(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0095455
(43) 공개일자 2018년08월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 3/12* (2017.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
G06F 3/1238 (2013.01)
(21) 출원번호 10-2018-0017362
(22) 출원일자 2018년02월13일
심사청구일자 없음
(30) 우선권주장
JP-P-2017-028424 2017년02월17일 일본(JP)

(71) 출원인
캐논 가부시끼가이샤
일본 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
카쿠타니 나오야
일본국 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고 캐논 가부시끼가이샤 나이
야마우치 히사유키
일본국 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고 캐논 가부시끼가이샤 나이
(74) 대리인
권태복

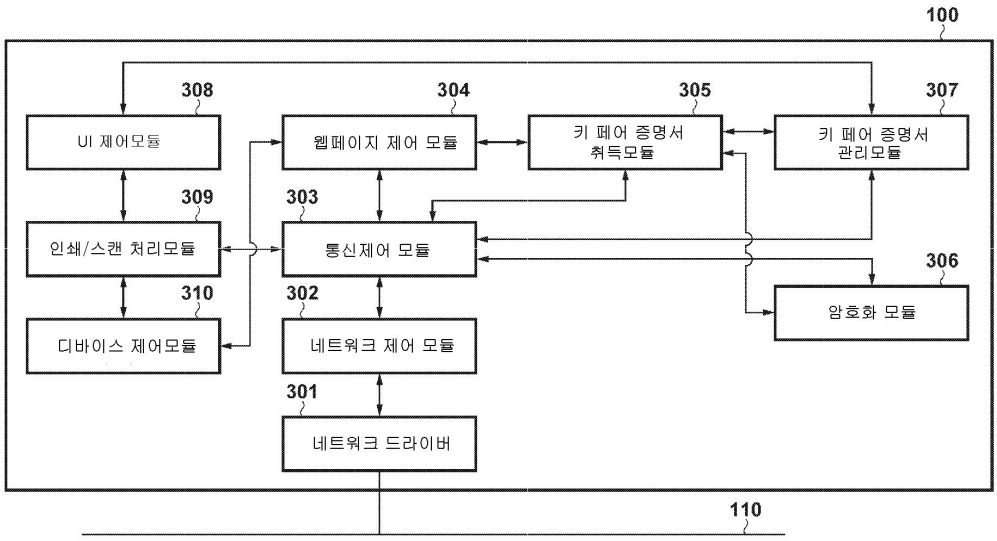
전체 청구항 수 : 총 29 항

(54) 발명의 명칭 **정보처리장치, 화상형성장치, 시스템, 그 제어 방법, 및 기억매체**

(57) 요 약

정보처리장치는, 증명서의 발행 요구에 따라 공개 키 페어를 생성하고, 해당 공개 키 페어에 근거하여 증명서의 서명 요구를 생성하여 외부장치에 송신한다. 정보처리장치는, 그 발행 요구에 대한 응답으로서 상기 외부장치로부터 증명서의 발행 요구의 결과 및 전자증명서를 취득하고, 그 취득한 전자증명서의 용도를 설정한다.

대 표 도



(52) CPC특허분류
G06F 3/1262 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/3247 (2013.01)

명 세 서

청구범위

청구항 1

공개 키 페어를 생성하고, 그 생성된 공개 키 페어에 근거해서 증명서의 서명 요구를 생성하는 생성부;

상기 생성된 증명서의 서명 요구를 포함하는 전자증명서의 발행 요구를 외부장치에 송신하는 송신부;

상기 전자증명서의 발행 요구에 대한 응답으로서 상기 외부장치로부터 송신된 응답을 수신하는 수신부;

상기 수신부에 의해 수신된 상기 응답에 포함된 전자증명서를 취득하는 제1 취득부; 및

상기 제1 취득부에 의해 취득된 상기 전자증명서의 사용을 용도(application)가 가능하게 하는 프로세서를 구비하는, 정보처리장치.

청구항 2

제 1 항에 있어서,

상기 수신된 응답을 상기 외부장치가 송신하였는지를 검증하기 위해 상기 수신된 응답에 포함된 전자서명을 인증하는 검증부를 더 구비하고,

상기 제1 취득부는 상기 검증부에 의한 상기 인증의 결과에 따라 상기 수신된 응답에 포함된 상기 전자증명서를 취득하는, 정보처리장치.

청구항 3

제 2 항에 있어서,

상기 외부장치로부터 CA증명서를 취득하는 제2 취득부를 더 구비하고,

상기 검증부는, 상기 제2 취득부가 취득한 상기 CA증명서를 사용하여 상기 전자서명의 인증을 행하는, 정보처리장치.

청구항 4

제 1 항에 있어서,

상기 수신부는, 상기 전자증명서의 발행 요구를 송신하기 위한 지시를, 상기 정보처리장치에 통신 네트워크를 통해 접속된 제2 정보처리장치로부터 수신하는, 정보처리장치.

청구항 5

제 4 항에 있어서,

상기 프로세서는, 유저 입력을 수신하기 위한 제1 유저 인터페이스를 표시하는 표시 제어 데이터를 생성하고,

상기 송신부는, 상기 제2 정보처리장치가 상기 제1 유저 인터페이스를 표시하게 하기 위해, 상기 생성된 표시 제어 데이터를 상기 제2 정보처리장치에 송신하고,

상기 전자증명서의 발행 요구를 송신하기 위한 상기 지시는, 상기 표시된 제1 유저 인터페이스를 통해 수신된 상기 유저 입력에 따라 상기 제2 정보처리장치에 의해 송신되는, 정보처리장치.

청구항 6

제 1 항에 있어서,

상기 프로세서는,

유저 입력을 수신하기 위한 제2 유저 인터페이스의 표시를 위한 접속 설정 표시 데이터를 생성하고,

상기 제2 유저 인터페이스를 거쳐 상기 유저 입력을 수신할 수 있도록, 상기 제2 유저 인터페이스를 표시시키고,

상기 수신된 유저 입력에 따라 상기 외부장치와의 접속을 확립시킴에 따라서,

상기 송신부는, 상기 전자증명서의 발행 요구를, 상기 접속을 확립시킨 상기 외부장치에 송신하는, 정보처리장치.

청구항 7

제 1 항에 있어서,

상기 프로세서는, 상기 정보처리장치가 상기 전자증명서를 상기 용도에서 사용하게 하는, 정보처리장치.

청구항 8

제 1 항에 있어서,

상기 전자증명서를 갱신하는 갱신 시간을 설정하고,

상기 설정된 갱신 시간에, 상기 송신부, 상기 수신부 및 상기 제1취득부를 기동하여서 상기 전자증명서의 발행 요구를 송신하고 제2 전자증명서를 취득함으로써, 상기 전자증명서를 갱신하는,

갱신부를 더 구비하는, 정보처리장치.

청구항 9

제 8 항에 있어서,

상기 갱신부는, 일시; 상기 전자증명서의 만기전의 기간을 규정하는 일수; 및 갱신 주기 중, 적어도 하나에 근거하여 상기 갱신 시간을 설정하는, 정보처리장치.

청구항 10

전자증명서를 사용하여 통신을 행하는 정보처리장치의 제어방법으로서,

공개 키 페어를 생성하고, 그 생성된 공개 키 페어에 근거해서 증명서의 서명 요구를 생성하는 단계;

상기 생성된 증명서의 서명 요구를 포함하는 전자증명서의 발행 요구를 외부장치에 송신하는 단계;

상기 전자증명서의 발행 요구에 대한 응답으로서 상기 외부장치로부터 송신된 응답을 수신하는 단계;

상기 수신하는 단계에서 수신된 상기 응답에 포함된 전자증명서를 취득하는 단계; 및

상기 취득하는 단계에서 취득된 상기 전자증명서의 사용을 용도가 가능하게 하는 단계를 포함하는, 정보처리장치의 제어방법.

청구항 11

제 10 항에 있어서,

상기 수신된 응답을 상기 외부장치가 송신하였는지를 검증하기 위해 상기 수신된 응답에 포함된 전자서명을 인증하는 단계를 더 포함하고,

상기 수신된 응답에 포함된 상기 전자증명서를 취득하는 단계는, 상기 인증하는 단계의 결과에 따라 행해지는, 정보처리장치의 제어방법.

청구항 12

제 11 항에 있어서,

상기 외부장치로부터 CA증명서를 취득하는 단계를 더 포함하고,

상기 전자서명 인증의 상기 인증하는 단계는, 상기 취득된 CA증명서를 사용하여 행해지는, 정보처리장치의 제어방법.

청구항 13

제 10 항에 있어서,

상기 전자증명서의 발행 요구를 송신하기 위한 지시를, 상기 정보처리장치에 통신 네트워크를 통해 접속된 제2 정보처리장치로부터 수신하는 단계를 더 포함하는, 정보처리장치의 제어방법.

청구항 14

제 13 항에 있어서,

유저 입력을 수신하기 위한 제1 유저 인터페이스를 표시하는 표시 제어 데이터를 생성하는 단계; 및

상기 제2 정보처리장치가 상기 제1 유저 인터페이스를 표시하게 하기 위해, 상기 생성된 표시 제어 데이터를 상기 제2 정보처리장치에 송신하는 단계를 더 포함하고,

상기 전자증명서의 발행 요구를 송신하기 위한 상기 지시는, 상기 표시된 제1 유저 인터페이스를 통해 수신된 상기 유저 입력에 따라 상기 제2 정보처리장치에 의해 송신되는, 정보처리장치의 제어방법.

청구항 15

제 10 항에 있어서,

유저 입력을 수신하기 위한 제2 유저 인터페이스의 표시를 위한 접속 설정 표시 데이터를 생성하는 단계;

상기 제2 유저 인터페이스를 거쳐 상기 유저 입력을 수신할 수 있도록, 상기 제2 유저 인터페이스를 표시시키는 단계; 및

상기 수신된 유저 입력에 따라 상기 외부장치와의 접속을 확립시키는 단계를 더 포함함에 따라서,

상기 전자증명서의 발행 요구를, 상기 접속을 확립시킨 상기 외부장치에 송신하는, 정보처리장치의 제어방법.

청구항 16

제 10 항에 있어서,

상기 정보처리장치가 상기 전자증명서를 상기 용도에서 사용하게 하는 단계를 더 포함하는, 정보처리장치의 제

어방법.

청구항 17

제 10 항에 있어서,

상기 전자증명서를 갱신하는 갱신 시간을 설정하는 단계; 및

상기 설정된 갱신 시간에, 상기 전자증명서의 발행 요구를 송신하고 제2 전자증명서를 취득함으로써, 상기 전자증명서를 갱신하는 단계를 더 포함하는, 정보처리장치의 제어방법.

청구항 18

전자증명서를 관리하는 관리부;

상기 관리부가 관리한 상기 전자증명서에 적용가능한 복수의 갱신 룰로부터 선택된 갱신 룰을 설정하는 갱신 관리부; 및

상기 설정된 갱신 룰에 근거하여, 전자증명서의 갱신 요구를 외부장치에 송신하는 송신부를 구비하는, 화상형성장치.

청구항 19

제 18 항에 있어서,

청구항 1 내지 9 중 어느 한 항의 상기 정보처리장치를 더 구비하는, 화상형성장치.

청구항 20

전자증명서를 사용하여 통신을 행하는 화상형성장치의 제어방법으로서,

상기 전자증명서를 관리하는 단계;

상기 관리한 상기 전자증명서에 적용가능한 복수의 갱신 룰로부터 선택된 갱신 룰을 설정하는 단계; 및

상기 설정된 갱신 룰에 근거하여, 전자증명서의 갱신 요구를 외부장치에 송신하는 단계를 포함하는, 화상형성장치의 제어방법.

청구항 21

청구항 1 내지 9 중 어느 한 항의 적어도 하나의 정보처리장치와, 외부장치를 구비하는, 시스템으로서, 상기 외부장치가,

상기 정보처리장치가 송신한 상기 전자증명서의 발행 요구를 수신하는 수신부;

상기 수신된 전자증명서의 발행 요구를 처리하고, 전자증명서를 취득하고, 이 취득된 전자증명서를 포함하는 응답을 생성하는 프로세서; 및

상기 생성된 응답을 상기 정보처리장치에 송신하는 송신부를 구비하는, 시스템.

청구항 22

제 21 항에 있어서,

상기 외부장치의 상기 프로세서는,

상기 정보처리장치가 상기 응답의 기점을 검증할 수 있도록 상기 송신된 응답에 전자서명을 포함하는, 시스템.

청구항 23

제 22 항에 있어서,

상기 외부장치의 상기 프로세서는,

CA증명서를 생성하고, 상기 송신부에 의해, 상기 정보처리장치가 상기 CA증명서를 사용하여 전자서명 인증을 행할 수 있도록 상기 생성된 CA증명서를 상기 정보처리장치에 송신시키는, 시스템.

청구항 24

제 21 항에 있어서,

청구항 18의 상기 화상형성장치를 더 구비하는, 시스템.

청구항 25

전자증명서를 사용하여 통신을 행하는 외부장치와 적어도 하나의 정보처리장치를 구비하는 시스템의 제어방법으로서, 상기 방법은, 청구항 10 내지 17 중 어느 한 항에 따른 정보처리장치의 제어방법과, 상기 외부장치에서:

상기 정보처리장치가 송신한 상기 전자증명서의 발행 요구를 수신하는 단계;

상기 수신된 전자증명서의 발행 요구를 처리하고, 전자증명서를 취득하고, 이 취득된 전자증명서를 포함하는 응답을 생성하는 단계; 및

상기 생성된 응답을 상기 정보처리장치에 송신하는 단계를 포함하는, 시스템의 제어방법.

청구항 26

제 25 항에 있어서,

상기 외부장치에서:

상기 정보처리장치가 상기 응답의 기점을 검증할 수 있도록 상기 송신된 응답에 전자서명을 포함하는 단계를 더 포함하는, 시스템의 제어방법.

청구항 27

제 26 항에 있어서,

상기 외부장치에서:

CA증명서를 생성하고, 상기 정보처리장치가 상기 CA증명서를 사용하여 전자서명 인증을 행할 수 있도록 상기 생성된 CA증명서를 상기 정보처리장치에 송신시키는 단계를 더 포함하는, 시스템의 제어방법.

청구항 28

제 25 항에 있어서,

상기 시스템은 전자증명서를 사용하여 통신을 행하는 화상형성장치를 더 구비하고, 상기 방법은 청구항 20에 따

른 상기 화상형성장치의 제어방법을 더 포함하는, 시스템의 제어방법.

청구항 29

프로세서에, 청구항 10 내지 17, 청구항 20, 또는 청구항 25 내지 28 중 어느 한 항의 방법을 실행시키기 위한 프로그램을 기억하는, 컴퓨터 판독 가능한 기억매체.

발명의 설명

기 술 분 야

[0001] 본 발명은, 정보처리장치, 화상형성장치, 시스템, 그 제어 방법, 및 기억매체에 관한 것이다.

배 경 기 술

[0002] 오피스 등의 네트워크에 접속하는 퍼스널 컴퓨터(PC)나, 개인이 소지하는 휴대 단말은, 외부의 서버와 통신할 때, 시큐어(secure) 통신과 인증을 행하기 위해서, 공개 키 증명서(예를 들면, 디지털 증명서)를 이용한다.

[0003] 최근에, 복합기는, 단순히 화상의 인쇄와 송신을 행할 뿐만 아니라, 그 복합기내에 화상 데이터를 격납하여서 PC에 대하여 파일 저장 서비스를 제공하는 기능을 갖고도 있다. 그 때문에, 복합기는, 네트워크상에 존재하는 그 밖의 서버 기기와 같은 정보처리장치로서의 역할을 하게 되어 있다. 이것들의 정보처리장치가 네트워크상에서 이용되는 동안에, 안전하고 안심한 오피스 환경을 유지하기 위해서는, 전자증명서(즉, 디지털 증명서)를 사용한 인증에 의거한 통신이 요구된다. 일반적으로, 이 전자증명서를 사용한 공개 키 기반(PKI: public key infrastructure)에 근거한 기술을 사용하여서 보다 안전한 네트워크의 식별과 인증이 실현되어 있다(RFC3647: Internet X.509 Public Key Infrastructure Certificate Polity and Certificate Practices Framework 참조).

[0004] 예를 들면, 정보처리장치가 클라이언트가 될 경우, 서버로부터 서버 공개 키 증명서와, 그 서버 공개 키 증명서를 발행할 때 사용된 인증국(CA: Certificate Authority)의 증명서를 취득하여서 서버의 인증성을 검증할 수 있다. 클라이언트(예를 들면, 정보처리장치)의 클라이언트 공개 키 증명서를 서버에 제공함으로써, 서버가 클라이언트의 인증성을 검증하는 것도 가능해진다. 추가로, 정보처리장치가 서버가 될 경우, 접속하는 클라이언트에 대하여, 정보처리장치의 서버 공개 키 증명서를 배포하는 것에 의해, 클라이언트가 그 서버인 정보처리장치의 인증성을 검증할 수 있다. 이렇게, 전자증명서는, 정보처리장치들이 네트워크 통신/환경의 인증/검증과 식별을 행하는 중요한 툴로서 이용되고 있다. 예를 들면, SSL, TLS, IEEE802.1X 및 IPSEC는, 이러한 전자증명서 기반 시큐어 통신에 이용되는 통신 프로토콜의 일부다.

[0005] 전자증명서가 정보처리장치내에 격납/보유될 필요가 있으므로, 종래는, 인증국이 발행한 전자증명서는, 정보처리장치의 유저가 수동으로 정보처리장치의 스토리지에 격납되었다. 이 격납방법은, 전자증명서를 발행하는 인증국으로부터 전자증명서를 다운로드하거나, USB메모리등의 외부 스토리지로부터 전자증명서를 복사하거나, 또는 이메일을 통해 수신한 전자증명서를 소정의 폴더에 복사하여서 행해진다.

[0006] 별도의 전자증명서는, 통신의 실제 구현에 따라서, 정보처리장치마다 이용되어도 된다. 예를 들면, IEEE802.1X 등이 그 통신을 위해 적용될 때, 클라이언트를 인증하기 위해서, 정보처리장치마다 개별적으로 전자증명서가 격납되는 것이 일반적이다. 또한, 전자증명서는, 유효기간(즉, 그 전자증명서가 인증/검증을 위해 더 이상 유효하지 않고/이용 가능하지 않은 시간의 기간 또는 일/시)을 갖고, 그 유효기간이 만료하면 그 전자증명서를 사용한 통신이 불가능하게 된다. 그 때문에, 유효기간이 만료하거나 또는 그 만료 전(바람직하게는 직전에) 기기(이를테면, 그 정보처리장치)내에 격납된 전자증명서를 갱신할 필요가 있다. 게다가, 전자증명서를 이용할 때, 각 정보처리장치에 의해 사용될 TLS나 IEEE802.1X 등의 각 통신의 용도(application)에 부합되게 사용될 각 전자증명서를 수동으로 설정하는 것이 필요하다.

[0007] 그러나, 전자증명서를 다루는/필요로 하는 정보처리장치가 대량으로 존재할 경우, 유저가 이들 정보처리장치의 각각에 대하여 각 전자증명서를 수동으로 추가, 갱신 및 설정해야 하면, 이것은, 유저에 있어서 작업량/부담이 과중될 수 있고 너무 많은 시간이 걸릴 수 있다.

발명의 내용

[0008] 본 발명의 일 측면은 종래기술이 갖는 상술한 과제를 해결하거나 적어도 그 과제로부터 일어나는 불리한 효과를

적어도 감소시키는 데에 있다.

[0009] 본 발명의 일 특징은, 정보처리장치에 있어서의 전자증명서의 추가와 갱신을 쉽게 하는 기술/메카니즘을 제공하는 데에 있다.

