

(21) Application No: **1802583.3**
 (22) Date of Filing: **16.02.2018**
 (30) Priority Data:
 (31) **2017028424** (32) **17.02.2017** (33) **JP**

(51) INT CL:
H04L 9/32 (2006.01) **G06F 21/44** (2013.01)
H04L 29/06 (2006.01) **G06F 21/45** (2013.01)
G06F 21/60 (2013.01) **G06F 21/64** (2013.01)

(56) Documents Cited:
US 20140258709 A1 **US 20130086377 A1**
US 20120023327 A1 **US 20070168658 A1**

(71) Applicant(s):
Canon Kabushiki Kaisha
30-2 Shimomaruko 3-Chome, Ohta-ku,
146-8501 Tokyo, Japan

(58) Field of Search:
 INT CL **G06F, H04L**
 Other: **WPI, EPDOC**

(72) Inventor(s):
Naoya Kakutani
Hisayuki Yamauchi

(74) Agent and/or Address for Service:
Canon Europe Limited
European Intellectual Property Group, 3 The Square,
Stockley Park, Uxbridge, Middlesex, UB11 1ET,
United Kingdom

(54) Title of the Invention: **Information processing apparatus, image forming apparatus, system, method of controlling the same, and storage medium**
 Abstract Title: **Obtaining an electronic certificate by an information processing apparatus**

(57) An information processing apparatus 100 generates a public key pair in accordance with a certificate issuance request, generates a certificate signing request CSR S421 based on the public key pair and transmits the certificate signing request to an external apparatus 102, such as a Certification Authority, CA. The information processing apparatus obtains an electronic certificate and a certificate issuance request result from the external apparatus as a response S422 to the issuance request, and sets the application of the obtained electronic certificate, such as using it for secure communication according to SSL, TLS, IEEE802.1X or IPSEC (certificate-based secure communication protocols), possibly after restart of the apparatus S427. The information processing apparatus may receive the certificate issuance request instruction S419 from a second information processing apparatus (e.g. PC, 103), wherein the information processing apparatus sends display control data to display as a user interface on the second information processing apparatus. A further embodiment relates to an information processing apparatus that automatically updates its certificate at a set update time or according to an update rule selected by an update management unit. The information processing apparatus may be a multi-function peripheral (MFP) or multi-function device (MFD) e.g. combined printer, scanner, copier.

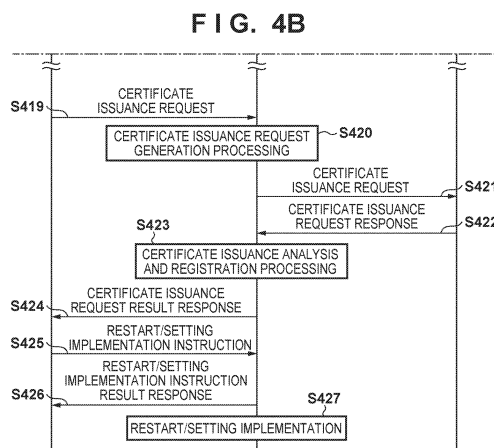
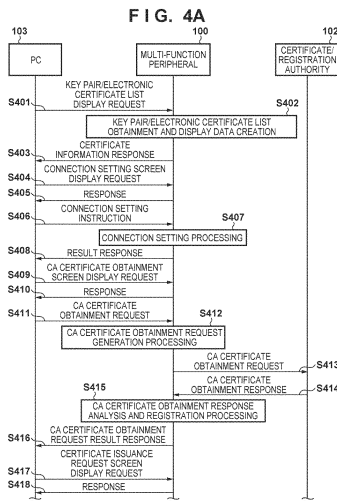


