

## SYSTEM AND METHOD FOR PAIRING A UTILITY METER WITH A REMOTE DISPLAY MODULE

### Technical field

5

The invention relates to a system for pairing an electric meter with a remote display module, and an associated method of pairing an electric meter with a remote display module.

### 10 Background

Metering devices are used to measure the consumption of a utility at residential or commercial premises. Metering devices may comprise, for example, electric metering devices for measuring the consumption of electrical power, water metering devices for  
15 measuring the consumption of water, or gas metering devices for measuring the consumption of gas, etc.

In some arrangements, the metering devices may be inaccessible to the owner of the residential or commercial premises. For example, centralised metering devices, such  
20 as centralised electricity metering devices, may be used to prevent energy theft in high-risk areas. In such arrangements, the metering devices may be located external to the premises and within a secure cabinet to minimise the risk of unwanted tampering.

The metering devices within the secure cabinet may be in wireless communication with  
25 corresponding remote display modules, which are located at the premises to which the utility is supplied (e.g. electrical power, water or gas). Therefore, utility consumption data may be provided to the remote display modules, which are accessible to the owners of the premises, from the metering devices which are inaccessible to the owners of the premises.

30

To further minimise errors and/or fraudulent action (e.g. energy theft), the remote display modules associated with the metering devices may be required to only accept  
communications from a metering device that is authorised. An authorised metering  
device may be one that is securely paired with the corresponding remote display  
35 module. In the context of this application "pairing" refers to a process by which the

metering device and the corresponding remote display module may form a communications link or other relationship so that data may be exchanged therebetween. Once the pairing process is completed, the metering device and the corresponding remote display module are said to be “paired”.

5

Typically, a field technician would visit the relevant site in order to securely pair a metering device with its corresponding remote display module. However the field technician is unlikely to know which metering device should be paired to which remote display module prior to visiting the relevant site. As such, in existing pairing methods, multiple pairing payloads (or packets) comprising the relevant metering device information and remote display module information to allow pairing thereof are created and stored within a pairing tool for use by the field technician in pairing a metering device to the relevant remote display module. The multiple pairing payloads created comprise every possible combination of the metering devices with the available remote display modules. The pairing payloads that are not relevant are then discarded. For example, if there are ten metering devices and ten remote display modules, one hundred pairing payloads are created and stored within the pairing tool, however only ten of those pairing payloads would be used. The remaining ninety pairing payloads would be discarded.

20

This creates a limit on how many pairings can be facilitated during a site visit, as pairing tools can only accommodate a finite number of pairing payloads, dependent on their memory capacity. The process of creating the multiple pairing payloads also places memory and processing demands on the system.

25

A more efficient way of securely pairing a metering device and a remote display module is needed.

**Summary**

30

According to the invention in a first aspect, there is provided a method of pairing a metering device with a remote display module, the method comprising: storing a pairing public key of an asymmetric key pair in a memory of the metering device and a memory of the remote display module; communicating to the metering device and the remote display module, a temporary public key of a temporary asymmetric key pair, the temporary public key signed using a pairing private key of the asymmetric key pair;

35

authenticating, by the metering device and the remote display module, the temporary public key, using the stored pairing public key; communicating to the metering device and the remote display module, a pairing request signed using a temporary private key of the temporary asymmetric key pair, wherein the pairing request comprises a meter public key of a meter asymmetric key pair; authenticating, by the metering device and the remote display module, the pairing request using the authenticated temporary public key; and storing the meter public key in the remote display module.

Optionally, following authentication of the temporary public key by the metering device and the remote display module, the method comprises temporarily storing the temporary public key in the metering device and the remote display module.

Optionally, the method further comprises deleting the temporary public key from the metering device and the remote display module once the metering device and the remote display module have been paired.

Optionally, the method further comprises deleting the temporary public key from the metering device and the remote display module on expiry of a predetermined time period.

Optionally, the meter further comprises sending a command to the metering device and the remote display module instructing the metering device and the remote display module to use the temporary public key to authenticate the pairing request and not the pairing public key.

