

[DESCRIPTION]

[Title of Invention]

SETTING METHOD, DEVICE AUTHENTICATION METHOD, DEVICE AUTHENTICATION SYSTEM, AND CONTROLLER

5 [Technical Field]

[0001]

The present invention relates to methods of setting identifications (IDs) and certificates of devices to smart meters, methods of authenticating devices including the smart meters, and the like.

10 [Background Art]

[0002]

Along with the introduction of a smart grid (next-generation grid-system), smart meters including a communication and controlling function is becoming widely used.

15 [0003]

On the other hand, the number of appliances, such as an air conditioner, which are used at home and having communication functions is increasing. Home energy management system (HEMS) which controls the appliances at home by a HEMS-controller using the communication functions of such appliances is gaining attention.

20

[0004]

Furthermore, through the communication between the smart meters, the HEMS-controllers and the appliances, provision of various services is considered which is made possible, for example, by transmitting control signals, such as demand response (DR) signal, from the smart meters to the HEMS controllers and appliances.

25

[Citation List]

[Patent Literature]

[0005]

30 [PTL 1]

US Patent Application Publication No. 2011/0047370

[PTL 2]

US Patent No. 7950044

[PTL 3]

35

US Patent Application Publication No. 2011/0302635

[Summary of Invention]

[Technical Problem]

[0006]

For the communication between a smart meter, a HEMS-controller, and
5 an appliance, it is necessary to set (store) in the smart meter the ID and the
certificate information of each of the HEMS-controller and the appliance
beforehand.

[0007]

In view of this, the present invention provides, for example, a method
10 of setting the ID and the certificate information of the appliance to the smart
meter easily.

[Solution to Problem]

[0008]

A method of setting according to an aspect of the present invention is a
15 method of setting an identification (ID) and a certificate for each of devices to
a smart meter, the ID and the certificate being used for authentication for
network connection between the smart meter and the devices, the method
including: obtaining, from a smart meter connected via a first communication
network, an ID of the smart meter associated with user information of the
20 smart meter; obtaining, from a controller which is one of the devices
connected via a second communication network, (i) an ID and a certificate of
the controller associated with user information of the controller and (ii) an ID
and a certificate of an appliance which is one of the devices controlled by the
controller; generating, based on the user information of the smart meter and
25 the user information of the controller, management information in which the ID
of the smart meter, the ID and the certificate of the controller, and the ID and
the certificate of the appliance are associated with one another; and
transmitting, based on the management information, the ID and the certificate
of the controller and the ID and the certificate of the appliance which are
30 associated with the ID of the smart meter, to the smart meter.

[0009]

These general and specific aspects may be implemented using an
apparatus, a system, an integrated circuit, a computer program, or a
computer-readable recording medium, such as a CD-ROM, or any combination
35 of apparatuses, systems, integrated circuits, computer programs, or

computer-readable recording media.

[Advantageous Effects of Invention]

[0010]

According to the present invention, ID and certificate information of a
5 device can be easily set to a smart meter.

[Brief Description of Drawings]

[0011]

[FIG. 1A]

FIG. 1A is a system configuration figure of a device authentication
10 system according to Embodiment 1.

[FIG. 1B]

FIG. 1B is a flowchart showing operations performed by the device
authentication system according to Embodiment 1.

[FIG. 2]

15 FIG. 2 is a block diagram showing a configuration of each of a smart
meter, a HEMS-controller, and a remote server according to Embodiment 1.

[FIG. 3]

FIG. 3 is a diagram showing an example of a configuration of an
authentication table saved in the database in the remote server according to
20 Embodiment 1.

[FIG. 4]

FIG. 4 is a sequence figure showing an exchange of data between
devices according to Embodiment 1.

[FIG. 5]

25 FIG. 5 is a system configuration figure of a device authentication
system according to Embodiment 2.

[FIG. 6]

FIG. 6 is a system configuration figure in which a utility system is
connected to the initial state (FIG. 5) in Embodiment 2.

30 [FIG. 7]

FIG. 7 is a system configuration figure of a device authentication
system according to Embodiment 3.

[FIG. 8]

FIG. 8 is a diagram showing an example of updating of data in a
35 database in a remote server, which occurs when a new appliance is connected

to a HEMS-controller in Embodiment 3.

[Description of Embodiments]

[0012]

A method of setting according to an aspect of the present invention is a
5 method of setting an identification (ID) and a certificate for each of devices to
a smart meter, the ID and the certificate being used for authentication for
network connection between the smart meter and the devices, the method
including: obtaining, from a smart meter connected via a first communication
10 network, an ID of the smart meter associated with user information of the
smart meter; obtaining, from a controller which is one of the devices
connected via a second communication network, (i) an ID and a certificate of
the controller associated with user information of the controller and (ii) an ID
and a certificate of an appliance which is one of the devices controlled by the
15 controller; generating, based on the user information of the smart meter and
the user information of the controller, management information in which the ID
of the smart meter, the ID and the certificate of the controller, and the ID and
the certificate of the appliance are associated with one another; and
transmitting, based on the management information, the ID and the certificate
20 of the controller and the ID and the certificate of the appliance which are
associated with the ID of the smart meter, to the smart meter.

[0013]

As described, the IDs and the certificates of devices (HEMS-controller
and appliance) can be set to the smart meter more easily.

[0014]

25 Furthermore, for example, when new device information that is (i) an
ID and a certificate of the controller which are not included in the management
information or (ii) an ID and a certificate of the appliance which are not
included in the management information is obtained via the second
communication network: in the generating, the management information may
30 be updated by adding the new device information to the management
information in association with the ID of the smart meter; and in the
transmitting, the new device information may be transmitted to the smart
meter having the ID associated with the new device information.

[0015]

35 Furthermore, for example, the first communication network may be a

secure communication network dedicated to communication with the smart meter.

[0016]

Furthermore, for example, the controller may be a home energy management system (HEMS) controller which controls a device among the devices.

[0017]

Furthermore, for example, the ID of each of the devices may be a media access control (MAC) address.

10 [0018]

A device authentication method according to an aspect of the present invention is a device authentication method for authenticating network connection between a smart meter and a plurality of devices by using a server, the method including: (a) obtaining, by a controller which controls an appliance, an identification (ID) and a certificate of the appliance, the controller and the appliance each being one of the devices; (b) transmitting, by the controller, the ID and the certificate of the appliance obtained in step (a) to the server; (c) obtaining, by the server, an ID of the smart meter associated with user information of the smart meter; (d) obtaining, by the server, an ID and a certificate of the controller and the ID and the certificate of the appliance which are associated with user information of the controller; (e) generating, by the server, management information based on the user information of the smart meter and the user information of the controller, the management information including the ID of the smart meter obtained in step (c), and the ID and the certificate of the controller and the ID and the certificate of the appliance obtained in step (d) in association with one another; and (f) transmitting, by the server, based on the management information, the ID and the certificate of the controller and the ID and the certificate of the appliance which are associated with the ID of the smart meter, to the smart meter.