FIG. 1

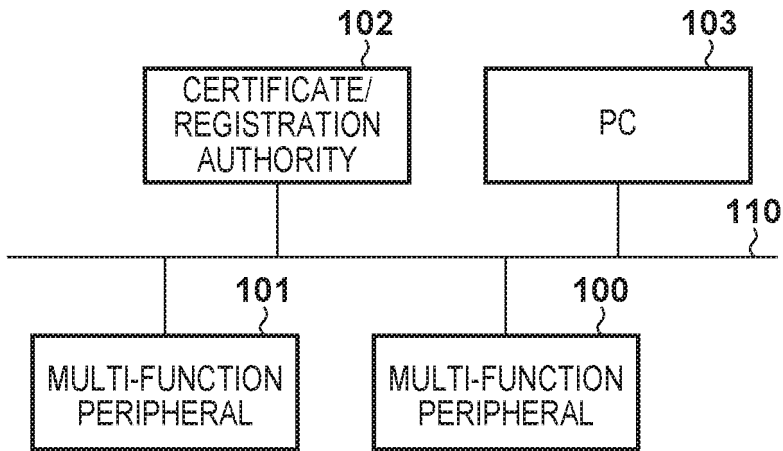


FIG. 2

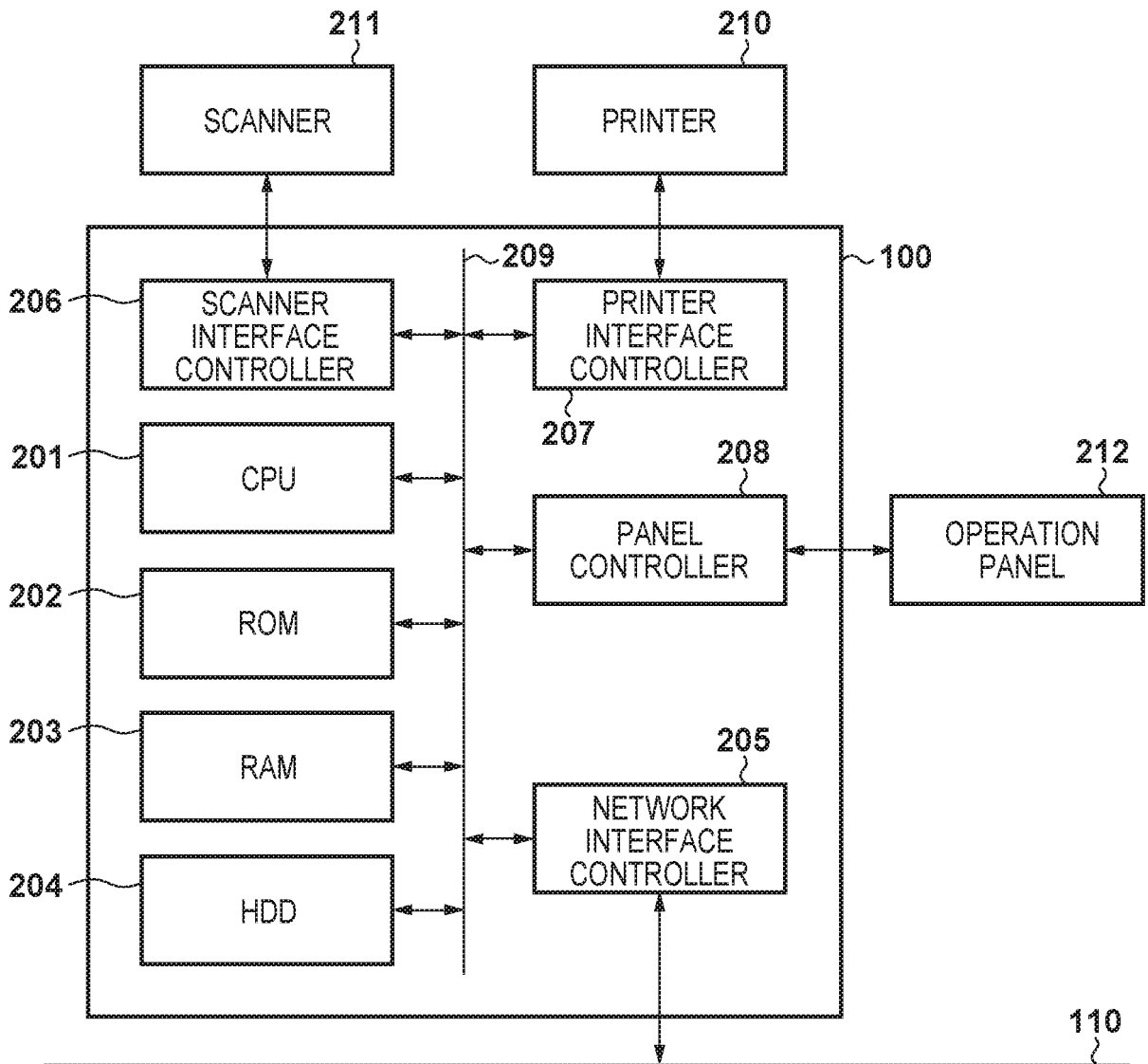


FIG. 3

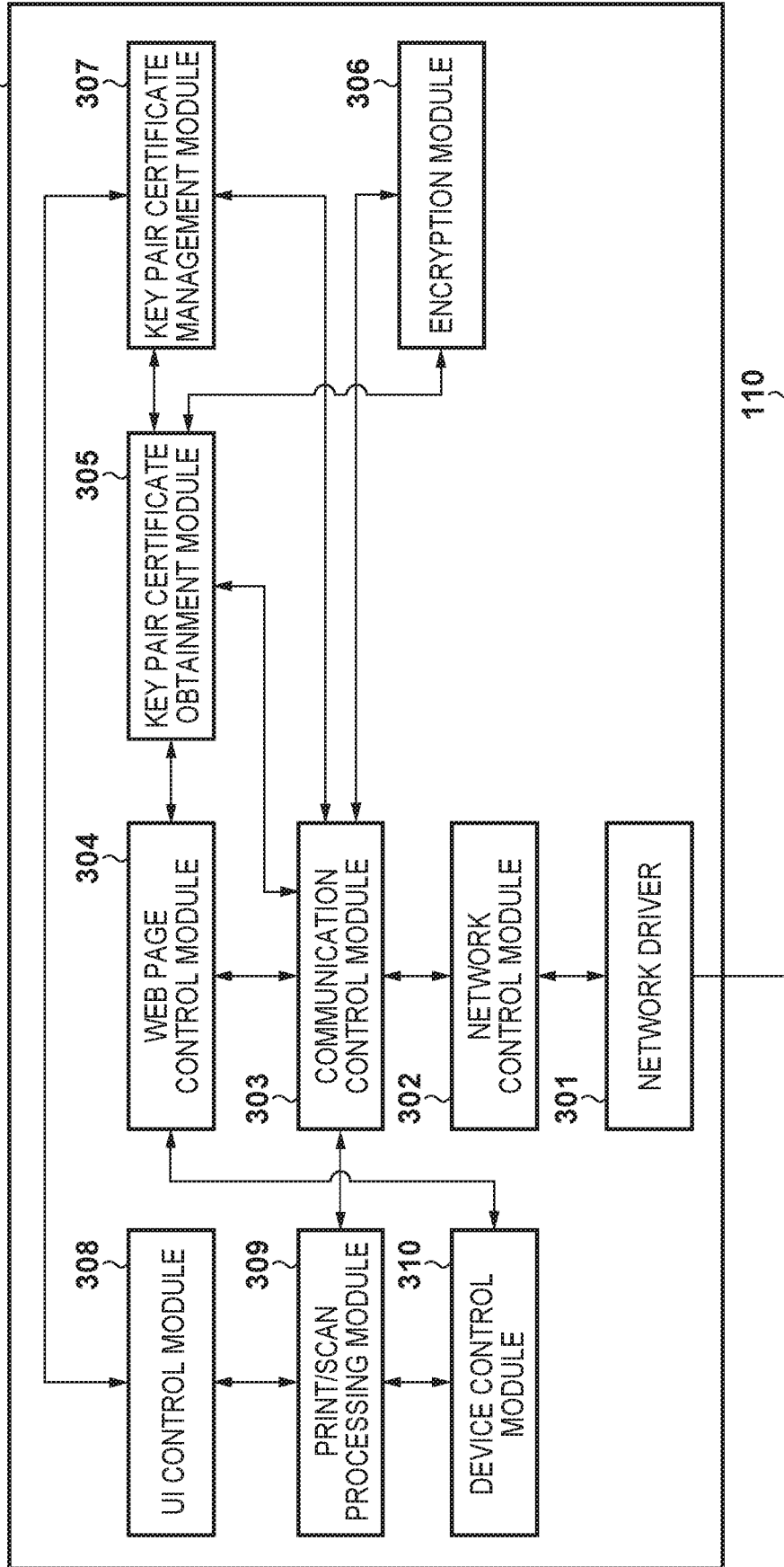


FIG. 4A

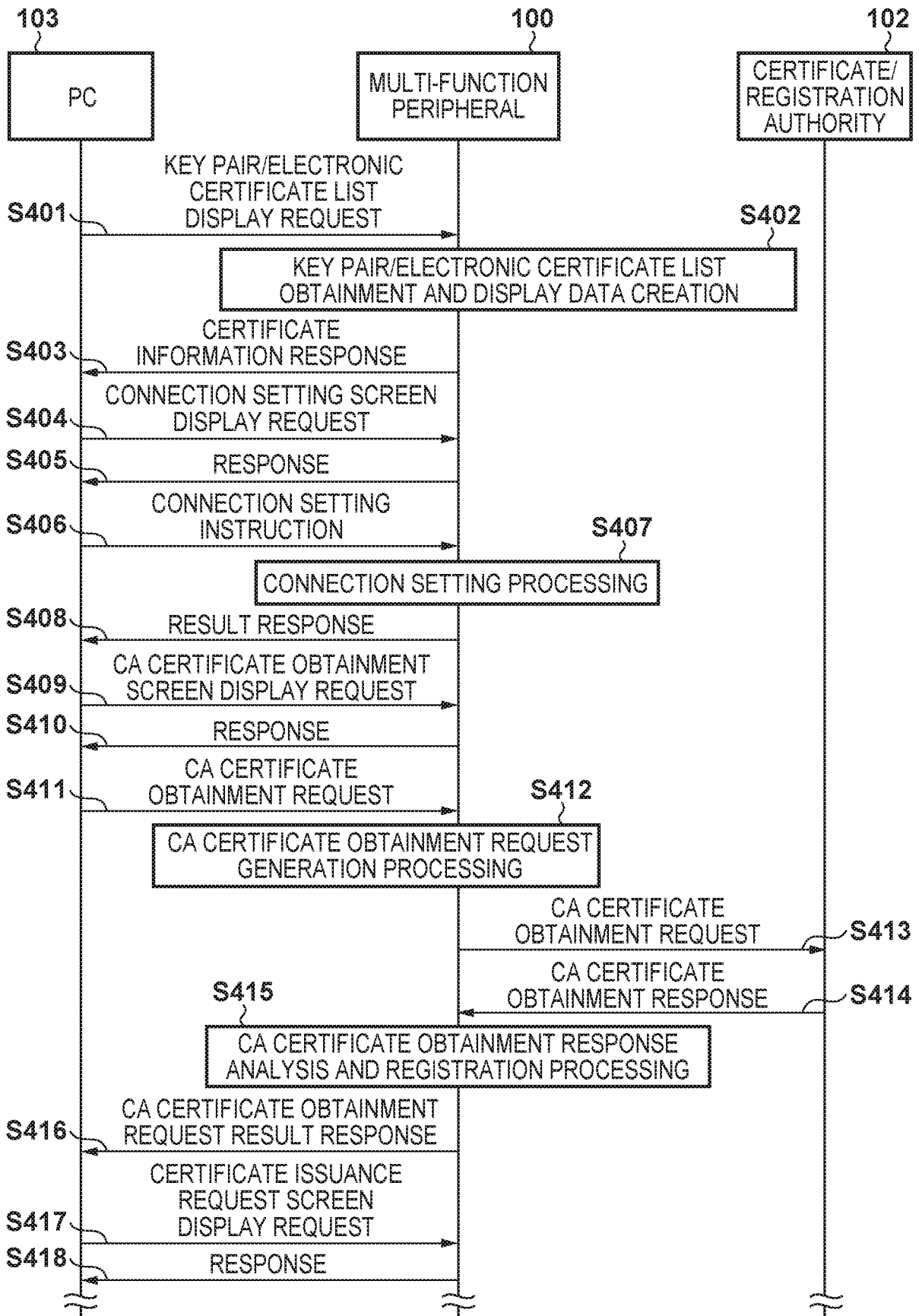


FIG. 4B

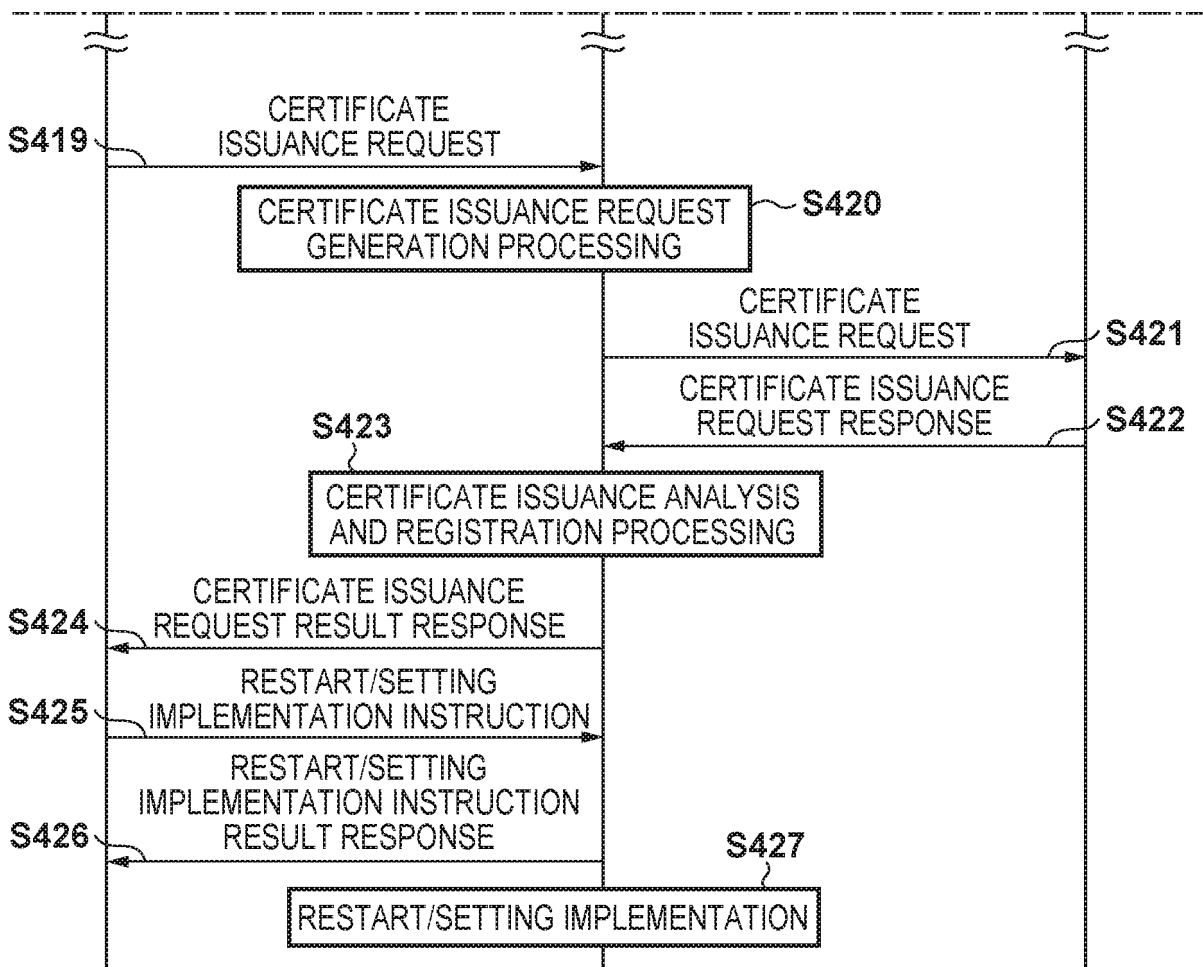


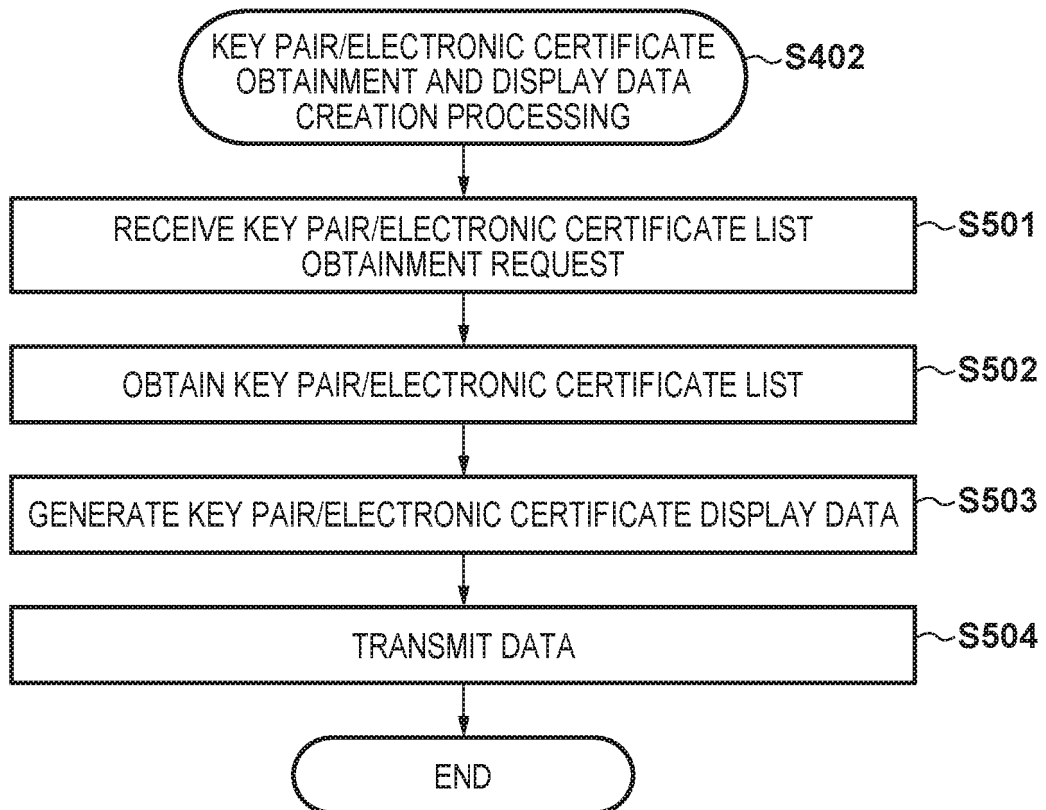
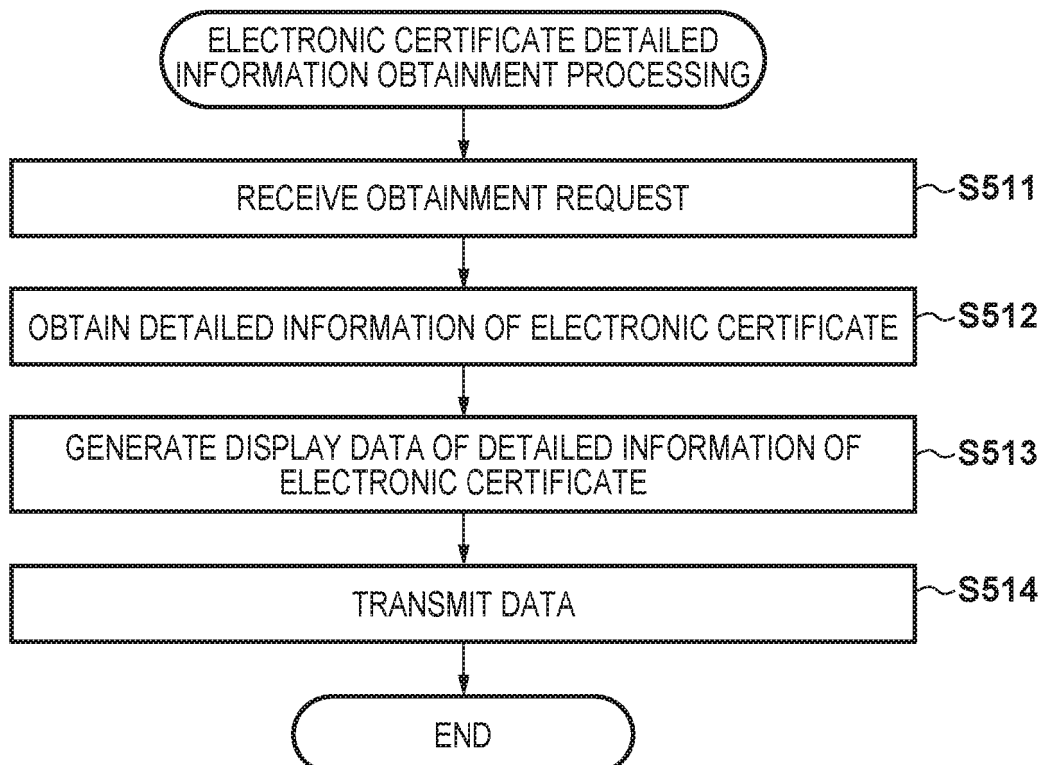
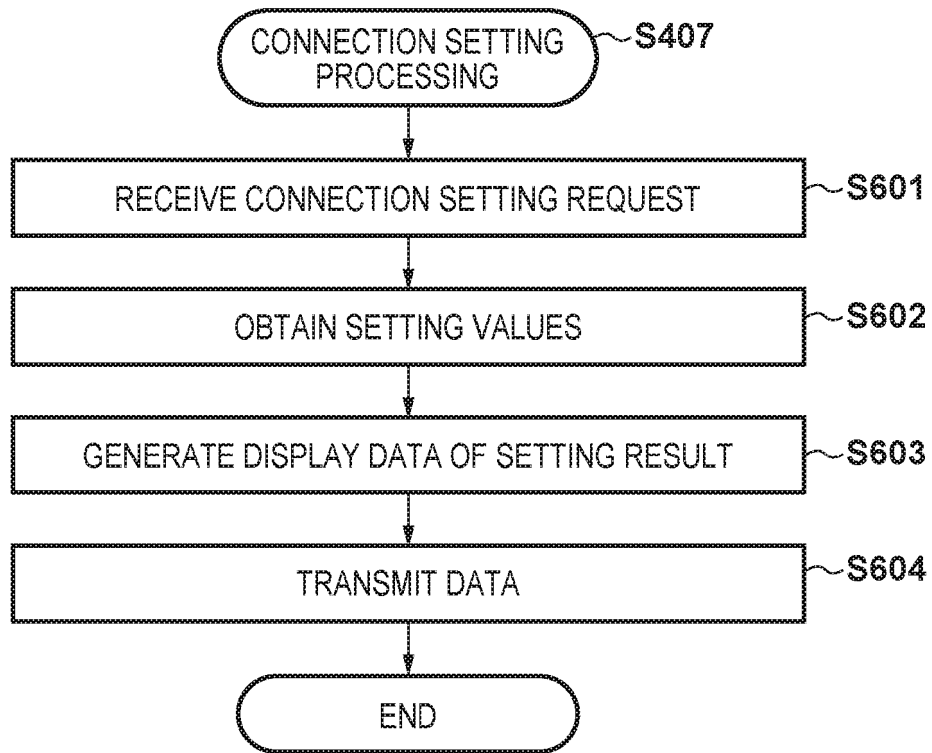
FIG. 5A**FIG. 5B**