Optionally, a pairing tool transmits the temporary public key signed using the pairing private key to the metering device and the remote display module.

Optionally, the method further comprises transmitting, by the pairing tool and to the metering device, a request for the meter public key; and receiving, by the pairing tool and from the metering device, the meter public key for use in the pairing request.

Optionally, the pairing tool generates the pairing request and signs the pairing request using the temporary private key, and transmits the pairing request signed by the temporary private key to the metering device and the remote display module.

Optionally, the method further comprises the preceding step of: generating, by the pairing tool, the temporary asymmetric key pair.

5      Optionally, the method further comprises transmitting, from the pairing tool and to a remote device, a request for the remote device to sign the temporary public key using the pairing private key; signing, by the remote device, the temporary public key using the pairing private key; and receiving, by the pairing tool and from the remote device, the temporary public key signed using the pairing private key.

10     Optionally, the pairing request further comprises a unique identifier of the remote display module and/or a unique identifier of the metering device.

15     Optionally, the pairing public key is stored in the metering device and the remote display module before installation or during manufacture of each of the metering device and the remote display module.

20     According to the invention in a further aspect, there is provided a system for pairing a metering device with a remote display module, the system comprising: the metering device comprising a memory within which a pairing public key of an asymmetric key pair is stored; and the remote display module comprising a memory within which the pairing public key is stored, wherein the metering device and the remote display module are configured to: receive a temporary public key of a temporary asymmetric key pair, the temporary public key signed using a pairing private key of the asymmetric key pair; authenticate the temporary public key using the stored pairing public key;

25     receive a pairing request signed using a temporary private key of the temporary asymmetric key pair, wherein the pairing request comprises a meter public key of a meter asymmetric key pair; and authenticate the pairing request using the authenticated temporary public key, wherein the remote display module is further configured to store the meter public key.

30     Optionally, the system further comprises a pairing tool, the pairing tool configured to: transmit the temporary public key signed using the pairing private key to the metering device and the remote display module; generate the pairing request and sign the pairing request using the temporary private key; and transmit the pairing request to the

35     metering device and the remote display module.

Optionally, the pairing tool is further configured to generate the temporary asymmetric key pair.

5 Optionally, the system further comprises a remote device configured to: generate the asymmetric key pair comprising the pairing public key and the pairing private key; receive, from the pairing tool, a request to sign the temporary public key using the pairing private key; and transmit, to the pairing tool, the temporary public key signed using the pairing private key.

#### 10 **Brief description of drawings**

Figure 1 is a block diagram showing an exemplary system;  
Figure 2 is a sequence diagram showing a method of preparing a pairing tool to facilitate pairing of a metering device with a corresponding remote display module; and  
15 Figure 3 is a sequence diagram showing a method of pairing a metering device with a corresponding remote display module.

#### **Detailed description**

20 Figure 1 is a schematic, or block, drawing of a system 100 for pairing a metering device with a remote display module. The system 100 may be a utility metering system. The system 100 comprises a plurality of metering devices 102a-n, a plurality of remote display modules 104a-n, a pairing tool 106 and a head end system 108 (also referred to as a remote device herein).

25 The plurality of metering devices may comprise electric metering devices, gas metering devices, water metering devices etc. For the purposes of this example, the metering devices 102a-n comprise electric metering devices for measuring electrical power consumption at an associated premises, however the skilled person will appreciate that  
30 in alternative arrangements, the metering devices may be for measuring consumption of a different utility.

In the arrangement shown in Figure 1, the metering devices 102a-n are located within an enclosure 110 that prevents unauthorised access to the metering devices 102a-n,  
35 such as a secure cabinet. The skilled person will appreciate however that in alternative arrangements, the metering devices may not be located within such an enclosure 110.

Typically, however, the metering devices 102a-n are inaccessible to both the owner of the premises in which consumption is measured and unauthorised users to prevent tampering with the metering devices 102a-n and/or energy fraud.

