

[0117]

If the certification path is not being used (No in step S605), the certification path is deleted (S606) and the certificate specified by CertificateID is deleted (S607). Thereafter, a key pair associated with the certificate is deleted. A key pair may not be deleted by any security command of the DM service, and therefore, the key pair is required to be deleted by the DeleteCertificates command.

[0118]

However, since the key pair may be associated with another certificate, it is determined whether the key pair is associated with another certificate in step S610. If the key pair is not associated with another certificate (TRUE in step S608), the key pair associated with the certificate which is a target of the deletion is deleted (S609). If the key pair is associated with another certificate (FALSE in step S608), the key pair is not deleted. Since the DeleteCertificates command may specify a plurality of CertificateIDs, if next CertificateID exists (Yes in step S610), the deletion process is performed on next Certificate ID (the process returns to step S603). After all CertificateIDs have been processed (No in step S610), the DM service unit 112 transmits information indicating that the process has been successfully terminated to the client apparatus 200.

CLAIMS

[Claim 1]

An information processing apparatus comprising:

first processing means for performing a setting for performing encrypted communication on the information processing apparatus in response to a command based on the device management service defined in the ONVIF standard;

second processing means for performing a setting for performing encrypted communication on the information processing apparatus in response to a command based on the advanced security service defined in the ONVIF standard; and

transmitting means for transmitting information indicating that the setting for performing the encrypted communication is made in response to the command based on the device management service to an external apparatus if the command based on the advanced security service is received from the external apparatus after the first processing means performs the setting for performing the encrypted communication on the information processing apparatus in response to the command based on the device management service.

[Claim 2]

The information processing apparatus according to claim 1, further comprising:

control means for performing control such that

information indicating that the setting has been performed on the information processing apparatus in response to the command based on the device management service is recorded in recording means.

[Claim 3]

The information processing apparatus according to claim 2, wherein

the first processing means executes a command for setting to the information processing apparatus at least one of first public key information which is used to perform the encrypted communication, first private key information which corresponds to the first public key information and which is used to perform the encrypted communication, and first certificate information which proves that the public key information is valid key information, the command being executed by a first external apparatus on the information processing apparatus on the basis of the device management service, and

the second processing means executes a command for setting to the information processing apparatus at least one of key pair information indicating that second public key information used to perform the encrypted communication corresponds to second private key information used to perform the encrypted communication, second certificate information which proves that the second public key

information is valid key information, and certification path information indicating third certificate information associated with the second certificate information, the command being executed by a second external apparatus on the information processing apparatus on the basis of the advanced security service.

[Claim 4]

The information processing apparatus according to Claim 2, wherein

the first processing means executes at least one of a command for recording in the recording means first key pair information indicating that first public key information used to perform the encrypted communication corresponds to first private key information used to perform the encrypted communication, a command for transmitting the first key pair information from the transmitting means, a command for disabling the first key pair information recorded in the recording means, and a command for generating certificate information which proves that the first public key information is valid key information and which includes sign information added thereto by the first processing means, the commands being executed by a first external apparatus on the information processing apparatus on the basis of the device management service,

the second processing means executes a command for

recording in the recording means at least one of key pair information indicating that second public key information used to perform the encrypted communication corresponds to second private key information used to perform the encrypted communication, second certificate information which proves that the second public key information is valid key information, and certification path information indicating third certificate information associated with the second certificate information, the command being executed by a second external apparatus on the information processing apparatus on the basis of the advanced security service, and

the transmitting means transmits, in response to the command based on the advanced security service, information indicating that a setting has been performed with the information processing apparatus in response to the command based on the device management service.

[Claim 5]

The information processing apparatus according to claim 3, wherein

the first processing means generates certificate information which proves that the public key information is valid key information and which includes sign information added thereto by the first processing means, the key pair information, and the certification path information in response to a command which is based on the device

management service and which is issued for generating the first certificate information, and records the certificate information, the key pair information, and the certification path information in the recording means, and

the control means performs control such that information indicating that the certificate information, the key pair information, and the certification path information have been generated in response to the command based on the device management service is recorded in the recording means.

[Claim 6]

The information processing apparatus according to claim 3, wherein

the first processing means executes a first command which is based on the device management service and which is issued for requesting disabling of the certificate information recorded in the recording mean so as to disable the key pair information corresponding to the certificate information specified by the first command or the certification path information corresponding to the certificate information specified by the first command.

[Claim 7]

The information processing apparatus according to claim 3, wherein

the certification path information indicates order of

reference of a plurality of certificate information recorded in the recording means performed by the information processing apparatus for performing the encrypted communication, and

in response to a second command which is used to specify certificate information to be used for the encrypted communication and which is based on the device management service, the first processing means records in the recording means the certification path information indicating that certificate information corresponding to identification information specified by the second command is in a leading portion of the order as certification path information to be used for performing the encrypted communication.

[Claim 8]

The information processing apparatus according to claim 3, wherein

the certification path information indicates order of reference of a plurality of certificate information recorded in the recording means performed by the information processing apparatus for performing the encrypted communication, and

the transmitting means transmits information indicating certificate information, among the plurality of certificate information recorded in the recording means, indicating that the certification path information is in a leading portion

of the order in response to a command which is based on the device management service and which is issued for requesting transmission of information on the certificate information recorded in the recording means.

