(12) UK Patent (19) GB (11) 2607298 (13) B

(45) Date of B Publication 20.09.2023

(54) Title of the Invention: Smart meter device refurbishment

(51) INT CL: ***G01D 4/02*** (2006.01) ***G01R 22/06*** (2006.01) ***G06Q 50/06*** (2012.01) ***H04L 9/10*** (2006.01) ***H04L 9/32*** (2006.01)

(21) Application No: **2107782.1**

(22) Date of Filing: **01.06.2021**

(43) Date of A Publication **07.12.2022**

(56) Documents Cited:
KR 101784409 B **US 20110035338 A1**

(58) Field of Search:
As for published application 2607298 A viz:
INT CL **G01D, G01R, H04L**
Other: **WPI, EPODOC**
updated as appropriate

Additional Fields
Other: **None**

(72) Inventor(s):
Ralf Thor
Frank Kullmann
Thorsten Peters
Ralph Rakers
Matthew Hallchurch

(73) Proprietor(s):
Honeywell International Inc.
300 S. Tryon Street, Suite 600, Charlotte 28202, North Carolina, United States of America

(74) Agent and/or Address for Service:
Patent Outsourcing Limited
1 King Street, BAKEWELL, Derbyshire, DE45 1DZ, United Kingdom

GB 2607298 B

Figure 1

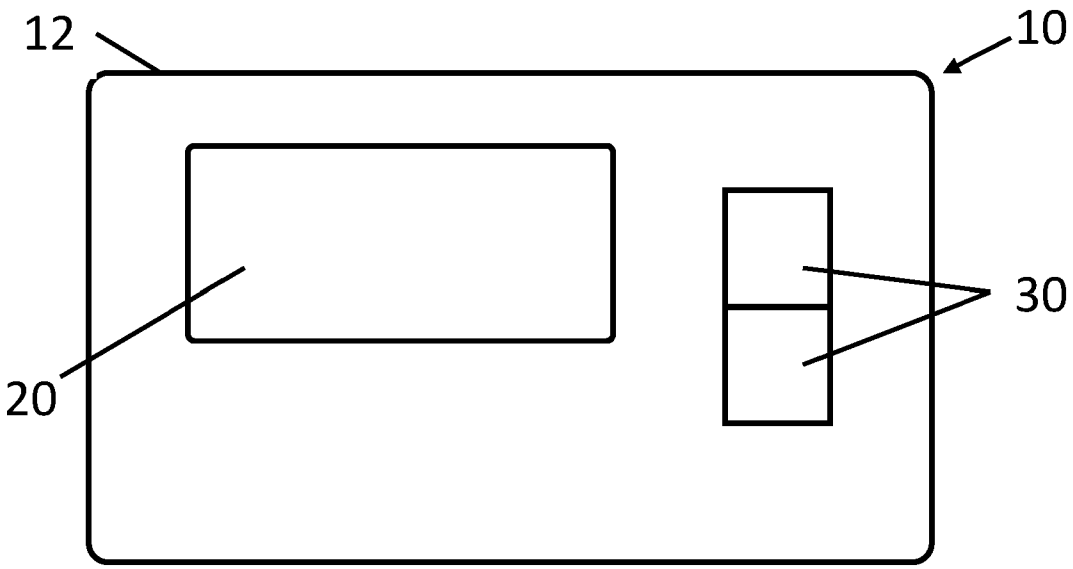


Figure 1A