30 [0019]

As described, the IDs and the certificates of devices can be set to the smart meter more easily with the device authentication system.

[0020]

Furthermore, for example, the device authentication method according to an aspect of the present invention may further include (g) obtaining, by the

smart meter, the ID and the certificate of the controller and the ID and the certificate of the appliance from the server; and (h) when the smart meter receives an authentication request from the controller or the appliance, (i) determining, by the smart meter, whether an ID and a certificate included in the authentication request match the ID and the certificate obtained in step (g) and, (ii) when the ID and the certificate in the authentication request match the ID and the certificate obtained in step (g), permitting, by the smart meter, a network connection between the controller or the appliance which transmitted the authentication request and the smart meter, the authentication request being information which requests authentication.

[0021]

Furthermore, for example, in step (a), the controller may communicate with the appliance by a wireless communication compliant with a Zigbee (Zigbee is a registered trademark) standard to obtain the ID and the certificate of the appliance.

[0022]

A device authentication system according to an aspect of the present invention is a device authentication system in which an identification (ID) and a certificate of each of devices are set to a smart meter by a server, the ID and the certificate being used for authentication for network connection between the smart meter and the devices, the system including: a controller which controls an appliance, the controller and the appliance each being one of the devices; and the server, wherein the controller includes: a first communication unit configured to obtain an ID and a certificate of the appliance; and a second communication unit configured to transmit the ID and the certificate of the appliance obtained by the first communication unit to the server, and the server includes: a first obtainment unit configured to obtain an ID of the smart meter associated with user information of the smart meter; a second obtainment unit configured to obtain an ID and a certificate of the controller and the ID and the certificate of the appliance which are associated with user information of the controller; a system manager which generates, based on the user information of the smart meter and the user information of the controller, management information in which the ID of the smart meter obtained by the first obtainment unit, and the ID and the certificate of the controller and the ID and the certificate of the appliance obtained by the

second obtainment unit are associated with one another; and a transmitting unit configured to transmit, based on the management information, the ID and the certificate of the controller and the ID and the certificate of the appliance which are associated with the ID of the smart meter, to the smart meter.

5 [0023]

A controller according to an aspect of the present invention is a controller which performs communication for a first pairing that is a wireless network connection between a device and a smart meter, the first pairing being performed after a server transmitted authentication information of the device to the smart meter, the controller including: a first communication unit
10 configured to perform a second pairing which is a wireless network connection with the device, to obtain authentication information of the device; and a second communication unit configured to transmit the authentication information of the device obtained by the first communication unit, to the
15 server.

[0024]

As described, before the final pairing (first pairing) in which the smart meter and the device are connected via a wireless network is performed, the controller performs the second pairing in which the controller and the
20 appliance are preliminary connected. With this, the controller can obtain the ID and the certificate of each of the appliances at one time, and can transmit the IDs and the certificates to the server in a batch. Thus, the IDs and the certificates can be transmitted to the smart meter more easily.

[0025]

25 Furthermore, for example, a controller may perform communication for a first pairing that is a wireless network connection between a device and a smart meter, the first pairing being performed after a server transmitted authentication information of the device to the smart meter. The controller may include: a first communication unit configured to perform a second
30 pairing which is a wireless network connection with the device, to obtain authentication information of the device; and a second communication unit configured to transmit the authentication information of the device obtained by the first communication unit, to the server.

[0026]

35 Furthermore, for example, the first communication unit may, after

obtaining the authentication information of the device, cancel the second pairing before the first pairing is performed.

[0027]

5 These general and specific aspects may be implemented using an apparatus, a system, a method, an integrated circuit, a computer program, or a computer-readable recording medium, such as a CD-ROM, or any combination of systems, methods, integrated circuits, computer programs, or computer-readable recording media.

[0028]

10 Hereinafter, embodiments are specifically described in greater detail with reference to the accompanying Drawings.

[0029]

15 Each of the embodiments described below shows a general or specific example. The numerical values, shapes, materials, structural elements, the arrangement and connection of the structural elements, steps, the processing order of the steps etc. shown in the following exemplary embodiments are mere examples, and therefore do not limit the scope of the present invention. Therefore, among the structural elements in the following embodiments, structural elements not recited in any one of the independent claims defining
20 the most generic concept are described as arbitrary structural elements.

[0030]

(Embodiment 1)

First, an outline of a device authentication system according to this embodiment is described.

25 [0031]

FIG. 1A is a system configuration figure of a device authentication system according to Embodiment 1.

[0032]

30 In FIG. 1A, a device authentication system 100 includes a smart meter (SM) 130, a HEMS-controller (HEMS-C) 110, and a remote server 120. Furthermore, the device authentication system 100 may further include appliances 141 and 142.

[0033]

35 A home network 101 shown in FIG. 1A is a network in the house of a user. Furthermore, a utility network 102 is, for example, a network of an

infrastructure business operator, such as a power company, a gas company, or a water company.

[0034]

Here, the smart meter 130 is a meter including a communication
5 function and is provided inside the house of a user. The smart meter 130 transmits the amount of power consumed, the amount of gas used, the amount of water used, or the like of the house of the user to the corresponding infrastructure business operator via an advanced metering infrastructure (AMI) 104.

10 [0035]

By making the smart meter 130, the HEMS-controller 110, and appliances 141 and 142 (hereafter collectively denoted as appliances 140) communicate mutually, provision of various services on the HEMS-controller 110 and the appliances 140 is conceivable using the information of the smart
15 meter 130. However, to enable the smart meter 130, the HEMS-controller 110, and appliances 140 to communicate securely, the device ID and the certificate (authentication information used for communication, such as an account and a password) of each of the HEMS-controller 110 and appliances 140 need to be set to the smart meter 130 beforehand.

20 [0036]

However, in most cases, business operators who provide the HEMS-controller 110 and appliances 140 are different from the infrastructure business operator who installed the smart meter 130 in the house of a user. Thus, to store the IDs and the certificates of the above-described devices into
25 the smart meter 130, it is usually necessary to request the infrastructure business operator to dispatch a worker, and the worker needs to perform a task (construction) of setting the device ID and the certificate to the smart meter 130. More specifically, every time new appliances 140 are added to the house of the user, registration (setting) of the device ID and the certificate to
30 the smart meter 130 needs to be requested to the infrastructure business operator. Thus, it is rather inconvenient and problematic.

