(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G06F 15/00

(45) 공고일자 2004년05월31일
(11) 등록번호 10-0433439
(24) 등록일자 2004년05월18일

(21) 출원번호 10-2001-0052476
(22) 출원일자 2001년08월29일

(65) 공개번호 10-2002-0018113
(43) 공개일자 2002년03월07일

(30) 우선권주장 JP-P-2000-00261065 2000년08월30일 일본(JP)

(73) 특허권자 가부시키가이샤 히타치세이사쿠쇼
일본 도쿄토 치요다쿠 간다스루가다이 4쪼메 6반치

(72) 발명자 후지시로다까히로
일본도꾜도지요다꾸마루노우찌1쪼메5-1신마루노우찌빌딩가부시키가이샤히타치세이사쿠쇼지적소유권본부내

데즈까사또루
일본도꾜도지요다꾸마루노우찌1쪼메5-1신마루노우찌빌딩가부시키가이샤히타치세이사쿠쇼지적소유권본부내

구마가이요꼬
일본도꾜도지요다꾸마루노우찌1쪼메5-1신마루노우찌빌딩가부시키가이샤히타치세이사쿠쇼지적소유권본부내

모리오도모하루
일본도꾜도지요다꾸마루노우찌1쪼메5-1신마루노우찌빌딩가부시키가이샤히타치세이사쿠쇼지적소유권본부내

미야자끼유따까
일본도꾜도지요다꾸마루노우찌1쪼메5-1신마루노우찌빌딩가부시키가이샤히타치세이사쿠쇼지적소유권본부내

(74) 대리인 장수길
구영창

심사관 : 복진요

(54) 증명서의 유효성 확인 방법 및 장치

요약

공개 키 증명서의 유효성 확인을 의뢰한 이후부터, 해당 유효성이 확인될 때까지 걸리는 시간을 단축한다. 증명서 유효성 확인 센터 VC는 브릿지 인증국 CA $_{bridge}$ 로부터 각 단말기 인증국 CA까지의 패스의 검색, 검증을 정기적으로 행하고, 검증이 성립한 패스를 단말기 수용 인증국에 대응하여 패스 DB에 등록한다. 또한, 엔드 엔티티 EE로부터 증명서의 유효성 확인 의뢰가 있었던 경우, 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA에 대응된 패스와 의뢰 대상 증명서를 발행한 단말기 수용 인증국 CA에 대응된 패스가 패스 DB에 등록되어 있는지의 여부를 조사하여, 양자가 등록되어 있는 경우에만 해당 증명서는 유효하다고 판단한다.

대표도

도 1

색인어

공개 키 증명서, 단말기 수용 인증국, 유효성, 엔드 엔티티, 대상 증명서

명세서

도면의 간단한 설명

도 1은 본 발명의 일 실시예가 적용된 PKI 시스템의 개략 구성도.
도 2는 도 1에 도시한 PKI 시스템에서의 각 인증국 CA의 관계의 일례를 나타내는 도면.
도 3은 도 1에 도시한 엔드 엔티티 EE의 개략 구성도.
도 4는 도 1에 도시한 인증국 CA의 개략 구성도.
도 5는 도 1에 도시한 증명서 유효성 확인 센터 VC의 개략 구성도.
도 6은 도 3 도 5에 도시한 엔드 엔티티 EE, 인증국 CA 및 증명서 유효성 확인 센터 VC의 각각의 하드웨어 구성예를 나타내는 도면.
도 7은 도 5에 도시한 증명서 유효성 확인 센터 VC에서 행해지는 패스의 검색, 검증 및 관리 동작을 설명하기 위한 순서도.
도 8은 도 5에 도시한 증명서 유효성 확인 센터 VC에서 행해지는 패스의 검색, 검증 및 관리 동작을 설명하기 위한 순서도.
도 9는 각 인증국 CA가 도 2에 도시한 관계에 있는 경우에, 증명서 유효성 확인 센터 VC의 패스 검색부(32)에서 검출되는 브릿지 인증국 CA_{bridge} 로부터 각 단말 기 수용 인증국 CA까지의 패스를 나타내는 도면.
도 10은 도 5에 도시한 증명서 유효성 확인 센터 VC에서 행해지는 공개 키 증명서의 유효성의 확인 동작을 설명하기 위한 순서도.
도 11은 도 5에 도시한 증명서 유효성 확인 센터 VC에서 행해지는 공개 키 증명서의 유효성의 확인 동작을 설명하기 위한 순서도.
도 12는 종래의 PKI에서 인증국이 복수개 있는 경우에 있어서의 각 인증국의 관계의 일례를 나타내는 도면.
〈도면의 주요 부분에 대한 부호의 설명〉
10a : 처리부
10b : 기억부
11 : 전자 문서 보유부
12 : 키 보유부
13 : 검증 대상 보유부
14 : 서명 생성부
15 : 서명 검증부
16 : 통신부
17 : 입출력부
18 : 제어부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 PKI(Public Key Infrastructure)에 있어서, 어떤 단말기가 수취한 전자 수속에 대한 서명을 검증하기 위한 공개 키 증명서가 해당 단말기가 신뢰하는 인증국과는 다른 인증국이 발행한 것인 경우에, 그 유효성을 확인하는 데 적합한 기술에 관한 것이다.
민간계, 공공계의 여러 조직, 단체에 있어서, 종래 지면에서 행한 여러가지 수속을 전자화하도록 PKI의 도입, 정비가 진행되고 있다.
도 12는 종래의 PKI에서 인증국이 복수있는 경우에 있어서의 각 인증국의 관계를 나타내고 있다.
도시한 바와 같이 공개 키 증명서의 발행과 그 관리를 행하는 각 인증국은 루트 인증국 CA1을 정점으로 하는 트리 구조를 갖는 그룹을 형성하고 있다. 이 그룹은 시큐리티 도메인이라 불리고 있다. 루트 인증국 CA1은 자신보다 하나 하

류측에 위치하는 각 인증국 CA2 $_1$ CA2 $_n$ 에 대하여 공개 키 증명서를 발행한다. 또한, 인증국 CA2 $_1$ CA2 $_{n1}$ 각각은 자신보다 하나 하류측에 위치하는 각 인증국 CA3 $_1$ CA3 $_{n2}$ 에 대하여 공개 키 증명서를 발행한다. 이와 같이 트리 상, 하나 상류측에 위치하는 인증국이 자신보다 하나 하류측에 위치하는 인증국에 대하여 공개 키 증명서를 발행한다. 그리고, 트리 상, 최하류에 위치하는 인증국(이하, 단말기 수용 인증국이라 함) CAS $_1$ CAS $_{nm}$ 은 전자 수속을 행하는 사용자 단말기(이하, 엔드 엔티티라 함) EE $_1$ EE $_x$ 에 대하여 공개 키 증명서를 발행한다.