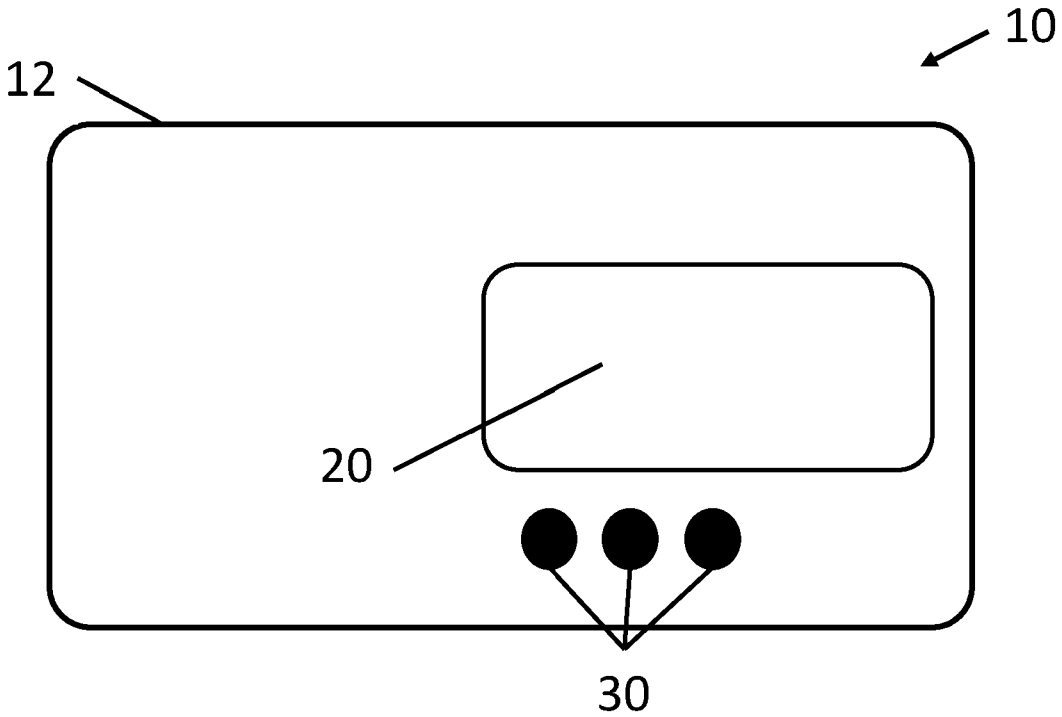


Figure 2

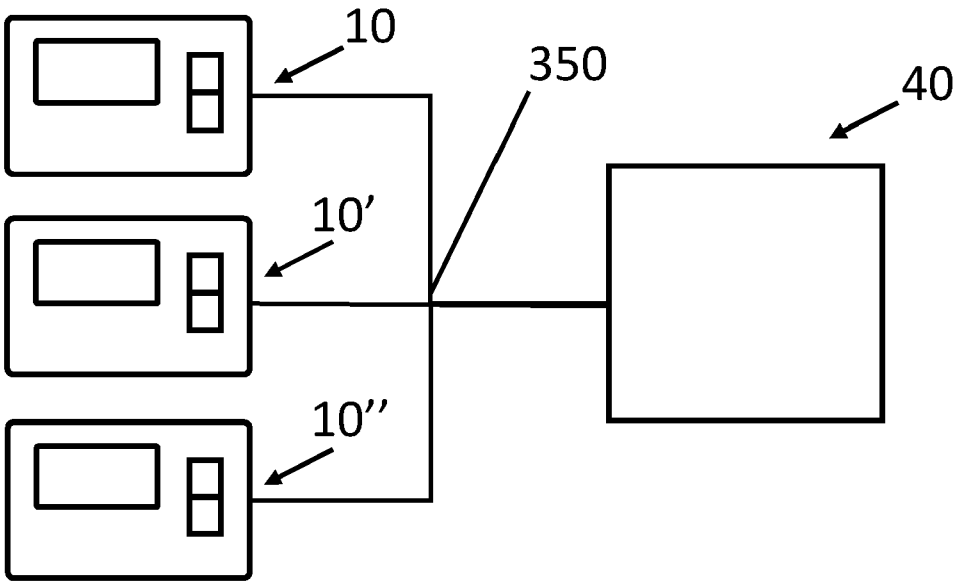


Figure 3

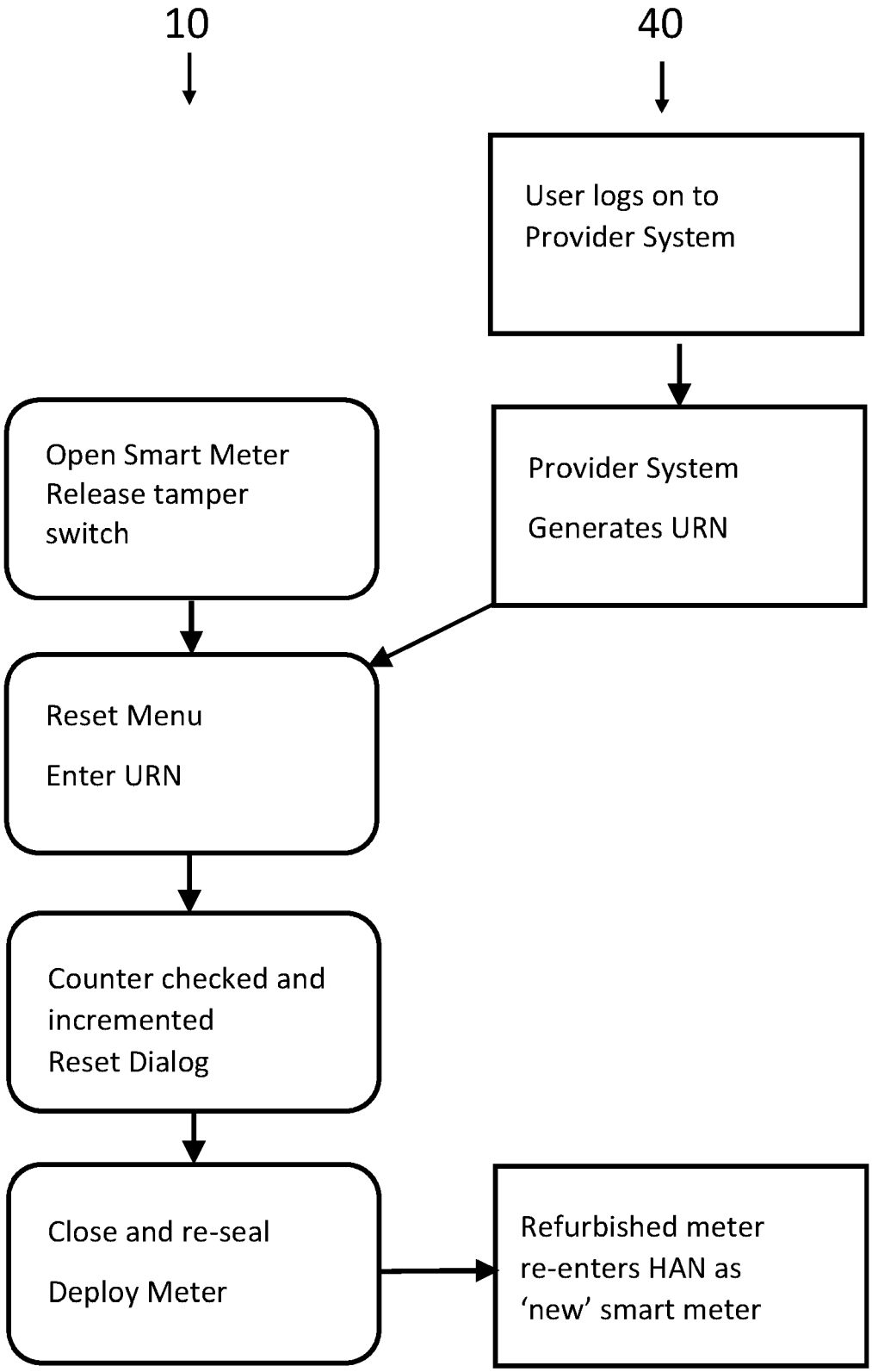
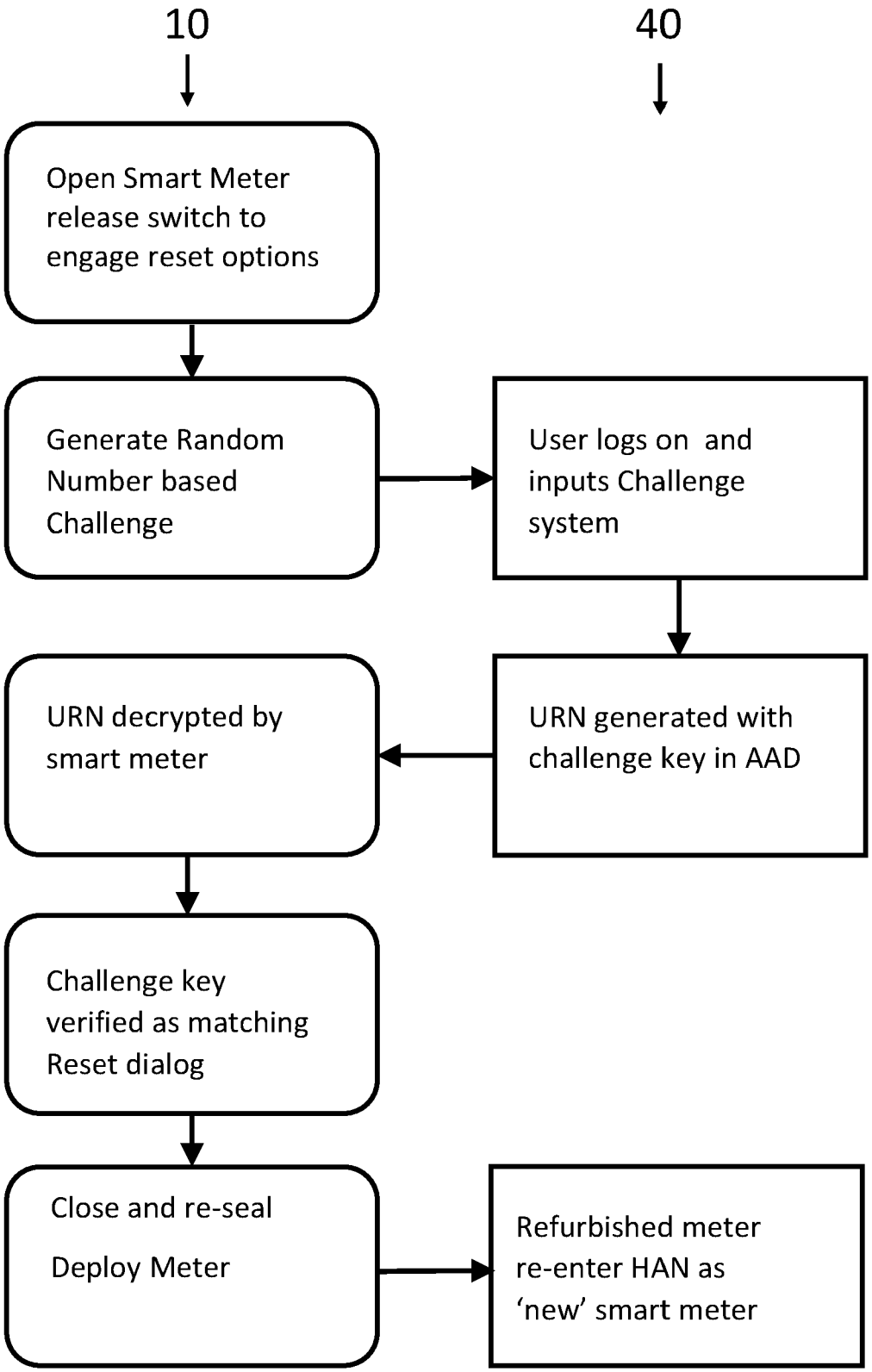

10
40
User logs on to Provider System
Provider System Generates URN
Open Smart Meter Release tamper switch
Reset Menu
Enter URN
Counter checked and incremented Reset Dialog
Close and re-seal
Deploy Meter
Refurbished meter re-enters HAN as 'new' smart meter

Figure 4


10
40
Open Smart Meter release switch to engage reset options
Generate Random Number based Challenge
User logs on and inputs Challenge system
URN decrypted by smart meter
URN generated with challenge key in AAD
Challenge key verified as matching Reset dialog
Close and re-seal
Deploy Meter
Refurbished meter re-enter HAN as 'new' smart meter

Smart Meter Device Refurbishment

The present invention relates to smart energy meters for monitoring the supply of utilities, such as electricity or gas, systems for using those meters and specifically smart meter configuration and use to enable device refurbishment, whilst maintaining security.