[0010] 본 발명의 제1 측면에서는, 공개 키 페어를 생성하고, 그 생성된 공개 키 페어에 근거해서 증명서의 서명 요구를 생성하는 생성부; 상기 생성된 증명서의 서명 요구를 포함하는 전자증명서의 발행 요구를 외부장치에 송신하는 송신부; 상기 전자증명서의 발행 요구에 대한 응답으로서 상기 외부장치로부터 송신된 응답을 수신하는 수신부; 상기 수신부에 의해 수신된 상기 응답에 포함된 전자증명서를 취득하는 제1 취득부; 및 상기 제1 취득부에 의해 취득된 상기 전자증명서의 사용을 용도(application)가 가능하게 하는 프로세서를 구비하는, 정보처리장치를 제공한다.

[0011] 본 발명의 제2 측면에서는, 전자증명서를 사용하여 통신을 행하는 정보처리장치의 제어방법을 제공하고, 이 방법은, 공개 키 페어를 생성하고, 그 생성된 공개 키 페어에 근거해서 증명서의 서명 요구를 생성하는 단계; 상기 생성된 증명서의 서명 요구를 포함하는 전자증명서의 발행 요구를 외부장치에 송신하는 단계; 상기 전자증명서의 발행 요구에 대한 응답으로서 상기 외부장치로부터 송신된 응답을 수신하는 단계; 상기 수신하는 단계에서 수신된 상기 응답에 포함된 전자증명서를 취득하는 단계; 및 상기 취득하는 단계에서 취득된 상기 전자증명서의 사용을 용도가 가능하게 하는 단계를 포함한다.

[0012] 본 발명의 제3 측면에서는, 전자증명서를 관리하는 관리부; 상기 관리부가 관리한 상기 전자증명서에 적용가능한 복수의 갱신 룰로부터 선택된 갱신 룰을 설정하는 갱신 관리부; 및 상기 설정된 갱신 룰에 근거하여, 전자증명서의 갱신 요구를 외부장치에 송신하는 송신부를 구비하는, 화상형성장치를 제공한다.

[0013] 본 발명의 제4 측면에서는, 전자증명서를 사용하여 통신을 행하는 화상형성장치의 제어방법을 제공하고, 이 방법은, 상기 전자증명서를 관리하는 단계; 상기 관리한 상기 전자증명서에 적용가능한 복수의 갱신 룰로부터 선택된 갱신 룰을 설정하는 단계; 및 상기 설정된 갱신 룰에 근거하여, 전자증명서의 갱신 요구를 외부장치에 송신하는 단계를 포함한다.

[0014] 본 발명의 제5 측면에서는, 청구항 1 내지 9 중 어느 한 항의 적어도 하나의 정보처리장치와, 외부장치를 구비하는 시스템을 제공하고, 상기 외부장치가, 상기 정보처리장치가 송신한 상기 전자증명서의 발행 요구를 수신하는 수신부; 상기 수신된 전자증명서의 발행 요구를 처리하고, 전자증명서를 취득하고, 이 취득된 전자증명서를 포함하는 응답을 생성하는 프로세서; 및 상기 생성된 응답을 상기 정보처리장치에 송신하는 송신부를 구비한다.

[0015] 본 발명의 제6 측면에서는, 전자증명서를 사용하여 통신을 행하는 외부장치와 적어도 하나의 정보처리장치를 구비하는 시스템의 제어방법을 제공하고, 상기 시스템의 제어방법은, 청구항 10 내지 17 중 어느 한 항에 따른 정보처리장치의 제어방법과, 상기 외부장치에서: 상기 정보처리장치가 송신한 상기 전자증명서의 발행 요구를 수신하는 단계; 상기 수신된 전자증명서의 발행 요구를 처리하고, 전자증명서를 취득하고, 이 취득된 전자증명서를 포함하는 응답을 생성하는 단계; 및 상기 생성된 응답을 상기 정보처리장치에 송신하는 단계를 포함한다.

[0016] 본 발명의 또 다른 특징들, 측면들 및 이점들은, 첨부도면을 참조하여 이하의 실시예들의 설명으로부터 명백해질 것이다. 후술한 본 발명의 각 실시예는, 단독으로 구현될 수 있거나, 복수의 실시예들의 조합으로서 구현될 수 있다. 또한, 다른 실시예들로부터의 특징들은, 필요한 경우, 또는 단일의 실시예에서 개개의 실시예로부터의 요소들 또는 특징들의 조합이 이로울 경우, 조합될 수 있다.

[0017] 본 명세서의 일부에 포함되고 그 일부를 구성하는 첨부도면들은, 본 발명의 실시예들을 예시하고, 이 설명과 함께, 본 발명의 원리를 설명하는 역할을 한다.

도면의 간단한 설명

[0018] 도 1은, 본 발명의 제1실시예에 따른 네트워크 구성 또는 시스템을 도시하는 블록도;

도 2는, 제1실시예에 따른 복합기의 하드웨어 구성을 도시하는 블록도;

도 3은, 제1실시예에 따른 복합기상에서 동작하는 프로그램에 구비되는 소프트웨어 모듈을 도시하는 블록도;

도 4a, 4b는, 제1실시예에 따른 네트워크 구성 또는 시스템상에 동작하는 전체 처리의 시퀀스를 도시하는 시퀀스 도;

도 5a는, 제1실시예에 따른 복합기에 의한, 도 4a의 단계 S402의 키 페어(pair)/전자증명서의 리스트의 취득

및 표시 데이터의 작성 처리를 도시하는 흐름도;

도 5b는, 제1실시예에 따른 복합기가, PC로부터 송신된 상세정보 표시 요구를 수신할 때 행해진 처리를 도시하는 흐름도;

도 6은, 제1실시예에 따른 복합기에 의해 행해진, 도 4a의 단계 S407의 인증국/등록국과의 접속을 확립하는 접속 셋업 처리를 도시하는 흐름도;

도 7은, 제1실시예에 따른 복합기에 의해 행해진, 도 4a의 단계 S412 내지 단계 S416에서의 인증국(CA) 증명서 취득/등록 처리를 도시하는 흐름도;

도 8a, 8b는, 제1실시예에 따른 복합기에 의해 행해진, 도 4b의 단계 S419 내지 단계 S424의 증명서의 발행 요구/취득 처리를 도시하는 흐름도;

도 9는, 제1실시예에 따른 복합기에 의해 행해진, 도 4b의 단계 S424 내지 단계 S427의 복합기의 재기동에 관한 처리를 도시하는 흐름도;

도 10a, 10b, 도 11a, 11b, 도 12a, 12b, 도 13a, 13b, 도 14a, 14b, 및 도 15는, 제1실시예에 따른 PC에 표시되는 리모트 유저 인터페이스(RUI)의 웹(Web) 페이지 화면의 예들을 도시하는 화면 뷰;

도 16은, 제1실시예에 따른 PC에 표시되는 전자증명서의 상세정보의 일례를 도시하는 화면 뷰;

도 17a~17c는, 제1실시예에 따른 복합기의 키 페어 증명서 관리모듈이 관리하고 있는 키 페어/전자증명서의 상세정보 데이터베이스의 개념도;

도 18은, 제2실시예에 따른 복합기에 의해 제공된 전자증명서의 갱신 예약 설정 화면의 일례를 도시하는 도;

도 19는, 제2실시예에 따른 복합기에 설정된, 전자증명서의 갱신 예약 설정에 근거하여 전자증명서의 자동갱신 기능을 실행/수행할 때에 행해진 처리를 도시하는 흐름도다.

발명을 실시하기 위한 구체적인 내용

[0019] 이후, 본 발명의 실시예들을 첨부도면들을 참조하여 상세히 설명한다. 이하의 실시예들은 본 발명의 청구항에 한정하는 것이 아니고, 또 이하의 실시예들에 따라 설명되어 있는 측면들의 조합의 모두가 본 발명에 따른 과제를 해결하는 수단에 대해 반드시 필요한 것은 아니라는 것을 알 것이다. 한편, 상기 실시예들에 따른 전자증명서를 이용 및 관리하는 정보처리장치의 일례로서, 복합기(디지털 복합기/MFP)를 설명한다. 그렇지만, 본 발명은 상기 복합기에 한정되지 않고, 본 발명은, 전자증명서가 이용 또는 관리될 수 있는 정보처리장치이면, 어떠한 기기 또는 그 구성요소에도 적용 가능하다.

[0020] [제1실시예]

[0021] 도 1은, 본 발명의 제1실시예에 따른 네트워크 구성(또는 시스템)을 설명하는 블록도다.

[0022] 인쇄 기능을 갖는 복합기(100)는, 네트워크(110)를 통해서 다른 정보처리장치와 인쇄 데이터, 스캔한 화상 데이터, 디바이스의 관리 정보 등을 교환할 수 있다. 복합기(100)는, 트랜스포트층 보안(TLS), 인터넷 프로토콜 보안(IPSEC), IEEE802.1X등의 통신/암호화 프로토콜을 이용한 암호화 통신을 행할 수 있고, 이들의 암호처리를 행하는데 사용되는 공개 키 페어와 전자증명서(즉, 디지털 증명서)를 보유(예를 들면, 보존 또는 관리)한다. 여기서, 복합기(100)는 화상형성장치의 일례이어도 된다. 이러한 화상형성장치는, 이 복합기에 한정되지 않고, 팩시밀리 장치, 프린터 또는 카피기로서만 기능하는 장치이어도 되거나, 혹은 이들의 단일 기능 장치들의 임의의 조합으로서 기능하는 장치이어도 된다는 것을 알 것이다. 네트워크(110)에는, 다른 복합기101도 접속되어 있고, 이 제2 복합기101은, 복합기100와 동등한 기능을 가지고 있거나, 그 기능들의 적어도 일부를 공유하여도 된다. 이하, 복합기100만을 주로 설명하지만, 전자증명서의 교환/통신은 복수대의 복합기 중에서/에 대해 행해져도 되는 것을 알 것이다.

[0023] 인증국/등록국(102)은, 전자증명서를 발행하는 인증국(CA)의 기능과, 전자증명서의 발행 요구를 (검증/인증을 포함하는 일부의 경우에,) 접수하고, 그 접수된 요구에 근거한 등록 처리를 행하는 등록국(RA)의 기능을 가진다. 다시 말해, 이 인증국/등록국(102)은, 예를 들면, 네트워크(110)를 통해 (예를 들면, 서버에 CA전자 서명을 인증하기 위한) CA증명서를 배포하고 (예를 들면, 보안 통신을 확립하기 위한) 전자증명서를 발행/등록하는 기능을, 수행하는 (정보처리장치의 일례인) 서버 장치다. 제1실시예에서는, 네트워크(110)의 통신 프로토콜로서, SCEP(Simple Certificate Enrollment Protocol)를 이용하는 것으로 가정한다. 그렇지만, 전자증명서를

발행/관리하는 각종 프로토콜들이, 대응한 기능들을 제공할 수 있으면 상기 제1실시예의 네트워크 구성으로 사용되어도 되는 것을 알 것이다. 복합기(100)등의 정보처리장치는, 이 SCEP를 이용하여, 네트워크(110)를 통해 전자증명서의 발행 요구를 송신하고, 그 발행된 전자증명서를 취득하기 위해 상기 인증국/등록국(102)과 통신한다. 제1실시예에 따른 복합기(100)는, 웹 서버 기능을 갖고, 전자증명서의 발행 요구 및 취득(획득)을 위한 처리를 실행/수행하는데 사용될 수 있는 웹 페이지형의 리모트 유저 인터페이스(RUI) 기능을 네트워크(110)에 공개할 수 있다.

[0024] 인증국/등록국(102)은, 네트워크(110)를 통해 정보처리장치로부터 전자증명서의 발행 요구를 수신하면, 그 수신된 발행 요구에 근거하는 전자증명서의 발행과 등록 처리를 행하고, 발행된 전자증명서를, 그 발행 요구의 응답으로서 송신한다. 한편, 이 제1실시예에서는, CA와 RA의 기능이 동일한 서버 장치로 실현되지만, 본 발명은, 이것에 한정되지 않는다. 또한, 상기 CA와 상기 RA가 별도의 서버 장치, 예를 들면 CA서버와 별도의 RA 서버에 의해 실현되는 구성을 채택하는 것도 가능하다. 추가로, 제1실시예에서는 전자증명서의 발행 요구를 하고 그 발행된 전자증명서를 취득하는 프로토콜로서 SCEP를 이용하고 있지만, 동등한 또는 호환 가능한 기능을 갖는 프로토콜이 채택되는 한, 본 발명은 이것에 한정되지 않는다. 예를 들면, CMP(Certificate Management Protocol)나 EST(Enrollment over Secure Transport) 등의 프로토콜을 사용하는 것이 가능하다.

[0025] PC(103)는 퍼스널 컴퓨터다. PC(103)는 웹 브라우저 기능을 갖는다. 이것은, 네트워크(110)에 접속된 정보처리장치가 공개하고 있는 HTML문서와 웹사이트를 열람 및 이용하는 것이 가능하다(즉, 유저나 정보처리장치를 가능하게 한다). 여기서는 상기 PC(103)를 도시/설명하였지만, 웹브라우저 기능을 제공하거나, 정보를 표시하고 유저 입력을 수신할 수 있는 어떠한 기기/단말(예를 들면, 그 중에서도 타블렛, 휴대폰, 웨어러블 기술 기반 기기)은, 대신에 상기 네트워크(110)상의 상기 정보처리장치와 통신 가능하면 사용될 수도 있다는 것을 알 것이다.

[0026] 다음에, 제1실시예에 따른 전자증명서의 취득 및 갱신의 처리 개요를 설명한다.

[0027] 복합기(100)의 관리자는, PC(103)에 설치된 웹브라우저를 이용하여, 복합기(100)가 (예를 들면, 공개함으로써) 액세스 가능한 전자증명서의 발행 요구 및 취득을 위해 웹 페이지에 접속한다. 그 관리자는, 전자증명서의 발행 요구 및 취득을 위한 처리(즉, 전자증명서 발행 요구 및 취득/획득 처리)를 실행하는 설정과 지시를 설정하기 위해 그 웹 페이지를 사용한다. 복합기(100)는, 상기 관리자가 설정한 설정 및 지시(예를 들면, 웹 페이지를 통해 지시된 것과 같은 정보/내용)에 따라서, 인증국/등록국(102)에 대하여 SCEP에 의한 CA증명서의 취득 요구(획득 요구) 및 전자증명서의 발행 요구를 행한다(즉, 생성한다). 또, 복합기(100)는, 전자증명서의 발행 요구의 응답에 포함되는 것처럼 인증국/등록국(102)에 의해 발행되는 전자증명서를 취득한다. 그 후, 복합기(100)는, 그 취득한 전자증명서를 복합기(100)에서 이용하기 위한 설정 동작(즉, 셋업 또는 초기화 동작)을 행한다.

[0028] 다음에, 제1실시예에 따른 복합기(100)의 하드웨어 구성을 설명한다.

[0029] 도 2는, 제1실시예에 따른 복합기(100)의 하드웨어 구성을 도시하는 블록도다.

[0030] CPU(201)는, 복합기(100)의 소프트웨어 프로그램을 실행하여, 장치 전체를 제어/동작시킨다. ROM(202)은 판독전용 메모리이고, 복합기(100)의 동작을 위해 부트 프로그램이나 고정 파라미터 등을 격납하고 있다. RAM(203)은 랜덤 액세스 메모리이고, CPU(201)가 복합기(100)를 제어할 때/동작시킬 때에, 프로그램들과 일시적 데이터를 격납하는데 사용된다. HDD(204)는 하드 디스크 드라이브이고, 시스템 소프트웨어, 애플리케이션, 및 다른 각종 데이터를 격납한다. CPU(201)는, ROM(202)에 격납된 부트 프로그램을 실행하고, HDD(204)에 격납된 프로그램을 RAM(203)에 전개(deploy)하고, 그 전개된 프로그램을 실행함에 의해, 이 복합기(100)의 동작을 제어한다. 네트워크 인터페이스 제어부(205)는, 네트워크(110)와 복합기(100)간의 데이터 교환을 제어한다. 입력 인터페이스 제어부(예를 들면, 스캐너 인터페이스 제어부206)는, 스캐너(211) 등의 입력기기에 의해 행해진 화상 데이터 획득(예를 들면, 원고의 스캐닝 또는 판독)을 제어한다. 출력 인터페이스 제어부(예를 들면, 프린터 인터페이스 제어부207)는, 프린터(210) 등의 출력에 의해 행해진 데이터 출력(예를 들면, 인쇄 처리)을 제어한다. 표시 제어부(예를 들면, 패널 제어부208)는, 표시 디바이스 및 입력디바이스(예를 들면, 터치패널식의 조작 패널212)를 제어하여, 각종 정보의 표시와 사용자에 의한 지시 입력의 수신/처리를 제어한다. CPU(201), ROM(202), RAM(203), HDD(204), 네트워크 인터페이스 제어부(205), 스캐너 인터페이스 제어부(206), 프린터 인터페이스 제어부(207), 및 패널 제어부(208)는 서로 통신 가능하고, 예를 들면, 그들은 버스(209)에 의해 서로 접속된다. 이 버스(209)를 통하여, CPU(201)로부터의 제어 신호들과 상기 장치의 다른 구성요소간의 데이터 신호들이 교환/통신된다.

[0031] 도 3은, 제1실시예에 따른 복합기(100)상에서 실행 또는 동작되는 프로그램들(의 기능적 구성요소 등)에 구비된 소프트웨어 모듈을 설명하는 블록도다. 한편, 도 3에 도시된 소프트웨어 모듈은, 예를 들면, CPU(201)에 의해 RAM(203)에 프로그램을 전개하고 그 전개된 프로그램을 실행 함에 의해 실현된다.

[0032] 네트워크 드라이버(301)는, 네트워크(110)에 접속된 네트워크 인터페이스 제어부(205)를 제어하여, 네트워크(110)를 통해 외부와 데이터를 교환(즉, 통신)한다. 네트워크 제어모듈(302)은, TCP/IP등의 네트워크 통신 프로토콜에 있어서의 트랜스포트층이하의 통신을 제어하여서 데이터의 교환을 행한다. 통신 제어모듈(303)은, 복합기(100)가 서포트하는 복수의 통신 프로토콜을 제어(및 구현)하기 위한 모듈이다. 제1실시예에 따른 전자증명서의 취득 및 갱신 처리에서는, 통신 제어모듈(303)이 HTTP프로토콜 통신 요구를 행하고(예를 들면, 생성 및 송신하고), 응답 데이터를 생성하고, 해석을 행하고, 데이터의 교환을 제어하고, 인증국/등록국(102) 및/또는 PC(103)와의 통신을 위한 처리들을 실행한다. 또, 통신 제어모듈(303)은, 복합기(100)가 서포트하는 경우, TLS, IPSEC, IEEE802.1X를 사용하여 암호화 통신을 (예를 들면, 적절한 처리들/프로그램들을 실행함으로써) 행할 수 있다.

[0033] 웹 페이지 제어모듈(304)은, 전자증명서의 발행 요구와 그 취득 처리를 (예를 들면, 적절한 프로그램을 실행함으로써) 지시/실행하는 것이 가능한 웹 페이지의 표시를 위한 HTML데이터의 생성 및 통신 제어를 행하는 모듈이다. 웹 페이지 제어모듈(304)은, 네트워크 드라이버(301)를 거쳐 통신 제어모듈(303)과 송/수신함으로써 웹 페이지의 표시 요구, 전자증명서의 발행 요구, 및 그 발행된 전자증명서의 취득을 실행/가능하게 하는 지시를 위한 처리를 실행/수행한다. 웹 페이지 제어모듈(304)은, RAM(203)과 HDD(204)에 기억된 소정의 웹 페이지의 HTML데이터, 또는 표시 요구(예를 들면, 전자증명서의 상세한 정보를 표시하기 위한 요구)의 내용에 따라 생성된 HTML데이터를, 웹브라우저(상에서 이루어진 입력을 사용하여)로부터 이루어진 요구에 대한 응답으로서 송신한다.