엔드 엔티티 EE $_1$ EE $_x$ 각각이 전자 문서의 서명에 사용하는 비밀 키(서명 키)의 정당성은 자신을 수용하는 단말기 수용 인증국 CAS $_1$ CAS $_{nm}$ 이 발행한 공개 키 증명서에 의해 증명되고, 단말기 수용 인증국 CAS $_1$ CAS $_{nm}$ 각각이 발행하는 공개 키 증명서의 서명에 사용하는 비밀 키의 정당성은 자신을 수용하는 인증국 CA(S-1) $_1$ CA(S-1) $_{n(m-1)}$ 이 발행한 공개 키 증명서에 의해 증명된다. 따라서, 엔드 엔티티 EE $_1$ EE $_x$ 각각이 서명에 사용하는 비밀 키는 최종적으로, 루트 인증국 CA1이 발행하는 공개 키 증명서에 의해 증명된다. 이 엔드 엔티티 EE $_1$ EE $_x$ 가 서명에 사용하는 키의 정당성을 최종적으로 증명하는 인증국, 다시 말하면, 엔드 엔티티 EE $_1$ EEx가 신뢰하는 트리 상, 최상류측의 인증국을 트러스트 앵커라 부른다.

그런데, 도 12에 있어서 엔드 엔티티 EE $_1$ 은 엔드 엔티티 EE $_x$ 로 송신해야 할 신청서 등의 전자 문서에 대하여 엔드 엔티티 EE $_1$ 이 보유하는 자신의 비밀 키로 서명을 행한다. 그리고, 서명한 전자 문서에 엔드 엔티티 EE $_1$ 을 수용하는 단말기 수용 인증국 CAS $_1$ 이 발행한 상기 비밀 키와 쌍인 공개 키 증명서를 첨부하여 엔드 엔티티 EE $_x$ 로 송신한다.

엔드 엔티티 EE $_x$ 는 엔드 엔티티 EE $_1$ 로부터 수취한 전자 문서 서명을 해당 전자 문서에 첨부된 공개 키 증명서를 이용하여 검증할 수 있다. 그러나, 공개 키 증명서는 엔드 엔티티 EE $_x$ 를 수용하는 단말기 수용 인증국 CAS $_{nm}$ 이 발행한 것이 아니기 때문에, 엔드 엔티티 EE $_x$ 는 해당 공개 키 증명서를 바로 신뢰할 수는 없다. 이 경우, 엔드 엔티티 EE $_x$ 는 자신의 트러스트 앵커인 루트 인증국 CA1에 의해 해당 공개 키 증명서의 유효성이 증명되는 것임을 확인해야 한다. 이 공개 키 증명서의 유효성 확인 처리는 다음 순서에 따라 행해진다.

① 트러스트 앵커로부터 공개 키 증명서의 발행처 인증국까지의 패스의 검색

트러스트 앵커(여기서는 루트 인증국 CA1)를 기점 인증국으로 하고, 기점 인증국이 발행한 공개 키 증명서의 피발행처를 조사하여, 해당 피발행처에 인증국이 포함되는 경우에는 해당 인증국이 발행한 공개 키 증명서의 피발행처를 더 조사하는 처리를 해당 공개 키 증명서의 피발행처에, 공개 키 증명서의 발행처 인증국(여기서는 엔드 엔티티 EE $_1$ 을 수용하는 단말기 수용 인증국 CAS $_1$)이 포함될 때까지 계속하고, 트러스트 앵커로부터 공개 키 증명서의 발행처 인증국까지의 패스를 검색한다.

② 검출한 패스의 검증

상기 ①에 의해 검출한 패스 상의 각 인증국으로부터 패스 상에 있어서 해당 인증국의 하나 하류측의 인증국에 대하여 발행한 공개 키 증명서를 입수한다. 그리고, 유효성 확인 대상의 공개 키 증명서(여기서는 단말기 수용 인증국 CAS $_1$ 이 엔드 엔티티 EE $_1$ 에 대해서 발행한 공개 키 증명서)의 서명을 해당 공개 키 증명서를 발행한 인증국(여기서는 단말기 수용 인증국 CAS $_1$)보다 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하여, 검증이 성립한 경우에는 하나 상류측의 인증국이 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하는 처리를 하나 상류측의 인증국이 트러스트 앵커가 될 때까지 계속한다. 그리고, 이러한 공개 키 증명서의 서명 검증이 트러스트 앵커까지 성립한 경우, 유효성 확인 대상의 공개 키 증명서의 유효성이 확인된 것으로 한다.

엔드 엔티티 EE $_x$ 는 엔드 엔티티 EE $_1$ 로부터 수취한 전자 문서의 서명을 해당 전자 문서에 첨부된 공개 키 증명서를 이용하여 검증함과 함께, 상기한 ①, ②에 나타내는 순서에 따라 해당 전자 문서의 서명 검증에 이용한 공개 키 증명서의 유효성을 확인함으로써, 해당 전자 문서의 정당성을 확인할 수 있다.

또, 이상에서는 공개 키 증명서의 유효성 확인 처리를 엔드 엔티티로 행하는 것을 전제로 하고 있다. 그러나, 공개 키 증명서의 유효성 확인 처리는 부하가 무겁고, 이를 엔드 엔티티로 행하기 위해서는 해당 엔드 엔티티에 높은 처리 능력이 요구된다. 그래서, 네트워크를 통해 엔드 엔티티에 접속된 증명서의 유효성 확인 서버를 설치하고, 해당 서버에 해당 엔드 엔티티 대신에 공개 키 증명서의 유효성 확인을 행하게 하는 것이 IETF에 의해 제안되어 있다.

발명이 이루고자 하는 기술적 과제

그런데, 종래 제안되어 있는 증명서의 유효성 확인 서버는 엔드 엔티티로부터 의뢰를 받는 때마다, 상기한 ①, ②에 나타내는 순서를 실행하여 공개 키 증명서의 유효성을 확인하고 있다. 이 때문에, 엔드 엔티티가 공개 키 증명서의 유효성 확인을 의뢰를 하고 나서 그 결과를 알 수 있기까지, 적어도 상기한 ①, ②에 나타내는 순서를 실행하기 위한 시간이 걸린다.