FIG. 6



CA CERTIFICATE OBTAINMENT PROCESSING S412~S416 FIG. 7

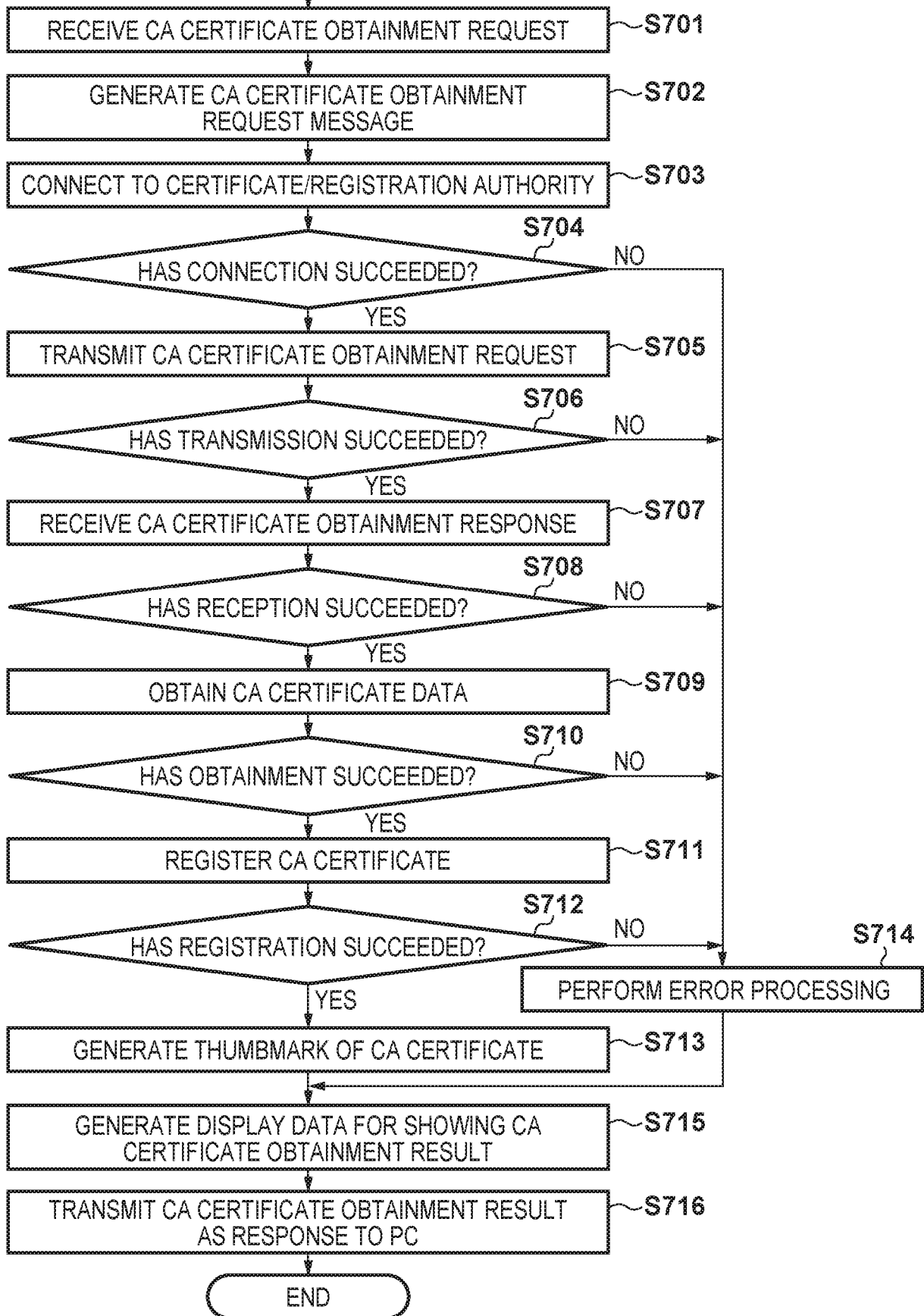


FIG. 8A

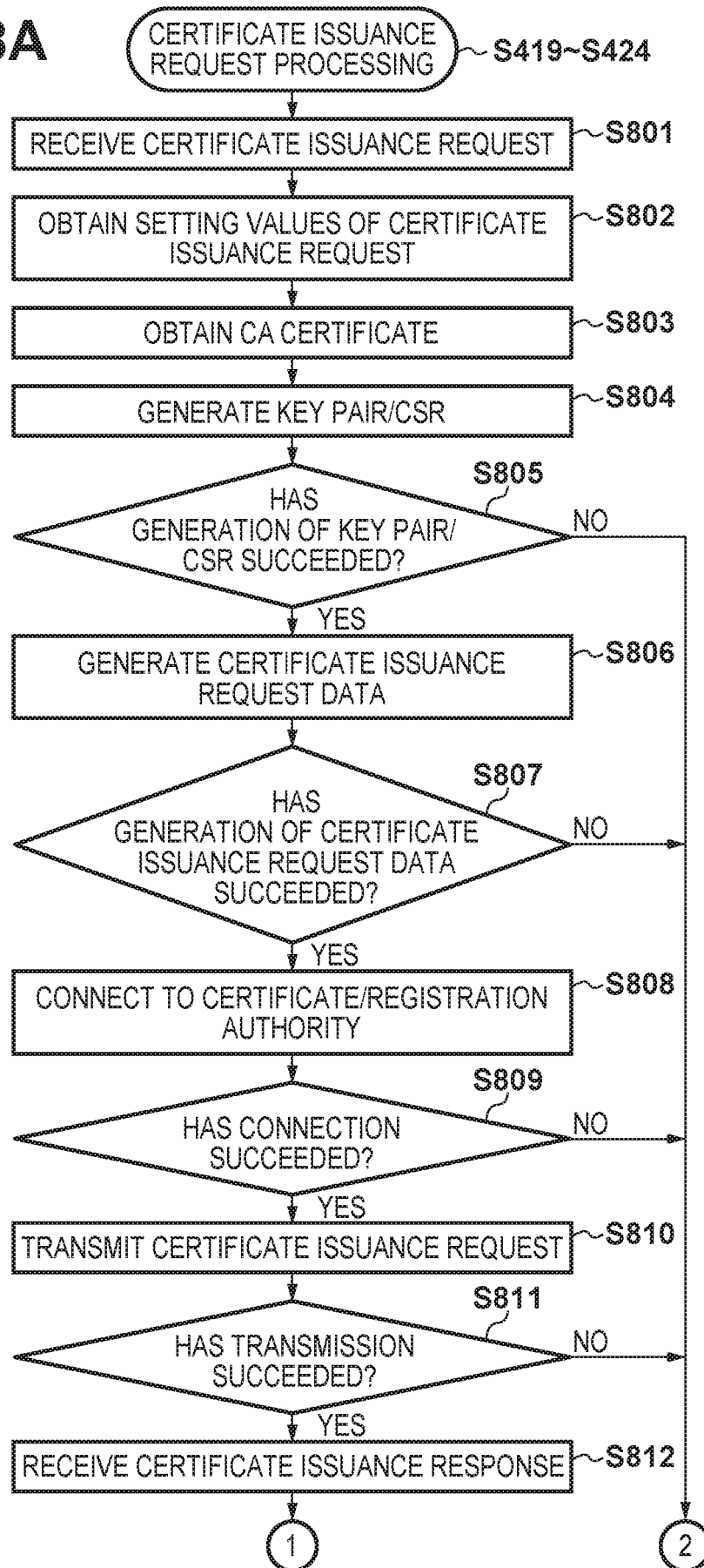


FIG. 8B

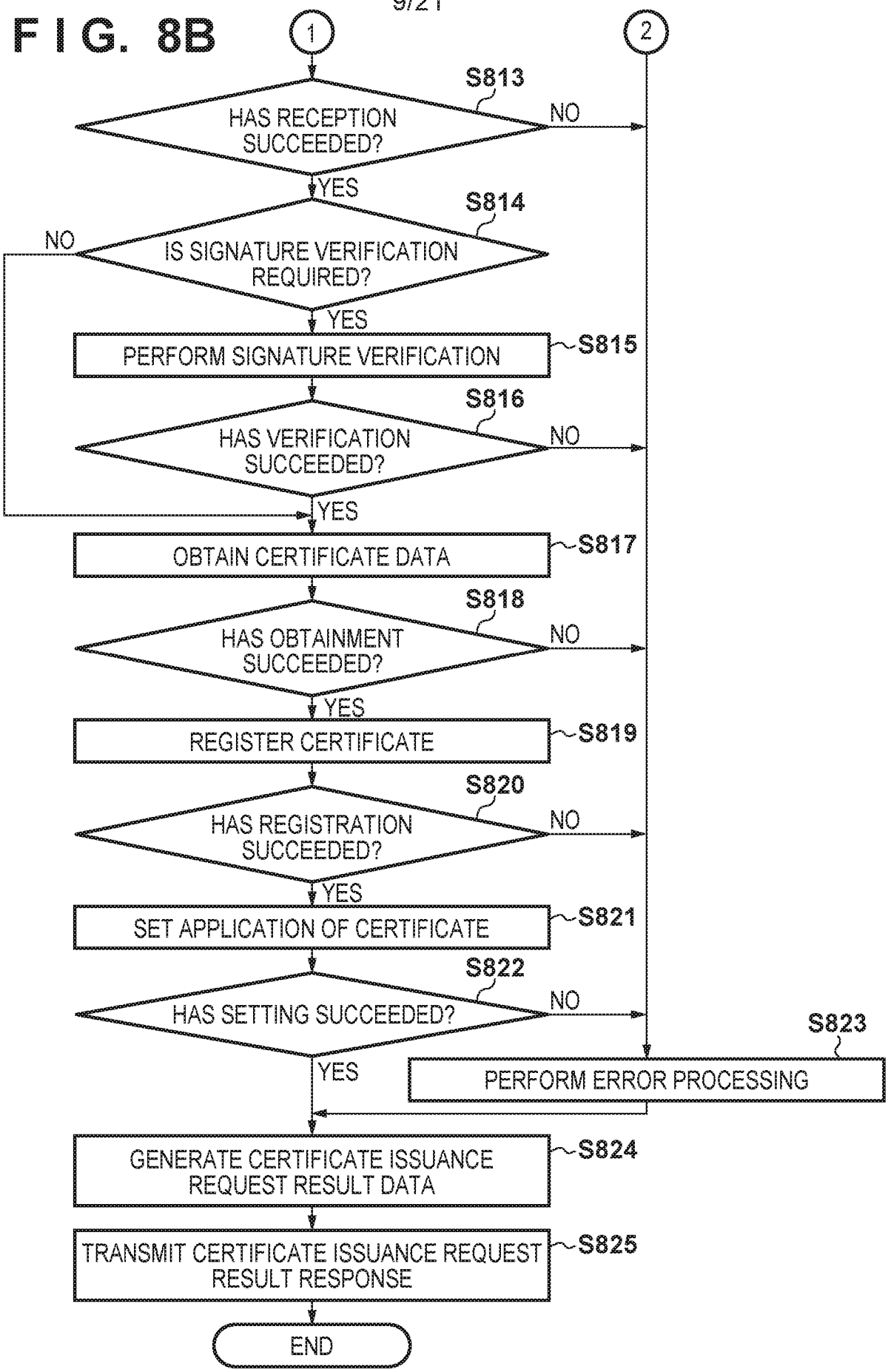


FIG. 9

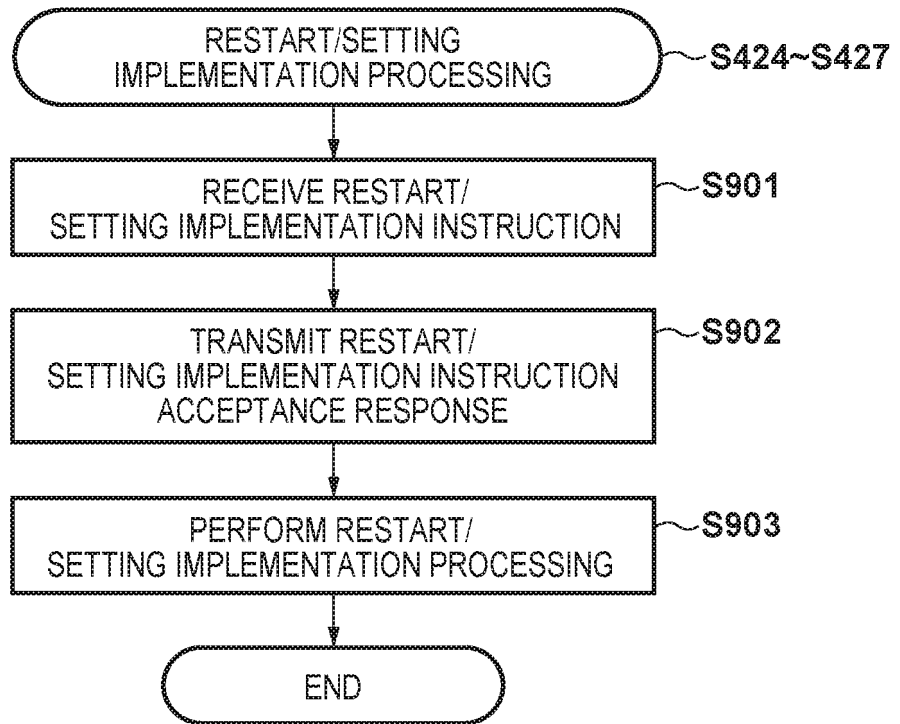


FIG. 10A

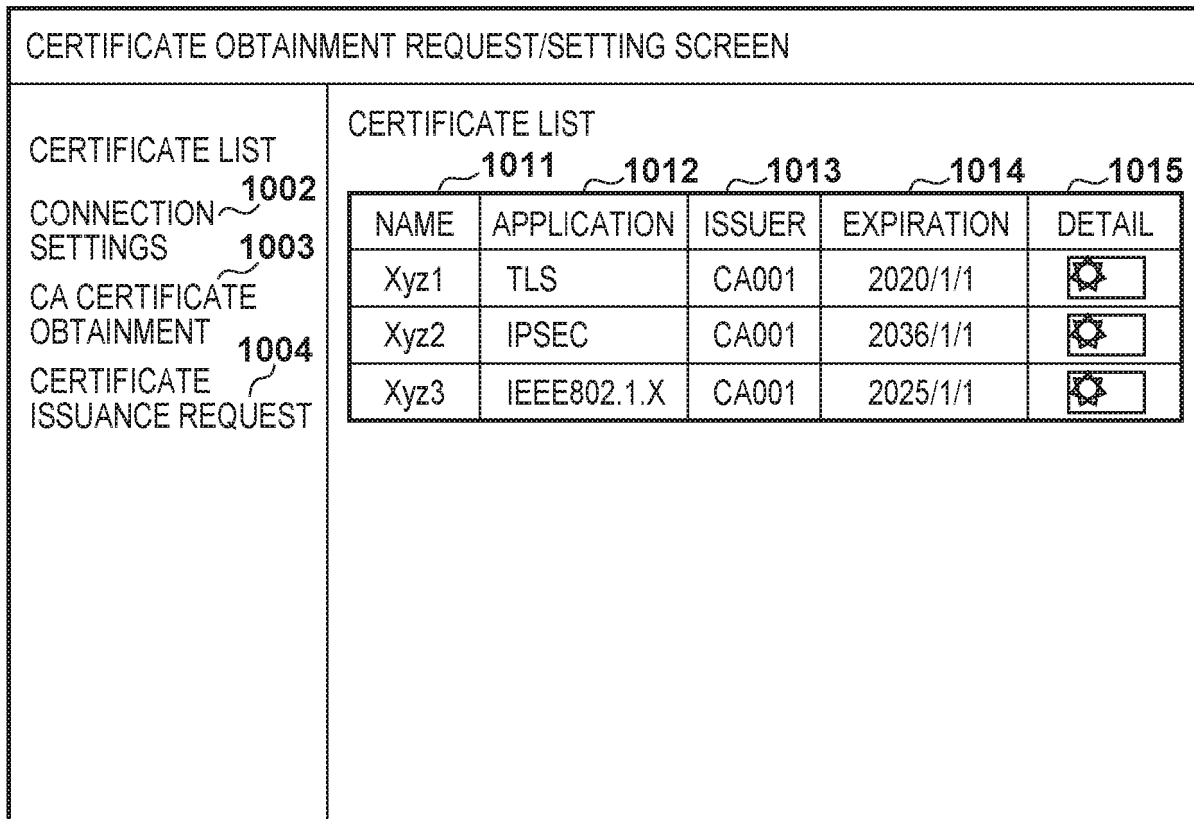


FIG. 10B

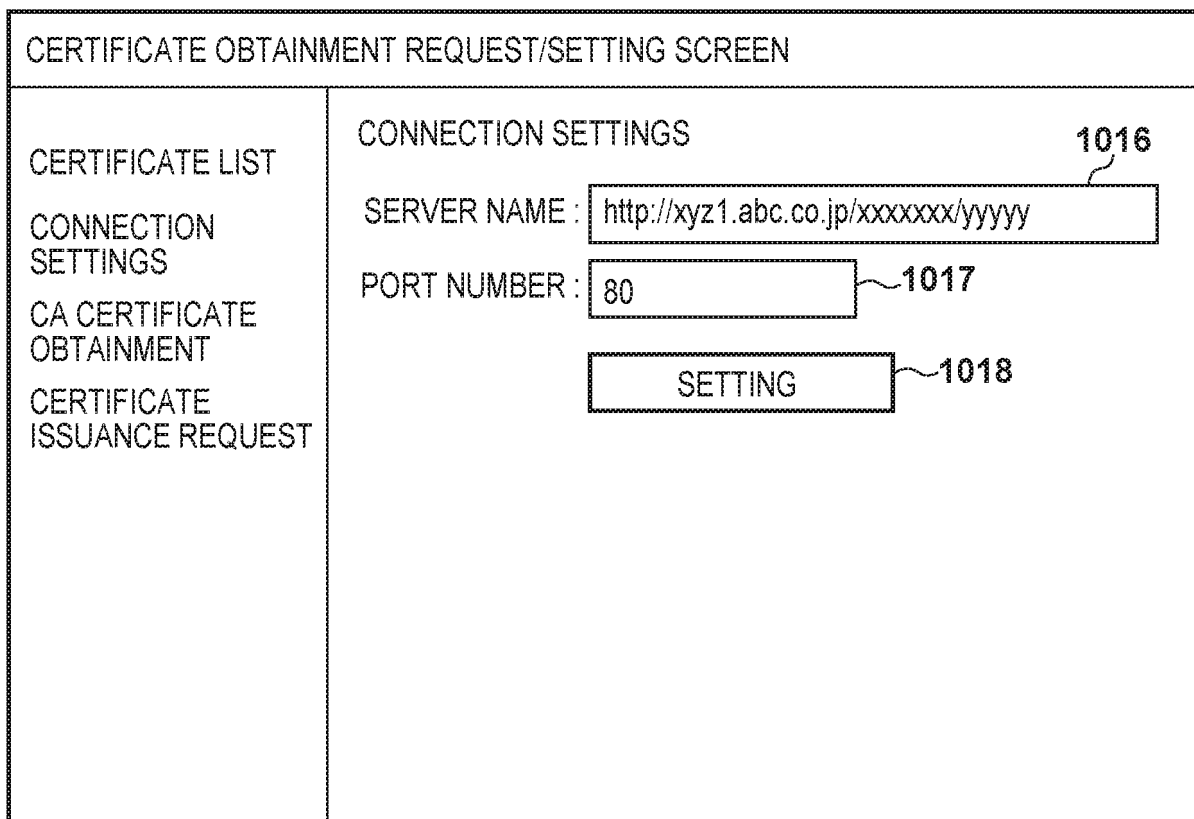


FIG. 11A

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CONNECTION SETTINGS SERVER NAME : <input type="text" value="http://xyz1.abc.co.jp/xxxxxxx/yyyy"/> PORT NUMBER : <input type="text" value="80"/> <input type="button" value="SETTING"/> 1101 SETTINGS HAVE BEEN IMPLEMENTED

FIG. 11B

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CA CERTIFICATE OBTAINMENT CA CERTIFICATE OBTAINMENT <input type="button" value="EXECUTE"/> 1102

FIG. 12A


CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CA CERTIFICATE OBTAINMENT CA CERTIFICATE OBTAINMENT  1201 THE FOLLOWING CA CERTIFICATE HAS BEEN OBTAINED AND REGISTERED AS A TRUSTED CERTIFICATE AUTHORITY THUMBMARK OF CERTIFICATE (SHA1) : OF 02 OF 03 OF 04 OF 05 OF 06 OF 07 OF 08 OF 09 OF 0A OF 0B

FIG. 12B


CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CA CERTIFICATE OBTAINMENT CA CERTIFICATE OBTAINMENT  1202 OBTAINMENT OF CA CERTIFICATE HAS FAILED

FIG. 13A

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CERTIFICATE ISSUANCE REQUEST TRANSMISSION NAME : <input type="text" value="Xyz4"/>
	KEY LENGTH <input type="radio"/> 1024bit <input checked="" type="radio"/> 2048bit <input type="radio"/> 3072bit <input type="radio"/> 4096bit
	INPUT ISSUANCE DESTINATION INFORMATION
	COUNTRY : <input type="text" value="JP"/>
	PREFECTURE : <input type="text"/>
	CITY : <input type="text"/>
	ORGANIZATION : <input type="text" value="ABC"/>
	ORGANIZATION UNIT : <input type="text" value="EV01"/>
	COMMON NAME : <input type="text" value="Device001"/>
	SIGNATURE VERIFICATION <input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
	KEY APPLICATION <input checked="" type="checkbox"/> TLS <input type="checkbox"/> IPSEC <input type="checkbox"/> IEEE802.1X
	PASSWORD : <input type="text" value="ABCDEFG12345"/>
	<input type="button" value="EXECUTE"/>

FIG. 13B

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CERTIFICATE ISSUANCE REQUEST TRANSMISSION
	CERTIFICATE ISSUANCE/OBTAINMENT HAS SUCCEEDED PLEASE CONFIRM THE ISSUED CERTIFICATE ON THE CERTIFICATE LIST PLEASE RESTART TO IMPLEMENT THE SETTINGS
	<input type="button" value="RESTART"/>