[0034] 키 페어 증명서 취득 모듈(305)은, 그 웹 페이지 제어모듈(304)로부터의 지시에 근거하는 전자증명서의 취득 처리를 실행하기 위한 모듈이다. 키 페어 증명서 취득 모듈(305)은, SCEP에 의한 통신 제어, PKCS#7, PKCS#10등의 SCEP를 사용한 통신에 필요한 암호화 데이터의 생성과 해석 처리 및, 취득한 전자증명서의 보존 및 용도 설정(예를 들면, 셋업 또는 초기화) 처리를 행하는 모듈이다. 암호화 모듈(306)은, 데이터의 암호화 및 복호처리, 전자서명의 생성 및 검증, 해시값 생성 등의 각종 암호처리를 실행하는 모듈이다. 암호화 모듈(306)은, 제1실시예에 따른 전자증명서의 취득 및 갱신 처리에서, SCEP의 요구/응답 데이터의 생성 및 해석 처리에 필요한 각 암호처리를 실행한다. 키 페어 증명서 관리모듈(307)은, 복합기(100)에 보유/보존된 공개 키 페어와 전자증명서를 관리하는 모듈이다. 예를 들면, 키 페어 증명서 관리모듈(307)은, 공개 키 페어와, 전자증명서의 데이터를, RAM(203) 및/또는 HDD(204)에 각종 설정 값과 함께 보존한다. 공개 키 페어와 전자증명서의 상세한 정보 표시, 생성 및 삭제를 위한 처리들이 도 3에서는 도시되지 않지만, (예를 들면, 조작 패널(212)을 통해 수신된) 유저의 지시에 의거한 그 처리를 실행하는 것이 가능하다. 조작 패널(212) 및 패널 제어부(208)의 제어는, UI제어모듈(308)에 의해 실행/수행된다. 한편, 본 실시예에 의하면, 통신 제어모듈(303)에 의해 실행되는 TLS, IPSEC, IEEE802.1X등의 암호화 통신 처리의 경우에도, 암호화 모듈(306)에서 암호처리 자체가 행해지고, 키 페어 및 증명서 관리모듈(307)로부터, 사용하는 공개 키 페어 및 전자증명서 데이터를 취득한다. 그렇지만, 상기 암호처리를 위한 그 밖의 구성과, 상기 공개 키 페어 및 전자증명서 데이터는, 기능적으로 동등 또는 호환 가능한 특징들이 이들 구성에 의해 제공되는 한, 가능하다는 것을 알 것이다.

[0035] 출력/입력 처리 모듈(예를 들면, 인쇄/스캔 처리모듈309)은, 데이터 출력 기능(예를 들면, 프린터(210)에 의한 인쇄)이나, 데이터 입력 기능(예를 들면, 스캐너(211)에 의한 원고의 판독/스캐닝 등의 출력/입력 기능의 실행을 제어하는 모듈이다. 디바이스 제어모듈(310)은, 복합기(100)의 동작을 위한 제어 커맨드들과 제어 데이터를 생성하여서 복합기(100)를 (예를 들면, 중심적으로) 제어하기 위한 모듈이다. 한편, 제1실시예에 따른 상기 암호화 모듈(306)은, 필요한 경우, 웹 페이지 제어모듈(304)로부터의 지시에 의거해 복합기(100)의 재기동 처리를 실행할 수 있도록, 복합기(100)에 대해 전원에 액세스한다.

[0036] 도 4a, 4b는, 제1실시예에 따른 네트워크 구성 또는 시스템에서 행해진 처리 전체에 포함된 시퀀스 처리 단계들을 설명하기 위한 시퀀스 도다. 그 시퀀스는, 전자증명서의 발행 요구에 관한 초기 셋업/초기화, 전자증명서의 정보표시, 전자증명서의 발행 요구와 수신부터 시작하고 나서, 그 전자증명서의 인에이블링 사용과 복합기의 재기동으로 이행한다.

[0037] 이 시퀀스는, 유저에 의해 입력된 키 페어 및 전자증명서 리스트의 표시 지시에 응답해서 시작된다. 본 실시예에서는 하나의 복합기(100)에 대해 행해진 처리의 일례를 설명하지만, 그 처리는, 일회의 시작 지시에

응답하여, 복수의 복합기 100 및 101에 의해 수행되어도 좋다. 예를 들면, PC(103)로부터 복합기 100 및 101 각각에 대하여 요구를 송신하고, 각 복합기에서, 이하의 도 5a 내지 도 9의 흐름도에 도시된 처리를 실행시켜도 좋다. 이러한 경우에, 복합기100 및 101 각각에서 증명서를 취득하고 표시하고 확인시키는 단계들을 스킵해도 좋다. 또한, 유효기간이 만료된 증명서를 자동적으로 각 복합기로 검출하고, 그 만료된 증명서의 서지정보(증명서ID와 유효기간)를 PC(103)에 송신하고, PC(103)는, 만료하거나 이미 만료된 유효기간을 갖는 상기 증명서의 갱신처리를, 복수의 복합기에 자동적으로 실행시켜도 좋다. 이렇게 상술한 동작이, 소위 사일런트 인스톨이다.

[0038] 우선, 단계 S401에서, 복합기(100)는, PC(103)로부터의 접속을 접수(즉, 그 PC와 통신채널을 확립)하면, PC(103)로부터, 복합기(100)가 보유한 상기 키 페어/전자증명서 리스트를 표시하는 요구를 수신한다. 제1실시예에서, 복합기(100)의 관리자는, PC(103)에 설치된 웹브라우저를 이용하여, 복합기(100)가 공개하고 있는 전자증명서의 발행 요구 및 취득을 위한 웹 페이지 형식의 RUI에 접속하고, 지시 관련 조작들을 행하는(예를 들면, 복합기 100 또는 101상에서 행해지는 조작을 위한 지시를 입력하는) 것으로 가정한다. 이 RUI는, Remote User Interface의 약어이며, 유저가, PC(103)의 웹 브라우저를 사용하여, 원격으로 복합기 100 또는 101의 조작 화면 데이터를 요구해서 PC(103)에 그 조작 화면을 표시할 수 있는 기술이다. 일례로서, 그 화면을 HTML과 서브릿으로 구현할 수 있다.

[0039] 다음에, 단계 S402에서, 복합기(100)는, 복합기(100)가 보유하고 있는 키 페어/전자증명서의 리스트 표시를 위한 데이터를 취득하고, 그 취득된 데이터를 표시하기 위해 웹 페이지 화면 생성 처리를 실행한다.

[0040] 도 5a는, 도 4a의 단계 S402의 키 페어/전자증명서의 리스트의 취득 및 표시 데이터 작성/생성에 포함된 처리를 도시하는 흐름도다. 한편, 이 처리는, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행함으로써 구현된다.

[0041] 도 17a 내지 17c는, 키 페어 증명서 관리모듈(307)이 관리하고 있는 키 페어/전자증명서 상세정보 데이터베이스의 개념도다. 본 실시예에 의하면, 이 데이터베이스는, 복합기(100)의 HDD(204)에 보존되어 있다. 그렇지만,

[0042] 이하, 도 5a의 흐름도를 설명한다. 이 처리는, 키 페어/전자증명서 리스트의 취득 요구를 수신할 때 시작된다(착수된다). 우선, 단계 S501에서, CPU(201)는, 키 페어/전자증명서 리스트의 취득 요구를 수신한다. 다음에, 단계 S502의 처리로 진행되고, CPU(201)는, 키 페어 증명서 관리모듈(307)이 관리하고 있는, 예를 들면 도 17a에 도시된 키 페어/전자증명서의 상세정보를 취득한다. 다음에, 단계 S503의 처리로 진행되어, CPU(201)는, 단계 S502에서 취득한 키 페어/전자증명서의 상세정보를 사용하여, RUI로서 제공되는 웹 페이지 화면을 위한 HTML 데이터를 생성한다.

[0043] 도 10a~도 15는, 제1실시예에 따른 PC(103)에 표시되는 웹 페이지 화면(즉, RUI)의 예들을 도시하는 도다. 제1실시예에 따른 도 5a의 단계 S503에서는, 도 10a에 도시된 웹 페이지 화면을 위한 HTML데이터가 생성되고, 그 생성된 HTML데이터가 PC(103)의 웹브라우저를 사용하여 표시된다고 가정한다. 이에 따라, PC(103)로부터 복합기(100)가 보유하고 있는 키 페어/전자증명서 리스트가 쉽게 확인 가능해진다.

[0044] 도 10a의 리스트에 표시되는 전자증명서의 정보는, 그 증명서의 이름(1011), 용도(1012), 발행자(1013), 만기(1014), 증명서의 상세(1015)를 포함하고 있다. 이름(1011)은, 키 페어/전자증명서가 발행될 때, 복합기(100)의 관리자등의 조작자가 임의로 부여한 문자열이다. 용도(1012)는, 그 키 페어/전자증명서가 TLS, IPSEC 또는 IEEE802.1X의 특별한 통신 프로토콜을 구현/이용하는 용도를 위해 사용되는 것을 나타내는 설정 값이다. 발행자(1013)는, 전자증명서를 발행한 상기 CA의 식별명(DN)(즉, 식별번호)이다. 그 만기(1014)는, 그 전자증명서의 유효기간이 만료하는 날짜를 가리키는 정보다. 상세(1015)는, 전자증명서의 상세정보를 표시시키기 위한 아이콘이다. 이후, 단계 S504의 처리로 진행되어, CPU(201)는, 단계 S503에서 생성한 HTML데이터를 단계 S501에의 응답으로서 PC(103)에 송신하고, 이 처리를 종료한다. 이렇게 해서, 도 4a의 단계 S403이 실행된다.

[0045] 한편, 도 4a, 4b의 시퀀스 도에는 도시하지 않지만, 복합기(100)의 관리자가, PC(103)에 표시될 때 도 10a의 상세(1015)의 아이콘을 클릭하면, 해당 전자증명서의 상세정보의 표시 요구가 PC(103)로부터 복합기(100)에 송신된다. 이 표시 요구를 수신한 복합기(100)는, 그 전자증명서의 상세정보를 취득하고, 그 취득한 정보에 근거하는 그 증명서의 상세정보를 위한 HTML데이터를 생성하고, 그 생성한 데이터를, 상기 표시 요구에 대한 응답으로서 PC(103)에 송신한다.

[0046] 이에 따라, 예를 들면 도 16에 도시된 방식으로, 전자증명서의 상세정보가 PC(103)의 웹브라우저에 표시된다. 도 16은, PC(103)에 표시되는 전자증명서의 상세정보의 뷰의 예를 도시한 도면이다.

[0047] 도 5b는, 제1실시예에 따른 복합기(100)가, 이 상세정보를 표시하는 요구를 PC(103)로부터 수신할 때 행해진 처

리를 도시하는 흐름도다. 한편, 이 처리는, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행함에 의해 실현된다.

[0048] 우선, 단계 S511에서, CPU(201)는, PC(103)로부터 전자증명서의 상세정보의 취득 요구를 수신한다. 다음에, 단계 S512의 처리로 진행되어, CPU(201)는, 키 페어 증명서 관리모듈(307)이 관리하고 있는 도 17a에 도시된 키 페어/전자증명서의 상세정보를 취득한다. 다음에, 단계 S513의 처리로 진행되어, CPU(201)는, 단계 S512에서 취득한 키 페어/전자증명서의 상세정보를 사용해서 웹 페이지 화면을 위한 HTML데이터를 생성하여, 단계 S514에서 PC(103)에 송신한다.

[0049] 도 16은, 제1실시예에 따른 전자증명서의 상세정보의 표시 화면 뷰의 일례를 도시한 화면 뷰를 도시한 도면이다. 이 화면 뷰는, PC(103)에 RUI로서 웹 페이지 형식으로 표시된다.

[0050] 다시 도 4a의 설명으로 되돌아가서, 단계 S403에서, 복합기(100)는, 단계S402에서 생성한 도 10a에 도시된 웹 페이지 화면을 위한 HTML데이터를, PC(103)로부터의 요구에 대한 응답으로서 송신한다.

[0051] 한편, 상술한 도 4a의 단계 S401~단계 S403 및, 도 5a의 단계 S501~단계 S504, 단계 S511~단계 S514에 도시된 처리는, 키 페어/전자증명서 리스트의 표시 요구를 수신할 때 복합기(100)에서 행해진 전자증명서정보의 표시 처리에 관한 제어 처리 단계들을 나타내고 있다.

[0052] 단계 S404에서, 복합기(100)는, PC(103)로부터, SCEP서버(CA/RA 102의 일례)의 접속 셋업 화면의 표시 요구를 수신한다. 제1실시예에 따른 복합기(100)의 관리자는, 인증국/등록국(102)과의 접속 셋업 조작(예를 들면, 통신 채널/접속을 확립하기 위한 접속 설정/파라미터들의 설정)을 행하기 위해서, 도 10a에 도시된 접속 설정(1002)을 클릭하여, 접속 셋업 화면의 표시 요구를 복합기(100)에 대하여 송신하는 것으로 가정한다.

[0053] 다음에, 단계 S405에서, 복합기(100)는, 단계 S404에서 수신한 요구에 대한 응답으로서, 도 10b에 도시된 소정의 SCEP서버의 접속 셋업 화면을 위한 HTML데이터를 PC(103)에 송신한다.

[0054] 도 10b에 도시된 접속 셋업 화면은, SCEP서버의 호스트명(예를 들면, 그것의 IP어드레스) 및 접속처 포트 번호를 각각 입력하는 서버명/어드레스(1016) 및 포트 번호(1017)와, 상기 접속을 위해 실시될 수 있도록 상기 입력된 설정 값의 설정 완료인 상기 셋업/설정 처리의 완료를 지시/가리키는 설정 버튼(1018)을 위한, 입력 필드들을 포함하고 있다.

[0055] 다음에, 단계 S406에서, 복합기(100)는, PC(103)로부터 접속 셋업 조작의 설정 지시 요구를 수신한다. 제1실시예에 따른 복합기(100)의 관리자는, PC(103)로부터 도 10b의 서버명(1016)과 포트 번호(1017)에 관한 필요한 정보를 입력한 후, 그 설정 버튼(1018)을 클릭하는 것으로 복합기(100)에 대하여, 이 설정 지시 요구를 송신하는 것으로 가정한다.

[0056] 다음에, 단계 S407에서, 복합기(100)는, 그 접속 셋업 조작을 행하고(즉, 그 입력 정보에 따라 접속 설정을 설정하고), 그 접속 셋업 조작의 설정 처리와 설정 결과를 표시하는 웹 페이지 화면 데이터의 생성을 실행한다. 단계 S408에서, 단계 S407에서 생성한 도 11a에 도시된 웹 페이지 화면 데이터에 근거한 웹 페이지 화면을 위한 HTML데이터를, PC(103)로부터의 요구에 대한 응답으로서 송신한다.

[0057] 도 6은, 제1실시예에 따른 복합기(100)에 의한, 도 4a의 단계 S407에서 행해진 인증국/등록국(102)과 접속/통신을 확립하기 위한 접속 셋업 처리를 설명하는 흐름도다. 한편, 이 처리는, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행함에 의해 실현된다.

[0058] 우선, 단계 S601에서, CPU(201)는, PC(103)로부터 접속 설정 요구를 수신한다. 다음에, 단계 S602의 처리로 진행되어, CPU(201)는, 그 접속 설정 요구에 포함된 호스트명과 포트 번호 등의 설정 값을 취득하고, 그 취득한 설정 값을 RAM(203) 혹은 HDD(204)에 보존한다. 다음에, 단계 S603의 처리로 진행되어, CPU(201)는, 예를 들면 도 11a에 도시된 것과 같은 웹 페이지 화면을 위한 HTML데이터를 생성한다. 단계S604의 처리로 진행되어, CPU(201)는, 단계 S603에서 생성된 HTML데이터를 단계 S601에서의 요구에 대한 응답으로서 PC(103)에 송신하고, 이 처리를 종료한다. 이렇게 해서 단계 S408의 처리로 진행된다.

[0059] 이에 따라, PC(103)에는, 도 11a에 도시한 바와 같이, 설정이 실현된 것을 나타내는(즉, CA/RA 102와의 접속 확립을 위한 설정 값이 설정/적용/실시되는) 문자열(1101)이 표시된다.

[0060] 상술한 단계 S406~S408 및 단계 S601~S604에 도시된 처리는, 복합기(100)의 접속 셋업 처리에 관한 제어동작이다.

[0061] 다음에, 도 4a의 단계 S409에서, 복합기(100)는, PC(103)의 상기 브라우저로부터 송신되는 CA증명서의 취득 화면의 표시 요구를 수신한다. 제1실시예에서는, 복합기(100)의 관리자가, 인증국/등록국(102)이 발행한 CA증명서의 취득을 행하므로, 그 관리자가 도 10a에 도시된 CA증명서 취득(1003)을 클릭할 때 CA증명서의 취득 화면의 표시 요구를 복합기(100)에 송신하는 것으로 가정한다.

[0062] 이에 따라, 단계 S410에서, 복합기(100)는, 단계 S409에서 상기 수신된 요구에 대한 응답으로서, 도 11b에 도시된 소정의 CA증명서의 취득 화면의 HTML데이터를 송신한다.

[0063] 도 11b에 도시된 접속 셋업 화면은, CA증명서의 실제의 취득을 지시하는 실행 버튼(1102)을 포함하고 있다.

[0064] 다음에, 단계 S411에서, 복합기(100)는, 도 11b에 도시된 실행 버튼(1102)이 클릭될 때 PC(103)의 브라우저로부터 송신된 상기 CA증명서의 취득 요구를 수신한다. 제1실시예에서는, 복합기(100)의 관리자가 도 11b에 도시된 실행 버튼(1102)을 클릭할 때, CA증명서의 취득 요구를 복합기(100)에 송신하는 것으로 가정한다.

[0065] 다음에, 단계 S412에서, 복합기(100)는, CA증명서의 취득 요구 데이터의 생성 처리를 실행/수행한다. 단계 S413의 처리로 진행되어, 복합기(100)는, 단계 S412에서 생성한 CA증명서의 취득 요구 데이터를, 단계S407에서 수행한 접속 셋업 조작에서 설정된 정보에 근거하여, SCEP서버인 인증국/등록국(102)에 송신한다. 단계 S414의 처리로 진행되어, 복합기(100)는, 인증국/등록국(102)으로부터 송신되는 CA증명서의 취득 응답을 수신한다. 이에 따라, 단계 S415에서, 복합기(100)는, 수신한 CA증명서의 취득 응답을 해석하고, 그 응답에 포함된 CA증명서를 취득하고, 그 취득한 CA증명서를 복합기(100)가 신뢰하는 CA증명서로서 등록하는 처리를 행한다. 복합기(100)는, 그 CA증명서 취득요구를 하는 결과/결말을 가리키는 웹페이지 화면을 위한 HTML데이터도 생성한다. 단계 S416의 처리로 진행되어, 복합기(100)는, CA증명서 취득 요구 결과를 포함하는 응답을 PC(103)에 송신한다. 그 응답은, 단계 S415에서 생성한 도 12a 또는 도 12b에 도시된 웹 페이지 화면을 위한 HTML데이터를, 상기 결과(즉, 그 요구를 한 결말)의 표시기로서 포함한다. 도 12a는, CA증명서의 취득에 성공하고 그 취득된 증명서를 신뢰된 CA증명서로서 등록했을 때에 표시되는 화면 예를 도시한 도면이다. 한편, 도 12b는, CA증명서의 취득에 실패했을 때에 표시되는 화면 예를 도시한다.