또, 도 12에서는 시큐리티 도메인이 하나인 것을 전제로 하고 있지만, 상술한 바와 같이 민간계, 공공계의 여러 조직, 단체에 있어서 PKI의 도입, 정비가 행해지고 있으며, 그 결과, 복수의 시큐리티 도메인이 배열되어 있음이 예상된다. 이들이 다른 시큐리티 도메인 사이에서도 각 시큐리티 도메인의 루트 인증국끼리, 상호 상대의 공개 키 증명서를 발행하는 등으로 하여 상호 인증을 행하거나, 각 시큐리티 도메인의 루트 인증국 각각 사이에서 이러한 상호 인증을 행한 브릿지 인증국을 설치함으로써, 상기한 ①, ②에 그 순서를 나타낸 공개 키 증명서의 유효성 확인 처리를 실현할 수 있다. 그러나, 이와 같이 복수의 시큐리티 도메인 사이에서 공개 키 증명서의 유효성 확인 처리를 행하면, 인증국 수가 증대하고, 또한 각 인증국의 관계도 도 12에 도시한 바와 같은 단순한 트리 구조가 아닌, 보다 복잡화하기 때문에, 상기한 ①, ②에 나타내는 순서를 실행하기 위한 부하가 증대한다. 이 때문에, 엔드 엔티티가 공개 키 증명서의 유효성 확인을 의뢰를 하고 나서 그 결과를 알 수 있기까지 걸리는 시간이 더욱 길어져, 서비스 저하를 초래한다.

본 발명은 상기 사정에 감안하여 이루어진 것으로, 본 발명의 목적은 공개 키 증명서의 유효성 확인을 의뢰하고 나서, 해당 유효성이 확인될 때까지 걸리는 시간을 짧게 하는 데 있다.
상기 과제를 해결하기 위해서, 본 발명에서는 네트워크를 통해 복수의 단말기(엔드 엔티티)나 인증국에 접속된 증명서의 유효성 확인 서버에 있어서, 어떤 단말기로부터의 의뢰에 따라 해당 단말기가 신뢰하는 인증국과는 다른 인증국이 발행한 공개 키 증명서의 유효성을 확인하기 위해 다음 처리를 행한다.
즉, 임의의 인증국을 기점 인증국으로 하여, 해당 기점 인증국이 발행한 공개 키 증명서의 피발행처를 조사하고, 해당 발행처에 인증국이 포함되는 경우에는 해당 인증국이 발행한 공개 키 증명서의 피발행처를 더 조사하는 처리를 해당 공개 키 증명서의 피발행처가 전부 단말기가 될 때까지 계속함으로써, 상기 기점 인증국에서 임의의 단말기에 대하여 공개 키 증명서를 발행한 단말기 수용 인증국까지의 패스를 검색하는 패스 검색 단계와,
상기 패스 검색 단계에 의해 검출된 패스에 대하여 상기 기점 인증국을 상류로 하고, 해당 패스 상의 단말기 수용 인증국이 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하여, 검증이 성립한 경우에는 하나 상류측의 인증국이 발행한 공개 키 증명서의 서명을 더 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하는 처리를 하나 상류측의 인증국이 상기 기점 인증국이 될 때까지 계속함으로써, 해당 패스를 검증하는 패스 검증 단계와,
상기 패스 검증 단계에 의해 검증이 성립한 패스를 데이터 베이스에 등록하는 패스 등록 단계를 단말기에서의 공개 키 증명서의 유효성 확인 의뢰와는 무관하게, 예를 들면 정기적으로 행한다.
그리고, 어떤 단말기로부터, 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있는 경우에, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있는지의 여부를 조사함으로써, 상기 공개 키 증명서의 유효성을 확인한다.
본 발명에 따르면, 어떤 단말기로부터 공개 키 증명서의 유효성 확인 의뢰를 받은 경우, 그리고 나서 상기한 ①, ②에 나타낸 해당 단말기의 트러스트 앵커로부터 해당 공개 키 증명서의 발행처 인증국까지의 패스의 검색 및 검출한 패스의 검증을 행할 필요가 없다. 따라서, 공개 키 증명서의 유효성 확인을 의뢰하고 나서, 해당 유효성이 확인될 때까지 걸리는 시간을 단축할 수 있다.

발명의 구성 및 작용

이하, 본 발명의 일 실시예에 대하여 설명한다.
도 1은 본 발명의 일 실시예가 적용된 PKI 시스템의 개략 구성도이다.
도시한 바와 같이 본 실시예의 PKI 시스템은 전자 수속을 행하는 사용자 단말기 또는 사용자 단말기로부터의 의뢰를 받아 전자 수속을 대행하는 접수 서버인 복수의 엔드 엔티티 EE와, 공개 키 증명서의 발행과 그 관리를 행하는 복수의 인증국 CA와, 엔드 엔티티 EE로부터의 의뢰에 따라 공개 키 증명서의 유효성 확인을 행하는 증명서 유효성 확인 센터 VC가 LAN, WAN 및 이들을 연결하는 인터넷 등에 의해 구성된 네트워크 NET를 통해 상호 접속되어 구성된다.
도 2는 도 1에 도시한 PKI 시스템에서의 각 인증국 CA의 관계의 일례를 나타내는 도면이다.
도시한 바와 같이 본 실시예의 PKI 시스템에서는 민간계, 정부계 등의 복수 의 시큐리티 도메인 SD(SD_1 SD_3)가 배열되어 있는 것을 전제로 하고 있다. 그리고, 그 중 몇 개인가의 시큐리티 도메인 SD(도 2에서는 SD_2, SD_3)는 루트 인증국 CA (도 2에서는 CA_{21}, CA_{31})끼리, 예를 들면 상호 공개 키 증명서를 발행함으로써, 상호 인증을 행하고 있는 것으로 한다. 또한, 각 시큐리티 도메인 SD의 루트 인증국 CA(도 2에서는 CA_{11}, CA_{21}, CA_{31})은 예를 들면, 브릿지 인증국 CA_{bridge}에 대하여 공개 키 증명서를 발행함과 함께, 브릿지 인증국 CA_{bridge}로부터 공개 키 증명서를 발행하여 받음으로써, 브릿지 인증국 CA_{bridge} 사이에서 상호 인증을 행하고 있는 것으로 한다. 이와 같이 함으로써, 어떤 시큐리티 도메인 SD에 속하는 인증국 CA와 다른 시큐리티 도메인 SD에 속하는 인증국 CA 사이에, 한쪽의 인증국 CA가 발행한 공개 키 증명서의 유효성을 다른 쪽의 인증국 CA에서 확인할 수 있도록 하기 위한 패스가 형성된다.
다음으로, 상기한 PKI 시스템을 구성하는 엔드 엔티티 EE, 인증국 CA 및 증명서 유효성 확인 센터 VC에 대하여 설명한다.
우선, 엔드 엔티티 EE에 대하여 설명한다.
도 3은 엔드 엔티티 EE의 개략 구성도이다.
도시한 바와 같이 엔드 엔티티 EE는 처리부(10a)와, 기억부(10b)와, 네트워크 NET를 통해 다른 장치와 통신을 행하기 위한 통신부(16)와, 사용자가 작성한 전자 문서나 다른 엔드 엔티티 EE 또는 사용자 단말기로부터 수취한 전자 문서의 입출력이나 사용자로부터의 지시의 접수를 행하는 입출력부(17)를 구비한다.
처리부(10a)는 서명 생성부(14)와, 서명 검증부(15)와, 엔드 엔티티 EE의 각 부를 통괄적으로 제어하는 제어부(18)를 구비한다.
기억부(10b)는 사용자가 작성한(엔드 엔티티 EE가 접수 서버의 경우에는 사용자 단말기로부터 수취한) 전자 문서를 보유하는 전자 문서 보유부(11)와, 비밀 키(서명 키)와 이와 쌍인 공개 키 증명서를 보유하는 키 보유부(12)와, 다른 엔드 엔티티 EE로부터 수취한 서명이 첨부된 전자 문서와 공개 키 증명서를 보유하는 검증 대상 보유부(13)를 구비한다.
이러한 구성에 있어서, 제어부(18)는 입출력부(17)를 통해 사용자로부터 전자 문서 보유부(11)에 보유되어 있는 전자 문서를 다른 엔드 엔티티 EE로 송신해야 할 취지의 지시를 접수하면, 해당 전자 문서를 전자 문서 보유부(11)로부터 판독하고, 이를 서명 생성부(14)에 건네 준다. 이를 받아, 서명 생성부(14)는 키 보유부 (12)에 보유되어 있는 비밀 키

