another device such as the IoT device 3. The SDK 12 is configured to be communicable with an SDK server 31, an issuance data generation server 32, and a private certificate authority (CA) 33, via a network such as the Internet. The SDK server 31 performs update of the function of the SDK 12, and the like. The issuance data generation server 32 and the private CA 33 perform issuance of a public key, issuance of a public key certificate, verification of an issuer's signature, and the like.

[0012] The IoT device 3 of the present embodiment is a device, an apparatus, a sensor, or the like having a predetermined function, and can be, for example, a home appliance, a camera, an automobile, a measuring instrument, or the like. The IoT device 3 is communicable with the communication device 2 via a predetermined network.

[0013] The IoT device 3 of the present embodiment includes an APL 21, a secure element (SE) 22, and a generic trust anchor application programming interface (GTAAPI) 23. The APL 21 is software for causing the IoT device 3 to implement a predetermined function. The SE 22 is a device that performs an encryption process, data protection, and the like for establishing the secure channel in communication with another device such as the communication device 2. The GTAAPI 23 has functions for implementing data relay between the SE 22 and the APL 21, establishment of the secure channel in communication with the other device such as the communication device 2, and the like. The GTAAPI 23 is configured to be communicable with a GTAAPI server 34, the issuance data generation server 32, and the private CA 33 via a network such as the Internet. The GTAAPI server 34 updates the function of the GTAAPI 23, and the like.

[0014] The communication device 2 and the IoT device 3 of the present embodiment use the functions of the SDK 12 and the SE22 to establish short range wireless communication such as Bluetooth (registered trademark), Wi-Fi (registered trademark), and NFC (registered trademark).

and L2. Similarly to the lists L1 and L2 stored in the storage unit 102 of the communication device 2, the lists L1 and L2 stored in the storage unit 201 each indicate the first information and the second information. The list L1 corresponds to the communication device 2, and the list L2 corresponds to the IoT device 3. In the IoT device 3, the list L2 is stored in advance in the storage unit 102, and the list L1 is acquired from the communication device 2 via the predetermined short range wireless communication and stored in the storage unit 201. Note that the above storage process may be performed by the SE 22.

[0026] The setting unit 202 performs settings related to the lists L1 and L2 through operation of an administrator of the IoT device 3. The setting unit 202 enables editing of the contents of the list L2 corresponding to the IoT device 3. Moreover, the setting unit 202 enables setting of, for example, whether to permit use of the list L1 acquired from the communication device 2. In addition, for example, the setting unit 202 enables setting of whether to permit transfer of the first information indicated by the list L1 acquired from the communication device 2 by the IoT device 3, to another device other than the IoT device 3 and the communication device 2. Note that the above setting process may be performed by the SE 22.

[0027] The communication unit 203 establishes communication between the IoT device 3 and the other device. The communication unit 203 establishes communication between the IoT device 3 and the communication device 2 via the predetermined short range wireless communication. Moreover, the communication unit 203 establishes communication between the IoT device 3 and a predetermined device (e.g., the SDK server 31, the issuance data generation server 32, the private CA 33, and the like.) via the appropriate network N such as a wide area network (WAN) or a local area network (LAN).

[0028] The authentication unit 204 performs the encryption process for establishing the secure channel in communication by the communication unit 203. Moreover, the authentication unit 204 performs a mutual authentication process for establishing the

Moreover, the IoT device 3A establishes a predetermined secure channel with the IoT device 3B as the other device (S411), and transfers the first information 301 acquired from the communication device 2A, to the IoT device 3B (S412).

[0053] By the above-described process, the first information 301 that is exchangeable without mutual authentication can be relayed and distributed among multiple devices.

[0054] As described above, according to the present embodiment, the lists L1 and L2 each indicating the first information that is exchangeable when no mutual authentication is performed and the second information that is exchangeable when the mutual authentication is performed are exchanged between the communication device 2 and the IoT device 3, and the processes such as information exchange and transfer are performed on the basis of the lists L1 and L2. This configuration makes it possible for the communication device 2 and the IoT device 3 to exchange the first information determined in advance (e.g., information with relatively low confidentiality or the like) without performing the mutual authentication, improving the degree of freedom and convenience of communication in the IoT system 1. In addition, when the mutual authentication is performed, it is possible to efficiently perform the process (e.g., encryption process or the like) for establishing the mutual authentication by using the second information.

[0055] A program for implementing the functions of the communication device 2 and the IoT device 3 in the IoT system 1 of the present embodiment may be configured to be provided by being recorded in the form of installable or executable file, on a computer-readable recording medium, such as a CD-ROM, a flexible disk (FD), a CD-R, and a digital versatile disk (DVD). In addition, the program may be configured to be stored on a computer connected to the network such as the Internet and provided by being downloaded via the network. Moreover, the program may be configured to be provided or distributed via the network such as the Internet.

[0056] Although the embodiments of the present invention have been described above, the above embodiments are merely examples, and are not intended to limit the scope of

CLAIMS

Claim 1. An IoT system comprising:

a communication device capable of identifying a user via a security device; and

an IoT device including a secure element, the secure element performing an encryption process for establishing a secure channel with the communication device, wherein

the communication device and the IoT device each stores a list indicating first information and second information, the first information being exchangeable when no mutual authentication is performed between the communication device and the IoT device, the second information being exchangeable when the mutual authentication is performed,

the communication device is configured to

acquire the list from the IoT device, and,

based on the acquired list, transmit the first information to the IoT device when the mutual authentication is not performed and transmit the second information to the IoT device when the mutual authentication is performed, and

the IoT device is configured to

acquire the list from the communication device, and,

based on the acquired list, transmit the first information to the communication device when the mutual authentication is not performed and transmit the second information to the communication device when the mutual authentication is performed.

Claim 2. The IoT system according to claim 1, wherein

the list includes information indicating whether the first information is transferable to another communication device or another IoT device, the other communication device or the other IoT device being different from the communication device and the IoT device between which the lists have been exchanged, and,

when the first information is transferable, the communication device and the IoT device between which the lists have been exchanged transfer the first information to the other communication device or the other IoT device.

Claim 3. The IoT system according to claim 2, wherein the communication device is configured to enable setting of whether to transfer the first information, the setting being performed through operation of a user who is identified by the security device.

Claim 4. The IoT system according to claim 2, wherein the IoT device is configured to enable setting of whether to transfer the first information, the setting being performed through operation of an administrator who is registered in advance in the IoT device.

Claim 5. The IoT system according to claim 1, wherein the communication device is configured to enable setting of availability of the list acquired from the IoT device, the setting being performed through operation of a user who is identified by the security device.

Claim 6. The IoT system according to claim 1, wherein the IoT device is configured to enable setting of availability of the list acquired from the communication device, the setting being performed through operation of an administrator who is registered in advance in the IoT device.

Claim 7. The IoT system according to claim 1, wherein the second information includes information about an authentication algorithm and a key used for performing the mutual authentication.

Claim 8. A computer-readable recording medium on which a program executable by a computer of a communication device is recorded, the program causing the communication device to perform processing, the communication device capable of identifying a user via a security device and capable of communicating with an IoT device, the IoT device including a secure element performing an encryption process for establishing a secure channel, the processing comprising:

a process of exchanging, with the IoT device, lists each indicating first information and second information, the first information being exchangeable when no mutual authentication is performed between the communication device and the IoT device, the second information being exchangeable when the mutual authentication is performed; and

a process of, based on the list acquired from the IoT device, transmitting the first information to the IoT device when the mutual authentication is not performed and transmitting the second information to the IoT device when the mutual authentication is performed.