Background

A smart meter is an electronic device that records information such as the consumption of electrical energy and is configured to communicate that information to a utility supplier, such as an energy supplier, for example a supplier of gas or electricity.

A smart meter may be an electricity meter, but may for example, measure natural gas, water or heating consumption. Smart meters communicate information to a consumer for monitoring utility usage, and to utility suppliers for system monitoring and customer billing. As such the meters must be secure and communicate securely.

Communication is a critical requirement for smart meters. Each meter must be able to reliably and securely communicate the information collected to a central location. Smart meters typically record energy in real-time, and report regularly, typically throughout the day. This allows utility suppliers to predict consumption according to the time of day and the season. Smart meters enable two-way communication between the meter and a central system. This is termed advanced metering infrastructure (AMI) and differs from automatic meter reading (AMR) in that it enables two-way communication between the smart meter and the supplier's central system. Communications from the meter to the network may be wireless or wired connections such as power line carrier (PLC). Wireless communication types include cellular communications, Wi-Fi (RTM), wireless ad hoc networks over Wi-Fi) RTM, wireless mesh networks, low power long-range wireless l (LoRa (RTM)), Wize (RTM) (high radio penetration rate, open, using the frequency 169 MHz) ZigBee (low power, low data rate wireless), and Wi-SUN (RTM) (Smart Utility Networks). Smart meters may communicate using a number of protocols, for example ANSI C12.18 is an ANSI Standard that describes a protocol used for two-way communications with a smart meter. Other smart meter protocols include IEC 61107 and IEC 62056 used in the European Union. Smart meter developments are constrained by the required to use these formats and to maintain interoperability of equipment between suppliers.

Security controls and assurance arrangements for the End-to-End Smart Metering Systems are defined, for example in the Smart Energy Code (SEC), and aim to provide confidence to all SEC Parties that the systems and devices supporting smart metering are appropriately secure. An appropriate form of secure encryption is therefore required.

Smart metering equipment is evaluated by independent, National Cyber Security Centre (NCSC) accredited Evaluation Facilities (Test Laboratories) before being Commercial Product Assurance (CPA) certified by a NCSC. Only equipment that has been CPA Certified can be included on the Central Product List (CPL) which allows Data Communications Company (DCC, a provider such as a utilities provider) Users to communicate with the equipment. Such standards do not as yet include means for enabling device reset, such as required in refurbishment and this gives rise to undesirable waste as smart meters cannot be re-used

Smart meters may also include functionality so that payments made by a consumer may be used by the meter to govern the supply, an established procedure for this is for supplier to issue a Unique Transaction Reference Number (UTRN) and this may be used to manually add credit to a meter. Such numbers are cryptographically secure and are generated using established protocols. However, they have single purpose and do not interact with system or smart meter hardware to enable it to change its use.

Implementing security protocols that protect smart meters from malicious attacks can be problematic, due to the limited computational resources and long operational life of a smart meter. Also, smart meters expose utility supplies, for example an electricity power grid, to cyberattacks that could lead to power outages, such as by cutting off electricity or by overloading the grid. Smart meter devices are Intelligent Measurement Devices which periodically record the measured values and send the data encrypted to the Service Provider. Communications with a smart meter, using established communication infrastructure and protocols as described above, is typically described as being by a home area network (HAN) of a supplier. Means to avoid purely remote attacks, particularly as regards reset and refurbishment is important to avoid control being seized from outside a HAN.

As an example of smart meter implementation, an example standard is SMETS1 which is the first industry-standard type of smart meter in the United Kingdom and which energy suppliers have been installing since 2013. Such devices and protocols are part of a smart energy code (SEC). This code defines constraints within which devices must operate and this provides a number of technical challenges.

Such first-generation meters have limitations and are been succeeded by SMETS2 smart meters which are cross-compatible with other SMETS2-ready energy suppliers. This means, for example, that if a customer changes supplier there is no need for any meter exchange. However, this opens up the possibility to pass control outside an initial HAN and means to guard against this in reset and refurbishment is required.

Security assurance for SMETS2+ smart meters is provided by ensuring the compliance of smart metering equipment against a set of NCSC Commercial Product Assurance Security Characteristics (SCs). In the United Kingdom the SCs are agreed and updated from time to time in line with SEC Section G 7.19(f) following discussion with industry, Department for Business, Energy & Industrial Strategy (BEIS), NCSC and the SSC.

However, it also means that any authorized person may have access using a common standard to access smart meter data. There is therefore a significant issue regarding smart meter devices and systems infrastructure in that there is a need for interoperability and access by a range of organizations but also a strong need for privacy and security. This is particularly significant when physical access and communication with smart meters to change their functionality during refurbish or repair, which requires a reset of software operation and parameters.

There is therefore a need for improved smart meter security for reset and refurbishment, and in particular whilst maintaining cross-supplier compatibility, such as under a SMETS2+ standard.

Experience of live smart metering operations has given rise to a number of queries, from Device manufacturers, Suppliers, Meter Asset Providers (MAPs) and others, collectively providers, as to whether certain processes to support device triage and refurbishment need changes to the SEC, or the SCs, or whether guidance (agreed by BEIS, NCSC and the SSC) can be adopted.

There is therefore a need such refurbishment and repair use cases to be undertaken securely and consistently.

In terms of smart meter refurbishment this provides an additional complication that the smart meter devices which have completed commissioning, or have been used and therefore had internal parameters changed, and in particular by an provider other than the original provider, need to be accessed and may need to be reset or reprogrammed. Additionally, the smart meter device would have captured, for example, SMETS Operational data during the period when it was operating, including consumption related information and the privacy of this data needs to be respected.

Having been installed, a smart meter must have established communications with a given system, such as a HAN of the utility supplier. Those will no longer be using a factory set Install Code for communications. This means that under established standards (SC) it is unable to join any other HAN. In turn, this means that some changes may have been applied to the Device's initial configuration, as applied during manufacturing. The challenge is to enable this without compromising security. Similarly, the need to triage a device to determine of refurbishment is required.

As can be seen, means or improved means to permit smart meter rest, refurbishment and/or triage is required while respecting the security controls (SC), such as defined in, for example the SEC, are required.

Description

The present invention in its various aspects is as set out in the appended claims.

The present invention provides:

a smart meter (10) for the supply of a utility, the smart meter comprising one or more manual keys (30), such as arranged in a keyboard, and a screen (20) controlled by a processor, which are enclosed in a case, the processor interfacing with the comprising one or more manual keys (30) for input and the screen for output and being connectable in use to a utility system (40) for the exchange of security credentials to govern the operation of the smart meter, the meter, by means of the processor being configured to:

upon input of a Unique Refurbishment Number, URN, the smart meter enters a reset mode in which the internal parameters can be cleared and the meter is reconfigured for deployment

the URN being generated based an identity descriptor of the smart meter and:

i) a cumulative index, such as a number, of the number of times (a counter value) that the meter has been reset or the URN generated such that upon receipt by a supplier system is usable to generate a unique transaction number (URN)

or

ii) a cryptographic key generated by the smart meter and provided by the meter for use by a user the key being such that upon receipt by a supplier system is usable to generate a unique transaction number (URN)

The present invention also provides a method and a system for using that smart meter.