[0037]

In view of this, in the device authentication system 100 according to this embodiment, the remote server 120 sets the HEMS-controller 110 and the
35 appliances 140 in the house of the user as the communication target devices of

the smart meter 130. This enables the user or the business operators (manufacturers) of the appliances 140 to store in the smart meter 130 the device IDs and the certificates of the appliances with a simple procedure, that is, transmission of the device IDs and the certificates via a packet network 103
5 from the HEMS-controller 110.

[0038]

As a result, the smart meter 130, the HEMS-controller 110, and the appliances 140 are connected via the same network, and thus these devices can communicate mutually. In other words, the aforementioned services that
10 use the above-described information of the smart meter 130 are realized.

[0039]

The following describes each of structural elements of the device authentication system 100 with reference to FIG. 1A.

[0040]

15 In FIG. 1A, it is assumed that the smart meter 130 is installed in the house of a user (not shown). The smart meter 130 is, as AMI 104, connected to the utility network 102. The smart meter 130 is controlled by a utility head end 105 in the utility network 102. It should be noted that the database 170 is provided in the utility network 102.

20 [0041]

Using the AMI, the utility head end 105 examines the amount of power consumed, the amount of gas used, the amount of water used, or the like of the house of the user from the smart meter 130. Furthermore, the smart meter 130 can transmit a control signal to the HEMS-controller 110 and each
25 of appliances 140 which are communication targets.

[0042]

The appliances 140, such as an air conditioner, a refrigerator, and a washing machine, are connected to the HEMS-controller 110 via a communication network. More specifically, the HEMS-controller 110 controls
30 the appliances 140 connected to the HEMS-controller 110. It should be noted that, here, the appliances 140 are not limited to the devices used at home, but represent various electrical devices, such as office appliance (e.g., a copying machine), medical equipment, or the like. In other words, the appliances 140 mentioned here represent general electrical devices.

35 [0043]

In FIG. 1A, the smart meter 130, the AMI 104, and the utility head end 105 are included in the utility network 102.

[0044]

Furthermore, the HEMS-controller 110 and the appliances 140 are
5 included in the home network 101 in the house of a user.

[0045]

The remote server 120 collects (obtains) the ID and the certificate of each of the appliances 140 connected to the HEMS-controller 110 and makes, based on the ID and the certificate of each of the appliances 140, an
10 authentication request to the target smart meter 130 in which the setting is to be made. It should be noted that the remote server 120 is provided outside the house of the user (outside of the building in which the smart meter 130, the HEMS-controller 110, and the appliances 140 are provided), and is managed by, for example, a manufacturer of the HEMS-controller 110 or the
15 appliances 140. Furthermore, the remote server 120 includes a database 160.

[0046]

Next, outline of operations performed by the device authentication system 100 is described with reference to FIG. 1A and FIG. 1B.

20 [0047]

FIG. 1B is a flowchart showing operations performed by the device authentication system 100.

[0048]

First, the HEMS-controller 110 obtains the ID and the certificate of each
25 of the appliances 140 (S101). The ID of each of the appliances 140 is, specifically, the media access control (MAC) address of the appliance. However, the ID may be other information that can identify the appliance. The same applies to the ID of the HEMS-controller 110 and the ID of the smart meter 130 which are to be described later.

30 [0049]

It should be noted that, at this time, the HEMS-controller 110 is connected to the appliances 141 and 142 via a wireless network. Details of the wireless connection (a second pairing) will be described later.

[0050]

35 Next, the HEMS-controller 110 transmits (i) the ID and the certificate of

the HEMS-controller 110 and (ii) the ID and the certificate of each of the appliances 140 obtained in Step S101 to the remote server 120 (S102). The HEMS-controller 110 and the remote server 120 communicate using the packet network 103. Specifically, an example of the packet network 103 is the Internet.

[0051]

Next, the remote server 120 saves in the database 160 the received ID and the certificate of the HEMS-controller 110 and the ID and the certificate of each of the appliances 140 as a HEMS-C and appliance management table (S103).

[0052]

Next, the smart meter 130 transmits the ID of the smart meter 130 to the remote server 120 (S104).

[0053]

The remote server 120 saves in the database 160 the received ID of the smart meter 130 as a smart meter 130 management table (S105).

[0054]

Furthermore, the remote server 120 generates information which is an authentication table (management list, management information) in which the ID of the smart meter, the ID and the certificate of the HEMS-controller 110, and the ID and the certificate of each of the appliances 140 are associated with one another, and saves the authentication table in the database 160 (S106).

[0055]

Lastly, the remote server 120 transmits to the smart meter 130, based on the authentication table generated in Step S106, the ID and the certificate of the HEMS-controller 110 and the ID and the certificate of each of the appliances 140 which are associated with the smart meter 130 (S107). The remote server 120 and the smart meter 130 communicate using a dedicated secure communication network. The secure network is a dedicated network to which only the infrastructure business operator which provides the smart meter 130 and the business operator of the remote server 120 can connect.

[0056]

Next, specific configuration of each of the smart meter 130, the HEMS-controller 110, and the remote server 120 is described.

[0057]

FIG. 2 is a block diagram showing a configuration of each of the smart meter 130, the HEMS-controller 110, and the remote server 120.

[0058]

First, the smart meter 130 is described.

5 [0059]

As shown in FIG. 2, the smart meter 130 includes an AMI network IF 134 (third obtainment unit) and a home network IF 135 as communication interfaces.

[0060]

10 The smart meter 130 also includes a commissioning manager 131, a certification manager 132 and a memory 136.

[0061]

The commissioning manager 131 transmits the ID of the smart meter 130 to the remote server 120 through the AMI network IF 134. Furthermore, through the AMI network IF 134, the commissioning manager 131 receives from the remote server 120 the certificate of the HEMS-controller 110 and the certificate of each of the appliances 140 which are associated with the smart meter 130. Furthermore, the commissioning manager 131 saves in the memory 136 the certificate of the HEMS-controller 110 and the certificate of each of the appliances 140 received from the remote server 120.

[0062]

The certification manager 132 authenticates the HEMS-controller 110 and the appliances 140 which are to be connected to the smart meter 130. Specifically, the certification manager 132 compares and determines whether or not the IDs and the certificates of the HEMS-controller 110 and the appliances 140 which made the authentication request to the smart meter 130 matches the IDs and certificates stored in the memory 136. If the matching is successful, the smart meter 130 permits network connection between (i) the HEMS-controller 110 and the appliances 140 which transmitted the authentication request and (ii) the smart meter 130.