5     The metering devices 102a-n may communicate with other devices of the system, for example one or more of the remote display modules 104a-n, the pairing tool 106 and the head end system 108 using a communications module 112. The communications module 112 may comprise a Network Interface Card, NIC, as depicted in Figure 1. The metering devices 102a-n may be coupled to the communications module 112 via a  
10    processor 114, such as a CPU.

An antenna 116 is also depicted in the example arrangement of Figure 1. The antenna is configured to facilitate radio frequency, RF, communications between the metering devices 102a-n and the remote display modules 104a-n (for example, via the  
15    communications module 112). Although the antenna 116 is depicted as a single antenna in the schematic view of Figure 1, the skilled person will appreciate that in practice, more than one antenna may be used. Furthermore, in alternative arrangements, each metering device 102a-n may comprise its own receiver and/or transmitter such that each metering device can receive and/or transmit data  
20    individually.

As can be seen in Figure 1, each remote display module 104a-d comprises a respective antenna for receiving data/communications from at least one metering device 102a-n, via the antenna 116. In exemplary arrangements, the remote display  
25    devices 104a-n may be configured as a receiver only, and not configured to transmit data.

In use, each remote display module 104a-d is configured to accept data/communications, such as radio packets, from an authorised metering device only.  
30    An authorised metering device may comprise a metering device 102a-d that is paired with the corresponding remote display module 104a-d. Each metering device 102a-n may be paired to a corresponding remote display module 104a-n using the method outlined in more detail below.

35    The system 100 further comprises the pairing tool 106 configured to facilitate pairing of each metering device 102a-n with a corresponding remote display module 104a-n.

The pairing tool 106 may be (or may comprise) a software product, e.g. a program installed on a computer or smart device. The pairing tool 106 may be used by a field engineer during a process of installation or maintenance of a remote display module 104a-n and/or electric meter 102a-n. The pairing tool 106 is configured for communications, for example RF communications and/or wireless communications via the internet or the like, with the metering devices 102a-n and the remote display modules 104a-d, and may comprise a transmitter and/or receiver to facilitate such communications.

The system 100 further comprises the head end system 108. The head end system 108 may be a server, a cloud based device or other remote device. The pairing tool 106 is configured to transmit data to and/or receive data from the head end system 108.

A method of pairing a metering device 102a-n with a corresponding remote display module 104a-n is described below with reference to Figures 2 and 3.

Figure 2 depicts a sequence diagram of a method of preparing a pairing tool to facilitate pairing of a metering device with a corresponding remote display module.

202: The head end system 108 generates an asymmetric key pair comprising a pairing public key and a pairing private key (which also may be referred to as a pair of utility asymmetric keys comprising a utility public key and a utility private key).

The skilled person will be familiar with the field of asymmetric cryptography and asymmetric keys. In summary, an asymmetric key pair comprises a public key and a corresponding private key. The public key may be used to encrypt data and only the intended recipient (who holds their own private key) can decrypt the data. The public key may be used to verify signatures applied by a corresponding private key. The private key may be used to decrypt incoming data, and/or to digitally sign outgoing data to authenticate the outgoing data (i.e. confirm the entity from which the outgoing data originates). Further detail is not provided, since as mentioned above, the skilled person will be familiar with the field of asymmetric cryptography.

In the example embodiment of Figure 2, a utility 120, which may be a utility provider, sends a command to the head end system 108 to generate the asymmetric key pair. The head end system 108 may comprise processing circuitry configured to execute instructions to generate the asymmetric key pair.

5

204: The pairing public key is stored in each metering device 102a-n and each remote display module 104a-n. The pairing public key may be used by the metering devices 102a-n and the remote display modules 104a-n to verify data/communications signed using the pairing private key.

10

In the arrangement depicted in Figure 2, the pairing public key is provided to a manufacturer/manufacturing user 122, for example by the utility 120 or the head end system 108, and stored in each metering device 102a-n and each remote display module 104a-n by the manufacturing user 122 during a process of manufacture, installation or programming of each metering device 102a-n and each remote display module 104a-n. As depicted in Figure 2, the pairing public key may be injected into, that is programmed into an internal memory of, each metering device 102a-n and each remote display module 104a-n. The pairing public key may be stored within a non-volatile memory of each of the metering devices 104a-n and each of the remote display modules 104a-n.

