[DESCRIPTION]

[Title of Invention]

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

[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.

[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.

[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.

[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.

[Citation List]

[Patent Literature]

[0005]

[PTL 1]

US Patent Application Publication No. 2011/0047370

[PTL 2]

US Patent No. 7950044

[PTL 3]

US Patent Application Publication No. 2011/0302635

[Summary of Invention]

[Technical Problem]

[0006]

For the communication between a smart meter, a HEMS-controller, and 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]

Embodiments of~~In view of this,~~ the present invention provides, for example, a method 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 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 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.~~In a first aspect, there is provided a method of setting an identification (ID) and authentication information for each of devices to a smart

meter, the ID and the authentication information being used for authentication for network connection between the smart meter and the devices, the method comprising: obtaining an ID of the smart meter connected via a first communication network, the ID being associated with user information of the smart meter; obtaining (i) an ID and authentication information of a controller which are associated with user information of the controller connected via a second communication network and (ii) an ID and authentication information of an appliance, the controller and the appliance each being one of the devices; 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 authentication information of the controller, and the ID and the authentication information of the appliance are associated with one another; and transmitting, based on the management information, the ID and the authentication information of the controller and the ID and the authentication information of the appliance which are associated with the ID of the smart meter, to the smart meter.

[0008a]

In a second aspect, there is provided a device authentication method for authenticating network connection between a smart meter and a plurality of devices by using a server connected to (i) the smart meter via a first communication network and (ii) a controller, which is one of the devices, via a second communication network, the method comprising: (a) obtaining, by the controller, an identification (ID) and authentication information of an appliance that is one of the devices; (b) transmitting, by the controller, the ID and the authentication information of the appliance obtained and the ID and the authentication information of the controller to the server; (c) obtaining, by the server, an ID of the smart meter, the ID being associated with user information of the smart meter; (d) obtaining, by the server, the ID and the authentication information of the controller and the ID and the authentication information 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, in association with one another, the ID of the smart meter, and the ID and the authentication information of the controller and the ID and the authentication information of the appliance obtained; and (f) transmitting, by the server, based on the management information, the ID and the authentication information of the controller and the ID and the authentication information of the appliance which are associated with the ID of the smart meter, to the smart meter.

[0008b]

In a third aspect, there is provided a device authentication system in which an identification (ID) and authentication information of each of devices are set to a smart meter by a server, the ID and the authentication information being used for authentication for network connection between the smart meter and the devices, the system comprising: a controller that is one of the devices; and the server connected to (i) the controller via a first communication network and (ii) the smart meter via a second communication network, wherein the controller includes: a first communication unit configured to obtain an ID and authentication information of an appliance that is one of the devices; and a second communication unit configured to transmit (i) the ID and the authentication information of the appliance obtained by the first communication unit and (ii) the ID and the authentication information of the controller to the server, and the server includes: a first obtainment unit configured to obtain an ID of the smart meter, the ID being associated with user information of the smart meter; a second obtainment unit configured to obtain an ID and authentication information of the controller and the ID and the authentication information 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 authentication information of the controller and the ID and the authentication information 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 authentication information of the controller and the ID and the authentication information of the appliance which are associated with the ID of the smart meter, to the smart meter.

[0008c]

In a fourth aspect, there is provided a server which sets an identification (ID) and authentication information for each of devices to a smart meter, the ID and the authentication information being used for authentication for network connection between the smart meter and the devices, the server comprising: a first obtainment unit configured to obtain an ID of the smart meter connected via a first communication network, the ID being associated with user information of the smart meter; a second obtainment unit configured to obtain (i) an ID and authentication information of a controller which are associated with user information of the controller connected via a second communication network and (ii) an ID and authentication information of an appliance, the controller and the appliance each being one of the devices; 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 authentication information of the controller and the ID and the authentication information 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 authentication information of the controller and the ID and the authentication information of the appliance which are 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 of apparatuses, systems, integrated circuits, computer programs, or

computer-readable recording media.

[Advantageous Effects of Invention]

[0010]

According to embodiments of the present invention, ID and certificate information of a 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 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]

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 Embodiment 1.

[FIG. 4]

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

[FIG. 5]

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.

[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 database in a remote server, which occurs when a new appliance is connected

[CLAIMS]

[Claim 1]

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

obtaining~~, from a~~ an ID of the smart meter connected via a first communication network, ~~an ID of the smart meter~~the ID being 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~~authentication information of ~~the~~a controller which are associated with user information of the controller connected via a second communication network and (ii) an ID and ~~a certificate~~authentication information of an appliance ~~which is~~, the controller and the appliance each being 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~~authentication information of the controller, and the ID and the ~~certificate~~authentication information of the appliance are associated with one another; and

transmitting, based on the management information, the ID and the ~~certificate~~authentication information of the controller and the ID and the ~~certificate~~authentication information 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 the ID of the smart meter and the user information of the smart meter are managed in a predetermined storage unit and associated with each other,

the ID of the controller and the user information of the controller are managed in the predetermined storage unit and associated with each other, and

in the generating of management information, the management

information is generated by referring to the predetermined storage unit.