[0063]

In this embodiment, the network connection is a wireless communication network connection compliant with the Zigbee (Zigbee is a registered trademark) standard. However, the above-described network connection may be other wireless LAN connection (e.g., Wi-Fi (Wi-Fi is a

registered trademark)) or a wired connection.

[0064]

5 In the memory 136, the ID and the certificate of the HEMS-controller 110 and the ID and the certificate of each of the appliances 140 transmitted by the remote server 120 are saved (stored). The memory 136 is, for example, a dynamic random access memory (DRAM) or a ferroelectric memory.

[0065]

Next, the HEMS-controller 110 is described.

[0066]

10 The HEMS-controller 110 includes a home network IF 114 (a first communication unit) and a packet network IF 115 (a second communication unit) as communication interfaces.

[0067]

15 Furthermore, the HEMS-controller 110 includes: a gathering manager 113, a commissioning manager 111, a certification manager 112, and a memory 116.

[0068]

20 The gathering manager 113 collects the IDs and the certificates of the appliances 140 from the appliances 140. The IDs and the certificates of the appliances 140 may be collected through a network by the gathering manager 113 or registered manually into the memory 116 by a manager of the HEMS-controller 110.

[0069]

25 In this embodiment, the gathering manager 113 collects the IDs and the certificates of the appliances 140 through the wireless communication network compliant with the Zigbee standard. However, the above-described network connection may be other wireless LAN connection (e.g., Wi-Fi) or a wired connection.

[0070]

30 The commissioning manager 111 transmits to the remote server 120 the ID and the certificate of the commissioning manager 111 itself, and the ID and the certificate of each of the appliances 140 collected by the gathering manager 113. At this time, the commissioning manager 111 also transmits, to the remote server 120, user information which indicates the user of the
35 HEMS-controller 110.

[0071]

The certification manager 112 makes an authentication request to the smart meter 130.

[0072]

5 In the memory 116, the ID and the certificate of the HEMS-controller 110 itself, the IDs and the certificates of the appliances 140 connected to the HEMS-controller 110 are saved. The memory 116 is, for example, a DRAM or a ferroelectric memory.

[0073]

10 Next, the remote server 120 is described.

[0074]

The remote server 120 is a so-called information processing apparatus, and includes a packet network IF 125 (second obtainment unit) and an AMI network IF 124 (first obtainment unit, transmitting unit) as communication
15 interfaces. Furthermore, the remote server 120 includes the database 160, and a system manager 121.

[0075]

The packet network IF 125 obtains, from the HEMS-controller 110 connected via the home network 101, the (i) ID and the certificate of the
20 HEMS-controller 110 and (ii) the IDs and the certificates of the appliances 140 controlled by the HEMS-controller 110.

[0076]

The AMI network IF 124 obtains the ID of the smart meter 130 from the smart meter 130 connected via the utility network 102.

25 [0077]

Furthermore, the AMI network IF 124 transmits, to the smart meter 130, the ID and the certificate of the HEMS-controller 110 and the IDs and the certificates of the appliances 140. The certificate of the HEMS-controller 110 and the certificates of the appliances 140 are certificates which have been
30 issued by the system manager 121 based on the authentication table.

[0078]

In the database 160, the certificate of the HEMS-controller 110, the certificate of the appliance, and the ID of the smart meter are saved. The database 160 is implemented by, for example, a hard disc drive (HDD), a
35 DRAM, or a ferroelectric memory.

[0079]

The system manager 121 creates, based on the user information, the authentication table in which (i) the ID of the smart meter 130 obtained by the AMI network IF 124 (ii) and the ID and the certificate of the HEMS-controller 110 and the IDs and the certificates of the appliances 140 obtained by the packet network IF 125 are associated with one another.

[0080]

It should be noted that, the user information is information which can identify the user. The user information may be transmitted from the HEMS-controller 110 and the smart meter 130 along with the ID. Furthermore, the ID itself may be information which includes the user information. Furthermore, in the database 160 in the remote server 120, the user information which corresponds to the obtained ID may be stored beforehand, and the ID and the user information may be thus associated with each other.

[0081]

Furthermore, based on the authentication table (management information) registered in the database 160, the system manager 121 issues, to the smart meter 130, the certificate of the HEMS-controller 110 and the certificates of the appliances 140 associated with the smart meter 130.

[0082]

It should be noted that, as mentioned earlier, the Zigbee can be used as a communication protocol of the home network 101 in FIG. 1A. More specifically, the Zigbee can be used as a communication protocol between each of (i) the smart meter 130 and the HEMS-controller 110, (ii) the HEMS-controller 110 and the appliances 140, and (iii) the smart meter 130 and the appliances 140.

[0083]

Next, the authentication table saved in the database 160 in the remote server 120 is described.

[0084]

FIG. 3 is a diagram showing an example of a configuration of the authentication table saved in the database 160 in the remote server 120 shown in FIG. 2.

[0085]

As shown in FIG. 3, the remote server 120 associates the ID information of the smart meter 130 with the IDs and the certificates of the HEMS-controller 110 and the appliances 140.

[0086]

5 First, as shown in (a) in FIG. 3, a HEMS-C and appliance management table in which the HEMS-controller 110 and each of the appliances 140 are associated is saved in the database 160 in the remote server 120. The management table stores each of the user IDs (individual IDs, user information), the ID and the certificate of the HEMS-controller 110, and the ID
10 and the certificate of the appliances 140 in association with one another.

[0087]

For example, in the case of (a) in FIG. 3, each of IDs "AOU1", "AIU1", and "AIU2" of the appliances 140 connected to the HEMS-controller 110, and each of certificates "AAA1", "AAA2", and "AAA3" are associated with "Pana1",
15 which is the HEMS-controller 110 of user "Mr. A", and certificate "AAA0".

[0088]

Furthermore, as shown in (b) in FIG. 3, each of the user IDs (individual IDs) are associated with a corresponding one of the IDs of the smart meter 130 (SM IDs) and stored as a smart meter 130 management table in the
20 database 160 in the remote server 120.

[0089]

For example, in the case of (b) in FIG. 3, users "Mr. A ", "Mr. B ", and "Mr. C " are respectively associated with "meter A", "meter B", and "meter C" each of which is the smart meter 130.

25 [0090]

Furthermore, the remote server 120 creates the authentication table from the HEMS-C and appliance management table and the smart meter 130 management table.