15

20

206: The pairing tool 106 generates a temporary (or ephemeral) asymmetric key pair comprising a temporary public key and a temporary private key. The skilled person will understand that temporary asymmetric key pair is configured for use in a specific transaction or communication session and then discarded after the intended use. In this case, the pairing tool 106 generates a temporary asymmetric key pair for use in the pairing process. Once the pairing process is completed, the temporary asymmetric key pair is deleted.

25

30

The pairing tool 106 may comprise processing circuitry configured to execute instructions to generate the temporary asymmetric key pair. The pairing tool 106 may be instructed to generate the temporary asymmetric key pair by a field technician, for example, who is responsible for undertaking the pairing process.

35

208: The pairing tool 106 sends a request to the head end system 108 for the temporary public key to be signed using the pairing private key (previously

generated by the head end system 108 in step 202). The request may be sent by the transmitter of the pairing tool 106, using wireless communications, or alternatively, the pairing tool 106 may be connected to the head end system 108 using a wired connection for communications therebetween.

5

210: In response to the request received from the pairing tool 106, the head end system 108 signs the temporary public key using the pairing private key. As described above, the pairing private key was generated by the head end system 108 in step 202 of this example.

10

The head end system 108 may send the signed temporary public key to the pairing tool 106 for storing in a memory of the pairing tool 106 for use in pairing a metering device to a corresponding remote display module.

15

The head end system 108 may send the signed temporary public key as a data packet, which in a non-limiting example, may have the below format:

| Field                | Description                                                   |
|----------------------|---------------------------------------------------------------|
| Temporary Public Key | Temporary public key generated by the pairing tool            |
| Signature            | Signature over temporary public key using pairing private key |

20

The skilled person will appreciate that other data packet formats may be used, and the above format is provided for the purposes of example only.

25

As will be described in more detail below, with reference to Figure 3, the signature provided by the pairing private key may be used by the metering devices 102a-n and the remote display modules 104a-n to authenticate the temporary public key during a pairing process. Furthermore, by using a temporary public key signed by the head end system 108, for pairing a metering device with a corresponding remote display module, the need for the head end system to generate and authenticate multiple pairing payloads comprising every possible metering device and remote display module combination, and for all of the pairing payloads to be stored on the pairing tool 106 is avoided. As such, a the pairing tool 106 is able to pair a larger number of metering devices and remote display modules during a single field visit, because the demands placed on the memory and processing power of the pairing tool 106 are reduced.

30

The above process, depicted in Figure 2, may be undertaken before a field technician visits a site in order to pair a metering device with a corresponding remote display module. In other arrangements, all or parts of the process depicted in Figure 2 may be undertaken at the site however. For example, if wireless communications between the pairing tool 106 and the head end system 108 are used, steps 206-210 may be undertaken by the field engineer on the way to a site or at a site.

Figure 3 depicts a sequence diagram of a method of pairing a metering device, in this example metering device 102a, with a corresponding remote display module, in this example remote display module 104a, using the pairing tool 106.

302: In an optional step, the field technician 124, who may be the individual visiting the site to pair the metering device 102a with the corresponding remote display module 104a, initiates a pairing mode of the pairing tool 106. This may comprise interacting with a graphical user interface, GUI, of the pairing tool 106 to select a "pairing mode" command.

304: The pairing tool 106 transmits a request to the metering device 102a for a meter public key.

Each metering device 102a-n is configured to generate a meter asymmetric key pair comprising the public meter key and a private meter key. In exemplary arrangements, each metering device 102a-n may comprise processing circuitry configured to execute instructions to generate the meter asymmetric key pair. The manufacturing user 122 may instruct the generation of the meter asymmetric key pair during the process of manufacture, installation or programming of each metering device 102a-n. Each meter asymmetric key pair may be stored on the corresponding metering device, for example in a memory (such as a non-volatile memory) of the corresponding metering device.