That method in a first manner is as follows:

a user of a smart meter is provided means interact with a provider system to generate a URN – Unique Refurbishment Number specific to the reset process, the user then opens the smart meter case and accesses a reset menu only available upon opening the case, the reset menu requires that the user enter the URN and upon the smart meter successfully validating the URN a reset functionality of the meter is enabled, this enables a reset function of the meter to occur so as to, after reset, enable it to be redeployed freshly onto a home area network, such as of the provider, the case is then closed and resealed and the meter ready for redeployment.

In this manner of the invention the URN has a specific structure in which the number comprises a counter, such as a 6-bit counter, therefore having a limited number of uses to record the number of resets or reset attempts so as to prevent multiple resets (reset attempts). The URN also comprises a provider Message Authentication Code (MAC) for secure authentication.

A second, preferred, method of the invention, is as follows:

a user opens the casing of the smart meter and thereby triggers an alert in the meter that the case has been opened, the user then is enabled to then navigate to a previously unavailable reset menu of the smart meter and that menu provides a challenge code generated by the smart meter, the user then inputs that challenge code to a provider system to generate a URN specific to the reset process, the smart meter reset menu then requires that the user enter the URN and upon the smart meter successfully validating the URN (by means of decryption) reset functionality of the meter is enabled, the case is then closed and resealed and the meter ready for redeployment. This enables a reset function of the meter to be securely accessed so as to enable it to be redeployed freshly onto a home area network, such as of the provider.

The challenge code is a cryptographic challenge key generated by the smart meter. This may be generated ahead of time as it is computationally intensive. If generated ahead of time the challenge code is stored in volatile RAM of the smart meter so that any disconnection of the smart meter to obtain the code would be frustrated by breaking power and thus erasing memory. This provides an additional level of security as it may be required that meter is externally powered and in communication with a HAN, for the challenge key to be calculated, this ensures that the meter removed from a permitted location must be re identified on the HAN for the challenge key to be generated.

In the present invention a user is a person that must be physically present with the meter to carry out at least one step. The user is typically a technician carrying out the refurbishment, such as for the provider.

In the present invention the provider is a generic term to encompass a utility supplier, device manufacturer or third party who provides a system for undertaking the method of the invention in conjunction with the smart meter. The system may be part of a HAN.

The case is described further below and can be thought of as the outside of the smart meter, i.e., it acts as a casing.

The triggering of the alert is further described below and requires a physical switching to take place in the smart meter, such as by means of a detector switch integrated in the casing.

A smart meter reset, is required to be actioned by physical interaction with the meter, this is as opposed to a remote communication such as by ethernet or other communication means. This stops attacks at scale to a HAN and also ensures that smart meter safety is maintained as the user (for example refurbishment technician) will be able to carry out, at least, a visual assessment of the meter. A smart meter reset, a reset, returns a smart meter to the software state of its original manufacture, accumulated data is cleared, access codes are set to enable linking to a fresh HAN and access granted to an installer to enable this to take place. In the first manner of the invention, and optionally the second, the reset will however leave evidence that a reset has taken place, preferably in the form of the counter. By the meter storing the counter value (or equivalent from which the counter can be retrieved) and the provider system retaining the counter value a comparison is possible so as to validate that a smart meter of a given identity, MAC, such as embodied in a serial number the UTN in including this information in cryptographically secure form only decodable by the smart meter enables a check – smart meter counter equals counter from the provider – to ensure that the UTN comes from the (valid source) of the provider before allowing the rest functionality to be accessed.

The counter need not start from zero (as in zero resets) as most meter will be by default in this condition. The counter preferably starts from a random value (c.f. the challenge code) generated by the meter on manufacture and retained by the provider. Preferably, no user may ever be able to access the counter as it need only be exchanged in cryptographically secure form between meter and provider.

In the manner when using the cryptographic challenge key, this may be valid from its generation until a URN is entered. If the URN is incorrect, then the challenge key will be invalid and as such the URN generated will no longer be valid for causing the smart meter to enter reset mode. The smart meets and may be configured that the engagement and release of the detector switch is required, thus terminating case opening, before a further challenge key may be created.

A calculated challenge key may alternatively, or in addition become invalid if the case is closed, as detected by the detector switch being engaged.

Alternatively, or in addition, the processor may start a timer upon creation or display of the challenge key, the smart meter configured to only receive the URN until the timer reaches a threshold time.

One means for providing a level of security is to provide a tamper-proof boundary, such as an enclosure for a smart meter, this is essential but is alone is insufficient and the present invention provides that the boundary (case) must be detected as opened before and reset dialog may take place but also the counter or challenge key process be used to enable that dialog to cause a reset.

In both manners of the present invention upon input of the URN the smart meter enters a reset mode in which the internal parameters may be are cleared and the meter is reconfigured for deployment.

The smart meter may preferably be configured to only receive the URN only for a given period of time after the smart meter triggers the physically initiated (by means of case opening) alert and for which time the challenge key is valid. This prevents replay attacks as the generated URN cannot be used at a later date to reset the meter a second time, for example.

The Smart Meter Case

The smart meter as defined at the beginning of the previous section may be configured such that cumulative index or cryptographic challenge key is only provided by the smart meter upon receipt of a prompt, being a signal provided to the meter such as by means of a switch in the smart meter other than from the key or keys.

The means of for providing which prompt may only available upon opening the case, such as a prompt generated by the switch as configured to detect case opening.

It is preferable that a signal is provided on opening the case (also termed a service cover), such as by means of a detector switch. This provides the benefit that the reset mode may only be entered following opening of the case and therefore the smart meter can only be reset if a user is in situ (i.e. in physical proximity to the smart meter) to open the case, this prevents wide scale online attacks. The case, i.e., a container bounding the functional components of the smart meter may be termed a service cover, as such a service cover encloses rather than just covers.

When refurbishment is completed, the cover may be replaced. Preferably a new cover, or service cover is used. The service cover is preferably a form of case in which removal to access the functional components of the smart meter requires damaging the service cover. The case preferably comprising a reusable case body and a disposable cover to complete the enclosure. The cover is preferably an injection moulded plastics component with a clip fastening to the case body that must be destroyed to access functional components. This provides a hard to replace part for a tamperer to replace. Preferably the cover includes a transparent portion as this makes damage more evident and also enhances the refurbishment by clearing a viewing window. The cover is most preferably the screen of the smart meter (described further below).

The functional components of smart meter include the metering electronics and communications hardware and software in firmware along with the metering mechanism for the utility being metered.

The case may be fitted with a tamper evident seal, such that it will be evident if the case has been opened. This provides an additional level of security preventing reset devices from being passed off as not having been reset. The case, service cover or cover may include that tamperproof seal, such as in the form of an adhesive component with security markings, such as a hologram. A tamperproof seal is a seal which must be broken for accessing the contents, particularly the functional components, of the case.

Case Opening

Upon opening the case the smart meter may be configured to send an alert signal for the supplier system to indicate that the case has been opened. This alert enables the supplier system to keep a record of when the case has been opened (as optionally required as a precursor to or incrementor of the counter). The alert signal may be sent out immediately if the device is connected to a HAN. If the device is not in the HAN the event is queued to send it out when the HAN is available. A subsequent device reset to complete refurbishment may be contingent on the provider having received the alert signal. The alert signal may include a location identity. Only if the location identify conforms to a list of pre-established

(i.e., approved) refurbishment locations may rest be made possible. For example, URN generation by a provider may require an alert signal to have been received. The location identify may be the IP address of a gateway, such as router to which the smart meter is connectable. This provides a simple but effective location check. Even if this is spoofed the likelihood that a tamperer will know the address is minimal. This improves security.