를 이용하여 해당 전자 문서에 대한 서명을 생성한다. 그리고 나서, 제어부(18)는 전자 문서 보유부(11)로부터 판독한 전자 문서에 서명 생성부(14)에서 생성된 서명을 넣어, 서명이 첨부된 전자 문서를 작성한다. 그리고, 작성한 서명이 첨부된 전자 문서에 키 보유부(12)에 보유되어 있는 공개 키 증명서를 첨부하여, 통신부(16)를 통해 사용자로부터 지시된 송신 목적지의 엔드 엔티티 EE의 어드레스로 송신한다.

또한, 제어부(18)는 통신부(16)를 통해 다른 엔드 엔티티 EE로부터 서명이 첨부된 전자 문서와 공개 키 증명서를 수취하면, 이들을 검증 대상 보유부(13)에 보유시킴과 함께, 그 취지를 서명 검증부(15)에 통지한다. 이를 받아, 서명 검증부 (15)는 검증 대상 보유부(13)에 보유되어 있는 서명이 첨부된 전자 문서의 서명을 해당 전자 문서와 함께 수취한 공개 키 증명서를 이용하여 검증한다. 그리고, 검증이 성립한 경우에만, 서명이 첨부된 전자 문서를 정당한 것으로서 취급하고, 필요에 따라 입출력부(17)로부터 출력한다.

단, 상기한 서명 검증이 성립한 경우라도 해당 서명 검증에 이용한 공개 키 증명서가 자(自) 엔드 엔티티 EE를 수용하는(즉, 자 엔드 엔티티 EE에 대하여 공개 키 증명서를 발행하였음) 단말기 수용 인증국 CA 이외의 단말기 수용 인증국 CA의 경우에는 증명서 유효성 확인 센터 VC로, 상기한 서명 검증에 이용한 공개 키 증명서의 유효성의 확인 의뢰를 송신한다. 이 때, 필요에 따라 인증국 CA의 인증 · 보증의 레벨을 나타내는 신뢰도(policy)를 상기 확인 의뢰에 포함시킨다. 그리고, 증명서 유효성 확인 센터 VC에서 해당 공개 키 증명서의 유효성이 확인된 경우에만, 서명이 첨부된 전자 문서를 정당한 것으로서 취급하고, 필요에 따라 입출력부(17)로부터 출력한다. 또, 여기서는 신뢰도를 상기 서명이 첨부된 전자 문서에 의해 행하고자 하는 전자 수속의 거래액 등으로 나타내고 있다. 단, 신뢰도는 예를 들면 취급하는 문서의 기밀도나 본인의 신뢰도(본인이 출두할 필요있다 라든가 네트워크 경유로 괜찮다는 등)를 이용하여 나타낼 수도 있다.

다음으로, 인증국 CA에 대하여 설명한다.

도 4는 인증국 CA의 개략 구성도이다.

도시한 바와 같이 인증국 CA는 처리부(20a)와, 기억부(20b)와, 네트워크 NET 를 통해 다른 장치와 통신을 행하기 위한 통신부(26)와, 공개 키 증명서 등의 입출력이나 사용자에서의 지시의 접수를 행하는 입출력부(27)를 갖는다.

처리부(20a)는 공개 키 증명서를 발행하는 발행부(21)와, 발행부(21)가 발행한 공개 키 증명서의 관리를 행하는 관리부(22)와, 인증국 CA의 각 부를 통괄적으로 제어하는 제어부(28)를 갖는다.

기억부(20b)는 발행부(21)가 발행한 공개 키 증명서를 보유하는 공개 키 증명서 데이터 베이스(23)와, 공개 키 증명서 데이터 베이스(23)에 보유되어 있는 각 공개 키 증명서의 피발행처가 기술된 발행처 관리 리스트를 보유하는 피발행처 관리 리스트 보유부(24)와, 실효(失效) 증명서 리스트 보유부(25)를 갖는다.

이러한 구성에 있어서, 제어부(28)는 입출력부(27) 또는 통신부(26)를 통해 공개 키 증명서의 발행 의뢰를 접수하면, 그 취지를 발행부(21)로 전한다. 이를 받아, 발행부(21)는 발행 의뢰주가 서명 생성에 이용하는 비밀 키(서명 키)와 이와 쌍인 공개 키 증명서를 작성한다. 이 때, 자인증국 CA의 비밀 키로 공개 키 증명서에 서명한다. 또한, 필요에 따라 공개 키 증명서 중에, 해당 공개 키 증명서의 유효 기한이나, 신뢰하지 않은 다른 인증국의 명칭(Name Constrains)이나, 해당 공개 키 증명서의 유효성 확인을 위해 허용되는 최대 패스 길이(패스 상의 허용 최대 인증국 수)나, 전자 수속의 거래액 등으로 나타낸 해당 공개 키 증명서와 쌍인 비밀 키에 의한 서명의 신뢰도(폴리시)를 기술한다. 그리고, 작성한 공개 키 증명서와 비밀 키를 입출력부(27) 또는 통신부(26)를 통해 우송, 또는 통신에 의해 발행 의뢰주에게 건네 준다. 또한, 이 공개 키 증명서를 공개 키 증명서 데이터 베이스 (23)에 등록함과 함께, 그 피발행처(즉 발행 의뢰주)의 정보를 피발행처 관리 리스트 보유부(24)에 보유되어 있는 피발행처 관리 리스트에 기술한다.