[0066] 도 7은, 제1실시예에 따른 복합기(100)에 의해 행해진, 도 4a의 단계 S412 내지 단계 S416에 도시된 CA증명서의 취득 및 등록 처리를 보다 상세히 설명하는 흐름도다. 한편, 이 처리들은, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행함에 의해 실현된다.

[0067] 우선, 단계 S701에서, CPU(201)는, PC(103)로부터 CA증명서의 취득 요구를 수신한다. 다음에, 단계 S702의 처리로 진행되어, CPU(201)는, 단계 S407에서 취득한 인증국/등록국(102)과의 접속/통신을 위해 설정된 접속 설정(셋업)의 정보를 기초로 CA증명서의 취득 요구의 메시지를 생성한다. 이하는, 제1실시예에 따라 생성된 그 취득 요구의 메시지의 일례가 도시되어 있다. 제1실시예에서는, 통신 프로토콜로서 SCEP를 이용하므로, 이하의 메시지를, 그 프로토콜을 이용한 요구 메시지로서 사용한다.

[0068] xxxxxxx/yyyyy?operation=GetCAXyz&message=CAIdentifier

[0069] 다음에, 단계 S703의 처리로 진행되어, CPU(201)는, 도 4a의 단계 S407에서 취득한 인증국/등록국(102)을 위한 접속 설정 정보에 근거하여, SCEP 서버인 인증국/등록국(102)에 대하여 TCP/IP프로토콜로 접속하도록 상기 네트워크 인터페이스 제어부(205)를 제어한다. 다음에, 단계 S704의 처리로 진행되어, CPU(201)는, 단계S703에 있어서의 접속이 성공했는지를 판단한다. 그 접속이 성공했을 경우는, 단계S705의 처리로 진행된다. 실패했을 경우는, 단계 S714의 처리로 진행되어 에러 처리 단계를 행한다.

[0070] 단계 S705에서, CPU(201)는, 단계 S702에서 생성한 CA증명서의 취득 요구 메시지를, 예를 들면 HTTP프로토콜의 GET 또는 POST방법을 사용하여 인증국/등록국(102)에 송신한다. 다음에, 단계 S706의 처리로 진행되어, CPU(201)는, 단계 S705에 있어서의 송신이 성공했는지를 판단한다. 그 송신이 성공했을 경우는, 단계 S707의 처리로 진행된다. 실패했을 경우는, 단계 S714의 처리로 진행되어 상기 에러 처리 단계를 행한다. 단계 S707에서, (상기 네트워크 인터페이스 제어부 205를 거쳐) CPU(201)는, CA증명서의 취득 요구 메시지에 대한 응답으로서 보내진, 상기 인증국/등록국(102)로부터의 응답 데이터를 수신한다. 단계 S708의 처리로 진행되어, CPU(201)는, 단계 S707에 있어서의 응답 데이터의 수신이 성공했는지를 판정한다. 그 수신이 성공했을 경우는, 단계 S709의 처리로 진행된다. 실패했을 경우는 단계 S714의 처리로 진행된다. 단계 S709에서, CPU(201)는, 단계 S707에서 수신한 응답 데이터를 해석하고, 그 응답 데이터에 포함된 그 CA증명서의 데이터를 취득한다. 이 응답 데이터의 해석과 CA증명서의 취득 처리는, 암호화 모듈(306)에 의해 행해진다.

[0071] 한편, 제1실시예에 따른 응답 데이터는, X.509(RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile)형식의 2진 데이터다. 단, 예를 들면, PKCS#7(RFC5652: Cryptographic Message Syntax)형식의 데이터가 응답으로서도 송신되어도 되고, 그 데이터 형식은 상기 CA증명서를 얻을 수 있으면 특정한 형식에 한정되지 않는다는 것을 알 것이다.

[0072] 단계 S710의 처리로 진행되어, CPU(201)는, 단계 S709에 있어서의 CA증명서의 취득이 성공했는지를 판정한다. 그 취득이 성공했을 경우는, 단계 S711의 처리로 진행된다. 실패했을 경우는 단계 S714의 처리로 진행된다. 단계 S711에서, CPU(201)는, 단계 S709에서 취득한 CA증명서를, 복합기(100)가 신뢰하는 CA증명서로서 등록한다. CPU(201)는, 취득한 CA증명서를 RAM(203)에 보유(일시적으로 저장)함과 아울러, 키 페어 증명서 관리모듈(307)에 의해 HDD(204)의 복합기(100)가 신뢰하는 CA증명서를 격납하는 소정의 디렉토리에 보존한다. 단계 S712의 처리로 진행되어, CPU(201)는, 단계 S711에 있어서의 CA증명서의 등록 처리가 성공한 것인가 아닌가를 판정한다. 이 처리가 성공했을 경우는, 단계 S713의 처리로 진행된다. 실패했을 경우는, 단계 S714의 처리로 진행된다. 단계 S713에서, CPU(201)는, CA증명서의 취득 및 등록을 성공했을 때 도 12a의 문자열(1201)로 나타낸 것과 같은 방식으로 표시되는 CA증명서의 무인(thumbmark)(SHA1 알고리즘을 사용하여 취득된 해시 값)을 생성한다. 이 무인의 생성은, 암호화 모듈(306)에 의해 실행/수행된다. 그후, 단계 S715의 처리로 진행되어, CPU(201)는, 단계 S703부터 단계 S714까지의 처리 결과에 근거하여, 적절하게 도 12a 혹은 도 12b에 도시된 CA증명서의 취득 결과의 표시 데이터를 위한 HTML데이터를 생성한다. 단계 S716의 처리로 진행되어, CPU(201)는, 단계 S715에서 생성한 HTML데이터를 단계 S701에서 수신한 요구에 대한 응답으로서 PC(103)에 송신하도록 제어하고, 이 취득 및 등록 처리를 종료한다. 그 후에, 도 4a의 단계 S417의 처리로 진행된다. 제1실시예에서는, CA증명서의 취득 및 등록 결과에 따라서 도 12a의 문자열(1201)을 표시한다. 이와는 달리, 단계 S714에서 에러 처리를 실행했을 경우는, 예를 들면, 도 12b의 문자열(1202)을 표시한다. 다음에, 도 4a의 설명으로 되돌아간다.

[0073] 단계 S417에서, 복합기(100)는, PC(103)의 브라우저로부터 송신되는 증명서의 발행 요구 화면의 표시 요구를 수신한다. 제1실시예에서는, 복합기(100)의 관리자가, 도 10a에 도시된 증명서 발행 요구(1004)를 클릭하여, 새롭게 발행된 전자증명서를 취득하기 위해서 상기 인증국/등록국(102)에 대한 증명서의 발행 요구를 행하는 것으로 가정한다.

[0074] 다음에, 단계 S418에서, 복합기(100)는, 단계 S417에서의 상기 표시 요구에 대한 응답으로서, 도 13a에 도시된 일례인, 소정의 증명서의 발행 화면을 위한 HTML데이터를, PC(103)에 송신한다. 이에 따라, PC(103)는, 도 13a에 도시된 화면을 표시하는 표시 제어를 행한다.

[0075] 도 13a의 증명서의 발행 요구 화면은, 그 증명서의 이름(1301), 생성되는 키 페어의 키 길이를 설정하는 키의 길이(1302), 발행처 정보의 입력 필드(1303), 인증국/등록국(102)으로부터 송신된 증명서의 발행 요구의 응답에 부여되는 서명을 검증/인증할 것인가 아닌가를 나타내는 서명 검증(1304), 발행된 증명서(에서 사용하는 통신 프로토콜)의 용도를 설정하는 키의 용도(1305), 증명서 발행 요구에 포함되는 패스워드(1306), 그 증명서의 발행 요구 송신을 실행/지시하는 실행 버튼(1307)을 포함하고 있다. 본 실시예에서는, 그 키의 용도(1305)를, 체크박스들의 그룹으로서 설정하고, 하나의 증명서에 대하여 복수의 용도(즉, 하나보다 많은 통신 프로토콜)를 설정할 수 있는 것을 나타내고 있다.

[0076] 다음에, 단계 S419에서, 예를 들면 도 13a에 도시된 화면의 실행 버튼(1307)을 클릭하여서 상기 증명서 발행 요구를 지시하였을 때, 복합기(100)는, PC(103)의 브라우저로부터 설정된 각각의 참조번호 1301~1306로 참조한 항목들과 관련된 입력/설정 정보/데이터를 포함하는 증명서의 발행 요구를 수신한다. 제1실시예에서는, 복합기(100)의 관리자가 도 13a에 도시된, 각각의 참조번호 1301~1306에서 참조한 항목들과 관련된 정보를 입력 및 설정하고 그 실행 버튼(1307)을 클릭하여, PC(103)로부터의 증명서의 발행 요구 지시를 복합기(100)에 송신한다.

[0077] 다음에, 단계 S420에서, 복합기(100)는, 상기 증명서의 발행 요구(데이터) 생성 처리를 실행/수행한다. 단계 S421에서, 복합기(100)는, 단계S420에서 생성한 증명서의 발행 요구 데이터를, 단계 S407에서 설정한 정보에 근거해 상기 SCEP서버인 인증국/등록국(102)에 대하여 송신한다. 그 후, 그 인증국/등록국(102)은, 발행 요구 데이터에 근거한 증명서를 발행하고, 증명서 발행 요구 응답을 송신한다. 단계 S422에서, 복합기(100)는, 인증국/등록국(102)으로부터 송신된 증명서의 발행 요구 응답을 수신한다. 다음에, 단계 S423에서, 복합기(100)는, 단계 S422에서 수신한 증명서의 발행 요구 응답의 해석 및 등록 처리를 행한다(그 설정에 따라 서명 검증/인증의 실행/수행, 그 응답에 포함되는 증명서의 취득, 취득한 증명서를 지정된/특정된 용도에, 즉 특정된 통신 프로토콜에 설정/등록). 그 후에, 복합기(100)는, 증명서의 발행 요구의 결과를 표시하는 웹 페이지 화면의 생성 처리

를 실행한다.

[0078] 여기서, 발행된 증명서의 증명서 발행 및 이후의 취득이 성공했을 경우는, 단계 S423의 처리에 의해, 전자증명서 데이터의 보존 및 용도설정(예를 들면, 통신 프로토콜 설정)이 행해진다. 여기서, 용도설정은, 제1실시예에서는, 전자증명서를 사용하는 통신 기능과, 설정가능/구성가능한(즉, 설정에 따라 사용하는데 이용 가능한) TLS, IPSEC, IEEE802.1X 등의 암호화 통신 프로토콜을 위한, 설정/파라미터를 설정하는 것에 관한 것이다. 또, 제1실시예에 따른 복합기(100)는, 복수의 전자증명서를 보유/보존할 수 있고, 전자증명서마다 하나 이상의 용도(예를 들면, 하나 이상의 통신 프로토콜)를 설정하는 것으로 가정한다. 예를 들면, 복합기(100)가 (웹 서버로서의 역할을 하는 TLS통신을 행함으로써) 서버 서비스를 제공하는데 사용된 전자증명서와, 복합기(100)가 (예를 들면, IEEE802.1X를 사용하여) 클라이언트 통신을 행하는데 사용된 전자증명서가 서로 다른 경우에, 다른 용도(예를 들면, 통신 프로토콜)를 설정 가능하다. 단, 1개의 전자증명서를, 적절하게, 전부 또는 하나보다 많은 통신 용도에도 적용/사용해도 좋다는 것을 알 것이다.

[0079] 단계 S424에서, 복합기(100)는, 단계 S423에서 생성한 도 13b 또는 도 14a에 도시된 웹 페이지 화면을 위한 HTML데이터를 PC(103)에 송신한다. 한편, 증명서의 발행 요구의 결과에 따라서 도 13b의 문자열 1308과 도 14a의 문자열 1401로 나타낸 바와 같이 설정 결과의 문자열이 표시된다. 도 13b는, 증명서의 발행 및 취득에 성공했을 경우의 화면의 일례를 도시하는 도면이다. 도 13b에 도시된 화면은, 증명서 발행 요구를 PC(103)로부터 복합기(100)에 송신하고 그 증명서를 그 발행 요구에 따라 발행하는 경우에 상기 PC(103)에 표시된다. 그 발행된 증명서는, 복합기(100)가 재기동될 경우에, 상기 복합기(100)가 안심된 통신을 행하는데 사용되는 증명서로서 설정된다. 유저에게 복합기(100)의 재기동을 강력히 촉구하는 메시지는, 도 13b에 도시된 화면에 포함된다. 도 14a는, 증명서의 발행 및 취득에 실패했을 경우의 화면 뷰의 일례를 도시한 도면이다. 도 14a에 도시된 화면은, 상기 PC(103)로부터 증명서 발행 요구를 복합기(100)에 송신하지만 그 증명서를 발행하지 않는 경우에 상기 PC(103)에 표시된다. 도 14a에 도시된 화면에는, 그 증명서의 발행 실패를 유저에게 통지하는 메시지가 포함되어 있다.

[0080] 이렇게 해서 증명서의 발행 및 취득이 성공했을 경우에는, 단계 S423의 처리에 의해, 전자증명서 데이터의 보존 및 용도(통신 프로토콜) 설정이 행해진다. 제1실시예에 따른 통신 제어모듈(303)은, TLS, IPSEC, IEEE802.1X의 암호화 통신에서 사용된 전자증명서의 데이터를 복합기(100)의 기동시에 취득(즉, 통신 제어모듈(303)은, 복합기(100)의 기동시에, 상기 통신 프로토콜을 사용하는 암호화된 통신 채널을 초기화 및 확립)하므로, 용도(통신 프로토콜 및 관련된 전자증명서)의 변경이 실시/실행되었을 경우는, 복합기(100)의 재기동이 필요하다.

[0081] 도 8a, 8b는, 제1실시예에 따른 복합기(100)에 의한, 도 4b의 단계 S419 내지 단계 S424에서 행해진 증명서의 발행 요구/취득 처리를 보다 상세히 설명하는 흐름도다. 한편, 이 처리는, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행함에 의해 실현된다.

[0082] 우선, 단계 S801에서, CPU(201)는, (예를 들면, 네트워크 인터페이스 제어부 205를 거쳐) PC(103)로부터 증명서의 발행 요구를 수신한다. 다음에, 단계 S802의 처리로 진행되어, CPU(201)는, 상기 요구의 설정값, 예를 들면, 단계S801에서 수신한 증명서의 발행 요구에 포함된, 증명서의 이름(1301), 키의 길이(1302), 발행처 정보의 입력 필드(1303), 서명 검증(1304), 및 키의 용도(1305)의 정보를 취득한다. 다음에, 단계 S803의 처리로 진행되어, CPU(201)는, 도 4a의 단계 S412 내지 단계 S415에서 취득한 CA증명서를 취득한다. 단계 S804의 처리로 진행되어, CPU(201)는, 단계 S802에서 취득한 이름(1301)과 키의 길이(1302)의 정보에 근거하는 키 페어의 생성하고, 발행처 정보의 입력 필드(1303)와, 패스워드(1306)의 정보에 근거하는 PKCS#10(RFC2986: PKCS#10: Certification Request Syntax Specification)형식의 증명서 서명 요구(CSR) 데이터를 암호화 모듈(306)을 사용하여서 생성하는, 처리를 행한다. 다음에, 단계 S805의 처리로 진행되어, CPU(201)는, 단계S804에 있어서의 키 페어/CSR의 생성이 성공했는지를 판정한다. 그 생성이 성공했다고 판정했을 경우는, 단계 S806의 처리로 진행된다. 실패했을 경우는, 단계 S823의 처리로 진행되어 에러 처리를 행한다. 단계 S806에서, CPU(201)는, 증명서의 발행 요구 데이터(예를 들면, CSR 데이터)를 생성한다. 단계 S806에서 생성된 CSR 데이터는, 도 4a의 단계 S407에서 취득한 인증국/등록국(102)과의 통신을 위해 설정된 접속 설정에 근거하여, 상기 SCEP에서 정의되어 있는 PKCS#7형식의 데이터가 된다. 다음에, 단계 S807의 처리로 진행되어, CPU(201)는, 상기 증명서 발행 요구 데이터를 생성할 때 단계 S806에 있어서의 데이터의 생성에 성공했는지를 판정한다. 그 데이터의 생성이 성공했을 경우는, 단계 S808의 처리로 진행된다. 실패했을 경우는 단계 S823의 처리로 진행된다.

[0083] 단계 S808에서, CPU(201)는, 도 4a의 단계 S407에서 취득한 인증국/등록국(102)에의 접속 설정에 근거해 SCEP서버인 인증국/등록국(102)에 TCP/IP프로토콜 접속을 행한다. 다음에, 단계 S809의 처리로 진행되어, CPU(201)는,

단계 S808에 있어서의 접속이 성공했는지를 판정한다. 그 접속이 성공했을 경우는, 단계 S810의 처리로 진행된다. 실패했을 경우는, 단계 S823의 처리로 진행된다. 단계 S810에서, CPU(201)는, 단계 S806에서 생성한 상기 CSR 데이터를, HTTP프로토콜의 GET 또는 POST방법으로 인증국/등록국(102)에 송신한다. 단계 S811에서, CPU(201)는, 단계 S810에 있어서의 송신이 성공했는지를 판정한다. 그 송신이 성공했을 경우는, 단계 S812의 처리로 진행된다. 그 송신이 실패했을 경우는, 단계 S823의 처리로 진행된다. 단계 S812에서, CPU(201)는, 인증국/등록국(102)으로부터, 증명서 발행 응답(예를 들면, CSR 응답 데이터를 포함함)을 (예를 들면, 네트워크 인터페이스 제어부 205를 거쳐) 수신한다. 그 응답 데이터가 상기 SCEP에 의해 규정되고, PKCS#7형식의 데이터가 응답으로서 송신된다. 그 밖의 데이터 형식을 사용하여도 된다는 것을 알 것이다.

[0084] 다음에, 단계 S813의 처리로 진행되어, CPU(201)는, 단계 S812에 있어서의 응답 데이터의 수신에 성공했는지를 판정한다. 그 수신이 성공했을 경우는, 단계 S814의 처리로 진행된다. 그 수신이 실패했을 경우는, 단계 S823의 처리로 진행된다. 단계 S814에서, CPU(201)는, 예를 들면, 단계 S802에서 취득한 서명 검증(1304)의 정보에 근거하여, 서명 검증 설정이 있는가 아닌가를 판정함으로써 서명 검증이 필요한가 아닌가를 판정한다. 서명 검증이 행해지면, 단계 S815의 처리로 진행된다. 그렇지 않을 경우, 단계 S817의 처리로 진행된다. 단계 S815에서, CPU(201)는, 단계 S812에서 수신한 그 응답 데이터에 부여되어 있는 서명 데이터를, 단계 S803에 있어서 취득한 CA증명서에 포함된 공개 키를 사용해서 검증/인증하도록 제어한다. 단계 S816의 처리로 진행되어, CPU(201)는, 단계 S815에서의 서명 검증의 결과가 성공한 것인가 아닌가(즉, 그 서명이 인증/유효로서 검증/인증되었는가)를 판정한다. 그 서명 검증이 성공했을 경우는 단계 S817의 처리로 진행된다. 실패했을 경우는 단계 S823의 처리로 진행된다.

