(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 413 224 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.12.2018 Bulletin 2018/50

(51) Int Cl.:
G06F 21/33 *(2013.01)* ***H04L 9/32*** *(2006.01)*
H04L 29/06 *(2006.01)*

(21) Application number: **18174721.3**

(22) Date of filing: **29.05.2018**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **08.06.2017 JP 2017113631**

(71) Applicant: **CANON KABUSHIKI KAISHA**
Ohta-ku
Tokyo 146-8501 (JP)

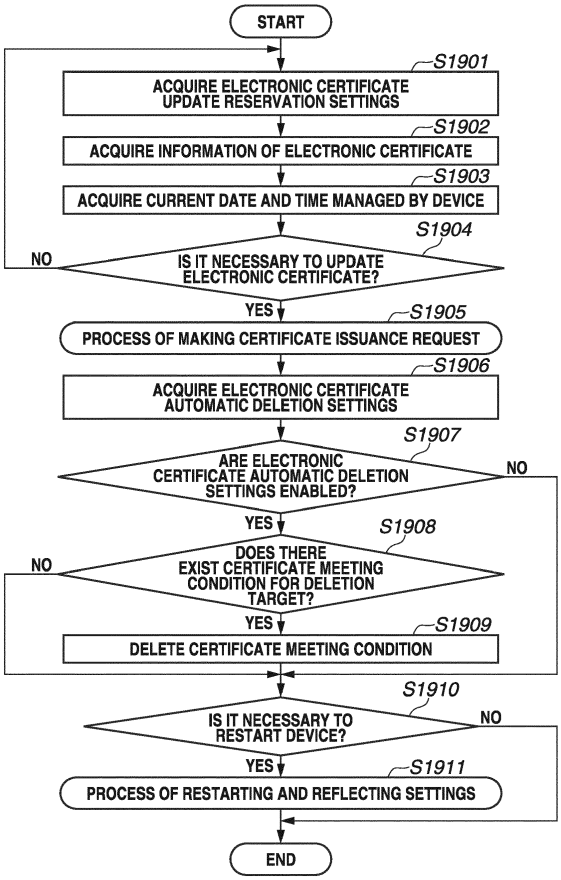
(72) Inventor: **KAKUTANI, Naoya**
Tokyo, 146-8501 (JP)

(74) Representative: **TBK**
Bavariaring 4-6
80336 München (DE)

(54) INFORMATION PROCESSING APPARATUS, CONTROL METHOD FOR CONTROLLING INFORMATION PROCESSING APPARATUS, AND PROGRAM

(57) An information processing apparatus automatically deletes an electronic certificate according to acquisition of an electronic certificate.

FIG.19



EP 3 413 224 A1

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to a technique for automatically deleting an electronic certificate.

Description of the Related Art

[0002] Conventionally, public key infrastructure (PKI) technology using an electronic certificate realizes identification and certification of a secure network (RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (https://www.ipa.go.jp/security/rfc/RFC3647JA.html)) .

[0003] For example, an information processing apparatus as a client can verify the validity of a server by acquiring a server's public key certificate from the server and a certificate authority certificate from a certificate authority having issued the server's public key certificate. Further, by providing the server with a client's public key certificate of the information processing apparatus, the server can also verify the validity of the client.

[0004] An electronic certificate has an expiration date. If the electronic certificate expires, communication using the electronic certificate becomes impossible. Thus, in a case where the electronic certificate expires, or immediately before the electronic certificate expires, it is necessary to update the electronic certificate.

[0005] Conventionally, a technique for automatically updating an electronic certificate at a predetermined timing before the electronic certificate expires is known (Japanese Patent Application Laid-Open No. 2016-178458). When a predetermined timing set in advance arrives, an information processing apparatus transmits an update request to a certificate management server via a network and receives an electronic certificate from the certificate management server.

[0006] In a case where the number of electronic certificates that can be stored in the information processing apparatus is limited, if an electronic certificate is acquired every time an electronic certificate is updated, the number of electronic certificates that can be stored reaches an upper limit, and an electronic certificate cannot be added.

[0007] Meanwhile, it is troublesome for a user to manually delete an electronic certificate that has become unnecessary due to expiration or the like.

SUMMARY OF THE INVENTION

[0008] An information processing apparatus described in the following exemplary embodiments has the following configuration.

[0009] According to a first aspect of the present invention, there is provided an information processing apparatus as specified in claims 1 to 9. According to a second aspect of the present invention, there is provided a control method as specified in claim 10. According to a third aspect of the present invention, there is provided a program as specified in claim 11.

[0010] Further features of the present invention will become apparent from the following description of exemplary embodiments with reference to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011]

Fig. 1 is a diagram illustrating a network configuration according to a first exemplary embodiment of the present invention.

Fig. 2 is a block diagram illustrating a hardware configuration of a multifunction peripheral according to the first exemplary embodiment.

Fig. 3 is a block diagram illustrating software modules included in the multifunction peripheral according to the first exemplary embodiment.

Fig. 4 is a sequence diagram illustrating a flow of entire processing performed by a system according to the first exemplary embodiment, including initialization regarding an electronic certificate issuance request, display of information of an electronic certificate, making of an issuance request to issue the electronic certificate, reception of the electronic certificate, a restart of the multifunction peripheral, and reflection of the received electronic certificate.

Fig. 5A is a flowchart illustrating a process of acquiring a list of key pairs and electronic certificates and generating display data in step S402 in Fig. 4, which is performed by the multifunction peripheral according to the first exemplary embodiment, and Fig. 5B is a flowchart illustrating a process performed when the multifunction peripheral according to the first exemplary embodiment receives a request to display detailed information from a personal computer (PC).

Fig. 6 is a flowchart illustrating a process of making connection settings for connection to a certificate/registration authority in step S407 in Fig. 4, which is performed by the multifunction peripheral according to the first exemplary embodiment.

Fig. 7 is a flowchart illustrating a process of acquiring and registering a CA certificate illustrated in steps S412 to S416 in Fig. 4, which is performed by the multifunction peripheral according to the first exemplary embodiment.

Fig. 8A and 8B are flowcharts illustrating a process of making a certificate issuance request and acquiring a certificate in steps S419 to S424 in Fig. 4, which is performed by the multifunction peripheral according to the first exemplary embodiment.

Fig. 9 is a flowchart illustrating a process regarding the restart of the multifunction peripheral in steps

S424 to S427 in Fig. 4, which is performed by the multifunction peripheral according to the first exemplary embodiment.

Fig. 10A is a diagram illustrating an example of a web page screen (a certificate list) as a remote user interface (RUI) displayed on the PC according to the first exemplary embodiment, and Fig. 10B is a diagram illustrating an example of a web page screen (connection settings) as an RUI displayed on the PC according to the first exemplary embodiment.

Fig. 11A is a diagram illustrating an example of a web page screen (the connection settings) as an RUI displayed on the PC according to the first exemplary embodiment, and Fig. 11B is a diagram illustrating an example of a web page screen (CA certificate acquisition) as an RUI displayed on the PC according to the first exemplary embodiment.

Fig. 12A is a diagram illustrating an example of a web page screen (success of the CA certificate acquisition) as an RUI displayed on the PC according to the first exemplary embodiment, and Fig. 12B is a diagram illustrating an example of a web page screen (failure of the CA certificate acquisition) as an RUI displayed on the PC according to the first exemplary embodiment.

Fig. 13A is a diagram illustrating an example of a web page screen (certificate issuance request settings) as an RUI displayed on the PC according to the first exemplary embodiment, and Fig. 13B is a diagram illustrating an example of a web page screen (success of a certificate issuance request) as an RUI displayed on the PC according to the first exemplary embodiment.

Fig. 14A is a diagram illustrating an example of a web page screen (failure of the certificate issuance request) as an RUI displayed on the PC according to the first exemplary embodiment, and Fig. 14B is a diagram illustrating an example of a web page screen (a restart) as an RUI displayed on the PC according to the first exemplary embodiment.

Fig. 15 is a diagram illustrating an example of a web page screen as an RUI displayed on the PC according to the first exemplary embodiment.

Fig. 16 is a diagram illustrating an example of detailed information of an electronic certificate displayed on the PC according to the first exemplary embodiment.

Figs. 17A, 17B, and 17C are conceptual diagrams illustrating a database of detailed information of key pairs and electronic certificates managed by a key pair/certificate management unit of the multifunction peripheral according to the first exemplary embodiment.

Fig. 18 is a diagram illustrating an example of an update reservation setting screen for electronic certificates included in the multifunction peripheral according to the first exemplary embodiment.

Fig. 19 is a flowchart illustrating a process of executing an electronic certificate automatic update function and an electronic certificate automatic deletion function based on electronic certificate update reservation settings, which is performed by the multifunction peripheral according to the first exemplary embodiment.

DESCRIPTION OF THE EMBODIMENTS

[0012] With reference to the attached drawings, exemplary embodiments of the present invention will be described in detail below. The following exemplary embodiments do not limit the present invention according to the appended claims, and not all the combinations of the features described in the exemplary embodiments are essential for solving the problems addressed by the present invention. An information processing apparatus for using and managing an electronic certificate according to an exemplary embodiment is described using a multifunction peripheral (a digital multifunction peripheral (MFP)) as an example. The scope of application of the information processing apparatus, however, is not limited to a multifunction peripheral, and the information processing apparatus may be any information processing apparatus that uses an electronic certificate.

[0013] Fig. 1 is a diagram illustrating a network configuration according to a first exemplary embodiment of the present invention.

[0014] A multifunction peripheral 100, which has a printing function, can transmit and receive print data, scanned image data, and management information of a device to and from another information processing apparatus via a network 110. Further, the multifunction peripheral 100 has the function of performing encrypted communication using Transport Layer Security (TLS), Internet Protocol Security (IPsec), and Institute of Electrical and Electronics Engineers (IEEE) 802.1X and holds public key pairs and electronic certificates for use in cryptographic processes using these protocols. A public key pair means a key pair including a public key and a private key and used to encrypt communication data by a public key cryptographic method.

[0015] The multifunction peripheral 100 is an example of an image forming apparatus. The image forming apparatus is not limited to this, and may be an apparatus having a single function of a facsimile apparatus, a printer, or a copying machine, or having multiple functions of these apparatuses. The network 110 is also connected to a multifunction peripheral 101, which has a function equivalent to that of the multifunction peripheral 100. Although the multifunction peripheral 100 is mainly described below, an electronic certificate can also be exchanged between a plurality of multifunction peripherals.

[0016] A certificate/registration authority 102 has the function of a certificate authority (CA) for issuing an electronic certificate, and the function of a registration authority (RA) for performing the process of receiving an electronic certificate issuance request and registering an

electronic certificate. That is, the certificate/registration authority 102 is a server apparatus having the function of distributing a CA certificate via the network 110, and issuing and registering an electronic certificate via the network 110. In the first exemplary embodiment, as a communication protocol on the network 110 at this time, Simple Certificate Enrollment Protocol (SCEP) is used. The communication protocol, however, need only to be able to request the certificate authority to issue an electronic certificate and acquire the electronic certificate from the certificate authority, and thus is not limited to SCEP. For example, the Certificate Management Protocol (CMP) or the Enrollment over Secure Transport (EST) protocol may also be used.

[0017] Using SCEP, the information processing apparatus such as the multifunction peripheral 100 communicates with the certificate/registration authority 102 via the network 110 to make an electronic certificate issuance request and acquire an electronic certificate. The multifunction peripheral 100 according to the first exemplary embodiment has a web server function and publishes on the network 110 a web page type remote user interface (RUI) function capable of executing the process of making an electronic certificate issuance request and acquiring an electronic certificate. The RUI function is the function of allowing an information terminal such as a personal computer (PC) to access a web server included in the multifunction peripheral 100 and displaying, on a display unit of the information terminal, a web page for operating the multifunction peripheral 100.

[0018] When the certificate/registration authority 102 receives an electronic certificate issuance request via the network 110, the certificate/registration authority 102 performs the process of, based on the issuance request, issuing an electronic certificate and registering the electronic certificate and transmits the issued electronic certificate as a response to the issuance request. In the first exemplary embodiment, the functions of the certificate authority and the registration authority are achieved by the same server apparatus. Alternatively, the configuration may be such that the certificate authority and the registration authority are achieved by different server apparatuses. The present invention is not particularly limited.

[0019] A PC 103 is a personal computer. The PC 103 has a web browser function and allows the browsing and the use of a HyperText Markup Language (HTML) document and a website published by an information processing apparatus connected to the network 110.

[0020] Next, a description is given of an overview of the process of acquiring and updating an electronic certificate according to the first exemplary embodiment.

[0021] Using the web browser provided in the PC 103, the administrator of the multifunction peripheral 100 connects to a web page to make an electronic certificate issuance request to issue an electronic certificate published by the multifunction peripheral 100, and acquire the electronic certificate. Then, the administrator makes settings and gives instructions for the execution of the process of making an electronic certificate issuance request and acquiring an electronic certificate. According to the contents of the settings made and the instructions given by the administrator, then using SCEP, the multifunction peripheral 100 acquires a CA certificate from the certificate/registration authority 102 and makes an electronic certificate issuance request to the certificate/registration authority 102. Further, the multifunction peripheral 100 acquires an electronic certificate included in a response to the electronic certificate issuance request and issued by the certificate/registration authority 102, and sets the use of the acquired electronic certificate in the multifunction peripheral 100.

[0022] Next, the hardware configuration of the multifunction peripheral 100 according to the first exemplary embodiment is described.

[0023] Fig. 2 is a block diagram illustrating the hardware configuration of the multifunction peripheral 100 according to the first exemplary embodiment.

[0024] A central processing unit (CPU) 201 executes a software program for the multifunction peripheral 100 and controls the entire apparatus. A read-only memory (ROM) 202 stores a boot program and a fixed parameter for the multifunction peripheral 100. A random-access memory (RAM) 203 is used to store a program and temporary data when the CPU 201 controls the multifunction peripheral 100. A hard disk drive (HDD) 204 stores system software, an application, and various types of data. The CPU 201 executes the boot program stored in the ROM 202, loads a program stored in the HDD 204 into the RAM 203, and executes the loaded program, thereby controlling the operation of the multifunction peripheral 100. A network interface (I/F) control unit 205 controls the transmission and reception of data to and from the network 110. A scanner I/F control unit 206 controls the reading of a document by a scanner 211. A printer I/F control unit 207 controls a printing process performed by a printer 210. A panel control unit 208 controls a touch panel type operation panel 212, thereby controlling the display of various pieces of information and an instruction input by a user. A bus 209 connects the CPU 201, the ROM 202, the RAM 203, the HDD 204, the network I/F control unit 205, the scanner I/F control unit 206, the printer I/F control unit 207, and the panel control unit 208 to each other. A control signal from the CPU 201 and a data signal between devices are transmitted and received via the bus 209.

[0025] Fig. 3 is a block diagram illustrating software modules of the multifunction peripheral 100 according to the first exemplary embodiment. The software modules illustrated in Fig. 3 are achieved by the CPU 201 executing a program loaded into the RAM 203.

[0026] A network driver 301 controls the network I/F control unit 205 connected to the network 110 to transmit and receive data to and from outside the multifunction peripheral 100 via the network 110. A network control unit 302 controls communication on the transport layer

or below in a network communication protocol such as the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit and receive data. A communication control unit 303 is a module for controlling a plurality of communication protocols supported by the multifunction peripheral 100. In the process of acquiring and updating an electronic certificate according to the first exemplary embodiment, the communication control unit 303 makes a request for Hypertext Transfer Protocol (HTTP) protocol communication, performs the process of generating response data and analyzing the response data, and controls the transmission and reception of data, thereby communicating with the certificate/registration authority 102 or the PC 103. Further, the communication control unit 303 also executes encrypted communication using TLS, IPSEC, and IEEE 802.1X supported by the multifunction peripheral 100.

[0027] A web page control unit 304 is a module for generating HTML data for displaying a web page on which the process of making an electronic certificate issuance request and acquiring an electronic certificate can be executed, and for controlling communication of the HTML data. The web page control unit 304 executes processes in response to a web page display request, an electronic certificate issuance request, and an electronic certificate acquisition execution instruction that are sent from the network driver 301 via the communication control unit 303. The web page control unit 304 transmits, as a response to a request from the web browser, HTML data of a predetermined web page saved in the RAM 203 or the HDD 204, or HTML data generated according to the content of a display request.

[0028] An acquisition control unit 305 is a module for executing the process of acquiring an electronic certificate based on an instruction from the web page control unit 304. The acquisition control unit 305 is a module for controlling communication using SCEP, for performing the process of generating encrypted data necessary for communication using SCEP such as PKCS #7 or PKCS #10 and analyzing the encrypted data, and for performing the process of saving an acquired electronic certificate and setting the purpose of the acquired electronic certificate.

[0029] An encryption processing unit 306 is a module for executing various cryptographic processes such as the process of encrypting and decrypting data, the process of generating and verifying an electronic signature, and the process of generating a hash value. In the process of acquiring and updating an electronic certificate according to the first exemplary embodiment, the encryption processing unit 306 executes various cryptographic processes necessary in the process of generating request data and response data using SCEP and analyzing the request data and the response data.

[0030] A key pair/certificate management unit 307 is a module for managing a public key pair and an electronic certificate held in the multifunction peripheral 100. The key pair/certificate management unit 307 saves data of a public key pair and an electronic certificate together with various setting values in the RAM 203 or the HDD 204. Further, although not illustrated in the figures in the first exemplary embodiment, the process of displaying the details of a public key pair and an electronic certificate, the process of generating a public key pair and an electronic certificate, and the process of deleting a public key pair and an electronic certificate can also be executed by an instruction from the user through the operation panel 212.