A record of the alert is preferably kept in the smart meter. Hence, in addition or in the alternative, to the sending of the alert signal upon opening the case the smart meter may be configured to register the opening of the case / cover in the smart meter, such as part of an internal event logging. The record is preferably by means of an entry into a non-volatile read-only memory of the meter, this provides an indelible record of the action and may form or act as the counter.

As such two variations are envisaged, counter increment on opening the case, which if nit recorded through the HAN to the provider puts the smart meter and provider counters out of sync and disables reset until communication is restored. Alternatively that case opening is a precursor to counter increment but preferably a necessary precursor. Both variations improve security by supplementing the cryptographic communication with a physical interaction.

In case of reset the device the generated alert may also be reset. However, until then the smart meter may log the alert signal to disable creation of further alert signals (such as to interface with a provider system to generate a URN) and thereby to increase security. Hence the physical interface, such as the case opening switch, becomes a single use actuation. The supplier system will not get an information that the service cover is opened.

In a further feature of the invention, if a prescribed sequence of actions (such as presented herein) is not followed upon case opening then the smart meter optionally prompts the user to enter a postal code or ZIP code of the meter, such as to assert refund of unused payment, and sends this to the Provider as a further alert, preferably in conjunction with an IP address. This assists in tracing the location of a tampered meter. In a preferred feature of the invention, upon the condition to generate an alert signal being achieved, or the signal being sent the smart meter closes the physical gateway for transference of the utility. For gas or water this would be to close a valve, for electricity to disengage a relay or similar.

Detailed Description

The present invention will be described with reference to the following schematic figures in which like features are identified by like numerals and which provide:

figure 1, provides a smart meter for use in the present invention;

figure 2, provides smart meters for use in the present invention interfacing with a secure supplier system, such as a HAN;

figure 3, provides a flowchart of a refurbishment procedure according to the present invention;

figure 4, provides a flowchart of the Challenge process for our dedicating reset of a smart meter according to the present invention.

In the present invention a number of industry abbreviations are used a summary is as follows:

Abbreviation	Explanation
AAD	Additional Authenticated Data
BEIS	Department for Business, Energy & Industrial Strategy
CPA	Commercial Product Assurance
CPL	Central Product List
DCC	Data Communications Company
ESME	Electricity Smart Metering Equipment
GBCS	Great Britain Companion Specification
GMAC	Galois Message Authentication Code
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
KDF	Key Derivation Function
MAC	Message Authentication Code
MAM	Meter Asset Manager
MAP	Meter Asset Provider
MOP	Meter Operator
NCSC	National Cyber Security Centre
SCs	Security Characteristics
SEC	Smart Energy Code
SMETS	Smart Meter Equipment Technical Specifications
SMI	Smart Metering Inventory
SMKI	Smart Metering Key Infrastructure
SSC	Standard Settlement Configurations
UTRN	Unique Transaction Reference Number
URN	Unique Refurbishment Number

Considering now the figures, which are illustrative and schematic:

Figures 1 and 1A provide a schematic of a smart meter 10 (effectively a front panel view) relevant to the present invention. The smart meter comprises a case 12 along with a screen 20 through which a display (not shown) is provided for communicating information to a user. Also included in the smart meter are keys 30 for the selection of options or the input of information, for example the input of a URN. The case 12 encloses the functional components and any tamper switch is not visible or accessible without breaking a seal of the case, such as a service cover component.

As noted, it is highly preferable that any reset procedure, such as part of a refurbishment, requires the physical presence of a user. It is therefore preferable that the URN may only be input by means of the manual switches 30. Whilst the manual switches 30, merely provide electrical signals to the smart meter to evidence of manual input is preferably required for the input to be valid. That evidence of manual input may be by means of the smart meter being configured so that a maximum speed of keypresses is permitted, such as no more than 5 (detected) key presses per second, preferably no more than 2 keypresses per second. In the alternative, but preferably in addition, detected keypresses with uniform intervals are rejected. Uniform interval is an interval which differs by no more than 1 preferably by no more than 10ms between detections, this enables the inherent nonuniformity of person machine interaction is to be harvested to improve security.

Figure 2 shows a plurality of smart meters 10, 10', 10'' as typically incorporated into a home area network, HAN, of a provider and wherein the smart meter interacts by means of communication channels 350 with a provider system 40 to form that HAN. The means of communication 350 may be any suitable means, such as the Internet. In the present invention may be required that the smart meter is connected by communication channels to the centralised system 40 of the provider for at least 1 of, enabling a reset dialogue on the smart meter, generating a challenge code, enabling a reset action to take place. Upon a reset action taking place it is preferable that communication with the provider system 40 sends a message to notify the provider system that it is a centralised system no longer recognises the smart meter. This improves security.

Figure 3 provides a schematic of the first manner of the present invention showing the workflow of the method and the manner in which the system and apparatus operates. On the left-hand side in the round cornered boxes are the actions undertaken by the smart meter 10 (and for which the smart meter is configured to carry out) are shown. On the right-hand side

in the rectangular boxes the actions undertaken by the provider system 40 are shown, and for the whole diagram are actions for which the system as a whole is configured to carry out.

That method, smart meter configuration and system configuration will now be described, in the following steps to disclose the refurbishment/reset method and system use of the present invention from which the smart meter may be configured:

For the first manner of the invention:

Step 1: User logs onto a provider system and enters smart meter details into the URN generation tool.

The smart meter details may comprise an identity descriptor. An identity descriptor is a unique descriptor, such as a serial number of a specific smart meter and serves to uniquely identify that device. Optionally the identity descriptor could include an element representative of the counter (or reset actions).

Step 2: Tool creates one off secure URN

After entering all required information to the tool, and the system validating that the smart meter is present on the system the system generates a unique URN and provides this to the user. The URN and the cryptography are as described below.

Step 3: User opens the case and/or removes Terminal Cover (ESME) or Service Cover (GSME)

By removing the cover, the Device generates a tamper alert and logs a tamper event to an internal security event log. The removed cover further allows access to an additional menu item (`Engineering') on the display that is hidden during normal operation.

Step 4: User navigates to `Reset' sub-menu

The user can navigate through the display menus by using the push button on the device. Entering the `Engineering' menu provides access to an installation specific menu structure that is hidden in normal operation.

A new sub-menu named `Reset' is now available which includes options for reset and refurbishment.

Step 5: Device display requests the URN

On entering the `Reset' menu the Device requests a URN. Preferably this request remains open for a predetermined period of time, such as in the range 5 to 10 minutes before the dialog closes and the URN can no longer be entered.

Step 6: User enters URN in the Device via the pushbutton

Via the pushbuttons (external smart meter controls 30), the user enters the generated URN into the Device.

Step 7: Device starts refurbishment session

On entering the correct URN, the smart meter checks the correct MAC has been received with a valid counter value and starts the refurbishment dialog and provides access to the refurbishment functionality by means of menu options.

Step 8: Device finishes refurbishment session

After finishing the refurbishment session, the Device returns to the same status as of Step 4.

Step 9: User replaces Terminal Cover (ESME) or Battery Cover (GSME)

Replacing the cover, closing any case opening detection switch (the switch). The device is now available for re-installation into a HAN of a provider for normal operation.

The features of steps described elsewhere in this document may be combined with the above steps.

Figure 4 provides a schematic of the second manner of the present invention showing the workflow of the method and the manner in which the system and apparatus operates. On the left-hand side in the round cornered boxes are the actions undertaken by the smart meter 10 (and for which the smart meter is configured to carry out) are shown. On the right-hand side in the rectangular boxes the actions undertaken by the provider system 40 are shown, and for the whole diagram are actions for which the system as a whole is configured to carry out.

That method, smart meter configuration and system configuration will now be described, in following steps to disclose the refurbishment/reset process:

Step 1: User removes Terminal Cover (ESME) or Service Cover (GSME).