또한, 제어부(28)는 입출력부(27) 또는 통신부(26)를 통해 공개 키 증명서의 실효 의뢰를 접수하면, 그 취지를 관리부(22)로 전한다. 이를 받아, 관리부(22)는 실효 대상의 공개 키 증명서를 공개 키 증명서 데이터 베이스(23)로부터 삭제함과 함께, 해당 공개 키 증명서의 피발행처의 정보를 발행처 관리 리스트 보유부(24)에 보유되어 있는 피발행처 관리 리스트로부터 삭제한다. 단, 실효 대상의 공개 키 증명서를 공개 키 증명서 데이터 베이스(23)로부터 삭제하는 처리는 필수가 아니다. 그리고, 관리부(22)는 실효 대상인 공개 키 증명서에 관한 정보가 기술된 실효 증명서 리스트(일반적으로, CRL (Certification Revocation List), ARL(Authority Revocation List)라 불리고 있음)를 정기적으로 작성하여, 이를 실효 증명서 리스트 보유부(25)에 보유시킨다. 또, 관리부(22)는 작성한 실효 증명서 리스트에 다음 회의 실효 증명서 리스트의 작성 예정 일시를 기술하는 것으로 한다.

또한, 제어부(28)는 통신부(26)를 통해 다른 장치보다 공개 키 증명서의 실효 정보의 문의를 수취하면, 실효 증명서 리스트 보유부(25)에 보유되어 있는 실효 증명서 리스트를 검색하고, 문의가 있었던 공개 키 증명서가 실효한지의 여부를 조사한다. 그리고, 그 결과를 통신부(26)를 통해 문의를 한 다른 장치에 응답한다[이러한 문의와 응답에 이용하는 통신 프로토콜로서, OSCP(Online Certification status protocol)가 있음].

또, 관리부(22)는 공개 키 증명서 데이터 베이스(23)에 저장되어 있는 각 공개 키 증명서의 유효 기한을 조사하여, 유효 기한이 경과한 공개 키 증명서를 공개 키 증명서 데이터 베이스(23)로부터 삭제함과 함께, 해당 공개 키 증명서의 피발행처의 정보를 피발행처 관리 리스트 보유부(24)에 보유되어 있는 피발행처 관리 리스트로부터 삭제하는 처리도 행한다.

다음으로, 증명서 유효성 확인 센터 VC에 대하여 설명한다.

도 5는 증명서 유효성 확인 센터 VC의 개략 구성도이다.

도시한 바와 같이 증명서 유효성 확인 센터 VC는 처리부(30a)와, 기억부 (30b)와, 네트워크 NET를 통해 다른 장치와 통신을 행하기 위한 통신부(36)와, 공개 키 증명서 등의 입출력이나 사용자로부터의 지시의 접수를 행하는 입출력부(37)를 갖는다.

처리부(30a)는 패스 검색부(32)와, 패스 검증부(33)와, 유효 기한/실효 상태 조사부(34)와, 유효성 확인부(35)와, 증명서 유효성 확인 센터 VC의 각 부를 통괄적으로 제어하는 제어부(38)를 갖는다. 또한, 기억부(30b)는 패스 데이터