[0091]

30 The authentication table in (c) in FIG. 3 shows that, for example, in the house of user "Mr. A", "meter A" which is the smart meter 130 is connected, and "Pana1" which is the HEMS-controller 110, and the appliances 140 having the IDs "AOU1", "AIU1", and "AIU2" are installed. The authentication table in (c) in FIG. 3 shows that the certificate of "Pana1" that is the HEMS-controller
35 110 which corresponds to "meter A" that is the smart meter 130 in the house

of "Mr. A" is "AAA0", and the certificates of the appliances "AOU1", "AIU1", and "AIU2" are "AAA1", "AAA2", and "AAA3", respectively.

[0092]

5 The smart meter 130 obtains the certificate of the HEMS-controller 110 and the certificates of the appliances 140 based on the authentication table in the remote server 120, and authenticates only an appliance for which the certificate is available. With this, spoofing of an appliance and unauthorized connection can be prevented.

[0093]

10 Furthermore, when the smart meter 130 is connected to the HEMS-controller 110 and the appliances 140 which are communication targets that have been permitted by the smart meter 130 to connect, the smart meter 130 can transmit a control signal to the connected devices. Specifically, it becomes possible to provide various services in which the HEMS-controller 110,
15 the appliances 140, and the smart meter 130 cooperate.

[0094]

The following describes the details of operations performed by the device authentication system 100 having the above configuration.

[0095]

20 FIG. 4 is a sequence figure showing an exchange of data among the devices according to Embodiment 1.

[0096]

First, the commissioning manager 131 of the smart meter 130 transmits, through the AMI network IF 134, the ID of the smart meter 130
25 itself to the remote server 120 (S201).

[0097]

Next, after receiving the ID of the smart meter 130 transmitted through the AMI network IF 124 in Step S201, the remote server 120 saves in the database 160 the ID of the smart meter 130 and its user ID in association
30 with each other (S202).

[0098]

On the other hand, when receiving connection request from the appliances 140 which are not yet connected to the HEMS-controller 110 (S203), the HEMS-controller 110 transmits a connection response to such
35 appliances 140, and thus connects such appliances 140 to the HEMS-controller

110 itself (S204). At this time, the HEMS-controller 110 obtains the ID of the appliances 140 which transmitted the connection request.

[0099]

After this, the gathering manager 113 of the HEMS-controller 110
5 transmits, through the home network IF 114, a certificate request to each of the newly connected appliances 140 (S205).

[0100]

Each of the appliances 140 which received the certificate request transmits its own certificate to the HEMS-controller 110 (S206). The
10 gathering manager 113 of the HEMS-controller 110 receives the certificate through the home network IF 114, and saves the certificate in the memory 116 (S207).

[0101]

When a plurality of appliances 140 is connected to the HEMS-controller
15 110, the HEMS-controller 110 obtains the certificate of each of the appliances 140 using a similar method.

[0102]

Next, through the packet network IF 115, the commissioning manager
20 111 of the HEMS-controller 110 transmits to the remote server 120 the ID and the certificate of the HEMS-controller 110 itself and the IDs and the certificates of the appliances 140 (S208).

[0103]

The remote server 120 saves in the database 160 the ID and the certificate of the HEMS-controller 110 and the IDs and the certificates of the
25 appliances 140, which are received through the packet network IF 125, in association with one another (S209). In the database 160, the ID of the smart meter 130 and the IDs and the certificate information of each of the HEMS-controller 110 and the appliances 140 are saved in association with one another.

30 [0104]

The system manager 121 of the remote server 120 refers to the database 160, and transmits the ID and the certificate of the HEMS-controller 110 and the ID and the certificate of the appliance which correspond to the ID of the smart meter 130, to the smart meter 130 (S210).

35 [0105]

The commissioning manager 131 of the smart meter 130 receives, through the AMI network IF 134, the ID and the certificate of the HEMS-controller 110 and the IDs and the certificates of the appliances 140. These IDs and the certificates are saved in the memory 136 of the smart meter 130 (S211).
[0106]

The certification manager 112 of the HEMS-controller 110 transmits the authentication request to the smart meter 130 through the home network IF 114 (S212). The timing for transmitting the authentication request is not particularly limited. For example, the HEMS-controller 110 may transmit the authentication request to the smart meter 130, when notified from the remote server 120 that the remote server 120 has transmitted the ID and the certificate of the HEMS-controller and the IDs and the certificates of the appliances 140 to the smart meter 130. Furthermore, the HEMS-controller 110 may transmit the authentication request to the smart meter 130 after a predetermined time from the time when the HEMS-controller 110 transmitted the ID and the certificate of the HEMS-controller 110 and the IDs and the certificates of the appliances 140 to the remote server 120 (S208).
[0107]

Next, when receiving the authentication request through the home network IF 135, the certification manager 132 of the smart meter 130 compares (i) the certificate which is saved in the memory 136 and corresponds to the ID of the HEMS-controller 110 that transmitted the authentication request and (ii) the certificate received through the home network IF 135 (S213). When both certificates are the same, the smart meter 130 permits (authenticates) connection of the HEMS-controller 110 (S214).
[0108]

Here, at the time of the authentication request, the certificate may be used as it is or an authentication key generated using the certificate may be used. For example, there is the method of generating and using an authentication key using a hash function from a certificate.
[0109]

With the connection permission received from the smart meter 130 through the home network IF 114, it becomes possible for the HEMS-controller 110 to communicate with the smart meter 130.

[0110]

It should be noted that each of the appliances 140 connected to the HEMS-controller 110 is also authenticated by the smart meter 130 using a similar method as the authentication processing (S212 to S214) of the HEMS-controller 110, so that it becomes possible for the appliances 140 to communicate with the smart meter 130 (S215 to S217).

[0111]

The certificates of the HEMS-controller 110 and the appliances 140 may be, for example, the same. Furthermore, it is also acceptable to set the same certificate for the appliances 140 of the same type. Moreover, the certificates of the HEMS-controller 110 and the appliances 140 may be different from one another.

[0112]

The user ID may be an arbitrary ID or information, such as the name or the address of the house of the user.

[0113]

As described above, in the device authentication system 100 according to this embodiment, the HEMS-controller 110 in the house of a user and the appliances 140 connected to the HEMS-controller 110 can be set as the communication target devices of the smart meter 130 through the remote server 120, without intervention of a human. After the setting is made, the HEMS-controller 110 and the appliances 140 connected to the HEMS-controller 110 can be connected to the smart meter 130. Thus, various services using the HEMS-controller 110, the appliances 140, and the smart meter 130 in cooperation with one another can be provided.

[0114]

Furthermore, the smart meter 130 obtains the certificate of the HEMS-controller 110 and the certificates of the appliances 140 based on the authentication table in the remote server 120. More specifically, only the HEMS-controller 110 and the appliances 140 for which the certificates are available can obtain the connection permission. Thus, an unauthorized connection by a device spoofing a communication target device or the like can be prevented.