FIG. 14A

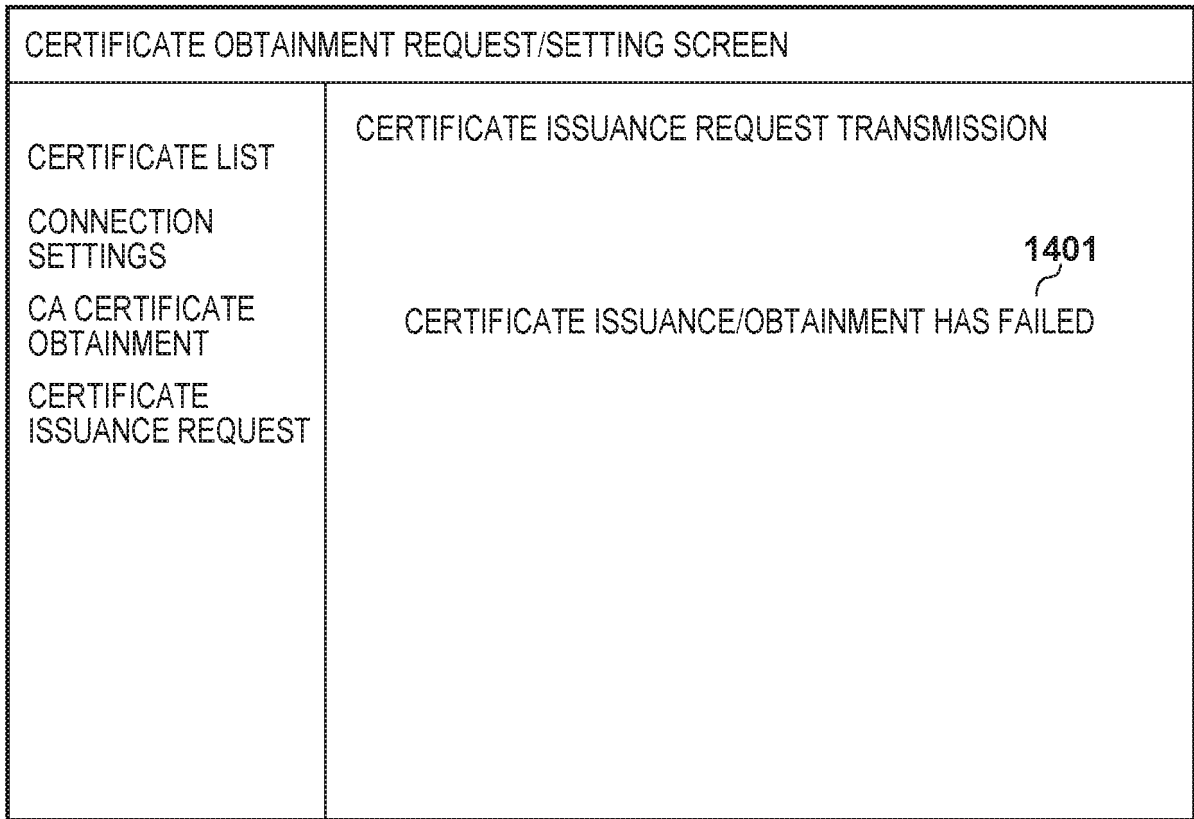


FIG. 14B

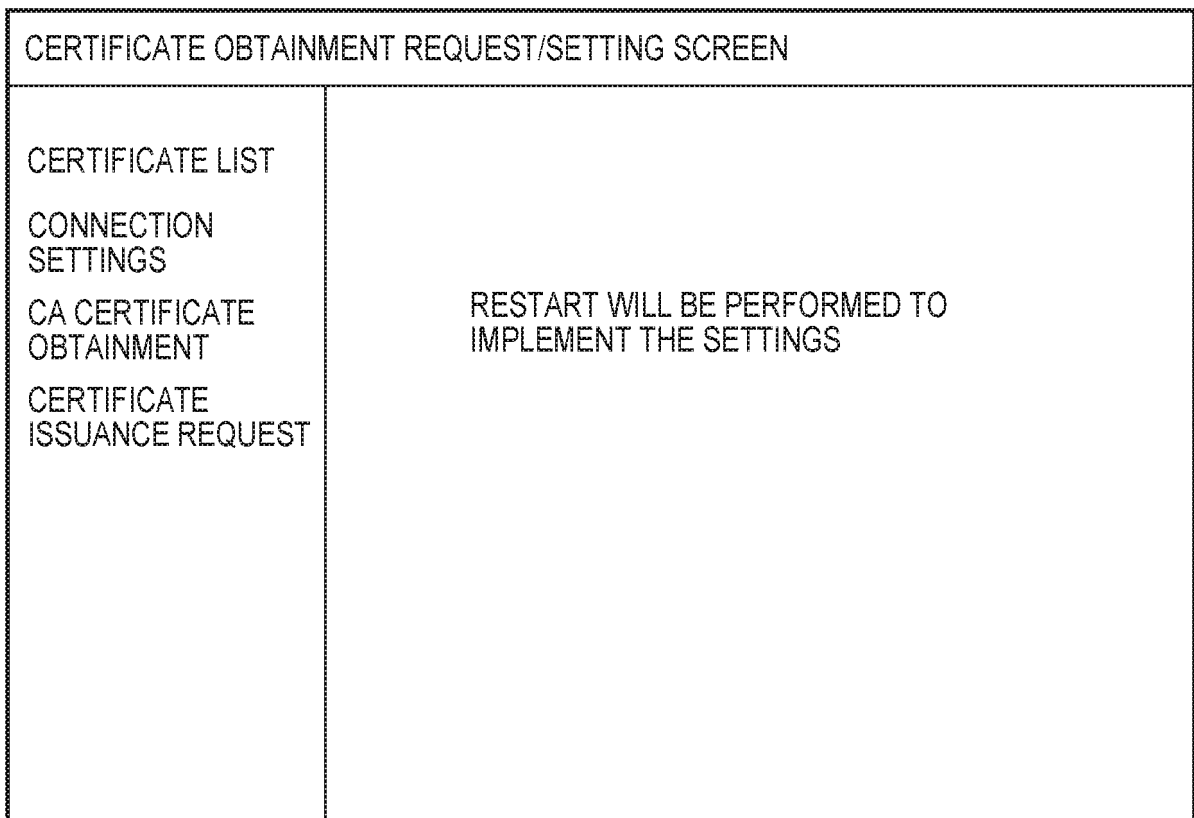


FIG. 15

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN																										
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	CERTIFICATE LIST <table border="1"> <thead> <tr> <th>NAME</th> <th>APPLICATION</th> <th>ISSUER</th> <th>EXPIRATION</th> <th>DETAIL</th> </tr> </thead> <tbody> <tr> <td>XYZ1</td> <td>-</td> <td>CA001</td> <td>2020/1/1</td> <td></td> </tr> <tr> <td>XYZ2</td> <td>IPSEC</td> <td>CA001</td> <td>2036/1/1</td> <td></td> </tr> <tr> <td>XYZ3</td> <td>IEEE802.1X</td> <td>CA001</td> <td>2025/1/1</td> <td></td> </tr> <tr> <td>XYZ4</td> <td>TLS</td> <td>CA001</td> <td>2021/1/1</td> <td></td> </tr> </tbody> </table> <p style="text-align: right;">1501</p>	NAME	APPLICATION	ISSUER	EXPIRATION	DETAIL	XYZ1	-	CA001	2020/1/1		XYZ2	IPSEC	CA001	2036/1/1		XYZ3	IEEE802.1X	CA001	2025/1/1		XYZ4	TLS	CA001	2021/1/1	
NAME	APPLICATION	ISSUER	EXPIRATION	DETAIL																						
XYZ1	-	CA001	2020/1/1																							
XYZ2	IPSEC	CA001	2036/1/1																							
XYZ3	IEEE802.1X	CA001	2025/1/1																							
XYZ4	TLS	CA001	2021/1/1																							

FIG. 16

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST	DETAILS OF CERTIFICATE INFORMATION NAME : XYZ1 APPLICATION : TLS ISSUER : CN=CA01, C=JP START OF VALIDITY PERIOD : 2017/1/1 EXPIRATION OF VALIDITY PERIOD : 2020/1/1 ISSUANCE DESTINATION : CN=Device001, OU=Dev.A, O=ABC, C=JP KEY ALGORITHM : RSA 2048bit SERIAL NUMBER : 01 02 03 04 05 THUMBMARK OF CERTIFICATE (SHA1) : 01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 0B

FIG. 17A

NAME	APPLICATION	ISSUER	START OF VALIDITY PERIOD	EXPIRATION OF VALIDITY PERIOD	ISSUANCE DESTINATION	ALGO-RITHM	KEY LENGTH	SERIAL NUMBER	THUMBMARK
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 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	APPLICATION	ISSUER	START OF VALIDITY PERIOD	EXPIRATION OF VALIDITY PERIOD	ISSUANCE DESTINATION	ALGO-RITHM	KEY LENGTH	SERIAL NUMBER	THUMBMARK
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 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	NONE	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 03 04 04 04 05 04 06 04 07 04 08 04 09 04 0A 04 0B

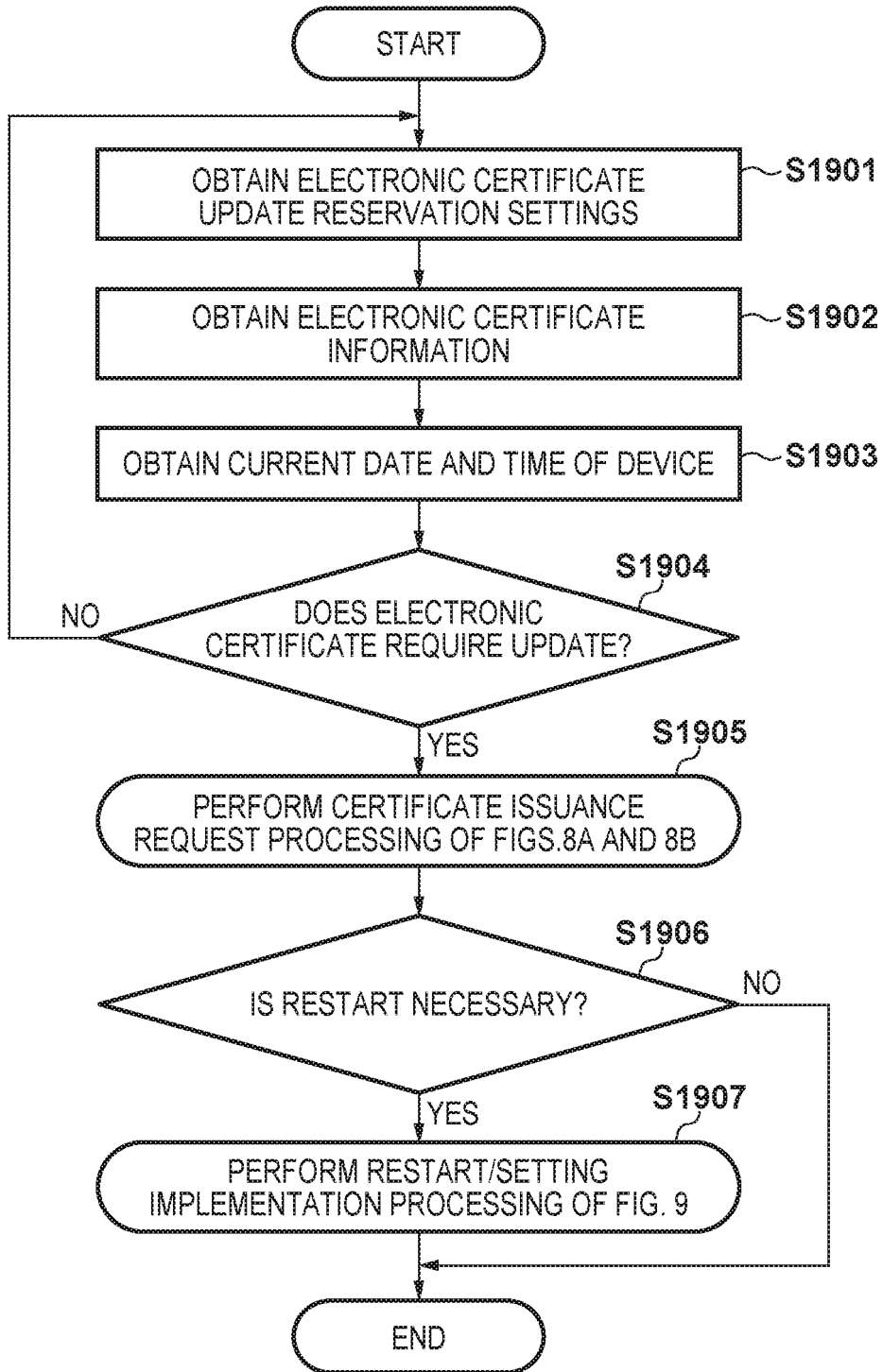
FIG. 17C

NAME	APPLICATION	ISSUER	START OF VALIDITY PERIOD	EXPIRATION OF VALIDITY PERIOD	ISSUANCE DESTINATION	ALGORITHM	KEY LENGTH	SERIAL NUMBER	THUMBMARK
Xyz1	NONE	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 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 03 04 04 04 05 04 06 04 07 04 08 04 09 04 0A 04 0B

FIG. 18

CERTIFICATE OBTAINMENT REQUEST/SETTING SCREEN	
CERTIFICATE LIST CONNECTION SETTINGS CA CERTIFICATE OBTAINMENT CERTIFICATE ISSUANCE REQUEST RESERVATION SETTING	<p>ELECTRONIC CERTIFICATE UPDATE RESERVATION SETTING 1801</p> <p><input type="radio"/> DESIGNATE AN UPDATE DATE</p> <p>OBTAINMENT REQUEST START DATE <input type="text"/> YEAR <input type="text"/> MONTH <input type="text"/> DAY</p> <p>OBTAINMENT REQUEST START TIME <input type="text"/> HOUR <input type="text"/> MINUTE</p> <p>1802</p> <p><input checked="" type="radio"/> UPDATE THE ELECTRONIC CERTIFICATE IN A CASE WHERE A NUMBER OF DAYS BEFORE THE EXPIRY OF THE VALIDITY PERIOD OF THE CURRENTLY USED ELECTRONIC CERTIFICATE IS A PREDETERMINED NUMBER OR LESS</p> <p><input type="text"/> 14 DAYS BEFORE THE EXPIRATION OF THE VALIDITY PERIOD</p> <p>1803</p> <p><input type="radio"/> UPDATE BASED ON A PREDETERMINED CYCLE</p> <p><input type="radio"/> UPDATE AT <input type="text"/> DAY INTERVAL</p> <p><input type="radio"/> UPDATE ON <input type="text"/> DAY OF EVERY MONTH</p> <p><input type="radio"/> UPDATE ON <input type="text"/> MONTH <input type="text"/> DAY OF EVERY YEAR</p>

FIG. 19



INFORMATION PROCESSING APPARATUS, IMAGE FORMING
APPARATUS, SYSTEM, METHOD OF CONTROLLING THE SAME, AND
STORAGE MEDIUM

5 Field of the Invention

[0001] The present invention relates to an
information processing apparatus, an image forming
apparatus, a system, a method of controlling the same,
and a storage medium.

10

BACKGROUND

[0002] When communicating with an external server,
a personal computer (PC) that connects to a network
such as that of an office and a mobile terminal that is
15 owned by an individual uses a public key certificate
(e.g. a digital certificate) to perform a secure
communication and authentication.

[0003] In recent years, a multi-function
peripheral not only simply prints and transmits images,
20 but also has a function of providing a file storage
service to a PC by storing image data in the multi-
function peripheral. Hence, a multi-function
peripheral has come to perform the role of an
information processing apparatus similar to that of
25 other server devices that are present on a network. In
order to maintain a safe and secure office environment
while these information processing apparatuses are used

on a network, communication based on an authentication using an electronic certificate (i.e. a digital certificate) is required. In general, a safer network identification and authentication have been implemented
5 by using the technique based on a public key infrastructure (PKI), which uses such an electronic certificate (see RFC3647: Internet X.509 Public Key Infrastructure Certificate Polity and Certificate Practices Framework).

10 **[0004]** For example, if an information processing apparatus is to be a client, the authenticity of a server can be verified by obtaining a server public key certificate from the server and a Certificate Authority (CA) certificate that was used in issuing the server
15 public key certificate. Also, it is possible for the server to verify the authenticity of the client by providing a client public key certificate of client (e.g. the information processing apparatus) to the server. Additionally, if the information processing
20 apparatus is to act as the server, a server public key certificate of the information processing apparatus can be distributed to a client to be connected so that the client can verify the authenticity of the information processing apparatus as the server. In this manner, an
25 electronic certificate has been used as an important tool for information processing apparatuses to perform an authentication/verification and an identification in

a network communication/environment. For example, SSL, TLS, IEEE802.1X, and IPSEC are some of the communication protocols that are used in such an electronic certificate based secure communication.

5 **[0005]** Conventionally, since an electronic certificate needs to be stored/held in an information processing apparatus, an electronic certificate that has been issued by a certificate authority is manually stored in a storage of the information processing
10 apparatus with a user of the information processing apparatus manually performing the storing. This storage method is performed by downloading the electronic certificate from the certificate authority that issues the electronic certificate, copying the
15 electronic certificate from an external storage such as a USB memory, or copying the electronic certificate received via email into a predetermined folder in the storage.

20 **[0006]** Depending on the actual implementation of the communication, a separate electronic certificate may be used for each information processing apparatus. For example, in general, when IEEE802.1X or the like is applied for the communication, an electronic certificate is individually stored for each information
25 processing apparatus for performing a client authentication. Also, an electronic certificate has a validity period (i.e. a period of time or a date/time

after which the electronic certificate is no longer valid/not useable for authentication/verification), and a communication using the electronic certificate is disabled when the validity period expires. Hence, an electronic certificate stored in a device (such as the information processing apparatus) needs to be updated when the validity period expires or (preferably immediately) before the expiration. Furthermore, when an electronic certificate is to be used, it is necessary to manually set each electronic certificate that is going to be used in correspondence with each communication application, such as TLS or IEEE802.1X, which is going to be used by each information processing apparatus.

