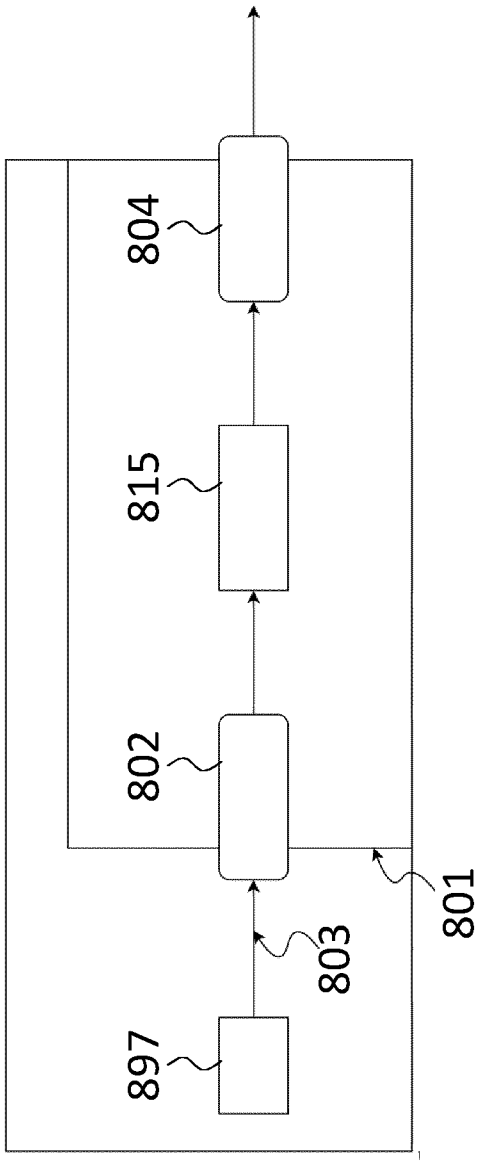
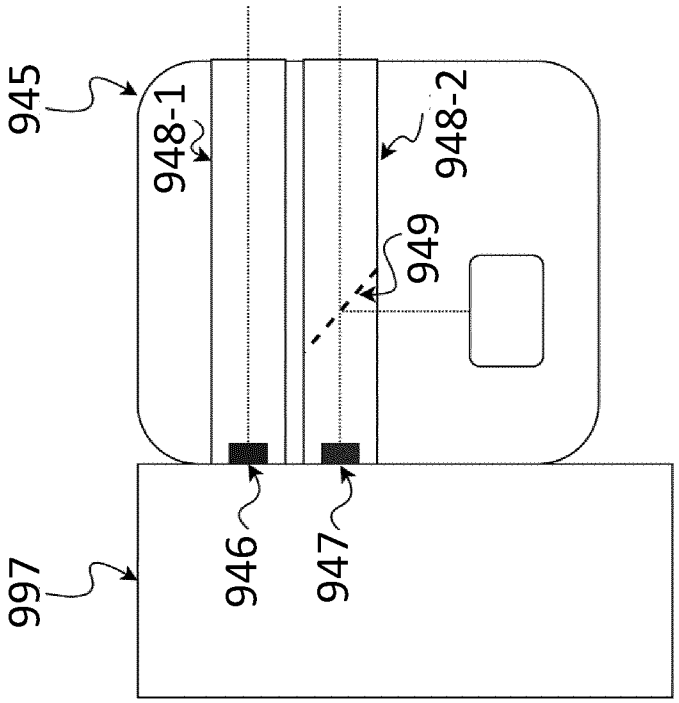
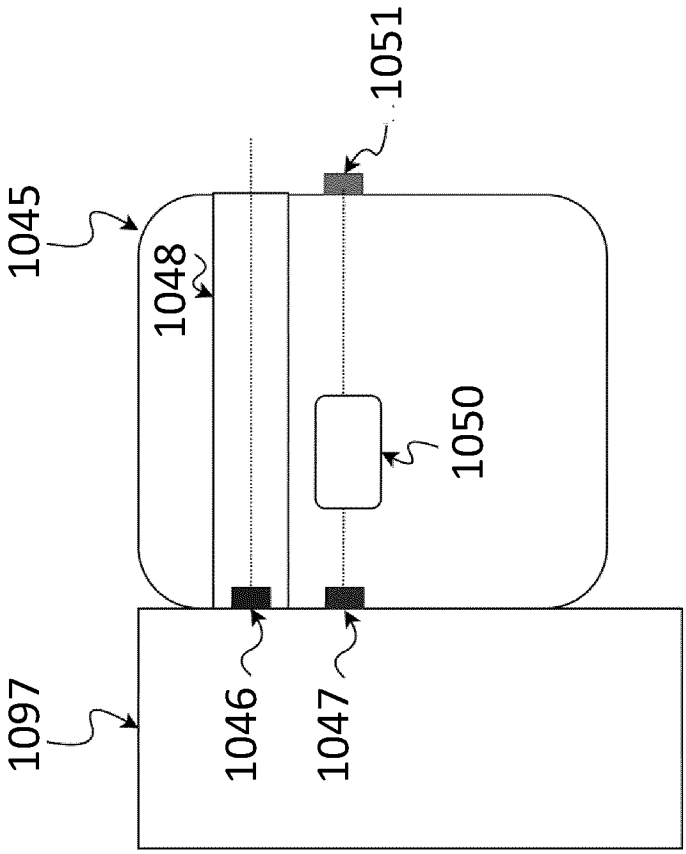