By removing the cover, the Smart Meter generates a tamper alert and logs a tamper event to the security event log. The removed cover further allows access to an additional menu item (Engineering) on the display that is hidden during normal operation.

The tamper alert is in the form of a signal sent, or intended to be sent to the Provider. In this case the tamper alert may enable a gateway for generation of a URN code. This ensures that speculative generation of URN code is not possible without starting the reset process.

The tamper alert is preferably generated by means of a physical switch engaged with the terminal cover or service cover structure to remove all the switch is actuated. In addition, a further switch may be present such that upon the tamper alert being evidenced on the smart meter the user must actuate this further switch within a given time period for the process to continue. This avoids a speculative opening of a smart meter to investigate the reset process.

This tamper alert generation optionally starts a countdown timer during which Step 2 (below) is available and after counter timeout is no longer available. This improves security.
The countdown timer is optionally displayed on a display of the Smart Meter.

Step 2: User navigates to `Reset' sub-menu.

The user is provided with the option to navigate through the display menus by using a push button or similar input feature on the device. For the purposes of automation, the input feature may be an automated radio signal to avoid repetitive manual work by the user. Entering the `Engineering' menu provides access to an installation specific menu structure that is hidden in normal operation. Particularly when an automated input is used there is no requirement that any visual indication of the process be provided on the Smart Meter, this improves security. However, the optional result is that a new sub-menu named `Reset' is now available to support the refurbishment use case.

Step 3: Smart Meter displays challenge (a form of access code) for URN generation.

On entering the `Reset' menu the meter generates and shows a challenge for the URN generation on the display. The challenge is a randomly generated number and a necessary input to generate the URN required to enter the refurbishment features of the meter. This feature may also be automated. The challenge is a unique number generated by the smart meter as described below.

Step 4: Use of a URN generation tool.

A URN generation tool is required in the method. URN generation tool is a piece of software, such as made available on a web interface the generation of a URN code. This URN code and its generation are similar, but not the same as the generation of a UTRN code such as used in a smart meter, pay as you go, top up. User enters meter details and challenge into the URN generation tool
The user enters the required meter details and the random number challenge on the display into the URN generation tool.

Step 5: The URN generation tool creates one off secure URN.

After entering all required information to the tool, a unique URN is generated and provided to the user. The URN generation is as described in more detail below.

Step 6: The URN is entered in the smart meter

A preferred method of entering the URN is by means of push buttons on the smart meter itself. However, this process may be automated, for example by means of a radio interface. A radio interface is not preferred as the GSME is joined to a network and therefor the UTRN can send down to the GSME via this interface. Acritical point here is that a GBCS tunnel might not be available and a telegram outside of GBCS could allow to transfer the URN.

Step 7: The smart meter enables refurbishment features

The smart meter may enable the refurbishment features by means of displaying options on a screen for example for the purposes of selection by manual input of keys on the meter. Whether manual or automatic entering the URN successfully provides access to a display menu, making available (for example by listing) the refurbishment features, that his actions which may be carried out for the purposes of refurbishment such as clearing a memory and

the initializing variables. In a typical refurbishment the user is now able to step through the refurbishment menu items and select individual reset features to be executed by the meter. A significant advantage of the URN use is that the system providing a UTRN depends on the input. The resulting URN includes the permissions of action and therefore a reset of the smart meter can execute immediately, direct after the UTRN input via the user interface, i.e., a key or keys, such as arranged in a keyboard.

Step 8: Meter exits the `Reset' menu

Exiting the `Reset' menu is possible by either user choice or inactivity timeout. In doing so the meter returns to the reset menu of Step 2. The refurbishment session may finish by closing the local communication session using the rest menu or due to an inactivity timeout.

Step 9: User replaces Terminal Cover (ESME) or Service Cover (GSME)
Replacing the cover again for setting the meter back into normal operation. The switch used for actuating the tamper alert is re-engaged and this completes the refurbishment process.

The features of steps described elsewhere in this document may be combined with the above steps.

With taking the Device out of normal operation and allowing access to the refurbishment functionality in a CPA compliant way, several options of executing the refurbishment use cases are possible. Even combinations of several option might be possible if required.

Starting the refurbishment session would preferably be at step 7 see figures 3 and 4.

Finishing the refurbishment session is represented by step 8 of the same.

A refurbishment session, as a component of the whole process, may comprise one or more of:

URN implicit reset

In this scenario the refurbishment actions are pre-defined and automatically executed as soon as the URN has been successfully validated by the Smart meter.

The refurbishment session is started and finished immediately after executing the reset actions as there are no further activities necessary.

URN specific action

In the case of URN specific action, the instruction of which refurbishment action is executed, e.g., reset alarm and/or logs, activate a download firmware. The action is automatically executed as soon as the URN has been successfully validated by the Smart meter.

The refurbishment session is started and finished immediately after executing the individual action.

A new URN can be entered for any further individual action.

Refurbishment display menu

In this case entering the correct URN starts the refurbishment session and provides access to a display menu, listing the individual refurbishment features. The user is now able to step through the refurbishment menu items and select individual reset actions to be executed by the smart meter.

The refurbishment session finishes by either user choice or inactivity timeout.

Refurbishment by communication interface

Referring to mentioned CPA security characteristics, non-operational logical and physical interfaces must not be accessible during normal operation. Taking the Smart meter explicitly out of normal operation in a CPA compliant way relieves the restriction on providing access via non-operational interfaces.

One or more of the following options on non-operational interfaces might be supported.

Enabling physical communication interface. In this case, entering the correct URN starts the refurbishment session and allows access to a local communication interface. All further refurbishment actions are executed via this local interface in a local communication session.

The local communication session must be started within the inactivity timeout period.

The refurbishment session finishes by closing the local communication session or inactivity timeout.

Enabling side protocol on existing communication interface. In this case, entering the correct URN starts the refurbishment session and allows via a proprietary telegram the communication via the RF communication interface.

The invention may include the following refurbishment functionality:

- update the existing GBCS certificates with the respect of the GBCS specified security mechanism, but manufacturer specific
- firmware update can be executed in a faster way as only via pure ZigBee
- reading and resetting of alarms and logs

The refurbishment session finishes by closing the communication via RF or an inactivity timeout.

Enabling manufacturer specific GBCS tunnel messages. In this case, entering the correct URN starts the refurbishment session and allows manufacturer specific GBCS messages. The meter is first joined into a ZigBee (RTM) network with the security credentials from manufacturer leave.

The manufacturer specific GBCS messages are used for the following refurbishment functionality:

- update the existing GBCS certificates with the respect of the GBCS specified security mechanism, but manufacturer specific
- firmware update can be executed in a faster way as only via pure ZigBee (RTM)
- reading and resetting of alarms and logs

The refurbishment session finishes by sending a close tunnel message or an inactivity timeout.

The invention is a system or is part of a system using a upon a predefined cryptographic scheme, and which is carried out or is capable of carried out as shown in the step shown below.

The provider preferably carries out all steps outside those described for the meter itself. The term user is an identifier for a person interacting with the meter, typically a maintenance technician of the provider.

The precursor steps to the method are as follows:

A. Provide a Smart Meter for monitoring a Utility, for example Gas or Electricity supply. This may be a commercial or domestic supply. Before distributing a new Smart meter for an end use, such as in an installation:

B. Receive and store in the smart meter, the remote party's static public key

C. Receive and store in the smart meter, required assurance for remote party's static public key

Steps B and C may be completed through the use of cryptographic Certificates.

The provider system may first check if the smart meter is registered as part of the HAN before issuing the URN.

The provider system may also, first check if the smart meter is disconnected from the HAN before issuing the URN as no meter in active function should be physically open, such as required during the reset/refurbishment procedure.

The checks may both be used.

The Smart Meter will then be typically distributed to an installation location and be used for its function of metering utility.