베이스 (31)와, 실효 증명서 리스트 작성 예정 일시 데이터 베이스(39)를 갖는다.
패스 검색부(31)는 정기적으로 브릿지 인증국 CA $_{bridge}$ 로부터 엔드 엔티티 EE에 대하여 공개 키 증명서를 발행한 각 단말기 수용 인증국 CA까지의 패스를 검색한다.
패스 검증부(32)는 패스 검색부(31)에서 패스 검색이 행해질 때마다, 패스 검색부(31)에서 검출된 패스 검증을 행한다. 그리고, 검증이 성립한 패스를 브릿지 인증국 CA $_{bridge}$ 를 상류로 한 경우에 해당 패스 상의 최하류에 위치하게 되는 단말기 수용 인증국 CA의 명칭과, 해당 패스 상의 각 인증국 CA로부터 입수한 해당 패스 상의 입수처 인증국 CA보다 하나 하류측에 위치하는 인증국 CA(발행처의 인증국 CA가 단말기 수용 인증국 CA의 경우에는 엔드 엔티티 EE)에 대하여 발행한 공개 키 증명서에 대응하여 패스 데이터 베이스(31)에 등록한다.
유효 기한/실효 상태 조사부(34)는 패스 데이터 베이스(31)에 등록되어 있는 패스 각각에 대하여 해당 패스 상의 각 인증국 CA가 해당 패스 상의 하나 하류측에 위치하는 인증국 CA(발행처의 인증국 CA가 단말기 수용 인증국 CA인 경우에는 엔드 엔티티 EE)에 대하여 발행한 공개 키 증명서의 유효 기한이나 실효 유무를 조사한다. 그리고, 그 결과에 따라 패스 데이터 베이스(31)를 갱신한다.
또한, 유효 기한/실효 상태 조사부(34)는 각 인증국 CA의 실효 증명서 리스트 보유부(25)로부터 입수한 실효 증명서 리스트에 기술되어 있는 다음 실효 증명서 리스트 작성 예정 일시를 해당 인증국 CA에 대응하여 실효 증명서 리스트 작성 예정 일시 데이터 베이스(39)에 등록한다.
유효성 확인부(35)는 엔드 엔티티 EE로부터의 의뢰에 따라 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA 이외의 단말기 수용 인증국 CA가 발행한 공개 키 증명서의 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA에 대한 유효성 확인을 행한다.
또, 도 3 도 5에 도시한 엔드 엔티티 EE, 인증국 CA 및 증명서 유효성 확인 센터 VC의 각각은 예를 들면, 도 6에 도시한 바와 같은 CPU(61)와, 메모리(62)와, 하드디스크 등의 외부 기억 장치(63)와, CD-ROM 등의 가반성(可搬性)을 갖는 기억 매체(69)로부터 정보를 판독하는 판독 장치(64)와, 네트워크를 통해 다른 장치와 통신을 행하기 위한 통신 장치(65)와, 키보드나 마우스 등의 입력 장치(66)와, 모니터나 프린터 등의 출력 장치(67)와, 이들 각 장치 사이의 데이터 송수신을 행하는 인터페이스(68)를 구비한 일반적인 컴퓨터에 있어서, CPU(61)가 메모리(62) 상에 로드된 소정의 프로그램을 실행함으로써 실현할 수 있다. 즉, 통신부(16, 26, 36)는 CPU(61)가 통신 장치(66)를 이용함으로써, 입출력부(17, 27, 37)는 CPU(61)가 입력 장치(66)나 출력 장치(67)나 판독 장치(64)를 이용함으로써, 그리고 기억부(10b, 20b, 30b)는 CPU(61)가 메모리(62)나 외부 기억 장치(63)를 이용함으로써 실현된다. 또한, 처리부(10a, 20a, 30a)는 CPU(61) 상의 프로세스로서 실현된다.
이러한 컴퓨터 상에 엔드 엔티티 EE, 인증국 CA 및 증명서 유효성 확인 센터 VC를 각각 실현하기 위한 소정의 프로그램은 판독 장치(64)를 통해 기억 매체 (69)로부터 판독되거나, 통신 장치(66)를 통해 네트워크 경유로 다른 서버로부터 다운로드되고, 일단 외부 기억 장치(63)에 저장된 후, 거기에서 메모리(62) 상에 로드되거나 외부 기억 장치(63)에 저장되지 않고 직접 메모리(62) 상에 로드되어 CPU(61)에 실행되도록 하면 좋다.
다음으로, 상기 구성의 증명서 유효성 확인 센터 VC의 동작에 대하여 설명한다.
본 실시예의 증명서 유효성 확인 센터 VC의 동작은 패스 검색, 검증 및 관리 동작과, 공개 키 증명서의 유효성의 확인 동작과 분리된다.
우선, 패스의 검색 · 검증 및 관리 동작에 대하여 설명한다.
도 7 도 8은 본 실시예의 증명서 유효성 확인 센터 VC에서 행해지는 패스의 검색, 검증 및 관리 동작을 설명하기 위한 순서도이다.
제어부(38)는 소정 시간(예를 들면 1일)을 경과하면(단계 S1001), 패스 검색부(32)에 패스 검색을 의뢰한다. 이를 받아, 패스 검색부(32)는 브릿지 인증국 CA $_{bridge}$ 으로부터 각 단말기 수용 인증국 CA까지의 패스를 검색한다(단계 S1002).
구체적으로는 패스 검색부(32)는 브릿지 인증국 CA $_{bridge}$ 의 피발행처 관리 리스트 보유부(24)를 액세스하고, 브릿지 인증국 CA $_{bridge}$ 가 발행한 공개 키 증명서의 피발행처 정보를 입수한다. 그리고, 입수한 각 피발행처가 인증국 CA의 경우에는 각 피발행처의 인증국 CA의 피발행처 관리 리스트 보유부(24)를 액세스하고, 각 인증국 CA가 발행한 공개 키 증명서의 피발행처를 더 조사한다. 이 처리를 공개 키 증명서의 피발행처가 엔드 엔티티 EE가 될 때까지 계속함으로써, 브릿지 인증국 CA $_{bridge}$ 으로부터 단말기 수용 인증국 CA까지의 패스를 검색한다. 여기서, 패스의 루프에 의해 상기한 처리가 무한히 반복되는 것을 방지하기 위해서, 어떤 인증국 CA의 피발행처 관리 리스트 보유부(24)로부터 입수한 피발행처에, 지금까지 형성된 부분 패스의 상류측에 위치하는 인증국 CA가 포함되는 경우에는 해당 인증국 CA를 피발행처로 한 상기한 처리를 행하지 않는 것으로 한다.
단계 S1002에서의 패스 검색 처리를 각 인증국 CA가 도 2에 도시한 관계에 있는 경우를 예로 들어, 보다 구체적으로 설명한다.
우선, 패스 검색부(32)는 브릿지 인증국 CA $_{bridge}$ 의 피발행처 관리 리스트 보유부(24)를 액세스하고, 브릿지 인증국 CA $_{bridge}$ 가 발행한 공개 키 증명서의 피발행처 정보로서, 인증국 CA $_{11}$, CA $_{21}$, CA $_{31}$ 의 정보를 입수한다.
다음으로, 패스 검색부(32)는 브릿지 인증국 CA $_{bridge}$ 로부터 입수한 피발행처(인증국 CA $_{11}$, CA $_{21}$, CA $_{31}$) 중 어느 하나에 주목하여 다음 처리를 실행한다.
즉, 주목한 피발행처가 인증국 CA(이하, 주목 인증국 CA라 부르기로 함)이면, 브릿지 인증국 CA $_{bridge}$ -주목 인증국 CA 사이에 브릿지 인증국 CA $_{bridge}$ 측을 상류로 하는 부분 패스를 설정한다. 그리고, 주목 인증국 CA의 피발행처 관리 리스트 보유부(24)를 액세스하고, 해당 주목 인증국 CA가 발행한 공개 키 증명서의 피발행처의 정보를 더 입수한다. 여기서는 주목한 피발행처가 인증국 CA $_{11}$ 이라고 하여, 브릿지 인증국 CA $_{bridge}$ -인증국 CA $_{11}$ 사이에 부분 패스를 설정하고, 인증국 CA $_{11}$ 로부터 피발행처 정보로서 인증국 CA $_{bridge}$, CA $_{12}$, CA $_{13}$ 의 정보를 입수한 것

으로 한다.

다음으로, 패스 검색부(32)는 인증국 CA_{11}로부터 입수한 피발행처(인증국 CA_{bridge}, CA_{12}, CA_{13})에 부분 패스 상의 인증국 CA(이하, 루트 인증국 CA라 부르기로 함)가 포함되어 있는지의 여부를 조사한다. 포함되어 있는 경우에는 그 피발행처를 주목 대상에서 제외한다. 따라서, 여기서는 인증국 CA_{bridge}를 주목 대상에서 제외하게 된다. 다음으로, 패스 검색부(32)는 인증국 CA_{11}로부터 입수한 피발행처에 엔드 엔티티 EE가 포함되는지의 여부를 조사한다. 엔드엔테이티 EE가 포함되어 있는 경우, 인증국 CA_{11}은 단말기 수용 인증국이 된다. 그러나, 인증국 CA_{11}로부터 입수한 피발행처에 엔드 엔티티 EE는 포함되어 있지 않다. 따라서, 브릿지 인증국 CA_{bridge}-인증국 CA_{11} 사이에 설정한 부분 패스를 단말기 수용 인증국 CA까지 연장하기 위해, 인증국 CA_{11}로부터 입수한 루트 인증국 CA를 제외한 피발행처(인증국 CA_{12}, CA_{13}) 중 어느 하나에 주목한다.

주목한 피발행처가 인증국 CA이면, 지금까지 설정한 부분 패스의 하류측에 이 주목 인증국 CA를 접속한 부분 패스를 설정한다. 그리고, 이 주목 인증국 CA의 피발행처 관리 리스트 보유부(24)를 액세스하고, 해당 주목 인증국 CA가 발행한 공개 키 증명서의 피발행처 정보를 더 입수한다. 여기서는 주목한 피발행처가 인증국 CA_{12}라고 하여, 브릿지 인증국 CA_{bridge}-인증국 CA_{11}-인증국 CA_{12} 사이에 부분 패스를 설정하고, 인증국 CA_{12}로부터 피발행처 정보로서 엔드 엔티티 EE_1, EE_2를 입수한 것으로 한다.