[0031] A user interface (UI) control unit 308 controls the operation panel 212 and the panel control unit 208. Also in an encrypted communication process using TLS, IPSEC, or IEEE 802.1X executed by the communication control unit 303, the encryption processing unit 306 performs an encryption process. The configuration is such that in the encryption process, the encryption processing unit 306 acquires data of a public key pair and an electronic certificate to be used from the key pair/certificate management unit 307.

[0032] A printing/reading processing unit 309 is a module for executing the function of printing by the printer 210 and the function of reading a document by the scanner 211. A device control unit 310 is a module for generating a control command and control data for the multifunction peripheral 100 and performing overall control of the multifunction peripheral 100. The device control unit 310 according to the first exemplary embodiment controls power supply to the multifunction peripheral 100, and according to an instruction from the web page control unit 304, executes the process of restarting the multifunction peripheral 100.

[0033] Fig. 4 is a sequence diagram illustrating the flow of entire processing performed by a system according to the first exemplary embodiment, including initialization regarding an electronic certificate issuance request, the display of information of an electronic certificate, the making of an issuance request to issue the electronic certificate, the reception of the electronic certificate, the restart of the multifunction peripheral 100, and the reflection of the received electronic certificate.

[0034] This sequence is started in response to the fact that the user inputs to the PC 103 a display instruction to display an electronic certificate list. According to the display instruction, the PC 103 may display key pairs together with the certificate list. A description is given below of an example where the PC 103 displays a list of key pairs and electronic certificates according to the display instruction.

[0035] In the first exemplary embodiment, the description is given using an example of processing on a single multifunction peripheral 100. Alternatively, processing may be executed on a plurality of multifunction peripherals 100 and 101 in response to a single start instruction. For example, the PC 103 may make requests to the multifunction peripherals 100 and 101, and each multifunction peripheral may execute processing illustrated in flowcharts described below. A step in which the PC 103 ac-

quires a certificate list from each of the multifunction peripherals 100 and 101, displays the certificate list, and prompts the user to confirm the certificate list may be skipped. Then, each multifunction peripheral may automatically detect an expired certificate and transmit bibliographic information (the certificate identification (ID) and the period of validity) of the expired certificate to the PC 103. Then, the PC 103 may cause the plurality of multifunction peripherals to automatically update a certificate which is about to expire or an expired certificate. This processing is termed "silent installation".

[0036] First, in step S401, the multifunction peripheral 100 receives a display request transmitted from the PC 103. The display request is a display request to display a list of electronic certificates held in the multifunction peripheral 100. In the first exemplary embodiment, using the web browser provided in the PC 103, the administrator of the multifunction peripheral 100 connects to a web page published by the multifunction peripheral 100 for making an electronic certificate issuance request and acquiring an electronic certificate, and performs operations such as giving instructions. In the present exemplary embodiment, an operation screen on the web page thus displayed on a display unit of the PC 103 is occasionally referred to as an "RUI". The RUI is a user interface displayed on the PC 103 by remotely requesting operation screen data of the multifunction peripheral 100 or 101 using the web browser of the PC 103. At this time, the screen can be implemented by HTML or a servlet.

[0037] Next, in step S402, the multifunction peripheral 100 executes the process of acquiring data for displaying a list of key pairs and electronic certificates held in the multifunction peripheral 100, and of generating a web page screen for displaying the list.

[0038] Fig. 5A is a flowchart illustrating the process of acquiring a list of key pairs and electronic certificates and generating display data in step S402 in Fig. 4. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0039] Further, Figs. 17A to 17C are conceptual diagrams illustrating a database of detailed information of key pairs and electronic certificates managed by the key pair/certificate management unit 307 of the multifunction peripheral 100. This database is saved in the HDD 204 of the multifunction peripheral 100.

[0040] The flowchart in Fig. 5A is described. This processing is started by receiving a key pair/electronic certificate list acquisition request. First, in step S501, the CPU 201 receives a key pair/electronic certificate list acquisition request. Next, in step S502, the CPU 201 acquires detailed information of key pairs and electronic certificates managed by the key pair/certificate management unit 307 as illustrated in Fig. 17A, for example. Next, in step S503, using the detailed information of the key pairs and the electronic certificates acquired in step S502, the CPU 201 generates HTML data of a web page screen to be provided as an RUI.

[0041] Figs. 10A to 15 are diagrams illustrating examples of a web page screen as an RUI displayed on the PC 103 according to the first exemplary embodiment. In step S503 in Fig. 5A according to the first exemplary embodiment, HTML data of a web page screen illustrated in Fig. 10A is generated, and the web page screen is displayed on the web browser of the PC 103. Consequently, it is possible to confirm on the PC 103 a list of key pairs and electronic certificates held in the multifunction peripheral 100.

[0042] Information of the electronic certificates displayed in the list in Fig. 10A includes a name 1011, a purpose 1012, an issuer 1013, an end date of a period of validity 1014, and details 1015 of each certificate. The name 1011 is a character string optionally assigned by an operator such as the administrator of the multifunction peripheral 100 when the key pair and the electronic certificate are issued. The purpose 1012 is a setting value indicating that the key pair and the electronic certificate are used for any of purposes such as TLS, IPSEC, and IEEE 802.1X. The issuer 1013 is a distinguished name (DN) of a certificate authority that has issued the electronic certificate. The end date of the period of validity 1014 is information about the day when the period of validity of the electronic certificate ends. The details 1015 is an icon for displaying the detailed information of the electronic certificate. Then, in step S504, the CPU 201 transmits to the PC 103 the HTML data generated in step S503 as a response to step S501, and this processing ends. Step S402 in Fig. 4 is thus executed.

[0043] Although not illustrated in the sequence diagram in Fig. 4, if the administrator of the multifunction peripheral 100 clicks an icon of the details 1015 in Fig. 10A displayed on the PC 103, the PC 103 transmits to the multifunction peripheral 100 a display request to display detailed information of an electronic certificate corresponding to the icon. Receiving the display request, the multifunction peripheral 100 acquires the detailed information of the electronic certificate, generates HTML data of the detailed information of the certificate based on the acquired information, and transmits to the PC 103 the generated data as a response.

[0044] Consequently, for example, detailed information of an electronic certificate as illustrated in Fig. 16 is displayed on the web browser of the PC 103. Fig. 16 is a diagram illustrating an example of the detailed information of the electronic certificate displayed on the PC 103.

[0045] Fig. 5B is a flowchart illustrating a process performed when the multifunction peripheral 100 according to the first exemplary embodiment receives from the PC 103 this request to display detailed information. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0046] First, in step S511, the CPU 201 receives an electronic certificate detailed information acquisition request from the PC 103. Next, in step S512, the CPU 201 acquires detailed information of a key pair and an electronic certificate managed by the key pair/certificate man-

agement unit 307 and illustrated in Fig. 17A. Next, in step S513, using the detailed information of the key pair and the electronic certificate acquired in step S512, the CPU 201 generates HTML data of a web page screen. In step S514, the CPU 201 transmits the generated HTML data to the PC 103.

[0047] Fig. 16 is a diagram illustrating an example of a display screen of the detailed information of the electronic certificate according to the first exemplary embodiment. This screen is displayed as an RUI in a web page format on the PC 103.

[0048] Referring back to Fig. 4, in step S403, the multifunction peripheral 100 transmits to the PC 103 the HTML data of the web page screen generated in step S402 and illustrated in Fig. 10A as a response.

[0049] The processes illustrated in steps S401 to S403 in Fig. 4, steps S501 to S504 in Fig. 5A, and steps S511 to S514 in Fig. 5B are a control process regarding the process of displaying electronic certificate information, which is performed by the multifunction peripheral 100 having received a key pair/electronic certificate list display request.

[0050] Then, in step S404, the multifunction peripheral 100 receives from the PC 103 a display request to display an SCEP server connection setting screen. In the first exemplary embodiment, to make connection settings for connection to the certificate/registration authority 102, the administrator of the multifunction peripheral 100 clicks "connection settings" 1002 in Fig. 10A, thereby transmitting to the multifunction peripheral 100 the display request to display a connection setting screen.

[0051] Next, in step S405, the multifunction peripheral 100 transmits, to the PC 103, HTML data of a predetermined SCEP server connection setting screen illustrated in Fig. 10B as a response to step S404.

[0052] The connection setting screen illustrated in Fig. 10B includes input fields, namely "server name" 1016 and "port number" 1017, to which a host name and a connection destination port number, respectively, of an SCEP server are input, and a "setting" button 1018 for giving an instruction to set input setting values.

[0053] Next, in step S406, the multifunction peripheral 100 receives from the PC 103 a setting instruction request to make connection settings. The administrator of the multifunction peripheral 100 according to the first exemplary embodiment provides inputs to the "server name" 1016 and the "port number" 1017 in Fig. 10B through the PC 103 and clicks the "setting" button 1018, thereby transmitting this setting instruction request to the multifunction peripheral 100.

[0054] Next, in step S407, the multifunction peripheral 100 executes the process of making connection settings and generating a web page screen indicating the setting results. In step S408, the multifunction peripheral 100 transmits, to the PC 103, HTML data of the web page screen generated in step S407 and illustrated in Fig. 11A as a response.

[0055] Fig. 6 is a flowchart illustrating the process of making connection settings for connection to the certificate/registration authority 102 in step S407 in Fig. 4, which is performed by the multifunction peripheral 100 according to the first exemplary embodiment. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0056] First, in step S601, the CPU 201 receives from the PC 103 a setting request to make connection settings. Next, in step S602, the CPU 201 acquires the setting values of a host name and a port number included in the setting request to make the connection settings, and saves the acquired setting values in the RAM 203 or the HDD 204. Next, in step S603, the CPU 201 generates HTML data of a web page screen in Fig. 11A, for example. Then, in step S604, the CPU 201 transmits the HTML data generated in step S603 as a response to step S601, and this processing ends. Thus, the processing proceeds to step S408.

[0057] Consequently, as illustrated in Fig. 11A, the PC 103 displays a character string 1101 indicating that the settings are reflected.

[0058] The processes illustrated in steps S406 to S408 and S601 to 604 are control regarding the process of making connection settings, which is performed by the multifunction peripheral 100.

[0059] Next, in step S409 in Fig. 4, the multifunction peripheral 100 receives a display request to display a CA certificate acquisition screen transmitted from the browser of the PC 103. In the first exemplary embodiment, the administrator of the multifunction peripheral 100 acquires a CA certificate issued by the certificate/registration authority 102. Thus, the administrator clicks "CA certificate acquisition" 1003 in Fig. 10A, thereby transmitting to the multifunction peripheral 100 the display request to display a CA certificate acquisition screen.

[0060] Consequently, in step S410, the multifunction peripheral 100 transmits HTML data of a predetermined CA certificate acquisition screen illustrated in Fig. 11B as a response to step S409.

[0061] The CA certificate acquisition screen in Fig. 11B includes an "execution" button 1102 for giving an instruction to acquire a CA certificate.

[0062] Next, in step S411, the "execution" button 1102 in Fig. 11B is clicked, and the multifunction peripheral 100 receives a CA certificate acquisition request transmitted from the browser of the PC 103. In the first exemplary embodiment, the administrator of the multifunction peripheral 100 clicks the "execution" button 1102 in Fig. 11B, thereby transmitting to the multifunction peripheral 100 the CA certificate acquisition request.

[0063] Next, in step S412, the multifunction peripheral 100 executes the process of generating CA certificate acquisition request data. Then, in step S413, based on the information set in step S407, the multifunction peripheral 100 transmits the CA certificate acquisition request data generated in step S412 to the certificate/registration authority 102 as the SCEP server. Then, in step S414, the multifunction peripheral 100 receives a re-

sponse to the CA certificate acquisition request transmitted from the certificate/registration authority 102. Consequently, in step S415, the multifunction peripheral 100 performs the process of analyzing the received response to the CA certificate acquisition request, acquiring a CA certificate included in the response, and registering the acquired CA certificate as a CA certificate trusted by the multifunction peripheral 100. Then, in step S416, the multifunction peripheral 100 transmits, to the PC 103, HTML data of a web page screen generated in step S415 as illustrated in Fig. 12A or Fig. 12B. Fig. 12A illustrates an example of a screen displayed when the acquisition of the CA certificate is successful, and the acquired CA certificate is registered as a CA certificate. On the other hand, Fig. 12B illustrates an example of a screen displayed when the acquisition of the CA certificate is failed.

[0064] Fig. 7 is a flowchart illustrating the process of acquiring and registering a CA certificate illustrated in steps S412 to S416 in Fig. 4, which is performed by the multifunction peripheral 100 according to the first exemplary embodiment. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0065] First, in step S701, the CPU 201 receives a CA certificate acquisition request from the PC 103. Next, in step S702, based on the information of the connection settings for connection to the certificate/registration authority 102 acquired in step S407, the CPU 201 generates a message of the CA certificate acquisition request. The following is an example of the message of the acquisition request generated in the first exemplary embodiment. In the first exemplary embodiment, SCEP is used as a communication protocol, and the message is a request message for using this protocol. xxxxxxx/yyyyy?operation=GetCAXyz&message=CAIdentifier

[0066] Next, in step S703, based on the connection settings for connection to the certificate/registration authority 102 acquired in step S407 in Fig. 4, the CPU 201 connects to the certificate/registration authority 102 as the SCEP server using the TCP/IP protocol. Next, in step S704, the CPU 201 determines whether the connection in step S703 is successful. If the connection is successful (YES in step S704), the processing proceeds to step S705. If the connection is failed (NO in step S704), the processing proceeds to step S714.

[0067] In step S705, using a GET or POST method of the HTTP protocol, the CPU 201 transmits the message of the CA certificate acquisition request generated in step S702 to the certificate/registration authority 102. Next, in step S706, the CPU 201 determines whether the transmission in step S705 is successful. If the transmission is successful (YES in step S706), the processing proceeds to step S707. If the transmission is failed (NO in step S706), the processing proceeds to step S714. In step S707, the CPU 201 receives, from the certificate/registration authority 102, response data in response to the CA certificate acquisition request. Then, in step S708, the CPU 201 determines whether the reception of the response data in step S707 is successful. If the reception is successful (YES in step S708), the processing proceeds to step S709. If the reception is failed (NO in step S708), the processing proceeds to step S714. In step S709, the CPU 201 analyzes the response data received in step S708 and acquires data of a CA certificate included in the response data. The encryption processing unit 306 performs the process of analyzing the response data and acquiring the CA certificate.

[0068] The response data according to the first exemplary embodiment is binary data in X.509 (RFC 5280) format. Alternatively, for example, data in PKCS #7 (RFC 5652: Cryptographic Message Syntax) format may be transmitted as the response, and the data format is not limited.

[0069] Next, in step S710, the CPU 201 determines whether the acquisition of the CA certificate in step S709 is successful. If the acquisition is successful (YES in step S710), the processing proceeds to step S711. If the acquisition is failed (NO in step S710), the processing proceeds to step S714. In step S711, the CPU 201 registers the CA certificate acquired in step S709 as a CA certificate trusted by the multifunction peripheral 100. At this time, the CPU 201 holds the acquired CA certificate in the RAM 203 and also causes the key pair/certificate management unit 307 to save the acquired CA certificate in a predetermined directory of the HDD 204 for storing a CA certificate trusted by the multifunction peripheral 100. Then, in step S712, the CPU 201 determines whether the process of registering the CA certificate in step S710 is successful. If it is determined that the registration process is successful (YES in step S712), the processing proceeds to step S713. If the registration process is failed (NO in step S712), the processing proceeds to step S714. In step S713, the CPU 201 generates a thumbprint (a hash value generated using Secure Hash Algorithm 1 (SHA-1)) of the CA certificate to be displayed in a character string 1201 in Fig. 12A when the acquisition of the CA certificate is successful. This thumbprint is generated by the encryption processing unit 306. Then, in step S715, according to the processing results in steps S703 to S714, the CPU 201 generates HTML data of display data indicating the acquisition result of the CA certificate in Fig. 12A. Then, in step S716, the CPU 201 transmits to the PC 103 the HTML data generated in step S715 as a response to step S701, and this processing ends. Then, the processing proceeds to step S417 in Fig. 4. In the first exemplary embodiment, according to the acquisition result of the CA certificate, the CPU 201 displays the character string 1201 in Fig. 12A. If an error process is executed in step S714, the CPU 201 displays a character string 1202 in Fig. 12B. Next, the description returns to Fig. 4.

[0070] In step S417, the multifunction peripheral 100 receives a display request to display a certificate issuance request screen transmitted from the browser of the PC 103. In the first exemplary embodiment, the administrator of the multifunction peripheral 100 clicks "certificate issuance request" 1004 in Fig. 10A, to make a cer-

tificate issuance request to the certificate/registration authority 102 and to acquire a certificate from the certificate/registration authority 102.

[0071] Next, in step S418, the multifunction peripheral 100 transmits, to the PC 103, HTML data of a predetermined certificate issuance request screen illustrated in Fig. 13A as a response to step S417. Consequently, the PC 103 performs display control to display the screen illustrated in Fig. 13A.

[0072] The certificate issuance request screen in Fig. 13A includes "name" 1301 of a certificate, "length of key" 1302 for setting the key length of a key pair to be generated, and an "input of issuance destination information" field 1303. Further, the certificate issuance request screen in Fig. 13A includes "signature verification" 1304 for setting whether to verify a signature assigned to a response to a certificate issuance request to be transmitted from the certificate/registration authority 102, and "purpose of key" 1305 for setting the purpose of an issued certificate. Further, the certificate issuance request screen in Fig. 13A includes "password" 1306 to be included in the certificate issuance request, and an "execution" button 1307 for making the certificate issuance request. The "purpose of key" 1305 is check boxes and indicates that a plurality of purposes can be set for a single key.

[0073] Next, in step S419, the multifunction peripheral 100 receives a certificate issuance request including information of inputs and settings regarding the items 1301 to 1306 transmitted from the browser of the PC 103 by clicking of the "execution" button 1307 on the screen in Fig. 13A. In the first exemplary embodiment, the administrator of the multifunction peripheral 100 provides inputs and makes settings regarding the items 1301 to 1306 in Fig. 13A and clicks the "execution" button 1307, thereby transmitting the certificate issuance request from the PC 103.