The meter public key may ultimately be used by the corresponding remote display module 104a, to which the metering device 102a is paired, in order to verify data/communications received from the metering device 102a and signed by the metering device 102a using the meter private key.

In the example depicted by Figure 3, the pairing tool 106 transmits the request for the meter public key to the communication module 116, and the communication module 116 transmits the request to the processor 114. The processor 114 may then transfer the request to the metering device 102a.

5

306: In response to the request received from the pairing tool 106, the metering device 102a transmits the meter public key, e.g. a data packet comprising the meter public key, to the pairing tool 106. The pairing tool 106 may store the meter public key for subsequent transmission to the remote display module 104a with which the metering device 102a is to be paired, as will be described in more detail below.

10

308: The pairing tool 106 transmits, to each of the metering device 102a and the remote display device 104a with which the metering device 102a is to be paired, the temporary public key signed using the pairing private key (obtained in step 210) and an indication that the temporary public key should be used for the duration of the pairing session.

15

The temporary public key, signed using the pairing private key, and the indication that the temporary public key should be used for the duration of the pairing session may be transmitted to the metering device 102a and the remote display device 104a in a message/packet. A non-limiting example of a format of the message/packet is given below. The skilled person will understand that in alternative arrangements, the message/packet may include one or more of the fields listed below in any combination, and/or alternative or additional fields.

20

25

| Field                           | Description                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Message standard data           | May include one or more of: a standard delimiter, a message identifier, a source identifier, a PDU header version etc. |
| Target Meter ID                 | The ID of the metering device to which the signed temporary public key and indication is to be sent                    |
| Target remote display module ID | The ID of the remote display module to which the signed temporary public key                                           |

|                                                 |                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                 | and indication is to be sent                                                                                                                                                                                                                                                                                                          |
| Indication of key to be used in pairing session | Indication of which public key should be used for verification during the pairing session (e.g. to verify the pairing request).<br>May take the form of:<br>Type of keyswap (indicating which public key should be changed):<br>00 = Meter public key Keyswap<br>01 = Pairing public key Keyswap<br>02 = Temporary public key Keyswap |
| Temporary public key                            | Temporary public key generated by the pairing tool                                                                                                                                                                                                                                                                                    |
| Signature                                       | Signature over temporary public key using pairing private key                                                                                                                                                                                                                                                                         |
| Expiration                                      | An indication of when the temporary public key should expire.                                                                                                                                                                                                                                                                         |

5           The metering device 102a and the remote display device 104a are able to authenticate the temporary public key signed by the pairing private key using the pairing public key stored within the respective memories of the metering device 102a and the remote display device 104a (in this example, the pairing public keys were stored within the respective memories in step 204 of Figure 2).

10           Once authenticated, the temporary public key may be stored in a memory of each of the metering device 102a and the remote display device 104a. The memory may comprise a volatile memory. The temporary public key does not overwrite the pairing public key stored within each of the metering device 102a and the remote display device 104a, and in this example, the temporary public key is stored in a separate memory to the memory in which the pairing public key is stored (i.e. the temporary public key is stored in a volatile memory, while  
15           the pairing public key is stored in a non-volatile memory).

20           For the duration of the pairing session, both the pairing public key and the temporary public key are stored by the metering device 102a and the remote display module 104a. However, once the temporary public key is authenticated and stored within the metering device 102a and the remote display device

104a, the metering device 102a and the remote display device 104a act on the indication provided by the pairing tool 106 to use the temporary public key (rather than the pairing public key) to authenticate communications received during the pairing session.

5

In exemplary arrangements, the indication provided by the pairing tool 106 may instruct the temporary public key to be used for a predetermined period of time (indicated by the expiration field in the packet outlined above). For example, the predetermined time period may be one of: 30 minutes, 45 minutes, 60 minutes etc. The predetermined time period may be selected to be of sufficient length to allow the pairing process to be completed.

10

310: The pairing tool 106 generates a pairing request. The pairing request is signed using the temporary private key.