[0085] 단계 S817에서, CPU(201)는, 단계 S812에서 수신한 그 응답 데이터를 해석하고, 그 응답 데이터에 포함된 증명서 데이터를 취득한다. 예를 들면, 암호화 모듈(306)에 의해 응답 데이터의 해석과 증명서의 취득 처리를 행한다. 다음에, 단계 S818에서, CPU(201)는, 단계S817에 있어서의 증명서의 취득에 성공했는지를 판정한다. 그 증명서 취득에 성공했을 경우는, 단계 S819의 처리로 진행된다. 실패했을 경우는 단계 S823의 처리로 진행된다. 단계 S819에서, CPU(201)는, 단계 S818에서 취득한 증명서를, 단계 S804에서 생성한 키 페어에 대응하는 전자증명서(즉, 디지털 증명서)로서 등록한다. 동시에, CPU(201)는, 단계 S804에서 생성한 공개 키 페어, 및 취득한 전자증명서를, 키 페어 증명서 관리모듈(307)에 의해 HDD(204)의 키 페어/전자증명서를 격납하는 소정의 디렉토리에 보존한다/보존하도록 제어한다. 키 페어 증명서 관리모듈(307)은, 도 17b에 도시한 바와 같이 키 페어 증명서의 상세정보의 리스트에, 단계 S804에서 생성한 공개 키 페어 및 취득한 전자증명서의 정보도 추가한다. 도 17b에서는, 새로운 키 페어/증명서Xyz4가 추가되어 있다.

[0086] 다음에, 단계 S820의 처리로 진행되어, CPU(201)는, 단계 S819에 있어서의 증명서의 등록 처리가 성공했는지를 판정한다. 그 등록이 성공했을 경우는 단계 S821의 처리로 진행된다. 실패했을 경우는 단계 S823의 처리로 진행된다. 단계S821에서, CPU(201)는, 단계 S802에서 취득한 키의 용도(1305)의 정보에 근거하여 상기 증명서를 사용할 용도를 위한 설정을 설정한다. 키 페어 증명서 관리모듈(307)은, 예를 들면 도 17c에 도시한 바와 같이 키 페어/증명서의 상세정보의 리스트에 있는 그 용도 정보(예를 들면, 상기 통신 프로토콜의 정보)를 갱신한다. 도 17c에서는, TLS에서 사용하는 키 페어/증명서가, Xyz1(도 17b)으로부터 Xyz4로 변경되어 있다. 다음에, 단계 S822의 처리로 진행된다. CPU(201)는, 단계S821에 있어서의 용도 설정(예를 들면, 전자증명서의 갱신)이 성공했는지를 판정한다. 그 용도 설정(예를 들면, 갱신)이 성공했을 경우는 단계S824의 처리로 진행된다. 실패했을 경우는 단계 S823의 처리로 진행된다.

[0087] 단계 S824에서, CPU(201)는, 단계 S801로부터 단계 S823까지의 처리 결과/결말에 대응하는, 도 13b에 도시된 바와 같은 증명서의 발행 요구 결과를 위한 HTML데이터를 생성한다. 단계 S825에서, CPU(201)는, 단계 S824에서 생성한 HTML데이터를 단계 S801의 증명서의 발행 요구에 대한 응답으로서 PC(103)에 송신하도록 제어하고, 그 증명서 발행 요구/취득 처리를 종료한다. 그 후에, 도 4b의 단계 S425의 처리로 진행된다.

[0088] 상술한 단계 S419~단계 S424 및 단계 S801~단계 S825의 처리가, 복합기(100)의 전자증명서의 발행 요구와 그것의 응답 처리, 통신(프로토콜) 용도의 설정에 관한 제어 동작의 일부를 형성한다. 이 제1실시예에서는, 그 발행 요구와 응답 처리로부터 통신(프로토콜) 용도의 설정까지 행해진 이들 처리를 총칭하여, "전자증명서의 자동갱신 기능"이라고 부른다.

[0089] 이 전자증명서의 자동갱신 기능을 실행함으로써, 복합기(100)는 네트워크를 통해 전자증명서의 발행 요구와 응답 처리를 자동으로 행하고, 또, 수신한 전자증명서의 용도(예를 들면, 통신 프로토콜)도 설정할 수 있다. 이에 따라, 유저의 작업량을 삭감할 수 있다. 도 4b의 설명에 되돌아간다.

[0090] 단계 S425에서, 복합기(100)는, 복합기(100)의 재기동의 요구를 수신한다. 제1실시예에서는, 복합기(100)의 관리자가, 도 13b에 도시된 재기동 버튼(1309)을 클릭하여서 복합기(100)를 재기동하는 것으로 가정한다.

[0091] 다음에, 단계 S426의 처리로 진행되어, 복합기(100)는, 단계 S425에서의 재기동 요구에 대한 응답으로서, 예를 들면 도 14b에서와 같이 도시된 소정의 재기동 실행 화면의 HTML데이터를 송신한다. 다음에, 단계 S427의 처리로 진행되어, 복합기(100)는, 복합기(100)를 위한 재기동 처리를 실행/수행한다.

[0092] 제1실시예에 따른 복합기(100)는, 예를 들면, 수신한 전자증명서를 위한 통신 프로토콜(용도)을 IEEE802.1X에 설정했을 때, 재기동이 그 용도 설정에 대해 이루어진 어떠한 변경도 실시하는 것이 필요하다는 가정하에 설명되어 있다. 이것은, 예를 들면, IEEE802.1X의 전자증명서가 복합기(100)의 기동/스타트 업시에 RAM(203)에 전개/초기화되어도 되고, 계속적으로 사용되어도 되기 때문이고, 이것은, HDD(204)에 보존되어 있는 상기 수신한 전자증명서로 대체되지 않아도 되는 것을 의미한다. 단, 만약 복합기(100)의 재기동 없이 그 특별한 통신 프로토콜을 사용하여 그 용도에 사용되는 전자증명서를 전환/변경하는 것이 가능하면, 재기동을 행하지 않도록 설정되어도 좋다. 예를 들면, TLS에 대한 용도가 설정되는 경우는, 그것은 재기동이 불필요하다고 생각되도록 설정되어도 좋다. 예를 들면, 복수의 용도의 각각에 대하여 재기동의 필요에 관한 표시기를 미리 설정해두는 것이 가능하고, 복합기(100)는, 그 재기동의 필요 정보에 따라 재기동의 유무를 자동적으로 판정해도 좋다. 다른 예에서, PC(103)는, 그러한 재기동 필요 표시기 정보를 보존하고, 그것에 근거하여 재기동 요구를 상기 복합기(100)에 송신할지 안할지를 판정하여도 된다.

[0093] 도 9는, 제1실시예에 따른 복합기(100)에 의해 행해진, 도 4b의 단계 S425 내지 단계 S427에서 복합기(100)의 재기동에 관한 처리를 설명하는 흐름도다. 한편, 이 처리는, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행함에 의해 실현된다.

[0094] 우선, 단계 S901에서, CPU(201)는, (예를 들면, 네트워크 인터페이스 제어부 205를 거쳐) PC(103)로부터 복합기(100)의 재기동 요구를 수신한다. 다음에, 단계 S902의 처리로 진행되어, CPU(201)는, 도 14b에 도시된 복합기(100)의 재기동 요구를 위한 소정의 HTML데이터를, 단계 S901에서의 재기동 요구에 대한 응답으로서 (예를 들면, 네트워크 인터페이스 제어부 205를 거쳐) PC(103)에 송신한다. 다음에, 단계 S903의 처리로 진행된다. CPU(201)는, 디바이스 제어모듈(310)에 재기동 처리의 시작을 지시하고/하게 하고/제어하여, 이 재기동 처리를 종료한다.

[0095] 이상의 동작의 시퀀스를 행함으로써, 재기동한 후의 복합기(100)에서는, 인증국/등록국(102)으로부터 취득한 전자증명서를 이용하는 것이 가능하다.

[0096] 도 15는, 증명서의 발행 및 취득이 성공한 후에, 다시 단계 S401 내지 S403의 처리를 실행함으로써 상기 키 페어/전자증명서 리스트를 표시했을 경우의 화면 뷰의 일례를 도시한 도면이다. 인증국/등록국(102)이 새롭게 발행한 증명서 Xyz4의 정보(1501)가 이 리스트에 추가되어 있다.

[0097] 이상이 제1실시예에 따라 전자증명서의 발행 요구에 관한 초기 셋업(설정), 전자증명서에 관한 정보의 표시, 그 발행 요구 및 그 발행된 전자증명서의 수신의 처리단계들로부터, 복합기를 재기동과 상기 발행된 전자증명서의 실시/실행/인에이블링의 처리까지의 전체 처리 시퀀스를, 설명하고 있다.

[0098] 한편, 도 4a 및 4b에 도시된 처리의 시퀀스는 단계 S404-S408에서의 초기의 접속 셋업부터 발행 요구까지와 동작의 단일의 시리얼 시퀀스로서 단계 S419-S427에서의 상기 발행된 전자증명서의 실시/실행/인에이블링을 포함한 처리들로 설명하였지만, 단계 S404-S408에서의 접속 설정등의 초기 접속 셋업 동작에 관한 처리(단계 S401-S418)는, 복합기(100)에 대하여 한번만 행해져도 좋고, 그 후, 다른 CA와의 접속 또는 상기 접속 설정값의 갱신을 위한 특정한 필요가 생기지 않으면 반복되지 않아도 좋다. 예를 들면, 단계 S401～단계 S403의 전자증명서 정보의 표시, 단계 S404～단계 S408의 초기의 접속 셋업 처리, 및 단계 S409～단계 S418의 CA증명서의 취득 처리의 설정 동작은, 첫번째 증명서 발행 요구에 대해서만 행해져도 된다. 그리고, 2회째이후의 전자증명서의 발행 요구에 대해, 동일한 설정을 이용하도록 운용되어도 좋다. 바꿔 말하면, 2회째이후의 전자증명서의 갱신/발행을 행할 때는, 단계 S419～단계 S424에서 전자증명서의 발행 요구와 그것의 응답 처리에 관한 처리 단계들과, 통신 용도의 설정에 관한 처리와, 필요한 경우, 단계 S425～단계 S427의 재기동과 실행/인에이블링에 관한 처리만을 실행하도록 운용되어도 좋다.

[0099] 상기 제1실시예에서는, 복합기(100)는, 자신이 보유한(즉, 자신에 보존된) 웹 페이지형의 RUI를 통해 PC(103)로부터 처리 지시들을 수신하고, 이 지시들에 근거해 제어를 행하였다. 그러나, 관리자로부터 복합기(100)에의 지시를 수신하는데 사용된 상기 인터페이스는, 특별히 이러한 구성에 한정되지 않는다. 각 지시는, 예를 들면, 각

웹 페이지형의 RUI 대신에, 복합기(100)가 보유한 프린터(210)를 이용하여 복합기(100) 자체 또는 복합기(100)에 접속된 또 다른 디바이스(예를 들면, 프린터(210)나 스캐너(211))에 설치된 로컬 유저 인터페이스(LUI)로부터 수신되어도 된다.

[0100] 추가로, 웹 페이지형의 RUI에 대하여, 관리자가 직접 수동으로 조작하여 요구하는 대신에, 예를 들면, 미리 웹 페이지의 입력 영역마다 템플릿과 웹 페이지의 조작 지시마다 룰을 작성하여서, PC 또는 다른 관리 서버로부터 복합기(100)에 요구를 자동으로 입력해 지시하도록, 배치되어도 좋다. 이 경우, 예를 들면, 웹 스크레이핑(scraping)(데이터 마이닝(mining)) 기술을 이용해도 좋다.

[0101] 또한, 제1실시예는 CA증명서의 취득 및 등록을 행하기 위한 조작을 복합기(100)의 관리자가 행하는 구성을 갖지만, CA 증명서가, 필요시에, 첫번째 또는 임의의 이후의 증명서의 발행 요구시에 자동으로 취득되는 구성을 가져도 좋다.

[0102] 또한, 제1실시예에서는, 인증국/등록국(102)으로부터의 증명서의 발행 요구의 응답에 포함된 (서명 검증을 행할 것인가를 가리키는) 서명 검증 설정을 제공하고 있다. 그렇지만, 이 설정가능/조정가능한 설정을 제공하는 대신에, 항상, 서명 검증을 행하거나 또는 서명 검증을 행하지 않도록 사전 설정되어도 좋다.

[0103] 추각로, 제1실시예는 증명서의 발행 요구의 데이터로서 패스워드를 포함하는(예를 들면, 상기 CSR에 패스워드를 포함하는) 구성을 갖지만, 패스워드가 불필요한(예를 들면, 사용되지 않는) 구성을 가져도 좋다.

[0104] 이상 설명한 바와 같이, 제1실시예에 의하면, RUI로부터의 지시에 근거하여 증명서의 자동갱신 프로토콜(즉, 전자증명서 자동갱신 기능)을 사용해서 인증국/등록국 등의 외부장치에 대하여 증명서의 추가/갱신 요구(예를 들면, 증명서 발행 요구)를 발행할 수 있다. 그리고, 그 요구에 대응하는 응답에 의거해, 증명서를 수신해서 복합기에 등록하고, 그 증명서를 사용한 용도를 동작시키는 여러가지의 설정 또는 파라미터들을 설정할 수 있다.

[0105] [제2실시예]

[0106] 다음에, 본 발명의 제2실시예에 대해서 설명한다. 전술한 제1실시예에서는, 복합기(100)가 보유한 웹 서버 기능을 사용해서 웹 페이지형의 RUI를 복합기(100)의 유저에게 제공하였다. 유저는, 그 RUI를 통해 복합기(100)에 지시를 함에 의해서 전자증명서를 사용하는 용도를 동작시키는 여러가지의 설정 또는 파라미터를 추가, 갱신 및 설정하였다. 이 전자증명서는 유효기간이 있으므로, 유효기간이 만료한 전자증명서는 무효가 된다. 이것은, 무효가 된 전자증명서로는 정확한 통신의 인증이 행해질 수 없으므로, 네트워크 통신을 방해할 수 있다. 따라서, 기기가 보유한(보존한) 전자증명서의 유효기간이 그 만기 시각/날짜에 근접하거나 만료한 경우, 전자증명서를 갱신할 필요가 있다. 그렇지만, 전자증명서를 이용하는 기기가 복수대 있을 경우, 그 기기의 관리자가 각 기기의 전자증명서의 유효기간을 취득하고/액세스하고/알아차리고/파악하여 그에 따라 각 전자증명서를 개별적으로 갱신하는 것은 어렵다.

[0107] 그러므로, 제2실시예에서는, 상기 제1실시예와 같은 전자증명서의 자동갱신 기능과, 유저 지시에 근거한 각 갱신을 수동으로 제어하는 대신에, 소정의 일시(즉, 예약시각)에 그 전자증명서의 갱신 기능을 자동적으로 기동하는 제어/관리 동작을, 행할 수 있는 정보처리장치에 대해서 설명한다. 한편, 제2실시예에 있어서, 네트워크 구성, 정보처리장치인 복합기(100)의 하드웨어 구성, 소프트웨어 구성, 키 페어/전자증명서의 리스트 표시 처리, 접속 셋업 처리는, 상기 제1실시예와 같아서, 그 설명을 생략한다.

[0108] 도 18은, 제2실시예에 따른 복합기(100)를 위해 설치된 전자증명서의 갱신 예약 설정 화면의 일례를 도시한 도면이다. 이 화면은, 예를 들면, 여기서 설명된 다른 화면과 같이 웹 페이지형의 RUI에 의해, 표시된다. 이 전자증명서의 갱신 예약의 설정 화면을 통해 전자증명서에 대한 갱신일시(즉, 예약 또는 소정의 시간)를 설정할 수 있다. 제2실시예에서는, 갱신일시(그리고 적절한 경우 갱신 간격의 지정)로서, 갱신일시(1801); 유효기간의 만기전의 기간(1802); 및 주기(1803)를 규정하는 간격 또는 날짜간의 기간의 2개의 설정을 설정하는 것이 가능하다. 그 갱신일시(1801)에서는, 그 갱신의 년, 월, 일, 시를 설정가능하고, 복합기(100)에 보유된(예를 들면, 복합기에 의해 관찰/측정된) 현재 시간이 이 갱신일시(1801)의 설정된 일시로 변경될 때에, 전자증명서의 자동갱신 기능을 실행한다. 그 기간(1802)은, 현재 이용된 전자증명서의 그 유효기간의 만기전의 일수를 지정한다. 복합기(100)에 보유된(즉, 복합기에 의해 관찰/측정된) 현재의 일시로부터 그 유효기간까지의 일이, 상기 기간(1802)에 의해 지정된 일수이하가 되는 경우에, 전자증명서의 자동갱신 기능을 실행한다. 그 기간/날짜(1803)는, 이 기간/날짜에 의해 규정된 것과 같은 주기에 근거한 전자증명서의 자동갱신 기능을 실행한다. 제2실시예에서는, 이 주기는, 소정의 일수(즉, 기간), 매월의 소정 일, 또는 매년의 소정의 일월(즉, 날짜)에 근거하여 설정될 수 있다. 각 전자증명서의 갱신의 갱신일시나 갱신 주기의 이 설정(또는 예약)을, "전자

증명서의 갱신 예약 설정"이라고 칭한다. 각 전자증명서의 갱신 예약 설정이 갱신되면, CPU(201)는 그 갱신된 예약 정보를 HDD(204)에 보존한다.

[0109] 도 18은, 상기 기간(1802)에서, 그 날짜가 유효기간의 만료전 14일이 되면 상기 전자증명서의 자동갱신 기능을 실행하도록 설정된 화면의 일례를 도시한다. 제2실시예에서는, 상술한 전자증명서의 갱신 예약 설정의 종별이 전자증명서의 자동갱신 동작/기능을 행하기 위해 예약하는데 사용되지만, 본 발명은 이것에 한정되지 않는다는 것을 알 것이다. 또한, 다른 시각 및/또는 날짜나 타이밍 지정/예약 방법은, 이 동작을 수행/실행하기 위한 시간에 조건 또는 포인트/기간을 규정하는 한 사용되어도 된다.

[0110] 도 19는, 제2실시예에 따른 복합기(100)에 설정된 전자증명서의 갱신 예약 설정에 근거하여 전자증명서의 자동갱신 기능을 실행할 때 행해진 처리를 설명하는 흐름도다. 여기에서는, 복합기(100)에 대하여 자동갱신을 설정한 예를 도시하지만, 복수의 복합기를 지정(복합기마다 다른 시간 또는 자동갱신 동작을 수행/실행하는 조건을 설정하는 것도 가능)함으로써, 복수의 복합기에 대하여 도 19에 도시된 처리를 실행시킬 수 있다. 이 경우, 도 19의 처리는, 복수의 복합기 사이에서 병렬로 실행된다. 한편, 이 처리는, 예를 들면, CPU(201)에 의해 RAM(203)에 전개된 프로그램을 실행 함에 의해 실현된다.

[0111] 우선, 단계 S1901에서, CPU(201)는, HDD(204)로부터 전자증명서의 갱신 예약 설정을 취득한다. 다음에, 단계 S1902의 처리로 진행되어, CPU(201)는, 현재 이용된 전자증명서의 정보를 취득한다. 이 정보는, 도 17a~17c에 나타낸 것과 같은 정보다. 다음에, 단계 S1903의 처리로 진행되어, CPU(201)는, 복합기(100)가 관찰/측정한 현재의 일시를 취득한다. 여기서는 다른 시간 구역간의 시간차를 고려하여도 된다는 것을 알 것이다. 다음에, 단계 S1904의 처리로 진행되어, CPU(201)는, 전자증명서의 갱신 예약 설정과 그 취득된 전자증명서 정보를 비교하여, 현재 이용된 전자증명서의 갱신이 필요한가 아닌가를 판정한다. 여기서, 전자증명서의 갱신이 필요하지 않다고 판정했을 경우는 단계 S1901의 처리로 되돌아간다. 그 처리는, 소정 기간동안, 또는 단계 S1901에 되돌아가기 전에 또 다른 소정 조건을 충족할 때까지, 대기하여도 된다. 한편, 전자증명서의 갱신이 필요하다고 판정했을 경우는 단계 S1905의 처리로 진행되고, 도 8a 및 8b에서 설명한 "증명서 발행 요구 처리" 제어의 처리로 진행된다. 도 8a 및 8b의 처리가 완료한 후, 단계 S1906의 처리로 진행된다.

