

CLAIMS

[Claim 1]

5 A client-side communication control device connectable to a gateway, which is provided between a client device and a network communication grid, and the client device, the client-side communication control device comprising:

an authentication unit; and

10 a control unit that is configured to request the authentication unit to perform at least ~~one of~~ a mutual authentication process among the mutual authentication process and an encryption/decryption process, the mutual authentication process performing mutual authentication in communication with a server-side communication control device using a client secret key and a client certificate, the client secret key and the client certificate being issued by a private authentication authority, transmitted to the client-side communication control device by the private authentication authority, and
15 stored in the authentication unit, the private authentication authority transmitting to the server-side communication control device a server secret key and a server certificate to be used for a server device, the server device being a communication destination of the client device, the private authentication authority being separated from the server device, the server-side communication control device being connected to the server device and
20 the network communication grid, the encryption/decryption process encrypting information, that is transmitted to the server device by the client device, using a common key determined for communication between the client-side communication control device and the server-side communication control device, the encryption/decryption process decrypting information, that is transmitted to the client
25 device by the server device, using the common key,

wherein

the client-side communication control device communicates by wire with the client device in plaintext, and

30 the client-side communication control device communicates by wire with the gateway.

[Claim 2]

The client-side communication control device according to claim 1, wherein the control unit requests the authentication unit to perform the mutual authentication in communication with a communication device transmitting information to the client device, determines whether or not to permit communication with the client device for
5 the communication device on the basis of a result of the mutual authentication, and transmits a determination result to the private authentication authority.

[Claim 3]

The client-side communication control device according to claim 1 or claim 2,
10 wherein the control unit requests the authentication unit to perform a firmware verification process of performing verification of whether or not details of information about firmware of the client device transmitted to the client device are correct using a key issued by the private authentication authority.

15 [Claim 4]

The client-side communication control device according to any one of claims 1 to 3, wherein the authentication unit determines whether or not to permit communication with the client device for a communication device transmitting information to the client device on the basis of a transmission destination list indicating
20 information about communication equipment for which communication with the client device is permitted.

[Claim 5]

The client-side communication control device according to any one of claims 1
25 to 4, wherein the client-side communication control device receives from the private authentication authority the client certificate updated on the basis of a validity period.

[Claim 6]

The client-side communication control device according to any one of claims 1
30 to 5, wherein the client certificate is invalidated by the private authentication authority when validity has not been mutually proved in the mutual authentication process of the client-side communication control device.

[Claim 7]

~~———— A server side communication control device connectable to a server device and a network communication grid, the server side communication control device comprising:~~

5 ~~———— an authentication unit; and~~

~~———— a control unit that is configured to request the authentication unit to perform at least one of a mutual authentication process and an encryption/decryption process, the mutual authentication process performing mutual authentication in communication with a client side communication control device using a server secret key and a server certificate, the server secret key and the server certificate being issued by a private authentication authority, transmitted to the server side communication control device by the private authentication authority, and stored in the authentication unit, the private authentication authority transmitting to the client side communication control device a client secret key and a client certificate to be used for a client device, the client device being a communication destination of the server device, the client side communication control device being connected to the client device and the network communication grid, the encryption/decryption process encrypting information, that is transmitted to the client device by the server device, using a common key determined for communication between the server side communication control device and the client side communication control device, the encryption/decryption process decrypting information, that is transmitted to the server device by the client device, using the common key.~~

10
15
20

[Claim 8]

25 ~~———— The server side communication control device according to claim 7, wherein the control unit requests the authentication unit to perform the mutual authentication in communication with a communication device transmitting information to the server device, determines whether or not to permit communication with the server device for the communication device on the basis of a result of the mutual authentication, and~~

30 ~~transmits a determination result to the private authentication authority.~~

[Claim 9]

~~—— The server side communication control device according to claim 7 or claim 8, wherein the control unit requests the authentication unit to perform a firmware verification process of performing verification of whether or not details of information about firmware of the server device transmitted to the server device are correct using a~~
5 ~~key issued by the private authentication authority.~~

~~{Claim 10}~~

~~—— The server side communication control device according to any one of claims 7 to 9, wherein the authentication unit determines whether or not to permit~~
10 ~~communication with the server device for a communication device transmitting information to the server device on the basis of a transmission destination list indicating information about communication equipment for which communication with the server device is permitted.~~

15 ~~{Claim 11}~~

~~—— The server side communication control device according to any one of claims 7 to 10, wherein the server side communication control device receives from the private authentication authority the server certificate updated on the basis of a validity period.~~

20 ~~{Claim 12}~~

~~—— The server side communication control device according to any one of claims 7 to 11, wherein the server certificate is invalidated by the private authentication authority when validity has not been mutually proved in the mutual authentication process of the server side communication control device.~~