15

The pairing request may comprise a pairing packet, and a non-limiting example of a format of the pairing packet is given below.

| Field                    | Description                                                     |
|--------------------------|-----------------------------------------------------------------|
| Remote display module ID | An identifier of the remote display device that is being paired |
| Meter ID                 | An identifier of the electric meter that is being paired        |
| Meter Public Key         | The electric meter public key of the meter being paired         |
| Hash                     | Hash of remote display module ID, meter ID, and public key      |
| Signature                | Signature over pairing packet using the temporary private key   |

20

25

The remote display module ID and the meter ID may comprise unique identifiers for identifying the metering device and the remote display module to be paired. The remote display module ID may, for example, comprise a LAN ID, and the meter ID may comprise a meter serial number, however these identifiers are provided as examples only, and the skilled person will appreciate that alternative identifiers may be used. This remote display module ID and the meter ID may be determined and input by the field technician 124 using the GUI of the field tool 106 for use in the pairing packet.

5 The pairing packet comprises the meter public key of the metering device 102a (which in this example, was obtained by the pairing tool 106 from the metering device 102a in step 306). As mentioned above, by providing the meter public key to the remote display module 104a to which the metering device 102a is to be paired, the remote display module 104a can authenticate communications sent by the metering device 102a and signed using the meter private key.

10 312: The pairing tool 106 transmits the pairing request (i.e. the pairing packet, or a packet based on or comprising the pairing packet) to the metering device 102a and the remote display module 104a with which the metering device 102a is to be paired.

15 In the example depicted in Figure 3, the pairing tool 106 transmits the pairing request to the communications module 116, and the communications module 116 transfers the pairing request to the processor 114. The processor 114 may then transfer the pairing request (or data from or based on the pairing request) to the metering device 102a.

20 The metering device 102a authenticates the pairing request using the temporary public key (stored in the metering device at step 308 in this example). The temporary public key verifies the digital signature of the pairing request made using the temporary private key (i.e. at step 310 in this example).

25 The remote display module 104a may also authenticate the received pairing request using the temporary public key (stored in the remote display module 104a at step 308 in this example). Again, the temporary public key verifies the digital signature of the pairing request made using the temporary private key (i.e. at step 310 in this example).

30 In this way, the metering device 102a and the remote display module 104a can verify that the pairing request is being received from an authorised source. This is because the temporary public key (received in this example in step 308) was signed by the pairing private key and authenticated by the metering device 102a and the remote display module 104a using the pairing public key, injected during manufacture, installation or maintenance. The authenticated temporary public key is then used then be used to authenticate the pairing request. As

35

such, a secure means to pair a metering device and a remote display module is provided.

5           The remote display module 104a may be configured to store the meter public key in a memory, such as the non-volatile memory of the remote display module 104a. As mentioned above, in this example, the remote display module 104a receives the meter public key as part of the pairing packet signed by the temporary private key. As such, the meter public key received by the remote display module 104a is authenticated using the temporary public key. Using the meter public key, the remote display module 104a may then authenticate subsequent communications received from the metering device 102a and signed by the metering device 102a using the meter private key. In this way, it is ensured that the remote display module 104a only accepts communications from a metering device 102a to which it has been paired.

15           314: After receipt and authentication of the pairing request by the metering device 102a and the remote display module 104a, the metering device 102a and the remote display module 104a are paired.

20           The metering device 102a has the remote display module 104a identification details (obtained from the pairing request), and therefore is able to send data to the remote display module 104a, for example data relating to the consumption of the utility measured by the metering device 102a. As mentioned above, this data is signed using the meter private key, and may be authenticated by the remote display module 104a using the meter public key stored in the remote display module 104a. In this way, the owner of the premises may be sure that the data being received by the remote display module 104a is accurate, has not been tampered with, and is associated with the correct metering device 102a.

25           316: Once the pairing process is complete (i.e. the metering device 102a and the remote display module 104a are paired), or else the predetermined time period has elapsed, the temporary public keys are deleted from the metering device 102a and the remote display module 104a.