다음으로, 패스 검색부(32)는 인증국 CA_{12}로부터 입수한 피발행처(EE_1, EE_2)에 루트 인증국 CA가 포함되어 있는지의 여부를 조사한다. 포함되어 있는 경우에는 그 피발행처를 주목 대상에서 제외한다. 여기서는 루트 인증국 CA는 포함되어 있지 않기 때문에, 패스 검색부(32)는 다음 처리로 이행하고, 단말기 수용 인증국 CA_{12}로부터 입수한 피발행처에 엔드 엔티티 EE가 포함되는지의 여부를 조사한다. 여기서, 입수한 피발행처는 전부 엔드 엔티티 EE이기 때문에, 인증국 CA_{12}는 단말기 수용 인증국이다. 그래서, 이 인증국 CA_{12}를 최하류로 하는 부분 패스를 브릿지 인증국 CA_{bridge}로부터 단말기 수용 인증국 CA_{12}까지의 패스(CA_{bridge}-CA_{11}-CA_{12})로서 검출한다.

다음으로, 패스 검색부(32)는 검출한 패스 상의 최하류측에 위치하는 인증국 CA_{12}로부터 입수한 피발행처 정보 중에, 아직 주목하지 않은 피발행처(루트 인증국 CA 이외의 인증국 CA)가 있는지의 여부를 조사하고, 그와 같은 발행처가 있으면, 이를 주목 인증국 CA로 하여 상기한 처리를 계속한다. 한편, 그와 같은 피발행처가 없으면, 하나 상류측에 위치하는 인증국 CA_{11}로부터 입수한 발행처 정보 중에, 아직 주목하지 않은 피발행처(루트 인증국 CA 이외의 인증국 CA)가 있는지의 여부를 조사한다. 그리고, 그와 같은 피발행처가 있으면, 이를 주목 인증국 CA로 하여 상기한 처리를 계속한다. 여기서는 인증국 CA_{11}로부터 입수한 피발행처 정보 중에서는, 인증국 CA_{13}에 대하여 아직 주목하지 않기 때문에, 이를 주목 인증국 CA로 하여 상기한 처리를 행함으로써, 브릿지 인증국 CA_{bridge}로부터 단말기 수용 인증국 CA_{13}까지의 패스(CA_{bridge}-CA_{11}-CA_{13})를 검출한다.

이와 같이, 패스 검색부(32)는 상기한 처리를 검출한 패스 상에 위치하는 모든 인증국 CA 각각에 대하여 해당 인증국 CA로부터 입수한 피발행처 정보 중에, 아직 주목하지 않은 피발행처(루트 인증국 CA 이외의 인증국 CA)가 없어질 때까지 계속함으로써, 브릿지 인증국 CA_{bridge}로부터 각 단말기 수용 인증국 CA까지의 패스를 검출한다. 그 결과, 각 인증국 CA가 도 2에 도시한 관계에 있는 경우, 패스 검색부 (32)에 의해 검출되는 브릿지 인증국 CA_{bridge}로부터 각 단말기 수용 인증국 CA까지의 패스는 도 9에 도시한 바와 같다.

그런데, 제어부(38)는 패스 검색부(32)에 의해 브릿지 인증국 CA_{bridge}로부터 각 단말기 수용 인증국 CA까지의 패스가 검출되면, 패스 검증부(33)에 패스 검증을 의뢰한다. 이를 받아, 패스 검증부(33)는 패스 검색부(32)에 의해 검출된 패스의 검증을 행한다(단계 S1003).

구체적으로는 패스 검색부(32)에 의해 검출된 패스 각각에 대하여 다음 처리를 행한다.

즉, 우선, 패스 검증부(33)는 패스 상의 각 인증국 CA의 공개 키 증명서 데이터 베이스(23)를 액세스하고, 각 인증국 CA가 해당 패스 상의 하나 하류측에 위치하는 인증국 CA(액세스처 인증국 CA가 단말기 인증국 CA의 경우에는 엔드 엔티티 EE)에 대하여 발행한 공개 키 증명서를 입수한다.

다음으로, 패스 검증부(33)는 패스의 최하류에 위치하는 단말기 수용 인증국 CA가 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국 CA가 발행한 공개 키 증명서로 검증하고, 검증이 성립한 경우에는 하나 상류측의 인증국 CA가 발행한 공개 키 증명서의 서명을 더 하나 상류측의 인증국 CA가 발행한 공개 키 증명서로 검증한다. 이 처리를 하나 상류측의 인증국 CA가 브릿지 인증국 CA_{bridge}가 될 때까지 계속함으로써, 해당 패스를 가검증한다.

예를 들면, 도 2에 있어서 브릿지 인증국 CA_{bridge}으로부터 단말기 수용 인증국 CA_{13}까지의 패스(CA_{bridge}-CA_{11}-CA_{13})를 가검증하는 경우, 우선 단말기 수용 인증국 CA_{13}이 발행한 공개 키 증명서의 서명을 단말기 수용 인증국 CA_{13}보다 하나 상류측의 인증국 CA인 루트 인증국 CA_{11}이 단말기 수용 인증국 CA_{13}에 대하여 발행한 공개 키 증명서를 이용하여 검증한다. 그리고, 검증이 성립한 경우에는 루트 인증국 CA_{11}이 발행한 공개 키 증명서의 서명을 루트 인증국 CA_{11}보다 하나 상류측의 인증국 CA 인 브릿지 인증국 CA_{bridge}가 루트 인증국 CA_{11}에 대하여 발행한 공개 키 증명서를 이용하여 검증한다. 그리고, 이 검증이 성립한 경우에, 브릿지 인증국 CA_{bridge}에서 단말기 수용 인증국 CA_{13}까지의 패스의 가검증이 성립한 것으로 한다.

다음으로, 패스 검증부(33)는 패스의 가검증이 성립하였으면, 해당 패스 상의 각 인증국 CA로부터 입수한 공개 키 증명서 중, 신뢰하지 않은 다른 인증국의 명칭이나 해당 공개 키 증명서의 유효성 확인을 위해 허용되는 최대 패스 길이(패스 상의 허용 최대 인증국 수) 등의 제한의 기술이 있는지의 여부를 조사한다. 그와 같은 기술이 있는 경우에는 해당 패스가 그 제한을 만족하고 있는지의 여부를 조사하여, 만족하고 있는 경우에만, 해당 패스의 검증이 성립한 것으로 한다.