[0074] Next, in step S420, the multifunction peripheral 100 executes the process of generating certificate issuance request data. Then, in step S421, based on the information set in step S407, the multifunction peripheral 100 transmits the certificate issuance request data generated in step S420 to the certificate/registration authority 102 as the SCEP server. Then, in step S422, the multifunction peripheral 100 receives a response to the certificate issuance request transmitted from the certificate/registration authority 102. Next, in step S423, the multifunction peripheral 100 performs the process of analyzing the response to the certificate issuance request received in step S422 (the execution of signature verification according to the setting, the acquisition of a certificate included in the response, and the setting of the acquired certificate to a specified purpose). Then, the multifunction peripheral 100 executes the process of generating a web page screen indicating the result of the certificate issuance request.

[0075] If the issuance and the acquisition of the certificate are successful, then in the process of step S423, the electronic certificate data is saved, and the purpose of the electronic certificate data is set. The setting of the purpose refers to a communication function using the electronic certificate. In the first exemplary embodiment, encrypted communication using TLS, IPSEC, or IEEE 802.1X can be set. Further, the multifunction peripheral 100 according to the first exemplary embodiment can have a plurality of electronic certificates, and the purpose is set for each electronic certificate. For example, in a case where an electronic certificate to be used when the multifunction peripheral 100 provides a server service for performing TLS communication as a web server, and an electronic certificate to be used by the multifunction peripheral 100 to perform client communication using IEEE 802.1X are different from each other, both electronic certificates can be set. Alternatively, a single electronic certificate may be automatically applied to all communication purposes.

[0076] Then, in step S424, the multifunction peripheral 100 transmits to the PC 103 HTML data of a web page screen generated in step S423 and illustrated in Fig. 13B or 14A. According to the result of the certificate issuance request, a character string indicating the setting result is displayed as illustrated in a character string 1308 in Fig. 13B or a character string 1401 in Fig. 14A. Fig. 13B illustrates an example of a screen in a case where the issuance and the acquisition of the certificate are successful. Fig. 14A illustrates an example of a screen in a case where the issuance and the acquisition of the certificate are failed.

[0077] If the issuance and the acquisition of the certificate are thus successful, then in the process of step S423, the electronic certificate data is saved, and the purpose of the electronic certificate data is set. When the multifunction peripheral 100 is started, the communication control unit 303 according to the first exemplary embodiment acquires data of an electronic certificate to be used in encrypted communication using TLS, IPSEC, or IEEE 802.1X. Thus, if the purpose is changed, it is necessary to restart the multifunction peripheral 100.

[0078] Fig. 8 is a flowchart illustrating the process of making a certificate issuance request and acquiring a certificate in steps S419 to S424 in Fig. 4, which is performed by the multifunction peripheral 100 according to the first exemplary embodiment. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0079] First, in step S801, the CPU 201 receives from the PC 103 a certificate issuance request.

[0080] Next, in step S802, the CPU 201 acquires information about the "name" 1301 of a certificate, the "length of key" 1302, the "input of issuance destination information" 1303, the "signature verification" 1304, and the "purpose of key" 1305 included in the certificate issuance request received in step S801.

[0081] Next, in step S803, the CPU 201 acquires the CA certificate acquired in steps S412 to S415 in Fig. 4.

[0082] Then, in step S804, the CPU 201 generates a

key pair/certificate signing request. In step S804, based on the information of the "name" 1301 and the "length of key" 1302 acquired in step S802, the CPU 201 performs the process of generating a key pair. Further, the encryption processing unit 306 generates certificate signing request data in PKCS #10 format based on the information of the "input of issuance destination information" 1303 and the "password" 1306. PKCS #10 is a format for a certificate signing request defined in RFC 2986: PKCS #10: Certification Request Syntax Specification. Further, a certificate signing request is occasionally referred to as a "CSR".

[0083] Next, in step S805, the CPU 201 determines whether the generation of the key pair/certificate signing request in step S804 is successful. If it is determined that the generation is successful (YES in step S805), the processing proceeds to step S806. If the generation is failed (NO in step S805), the processing proceeds to step S823.

[0084] In step S806, the CPU 201 generates certificate issuance request data. The issuance request data generated in step S806 is based on the connection settings for connection to the certificate/registration authority 102 acquired in step S407 in Fig. 4 and is data in PKCS #7 format defined by SCEP.

[0085] Next, in step S808, based on the connection settings for connection to the certificate/registration authority 102 acquired in step S407 in Fig. 4, the CPU 201 connects to the certificate/registration authority 102 as the SCEP server using the TCP/IP protocol. Next, in step S809, the CPU 201 determines whether the connection in step S808 is successful. If the connection is successful (YES in step S809), the processing proceeds to step S810. If the connection is failed (NO in step S809), the processing proceeds to step S823.

[0086] In step S810, using a GET or POST method of the HTTP protocol, the CPU 201 transmits the certificate issuance request data generated in step S806. Then, in step S811, the CPU 201 determines whether the transmission in step S810 is successful. If the transmission is successful (YES in step S811), the processing proceeds to step S812. If the transmission is failed (NO in step S811), the processing proceeds to step S823.

[0087] In step S812, the CPU 201 receives, from the certificate/registration authority 102, response data in response to the certificate issuance request. The response data transmitted as a response is data in PKCS #7 format defined by SCEP.

[0088] Next, in step S813, the CPU 201 determines whether the reception of the response data in step S812 is successful. If the reception is successful (YES in step S813), the processing proceeds to step S814. If the reception is failed (NO in step S813), the processing proceeds to step S823.

[0089] In step S814, based on the setting of the "signature verification" 1304 acquired in step S802, the CPU 201 determines whether a setting is made so that the signature is to be verified. If a setting is made so that the signature is to be verified (YES in step S814), the processing proceeds to step S815. If a setting is made so that the signature is not to be verified (NO in step S814), the processing proceeds to step S817.

[0090] In step S815, using the public key included in the CA certificate acquired in step S803, the CPU 201 verifies signature data assigned to the data received in step S812. Then, in step S816, the CPU 201 determines whether the verification of the signature in step S815 is successful. If the verification is successful (YES in step S816), the processing proceeds to step S817. If the verification is failed (NO in step S816), the processing proceeds to step S823.

[0091] In step S817, the CPU 201 analyzes the data received in step S812 and acquires data of a certificate included in the response data. At this time, the encryption processing unit 306 performs the process of analyzing the response data and acquiring the certificate.

[0092] Next, in step S818, the CPU 201 determines whether the acquisition of the certificate in step S817 is successful. If the acquisition is successful (YES in step S818), the processing proceeds to step S819. If the acquisition is failed (NO in step S818), the processing proceeds to step S823.

[0093] In step S819, the CPU 201 registers the certificate acquired in step S818 as an electronic certificate corresponding to the key pair generated in step S804. At this time, the CPU 201 causes the key pair/certificate management unit 307 to save the public key pair generated in step S804 and the acquired electronic certificate in a predetermined directory of the HDD 204 for storing a key pair and an electronic certificate. At this time, the key pair/certificate management unit 307 adds information about the public key pair generated in step S804 and the acquired electronic certificate to a list of detailed information of key pairs and certificates as illustrated in Fig. 17B. In Fig. 17B, a key pair and a certificate Xyz4 are newly added.

[0094] Next, in step S820, the CPU 201 determines whether the process of registering the certificate in step S819 is successful. If the registration process is successful (YES in step S820), the processing proceeds to step S821. If the registration process is failed (NO in step S820), the processing proceeds to step S823.

[0095] In step S821, based on the information of the "purpose of key" 1305 acquired in step S802, the CPU 201 sets the purpose of the certificate. At this time, the key pair/certificate management unit 307 updates information of the purpose in the list of detailed information of key pairs and certificates as illustrated in Fig. 17C, for example. In Fig. 17C, a key pair and a certificate to be used for TLS are changed from Xyz1 to Xyz4.

[0096] Next, in step S824, according to the processing results in steps S801 to S823, the CPU 201 generates HTML data of the result of the certificate issuance request illustrated in Fig. 13B. Then, in step S825, the CPU 201 transmits to the PC 103 the HTML data generated in step S824 as a response to the certificate issuance request

in step S801, and this processing ends. Then, the processing proceeds to step S425 in Fig. 4.

[0097] The processes of steps S419 to S424 and S801 to S825 are control regarding the process of making an electronic certificate issuance request and receiving an electronic certificate, and the setting of a communication purpose, which is performed by the multifunction peripheral 100. In the first exemplary embodiment, the process of making an electronic certificate issuance request and receiving an electronic certificate, and the setting of a communication purpose are collectively referred to as "an electronic certificate automatic update function".

[0098] With this electronic certificate automatic update function, the multifunction peripheral 100 can automatically perform the process of making an electronic certificate issuance request and receiving an electronic certificate via the network 110. Further, the multifunction peripheral 100 can also set the purpose of the received electronic certificate. Thus, it is possible to save the user the trouble of working. The description returns to Fig. 4.

[0099] In step S425, the multifunction peripheral 100 receives a request to restart the multifunction peripheral 100. In the first exemplary embodiment, the administrator of the multifunction peripheral 100 restarts the multifunction peripheral 100. Thus, the administrator clicks a "restart" button 1309 in Fig. 13B.

[0100] Next, in step S426, the multifunction peripheral 100 transmits HTML data of a predetermined restart execution screen illustrated in Fig. 14B as a response to step S425. Next, in step S427, the multifunction peripheral 100 executes the process of restarting the multifunction peripheral 100.

[0101] It is assumed that when the purpose of communication using IEEE 802.1X is set for a received electronic certificate, the multifunction peripheral 100 according to the first exemplary embodiment cannot reflect the set purpose unless being restarted. This is because an electronic certificate for, for example, IEEE 802.1X is loaded into the RAM 203 when the multifunction peripheral 100 is started, and the electronic certificate continues to be used. Thus, the electronic certificate may not be replaced with a received electronic certificate saved in the HDD 204. If, however, the multifunction peripheral 100 can switch an electronic certificate to be used in the purpose of communication without needing to restart the multifunction peripheral 100, it may not be necessary to restart the multifunction peripheral 100. For example, if an electronic certificate is set for the purpose of TLS, it may not be necessary to restart the multifunction peripheral 100. For example, the necessity of a restart may be set in advance for each of a plurality of purposes, and according to information regarding the necessity of a restart, the multifunction peripheral 100 may automatically determine whether the multifunction peripheral 100 is to be restarted.

[0102] Fig. 9 is a flowchart illustrating a process regarding the restart of the multifunction peripheral 100 in steps S424 to S427 in Fig. 4, which is performed by the multifunction peripheral 100 according to the first exemplary embodiment. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0103] First, in step S901, the CPU 201 receives from the PC 103 a restart request to restart the multifunction peripheral 100. Next, in step S902, the CPU 201 transmits, to the PC 103, HTML data of a predetermined screen for making a restart request to restart the multifunction peripheral 100 illustrated in Fig. 14B as a response to step S901. Next, in step S903, the CPU 201 instructs the device control unit 310 to start a restart process, and this processing ends.

[0104] By the above series of operations, after being restarted, the multifunction peripheral 100 uses the electronic certificate acquired from the certificate/registration authority 102.

[0105] Fig. 15 is a diagram illustrating an example of a screen in a case where the list of key pairs and electronic certificates is displayed again by the process of step S401 after the issuance and the acquisition of the electronic certificate are successful. In this case, information 1501 of the certificate (Xyz4) issued by the certificate/registration authority 102 is added.

[0106] Fig. 18 is a diagram illustrating an example of a setting screen (hereinafter referred to as "an update reservation setting screen") regarding the update of an electronic certificate held in the multifunction peripheral 100 according to the first exemplary embodiment. This setting screen is displayed as an RUI on a display screen of the PC 103, similarly to other screens. The update timing of an electronic certificate can be set through the update reservation setting screen. Further, on the update reservation setting screen, an electronic certificate that should be deleted among one or more electronic certificates stored in the HDD 204 can be set.

[0107] In the first exemplary embodiment, an example is described where, as a method for setting the update timing of an electronic certificate, a setting method can be selected from among settings 1801, 1802, and 1803. In the present exemplary embodiment, the settings 1801, 1802, and 1803 are collectively referred to as "certificate update reservation settings".

[0108] The setting 1801 is a setting for specifying the date and time when an electronic certificate is to be updated, thereby specifying the update timing of the electronic certificate. If the current date and time measured by a time measurement unit of the multifunction peripheral 100 reach set date and time, the multifunction peripheral 100 executes the electronic certificate automatic update function.

[0109] The setting 1802 is a setting for specifying the number of days until the expiration date of an electronic certificate that is being used, thereby specifying the update timing of the electronic certificate. If the current date and time measured by the time measurement unit of the multifunction peripheral 100 reach or pass the date and time before the expiration date by a specified number of days, the multifunction peripheral 100 executes the elec-

tronic certificate automatic update function.

[0110] The setting 1803 is a setting for setting the cycle in which the electronic certificate automatic update function is to be executed, thereby specifying the update timing of an electronic certificate. In the first exemplary embodiment, this cycle can be set to the number of days, a predetermined date every month, or a predetermined date every year. If a period corresponding to the set cycle elapses after the electronic certificate is updated, the electronic certificate automatic update function is executed. If the certificate update reservation settings are updated, the CPU 201 saves the updated certificate update reservation settings in the HDD 204.

[0111] Fig. 18 illustrates an example where the setting 1802 for, based on the expiration date described in an electronic certificate, determining the update timing of the electronic certificate is made. 14 days before the expiration date, the multifunction peripheral 100 executes the certificate automatic update function. Fig. 18 is merely an example, and a method for setting the timing of the automatic update may be another specifying method. The present invention is not particularly limited.

[0112] The multifunction peripheral 100 according to the present exemplary embodiment has deletion settings 1804 as settings for automatically deleting an unnecessary certificate after the update. In the example of Fig. 18, the user makes a deletion setting by selecting either of a radio button 18041 for specifying a certificate to be automatically deleted, and a radio button 18042 for specifying a certificate not to be automatically deleted. The user only needs to be able to specify whether an unnecessary certificate is to be automatically deleted, and the setting method is not particularly limited. The selection may be made using not only radio buttons but also a pull-down menu. Alternatively, the on/off state of a certificate automatic deletion function may be set.

[0113] In a case where the setting for executing automatic deletion is enabled, a check box 18043 and check boxes 1805 can be selected.

[0114] By selecting the check box 18043, it is possible to enable a setting for deleting an electronic certificate in a case where the number of stored electronic certificates reaches a predetermined upper limit. In a case where the check box 18043 is selected, and if an electronic certificate is to be acquired, and also if the number of electronic certificates stored in the HDD 204 is a predetermined number or more, an electronic certificate is automatically deleted.

[0115] If the remaining storage capacity of an area reserved as a storage area for storing electronic certificates reaches a predetermined value or less, an electronic certificate may be deleted.

[0116] Further, by selecting the check boxes for detailed settings 1805, it is possible to make detailed settings of automatic deletion. A setting method for making these settings is not limited to check boxes.

[0117] In a case where the check box 18043 is not selected, and if a condition specified by any of the automatic deletion detailed settings 1805 is satisfied, a certificate is deleted, regardless of the number of stored electronic certificates.

[0118] The automatic deletion detailed settings 1805 include settings 18051 to 18055. An electronic certificate set by the detailed settings 1805 as an electronic certificate that should be deleted is automatically deleted from the HDD 204 according to the acquisition of a new electronic certificate.

[0119] In a case where the setting 18051 is enabled, an electronic certificate before the update having the same purpose as the purpose of an electronic certificate to be newly acquired is set as an electronic certificate that should be automatically deleted. The purpose of an electronic certificate is set using the "purpose of key" 1305 in Fig. 13A. In this case, the purpose of the electronic certificate corresponds to, for example, the use of the electronic certificate for TLS communication, or the use of the electronic certificate for Secure Sockets Layer (SSL) communication. The purpose of the electronic certificate is managed in association with the electronic certificate.

[0120] In a case where the setting 18052 is enabled, and if the purpose of an electronic certificate among electronic certificates held in the multifunction peripheral 100 before the update is not set, it is determined that the electronic certificate is not used, and the electronic certificate is set as an electronic certificate that should be deleted.

[0121] In a case where the setting 18053 is enabled, a self-certificate held in the multifunction peripheral 100 before the update is set as an electronic certificate that should be deleted. The self-certificate is a certificate that is not signed by the certificate authority, and is electronically signed by the information processing apparatus itself that holds the certificate. The condition is set such that a certificate other than a self-certificate is not deleted, assuming a case where the multifunction peripheral 100 may hold a certificate purchased from outside the multifunction peripheral 100, and it is not possible to determine whether it is all right to automatically delete the certificate.

[0122] In a case where the setting 18054 is enabled, an electronic certificate held in the multifunction peripheral 100 before the update and set before the multifunction peripheral 100 is shipped from the factory is set as an electronic certificate that should be deleted. The condition is set such that an electronic certificate other than an electronic certificate set before the multifunction peripheral 100 is shipped from the factory is not deleted, assuming a case where it is not possible to determine whether it is all right to automatically delete an electronic certificate held later in the multifunction peripheral 100.

[0123] In a case where the setting 18055 is enabled, among electronic certificates held in the multifunction peripheral 100 before the update, an expired electronic certificate is set as an electronic certificate that should be deleted. This is because an expired electronic certificate cannot be used.

[0124] The CPU 201 saves these setting values in the HDD 204. The above settings are made by selecting check boxes. The present invention, however, is not limited to this. It is sufficient to be able to specify each setting item as enabled or disabled. For example, each setting item may be selected as enabled or disabled, using a pull-down menu or a radio button.