[0115]

It should be noted that, in the device authentication system 100

according to this embodiment, the operations performed by the HEMS-controller 110 are particularly distinctive.

[0116]

5 The operations performed by the HEMS-controller 110 in Step S203 and Step S204 are so called a pairing operation (second pairing) that connects the HEMS-controller 110 and the appliances 140 via the wireless network. It should be noted that, the second pairing is performed, for example, by simultaneously holding down a button switch provided on the HEMS-controller 110 and a button switch provided on each of the appliances 140.

10 [0117]

The second pairing is performed to enable the HEMS-controller 110 to obtain the IDs and the certificates of the appliances 140. Specifically, the second pairing is, so to speak, a temporary pairing that is performed preliminarily before the final pairing (first pairing) that connects the smart meter 130, the HEMS-controller 110, and the appliances 140 via the wireless network. Therefore, after obtaining the authentication information of the appliances 140, the second pairing is usually canceled before the first pairing is performed.

[0118]

20 Primarily, the second pairing is performed to enable the HEMS-controller 110 to obtain the IDs and the certificates of the appliances 140. However, the second pairing also makes it possible to determine beforehand whether the HEMS-controller 110 and the appliance can be connected via the wireless network.

25 [0119]

For example, with the second pairing, the business operator who installed the device (or the user) can find beforehand whether the HEMS-controller 110 and the appliances 140 are installed at locations in a range which allows wireless network connection. Furthermore, for example, existence or absence of trouble in wireless communication functions of the HEMS-controller 110 and the appliances 140 can also be found beforehand.

[0120]

(Embodiment 2)

FIG. 5 is a system configuration figure of a device authentication system according to Embodiment 2. Different from Embodiment 1, a device

35

authentication system 100a shown in FIG. 5 shows a system configuration which does not include a smart meter 130.

[0121]

In FIG. 5, in a similar manner as in Embodiment 1, the ID and the certificate of a HEMS-controller 110 and the IDs and the certificates of appliances 140 are saved in a database 160 in a remote server 120. For example, the management table in FIG. 5 shows that the HEMS-controller 110 having the ID "Pana3" and appliances having the IDs "AOU2" and "AIU3" are installed for user "Mr. C". Furthermore, the management table in FIG. 5 shows that the certificate of "Pana3", which is the HEMS-controller 110, is "CCC0", and certificates of the appliances "AOU2" and "AIU3" are "CCC1" and "CCC2", respectively.

[0122]

FIG. 6 shows a system configuration figure in which, in addition to the initial state of this embodiment (FIG. 5), a utility system (a utility network 102) including the smart meter 130 is connected to the device authentication system 100a. In FIG. 6, the smart meter 130 which does not exist in the initial state (FIG. 5) is connected to the HEMS-controller 110, and a utility head end 105 starts providing a service to each of users.

[0123]

In the device authentication system 100a, after the utility network 102 is connected to the device authentication system 100a as shown in FIG. 6, ID information of the smart meter 130 is registered into the database 160 in the remote server 120 as with Embodiment 1. When the ID information of the smart meter 130 is registered into the database 160, the remote server 120 creates an authentication table.

[0124]

The authentication processing to the smart meter 130 after the creation of the authentication table is executed in a similar manner as in Embodiment 1.

[0125]

According to this embodiment, before the smart meter 130 is connected to the remote server 120, the HEMS-controller 110 performs beforehand the setting of the appliances 140 connected to the HEMS-controller 110 itself, and transmits the ID and the certificate of the HEMS-controller 110

and the IDs and the certificates of the appliances 140 to the remote server 120.

[0126]

With this, when the smart meter 130 is connected to the remote server 120, the ID and the certificate of the HEMS-controller 110 and the IDs and the certificates of the appliances 140 are already saved in the database 160 in the remote server 120. Thus, an authentication time, which is the time from when the smart meter 130 is connected till when the HEMS-controller 110 and the appliances 140 are authenticated by the smart meter 130, can be reduced.

[0127]

(Embodiment 3)

FIG. 7 is a system configuration figure of a device authentication system according to Embodiment 3. Embodiment 3 describes an example in which, after the network has been formed as described in Embodiment 1, new appliances 140 are connected to a HEMS-controller 110 in a device authentication system 100b.

[0128]

FIG. 7 is a diagram showing an example in which an appliance 143 is newly installed in a house of a user.

[0129]

FIG. 8 is a diagram showing an example of updating of data in a database 160 in a remote server 120, which occurs when the new appliance 143 is connected to the HEMS-controller 110 in Embodiment 3.

[0130]

Shown in (a) in FIG. 8 is a HEMS-C and appliance management table before the installation of the appliance 143. When the new appliance 143 is registered, the HEMS-controller 110 transmits to the remote server 120 the ID and the certificate ((b) in FIG. 8) of the new appliance 143 in a similar manner as in Embodiment 1. FIG. 8 shows an example in which the ID and the certificate of the newly registered appliance 143 are "AIU4" and "CCC3", respectively.

[0131]

When the HEMS-C and appliance management table is updated, the authentication table is also updated, as shown in (c) in FIG. 8. When the authentication table is updated, as described in Embodiment 1, the remote

server 120 transmits the certificate of the new appliance 143 to the smart meter 130. With the certificate of the new appliance 143, the smart meter 130 can authenticate the new appliance 143.

[0132]

5 (Variations)

It should be noted that although the present invention has been described based on the above-described embodiments, the present invention is not limited to these embodiments.

[0133]

10 For example, in each of Embodiments 1 to 3 above, the number of the appliances 140 is two or three. However, the number of the appliances 140 may be four or more. More specifically, irrespective of the number of the appliances 140, authentication processing to the smart meter 130 can be executed.

15 [0134]

Furthermore, although each of the above embodiments described an example in which a single smart meter 130 and a single HEMS-controller 110 are provided in one house, a plurality of the smart meters 130 may be provided in one house, and a plurality of HEMS-controllers 110 may be provided in one house. Furthermore, a plurality of households (users) may be managed by a single smart meter 130, or appliances of a plurality of households (users) may be managed by a single HEMS-controller 110. Furthermore, a plurality of the HEMS-controllers 110 may be connected to a single smart meter 130.

25 [0135]

Furthermore, it has been described in each of the above embodiments that each of the HEMS-controller 110 and the appliances 140 makes the authentication request to the smart meter 130. However, the HEMS-controller 110 may transmit to the smart meter 130, in a batch, an authentication request for the HEMS-controller 110 itself and an authentication request for each of the appliances 140 on which the HEMS-controller 110 performs control. This makes the processing of authentication to the smart meter 130 more easy.