15 [0007] However, in a case in which there are many information processing apparatuses that handle/need electronic certificates, if a user has to manually add, update, and set each electronic certificate for each of these information processing apparatuses, this can place a heavy workload/burden on the user and can take too much time.

SUMMARY OF THE INVENTION

25 [0008] An aspect of the present invention is to eliminate, or at least reduce disadvantageous effect arising from, the above-mentioned problem with the conventional technology.

[0009] A feature of the present invention is to provide a technique/mechanism to easily add and update an electronic certificate in an information processing apparatus.

5 [0010] According to the present invention there is provided an apparatus, a system, a method, and a computer readable storage medium as set forth in the appended claims. Other features of the invention will be apparent from the dependent claims, and the
10 description which follows.

[0011] According to aspects of the present invention, there are provided an apparatus, a system, a method or a computer readable storage medium as set out by the accompanying independent claims.

15 [0012] Further features, aspects, and advantages of the present invention will become apparent from the following description of embodiments with reference to the attached drawings. Each of the embodiments of the present invention described below can be implemented
20 solely or as a combination of a plurality of the embodiments. Also, features from different embodiments can be combined where necessary or where the combination of elements or features from individual embodiments in a single embodiment is beneficial.

25 [0013] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention

and, together with the description, serve to explain the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

5 [0014] Fig. 1 is a block diagram illustrating a network arrangement or a system according to a first embodiment of the present invention;

[0015] Fig. 2 is a block diagram illustrating a hardware arrangement of a multi-function peripheral
10 according to the first embodiment;

[0016] Fig. 3 is a block diagram illustrating software modules to be included in a program running on the multi-function peripheral according to the first embodiment;

15 [0017] Figs. 4A and 4B are sequence charts illustrating an overall process sequence to be run on a network arrangement or a system according to the first embodiment;

[0018] Fig. 5A is a flowchart illustrating a key
20 pair/electronic certificate list obtainment and display data creation processing in step S402 of Fig. 4A by the multi-function peripheral according to the first embodiment;

[0019] Fig. 5B is a flowchart illustrating
25 processing performed when a detailed information display request transmitted from a PC is received by the multi-function peripheral according to the first

embodiment;

[0020] Fig. 6 is a flowchart illustrating a connection setup process for establishing a connection with a certificate/registration authority in step S407 of Fig. 4A performed by the multi-function peripheral according to the first embodiment;

[0021] Fig. 7 is a flowchart illustrating a Certificate Authority (CA) certificate obtainment/registration process in step S412 to step S416 of Fig. 4A performed by the multi-function peripheral according to the first embodiment;

[0022] Figs. 8A and 8B are flowcharts illustrating a certificate issuance request/obtainment process in step S419 to step S424 of Fig. 4B performed by the multi-function peripheral according to the first embodiment;

[0023] Fig. 9 is a flowchart illustrating processing related to a restart of the multi-function peripheral in step S424 from step S427 of Fig. 4B performed by the multi-function peripheral according to the first embodiment;

[0024] Figs. 10A-10B, 11A-11B, 12A-12B, 13A-13B, 14A-14B, and 15 depict screen views showing examples of a web page screen of a Remote User Interface (RUI) which is to be displayed on a PC according to the first embodiment;

[0025] Fig. 16 depicts a screen view showing an

example of detailed information of the electronic certificate which is to be displayed on the PC according to the first embodiment;

5 [0026] Figs. 17A to 17C depict conceptual views of a key pair/electronic certificate detailed information database managed by a key pair certificate management module of the multi-function peripheral according to the first embodiment;

10 [0027] Fig. 18 depicts a view illustrating an example of an electronic certificate update reservation setting screen provided by a multi-function peripheral according to a second embodiment; and

15 [0028] Fig. 19 is a flowchart illustrating processing performed when an electronic certificate automatic update function is executed/performed based on the electronic certificate update reservation setting set on the multi-function peripheral according to the second embodiment.

20 DESCRIPTION OF THE EMBODIMENTS

[0029] Embodiments of the present invention will be described hereinafter in detail, with reference to the accompanying drawings. It is to be understood that the following embodiments are not intended to limit the 25 claims of the present invention, and that not all of the combinations of the aspects that are described according to the following embodiments are necessarily

required with respect to the means to solve the problems according to the present invention. Note that as an example of an information processing apparatus that uses and manages an electronic certificate
5 according the embodiments, a multi-function peripheral (a digital multi-function peripheral/MFP) will be described. However, the present invention is not limited to the multi-function peripheral, and the present invention is applicable to any device or a
10 component thereof as long as it is an information processing apparatus in which an electronic certificate can be used or managed.

[0030] [First Embodiment]

Fig. 1 is a block diagram for explaining a
15 network arrangement (or a system) according to the first embodiment of the present invention.

[0031] A multi-function peripheral 100 having a print function can exchange print data, scanned image data, device management information, and the like with
20 another information processing apparatus via a network 110. The multi-function peripheral 100 is capable of performing an encrypted communication using communication/cryptographic protocols such as Transport Layer Security (TLS), Internet Protocol Security
25 (IPSEC), and IEEE802.1X and holds (e.g. stores or manages) a public key pair and an electronic certificate (i.e. a digital certificate) that are used

for performing these encryption processes. Here, the multi-function peripheral 100 may be an example of an image forming apparatus. It is understood that such an image forming apparatus is not limited to the multi-
5 function peripheral and may be an apparatus that functions solely as a facsimile apparatus, a printer, or a copy machine or may be an apparatus that functions as any combination of these single function apparatuses. Another multi-function peripheral 101 is
10 also connected to the network 110, and this second multi-function peripheral 101 may have the same functions as those of the multi-function peripheral 100, or share at least some of its functions. Although only the multi-function peripheral 100 will be mainly
15 described hereinafter, it is understood that the exchange/communication of electronic certificates may be performed among/for a plurality of multi-function peripherals.

[0032] A certificate/registration authority 102
20 has a certificate authority (CA) function of issuing an electronic certificate and a registration authority (RA) function of accepting (in some cases, including verification/authentication) an electronic certificate issuance request and performing a registration process
25 based on the accepted request. That is, this certificate/registration authority 102 is, for example, a server apparatus (which is an example of an

information processing apparatus) that performs a function of distributing a CA certificate (e.g. for authenticating a CA electronic signature on a server certificate) and issuing/registering an electronic certificate (e.g. for establishing a secure communication) via the network 110. In the first embodiment, assume that SCEP (Simple Certificate Enrollment Protocol) is used as the communication protocol of the network 110. However, it is understood that various other types of protocols for issuing/managing an electronic certificate may also be used with the network arrangement of the first embodiment as long as they are able to provide corresponding functions. An information processing apparatus such as the multi-function peripheral 100 uses this SCEP to communicate with the certificate/registration authority 102 via the network 110 to transmit an electronic certificate issuance request and to obtain the issued electronic certificate. The multi-function peripheral 100 according to the first embodiment has a Web server function and can publish, on the network 110, a Web-page-format remote user interface (RUI) function that can be used to execute/perform processing for the electronic certificate issuance request and obtainment (acquisition).

[0033] When an electronic certificate issuance

request is received from an information processing apparatus via the network 110, the certificate/registration authority 102 performs an electronic certificate issuance and registration processing based on the received issuance request and transmits the issued electronic certificate as a response to the issuance request. Note that although the function of a CA and the function of an RA are implemented by the same server apparatus in this first embodiment, the present invention is not limited to this. It is also possible to adopt an arrangement in which the CA and the RA are implemented as separate server apparatuses, for example a CA server and a separate RA server. Additionally, although the first embodiment uses SCEP as the protocol for making an electronic certificate issuance request and for obtaining the issued electronic certificate, the present invention is not limited to this as long as a protocol that has the same or compatible functions is adopted. For example, it is possible to use a protocol such as CMP (Certificate Management Protocol) or EST (Enrollment over Secure Transport).

[0034] A PC 103 is a personal computer. The PC 103 has a Web browser function. This makes it possible (i.e. enables a user or an information processing apparatus) to browse and use HTML documents and Websites which have been made public by an information

processing apparatus that is connected to the network 110. It is understood that although the PC 103 is shown/described herein, any device/terminal capable of providing a web browser function, or displaying information and receive a user input (e.g. a tablet, a mobile phone, a wearable technology based device, inter alias), may be used instead as long as it is communicable with the information processing apparatus on the network 110.

10 [0035] The outline of the electronic certificate obtainment and an update process according to the first embodiment will be described next.

[0036] An administrator of the multi-function peripheral 100 uses a Web browser installed on the PC 15 103 to connect to a Web page for an electronic certificate issuance request and obtainment, which is made accessible (e.g. by making it public) by the multi-function peripheral 100. The administrator uses the webpage to set settings and instructions for 20 executing the processes for the electronic certificate issuance request and obtainment (i.e. the electronic certificate issuance request and obtainment/acquisition processes). The multi-function peripheral 100 makes (i.e. generates), in accordance with the settings and 25 the instructions (e.g. information/contents as instructed via the webpage) set by the administrator, an obtainment request (an acquisition request) for a CA

certificate and an electronic certificate issuance request to the certificate/registration authority 102 by SCEP. The multi-function peripheral 100 also obtains the electronic certificate, which is issued by the certificate/registration authority 102 as it is included in the response to the electronic certificate issuance request. The multi-function peripheral 100 then performs a setting operation (i.e. a setup or initialization operation) to use the obtained electronic certificate in the multi-function peripheral 100.

[0037] The hardware arrangement of the multi-function peripheral 100 according to the first embodiment will be described next.

[0038] Fig. 2 is a block diagram for explaining the hardware arrangement of the multi-function peripheral 100 according to the first embodiment.

[0039] A CPU 201 executes a software program of the multi-function peripheral 100 to control/operate the overall apparatus. A ROM 202 is a read-only memory and stores boot programs, fixed parameters, and the like for the operation of the multi-function peripheral 100. A RAM 203 is a random access memory and is used to store programs and temporary data when the CPU 201 is to control/operate the multi-function peripheral 100. An HDD 204 is a hard disk drive and stores system software, applications, and various other kinds of

data. The CPU 201 controls the operation of the multi-function peripheral 100 by executing a boot program stored in the ROM 202, deploying a program stored in the HDD 204 to the RAM 203, and executing the deployed
5 program. A network interface controller 205 controls the data exchange between the network 110 and the multi-function peripheral 100. An input interface controller (e.g. a scanner interface controller 206) controls an image data acquisition (e.g. a scanning or
10 reading of a document) performed by an input device such as a scanner 211. An output interface controller (e.g. a printer interface controller 207) controls a data output (e.g. a printing process) performed by an output such as the printer 210. A display controller
15 (e.g. a panel controller 208) controls a display device and an input device (e.g. a touch-panel-type operation panel 212) to control displaying of various kinds of information and receiving/processing of instructions input by a user. The CPU 201, the ROM 202, the RAM
20 203, the HDD 204, the network interface controller 205, the scanner interface controller 206, the printer interface controller 207, and the panel controller 208 are communicable with each other, for example they are connected to each other by a bus 209. Control signals
25 from the CPU 201 and data signals between different components of the apparatus are exchanged/communicated via the bus 209.

[0040] Fig. 3 is a block diagram for explaining software modules included in (e.g. functional components of) programs to be executed or run on the multi-function peripheral 100 according to the first embodiment. Note that the software modules shown in Fig. 3 are implemented by the CPU 201 deploying a program in the RAM 203 and executing the deployed program, for example.

[0041] A network driver 301 controls the network interface controller 205 connected to the network 110 and exchanges data (i.e. communicates) with the outside via the network 110. A network control module 302 performs data exchange by controlling communication in the transport layer and the lower layers in a network communication protocol such as TCP/IP. A communication control module 303 is a module for controlling (and implementing) a plurality of communication protocols supported by the multi-function peripheral 100. In the electronic certificate obtainment and update processes according to the first embodiment, the communication control module 303 makes (e.g. generates and transmits) an HTTP protocol communication request, generates response data, performs an analysis, controls the exchange of data, and executes processes for a communication with the certificate/registration authority 102 and/or the PC 103. The communication control module 303 is also capable of performing (e.g.

by executing appropriate processes/programs) an encrypted communication using TLS, IPSEC, and IEEE802.1X, if supported by the multi-function peripheral 100.

5 **[0042]** A web page control module 304 is a module that performs HTML data generation and communication control to display a Web page capable of instructing/executing (e.g. by executing an appropriate program) the electronic certificate issuance request
10 and obtainment processes. The web page control module 304 executes/performs processing for a Web page display request, an electronic certificate issuance request, and an instruction for executing/enabling the obtainment of the issued electronic certificate by
15 transmitting/receiving them with the communication control module 303 via the network driver 301. The web page control module 304 transmits, as a response to a request made from (using an input made on) the Web browser, the HTML data of a predetermined Web page
20 stored in the RAM 203 and the HDD 204 or the HTML data generated in accordance with the content of a display request (e.g. a request for displaying detailed information of an electronic certificate).

[0043] A key pair certificate obtainment module
25 305 is a module for executing the electronic certificate obtainment process based on an instruction from the web page control module 304. The key pair

certificate obtainment module 305 is a module that performs a communication control by SCEP, an encrypted data generation and an analysis processing necessary for a communication using SCEP such as PKCS#7 and
5 PKCS#10, and storage and application setting (e.g. setup or initialization) processing of the obtained electronic certificate. An encryption module 306 is a module that executes various kinds of encryption processes such as data encryption and decryption
10 processes, generation and verification of an electronic signature, and hash value generation. In the electronic certificate obtainment and update processing according to the first embodiment, the encryption module 306 executes encryption processes necessary for
15 the generation and analysis of SCEP request/response data. A key pair certificate management module 307 is a module that manages public key pairs and electronic certificates held/stored in the multi-function peripheral 100. For example, the key pair certificate
20 management module 307 stores the public key pair and the data of each electronic certificate in the RAM 203 and/or the HDD 204 together with various kinds of setting values. Although processes for detailed information display, generation, and deletion of the
25 public key pair and the electronic certificate are not shown in Fig.3, it is possible to execute the processes based on user instructions (e.g. received via the

operation panel 212). A UI control module 308 executes/performs a control of the operation panel 212 and the panel controller 208. Note that according to this embodiment even in the case of an encrypted communication processes such as TLS, IPSEC, IEEE802.1X being executed by the communication control module 303, the encryption processing itself is performed in the encryption module 306, and the public key pair and electronic certificate data which are to be used will be obtained from the key pair certificate management module 307. However, it is understood that other arrangements for the encryption processes, and the publish key pair and electronic certificate data are also possible as long as functionally equivalent or compatible features are provided by these arrangements.

[0044] An output/input processing module (e.g. a print/scan processing module 309) is a module for controlling the execution of output/input functions such as a data output function (e.g. printing by the printer 210) and a data input function (e.g. document reading/scanning by the scanner 211). A device control module 310 is a module for controlling (e.g. centrally) the multi-function peripheral 100 by generating control commands and control data for the operation of the multi-function peripheral 100. Note that the encryption module 306 according to the first embodiment has access to the power supply to the multi-function

peripheral 100 so that, if needed, it can execute a restart processing of the multi-function peripheral 100 based on an instruction from the web page control module 304.

5 **[0045]** Figs. 4A and 4B are sequence charts for explaining a sequence process steps involved in an overall processing performed in a network arrangement or a system according to the first embodiment. The sequence starts from an initial setup/initialization of settings related to an issuance request for an
10 electronic certificate, displaying information on the electronic certificate, the issuance request and reception of the electronic certificate, and then moves on to an enabling use of the electronic certificate a
15 restart of the multi-function peripheral.

[0046] This sequence is started in response to a key pair and electronic certificate list display instruction input by a user. Although an example of the processes that are performed for one multi-function
20 peripheral 100 is described in this embodiment, the same processes may be performed by a plurality of multi-function peripherals 100 and 101 in response to one start instruction. For example, a request may be transmitted from the PC 103 to each of the multi-
25 function peripherals 100 and 101, and the processes shown in the following flowcharts of Figs. 5A to Fig. 9 may be executed in each multi-function peripheral. In

such a case, the steps in which a certificate is obtained, displayed, and confirmed in each of the multi-function peripherals 100 and 101 may be skipped. Also, a certificate with an expired validity period may
5 be automatically detected by each multi-function peripheral, the bibliographic information (a certificate ID and the validity period) of the expired certificate may be transmitted to the PC 103, and the PC 103 may cause the plurality of multi-function
10 peripherals to automatically execute the update process of the certificate which has a validity period that is about to expire or has already expired. This aforementioned operation is a so-called silent installation.