[0125] In the present exemplary embodiment, certificate automatic deletion settings can be made through the update reservation setting screen in Fig. 18. Alternatively, the same settings may be able to be made through the certificate issuance request screen in Fig. 13A. The present invention is not particularly limited.

[0126] With reference to Fig. 19, a description is given of a process in which the multifunction peripheral 100 executes the electronic certificate automatic update function based on the electronic certificate update reservation settings. This processing is achieved by the CPU 201 executing a program loaded into the RAM 203.

[0127] First, in step S1901, the CPU 201 acquires the electronic certificate update reservation settings from the HDD 204.

[0128] Next, in step S1902, the CPU 201 acquires information of an electronic certificate that is currently used. This information corresponds to, for example, information stored in tables illustrated in Figs. 17A to 17C.

[0129] Next, in step S1903, the CPU 201 acquires the current date and time managed by the multifunction peripheral 100.

[0130] Then, in step S1904, the CPU 201 compares the electronic certificate update reservation settings with the information of the electronic certificate and determines whether it is necessary to update the electronic certificate currently in use. This determination is made according to a setting selected among the settings 1801, 1802, and 1803 illustrated in Fig. 18. If it is determined that it is not necessary to update the electronic certificate (NO in step S1904), the processing returns to step S1901.

[0131] On the other hand, if it is determined that it is necessary to update the electronic certificate (YES in step S1904), the processing proceeds to step S1905, and the control of the certificate issuance request process illustrated in Fig. 8 is performed. Then, if the certificate issuance request process is completed, the processing proceeds to step S1906.

[0132] In step S1906, the CPU 201 acquires from the HDD 204 the electronic certificate automatic deletion settings described with reference to Fig. 18.

[0133] Next, in step S1907, the CPU 201 determines whether the electronic certificate automatic deletion settings are enabled. If it is determined that the electronic certificate automatic deletion settings are not enabled (NO in step S1907), the processing proceeds to step S1910. For example, if the radio button 18041 in Fig. 18 is selected, it is determined that the electronic certificate automatic deletion settings are enabled.

[0134] If it is determined in step S1907 that the electronic certificate automatic deletion settings are enabled (YES in step S1907), then in step S1908, the CPU 201 determines whether there exists a certificate meeting a condition for a deletion target.

[0135] In step S1908, the CPU 201 determines whether there exists a certificate as a deletion target among all the electronic certificates stored in the multifunction peripheral 100. Based on the settings described with reference to Fig. 18, the CPU 201 determines whether each electronic certificate is set as a deletion target. For example, in a case where the check box 18043 is selected, if the number of electronic certificates stored in the multifunction peripheral 100 reaches the predetermined upper limit and if an electronic certificate satisfies a condition specified by any of the detailed settings 1805, the electronic certificate is set as a deletion target. Further, for example, in a case where the check box 18043 is not selected, an electronic certificate satisfying a condition specified by any of the detailed settings 1805 is set as a deletion target, regardless of whether the number of electronic certificates stored in the multifunction peripheral 100 reaches the upper limit.

[0136] If it is determined in step S1908 that there exists a certificate as a deletion target (YES in step S1908), the processing proceeds to step S1909. In step S1909, the CPU 201 deletes the electronic certificate as the deletion target in the HDD 204. Then, the processing proceeds to step S1910. If it is determined in step S1908 that there exists no electronic certificate as a deletion target (NO in step S1908), the processing proceeds to step S1910.

[0137] In this manner, if an electronic certificate is to be acquired from an external apparatus such as the certificate/registration authority 102, then according to settings, it is possible to delete an electronic certificate that should be deleted.

[0138] In the present exemplary embodiment, after an electronic certificate is acquired from the certificate/registration authority 102 and the purpose of the electronic certificate is set, an electronic certificate that should be deleted is deleted. Alternatively, an electronic certificate may be acquired from the certificate/registration authority 102 after the electronic certificate is deleted in step S1909.

[0139] According to the above exemplary embodiment, it is possible to automatically delete a certificate according to a particular condition even if a user does not manually give an instruction to delete an electronic certificate. Thus, even if the number of electronic certificates that can be stored in a multifunction peripheral is limited, it is possible to automatically update an electronic certificate while saving the user the trouble of deleting an electronic certificate.

Other Embodiments

[0140] Embodiment(s) of the present invention can also be realized by a computer of a system or apparatus that reads out and executes computer executable in-

structions (e.g., one or more programs) recorded on a storage medium (which may also be referred to more fully as a 'non-transitory computer-readable storage medium') to perform the functions of one or more of the above-described embodiment(s) and/or that includes one or more circuits (e.g., application specific integrated circuit (ASIC)) for performing the functions of one or more of the above-described embodiment(s), and by a method performed by the computer of the system or apparatus by, for example, reading out and executing the computer executable instructions from the storage medium to perform the functions of one or more of the above-described embodiment(s) and/or controlling the one or more circuits to perform the functions of one or more of the above-described embodiment(s). The computer may comprise one or more processors (e.g., central processing unit (CPU), micro processing unit (MPU)) and may include a network of separate computers or separate processors to read out and execute the computer executable instructions. The computer executable instructions may be provided to the computer, for example, from a network or the storage medium. The storage medium may include, for example, one or more of a hard disk, a random-access memory (RAM), a read only memory (ROM), a storage of distributed computing systems, an optical disk (such as a compact disc (CD), digital versatile disc (DVD), or Blu-ray Disc (BD)™), a flash memory device, a memory card, and the like.

[0141] While the present invention has been described with reference to exemplary embodiments, it is to be understood that the invention is not limited to the disclosed exemplary embodiments. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

[0142] An information processing apparatus automatically deletes an electronic certificate according to acquisition of an electronic certificate.

Claims

1. An information processing apparatus comprising:

generation means for generating an electronic certificate signing request based on a key pair;
transmission means for transmitting an electronic certificate issuance request including the electronic certificate signing request to an external apparatus;
reception means for receiving a response transmitted from the external apparatus in response to the issuance request;
acquisition means for acquiring a result of the certificate issuance request and an electronic certificate included in the response received by the reception means;
storage means for storing the electronic certificate acquired by the acquisition means;
setting means for making a setting for determining an electronic certificate that should be deleted among one or more electronic certificates stored in the storage means; and
deletion means for, in a case where the acquisition means is to acquire the electronic certificate from the external apparatus, deleting the electronic certificate that should be deleted according to the setting made by the setting means.

2. The information processing apparatus according to claim 1, wherein the deletion means deletes the electronic certificate that should be deleted in a case where the acquisition means is to acquire the electronic certificate from the external apparatus and the number of electronic certificates stored in the storage means is a predetermined number or more.

3. The information processing apparatus according to claim 1, wherein the setting means sets, as the electronic certificate that should be deleted, an electronic certificate associated with the same purpose as a purpose of the electronic certificate to be acquired from the external apparatus by the acquisition means.

4. The information processing apparatus according to claim 1, wherein the setting means sets, as the electronic certificate that should be deleted, an electronic certificate that is not associated with a purpose.

5. The information processing apparatus according to claim 1, wherein the setting means sets a self-certificate as the electronic certificate that should be deleted.

6. The information processing apparatus according to claim 1, wherein the setting means sets, as the electronic certificate that should be deleted, an electronic certificate stored in advance in the information processing apparatus before the information processing apparatus is shipped from a factory.

7. The information processing apparatus according to claim 1, wherein the setting means sets an expired electronic certificate as the electronic certificate that should be deleted.

8. The information processing apparatus according to any one of claims 1 to 7, wherein the setting means sets the electronic certificate that should be deleted according to an instruction from a user.

9. The information processing apparatus according to claim 1, wherein the deletion means deletes the electronic certificate that should be deleted after a pur-

pose of the electronic certificate acquired from the external apparatus by the acquisition means is set.

10. A control method for controlling an information processing apparatus for performing communication using an electronic certificate, the control method comprising:

setting an electronic certificate that should be deleted among one or more electronic certificates stored in the information processing apparatus;
generating an electronic certificate signing request based on a key pair;
transmitting an electronic certificate issuance request including the electronic certificate signing request to an external apparatus;
receiving a response transmitted from the external apparatus in response to the issuance request;
deleting the electronic certificate that should be deleted according to the made setting, in a case where an electronic certificate is to be acquired as the response from the external apparatus;
acquiring a result of the certificate issuance request and an electronic certificate included in the received response; and
storing the acquired electronic certificate in storage means.

11. A program for causing a computer to execute a control method for controlling an information processing apparatus for performing communication using an electronic certificate, the control method comprising:

setting an electronic certificate that should be deleted among one or more electronic certificates stored in the information processing apparatus;
generating an electronic certificate signing request based on a key pair;
transmitting an electronic certificate issuance request including the electronic certificate signing request to an external apparatus;
receiving a response transmitted from the external apparatus in response to the issuance request;
deleting the electronic certificate that should be deleted according to the made setting, in a case where an electronic certificate is to be acquired as the response from the external apparatus;
acquiring a result of the certificate issuance request and an electronic certificate included in the received response; and
storing the acquired electronic certificate in storage means.

FIG.1

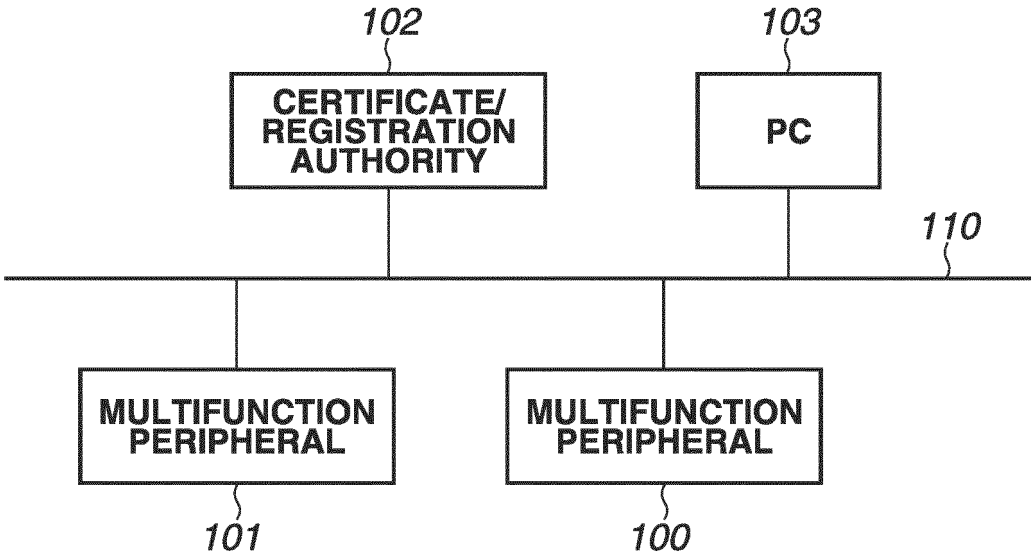

102
CERTIFICATE/
REGISTRATION
AUTHORITY
103
PC
110
MULTIFUNCTION
PERIPHERAL
MULTIFUNCTION
PERIPHERAL
101
100

FIG.2

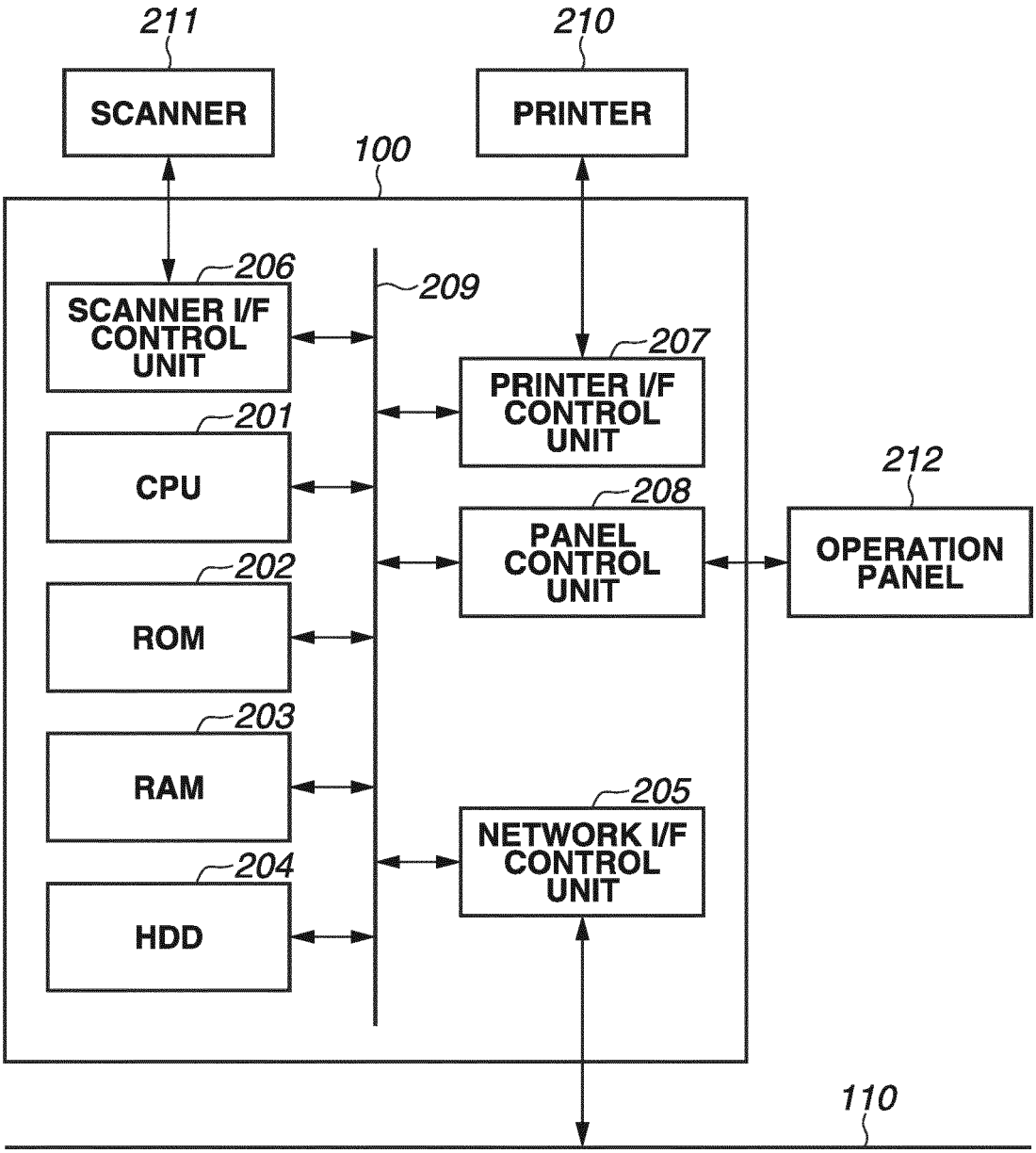

211
SCANNER
210
PRINTER
100
206
SCANNER I/F CONTROL UNIT
209
207
PRINTER I/F CONTROL UNIT
201
CPU
208
PANEL CONTROL UNIT
212
OPERATION PANEL
202
ROM
203
RAM
205
NETWORK I/F CONTROL UNIT
204
HDD
110

FIG.3

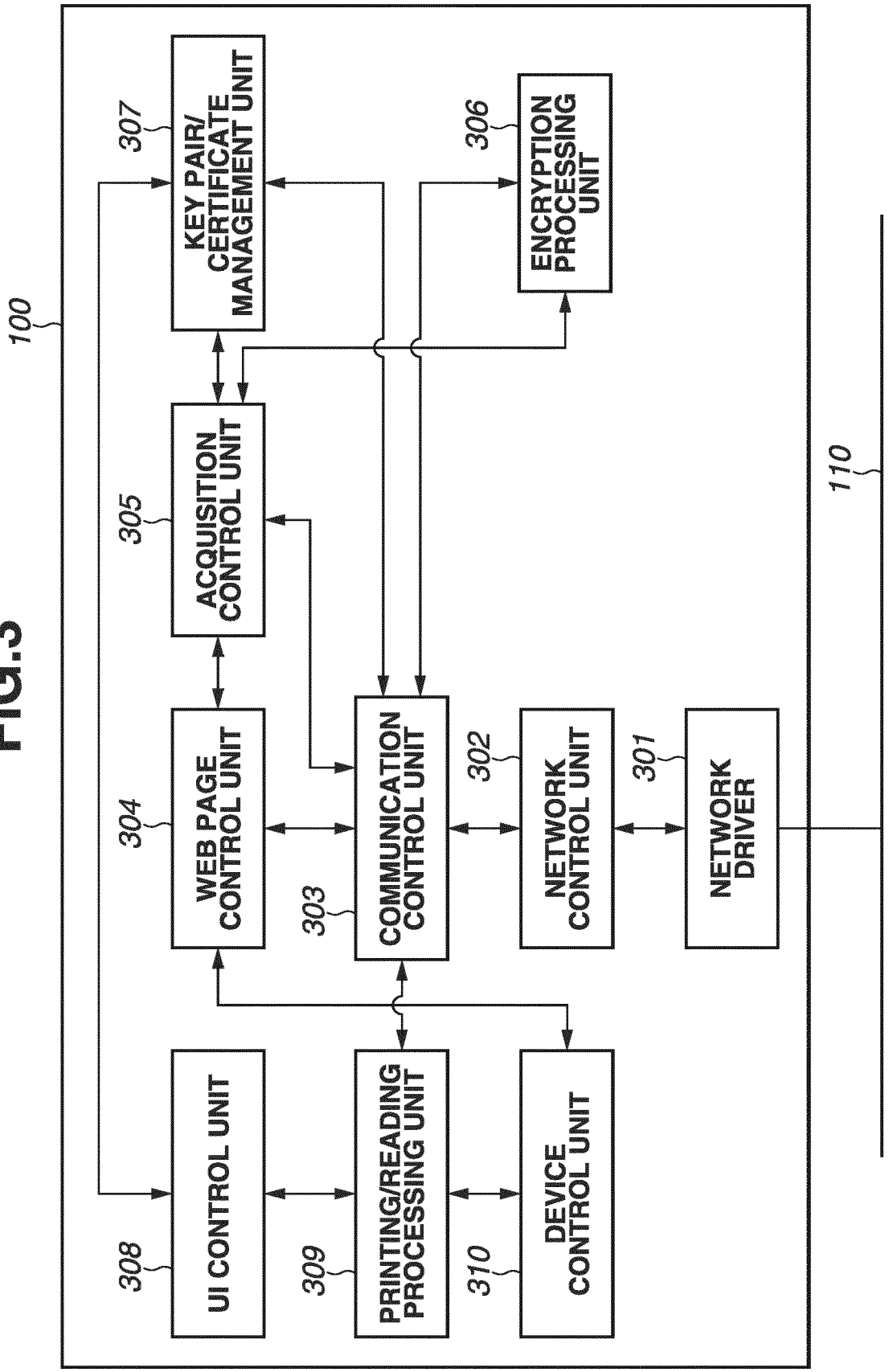

100
110
307
KEY PAIR/ CERTIFICATE MANAGEMENT UNIT
306
ENCRYPTION PROCESSING UNIT
305
ACQUISITION CONTROL UNIT
304
WEB PAGE CONTROL UNIT
303
COMMUNICATION CONTROL UNIT
302
NETWORK CONTROL UNIT
301
NETWORK DRIVER
308
UI CONTROL UNIT
309
PRINTING/READING PROCESSING UNIT
310
DEVICE CONTROL UNIT