[0112] 상술한 처리에 의해, 유저로부터의 수동 지시없이, 지정한/사전설정된 갱신일시나 갱신 주기에 근거하여, 자동적으로 전자증명서의 갱신이 가능해진다. 이에 따라, 관리자에게 각 기기의 전자증명서의 유효기간을 파악하고/알아차리고/결정하도록 요구하지 않고, 유저의 작업부담을 삭감하면서, 각 기기의 전자증명서를 유지, 즉 소망한 타이밍에서 갱신할 수 있다.

[0113] 단계 S1906에서, CPU(201)는, 전자증명서를 갱신했을 때, 복합기(100)의 재기동이 필요한가 아닌가를 판단한다. 여기서, CPU(201)가, 재기동이 필요하다고 판정했을 경우는, 단계 S1907의 처리로 진행되어, 도 9에 도시된 "재기동/설정 실행/인에이블링 처리"를 실행한다. 한편, CPU(201)가, 재기동이 불필요하다고 판단했을 경우는, 그 자동 갱신동작 처리를 종료한다. 이것은, 필요한 경우에만 재기동하도록, 복합기(100)의 재기동을 제어하는 것이다. 예를 들면, 이것은, 복합기(100)가 이용하는 전자증명서를 전환한 경우와, 재기동을 요구하지 않는 TLS와 재기동을 요구하는 IEEE802.1X에 대해 네트워크 구성을 변경하는 경우를 구별한다.

[0114] 이상 설명한 바와 같이, 제2실시예에 의하면, 전자증명서의 갱신의 타이밍을 예약/특정/규정해두는 것에 의해, 유저 지시없이, 복합기가 자동적으로 전자증명서의 발행 요구를 송신하여 전자증명서의 갱신 및 등록을 행할 수 있다. 이에 따라, 유저가 전자증명서의 유효기간을 (예를 들면, 그러한 지식/정보에 액세스하지 못하는 것으로 인해) 알지 못할 경우에도, 전자증명서가 (예를 들면, 그것이 만료되었기 때문에) 무효가 되고 그 네트워크 통신이 방해되는 사태를 방지할 수 있다.

[0115] 그 밖의 실시예

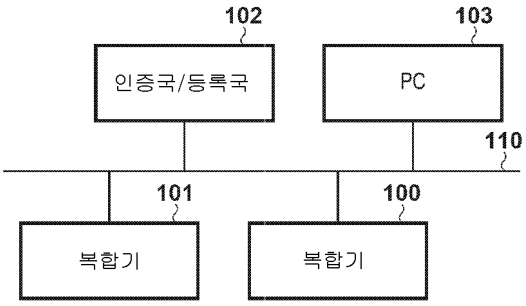
[0116] 또한, 본 발명의 실시예들은, 기억매체(보다 완전하게는 '(비일시적) 컴퓨터 판독 가능한 기억매체'라고도 함)에 레코딩된 컴퓨터 실행가능한 명령어들(예를 들면, 하나 이상의 프로그램)을 판독하고 실행하여 상술한 실시예들의 하나 이상의 기능을 수행하는 것 및/또는 상술한 실시예들의 하나 이상의 기능을 수행하기 위한 하나 이상의 회로(예를 들면, 특정 용도 지향 집적회로(ASIC))를 구비하는 것인, 시스템 또는 장치를 갖는 컴퓨터에 의해 실현되고, 또 예를 들면 상기 기억매체로부터 상기 컴퓨터 실행가능한 명령어를 판독하고 실행하여 상기 실시예들의 하나 이상의 기능을 수행하는 것 및/또는 상술한 실시예들의 하나 이상의 기능을 수행하는 상기 하나 이상의 회로를 제어하는 것에 의해 상기 시스템 또는 상기 장치를 갖는 상기 컴퓨터에 의해 행해지는 방법에 의해 실현될 수 있다. 상기 컴퓨터는, 하나 이상의 프로세서(예를 들면, 중앙처리장치(CPU), 마이크로처리장치

(MPU))를 구비하여도 되고, 컴퓨터 실행 가능한 명령어를 판독하여 실행하기 위해 별개의 컴퓨터나 별개의 프로세서의 네트워크를 구비하여도 된다. 상기 컴퓨터 실행가능한 명령어를, 예를 들면 네트워크나 상기 기억매체로부터 상기 컴퓨터에 제공하여도 된다. 상기 기억매체는, 예를 들면, 하드 디스크, 랜덤액세스 메모리(RAM), 판독전용 메모리(ROM), 분산형 컴퓨팅 시스템의 스토리지, 광디스크(콤팩트 디스크(CD), 디지털 다기능 디스크(DVD) 또는 블루레이 디스크(BD)™등), 플래시 메모리 소자, 메모리 카드 등 중 하나 이상을 구비하여도 된다.

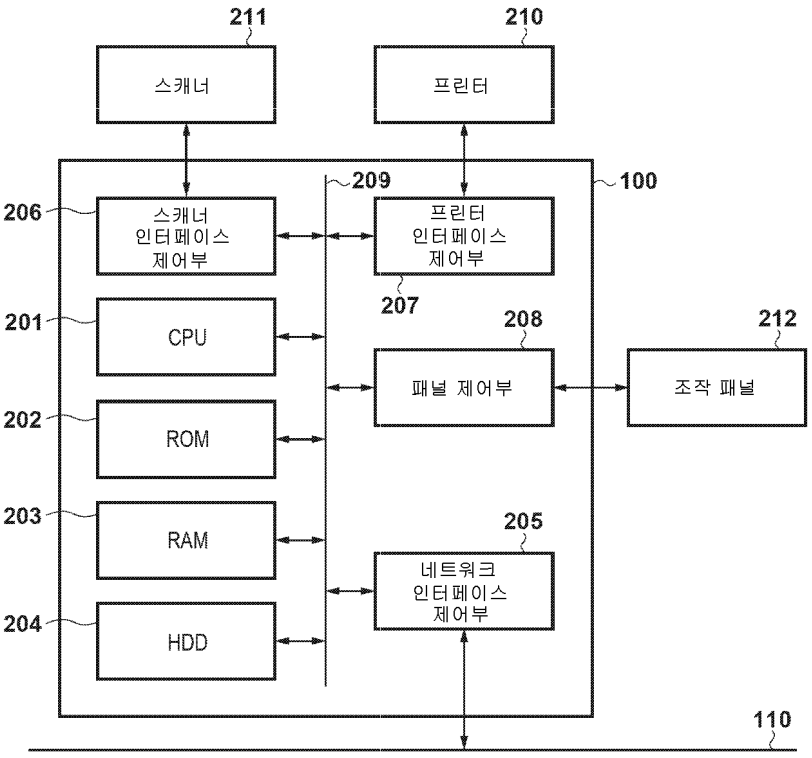
[0117] 본 발명을 실시예들을 참조하여 설명하였지만, 본 발명은 상기 개시된 실시예들에 한정되지 않는다는 것을 알 것이다. 당업자라면 첨부된 청구항에 기재된 것처럼, 본 발명의 범위로부터 벗어나지 않고 여러가지로 변경 및 변형할 수도 있다는 것을 알 것이다. (임의의 첨부하는 청구항, 요약서 및 도면을 포함하는) 본 명세서에 개시된 특징들 전부, 및/또는 그렇게 개시된 임의의 방법 또는 처리의 단계들의 전부는, 이러한 특징들 및/또는 단계들 중 적어도 일부가 상호 배타적인 조합을 제외하고는 어떠한 조합으로도 조합되어도 된다.

도면

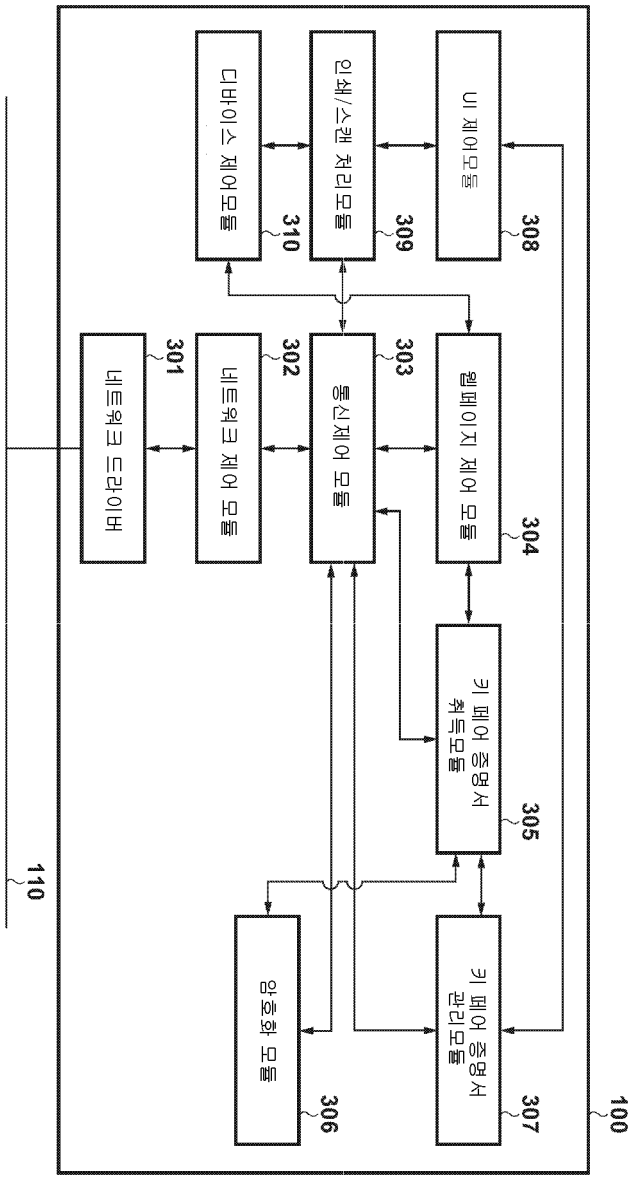
도면1



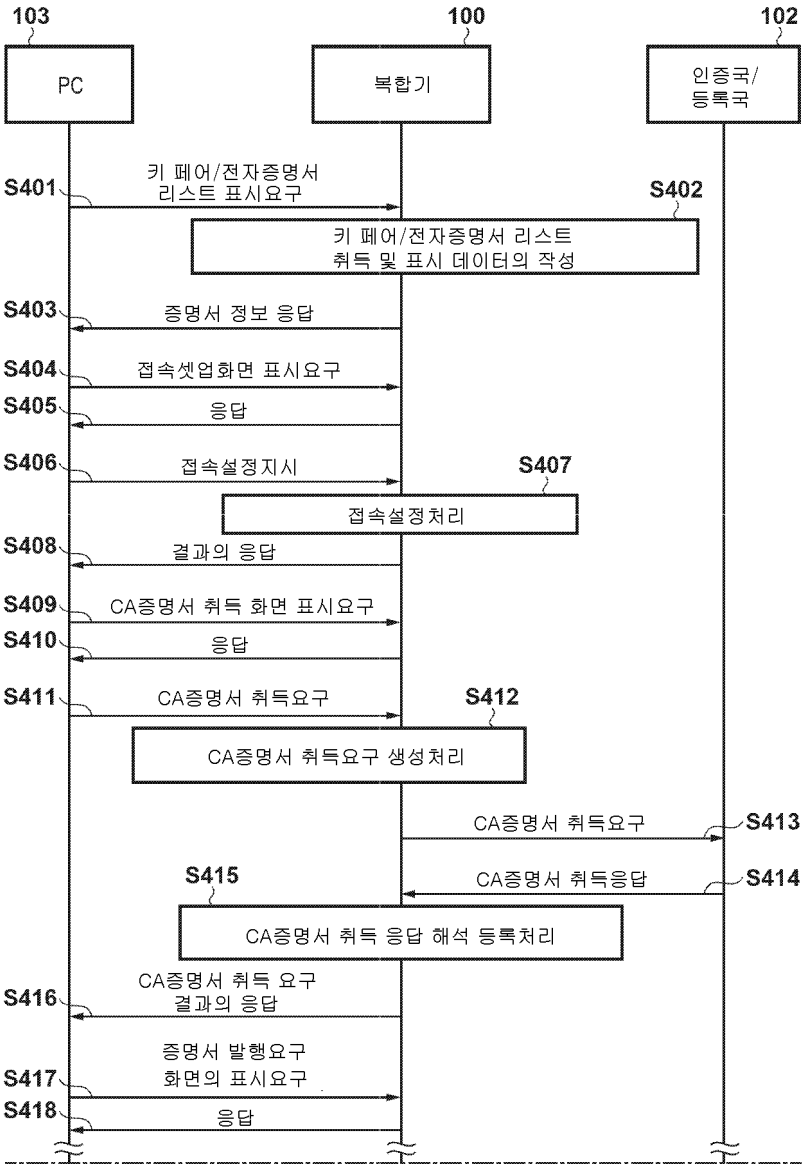
도면2



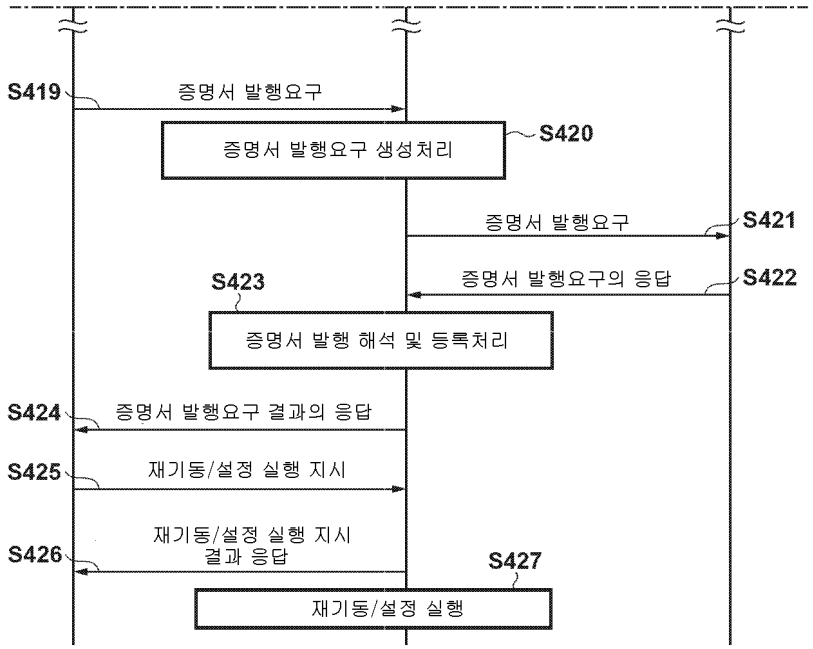
도면3


UI 제어모듈
308
인쇄/스캔 처리모듈
309
디바이스 제어모듈
310
웹페이지 제어 모듈
304
통신제어 모듈
303
네트워크 제어 모듈
302
네트워크 드라이버
301
키 페어 증명서 취득모듈
305
키 페어 증명서 관리모듈
307
암호화 모듈
306
100
110

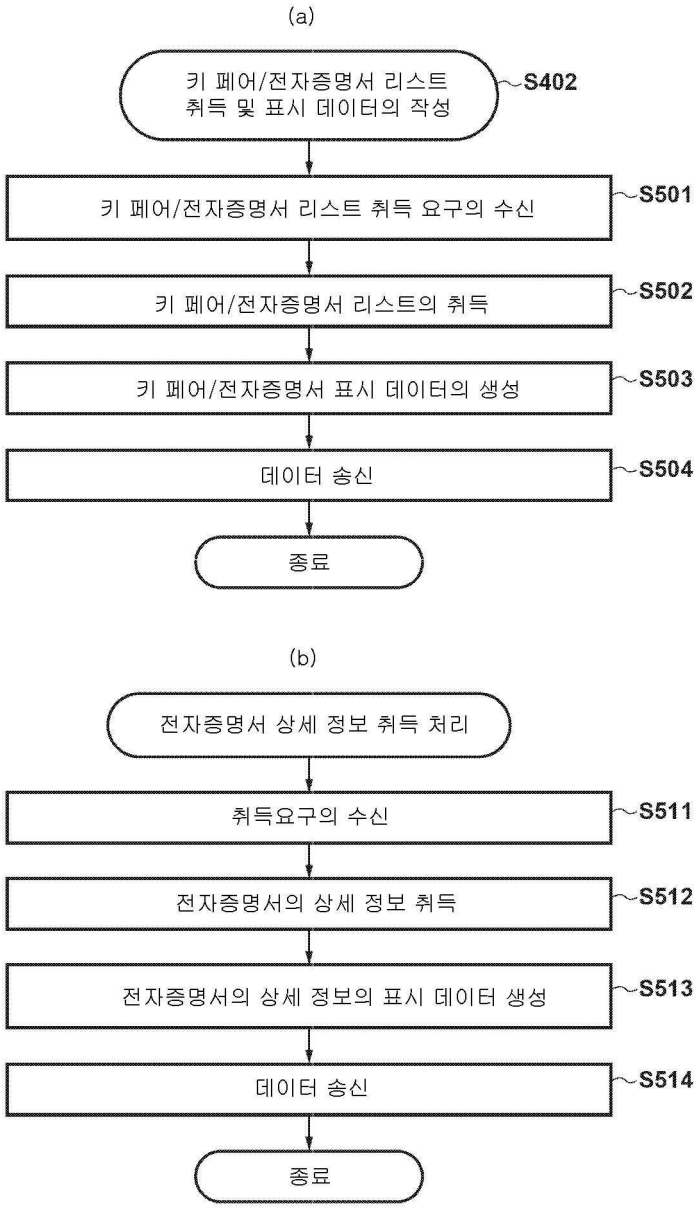
도면4a


103
PC
100
복합기
102
인증국/
등록국
S401
키 페어/전자증명서
리스트 표시요구
S402
키 페어/전자증명서 리스트
취득 및 표시 데이터의 작성
S403
증명서 정보 응답
S404
접속셋업화면 표시요구
S405
응답
S406
접속설정지시
S407
접속설정처리
S408
결과의 응답
S409
CA증명서 취득 화면 표시요구
S410
응답
S411
CA증명서 취득요구
S412
CA증명서 취득요구 생성처리
CA증명서 취득요구
S413
S415
CA증명서 취득응답
S414
CA증명서 취득 응답 해석 등록처리
S416
CA증명서 취득 요구
결과의 응답
S417
증명서 발행요구
화면의 표시요구
S418
응답