15 **[0047]** First, in step S401, upon accepting a connection from (i.e. establishing a communication channel with) the PC 103, the multi-function peripheral 100 receives, from the PC 103, a request to display the key pair/electronic certificate list held by the multi-
20 function peripheral 100. In the first embodiment, assume that the administrator of the multi-function peripheral 100 will use a Web browser installed on the PC 103 to connect to a Web-page-format RUI, which is used to make an issuance request and to obtain an
25 electronic certificate published by the multi-function peripheral 100, and perform instruction related operations (e.g. input an instruction for an operation

to be performed on the multi-function peripheral 100 or 101). This RUI is an acronym of Remote User Interface and is a technique that allows a user to use the Web browser of the PC 103 to remotely make a request for operation screen data of the multi-function peripheral 100 or 101 to display the operation screen on the PC 103. As an example, it is possible to implement the screen using HTML and servlet.

[0048] Next, in step S402, the multi-function peripheral 100 obtains data for displaying the key pair/electronic certificate list held in the multi-function peripheral 100 and executes a Web page screen generation processing to display the obtained data.

[0049] Fig. 5A is a flowchart for describing processes involved in a key pair/electronic certificate list obtainment and display data creation/generation in step S402 of Fig. 4A. Note that this processing is implemented by the CPU 201 executing a program deployed in the RAM 203, for example.

[0050] Figs. 17A to 17C depict conceptual views of the key pair/electronic certificate detailed information database managed by a key pair certificate management module 307. According to this embodiment, this database is stored in the HDD 204 of the multi-function peripheral 100. However, it is understood that this database may be stored elsewhere as long as it is accessible by the multi-function peripheral 100

when needed.

[0051] The flowchart of Fig. 5A will now be described. This processing is started (instigated) when a key pair/electronic certificate list obtainment request is received. First, in step S501, the CPU 201 receives the key pair/electronic certificate list obtainment request. Next, the process advances to step S502, and the CPU 201 obtains, for example, the detailed information of the key pair/electronic certificate shown in Fig. 17A which is managed by the key pair certificate management module 307. Next, the process advances to step S503, and the CPU 201 uses the detailed information of the key pair/electronic certificate obtained in step S502 to generate HTML data for a Web page screen which is to be provided as an RUI.

[0052] Figs. 10A to 15 depict views showing examples of the Web page screens (i.e. RUIs) that are to be displayed on the PC 103 according to the first embodiment. In step S503 of Fig. 5 according to the first embodiment, assume that the HTML data for the Web page screen shown in Fig. 10A will be generated and that the generated HTML data will be displayed using the Web browser of the PC 103. As a result, the key pair/electronic certificate list held by the multi-function peripheral 100 can easily be confirmed from the PC 103.

[0053] The information of the electronic certificate that is displayed in the list of Fig. 10A includes a name 1011, an application 1012, an issuer 1013, expiration 1014, and detail 1015 of the
5 certificate. The name 1011 is a character string arbitrarily added by an operator such as the administrator of the multi-function peripheral 100 when the key pair/electronic certificate is issued. The application 1012 is a setting value indicating that the
10 key pair/electronic certificate will be used for an application implementing/using a particular communication protocol of TLS, IPSEC, or IEEE802.1X. The issuer 1013 is a distinguished name (DN) (i.e. an identification) of the CA that issued the electronic
15 certificate. The expiration 1014 is information indicating the date on which the validity period of the electronic certificate will expire. The detail 1015 is an icon for displaying the detailed information of the electronic certificate. The process subsequently
20 advances to step S504, and the CPU 201 transmits, as a response to step S501, the HTML data generated in step S503 to the PC 103 and ends the processing. Thus, step S403 of Fig. 4A is executed in this manner.

[0054] Note that although not shown in the
25 sequence charts of Figs. 4A and 4B, a request to display the detailed information of the electronic certificate is transmitted from the PC 103 to the

multi-function peripheral 100 when the administrator of the multi-function peripheral 100 clicks the icon of the detail 1015 in Fig. 10A when it is displayed on the PC 103. The multi-function peripheral 100 that
5 received this display request will obtain the detailed information of the electronic certificate, generate the HTML data for the detailed information of the certificate based on the obtained information, and transmit the generated data to the PC 103 as a response
10 to the display request.

[0055] As a result, the detailed information of the electronic certificate is displayed on the Web browser of the PC 103, for example, in the manner shown in Fig. 16. Fig. 16 depicts an example view of the
15 detailed information of the electronic certificate that is displayed on the PC 103.

[0056] Fig. 5B is a flowchart for describing the processing performed when a request to display this detailed information is received from the PC 103 by the
20 multi-function peripheral 100 according to the first embodiment. Note that this processing is implemented by the CPU 201 executing a program deployed in the RAM 203, for example.

[0057] First, in step S511, the CPU 201 receives a
25 request to obtain the detailed information of the electronic certificate from the PC 103. Next, the process advances to step S512, and the CPU 201 obtains

the detailed information of the key pair/electronic certificate shown in Fig. 17A which is managed by the key pair certificate management module 307. Next, the process advances to step S513, and the CPU 201

5 generates the HTML data for a Web page screen by using the detailed information of the key pair/electronic certificate obtained in step S512 and transmits the generated HTML data to the PC 103 in step S514.

[0058] Fig. 16 depicts a screen view showing an
10 example of the display screen view of the detailed information of the electronic certificate according to the first embodiment. This screen view is displayed as an RUI in a Web-page format on the PC 103.

[0059] Returning to the description of Fig. 4A
15 again, in step S403, the multi-function peripheral 100 transmits, as a response to a request from the PC 103, the HTML data for the Web-page screen shown in Fig. 10A which is generated in step S402.

[0060] Note that the processes shown in the above-
20 described step S401 to step S403 of Fig. 4A, step S501 to step S504 of Fig. 5A, and step S511 to step S514 of Fig. 5B show control process steps related to the electronic certificate information display processing performed by the multi-function peripheral 100 when a
25 request to display the key pair/electronic certificate list is received.

[0061] In step S404, the multi-function peripheral

100 receives a request to display a connection setup screen of a SCEP server (an example of a CA/RA 102) from the PC 103. Assume that in order to perform a connection setup operation (e.g. a setting of
5 connection settings/parameters for establishing a communication channel/connection) with the certificate/registration authority 102, the administrator of the multi-function peripheral 100 according to the first embodiment clicks on connection
10 settings 1002 shown in Fig. 10A to transmit a connection setup screen display request to the multi-function peripheral 100.

[0062] Next, in step S405, the multi-function peripheral 100 transmits, as a response to the request
15 received in step S404, HTML data for a predetermined SCEP server connection setup screen shown in Fig. 10B to the PC 103.

[0063] The connection setup screen shown in Fig. 10B includes input fields for a server name/address
20 1016 and a port number 1017 for inputting the SCEP server host name (e.g. its IP address) and the connection destination port number, respectively, and a setting button 1018 for instructing/indicating the completion of the setup/setting process, i.e. the
25 completion of setting of the input setting values so that these can be effected for the connection.

[0064] Next, in step S406, the multi-function

peripheral 100 receives a setting instruction request of the connection setup operation from the PC 103.

Assume that the administrator of the multi-function peripheral 100 according to the first embodiment will

5 transmit this setting instruction request to the multi-function peripheral 100 by clicking on the setting button 1018 after inputting the necessary information relating to the server name 1016 and the port number 1017 of Fig. 10B from the PC 103.

10 **[0065]** Next, in step S407, the multi-function peripheral 100 performs the connection setup operation (i.e. sets the connection settings in accordance with the input information), and executes the generation of a Web page screen data for displaying the setting
15 process and the setting result of the connection setup operation. In step S408, the multi-function peripheral 100 transmits, as a response to the request from the PC 103, the HTML data for the Web page screen based on the web page screen data generated in step S407 and shown
20 in Fig. 11A.

[0066] Fig. 6 is a flowchart for describing the connection setup process for establishing a connection/communication with the certificate/registration authority 102 performed in
25 step S407 of Fig. 4A by the multi-function peripheral 100 according to the first embodiment. Note that the processing is implemented by the CPU 201 executing a

program deployed in the RAM 203, for example.

[0067] First, in step S601, the CPU 201 receives a connection setting request from the PC 103. Next, the process advances to step S602, and the CPU 201 obtains the setting values, e.g. the host name and the port number included in the connection setting request, and stores the obtained setting values in the RAM 203 or the HDD 204. Next, the process advances to step S603, and the CPU 201 generates, for example, the HTML data for the Web page screen as shown in Fig. 11A. The process advances to step S604, and the CPU 201 transmits the HTML data generated in step S603 to the PC 103 as a response to the request in step S601 and ends the processing. The process advances to step S408 in this manner.

[0068] As a result, as shown in Fig. 11A, a character string 1101 indicating that the settings have been implemented (i.e. the setting values for establishing a connection with the CA/RA 102 are set/applied/effected) is displayed on the PC 103.

[0069] The processes shown in the above-described step S406 to step S408 and step S601 to step S604 are the control operations related to the connection setup process of the multi-function peripheral 100.

[0070] Next, in step S409 of Fig. 4A, the multi-function peripheral 100 receives a request to display the CA certificate obtainment screen which is

transmitted from the browser of the PC 103. In the first embodiment, since the administrator of the multi-function peripheral 100 will obtain the CA certificate issued by the certificate/registration authority 102, assume that the request to display the CA certificate obtainment screen is transmitted to the multi-function peripheral 100 when the administrator clicks CA certificate obtainment 1003 shown in Fig. 10A.

[0071] As a result, in step S410, the multi-function peripheral 100 transmits, as a response to the received request in step S409, HTML data of the predetermined CA certificate obtainment screen shown in Fig. 11B.

[0072] The connection setting screen shown in Fig. 11B includes an execute button 1102 for instructing the actual obtainment of the CA certificate.

[0073] Next, in step S411, the multi-function peripheral 100 receives the CA certificate obtainment request transmitted from the browser of the PC 103 when the execute button 1102 shown in Fig. 11B is clicked. In the first embodiment, assume that the CA certificate obtainment request is transmitted to the multi-function peripheral 100 when the administrator of the multi-function peripheral 100 clicks the execute button 1102 shown in Fig. 11B.

[0074] Next, in step S412, the multi-function peripheral 100 executes/performs processing for

generating CA certificate obtainment request data. The process advances to step S413, and the multi-function peripheral 100 transmits the CA certificate obtainment request data generated in step S412 to the

5 certificate/registration authority 102, which is serving as the SCEP server, based on the information set in the connection setup operation performed in step S407. The process advances to step S414, and the multi-function peripheral 100 receives a CA certificate

10 obtainment response which is transmitted from the certificate/registration authority 102. As a result, in step S415, the multi-function peripheral 100 analyses the received CA certificate obtainment response, obtains the CA certificate included in the

15 response, and performs processing to register the obtained CA certificate as a CA certificate trusted by the multi-function peripheral 100. The multi-function peripheral 100 also generates HTML data for a webpage screen for indicating a result/outcome of making the CA

20 certificate obtainment request. The process advances to step S416, and the multi-function peripheral 100 transmits, to the PC 103, a response including a CA certificate obtainment request result. The response includes the HTML data for the Web page screen

25 generated in step S415 and shown in Figs. 12A or 12B as indicators of the result (i.e. outcome of making the request). Fig. 12A shows an example of a screen that

is displayed when the obtainment of the CA certificate has been successful and the obtained certificate is registered as the trusted CA certificate. On the other hand, Fig.12B shows an example of a screen that is
5 displayed when the obtainment of the CA certificate has failed.

[0075] Fig. 7 is a flowchart for describing the CA certificate obtainment and registration processes shown in step S412 to step S416 of Fig. 4A and performed by
10 the multi-function peripheral 100 according to the first embodiment in more detail. Note that these processes are implemented by the CPU 201 executing a program deployed in the RAM 203, for example.

[0076] First, in step S701, the CPU 201 receives a
15 CA certificate obtainment request from the PC 103. Next, the process advances to step S702, and the CPU 201 generates a CA certificate obtainment request message based on the connection setting (setup) information set for a connection/communication with the
20 certificate/registration authority 102 which was obtained in step S407. An example of the obtainment request message generated in accordance with the first embodiment is shown below. Since SCEP is used as the communication protocol in the first embodiment, the
25 following message is used as a request message using this protocol.

xxxxxxx/yyyy?operation=GetCAXyz&message=CAIdenti

fier

[0077] Next, the process advances to step S703, and the CPU 201 controls the network interface controller 205 to connect to the

5 certificate/registration authority 102, which is serving as the SCEP server, by TCP/IP protocol based on the connection setting information for the certificate/registration authority 102 obtained in step S407 of Fig. 4A. Next, the process advances to step
10 S704, and the CPU 201 determines whether or not the connection in step S703 has succeeded. If the connection has succeeded, the process advances to step S705. Otherwise, the process advances to step S714 for performing an error processing step.

15 **[0078]** In step S705, the CPU 201 transmits the CA certificate obtainment request message generated in step S702 to the certificate/registration authority 102 using, for example, the GET or POST method of HTTP protocol. Next, the process advances to step S706, and
20 the CPU 201 determines whether or not the transmission in step S705 has succeeded. If the transmission has succeeded, the process advances to step S707.

Otherwise, the process advances to step S714 for the error processing. In step S707, the CPU 201 (via the
25 network interface controller 205) receives response data from the certificate/registration authority 102, which is sent as a response to the CA certificate

obtainment request message. The process advances to step S708, and the CPU 201 determines whether or not the reception of the response data in step S707 has succeeded. If the reception has succeeded, the process advances to step S709. Otherwise, the process advances to step S714. In step S709, the CPU 201 analyses the response data received in step S707 and obtains the data of the CA certificate included in the response data. The analysis of this response data and the obtainment process for the CA certificate are performed by the encryption module 306.

[0079] Note that the response data according to the first embodiment is binary data in a X.509 (RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) format. However, for example, data in a PKCS#7 (RFC5652: Cryptographic Message Syntax) format may be transmitted as a response as well, and it is understood that the data format is not limited to a specific one as long as the CA certificate can be obtained from it.

[0080] The process advances to step S710, and the CPU 201 determines whether or not the obtainment of the CA certificate in step S709 has succeeded. If the obtainment has succeeded, the process advances to step S711. Otherwise, the process advances to step S714. In step S711, the CPU 201 registers the CA certificate

obtained in step S709 as a CA certificate trusted by the multi-function peripheral 100. The CPU 201 holds (temporarily stores) the obtained CA certificate in the RAM 203 and causes the key pair certificate management module 307 to store the CA certificate in a predetermined directory of the HDD 204 for storing the CA certificate that is trusted by the multi-function peripheral 100. The process advances to step S712, and the CPU 201 determines whether or not the CA certificate registration process in step S711 has succeeded. If the process has succeeded, the process advances to step S713. Otherwise, the process advances to step S714. In step S713, the CPU 201 generates a thumbmark (a hash value obtained using an SHA1 algorithm) of the CA certificate which is to be displayed in a manner as indicated by a character string 1201 of Fig. 12A when the obtainment and registration of the CA certificate has succeeded. The generation of this thumbmark is executed/performed by the encryption module 306. The process then advances to step S715, and the CPU 201 generates, based on the processing results from step S703 to S714, HTML data for CA certificate obtainment result display data shown in Fig. 12A or 12B as appropriate. The process advances to step S716, and the CPU 201 controls to transmit, to the PC 103, the HTML data generated in step S715 as a response to the received request in step S701 and ends

the obtainment and registration processing.

Subsequently, the process advances to step S417 of Fig. 4A. In the first embodiment, the character string 1201 of Fig. 12A is displayed in accordance with the CA certificate obtainment and registration result.

Alternatively, if the error processing is executed in step S714, a character string 1202 of Fig. 12B is displayed, for example. Next, the description will return to Fig. 4A.

10 **[0081]** In step S417, the multi-function peripheral 100 receives a request, which is transmitted from the browser of the PC 103, to display the certificate issuance request screen. In the first embodiment, assume that the administrator of the multi-function peripheral 100 will click on a certificate issuance request 1004, shown in Fig. 10A to make a certificate issuance request to the certificate/registration authority 102 in order to obtain a newly issued electronic certificate.

20 **[0082]** Next in step S418, the multi-function peripheral 100 transmits, as a response to the display request in step S417, HTML data for a predetermined certificate issuance screen, an example of which is shown in Fig. 13A, to the PC 103. As a result, the PC 103 performs a display control to display the screen shown in Fig. 13A.

[0083] The certificate issuance request screen of

Fig. 13A includes a name 1301 of the certificate, a key length 1302 for setting a key length for a key pair to be generated, an issuance destination information input field 1303, a signature verification 1304 indicating whether a signature which is to be added to a certificate issuance request response transmitted from the certificate/registration authority 102 is to be verified/authenticated, a key application 1305 for setting the application of (i.e. the communication protocol to be used with) the issued certificate, a password 1306 which is to be included in the certificate issuance request, and an execute button 1307 for executing/instructing the certificate issuance request transmission. In this embodiment, the key application 1305 is set as a group of checkboxes and shows that it is possible to set a plurality of applications (i.e. more than one communication protocols) for one certificate.