Fig. 8



930

Fig. 9



1030

Fig. 10

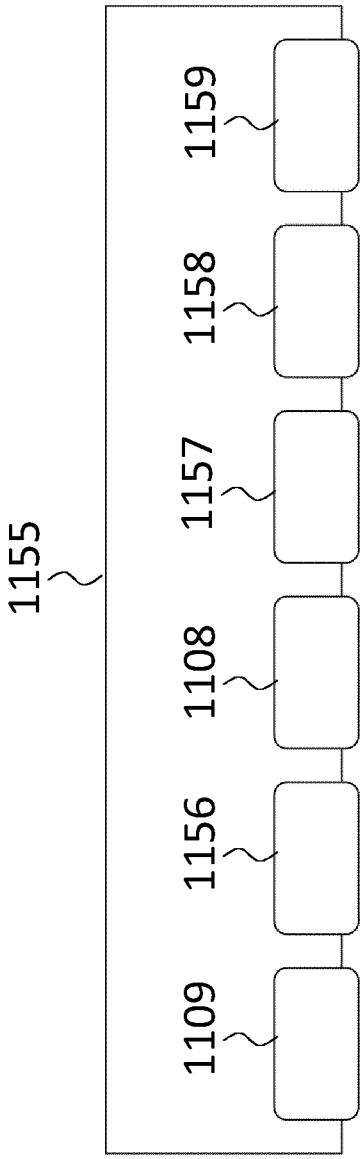


Fig. 11

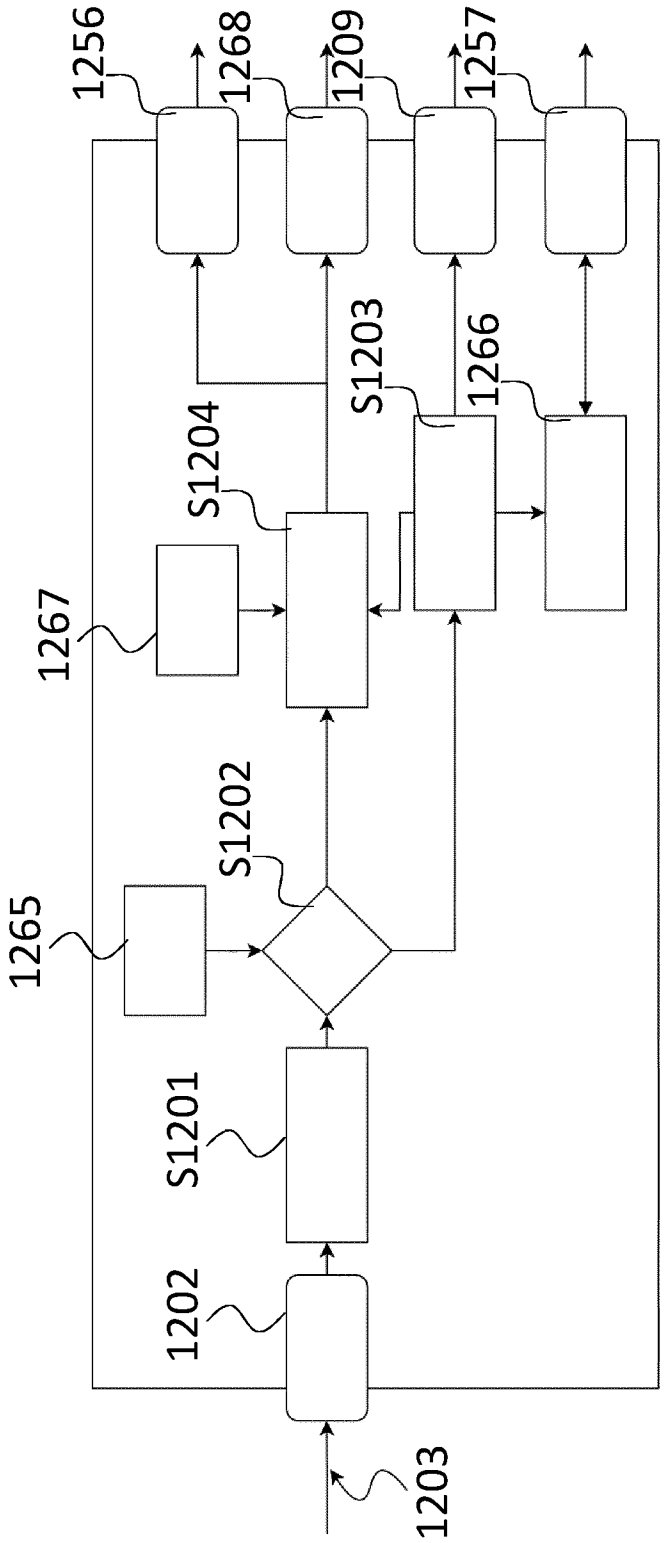

1256
1268
1209
1257
S1203
1266
S1204
1267
S1202
1265
S1201
1202
1203

Fig. 12

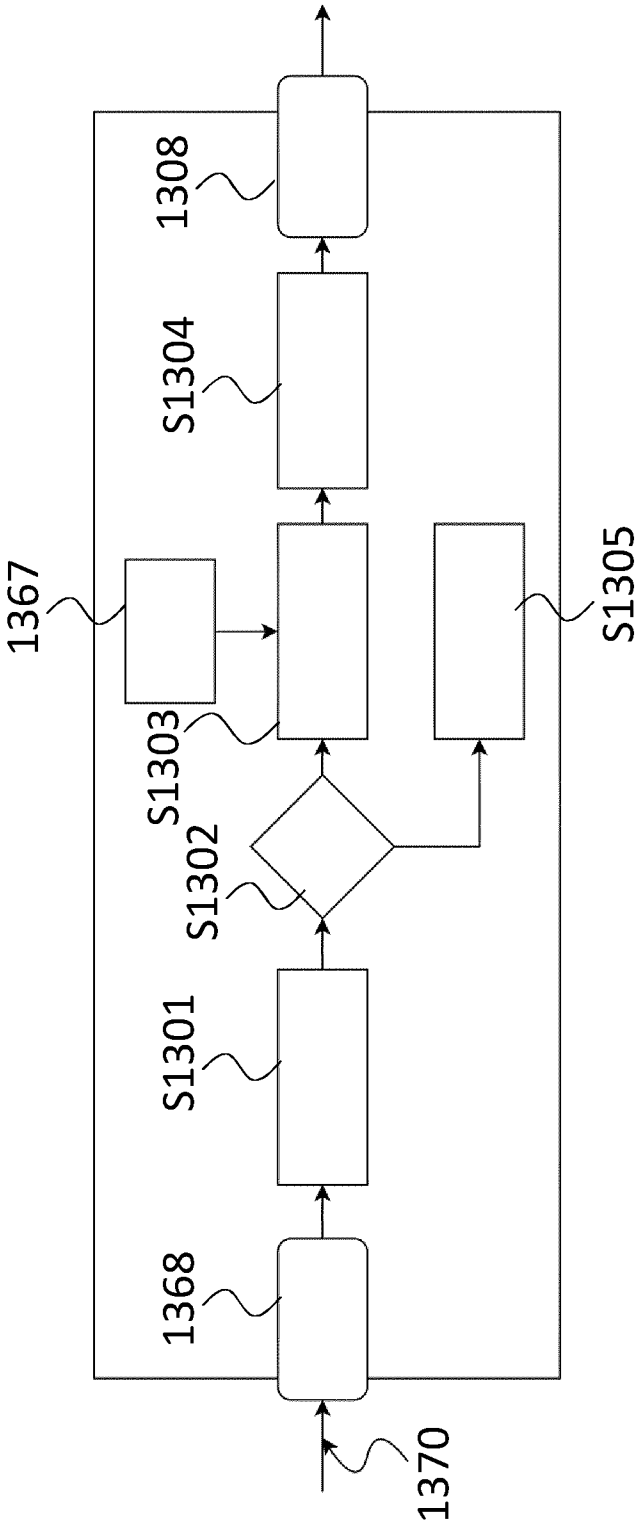


Fig. 13

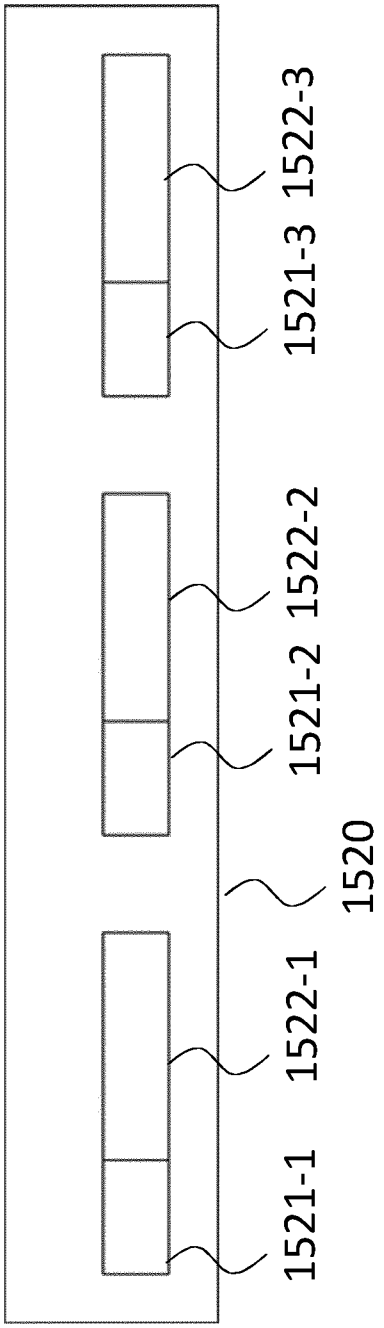


Fig. 14

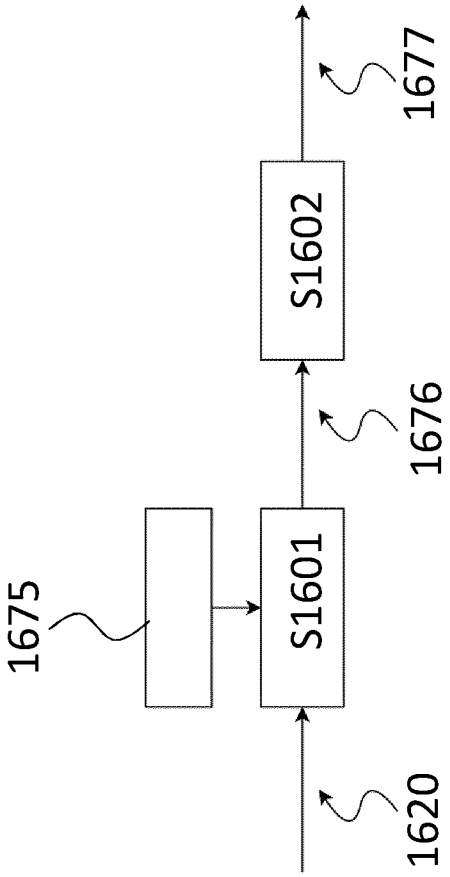


Fig. 15

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2024/062291

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/40 H04L67/12 H04Q9/00
ADD. G01D4/00 H04L67/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04Q G01D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2020 000481 A1 (UTILITOOLS GMBH [DE]) 29 July 2021 (2021-07-29)	1,2,9-13