FIG.4

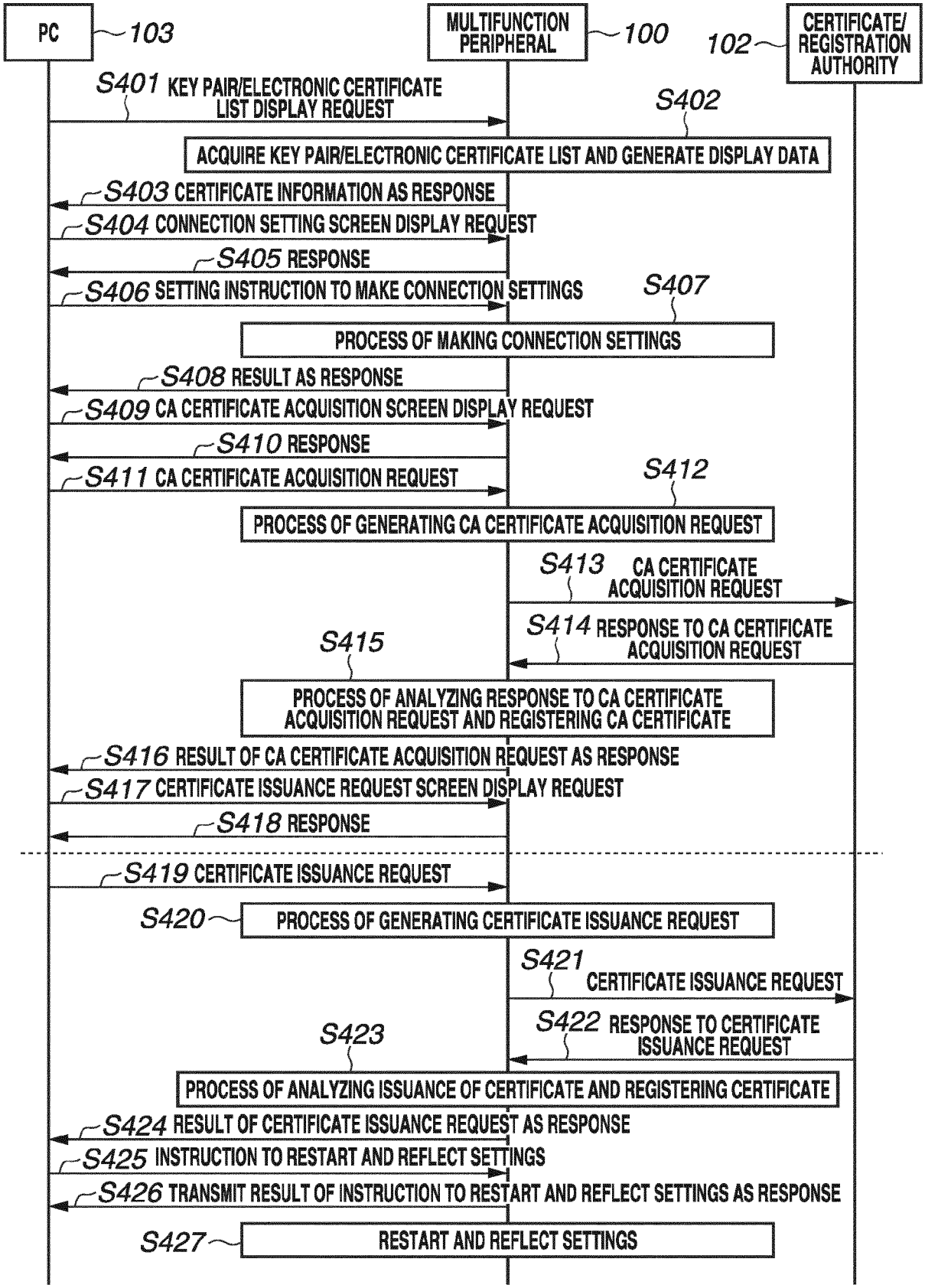

PC
103
MULTIFUNCTION PERIPHERAL
100
102
CERTIFICATE/ REGISTRATION AUTHORITY
S401 KEY PAIR/ELECTRONIC CERTIFICATE LIST DISPLAY REQUEST
S402
ACQUIRE KEY PAIR/ELECTRONIC CERTIFICATE LIST AND GENERATE DISPLAY DATA
S403 CERTIFICATE INFORMATION AS RESPONSE
S404 CONNECTION SETTING SCREEN DISPLAY REQUEST
S405 RESPONSE
S406 SETTING INSTRUCTION TO MAKE CONNECTION SETTINGS
S407
PROCESS OF MAKING CONNECTION SETTINGS
S408 RESULT AS RESPONSE
S409 CA CERTIFICATE ACQUISITION SCREEN DISPLAY REQUEST
S410 RESPONSE
S411 CA CERTIFICATE ACQUISITION REQUEST
S412
PROCESS OF GENERATING CA CERTIFICATE ACQUISITION REQUEST
S413 CA CERTIFICATE ACQUISITION REQUEST
S414 RESPONSE TO CA CERTIFICATE ACQUISITION REQUEST
S415
PROCESS OF ANALYZING RESPONSE TO CA CERTIFICATE ACQUISITION REQUEST AND REGISTERING CA CERTIFICATE
S416 RESULT OF CA CERTIFICATE ACQUISITION REQUEST AS RESPONSE
S417 CERTIFICATE ISSUANCE REQUEST SCREEN DISPLAY REQUEST
S418 RESPONSE
S419 CERTIFICATE ISSUANCE REQUEST
S420
PROCESS OF GENERATING CERTIFICATE ISSUANCE REQUEST
S421 CERTIFICATE ISSUANCE REQUEST
S422 RESPONSE TO CERTIFICATE ISSUANCE REQUEST
S423
PROCESS OF ANALYZING ISSUANCE OF CERTIFICATE AND REGISTERING CERTIFICATE
S424 RESULT OF CERTIFICATE ISSUANCE REQUEST AS RESPONSE
S425 INSTRUCTION TO RESTART AND REFLECT SETTINGS
S426 TRANSMIT RESULT OF INSTRUCTION TO RESTART AND REFLECT SETTINGS AS RESPONSE
S427
RESTART AND REFLECT SETTINGS

FIG.5A

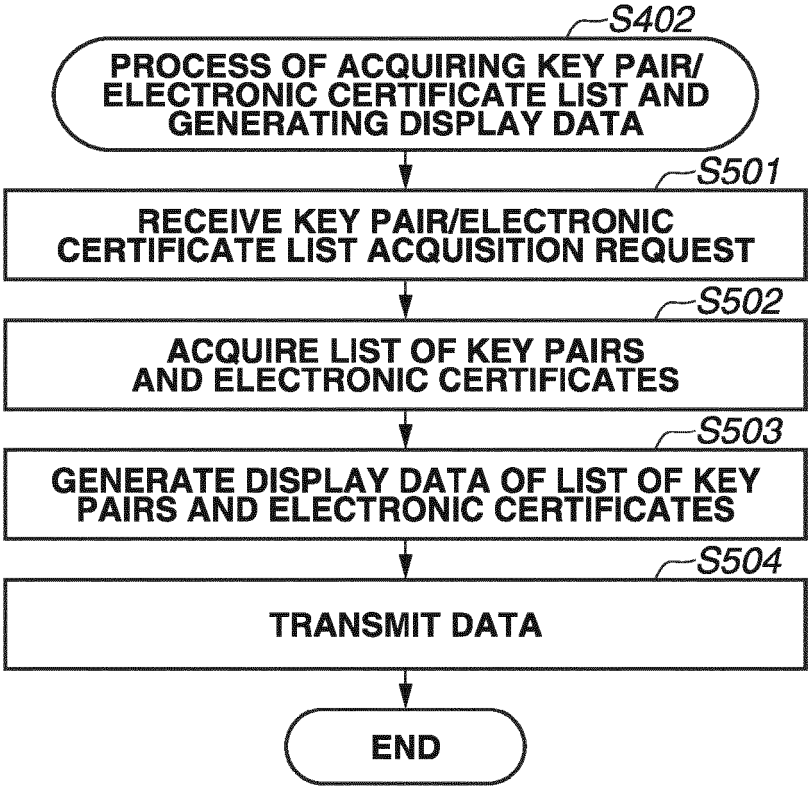

S402
PROCESS OF ACQUIRING KEY PAIR/ ELECTRONIC CERTIFICATE LIST AND GENERATING DISPLAY DATA
S501
RECEIVE KEY PAIR/ELECTRONIC CERTIFICATE LIST ACQUISITION REQUEST
S502
ACQUIRE LIST OF KEY PAIRS AND ELECTRONIC CERTIFICATES
S503
GENERATE DISPLAY DATA OF LIST OF KEY PAIRS AND ELECTRONIC CERTIFICATES
S504
TRANSMIT DATA
END

FIG.5B

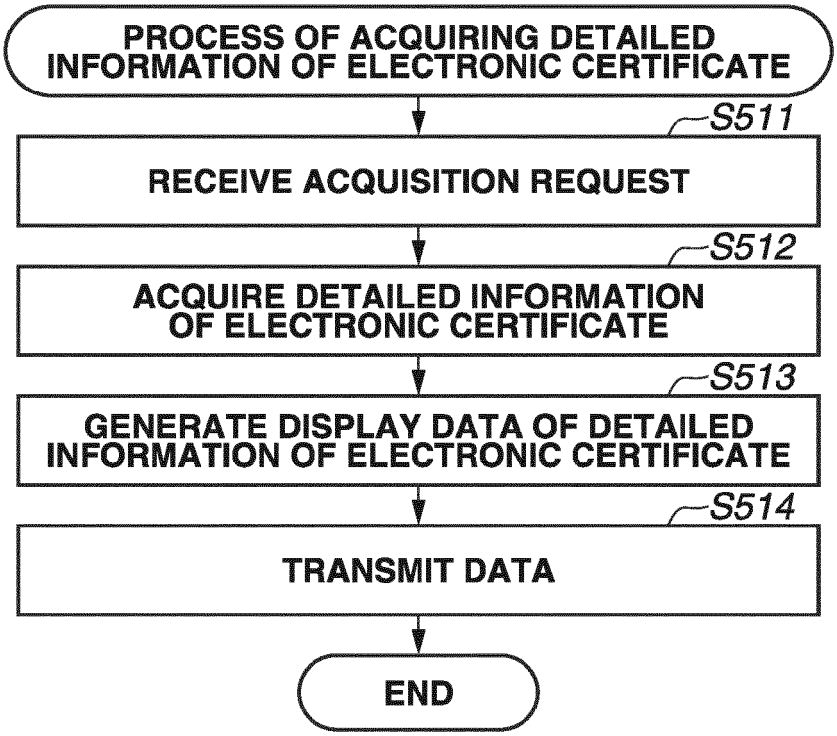

PROCESS OF ACQUIRING DETAILED INFORMATION OF ELECTRONIC CERTIFICATE
S511
RECEIVE ACQUISITION REQUEST
S512
ACQUIRE DETAILED INFORMATION OF ELECTRONIC CERTIFICATE
S513
GENERATE DISPLAY DATA OF DETAILED INFORMATION OF ELECTRONIC CERTIFICATE
S514
TRANSMIT DATA
END

FIG.6

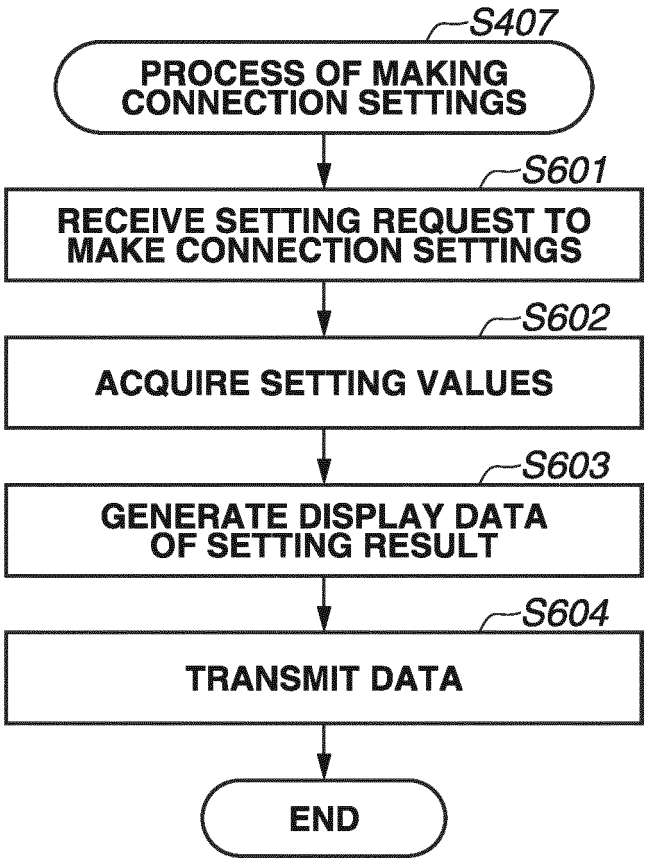

S407
PROCESS OF MAKING CONNECTION SETTINGS
S601
RECEIVE SETTING REQUEST TO MAKE CONNECTION SETTINGS
S602
ACQUIRE SETTING VALUES
S603
GENERATE DISPLAY DATA OF SETTING RESULT
S604
TRANSMIT DATA
END

FIG.7

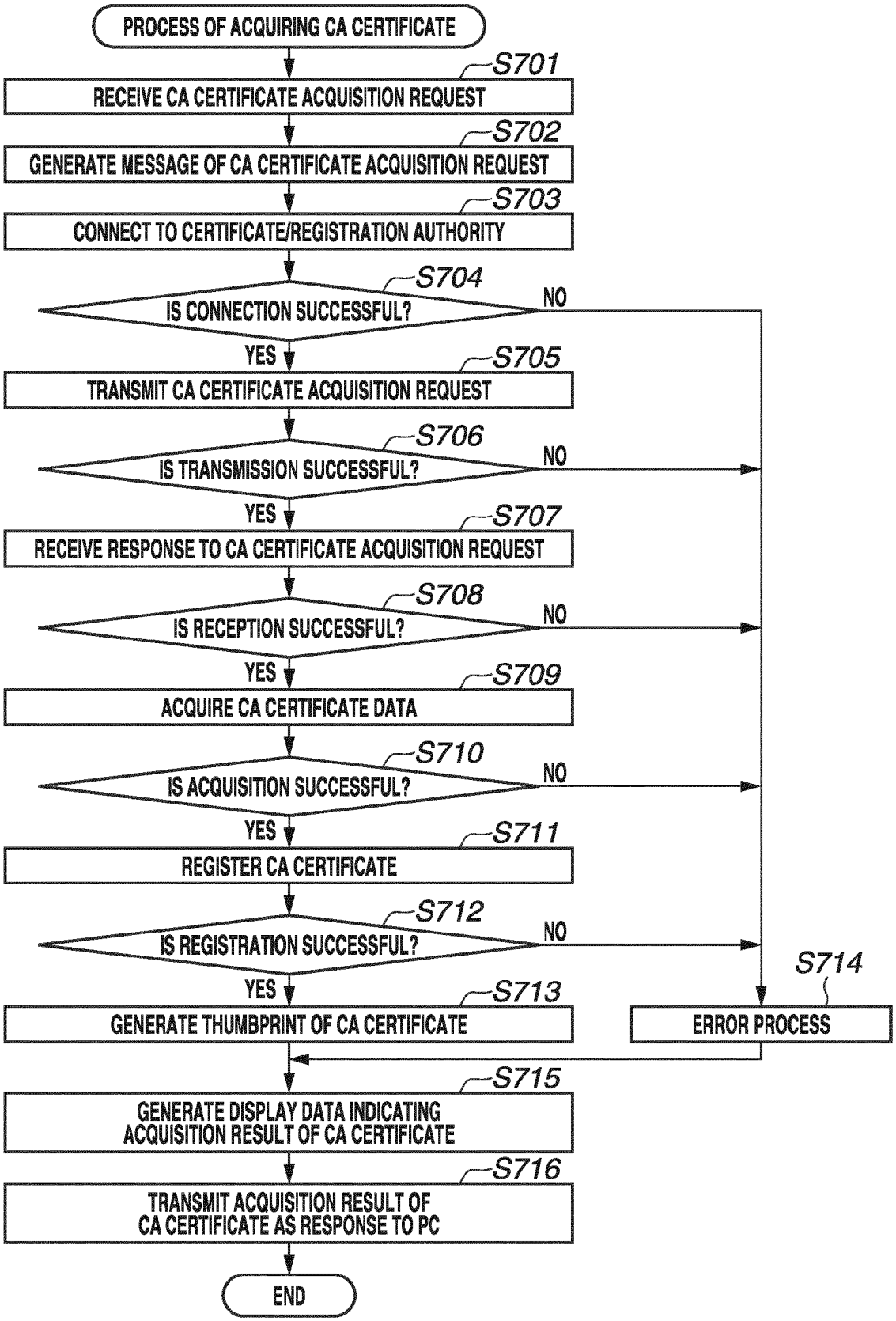

PROCESS OF ACQUIRING CA CERTIFICATE
S701
RECEIVE CA CERTIFICATE ACQUISITION REQUEST
S702
GENERATE MESSAGE OF CA CERTIFICATE ACQUISITION REQUEST
S703
CONNECT TO CERTIFICATE/REGISTRATION AUTHORITY
S704
IS CONNECTION SUCCESSFUL?
NO
YES
S705
TRANSMIT CA CERTIFICATE ACQUISITION REQUEST
S706
IS TRANSMISSION SUCCESSFUL?
NO
YES
S707
RECEIVE RESPONSE TO CA CERTIFICATE ACQUISITION REQUEST
S708
IS RECEPTION SUCCESSFUL?
NO
YES
S709
ACQUIRE CA CERTIFICATE DATA
S710
IS ACQUISITION SUCCESSFUL?
NO
YES
S711
REGISTER CA CERTIFICATE
S712
IS REGISTRATION SUCCESSFUL?
NO
YES
S713
GENERATE THUMBPRINT OF CA CERTIFICATE
S714
ERROR PROCESS
S715
GENERATE DISPLAY DATA INDICATING ACQUISITION RESULT OF CA CERTIFICATE
S716
TRANSMIT ACQUISITION RESULT OF CA CERTIFICATE AS RESPONSE TO PC
END