At some point it may then be determined that the Smart Meter requires resetting or refurbishment. The Smart Meter will then usually be disconnected from communication with the Provider and taken to a facility for reset/refurbishment where it may optionally be reconnected for communication with the Provider for example in the manner of restarting communication after a network outage of the HAN. However. A significant issue is that the Provider HAN may be lock out the smart meter from communications upon detecting removal. As such the present invention can avoid this problem by using a web portal and the

generation of a URN to enable the option for re-establishing communications by means of resetting the smart meter so that it may be re-introduced into a HAN. such as for fresh install of a refurbished meter.

5

Generation of the URN

As described above, the present invention utilises a Unique Refurbishment Number (URN) for the purposes of enabling the resetting of a smart meter for the purposes of refurbishment or repair and specifically for the purposes of resetting the smart meter to an initial condition for fresh installation in the manner of any `new' installation of a smart meter.

The present invention preferably generates a URN using cryptographic standard as set out in a GBCS standard, preferably V4.0 specification [A].

The most preferred cryptographic basis for generating a URN, which is applied in the present invention in a new manner, is as follows. The GMAC technique is used. This is based on the use of AES-128, for the calculation of Message Authentication Codes (MACs), as specified in NIST Special Publication 800-38D; this technique is used, to calculate Shared Secret (`Z') as required by the technique. In a preferred feature the shared secret is calculated using the Static Unified Model, C (0e, 2s, ECC CDH) Key Agreement technique to calculate Shared Secret (`Z') as required by the Single-step Key Derivation Function (KDF)

Further the Static Unified Model, C (0e, 2s, ECC CDH) Key Agreement technique (as specified in NIST Special Publication 800-56Ar2 is used, preferably with a requirement to zeroize the Shared Secret) with the Single-step Key Derivation Function (KDF) based on SHA-256, as specified in NIST Special Publication 800-56Ar2; and the P-256 curve for the elliptic curve operations.

The use of this technique is particularly appropriate for the processing power available in a smart meter as it provides a high level of security, appropriate to the value of the asset being protected whilst being within the processing power of a microcontroller.

Specifically, using the symmetric Algorithms like AES-128 or AES-256 (that is 128bit and 256bit respectively) is preferred.

Further referred is the use of Public Key cryptography using Elliptic-curve cryptography. This is beneficial as it utilises relatively small key lengths. Preferably the public key is generated using the P-256 curve, with a key length of 256bits.

Whilst this level of calculation takes time it has been found as an optimal balance between computational time and security.

The present invention uses a message authentication code (MAC) this code may be generated in one of two ways:

A first Option with a MAC based on 32bits and further include a counter against replay attack (increases number of URN digits) with optional spare fields info for future extension (increases number URN of digits)

A Second Option with a MAC based on 32bits and further includes a challenge key generated by the smart meter with optional spare fields info for future extension (increases number URN of digits)

URN structure

Preferred URN code structures for use in the present invention are as follows.

Preferred URN code structures, for the first manner:

Component	Value	Bits	Note
Lead	0b00	39-38	Fixed value (reserved for future options)
Counter	6 bits originator counter	37-32	used for protections against replay purposes
Provider MAC	32 least significant bits of the 128bit Provider MAC produced by the MAC calculation.	31-0	The Device shall calculate the MAC, then ensure the 32 least significant bits of the 128bit MAC produced by the MAC calculation has the same value as the Provider MAC

Lead: 2 bits (0 – 3)

Allows for future extensions in the usage of this feature

Currently fixed to 0b00 (others reserved)

Counter: 6 bits (0 – 5)

Protection against replay attack

- next counter value mast be exactly current value +1

- wrap around at 63

Counter value on the display when RESET menu is show. No need to keep track in database.

Provider MAC: 32 bits (0 – 31)

32 least significant bits of the 128bit Provider MAC produced by the MAC calculation.

Preferred URN code structures, for the second manner:

In the second manner the case of the challenge-based replay protection, the protective information is already provided by the Device itself and doesn't need adding to the URN information anymore. This limits the URN structure to include only the MAC.

Component	Value	Bits	Note
Provider MAC	32 least significant bits of the 128bit Provider MAC produced by the MAC calculation.	31-0	The Device shall calculate the MAC, then ensure the 32 least significant bits of the 128bit MAC produced by the MAC calculation has the same value as the Provider MAC

Provider/Provider MAC: 32 bits (0 – 31)

32 least significant bits of the 128bit Provider MAC produced by the MAC calculation as defined in 3.4.3.

Entering the URN to the Device is preferably [performed using the display and the pushbuttons.

Based on the above 32bit structure of the URN, the following options are preferred:

1. Entering the URN as a 10-digit decimal representation of the 32bit value
   10 decimal digits, ranging from 00000 00000 - 42949 67295
2. Entering the URN as an 8-digit hexa-decimal representation of the 32bit value
   8 hexa-decimal digits, ranging from 0000 0000 – FFFF FFFF
   This is preferred as it requires fewer key entries.

3. Entering the `x' last significant digits of the URN based on 10 digit decimal representation of the 32bit value.
    - `x' = 3 decimal digits, ranging from 000 – 999, or
    - `x' = 4 decimal digits, ranging from 0000 – 9999, or
    - `x' = 5 decimal digits, ranging from 00000 – 99999, or
    - ....

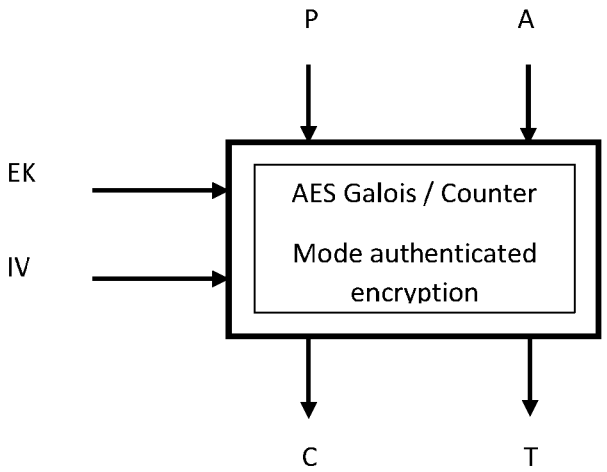
Optionally the URN may be limited to 16bit, as a Brute Force (many repeated attempts) attack via display and pushbuttons is not realistic.

Using a 16bit (16 least significant bits of the 128bit Provider MAC produced by the MAC calculation) still reduces the chances to guess the correct URN to 1: 65535, which might be an acceptable level for this a smart meter.

Calculation of the MAC using GMAC

The calculation of the MAC in the present invention is preferably based on the AES-128 Galois/Counter Mode (GCM). The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. GCM is defined for block ciphers with a block size of 128 bits.

Galois Message Authentication Code (GMAC) is an authentication-only variant of the GCM which can form an incremental message authentication code. Schematically



Scheme 1

The authenticated encryption function has four input strings:

EK is the Encryption Key or Shared Key (see 3.4.2)

IV is the Initialization Vector (see 3.4.4.4)

P is the Plaintext (see 3.4.4.5)

A is the Additional Authenticated Data (AAD) (see 3.4.4.6)

The authenticated encryption function has two output strings:

C is the Ciphertext whose bit length is the same as that of the plaintext *P*

T is the Tag (128-bit authentication tag) or MAC

URN Generation parameters

Identifiers / System-Title

The identifiers used on the generation of the URN and the calculation of the MAC in the present invention preferably follow the definition of chapter 4.3.1.1 Identifiers in the GBCS V4.0 specification [A]. The section defines the Entity Identifiers to be an octet string of length 8 and unique across GB Smart Metering.