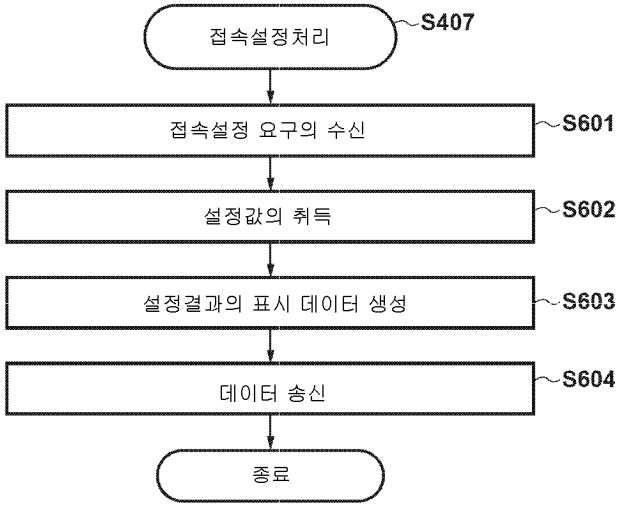
도면4b


S419
증명서 발행요구
증명서 발행요구 생성처리
S420
증명서 발행요구
S421
S423
증명서 발행요구의 응답
S422
증명서 발행 해석 및 등록처리
S424
증명서 발행요구 결과의 응답
S425
재기동/설정 실행 지시
재기동/설정 실행 지시
결과 응답
S426
S427
재기동/설정 실행

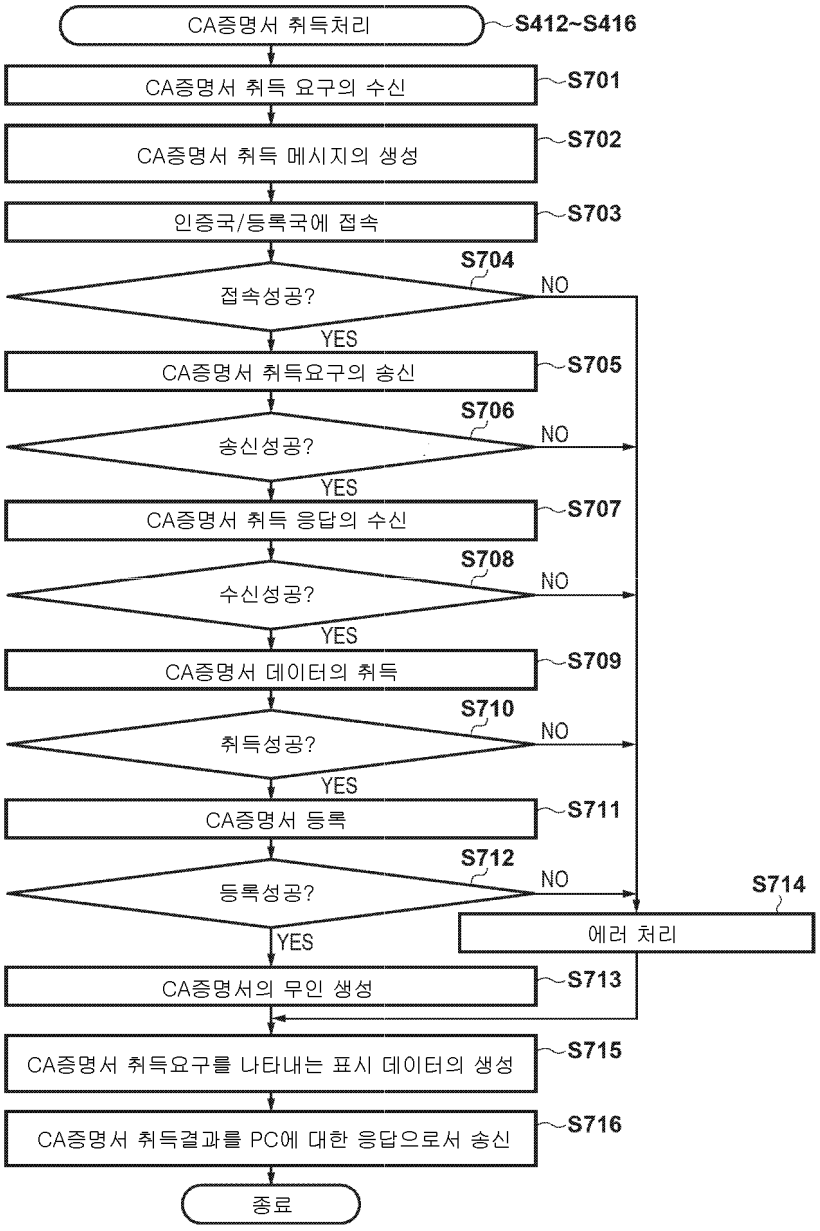
도면5


(a)
키 페어/전자증명서 리스트 취득 및 표시 데이터의 작성
S402
키 페어/전자증명서 리스트 취득 요구의 수신
S501
키 페어/전자증명서 리스트의 취득
S502
키 페어/전자증명서 표시 데이터의 생성
S503
데이터 송신
S504
종료
(b)
전자증명서 상세 정보 취득 처리
취득요구의 수신
S511
전자증명서의 상세 정보 취득
S512
전자증명서의 상세 정보의 표시 데이터 생성
S513
데이터 송신
S514
종료

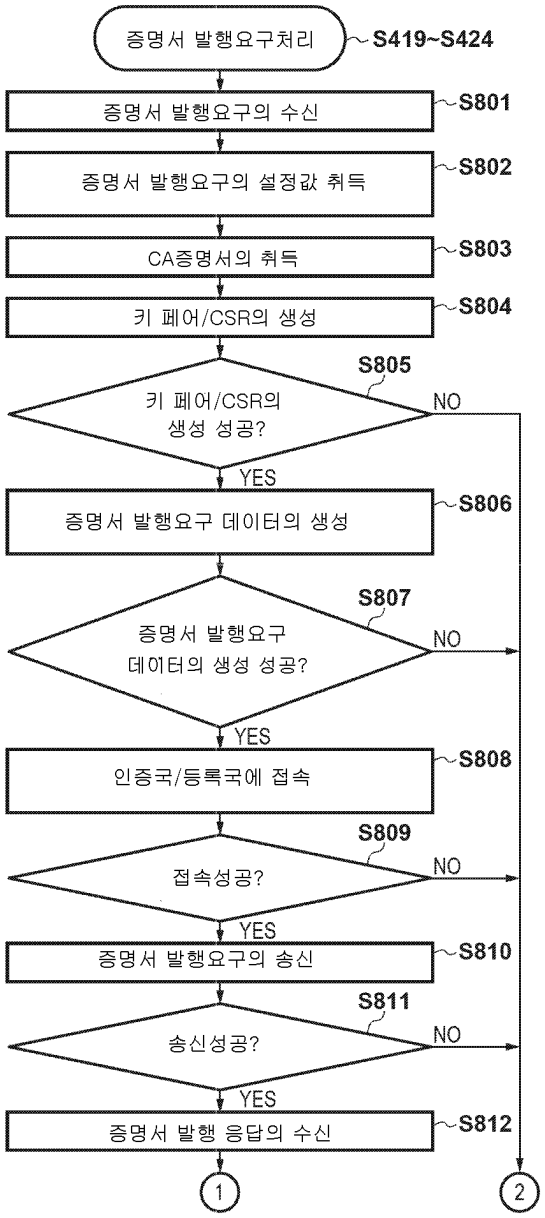
도면6


접속설정처리
S407
접속설정 요구의 수신
S601
설정값의 취득
S602
설정결과의 표시 데이터 생성
S603
데이터 송신
S604
종료

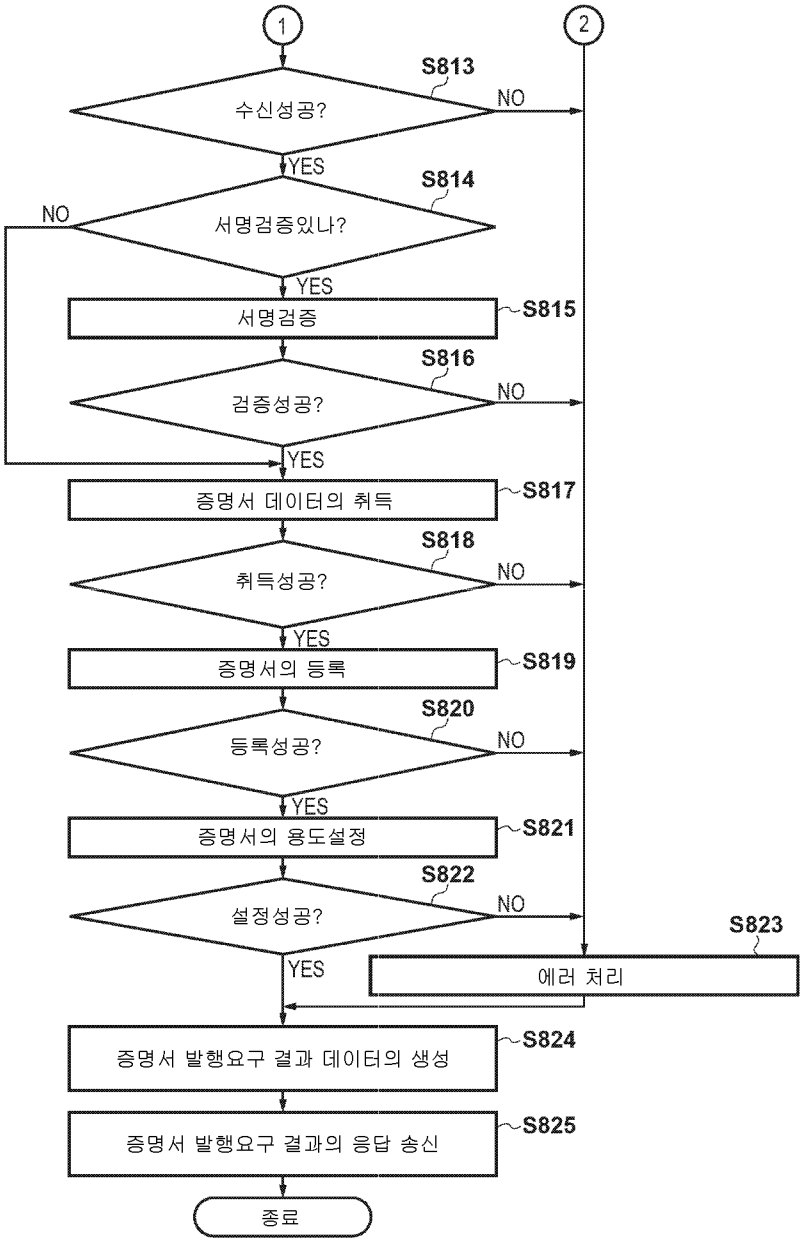
도면7


CA증명서 취득처리
S412~S416
CA증명서 취득 요구의 수신
S701
CA증명서 취득 메시지의 생성
S702
인증국/등록국에 접속
S703
S704
접속성공?
NO
YES
CA증명서 취득요구의 송신
S705
S706
송신성공?
NO
YES
CA증명서 취득 응답의 수신
S707
S708
수신성공?
NO
YES
CA증명서 데이터의 취득
S709
S710
취득성공?
NO
YES
CA증명서 등록
S711
S712
등록성공?
NO
YES
S714
에러 처리
CA증명서의 무인 생성
S713
CA증명서 취득요구를 나타내는 표시 데이터의 생성
S715
CA증명서 취득결과를 PC에 대한 응답으로서 송신
S716
종료

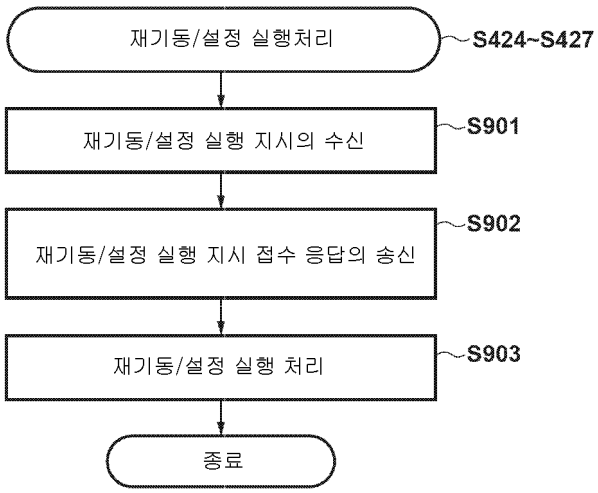
도면8a


증명서 발행요구처리
S419~S424
증명서 발행요구의 수신
S801
증명서 발행요구의 설정값 취득
S802
CA증명서의 취득
S803
키 페어/CSR의 생성
S804
S805
키 페어/CSR의 생성 성공?
NO
YES
증명서 발행요구 데이터의 생성
S806
S807
증명서 발행요구 데이터의 생성 성공?
NO
YES
인증국/등록국에 접속
S808
S809
접속성공?
NO
YES
증명서 발행요구의 송신
S810
S811
송신성공?
NO
YES
증명서 발행 응답의 수신
S812
1
2

도면8b

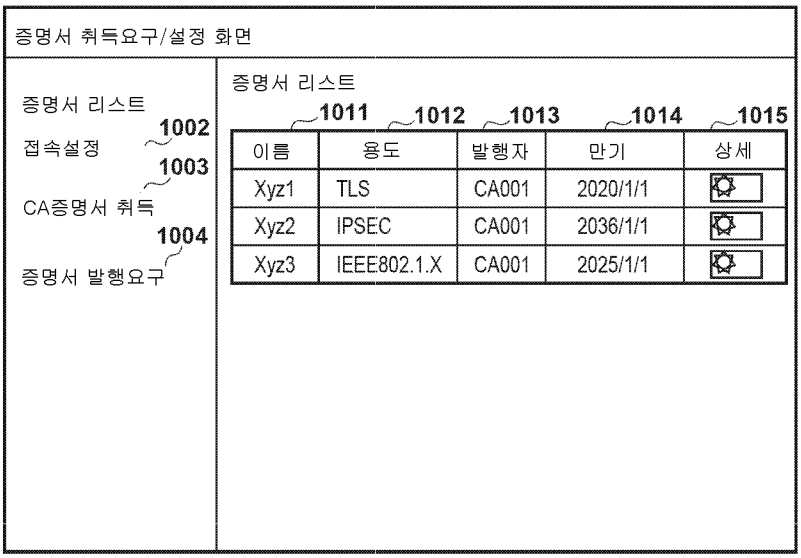

1
2
S813
수신성공?
NO
YES
S814
서명검증있나?
NO
YES
서명검증
S815
S816
검증성공?
NO
YES
증명서 데이터의 취득
S817
S818
취득성공?
NO
YES
증명서의 등록
S819
S820
등록성공?
NO
YES
증명서의 용도설정
S821
S822
설정성공?
NO
S823
YES
에러 처리
증명서 발행요구 결과 데이터의 생성
S824
증명서 발행요구 결과의 응답 송신
S825
종료

도면9

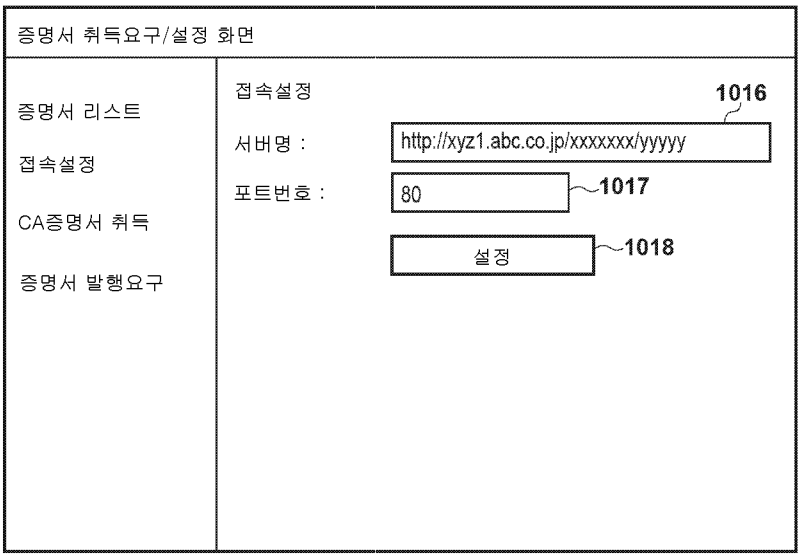

재기동/설정 실행처리
S424~S427
재기동/설정 실행 지시의 수신
S901
재기동/설정 실행 지시 접수 응답의 송신
S902
재기동/설정 실행 처리
S903
종료

도면10

(a)

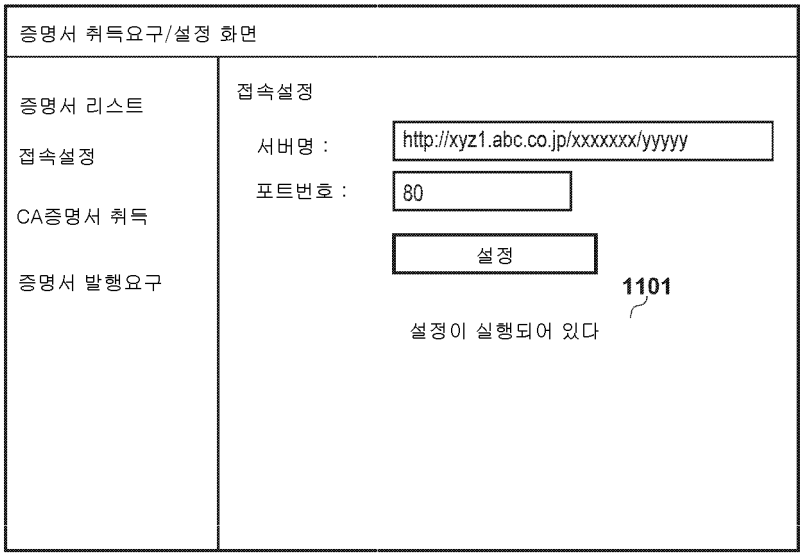

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
1002
1003
1004
증명서 리스트
1011
1012
1013
1014
1015
이름
용도
발행자
만기
상세
Xyz1
TLS
CA001
2020/1/1
Xyz2
IPSEC
CA001
2036/1/1
Xyz3
IEEE802.1.X
CA001
2025/1/1

(b)

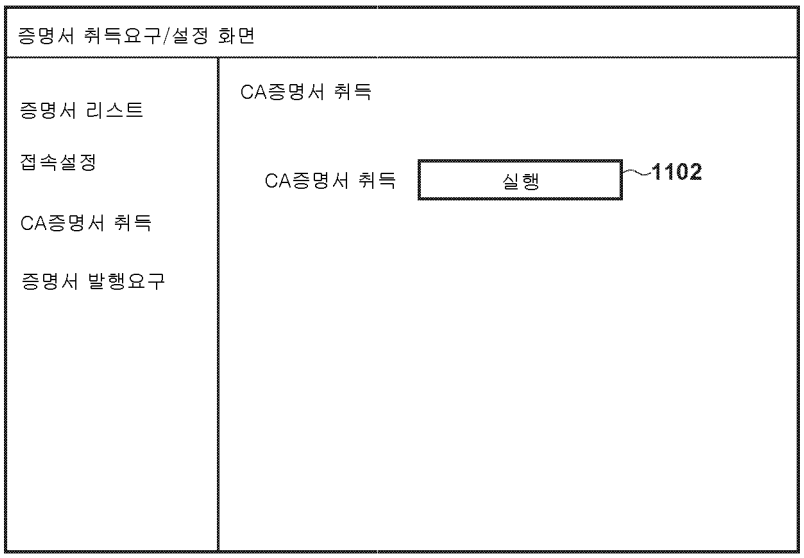

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
접속설정
1016
서버명 :
http://xyz1.abc.co.jp/xxxxxxx/yyyyy
포트번호 :
80
1017
설정
1018

도면11

(a)