FIG.8

FIG.8A

FIG.8B

FIG.8A

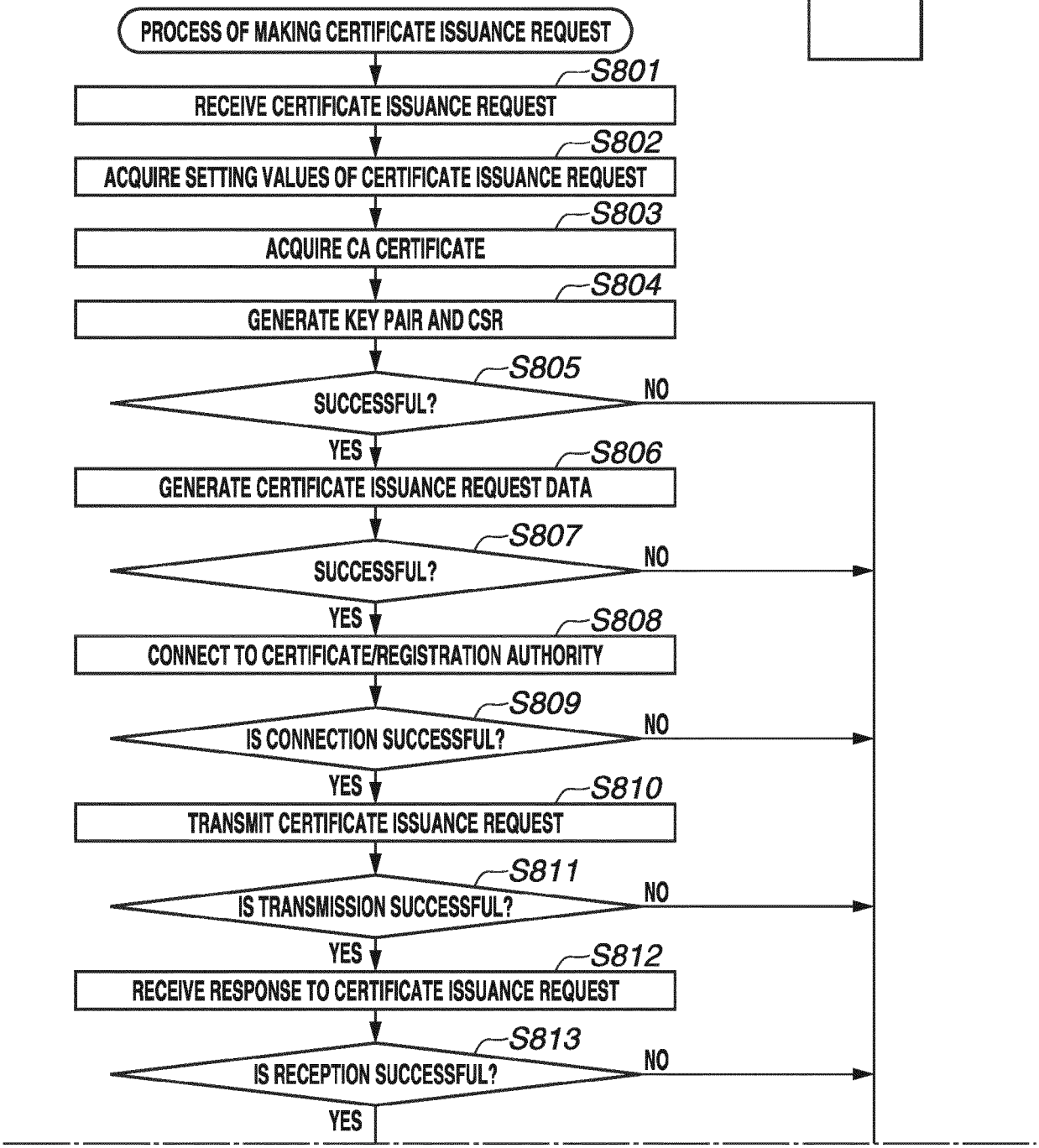


FIG.8B

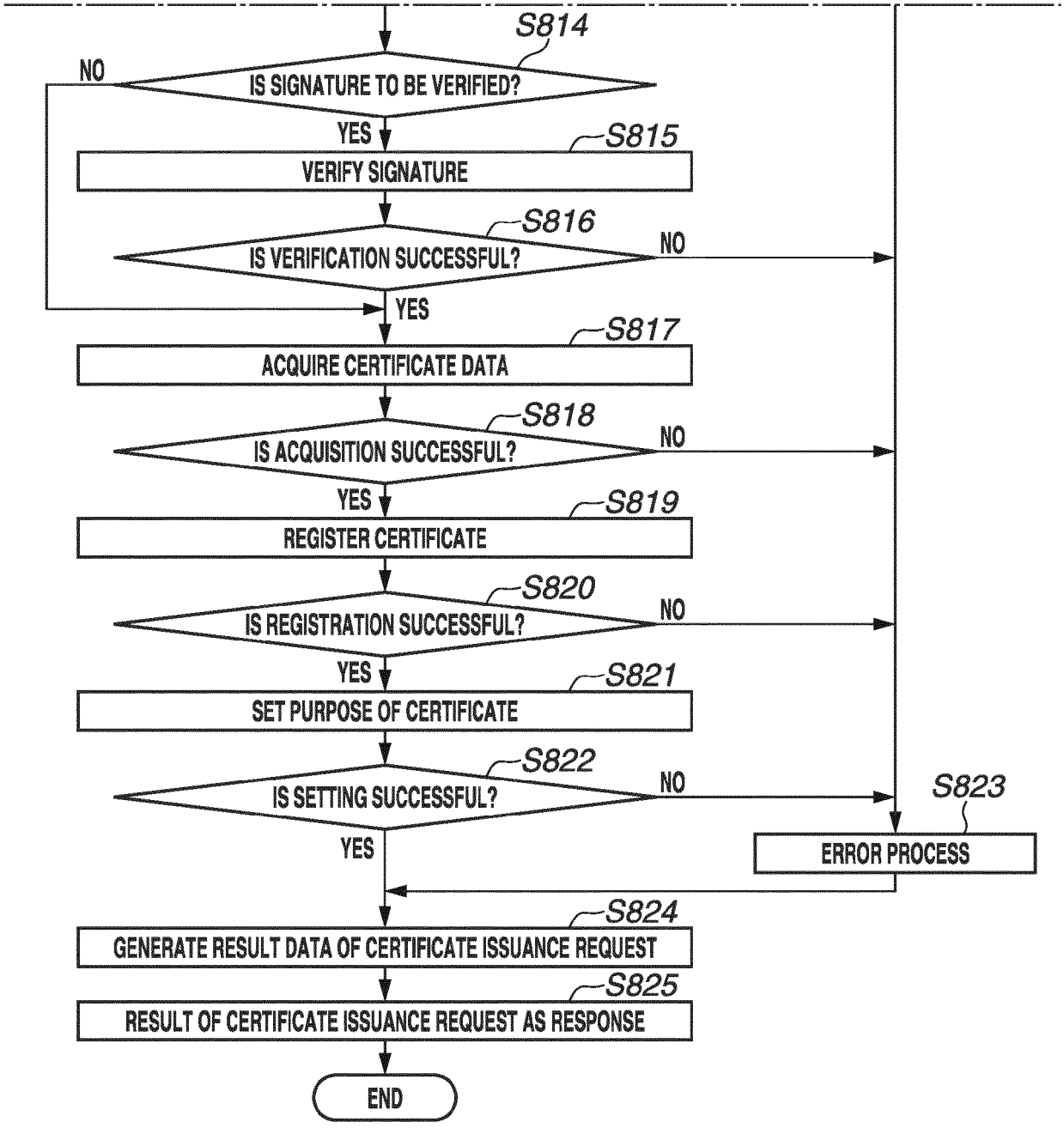

S814
IS SIGNATURE TO BE VERIFIED?
NO
YES
S815
VERIFY SIGNATURE
S816
IS VERIFICATION SUCCESSFUL?
NO
YES
S817
ACQUIRE CERTIFICATE DATA
S818
IS ACQUISITION SUCCESSFUL?
NO
YES
S819
REGISTER CERTIFICATE
S820
IS REGISTRATION SUCCESSFUL?
NO
YES
S821
SET PURPOSE OF CERTIFICATE
S822
IS SETTING SUCCESSFUL?
NO
YES
S823
ERROR PROCESS
S824
GENERATE RESULT DATA OF CERTIFICATE ISSUANCE REQUEST
S825
RESULT OF CERTIFICATE ISSUANCE REQUEST AS RESPONSE
END

FIG.9

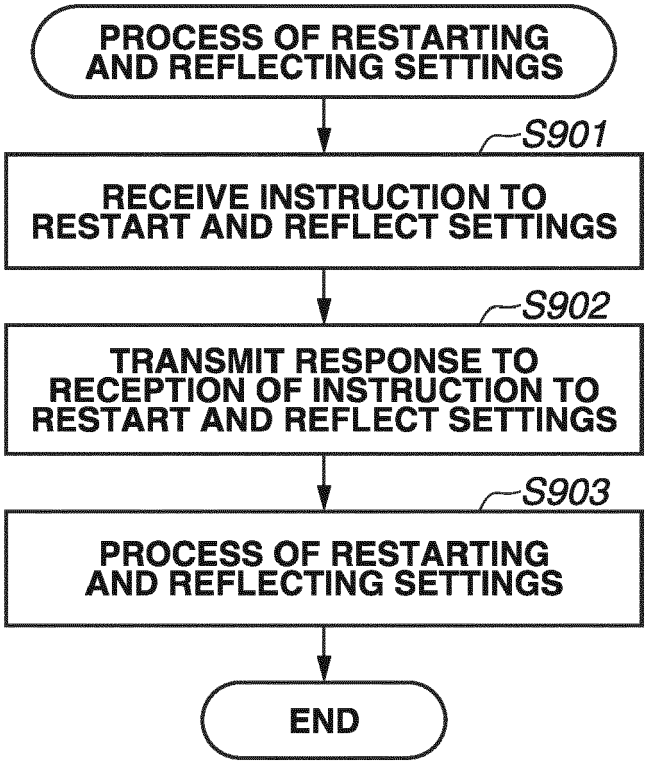

PROCESS OF RESTARTING AND REFLECTING SETTINGS
S901
RECEIVE INSTRUCTION TO RESTART AND REFLECT SETTINGS
S902
TRANSMIT RESPONSE TO RECEPTION OF INSTRUCTION TO RESTART AND REFLECT SETTINGS
S903
PROCESS OF RESTARTING AND REFLECTING SETTINGS
END