[0136]

35 It should be noted that, although each of the above embodiments

described an example in which the HEMS-controller 110 controls each of the appliances 140, it is also acceptable to have a configuration in which one of the appliances 140 includes the function of the HEMS-controller 110 and controls the rest of the appliances 140. In other words, the HEMS-controller 110 may
5 be implemented as one of the functions of the appliances 140.

[0137]

Furthermore, although a dedicated secure communication network is used for communication between the remote server 120 and the smart meter 130 in each of the above-described embodiments, a general-purpose network,
10 such as the Internet, may be used for communication between the remote server 120 and the smart meter 130. In this case, it is preferable that the ID and the certificate are transmitted in a secure manner, for example by encrypting the ID and the certificate.

[0138]

15 It should be noted that an extensible markup language (XML) or a simple object access protocol (SOAP) may be used for communication between the remote server 120 and the smart meter 130.

[0139]

Furthermore, although the above embodiments described that the
20 HEMS-controller 110 obtains the IDs and the certificates from the appliances 140, the HEMS-controller 110 may obtain only the IDs from the appliances 140.

[0140]

In this case, as the above-described IDs, the HEMS-controller 110
25 obtains, from the appliances 140, manufacturer install codes or other numbers that can identify the appliances 140, and transmits such codes or numbers to the remote server 120. The respective manufacturers of the appliances 140 can uniquely identify each of the appliances 140 with the manufacture install code. Specifically, an example of the manufacture codes is the MAC
30 addresses of the appliances 140.

[0141]

Furthermore, for example, Zigbee manufacturer specific extension codes may be used as the IDs of the appliances 140. The extended codes are the codes that are assigned when the HEMS-controller 110 and the appliances
35 140 are connected wirelessly via Zigbee.

[0142]

As above, in the case where the HEMS-controller 110 obtains from the appliances 140 only the IDs, the manufacturer of the appliances 140 creates a database of the IDs of the appliances 140 and certificates corresponding to the IDs. Furthermore, the remote server 120 accesses the database or stores therein the database in advance. With this, by obtaining only the ID from the HEMS-controller 110, the remote server 120 can transmit to the smart meter 130 the corresponding certificate.

[0143]

Such a configuration is more secure because transmitting and receiving of the certificate is not performed between the HEMS-controller 110 and the remote server 120.

[0144]

Furthermore, the configuration in which the HEMS-controller 110 queries the remote server 120 to find out whether the HEMS-controller 110 is selecting the correct smart meter 130 corresponding to the HEMS-controller 110 is also acceptable.

[0145]

When a plurality of the wirelessly connectable smart meters 130 exist, there are cases where the HEMS-controller 110 cannot determine which one of the smart meters 130 is the correct smart meter 130 corresponding to the HEMS-controller 110 itself. In such a case, the HEMS-controller 110 may transmit to the remote server 120 a query request regarding the smart meter 130. At this time, along with the query request, the HEMS-controller 110 may transmit, as position information of the detected nearby smart meters 130, a relative strength of the signal used for wireless communication, GPS coordinates, fingerprints of the wireless environment, or the like of each of the smart meters 130.

[0146]

When receiving the query request from the HEMS-controller 110, the remote server 120 further retrieves related information, such as the customer premise postal address in the house of the user in which the HEMS-controller 110 is provided, a customer name, and a customer identifier (e.g., a national registration number, a driving license number, and a passport number). It should be noted that such information may have been obtained at the time of

a customer registration for a service that uses the remote server 120 or the smart meter 130. Based on the retrieved information, the remote server 120 notifies the HEMS-controller 110 the correct smart meter 130 which corresponds to the HEMS-controller 110.

5 [0147]

Furthermore, at this time, the remote server 120 may query the utility network 102 (the utility head end 105) to find out which one of the smart meters 130 is the correct smart meter 130 corresponding to the HEMS-controller 110.

10 [0148]

At this time, a part of the customer identifier above may be used as a basis which enables the utility network 102 to determine the correct smart meter 130.

[0149]

15 Furthermore, the present invention also includes the following.

[0150]

(1) Each of the above apparatuses can be, specifically, realized by a computer system configured from a microprocessor, a ROM, a RAM, a hard disk unit, a display unit, a keyboard, and a mouse, for example. A computer
20 program is stored in the RAM or the hard disk unit. Each of the apparatuses achieves its function as a result of the microprocessor operating according to the computer program. Here, the computer program is configured of a plurality of pieced together instruction codes indicating a command to the computer in order to achieve a given function.

25 [0151]

(2) A portion or all of the structural elements of each of the above apparatuses may be configured from one system large scale integration (LSI). A system LSI is a super-multifunction LSI manufactured with a plurality of structural units integrated on a single chip, and is specifically a computer
30 system configured of a microprocessor, a ROM, and a RAM, for example. A computer program is stored in the ROM. The system LSI achieves its function as a result of the microprocessor loading the computer program into the RAM from the ROM, and performing an operation or the like according to the loaded computer program.

35 [0152]

(3) A portion or all of the structural elements of each of the above apparatuses may each be configured from an IC card detachable from the apparatus or a stand-alone module. The IC card or the module is a computer system configured from a microprocessor, a ROM, and a RAM, for example.

5 The IC card or the module may include the super-multifunction LSI described above. The IC card or the module achieves its function as a result of the microprocessor operating according to a computer program. The IC card and the module may be tamper-proof.

[0153]

10 (4) The present invention may be realized using a method shown above. Moreover, the present invention may also be realized by a computer program realizing these methods with a computer or by a digital signal of the computer program.

[0154]

15 Moreover, the present invention may also be realized as a computer-readable recording medium, such as a flexible disk, a hard disk, a CD-ROM, a MO, a DVD, a DVD-ROM, a DVD-RAM, a Blu-ray disc (BD), or a semiconductor memory, on which the computer program or the digital signal is recorded. The present invention may also be realized by the digital signal
20 recorded in the above mentioned recording media.

[0155]

Moreover, the present invention may also be realized by transmitting the computer program or the digital signal, via an electric communication line, a wireless or wired line, a network typified by the Internet, data broadcasting,
25 or the like.

[0156]

Moreover, the present invention may be a computer system including a microprocessor and a memory, the memory storing the computer program and the microprocessor operating according to the computer program.

30 [0157]

Moreover, the program or the digital signal may be executed by another independent computer system, with the program or the digital signal recorded and transported in a recording media or with the program or the digital signal transported via the network or the like.