The skilled person will appreciate that a similar process to that outlined above may be undertaken to pair the other metering devices 102b-n with a corresponding remote display module 104b-n.

5 The above method and system provides a means of efficiently and securely pairing a metering device with a remote display module.

10 Although the disclosure has been described in terms of particular embodiments as set forth above, it should be understood that these embodiments are illustrative only and that the claims are not limited to those embodiments. Those skilled in the art will be able to make modifications and alternatives in view of the disclosure, which are contemplated as falling within the scope of the appended claims. Each feature disclosed or illustrated in the present specification may be incorporated in any embodiments, whether alone or in any appropriate combination with any other feature disclosed or illustrated herein. The word "exemplary" is used herein to mean "an example". Any embodiment described herein as "exemplary" is not necessarily to be  
15 construed as preferred or advantageous over other embodiments.

A computer program may be configured to provide any of the above described methods. The computer program may be provided on a computer readable medium.  
20 The computer program may be a computer program product. The product may comprise a non-transitory computer usable storage medium. The computer program product may have computer-readable program code embodied in the medium configured to perform the method. The computer program product may be configured to cause at least one processor to perform some or all of the method.

25 Various methods and apparatus are described herein with reference to block diagrams, sequence diagrams or flowchart illustrations of computer-implemented methods, apparatus (systems and/or devices) and/or computer program products. It is understood that a block of the block diagrams, sequence diagrams and/or flowchart illustrations, and combinations of blocks in the block diagrams, communications in the sequence diagrams, and/or flowchart illustrations, can be implemented by computer program instructions that are performed by one or more computer circuits associated with the entities of the system. These computer program instructions may be provided  
30 to a processor circuit of a general purpose computer circuit, special purpose computer circuit, and/or other programmable data processing circuit to produce a machine, such that the instructions, which execute via the processor of the computer and/or other

programmable data processing apparatus, transform and control transistors, values stored in memory locations, and other hardware components within such circuitry to implement the functions/acts specified in the block diagrams, sequence diagrams and/or flowchart block or blocks, and thereby create means (functionality) and/or structure for implementing the functions/acts specified in the block diagrams, sequence diagrams and/or flowchart block(s).

Computer program instructions may also be stored in a computer-readable medium that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable medium produce an article of manufacture including instructions which implement the functions/acts specified in the block diagrams and/or flowchart block or blocks.

A tangible, non-transitory computer-readable medium may include an electronic, magnetic, optical, electromagnetic, or semiconductor data storage system, apparatus, or device. More specific examples of the computer-readable medium would include the following: a portable computer diskette, a random access memory (RAM) circuit, a read-only memory (ROM) circuit, an erasable programmable read-only memory (EPROM or Flash memory) circuit, a portable compact disc read-only memory (CD-ROM), and a portable digital video disc read-only memory (DVD/Blu-ray).

The computer program instructions may also be loaded onto a computer and/or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer and/or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the block diagrams, sequence diagrams and/or flowchart block or blocks.

Accordingly, the invention may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.) that runs on a processor, which may collectively be referred to as "circuitry," "a module" or variants thereof.

It should also be noted that in some alternate implementations, the functions/acts noted in the blocks or sequence diagram stages may occur out of the order noted in the

flowcharts or sequence diagrams. For example, two blocks shown in succession, or two sequence communications shown in succession in a sequence diagram, may in fact be executed substantially concurrently or the blocks/sequence communications may sometimes be executed in the reverse order, depending upon the functionality/acts involved. Moreover, the functionality of a given block of the flowcharts and/or block diagrams, or sequence communication of the sequence diagrams, may be separated into multiple blocks or communications, and/or the functionality of two or more blocks of the flowcharts and/or block diagrams may be at least partially integrated. Finally, other blocks or sequence communications may be added/inserted between the blocks/sequence communications that are illustrated.