A	figure 2 paragraph [0038] claim 1 claim 9 claim 5	3-8

A	DE 10 2020 116358 A1 (E KUNDENSERVICE NETZ GMBH [DE]) 23 December 2021 (2021-12-23) the whole document	1-13

	-/--	

[x] Further documents are listed in the continuation of Box C.

[x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 September 2024	25/09/2024

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schmidbauer, Philipp

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange", IEC 62056-21:2002, IEC, 3, RUE DE VAREMBÉ, PO BOX 131, CH-1211 GENEVA 20, SWITZERLAND, 15 May 2002 (2002-05-15), pages 1-70, XP082003960, [retrieved on 2002-05-15] the whole document	1-13
A	Bundesamt: "Technische Richtlinie BSI TR-03109-1", , 16 January 2019 (2019-01-16), pages 1-146, XP055809276, Retrieved from the Internet: URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.html the whole document	1-13
A	DETKEN KAI-OLIVER ET AL: "Integrity protection in a smart grid environment for wireless access of smart meters", 2014 2ND INTERNATIONAL SYMPOSIUM ON WIRELESS SYSTEMS WITHIN THE CONFERENCES ON INTELLIGENT DATA ACQUISITION AND ADVANCED COMPUTING SYSTEMS, IEEE, 11 September 2014 (2014-09-11), pages 79-86, XP032685288, DOI: 10.1109/IDAACS-SWS.2014.6954628 [retrieved on 2014-11-12] the whole document	3-8
A	GENZEL CARL-HEINZ ET AL: "Custom Transport Interface for the Integration of Trusted Network Connect in German Smart Metering Systems", 2015 EUROPEAN INTELLIGENCE AND SECURITY INFORMATICS CONFERENCE, IEEE, 7 September 2015 (2015-09-07), pages 45-52, XP032847659, DOI: 10.1109/EISIC.2015.25 [retrieved on 2016-01-12] the whole document	3-8
A	DANIEL ANGERMEIER ET AL: "A Secure Architecture for Smart Meter Systems", 12 December 2012 (2012-12-12), 20121212, PAGE(S) 108 - 122, XP047006623, the whole document	3-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2024/062291

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102020000481 A1	29-07-2021	NONE	
DE 102020116358 A1	23-12-2021	DE 102020116358 A1	23-12-2021
		EP 3930291 A1	29-12-2021
		PL 3930291 T3	26-08-2024