[0084] Next, in step S419, when the certificate issuance request is instructed, for example by clicking on the execute button 1307 of the screen shown in Fig. 13A, the multi-function peripheral 100 receives the certificate issuance request including pieces of input/setting information/data associated with the items referred by respective reference numerals 1301 to 1306 that are set from the browser of the PC 103. In the first embodiment, assume that the administrator of

the multi-function peripheral 100 inputs and sets the information associated with the items referred by the respective reference numerals 1301 to 1306 and clicks on the execute button 1307 shown in Fig. 13A to

5 transmit the certificate issuance request instruction from the PC 103 to the multi-function peripheral 100.

[0085] Next, in step S420, the multi-function peripheral 100 executes/performs the certificate issuance request (data) generation process. In step

10 S421, the multi-function peripheral 100 transmits, based on the information set in step S407, the certificate issuance request data generated in step S420 to the certificate/registration authority 102, which is serving as the SCEP server. The

15 certificate/registration authority 102 then issues the certificate based on issuance request data and transmits a certificate issuance request response. In step S422, the multi-function peripheral 100 receives the certificate issuance request response transmitted

20 from the certificate/registration authority 102. Next, in step S423, the multi-function peripheral 100 performs analysis and registration processes (executing/performing a signature verification/authentication in accordance with the

25 setting, obtaining the certificate included in the response, and setting/registering the obtained certificate to the designated/specified application,

i.e. to the specified communication protocol) of the certificate issuance request response received in step S422. Subsequently, the multi-function peripheral 100 executes a Web page screen generation process for displaying the result of the certificate issuance request.

[0086] Here, if the certificate issuance and the subsequent obtainment of the issued certificate have succeeded, storing and application setting (e.g. communication protocol setting) of the electronic certificate data will be performed by the processing in step S423. Here, the application setting is related to setting settings/parameters for the communication function which uses the electronic certificate, and for the encrypted communication protocols such as TLS, IPSEC, and IEEE802.1X, which are settable/configurable (i.e. available for use dependent on a setting) in the first embodiment. Also, assume that the multi-function peripheral 100 according to the first embodiment can hold/store a plurality of electronic certificates and set one or more application (e.g. one or more communication protocol) for each electronic certificate. For example, different applications (e.g. communication protocols) are settable when an electronic certificate used by the multi-function peripheral 100 to provide a server service (by performing a TLS communication to serve as a Web

server) and an electronic certificate used by the multi-function peripheral 100 to perform a client communication (e.g. using IEEE802.1X) differ from each other. However, it is understood that a single
5 electronic certificate may also be applied/used for, all or more than one of the communication applications as appropriate.

[0087] In step S424, the multi-function peripheral 100 transmits, to the PC 103, HTML data of the Web page
10 screen shown in Fig. 13B or Fig. 14A which was generated in step S423. Note that a setting-result character string as shown by a character string 1308 in Fig. 13B and a character string 1401 in Fig. 14A will be displayed in accordance with the certificate
15 issuance request result. Fig. 13B shows a view illustrating an example of a screen when certificate issuance and obtainment have succeeded. The screen shown in Fig. 13B is displayed on the PC 103 in a case where a certificate issuance request is transmitted
20 from the PC 103 to the multi-function peripheral 100 and the certificate is issued according to the issuance request. The issued certificate is set as a certificate that is used by the multi-function peripheral 100 to perform a secured communication, in a case where the
25 multi-function peripheral 100 is restarted. A message urging a user to restart the multi-function peripheral 100 is included in the screen shown in Fig. 13B. Fig.

14A shows a view illustrating an example of a screen view when certificate issuance and obtainment have failed. The screen shown in Fig. 14A is displayed on the PC 103 in a case where a certificate issuance request is transmitted from the PC 103 to the multi-function peripheral 100 but the certificate is not issued. A message notifying a user of a failure of issuance of the certificate is included in the screen shown in Fig. 14A.

10 **[0088]** If certificate issuance and obtainment have succeeded in this manner, storing and application (communication protocol) setting of the electronic certificate data is performed by the process in step S423. Since the communication control module 303 according to the first embodiment obtains the electronic certificate data used in the encrypted communication such as TLS, IPSCE, and IEEE802.1X at the time of an activation of the multi-function peripheral 100 (i.e. the communication control module 303 initialises and establishes an encrypted communication channel, which uses the communication protocol, during the start-up of the multi-function peripheral 100), a restart of the multi-function peripheral 100 is necessary if the changes in the application (the communication protocol and related electronic certificate) are to be effected/implemented.

[0089] Figs. 8A and 8B are flowcharts for

describing the certificate issuance request/obtainment processing performed in step S419 to step S424 of Fig. 4B by the multi-function peripheral 100 according to the first embodiment in more detail. Note that this processing is implemented by the CPU 201 executing a program deployed in the RAM 203, for example.

[0090] First, in step S801, the CPU 201 receives a certificate issuance request from the PC 103 (e.g. via the network interface controller 205). Next, the process advances to step S802, and the CPU 201 obtains setting values of the request, e.g. the information on the name 1301 of the certificate, the key length 1302, the issuance destination information input field 1303, the signature verification 1304, and the key application 1305 included in the certificate issuance request received in step S801. Next, the process advances to step S803, and the CPU 201 obtains the CA certificate obtained in step S412 to step S415 of Fig. 4A. The process advances to step S804, and the CPU 201 performs processing to generate a key pair based on the information of the name 1301 and the key length 1302 obtained in step S802 and to generate certificate signing request (CSR) data of a PKCS#10 (RFC2986: PKCS#10: Certification Request Syntax Specification) format based on the information of the issuance destination information input field 1303 and the password 1306 using the encryption module 306. Next,

the process advances to step S805, and the CPU 201 determines whether or not the generation of the key pair/CSR in step S804 has succeeded. If it is determined that the generation has succeeded, the process advances to step S806. Otherwise, the process advances to step S823 for performing an error processing. In step S806, the CPU 201 generates certificate issuance request data (e.g. the CSR data). The CSR data generated in step S806 becomes the PKCS#7-format data defined in the SCEP based on the connection settings set for communicating with the certificate/registration authority 102 obtained in step S407 of Fig. 4A. Next, the process advances to step S807, and the CPU 201 determines whether or not data generation in step S806 has succeeded in generating the certificate issuance request data. If the data generation has succeeded, the process advances to step S808. Otherwise, the process advances to step S823.

[0091] In step S808, the CPU 201 executes TCP/IP-protocol connection to the certificate/registration authority 102 serving as a SCEP server based on the connection setting to the certificate/registration authority 102 that was obtained in step S407 of Fig. 4A. Next, the process advances to step S809, and the CPU 201 determines whether or not the connection in step S808 has succeeded. If the connection has succeeded, the process advances to step S810.

Otherwise, the process advances to step S823. In step S810, the CPU 201 transmits the CSR data generated in step S806 by the GET or POST method of HTTP protocol to the certificate/registration authority 102. In step 5 S811, the CPU 201 determines whether or not the transmission in step S810 has succeeded. If the transmission has succeeded, the process advances to step S812. Otherwise, the process advances to step S823. In step S812, the CPU 201 receives (e.g. via the 10 network interface controller 205) a certificate issuance response (e.g. including CSR response data) from the certificate/registration authority 102. As the response data is defined by the SCEP, and PKCS#7-format data is transmitted as a response. It is 15 understood that other data formats may also be used.

[0092] Next, the process advances to step S813, and the CPU 201 determines whether or not reception of the response data in step S812 has succeeded. If the reception has succeeded, the process advances to step 20 S814. Otherwise, the process advances to step S823. In step S814, the CPU 201 determines whether or not a signature verification is needed by, for example, determining whether a signature verification setting is present based on the information on the signature 25 verification 1304 obtained in step S802. If the signature verification is to be performed, the process advances to step S815. Otherwise, the process advances

to step S817. In step S815, the CPU 201 controls to verify/authenticate the signature data added to the response data received in step S812 using the public key included in the CA certificate obtained in step
5 S803. The process advances to step S816, and the CPU 201 determines whether or not the result of the signature verification in step S815 is successful (i.e. the signature has been verified/authenticated as authentic/valid). If the signature verification has
10 succeeded, the process advances to step S817. Otherwise, the process advances to step S823.

[0093] In step S817, the CPU 201 controls to analyse the response data received in step S812 and obtain certificate data included in the response data.
15 The response data analysis and certificate obtainment processes are performed by the encryption module 306, for example. Next, in step S818, the CPU 201 determines whether or not certificate obtainment in step S817 has succeeded. If the certificate obtainment
20 has succeeded, the process advances to step S819. Otherwise, the process advances to step S823. In step S819, the CPU 201 registers the certificate obtained in step S818 as the electronic certificate (i.e. digital certificate) corresponding to the key pair generated in
25 step S804. At the same time, the CPU 201 causes/controls the key pair certificate management module 307 to store the public key pair generated in

step S804 and the obtained electronic certificate in a predetermined directory of the HDD 204 for storing the key pair/electronic certificate. The key pair certificate management module 307 also adds the
5 information on the public key pair generated in step S804 and the obtained electronic certificate to the key pair certificate detailed information list as shown in Fig. 17B. In Fig. 17B, a new key pair/certificate Xyz4 has been added.

10 **[0094]** Next, the process advances to step S820, and the CPU 201 determines whether or not the certificate registration process in step S819 has succeeded. If the registration has succeeded, the process advances to step S821. Otherwise, the process
15 advances to step S823. In step S821, the CPU 201 sets settings for an application that is going to use the certificate based on the information on the key application 1305 obtained in step S802. For example, the key pair certificate management module 307 updates
20 the application information (e.g. information on the communication protocol) in the key pair/certificate detailed information list as shown in Fig. 17C. In Fig. 17C, the key pair/certificate to be used in TLS has been changed from Xyz1 (in Fig 17B) to Xyz4. Next,
25 the process advances to step S822. The CPU 201 determines whether or not the application setting (e.g. update of the electronic certificate) in step S821 has

succeeded. If the application setting (e.g. the update) has succeeded, the process advances to step S824. Otherwise, the process advances to step S823.

[0095] In step S824, the CPU 201 generates HTML data for the certificate issuance request result, as shown in Fig. 13B, which corresponds to a result/outcome of the processing from step S801 to step S823. In step S825, the CPU 201 controls to transmit the HTML data generated in step S824 to the PC 103 as a response to the certificate issuance request of step S801 and ends the certificate issuance request/obtainment processing. Subsequently, the process advances to step S425 of Fig. 4B.

[0096] The processes of above-described step S419 to step S424 and step S801 to step S825 form parts of control operations related to the electronic certificate issuance request and its response processing and the communication (protocol) application setting of the multi-function peripheral 100. In the first embodiment, these processes performed from the issuance request and response processing to the communication protocol application setting are collectively referred to as "the electronic certificate automatic update function".

[0097] By executing this electronic certificate automatic update function, the multi-function peripheral 100 can automatically perform the electronic

certificate issuance request and response processing via the network and also set the application (e.g. the communication protocol) of the received electronic certificate. This can reduce the user's workload. The description will return to Fig. 4B.

5
[0098] In step S425, the multi-function peripheral 100 receives a request to restart the multi-function peripheral 100. In the first embodiment, assume that the administrator of the multi-function peripheral 100
10 restarts the multi-function peripheral 100 by clicking on a restart button 1309 shown in Fig. 13B.

[0099] Next, the process advances to step S426, and the multi-function peripheral 100 transmits, as a response to the restart request in step S425, HTML data
15 of the predetermined restart execution screen shown, for example as in Fig. 14B. Next, the process advances to step S427, and the multi-function peripheral 100 executes/performs the restart process for the multi-function peripheral 100.

20 **[0100]** The multi-function peripheral 100 according to the first embodiment has been described under the assumption that a restart is necessary to effect any changes made to the application settings, e.g. when setting a communication protocol (application) for the
25 received electronic certificate to IEEE802.1X. This is because, for example, an electronic certificate for IEEE802.1X may be deployed/initialised in the RAM 203

at the time of an activation/start-up of the multi-
function peripheral 100 and may be in use continuously,
which means it may not be replaced by the received
electronic certificate that has been stored in the HDD
5 204. However, if it is possible to switch/change the
electronic certificate that is to be used for the
application using that particular communication
protocol without the restart of the multi-function
peripheral 100, it may be set so that the restart is
10 not performed. For example, if the application is set
for TLS, it may be set so that the restart is deemed
unnecessary. For example, it is possible to preset an
indicator regarding the necessity of a restart for each
of the plurality of applications, and the multi-
15 function peripheral 100 may automatically determine
whether to restart in accordance with this restart
necessity indicator information. In another example,
the PC 103 may store such restart necessity indicator
information, and determine whether to transmit, to the
20 multi-function peripheral 100, the restart request or
not based on it.

[0101] Fig. 9 is a flowchart for describing the
process related to the restart of the multi-function
peripheral 100 in step S425 to step S427 of Fig. 4B
25 performed by the multi-function peripheral 100
according to the first embodiment. Note that this
processing is implemented by the CPU 201 executing a

program deployed in the RAM 203, for example.

5 **[0102]** First, in step S901, the CPU 201 receives a request to restart the multi-function peripheral 100 from the PC 103 (e.g. via the network interface controller 205). Next, the process advances to step S902, and the CPU 201 transmits (e.g. via the network interface controller 205), to the PC 103 as a response to the restart request in step S901, predetermined HTML data for the restart request of the multi-function peripheral 100 shown in Fig. 14B. Next, the process advances to step S903. The CPU 201 instructs/causes/controls the device control module 310 to start the restart process and ends the restart processing.

15 **[0103]** By performing the sequence of operations described above, it is possible to use the electronic certificate obtained from the certificate/registration authority 102 in the restarted multi-function peripheral 100.

20 **[0104]** Fig. 15 depicts a view showing an example of a screen view when the key pair/electronic certificate list is displayed by executing the processing of step S401 to step S403 again after the certificate issuance and obtainment have succeeded.

25 Information 1501 of the certificate Xyz4 newly issued by the certificate/registration authority 102 has been added to this list.

[0105] The overall process sequence from the process steps for the initial setup (setting) related to the electronic certificate issuance request, the display of the information regarding the electronic certificate, the issuance request and the reception of the issued electronic certificate, to the process for restarting the multi-function peripheral and the effecting/implementation/enabling of the issued electronic certificate according to the first embodiment has been described above.

[0106] Note that although the sequence of the processing shown in Figs. 4A and 4B has been described with the processes involved from the initial connection setup in steps S404-S408 to the issuance request and effecting/implementation/enabling of the issued electronic certificate in steps S419-S427 as a single serial sequence of operations, the processes related to the initial connection setup operation (steps S401-S418) such as the connection setting in steps S404-S408 may be just performed once for the multi-function peripheral 100, and not repeated thereafter unless a specific need for a connection with another CA or an update in the connection setting values arises. For example, the setting operations of the displaying of the electronic certificate information in step S401 to step S403, the initial connection setup process in step S404 to step S408, and the CA certificate obtainment

process of step S409 to step S418 may be performed for only the first certificate issuance request. Then it may be operated so that the same settings are used for the second and any subsequent electronic certificate issuance requests. In other words, at the time of performing the second or subsequent electronic certificate update/issuance, it may be operated so as to execute only the processing steps related to the electronic certificate issuance request and its response processing and the processes related to the communication application settings in step S419 to step S424, and, if required, the restart and implementation/enabling processing of step S425 to step S427.

15 **[0107]** In the first embodiment, the multi-function peripheral 100 receives processing instructions from the PC 103 via the Web-page-format RUIs held by (i.e. stored in) the multi-function peripheral 100 itself and performs controls based on these instructions.

20 However, the interface used to receive an instruction from the administrator to the multi-function peripheral 100 is not particularly limited to such an arrangement. Each instruction may be received from a local user interface (LUI) provided on the multi-function peripheral 100 itself or on another device connected to the multi-function peripheral 100 (e.g. the printer 210 or the scanner 211) using the printer 210 held by the

multi-function peripheral 100 instead of each Web-page-format RUI, for example.

[0108] In addition, instead of the administrator manually making a request by operating the Web-page-format RUI directly, it may be arranged so that a request can be automatically input and instructed from a PC or another management server to the multi-function peripheral 100 by, for example, creating a template for each Web-page input region and a rule for each Web-page operation instruction in advance. In this case, for example, a Web scraping (data mining) technique may be used.

[0109] Also, although the first embodiment has an arrangement in which the operation for obtaining and registering a CA certificate is performed by the administrator of the multi-function peripheral 100, it may have an arrangement in which the CA certificate is, when needed, automatically obtained at the time of the first, or any subsequent, certificate issuance request.

[0110] Also, the first embodiment has been provided with a signature verification setting (for indicating whether to perform a signature verification) included in the certificate issuance request response from the certificate/registration authority 102.

However, instead of providing this settable/adjustable setting, it may be preset so as to always perform the signature verification or not perform the signature

verification.

[0111] In addition, although the first embodiment has an arrangement in which a password is included as data in the certificate issuance request (e.g. the password is included in the CSR), it may have an arrangement in which the password is unnecessary (e.g. not used).