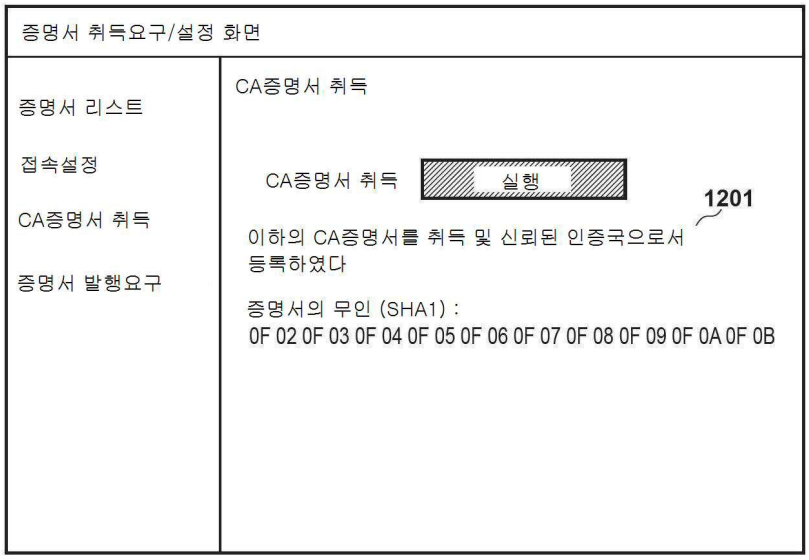

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
접속설정
서버명 :
http://xyz1.abc.co.jp/xxxxxxx/yyyyy
포트번호 :
80
설정
1101
설정이 실행되어 있다

(b)

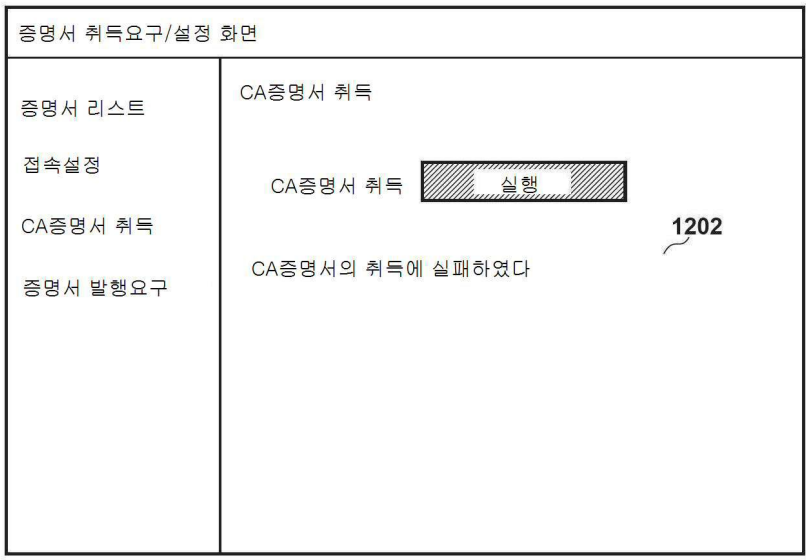

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
CA증명서 취득
CA증명서 취득
실행
1102

도면12

(a)

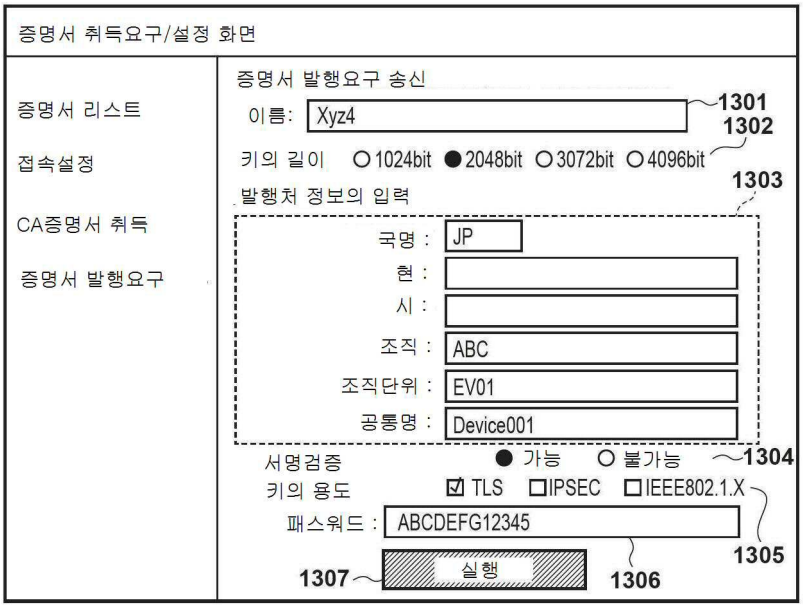

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
CA증명서 취득
CA증명서 취득
실행
1201
이하의 CA증명서를 취득 및 신뢰된 인증국으로서 등록하였다
증명서의 무인 (SHA1) :
0F 02 0F 03 0F 04 0F 05 0F 06 0F 07 0F 08 0F 09 0F 0A 0F 0B

(b)

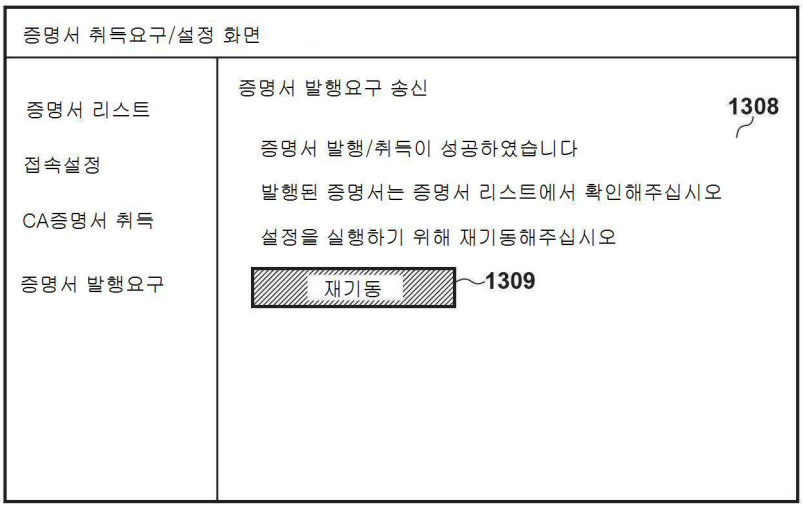

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
CA증명서 취득
CA증명서 취득
실행
1202
CA증명서의 취득에 실패하였다

도면13

(a)

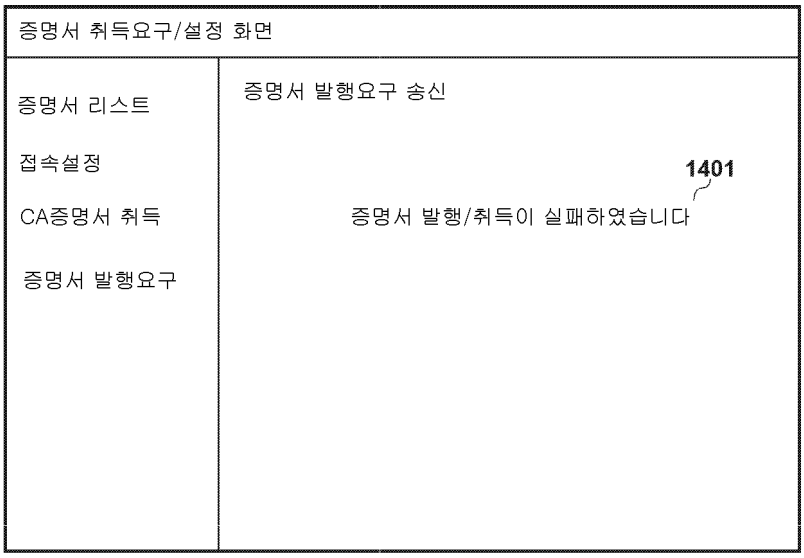

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
증명서 발행요구 송신
이름: Xyz4
1301
1302
키의 길이 ○1024bit ●2048bit ○3072bit ○4096bit
1303
발행처 정보의 입력
국명 : JP
현 :
시 :
조직 : ABC
조직단위 : EV01
공통명 : Device001
서명검증 ● 가능 ○ 불가능
1304
키의 용도 ☑ TLS ☐IPSEC ☐IEEE802.1.X
패스워드 : ABCDEFG12345
1305
1307
실행
1306

(b)

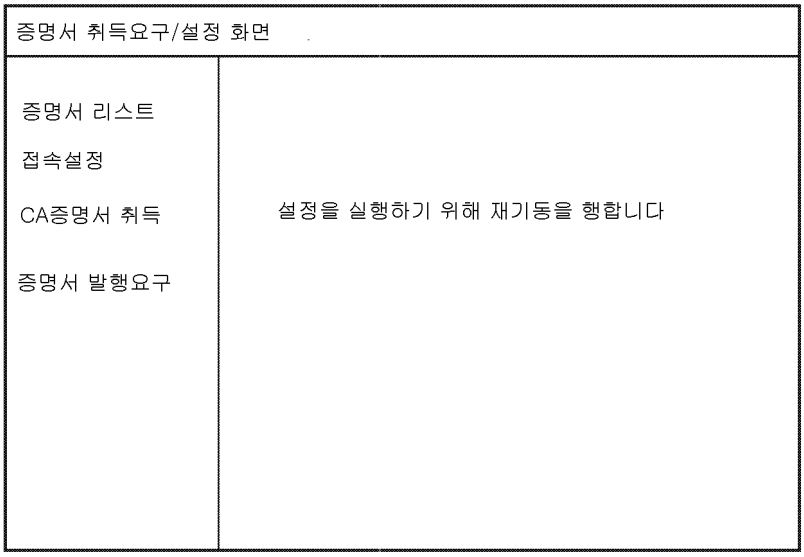

증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
증명서 발행요구 송신
1308
증명서 발행/취득이 성공하였습니다
발행된 증명서는 증명서 리스트에서 확인해주십시오
설정을 실행하기 위해 재기동해주십시오
재기동
1309

도면14

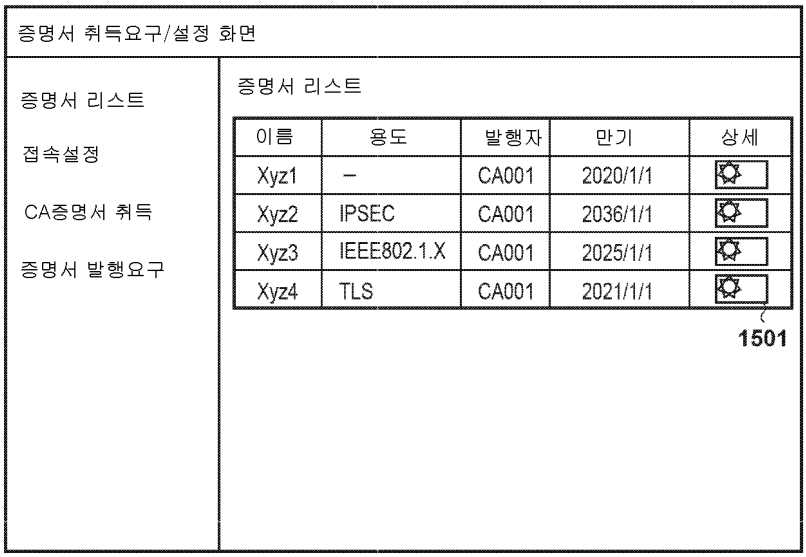
(a)


증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
증명서 발행요구 송신
1401
증명서 발행/취득이 실패하였습니다

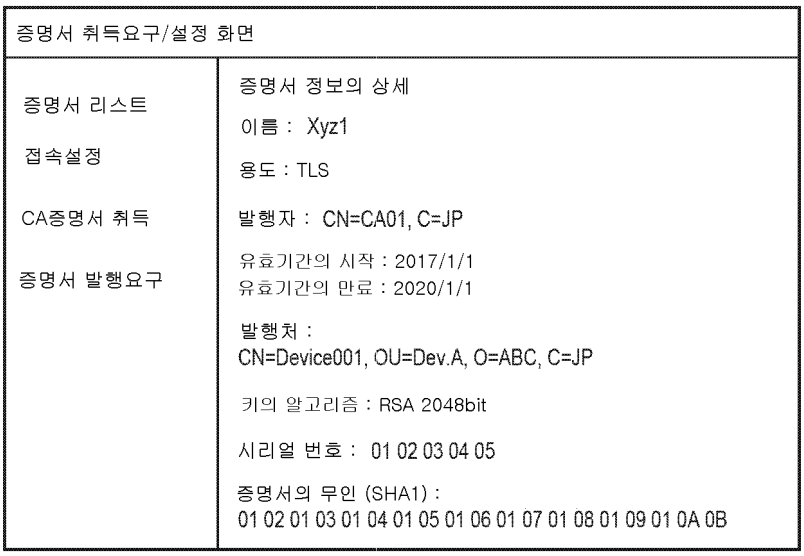
(b)


증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
설정을 실행하기 위해 재기동을 행합니다

도면15


증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
증명서 리스트
이름 용도 발행자 만기 상세
Xyz1 – CA001 2020/1/1
Xyz2 IPSEC CA001 2036/1/1
Xyz3 IEEE802.1.X CA001 2025/1/1
Xyz4 TLS CA001 2021/1/1
1501

도면16


증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
증명서 정보의 상세
이름 : Xyz1
용도 : TLS
발행자 : CN=CA01, C=JP
유효기간의 시작 : 2017/1/1
유효기간의 만료 : 2020/1/1
발행처 :
CN=Device001, OU=Dev.A, O=ABC, C=JP
키의 알고리즘 : RSA 2048bit
시리얼 번호 : 01 02 03 04 05
증명서의 무인 (SHA1) :
01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 0B

도면17a

이름	용도	발행자	유효 기간의 시작	유효 기간의 만료	발행처	알고 리즘	키의 길이	시리얼 번호	무인
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

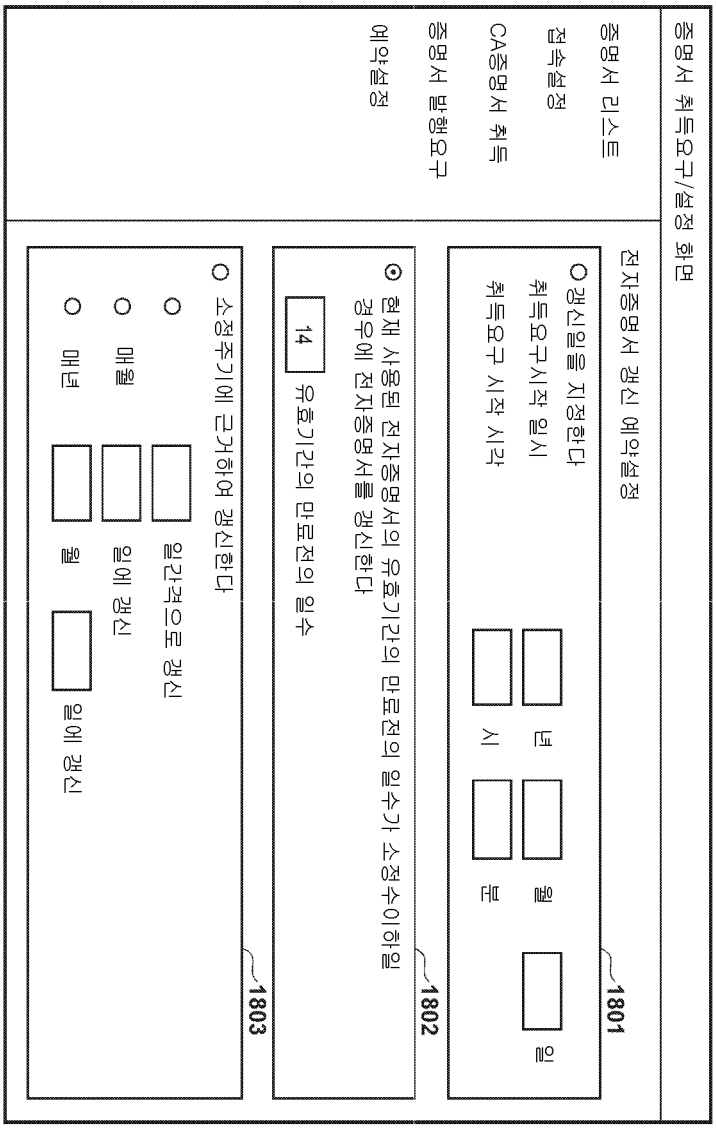
도면17b

이름	용도	발행자	유효 기간의 시작	유효 기간의 만료	발행처	알고 리즘	키의 길이	시리얼 번호	무인
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	무	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

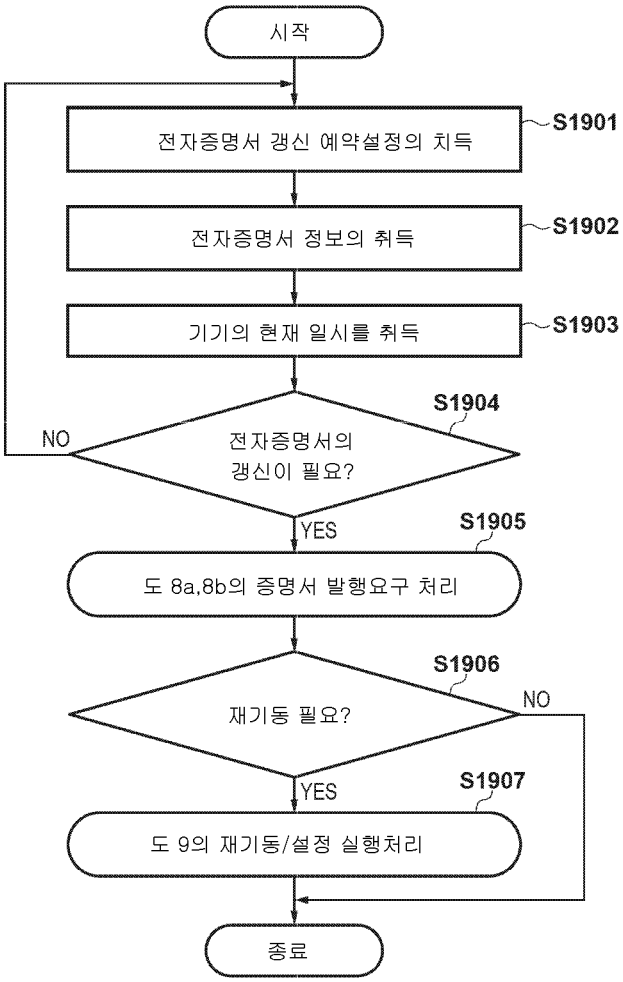
도면17c

이름	용도	발행자	유효 기간의 시작	유효 기간의 만료	발행처	알고리즘	키의 길이	시리얼 번호	무인
Xyz1	무	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

도면18


증명서 취득요구/설정 화면
증명서 리스트
접속설정
CA증명서 취득
증명서 발행요구
예약설정
전자증명서 갱신 예약설정
1801
○ 갱신일을 지정한다
취득요구시작 일시
취득요구 시작 시각
년
월
일
시
분
1802
⊙ 현재 사용된 전자증명서의 유효기간의 만료전의 일수가 소정수이하일 경우에 전자증명서를 갱신한다
14
유효기간의 만료전의 일수
1803
○ 소정주기에 근거하여 갱신한다
○
일간격으로 갱신
○ 매월
일에 갱신
○ 매년
월
일에 갱신

도면19


시작
전자증명서 갱신 예약설정의 치득
S1901
전자증명서 정보의 취득
S1902
기기의 현재 일시를 취득
S1903
S1904
NO
전자증명서의
갱신이 필요?
YES
S1905
도 8a,8b의 증명서 발행요구 처리
S1906
재기동 필요?
NO
YES
S1907
도 9의 재기동/설정 실행처리
종료