[Claim 3]

The method according to Claim 1,

wherein the ID of the smart meter includes the user information of the smart meter and is associated with the user information of the smart meter, and

the ID of the controller includes the user information of the controller and is associated with the user information of the controller.

[Claim 4]

The method according to Claim 1,

wherein the ID of the smart meter is obtained along with the user information of the smart meter and is associated with the user information of the smart meter, and

the ID of the controller is obtained along with the user information of the controller and is associated with the user information of the controller.

~~[Claim 2]~~[Claim 5]

The method according to ~~Claim 1,~~any one of Claims 1 to 4, further comprising:

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

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

~~[Claim 3]~~[Claim 6]

The method according to ~~one of Claim 1 and Claim 2,~~any one of Claims

1 to 5,

wherein the first communication network is a secure communication network dedicated to communication with the smart meter.

[Claim 4][Claim 7]

The method according to any one of Claims 1 to 3,to 6,

wherein the controller is a home energy management system (HEMS) controller which controls a device among the devices.

[Claim 5][Claim 8]

The method according to any one of Claims 1 to 4,to 7,

wherein the ID of each of the devices is a media access control (MAC) address.

[Claim 6][Claim 9]

A device authentication method for authenticating network connection between a smart meter and a plurality of devices by using a server connected to (i) the smart meter via a first communication network and (ii) a controller, which is one of the devices, via a second communication network, the method comprising:

(a) obtaining, by athe controller which controls an appliance, an identification (ID) and a certificateauthentication information of thean appliance, the controller and the appliance each being that is one of the devices;

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

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

(d) obtaining, by the server, anthe ID and a certificatethe authentication information of the controller and the ID and the certificateauthentication information 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, in association with one another, the ID of the smart meter ~~obtained in step (c)~~, and the ID and the ~~certificate~~authentication information of the controller and the ID and the ~~certificate~~authentication information 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~~authentication information of the controller and the ID and the ~~certificate~~authentication information of the appliance which are associated with the ID of the smart meter, to the smart meter.

~~[Claim 7]~~[Claim 10]

The method according to ~~Claim 6~~Claim 9, the method further comprising:

(g) obtaining, by the smart meter, the ID and the ~~certificate~~authentication information of the controller and the ID and the ~~certificate~~authentication information 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~~authentication information included in the authentication request match the ID and the ~~certificate~~authentication information obtained in step (g) and, (ii) when the ID and the ~~certificate~~authentication information in the authentication request match the ID and the ~~certificate~~authentication information 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.

~~[Claim 8]~~[Claim 11]

The method according to one of Claim ~~6 and Claim 7,~~9 and Claim 10,

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

~~[Claim 9]~~[Claim 12]

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

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

the server connected to (i) the controller via a first communication network and (ii) the smart meter via a second communication network,

wherein the controller includes:

a first communication unit configured to obtain an ID and ~~a certificate~~authentication information of ~~the~~an appliance that is one of the devices; and

a second communication unit configured to transmit (i) the ID and the ~~certificate~~authentication information of the appliance obtained by the first communication unit ~~to the server~~ and (ii) the ID and the authentication information of the controller to the server, and

the server includes:

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

a second obtainment unit configured to obtain an ID and ~~a certificate~~authentication information of the controller and the ID and the ~~certificate~~authentication information 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~~authentication information of the controller and the ID and the ~~certificate~~authentication information 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~~authentication information of the controller and the ID and the ~~certificate~~authentication information of the appliance which are associated with the ID of the smart meter, to the smart

meter.

[Claim 13]

A server which sets an identification (ID) and authentication information for each of devices to a smart meter, the ID and the authentication information being used for authentication for network connection between the smart meter and the devices, the server comprising:

a first obtainment unit configured to obtain an ID of the smart meter connected via a first communication network, the ID being associated with user information of the smart meter ;

a second obtainment unit configured to obtain (i) an ID and authentication information of a controller which are associated with user information of the controller connected via a second communication network and (ii) an ID and authentication information of an appliance, the controller and the appliance each being one of the devices;

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 authentication information of the controller and the ID and the authentication information 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 authentication information of the controller and the ID and the authentication information of the appliance which are associated with the ID of the smart meter, 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 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~~

~~a second communication unit configured to transmit the authentication~~

~~information of the device obtained by the first communication unit, to the server.~~

~~[Claim 11]~~

~~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.~~

~~[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.~~