[Claim 9]

The information processing apparatus according to claim 3, wherein

the certification path information indicates order of reference of a plurality of certificate information recorded in the recording means performed by the information processing apparatus for performing the encrypted communication, and

in response to a third command for requesting obtainment of information indicates whether certificate information recorded in the recording means is set as a certificate information used for performing the encrypted communication, the first processing means records in the recording means information indicating that fourth certificate information indicating that the certification path information among the plurality of certificate information is in a leading portion of the order is set as certificate information used to perform the encrypted communication and records in the recording means information indicating that a setting for using fifth certificate information different from the fourth certificate

information, among the plurality of certificate information, for performing the encrypted communication has not been made.

[Claim 10]

The information processing apparatus according to claim 9, wherein

if the first processing means executes the third command, the transmitting means does not transmit certificate information which is not associated with the key pair information among the plurality of certificate information.

[Claim 11]

The information processing apparatus according to claim 3, wherein

the control means records keystore information and alias information which are based on the advanced security service in the recording means and records information indicating that a setting has been performed on the information processing apparatus in response to a command based on the device management service in the recording means as the alias information.

[Claim 12]

The information processing apparatus according to claim 11, wherein

the first processing means executes at least one of a

LoadCertificates command, a LoadCACertificates command, a LoadCertificateWithPrivateKey command, and the LoadCertificateWithPrivateKey command which are commands based on the device management service and which are commands used to load the first certificate information in the information processing apparatus, and

if the first processing means executes at least one of the LoadCertificates command, the LoadCACertificates command, the LoadCertificateWithPrivateKey command, and the LoadCertificateWithPrivateKey command on the basis of the device management service, the control means records information indicating that loading of a certificate has been performed using the device management service in the recording means as the alias information.

[Claim 13]

The information processing apparatus according to claim 11, wherein

the control means records the key pair information and the second certificate information which are associated with each other in the recording means,

the first processing means executes a GetCertificates command which is a command based on the device management service and which is a command for requesting the information processing apparatus to transmit certificate information and a GetCACertificates which is a command

provided by the device management service and which is a command for requesting the information processing apparatus to transmit certificate information issued by a certification authority, and

the transmitting means transmits the second certificate information associated with the key pair information if the first processing means executes the GetCertificates command and transmits third certificate information which is not associated with the key pair information if the first processing means executes the GetCACertificates command.

[Claim 14]

The information processing apparatus according to claim 11, wherein

the first processing means executes a DeleteCertificates command which is a command based on the device management service and which is a command for requesting deletion of certificate information recorded in the recording means so as to delete the key pair information corresponding to the certificate information specified by the DeleteCertificates command or the certification path information corresponding to the certificate information specified by the DeleteCertificates command from the recording means.

[Claim 15]

The information processing apparatus according to claim

2, further comprising:

imaging means,

wherein the transmitting means transmits an image captured by the imaging means through the encrypted communication in accordance with the information recorded in the recording means.

[Claim 16]

A method for controlling an information processing apparatus, the method comprising:

a first processing step of performing a setting for performing encrypted communication on the information processing apparatus in response to a command based on the device management service;

a second processing step of performing a setting for performing encrypted communication on the information processing apparatus in response to in command based on the advanced security service; and

a transmitting step of transmitting information indicating that the setting for performing the encrypted communication is made in response to the command based on the device management service to an external apparatus if the command based on the advanced security service is received from the external apparatus after the setting for performing the encrypted communication is performed on the information processing apparatus in response to the command

based on the device management service in the first processing step.

[Claim 17]

The control method according to claim 16, further comprising:

a control step of performing control such that information including that the setting has been performed on the information processing apparatus in response to the command based on the device management service is recorded in recording means.

[Claim 18]

The control method according to claim 17, wherein in the first processing step, a command for setting to the information processing apparatus at least one of first public key information which is used to perform the encrypted communication, first private key information which corresponds to the first public key information and which is used to perform the encrypted communication, and first certificate information which proves that the public key information is valid key information is executed, the command being executed by a first external apparatus on the information processing apparatus on the basis of the device management service, and

in the second processing step, a command for setting to the information processing apparatus at least one of key

pair information indicating that second public key information used to perform the encrypted communication corresponds to second private key information used to perform the encrypted communication, second certificate information which proves that the second public key information is valid key information, and certification path information indicating third certificate information associated with the second certificate information is executed, the command being executed by a second external apparatus on the information processing apparatus on the basis of the advanced security service.

[Claim 19]

A program that cause a computer to execute:

a first processing process of performing a setting for performing encrypted communication on the computer in response to a command based on the device management service;

a second processing process of performing a setting for performing encrypted communication on the computer in response to in command based on the advanced security service; and

a transmitting process of transmitting information indicating that the setting for performing the encrypted communication is made in response to the command based on the device management service to an external apparatus if

the command based on the advanced security service is received from the external apparatus after the setting for performing the encrypted communication is performed on the computer in response to the command based on the device management service in the first processing process.