35 [0158]

(5) The above embodiments and variations may be combined with each other.

[0159]

Although the device authentication system according to one or more
5 aspects have been thus far described based on the embodiments, the present
invention is not limited to these embodiments. Various modifications of the
embodiments as well as embodiments resulting from combinations of
structural elements of different embodiments that may be conceived by those
skilled in the art may also be included within the scope of the one or more
10 aspects as long as these do not depart from the essence of the present
invention.

[0160]

[Industrial Applicability]

The present invention is useful as a device authentication method or
15 the like used for authentication of a device by a smart meter in a home energy
management system (HEMS) or the like.

[Reference Signs List]

[0161]

100, 100a, 100b Device authentication system
20 101 Home network
102 Utility network
103 Packet network
104 AMI
105 Utility head end
25 110 HEMS-controller
111, 131 Commissioning manager
112, 132 Certification manager
113 Gathering manager
114, 135 Home network IF
30 115, 125 Packet network IF
116, 136 Memory
120 Remote server
121 System manager
124, 134 AMI network IF
35 130 Smart meter

140, 141, 142, 143 Appliance
160, 170 Database

[CLAIMS]

[Claim 1]

A method of setting an identification (ID) and a certificate for each of devices to a smart meter, the ID and the certificate being used for authentication for network connection between the smart meter and the devices, the method comprising:

obtaining, from a smart meter connected via a first communication network, an ID of the smart meter associated with user information of the smart meter;

obtaining, from a controller which is one of the devices connected via a second communication network, (i) an ID and a certificate of the controller associated with user information of the controller and (ii) an ID and a certificate of an appliance which is one of the devices controlled by the controller;

generating, based on the user information of the smart meter and the user information of the controller, management information in which the ID of the smart meter, the ID and the certificate of the controller, and the ID and the certificate of the appliance are associated with one another; and

transmitting, based on the management information, the ID and the certificate of the controller and the ID and the certificate of the appliance which are associated with the ID of the smart meter, to the smart meter.

[Claim 2]

The method according to Claim 1,

wherein, when new device information that is (i) an ID and a certificate of the controller which are not included in the management information or (ii) an ID and a certificate of the appliance which are not included in the management information is obtained via the second communication network:

in the generating, the management information is updated by adding the new device information to the management information in association with the ID of the smart meter; and

in the transmitting, the new device information is transmitted to the smart meter having the ID associated with the new device information.

[Claim 3]

The method according to one of Claim 1 and Claim 2,
wherein the first communication network is a secure communication
network dedicated to communication with the smart meter.

5 [Claim 4]

The method according to any one of Claims 1 to 3,
wherein the controller is a home energy management system (HEMS)
controller which controls a device among the devices.

10 [Claim 5]

The method according to any one of Claims 1 to 4,
wherein the ID of each of the devices is a media access control (MAC)
address.

15 [Claim 6]

A device authentication method for authenticating network connection
between a smart meter and a plurality of devices by using a server, the method
comprising:

(a) obtaining, by a controller which controls an appliance, an
20 identification (ID) and a certificate of the appliance, the controller and the
appliance each being one of the devices;

(b) transmitting, by the controller, the ID and the certificate of the
appliance obtained in step (a) to the server;

(c) obtaining, by the server, an ID of the smart meter associated with
25 user information of the smart meter;

(d) obtaining, by the server, an ID and a certificate of the controller and
the ID and the certificate of the appliance which are associated with user
information of the controller;

(e) generating, by the server, management information based on the
30 user information of the smart meter and the user information of the controller,
the management information including the ID of the smart meter obtained in
step (c), and the ID and the certificate of the controller and the ID and the
certificate of the appliance obtained in step (d) in association with one another;
and

35 (f) transmitting, by the server, based on the management information,

the ID and the certificate of the controller and the ID and the certificate of the appliance which are associated with the ID of the smart meter, to the smart meter.

5 [Claim 7]

The method according to Claim 6, the method further comprising:

(g) obtaining, by the smart meter, the ID and the certificate of the controller and the ID and the certificate of the appliance from the server; and

10 (h) when the smart meter receives an authentication request from the controller or the appliance, (i) determining, by the smart meter, whether an ID and a certificate included in the authentication request match the ID and the certificate obtained in step (g) and, (ii) when the ID and the certificate in the authentication request match the ID and the certificate obtained in step (g),
15 permitting, by the smart meter, a network connection between the controller or the appliance which transmitted the authentication request and the smart meter, the authentication request being information which requests authentication.

20 [Claim 8]

The method according to one of Claim 6 and Claim 7,

wherein in step (a), the controller communicates with the appliance by a wireless communication compliant with a Zigbee standard to obtain the ID and the certificate of the appliance.

25

[Claim 9]

A device authentication system in which an identification (ID) and a certificate of each of devices are set to a smart meter by a server, the ID and the certificate being used for authentication for network connection between
30 the smart meter and the devices, the system comprising:

a controller which controls an appliance, the controller and the appliance each being one of the devices; and

the server,

wherein the controller includes:

35 a first communication unit configured to obtain an ID and a certificate

of the appliance; and

a second communication unit configured to transmit the ID and the certificate of the appliance obtained by the first communication unit to the server, and

5 the server includes:

a first obtainment unit configured to obtain an ID of the smart meter associated with user information of the smart meter;

a second obtainment unit configured to obtain an ID and a certificate of the controller and the ID and the certificate of the appliance which are
10 associated with user information of the controller;

a system manager which generates, based on the user information of the smart meter and the user information of the controller, management information in which the ID of the smart meter obtained by the first obtainment unit, and the ID and the certificate of the controller and the ID and
15 the certificate of the appliance obtained by the second obtainment unit are associated with one another; and

a transmitting unit configured to transmit, based on the management information, the ID and the certificate of the controller and the ID and the certificate of the appliance which are associated with the ID of the smart meter,
20 to the smart meter.

[Claim 10]

A controller which performs communication for a first pairing that is a wireless network connection between a device and a smart meter, the first
25 pairing being performed after a server transmitted authentication information of the device to the smart meter, the controller comprising:

a first communication unit configured to perform a second pairing which is a wireless network connection with the device, to obtain authentication information of the device; and

30 a second communication unit configured to transmit the authentication information of the device obtained by the first communication unit, to the server.

[Claim 11]

35 The controller according to Claim 10,

wherein the first communication unit is configured to, after obtaining the authentication information of the device, cancel the second pairing before the first pairing is performed.

5 [Claim 12]

The controller according to one of Claim 10 and Claim 11,
wherein the first pairing and the second pairing are wireless network connections compliant with a Zigbee standard.