FIG.10A

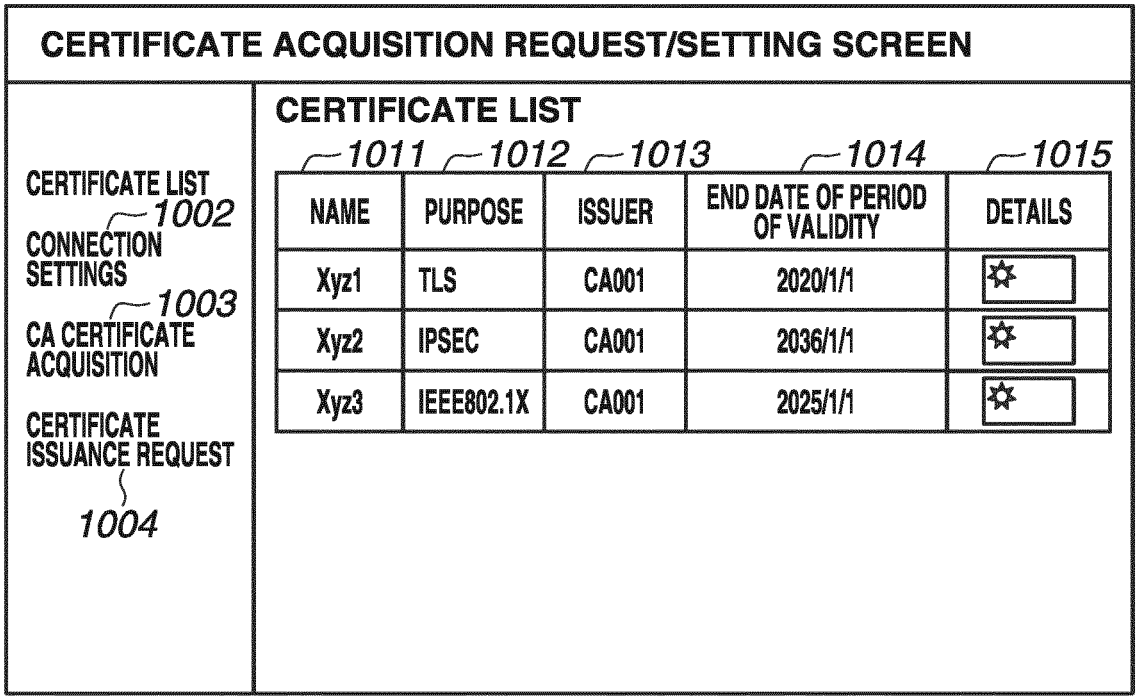


FIG.10B

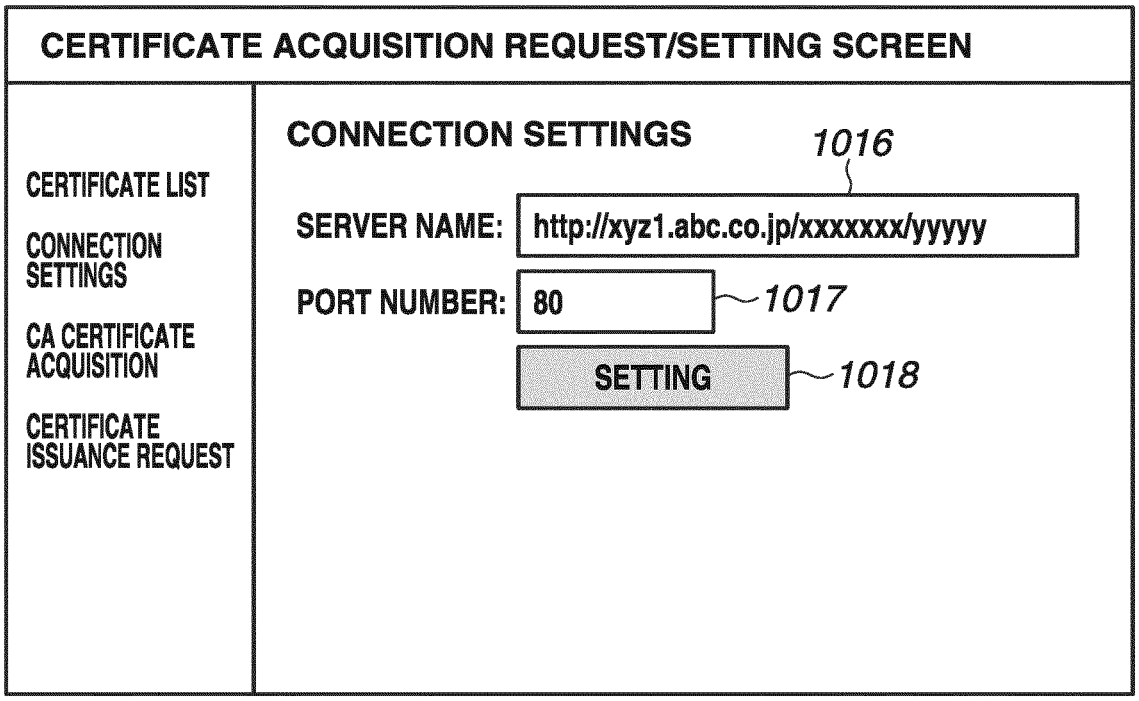


FIG.11A

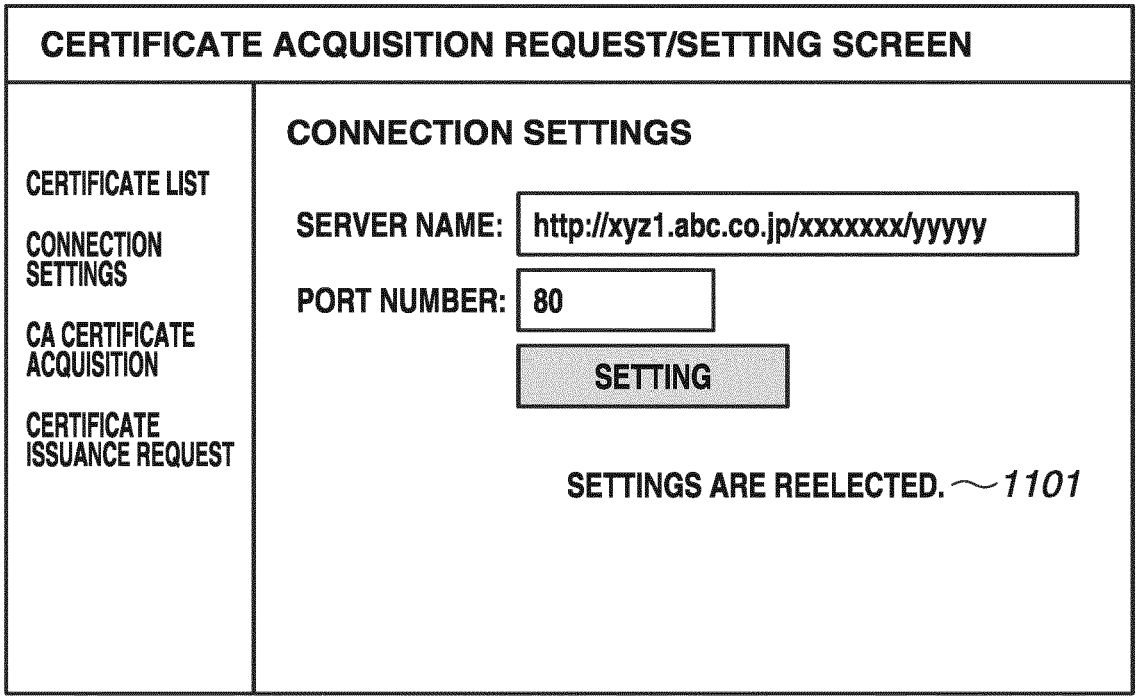


FIG.11B

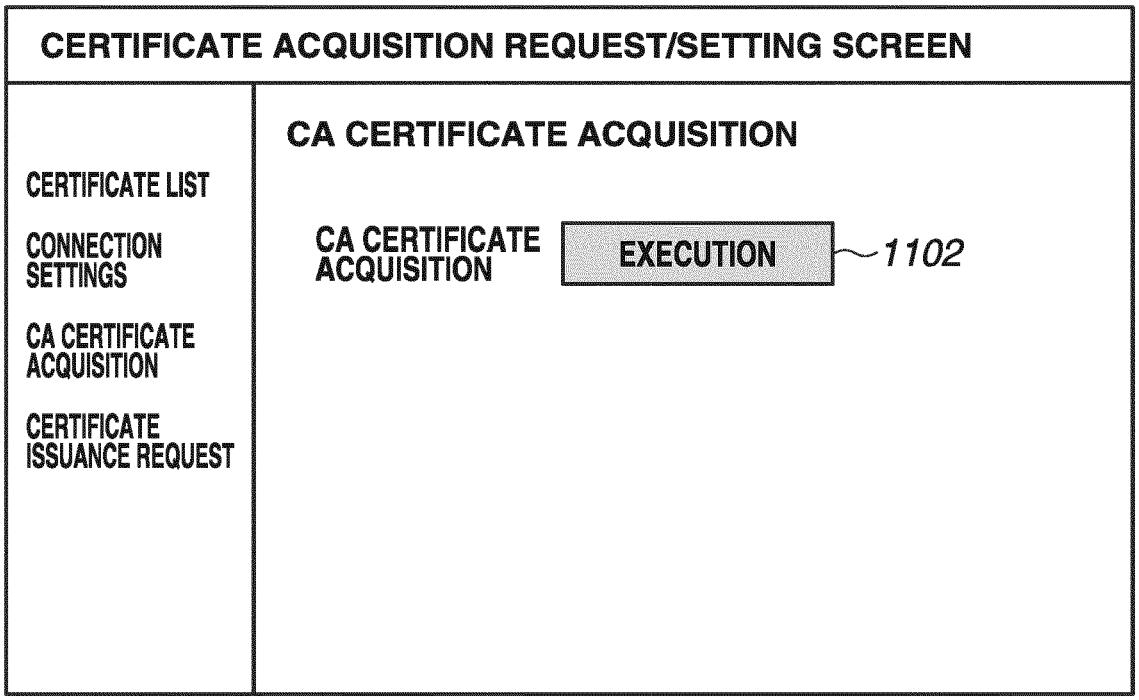


FIG.12A

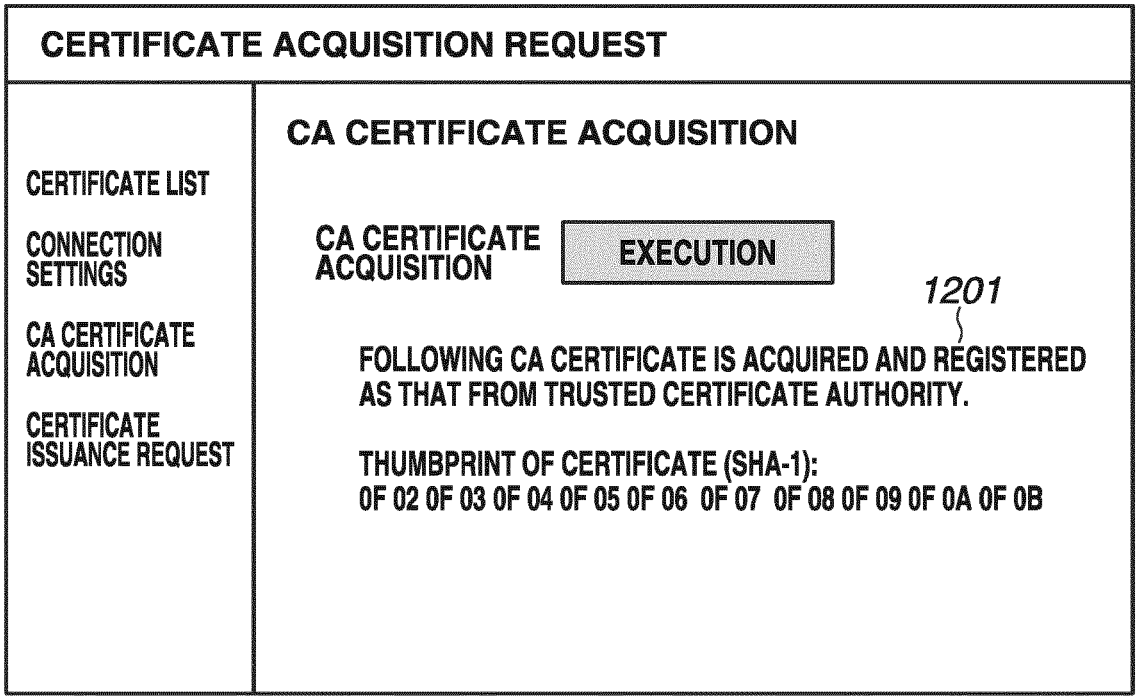


FIG.12B

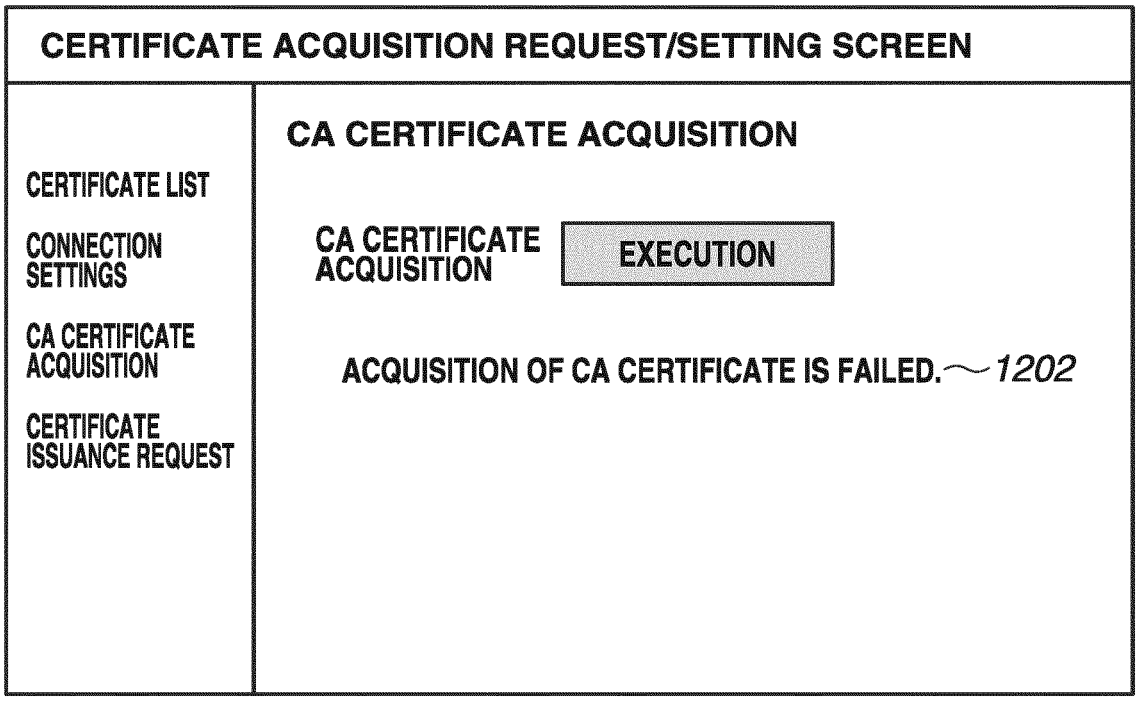


FIG.13A

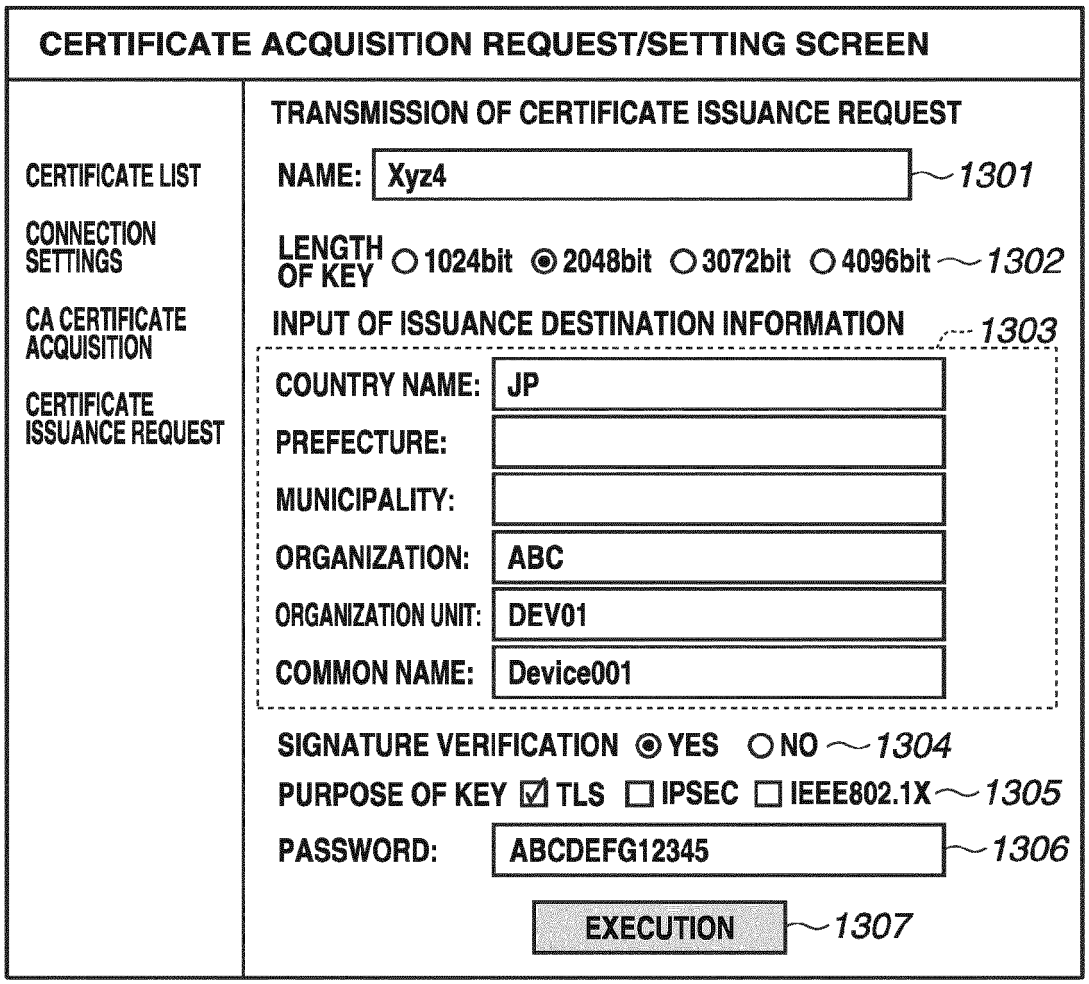


FIG.13B

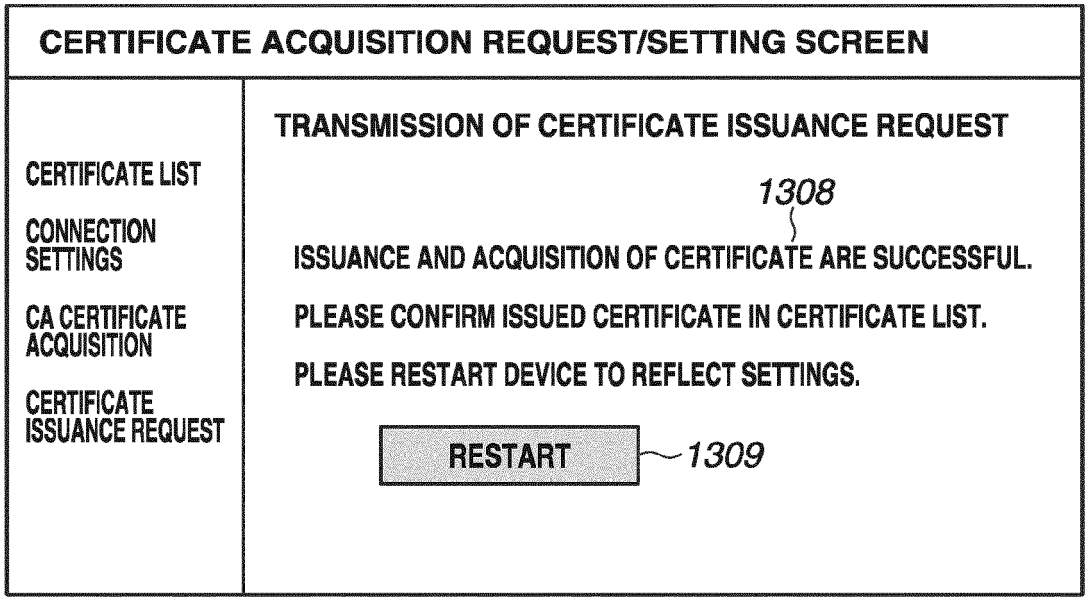


FIG.14A

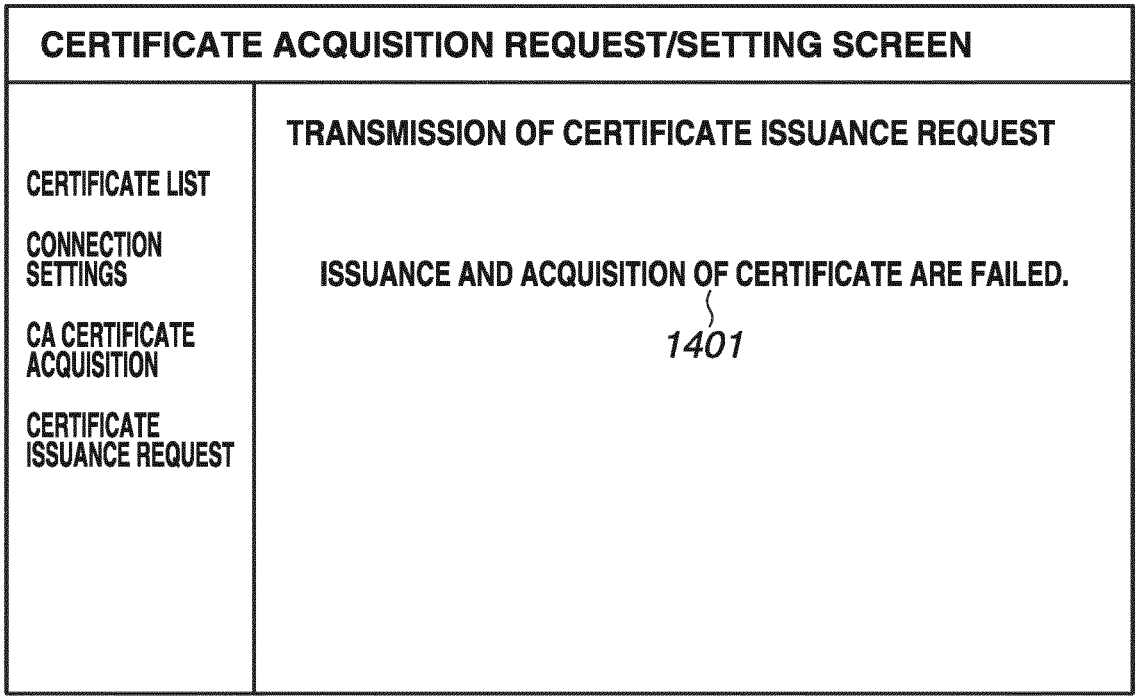


FIG.14B

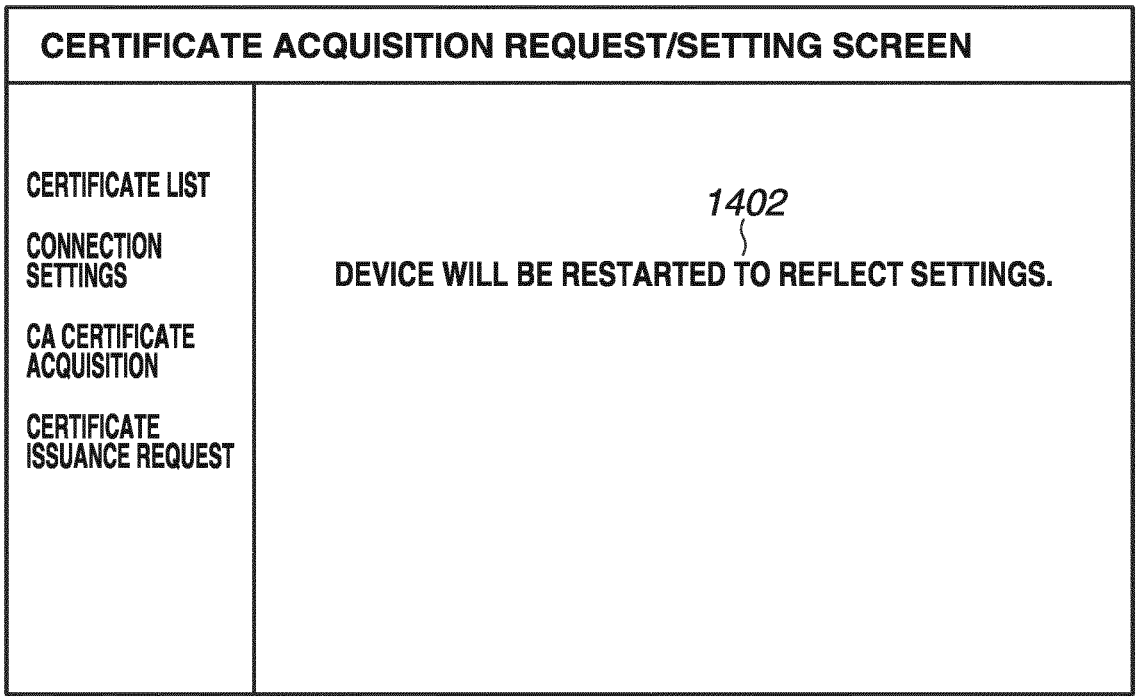


FIG.15

CERTIFICATE ACQUISITION REQUEST/SETTING SCREEN

CERTIFICATE LIST

CONNECTION SETTINGS

CA CERTIFICATE ACQUISITION

CERTIFICATE ISSUANCE REQUEST

CERTIFICATE LIST

NAME	PURPOSE	ISSUER	END DATE OF PERIOD OF VALIDITY	DETAILS
Xyz1	—	CA001	2020/1/1	☼
Xyz2	IPSEC	CA001	2036/1/1	☼
Xyz3	IEEE802.1X	CA001	2025/1/1	☼
Xyz4	TLS	CA001	2021/1/1	☼

1501

FIG.16

CERTIFICATE ACQUISITION REQUEST/SETTING SCREEN

CERTIFICATE LIST

CONNECTION SETTINGS

CA CERTIFICATE ACQUISITION

CERTIFICATE ISSUANCE REQUEST

DETAILS OF CERTIFICATE INFORMATION

NAME: Xyz1

PURPOSE: TLS

ISSUER: CN=CA01, C=JP

START OF PERIOD OF VALIDITY: 2017/1/1
END OF PERIOD OF VALIDITY: 2020/1/1

ISSUANCE DESTINATION: CN=Device001, OU=Dev.A, O=ABC, C=JP

ALGORITHM OF KEY: RSA 2048bit

SERIAL NUMBER: 01 02 03 04 05

THUMBPRINT OF CERTIFICATE (SHA-1):
01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 01 0B

FIG.17A

NAME	PURPOSE	ISSUER	START DATE OF PERIOD OF VALIDITY	END DATE OF PERIOD OF VALIDITY	ISSUANCE DESTINATION	ALGORITHM	KEY LENGTH	SERIAL NUMBER	THUMBPRINT
Xyz1	TLS	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 01 0B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2036/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	02 02 02 03 02 04 02 05 02 06 02 07 02 08 02 09 02 0A 02 0B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	03 02 03 03 03 04 03 05 03 06 03 07 03 08 03 09 03 0A 03 0B

FIG.17B

NAME	PURPOSE	ISSUER	START DATE OF PERIOD OF VALIDITY	END DATE OF PERIOD OF VALIDITY	ISSUANCE DESTINATION	ALGORITHM	KEY LENGTH	SERIAL NUMBER	THUMBPRINT
Xyz1	TLS	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 01 0B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2036/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	02 02 02 03 02 04 02 05 02 06 02 07 02 08 02 09 02 0A 02 0B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	03 02 03 03 03 04 03 05 03 06 03 07 03 08 03 09 03 0A 03 0B
Xyz4	ABSENT	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 08	04 02 04 04 04 04 04 05 04 06 04 07 04 08 04 09 04 0A 04 0B

FIG.17C

NAME	PURPOSE	ISSUER	START DATE OF PERIOD OF VALIDITY	END DATE OF PERIOD OF VALIDITY	ISSUANCE DESTINATION	ALGORITHM	KEY LENGTH	SERIAL NUMBER	THUMBPRINT
Xyz1	ABSENT	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 01 0B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2036/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	02 02 02 03 02 04 02 05 02 06 02 07 02 08 02 09 02 0A 02 0B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	03 02 03 03 03 04 03 05 03 06 03 07 03 08 03 09 03 0A 03 0B