[0112] As described above, according to the first embodiment, a certificate addition/update request (e.g. the certificate issuance request) can be issued to an external apparatus such as a certificate/registration authority by using a certificate automatic update protocol (i.e. the electronic certificate automatic update function) based on an instruction from an RUI. Then, based on the response corresponding to the request, a certificate can be received and registered in the multi-function peripheral, and various settings or parameters for running an application using the certificate can be set.

[0113] [Second Embodiment]

The second embodiment of the present invention will be described next. In the aforementioned first embodiment, a Web-page-format RUI was provided to the user of the multi-function peripheral 100 by using the Web server function held by the multi-function peripheral 100. The user added, updated, and set various settings or parameters for running an

application which is to use the electronic certificate
by giving instructions to the multi-function peripheral
100 via the RUI. Since this electronic certificate has
a validity period, an electronic certificate for which
5 the validity period has expired is disabled. This can
disrupt network communication since a correct
communication authentication cannot be performed with a
disabled electronic certificate. Hence, when the
validity period of the electronic certificate held by
10 (stored in) a device is near its expiration time/date
or has expired, the electronic certificate needs to be
updated. However, if there are a plurality of devices
using the electronic certificate, it is difficult for
the administrator of the devices to
15 obtain/access/discern/grasp the validity period of the
electronic certificate of each device and to update
each electronic certificate individually/accordingly.

[0114] Therefore, the second embodiment will
describe, an information processing apparatus which is
20 capable of performing an electronic certificate
automatic update function such as that in the first
embodiment, a control/management operation that
automatically activates the electronic certificate
update function at a predetermined date and time (i.e.
25 at a reserved time), instead of manually controlling
each update based on a user instruction. Note that in
the second embodiment, the network arrangement, the

hardware arrangement, the software arrangement, the key pair/electronic certificate list display processing, the connection setup process of the multi-function peripheral 100 as the information processing apparatus are the same as those of the first embodiment, and a description thereof are omitted.

[0115] Fig. 18 depicts a view showing an example of an electronic certificate update reservation setting screen provided for the multi-function peripheral 100 according to the second embodiment. This screen is shown, for example, by a Web-page-format RUI in the same manner as the other screens described herein. An update date and time (i.e. a reserved or predetermined time) for the electronic certificate can be set via this electronic certificate update reservation setting screen. In the second embodiment, it is possible to set, as the update date and time (and update interval designation where appropriate), three settings of: an update date and time 1801; a time period 1802 prior to the expiration of the validity period; and a time period between intervals or a date for defining a cycle 1803. In the update date and time 1801, the year, the month, the day, and the time for the update can be set, and when the current time held in (e.g. observed/measured by) the multi-function peripheral 100 changes to the set time and date of this update date and time 1801, the electronic certificate automatic

update function is executed. The time period 1802 designates a number of days before the expiry of the validity period of the currently used electronic certificate. If the days from the current time and date held in (i.e. observed/measured by) the multi-function peripheral 100 to the validity period becomes equal to or less than the number of days designated by the time period 1802, the electronic certificate automatic update function is executed. The time period/date 1803 executes the electronic certificate automatic update function based on a cycle as defined by this time period/date. In the second embodiment, this cycle can be set based on a predetermined number of days (i.e. a time period), a predetermined day of each month, or a predetermined day and month of each year (i.e. date). This setting (or reserving) of the update date and time or the update cycle of each electronic certificate's update is called "an electronic certificate update reservation setting".

When the update reservation setting of each electronic certificate is updated, the CPU 201 stores the updated reservation information in an HDD 204.

[0116] Fig. 18 shows, in the time period 1802, an example of a screen where it has been set to execute the electronic certificate automatic update function when the date becomes 14 days before the expiration of the validity period. Although the above-described

electronic-certificate update reservation setting types are used to make a reservation for performing the electronic certificate automatic update operation/function in the second embodiment, it is understood that the present invention is not limited to this. Another time and/or date or timing designation/reservation method may also be used as long as it can define a condition or a point/period in time for performing/executing this operation.

10 [0117] Fig. 19 is a flowchart for describing the processing performed when the electronic certificate automatic update function is to be executed based on the electronic-certificate update reservation setting set on the multi-function peripheral 100 according to the second embodiment. Although an example in which the automatic update function has been set for the multi-function peripheral 100 is shown here, it is possible to execute the process shown in Fig. 19 on a plurality of multi-function peripherals by designating the plurality of multi-function peripherals (it is also possible to set a different time or condition for performing/executing the automatic update operation for each multi-function peripheral). In this case, the processes of Fig. 19 are executed in parallel among the plurality of multi-function peripherals. Note that the processing is implemented by the CPU 201 executing a program deployed in a RAM 203, for example.

[0118] First, in step S1901, the CPU 201 obtains the electronic certificate update reservation setting from the HDD 204. Next, the process advances to step S1902, and the CPU 201 obtains the information on the currently used electronic certificate. This information is information such as that indicated in Figs. 17A to 17C. Next, the process advances to step S1903, and the CPU 201 obtains the current time and date observed/measured by the multi-function peripheral 100. It is understood that time differences among different time zones may also be taken into account here. Next, the process advances to step S1904, and the CPU 201 compares the electronic certificate update reservation setting and the obtained electronic certificate information to determine whether or not the currently used electronic certificate needs to be updated. Here, if it is determined that the electronic certificate need not be updated, the process returns to step S1901. The process may wait for a predetermined period, or until another predetermined condition has been met before returning to step S1901. On the other hand, if it is determined that the electronic certificate needs to be updated, the process advances to step S1905 and the process advances to the "certificate issuance request processing" control described in Figs. 8A and 8B. After the processing of Figs. 8A and 8B is completed, the process advances to

step S1906.

[0119] According to the above-described process, it is possible to automatically update the electronic certificate based on a designated/preset update date and time or an update cycle without a manual instruction from the user. This allows the electronic certificate of each device to be maintained, i.e. updated at a desirable timing, while reducing the user's workload, and without requiring the administrator to grasp/discern/determine the validity period of the electronic certificate of each device.

[0120] In step S1906, the CPU 201 determines, upon updating the electronic certificate, whether the multi-function peripheral 100 needs to be restarted. Here, if the CPU 201 determines that a restart is necessary, the process advances to step S1907 to execute the "restart/setting implementation/enabling process" shown in Fig. 9. On the other hand, if the CPU 201 determines that the restart is unnecessary, it ends the automatic update operation processing. This is to control the restart of the multi-function peripheral 100 so that it is restarted only when necessary. For example, this differentiates between cases where the multi-function peripheral 100 has switched the electronic certificate to be used and the network configuration is changed for TLS, which does not require a restart, and for IEEE802.1X which requires

restart.

[0121] As described above, according to the second embodiment, by reserving/specifying/defining the update timing of the electronic certificate, it is possible
5 for the multi-function peripheral to automatically transmit an electronic certificate issuance request to update and register an electronic certificate without user instruction. As a result, even when the user is not aware of (e.g. due to not having access to such
10 knowledge/information) the validity period of the electronic certificate, it is possible to prevent a situation in which the electronic certificate is disabled (e.g. because it has expired) and the network communication is disrupted.

15 **[0122]** Other Embodiments

Embodiments of the present invention can also be realized by a computer of a system or apparatus that reads out and executes computer executable instructions (e.g., one or more programs) recorded on a storage
20 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 embodiments and/or that includes one or more circuits (e.g., application specific integrated circuit
25 (ASIC)) for performing the functions of one or more of the above-described embodiments, 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 embodiments and/or controlling the one or more circuits to perform the functions of one or more of the above-described embodiments. 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.

20 **[0123]** While the present invention has been described with reference to embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. It will be appreciated by those skilled in the art that various changes and
25 modification might be made without departing from the scope of the invention, as defined in the appended claims. All of the features disclosed in this

specification (including any accompanying claims,
abstract and drawings), and/or all of the steps of any
method or process so disclosed, may be combined in any
combination, except combinations where at least some of
5 such features and/or steps are mutually exclusive.

CLAIMS:

1. An information processing apparatus comprising:
a generator configured to generate a public key pair and generate a certificate signing request based
5 on the generated public key pair;
a transmitter configured to transmit an electronic certificate issuance request that includes the generated certificate signing request to an external apparatus;
10 a receiver configured to receive a response transmitted from the external apparatus as a response to the electronic certificate issuance request;
a first obtaining unit configured to obtain an electronic certificate included in the response
15 received by the receiver; and
a processor configured to cause an application to enable its use of the electronic certificate obtained by the first obtaining unit.
- 20 2. The apparatus according to claim 1, further comprising:
a verifying unit configured to authenticate an electronic signature included in the received response to verify whether the received response had been
25 transmitted by the external apparatus,
wherein the first obtaining unit is configured to obtain the electronic certificate included in the

received response depending on the outcome of the authentication by the verifying unit.

3. The apparatus according to claim 2, further
5 comprising:

a second obtaining unit configured to obtain a CA certificate from the external apparatus,

wherein the verifying unit is configured to perform the electronic signature authentication using
10 the CA certificate obtained by the second obtaining unit.

4. The apparatus according to any one of claims 1 to 3, wherein the receiver is configured to receive an
15 instruction for the transmission of the electronic certificate issuance request from a second information processing apparatus that is connected to the information processing apparatus via a communication network.

20

5. The apparatus according to claim 4, wherein:

the processor is configured to generate display control data for displaying a first user interface for receiving a user input; and

25 the transmitter is configured to transmit the generated display control data to the second information processing apparatus to cause the second

information processing apparatus to display the first user interface,

wherein the instruction for the transmission of the electronic certificate issuance request is transmitted by the second information processing apparatus in accordance with the user input received via the displayed first user interface.

6. The apparatus according to any preceding claim, wherein the processor is configured to:

generate connection setup display data for displaying a second user interface for receiving a user input;

cause the second user interface to be displayed so that the user input can be received via the second user interface; and

cause a connection with the external apparatus to be established in accordance with the received user input,

whereby the transmitter transmits the electronic certificate issuance request to the external apparatus with which the connection has been established.

7. The apparatus according to any preceding claim, wherein:

the processor is configured to cause the information processing apparatus to use the electronic

certificate in the application.

8. The apparatus according to any preceding claim, further comprising an updating unit configured to:

5 set an update time for updating the electronic certificate; and

at the set update time, update the electronic certificate by activating the transmitter, the receiver, and the first obtaining unit to transmit the
10 electronic certificate issuance request and obtain a second electronic certificate.

9. The apparatus according to claim 8, wherein the updating unit is configured to set the update time

15 based on at least one of: a date and a time; a number of days defining a time period before an expiry of the electronic certificate; and an update cycle.

10. A method of controlling an information processing apparatus configured to perform communication using an
20 electronic certificate, the method comprising:

generating a public key pair and generating a certificate signing request based on the generated public key pair;

25 transmitting an electronic certificate issuance request that includes the generated certificate signing request to an external apparatus;

receiving a response transmitted from the external apparatus as a response to the electronic certificate issuance request;

obtaining an electronic certificate included in the response received in the receiving; and

causing an application to enable its use of the electronic certificate obtained in the obtaining.

11. The method according to claim 10, further comprising:

authenticating an electronic signature included in the received response to verify whether the received response had been transmitted by the external apparatus,

wherein the obtaining the electronic certificate included in the received response is performed depending on the outcome of the authenticating.

12. The method according to claim 11, further comprising:

obtaining a CA certificate from the external apparatus,

wherein the authenticating of the electronic signature authentication is performed using the obtained CA certificate.

13. The method according to any one of claims 10 to

12, further comprising:

receiving an instruction for the transmitting of
the electronic certificate issuance request from a
second information processing apparatus that is
5 connected to the information processing apparatus via a
communication network.

14. The method according to claim 13, further
comprising:

10 generating display control data for displaying a
first user interface for receiving a user input; and
transmitting the generated display control data
to the second information processing apparatus to cause
the second information processing apparatus to display
15 the first user interface,

wherein the instruction for the transmitting of
the electronic certificate issuance request is
transmitted by the second information processing
apparatus in accordance with the user input received
20 via the displayed first user interface.

15. The method according to any one of claims 10 to
14, further comprising:

generating connection setup display data for
25 displaying a second user interface for receiving a user
input;

causing the second user interface to be displayed

so that the user input can be received via the second user interface; and

causing a connection with the external apparatus to be established in accordance with the received user
5 input,

whereby the transmitting of the electronic certificate issuance request is to the external apparatus with which the connection has been established.

10

16. The method according to any one of claims 10 to 15, further comprising:

causing the information processing apparatus to use the electronic certificate in the application.

15

17. The method according to any one of claims 10 to 16, further comprising:

setting an update time for updating the electronic certificate; and

20

at the set update time, updating the electronic certificate by performing the transmitting of the electronic certificate issuance request and obtaining a second electronic certificate.

25

18. An image forming apparatus comprising:

a management unit configured to manage an electronic certificate;

an update management unit configured to set an update rule selected from a plurality of update rules applicable to the electronic certificate managed by the management unit; and

5 a transmitter configured to transmit, based on the set update rule, an electronic certificate update request to an external apparatus.

19. The image forming apparatus according to claim 10 18, further comprising the information processing apparatus of any one of claims 1 to 9.

20. A method of controlling an image forming apparatus configured to perform communication using an 15 electronic certificate, the method comprising:

managing the electronic certificate;

setting an update rule selected from a plurality of update rules applicable to the managed electronic certificate; and

20 transmitting, based on the set update rule, an electronic certificate update request to an external apparatus.

21. The method according to claim 20, wherein the 25 image forming apparatus further comprises an information processing apparatus, and the method further comprises the method of controlling the

information processing apparatus according to any one of claims 10 to 17.

22. A system comprising at least one information processing apparatus of any one of claims 1 to 9, and an external apparatus comprising:

a receiver configured to receive the electronic certificate issuance request transmitted by the information processing apparatus;

10 a processor configured to process the received electronic certificate issuance request, obtain an electronic certificate and generate a response that includes the obtained electronic certificate; and

15 a transmitter configured to transmit the generated response to the information processing apparatus.

23. The system according to claim 22, wherein the processor of the external apparatus is configured to:

20 include an electronic signature in the transmitted response so that the information processing apparatus can verify the origin of the response.

24. The system according to claim 23, wherein the processor of the external apparatus is configured to:

generate a CA certificate and cause the transmitter to transmit the generated CA certificate to

the information processing apparatus so that the information processing apparatus can perform an electronic signature authentication using the CA certificate.

5

25. The system according to any one of claims 22 to 24, further comprising the image forming apparatus of claim 18 or 19.

10 26. A method of controlling a system comprising an external apparatus and at least one information processing apparatus configured to perform communication using an electronic certificate, the method comprising the method of controlling an
15 information processing apparatus according to any one of claims 10 to 17, and, at the external apparatus:

receiving the electronic certificate issuance request transmitted by the information processing apparatus;

20 processing the received electronic certificate issuance request, obtaining an electronic certificate and generating a response that includes the obtained electronic certificate; and

transmitting the generated response to the
25 information processing apparatus.

27. The method according to claim 26, further

comprising, at the external apparatus:

including an electronic signature in the transmitted response so that the information processing apparatus can verify the origin of the response.

5

28. The method according to claim 27, further comprising, at the external apparatus:

generating a CA certificate and causing to transmit the generated CA certificate to the information processing apparatus so that the information processing apparatus can perform an electronic signature authentication using the CA certificate.

10

29. The method according to any one of claims 26 to 28, wherein the system further comprises an image forming apparatus configured to perform communication using an electronic certificate, and the method further comprises the method of controlling the image forming apparatus according to claim 20 or 21.

15

20

30. A computer-readable storage medium storing a program for causing a processor to operate a method of any one of claims 10 to 17, 20, 21, or 26 to 29.

25



Application No: GB1802583.3
Claims searched: 1-17 and 22-30

Examiner: Adam Tucker
Date of search: 25 August 2018

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-17, 22-30	US 2014/0258709 A1 (Canon) See the whole document and in particular claims 1 & 8-10, paragraphs 44, 46-48, 51, 53, 58, 60 & 72 and the Figures
X	1-3, 7, 10-12, 16, 22-24, 26-30	US 2007/0168658 A1 (Canon) See the whole document and in particular the Figures and paragraphs 13-15, 100, 110
X	1-3, 7, 10-12, 16, 22-24 & 26-30	US 2013/0086377 A1 (Resch et al.) See the whole document and in particular Figures 11A & 11E and paragraphs 152, 153 & 162
X	1-7, 10-16, 22-24, 26-28 & 30 at least	US 2012/0023327 A1 (Nagasaki) See the whole document and in particular Figures 1 & 2 and paragraphs 49, 58-61 & 87

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^X :

--

Worldwide search of patent documents classified in the following areas of the IPC

G06F; H04L

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC



International Classification:

Subclass	Subgroup	Valid From
H04L	0009/32	01/01/2006
G06F	0021/44	01/01/2013
H04L	0029/06	01/01/2006
G06F	0021/45	01/01/2013
G06F	0021/60	01/01/2013
G06F	0021/64	01/01/2013