**CLAIMS:**

1. A method of pairing a metering device with a remote display module, the method comprising:
  - 5 storing a pairing public key of an asymmetric key pair in a memory of the metering device and a memory of the remote display module;  
communicating to the metering device and the remote display module, a temporary public key of a temporary asymmetric key pair, the temporary public key signed using a pairing private key of the asymmetric key pair;
  - 10 authenticating, by the metering device and the remote display module, the temporary public key, using the stored pairing public key;  
communicating to the metering device and the remote display module, a pairing request signed using a temporary private key of the temporary asymmetric key pair, wherein the pairing request comprises a meter public key of a meter asymmetric key pair;
  - 15 authenticating, by the metering device and the remote display module, the pairing request using the authenticated temporary public key; and  
storing the meter public key in the remote display module.
- 20 2. A method according to claim 1, wherein, following authentication of the temporary public key by the metering device and the remote display module, the method comprises temporarily storing the temporary public key in the metering device and the remote display module.
- 25 3. A method according to claim 2, further comprising deleting the temporary public key from the metering device and the remote display module once the metering device and the remote display module have been paired.
4. A method according to claim 2, further comprising deleting the temporary public key from the metering device and the remote display module on expiry of a predetermined time period.
- 30 5. A method according to any preceding claim, further comprising sending a command to the metering device and the remote display module instructing the

metering device and the remote display module to use the temporary public key to authenticate the pairing request and not the pairing public key.

5 6. A method according to any preceding claim, wherein a pairing tool transmits the temporary public key signed using the pairing private key to the metering device and the remote display module.

7. A method according to claim 6, further comprising transmitting, by the pairing tool and to the metering device, a request for the meter public key; and  
10 receiving, by the pairing tool and from the metering device, the meter public key for use in the pairing request.

8. A method according to claim 7, wherein the pairing tool generates the pairing request and signs the pairing request using the temporary private key, and transmits  
15 the pairing request signed by the temporary private key to the metering device and the remote display module.

9. A method according to any of claims 6 to 8, further comprising the preceding step of:  
20 generating, by the pairing tool, the temporary asymmetric key pair.

10. A method according to claim 9, further comprising:  
transmitting, from the pairing tool and to a remote device, a request for the remote device to sign the temporary public key using the pairing private key;  
25 signing, by the remote device, the temporary public key using the pairing private key; and  
receiving, by the pairing tool and from the remote device, the temporary public key signed using the pairing private key.

30 11. A method according to any of claims 6 to 10, wherein the pairing request further comprises a unique identifier of the remote display module and/or a unique identifier of the metering device.

12. A method according to any preceding claim, wherein the pairing public key is  
35 stored in the metering device and the remote display module before installation or during manufacture of each of the metering device and the remote display module.

13. A system for pairing a metering device with a remote display module, the system comprising:
- 5 the metering device comprising a memory within which a pairing public key of an asymmetric key pair is stored; and
- the remote display module comprising a memory within which the pairing public key is stored,
- wherein the metering device and the remote display module are configured to:
- 10 receive a temporary public key of a temporary asymmetric key pair, the temporary public key signed using a pairing private key of the asymmetric key pair;
- authenticate the temporary public key using the stored pairing public key;
- 15 receive a pairing request signed using a temporary private key of the temporary asymmetric key pair, wherein the pairing request comprises a meter public key of a meter asymmetric key pair; and
- authenticate the pairing request using the authenticated temporary public key,
- 20 wherein the remote display module is further configured to store the meter public key.
14. The system of claim 13, further comprising a pairing tool, the pairing tool configured to:
- 25 transmit the temporary public key signed using the pairing private key to the metering device and the remote display module;
- generate the pairing request and sign the pairing request using the temporary private key; and
- 30 transmit the pairing request to the metering device and the remote display module.
15. The system of claim 14, wherein the pairing tool is further configured to generate the temporary asymmetric key pair.
16. The system of claim 15, further comprising a remote device configured to:
- 35 generate the asymmetric key pair comprising the pairing public key and the pairing private key;

receive, from the pairing tool, a request to sign the temporary public key using the pairing private key; and

transmit, to the pairing tool, the temporary public key signed using the pairing private key.