If that specification is used then following interpretation is used in the URN generation process:

- *Business Originator ID* => also referred to as *originator-system-title*
  Entity Identifier for the Known Provider which is requesting generation of the URN
- *Business Target ID* => also referred to as *recipient-system-title*
  Entity Identifier for the Device that the Provider wants to action generated URN

Cryptographic setup

In the present invention a preferred cryptographic setup of the invention, method system or device is as follows:

The provider, whose Security Credentials are stored in the target Device, shall calculate a Message Authentication Code using the defined parameters, then setting the Message Authentication Code to be the 32 least significant bits of the 128bit Message Authentication Code produced by the Message Authentication Code calculation.

First a shared secret is generated during the execution of a key-establishment scheme such as specified in SP 800-56A or SP 800-56B

A single step key function is then used, for example as defined in NIST 800-56C Rev1

The Single Step KDF specifies a family of approved key-derivation functions (KDFs) that are executed in a single step; The input to each specified KDF includes the shared secret generated during the execution of a key-establishment scheme, such as mentioned as specified in SP 800-56A or SP 800-56B, an indication of the desired bit length of the keying material to be output.

Implementations of these one-step KDFs depend upon the choice of an auxiliary function H, which can be either:

1. an approved hash function, denoted as hash, as defined in FIPS 180 or FIPS 202;

2. HMAC with an approved hash function, hash, denoted as HMAC-hash, and defined in FIPS 198; or

3. a KMAC variant, as defined in SP 800-185. H shall be chosen in accordance with the selection requirements specified in 800-56C Rev1/Section 7.

When an approved MAC algorithm (HMAC or KMAC) is used to define the auxiliary function H, it is permitted to use a known salt value as the MAC key. In such cases, it is assumed that the MAC algorithm will satisfy the following property (for each of its supported security strengths):

A number of actions are attributed to the smart meter in this document. It is to be understood that these will be carried out by the functional components of the meter. For example, a microcontroller or other processor. The functional components are known in the art and the present invention is to the interaction, set-up and configuration of those components, either alone or as part of a Provider system (termed a HAN).

The smart meter disclosed also comprises apparatus to meter and control supply of the utility.

An identity descriptor is a unique descriptor, such as a serial number of a specific smart meter and serves to uniquely identify that device.

In the present invention the cumulative index or the cryptographic challenge key terms can also refer to a signal or data which comprises that information.

The cryptographic challenge key herein may also be referred to as the challenge key.

The term `based on' can be interpreted to mean provided as a specific piece of information.

Claims

1. A smart meter (10) for the supply of a utility, the smart meter comprising one or more manual keys (30) and a screen (20) controlled by a processor, which are enclosed in a case, the processor interfacing with the one or more manual keys (30) for input and the screen for output and being connectable in use to a utility system (40) for the exchange of security credentials to govern the operation of the smart meter, the meter, by means of the processor being configured to:
upon input of a Unique Refurbishment Number, URN, the smart meter enters a reset mode in which the internal parameters can be cleared and the meter is reconfigured for deployment
the URN being generated based an identity descriptor of the smart meter and:

i) a cumulative index, such as a number, of the number of times (a counter value) that the meter has been reset or the URN generated such that upon receipt by a supplier system is usable to generate the URN
or

ii) a cryptographic challenge key generated by the smart meter and provided by the meter for use by a user the key being such that upon receipt by a supplier system is usable to generate the URN.

2. The smart meter of claim 1 wherein the meter is configured such that cumulative index or cryptographic challenge key is only provided by the smart meter upon receipt of a prompt being a signal provided to the meter such as by means of a switch in the smart meter other than from the key or keys.

3. The smart meter of claim 2 wherein the means of for providing which prompt is only available upon opening the case, such as a prompt generated by the switch as configured to detect case opening.

4. The smart meter of any of claims 1, 2 or 3 wherein the cryptographic key is based upon a random number generated by the processor and decryption of the URN by the smart meter confers the random number to the decryption and requires a much for entering the reset mode.

5. The smart meter of any preceding claim wherein the URN is constructed from a series of underlying parameters those underlying parameters in the form of a method authentication code (MAC) the parameters being selected from one or more of:

a) a counter for the number of URN codes issued for the device

b) a code unique to the supplier for which the smart meter was previously installed

c) the cryptographic challenge key

6. The smart meter of any preceding claim wherein the smart meter is configured to only receive the URN number during a predefined time period in which the cryptographic challenge key is defined as being valid.

7. The smart meter of any preceding claim wherein the challenge key is valid from its generation until a URN is entered.

8. The smart meter of any preceding claim wherein the challenge key is invalidated in response to the cover being closed.

9. The smart meter of any preceding claim wherein the processor starts a timer upon creation or display of the cryptographic challenge key and the smart meter is configured to only receive the URN until the timer reaches a threshold.

10. The smart meter of any preceding claim wherein the case is fitted with a tamper evident seal.

11. The smart meter of any preceding claim wherein the smart meter is configured to send a signal to the supplier system in response to the case being opened.

12. The smart meter of any preceding claim wherein the smart meter is configured to send a signal to the supplier system in response to the case being opened.

13. The smart meter of any preceding claim wherein the URN comprises a MAC and Additional Authenticated data, AAD, wherein the AAD includes at least the cryptographic challenge key.

14. The smart meter of any preceding claim being configured to carry out a method having the steps:

prompting the smart meter to display the challenge key;

providing the challenge key to the supplier system to generate a URN;

inputting, by the one or more manual keys (30) the URN into the smart meter causing the smart meter to enter the reset mode;

resetting internal parameters of the smart meter.

15. A system comprising the smart meter according to any preceding claim and a provider system, the provider system being configured to provide a portal to receive the cumulative index or the cryptographic challenge key and in response, generate a URN.

16. The system of claim 1 wherein i) cumulative index or ii) cryptographic challenge key is used to generate the URN such that upon decryption of the URN by the smart meter the i) cumulative index or ii) cryptographic challenge key respectively is recovered for comparison against the equivalent value stored in the meter and only if a match is obtained is a reset made available.

17. The system of claim 2 wherein the system utilises a cryptographic shared secret calculated using the Static Unified Model.

18. The system of any of claims 15 to 17 wherein the provider system first checks of the smart meter is registered as part of the HAN before issuing the URN.

19. The system of any of claim 19 wherein the provider system first checks of the smart meter is disconnected from the HAN before issuing the URN.

20. The system of any of claims 15 to 18 wherein a i) cumulative index or ii) cryptographic challenge key is only provided by the smart meter upon receipt of a prompt being a signal provided to the meter such as by means of a switch in the smart meter other than from the key or keys and upon receipt of that prompt an alert is sent to the provider system, the provider system being configured to provide no URN until that alert is received.

21. A method for use with the smart meter of any preceding claim with feature i) the method comprising the following steps:

Step 1: User logs onto a provider system and enters smart meter details into the URN generation tool.

Step 2: Tool creates one off secure URN

Step 3: User opens the case and/or removes Terminal Cover (ESME) or Service Cover (GSME)

Step 4: User navigates to `Reset' sub-menu

Step 5: Device display requests the URN

Step 6: User enters URN in the Device via the pushbutton

Step 7: Device starts refurbishment session

Step 8: Device finishes refurbishment session

Step 9: User replaces Terminal Cover (ESME) or Battery Cover (GSME)

22. A method for use with the smart meter of any preceding claim with feature ii) the method comprising the following steps:

Step 1: User removes Terminal Cover (ESME) or Service Cover (GSME).

Step 2: User navigates to `Reset' sub-menu.

Step 3: Smart Meter displays challenge (a form of access code) for URN generation.

Step 4: Use of a URN generation tool.

Step 5: The URN generation tool creates one off secure URN.

Step 6: The URN is entered in the smart meter

Step 7: The smart meter enables refurbishment features

Step 8: Meter exits the `Reset' menu

Step 9: User replaces Terminal Cover (ESME) or Service Cover (GSME)