Xyz4	TLS	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001,OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 08	04 02 04 04 04 04 04 05 04 06 04 07 04 08 04 09 04 0A 04 0B

FIG.18

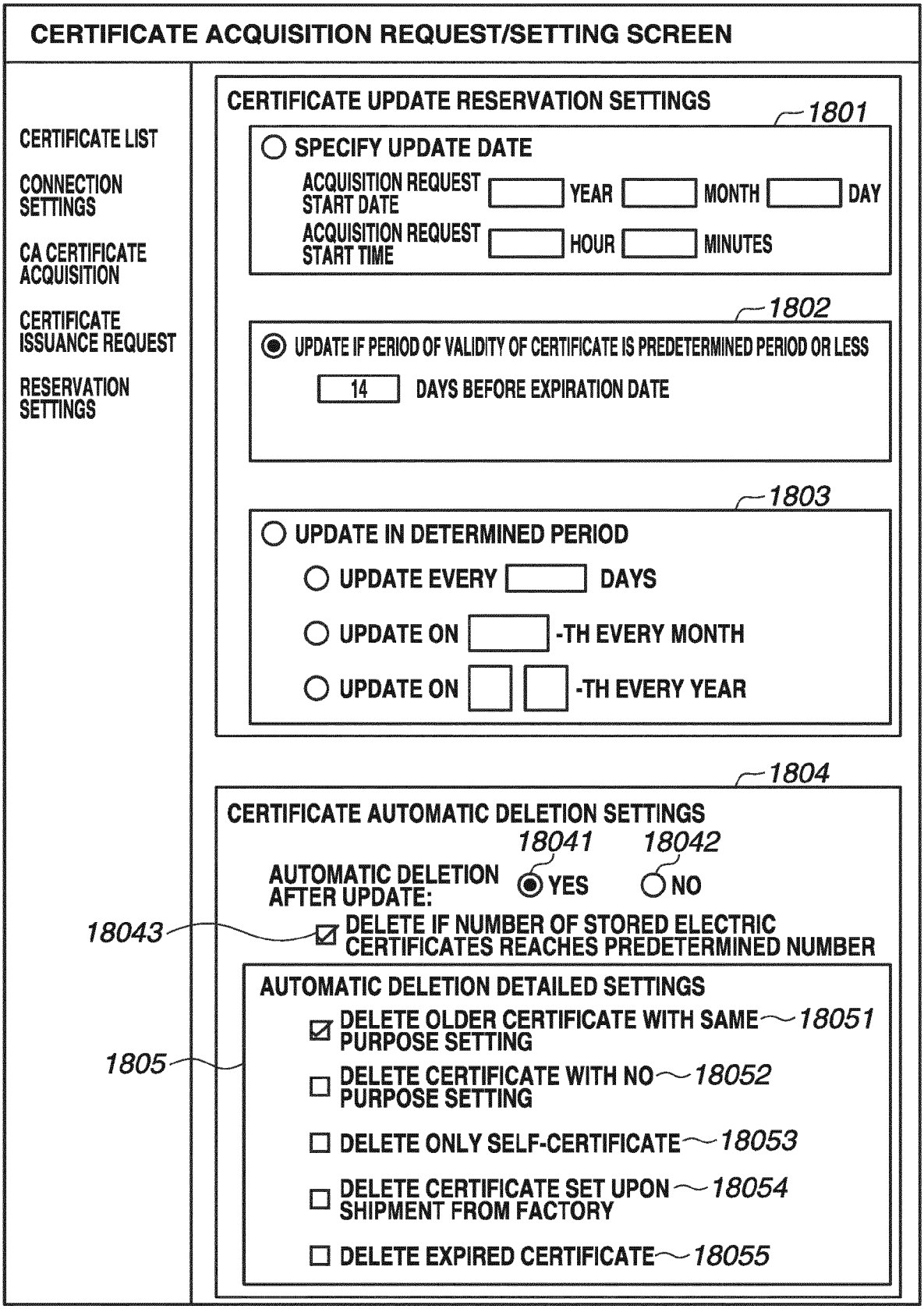
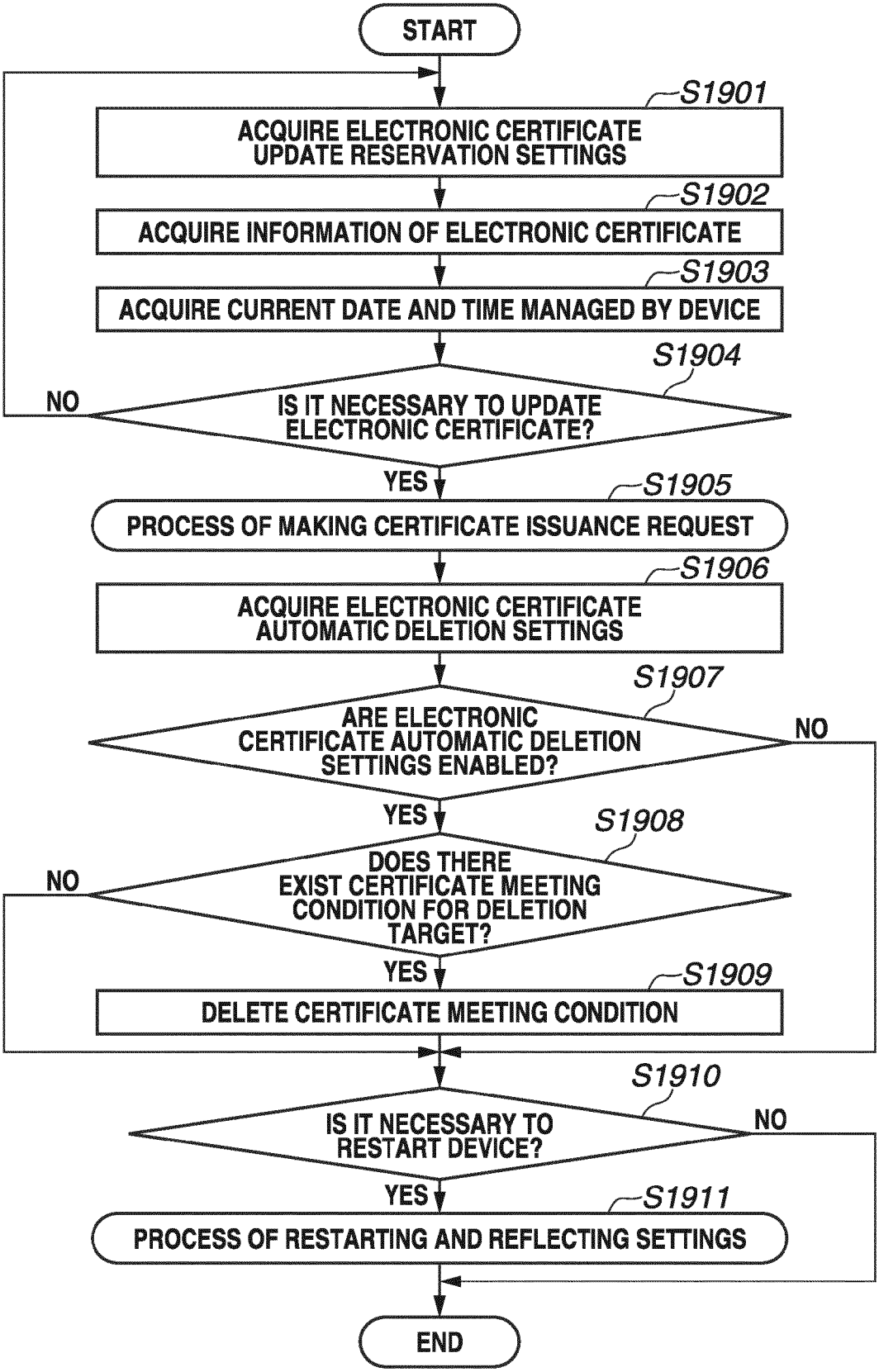

CERTIFICATE ACQUISITION REQUEST/SETTING SCREEN
CERTIFICATE LIST
CONNECTION SETTINGS
CA CERTIFICATE ACQUISITION
CERTIFICATE ISSUANCE REQUEST
RESERVATION SETTINGS
CERTIFICATE UPDATE RESERVATION SETTINGS
1801
SPECIFY UPDATE DATE
ACQUISITION REQUEST START DATE
YEAR
MONTH
DAY
ACQUISITION REQUEST START TIME
HOUR
MINUTES
1802
UPDATE IF PERIOD OF VALIDITY OF CERTIFICATE IS PREDETERMINED PERIOD OR LESS
14
DAYS BEFORE EXPIRATION DATE
1803
UPDATE IN DETERMINED PERIOD
UPDATE EVERY
DAYS
UPDATE ON
-TH EVERY MONTH
UPDATE ON
-TH EVERY YEAR
1804
CERTIFICATE AUTOMATIC DELETION SETTINGS
18041
18042
AUTOMATIC DELETION AFTER UPDATE:
YES
NO
18043
DELETE IF NUMBER OF STORED ELECTRIC CERTIFICATES REACHES PREDETERMINED NUMBER
1805
AUTOMATIC DELETION DETAILED SETTINGS
DELETE OLDER CERTIFICATE WITH SAME PURPOSE SETTING
18051
DELETE CERTIFICATE WITH NO PURPOSE SETTING
18052
DELETE ONLY SELF-CERTIFICATE
18053
DELETE CERTIFICATE SET UPON SHIPMENT FROM FACTORY
18054
DELETE EXPIRED CERTIFICATE
18055

FIG.19


START
S1901
ACQUIRE ELECTRONIC CERTIFICATE UPDATE RESERVATION SETTINGS
S1902
ACQUIRE INFORMATION OF ELECTRONIC CERTIFICATE
S1903
ACQUIRE CURRENT DATE AND TIME MANAGED BY DEVICE
S1904
IS IT NECESSARY TO UPDATE ELECTRONIC CERTIFICATE?
NO
YES
S1905
PROCESS OF MAKING CERTIFICATE ISSUANCE REQUEST
S1906
ACQUIRE ELECTRONIC CERTIFICATE AUTOMATIC DELETION SETTINGS
S1907
ARE ELECTRONIC CERTIFICATE AUTOMATIC DELETION SETTINGS ENABLED?
NO
YES
S1908
DOES THERE EXIST CERTIFICATE MEETING CONDITION FOR DELETION TARGET?
NO
YES
S1909
DELETE CERTIFICATE MEETING CONDITION
S1910
IS IT NECESSARY TO RESTART DEVICE?
NO
YES
S1911
PROCESS OF RESTARTING AND REFLECTING SETTINGS
END

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 18 17 4721

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	JP 2010 177744 A (SOFTBANK MOBILE CORP) 12 August 2010 (2010-08-12) * paragraph [0049] - paragraph [0051] *	1-11	INV. G06F21/33 H04L9/32 H04L29/06
X	US 2011/161662 A1 (LEE CHUNG-I [TW] ET AL) 30 June 2011 (2011-06-30) * paragraphs [0015], [0022], [0023] *	1,10,11	
X	JP 2013 223171 A (NIPPON TELEGRAPH & TELEPHONE) 28 October 2013 (2013-10-28) * paragraph [0030] - paragraph [0032] *	1,10,11	

TECHNICAL FIELDS SEARCHED (IPC)
G06F
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	19 July 2018	Frank, Mario

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 18 17 4721

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-07-2018

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2010177744 A	12-08-2010	JP 5412120 B2	12-02-2014
		JP 2010177744 A	12-08-2010
US 2011161662 A1	30-06-2011	CN 102118374 A	06-07-2011
		US 2011161662 A1	30-06-2011
JP 2013223171 A	28-10-2013	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2016178458 A **[0005]**