예를 들면, 도 2에 있어서 브릿지 인증국 CA_{bridge}로부터 단말기 수용 인증국 CA_{26}까지의 패스(CA_{bridge}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26})의 가검증이 성립한 경우에 있어서, 인증국 CA_{26}으로부터 입수한 공개 키 증명서 중에 신뢰하지 않은 다른 인증국의 명칭으로서 인증국 CA_{31}이 기술되어 있는 경우, 해당 패스의 검증은 성립

하지 않은 것으로 한다. 또한, 상기한 경우에 있어서, 인증국 CA_{26}으로부터 입수한 공개 키 증명서 중에 패스 길이로서 인증국 수=5가 기술되어 있는 경우, 해당 패스의 검증은 성립하지 않은 것으로 한다.
그런데, 제어부(38)는 상기한 바와 같이 하여, 패스 검색부(32)에 의해 검출된 패스 각각에 대한 패스 검증부(33)에서의 검증이 종료하였으면, 패스 데이터 베이스(31)의 등록 내용을 일단 클리어하고, 그 다음에 패스 검증부(33)에서의 검증이 성립한 패스 각각을 해당 패스 상의 최하류에 위치하는 단말기 수용 인증국 CA와, 해당 패스 상의 각 인증국 CA로부터 입수한 공개 키 증명서에 대응하여 패스 데이터 베이스(31)에 등록한다(단계 S1004).
한편, 유효 기한/실효 상태 조사부(34)는 패스 데이터 베이스(31)에 등록되어 있는 공개 키 증명서 중, 유효 기한 마감의 공개 키 증명서가 있는지의 여부를 조사한다(단계 S1005). 유효 기한 마감의 공개 키 증명서가 있는 경우에는 해당 공개 키 증명서의 발행처 인증국 CA의 공개 키 증명서 데이터 베이스(23)를 액세스하고, 해당 공개 키 증명서의 피발행처에 대하여 새롭게 발행된 공개 키 증명서를 검색한다(단계 S1006).
그리고, 그와 같은 공개 키 증명서가 상기 발행처 인증국 CA의 공개 키 증명서 데이터 베이스(23) 중에 없으면, 상기 유효 기한 마감의 공개 키 증명서에 대응하여 등록되어 있는 패스에 관한 정보를 패스 데이터 베이스(31)로부터 삭제한다(단계 S1007). 한편, 그와 같은 공개 키 증명서가 상기 발행처 인증국 CA의 공개 키 증명서 데이터 베이스(23) 중에 있으면 이를 입수한다. 그리고, 상기 유효 기한 마감의 공개 키 증명서에 대응하여 패스 데이터 베이스(31)에 등록되어 있는 패스 검증을 해당 유효 기한 마감의 공개 키 증명서 대신에 새롭게 입수한 공개 키 증명서를 이용하여, 상기한 단계 S1003과 동일한 요령으로 행한다(단계 S1008).
또, 단계 S1008에서의 패스 검증 대신에, 새롭게 입수한 공개 키 증명서의 서명을 해당 패스 상에 있어서 해당 공개 키 증명서의 발행처 인증국 CA보다 하나 상류측에 위치하는 인증국 CA가 발행한 공개 키 증명서로 검증하여, 검증이 성립한 경우, 해당 패스의 검증이 성립한 것으로서 취급하도록 하여도 좋다.
그런데, 패스의 검증이 성립한 경우(단계 S1009에서 Yes)는 해당 패스에 대응되어 패스 데이터 베이스(31)에 등록되어 있는 상기 유효 기한 마감의 공개 키 증명서를 새롭게 입수한 공개 키 증명서로 치환한다(단계 S1010). 한편, 패스의 검증이 성립하지 않았던 경우(단계 S1009에서 No)는 상기 유효 기한 마감의 공개 키 증명서에 대응하여 등록되어 있는 패스를 패스 데이터 베이스(31)에서 삭제한다 (단계 S1011).
다음으로, 유효 기한/실효 상태 조사부(34)는 실효 증명서 리스트 작성 예정 일시 데이터 베이스(39)를 조사하고, 이미 경과한 실효 증명서 리스트 작성 예정 일시에 대응되어 있는 인증국 CA를 검색한다(단계 S1012). 그와 같은 인증국 CA가 존재하는 경우(단계 S1013에서 Yes)는 해당 인증국 CA의 실효 증명서 리스트 보유부(25)를 액세스하고, 해당 인증국 CA가 발행한 최신의 실효 증명서 리스트를 입수한다(단계 S1014). 그리고, 실효 증명서 리스트 작성 예정 일시 데이터 베이스 (39)로, 해당 인증국 CA에 대응하여 등록되어 있는 실효 증명서 리스트 작성 예정 일시를 입수한 최신의 실효 증명서 리스트에 기술되어 있는 실효 증명서 리스트 작성 예정 일시로 갱신한다(단계 S1015).
그리고, 유효 기한/실효 상태 조사부(34)는 입수한 최신의 실효 증명서 리스트에 기술되어 있는 공개 키 증명서가 패스 데이터 베이스(31)에 등록되어 있는지의 여부를 조사하고(단계 S1016), 등록되어 있는 경우에는 해당 공개 키 증명서에 대응되어 있는 패스에 관한 정보를 패스 데이터 베이스(31)로부터 삭제한다(단계 S1017).
다음으로, 공개 키 증명서의 유효성 확인 동작에 대하여 설명한다.
도 10 도 11은 본 실시예의 증명서 유효성 확인 센터 VC에서 행해지는 공개 키 증명서의 유효성의 확인 동작을 설명하기 위한 순서도이다.
제어부(38)는 통신부(36)를 통해 엔드 엔티티 EE로부터 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA의 명칭을 포함한, 해당 단말기 수용 인증국 CA 이외의 단말기 수용 인증국 CA가 발행한 공개 키 증명서의 유효성 확인 의뢰를 수취하면(단계 S2001), 그 취지를 유효성 확인부(35)에 통지한다. 또, 공개 키 증명서의 유효성 확인 의뢰에 인증국 CA의 명칭이 포함되어 있지 않은 경우에는 증명서 유효성 확인 센터 VC에서 사전에 설정되어 있는 디폴트의 인증국 CA를 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA에 설정한다. 그리고, 유효성 확인 대상의 공개 키 증명서를 발행한 단말기 수용 인증국 CA가 상기 설정한 단말기 수용 인증국 CA 이외이면 그 취지를 유효성 확인부(35)에 통지한다.
이를 받아, 유효성 확인부(35)는 의뢰 대상의 공개 키 증명서의 기술로부터 특정되는 해당 증명서를 발행한 단말기 수용 인증국 CA에 대응된 패스와, 의뢰주의 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA에 대응된 패스가 패스 데이터 베이스(31)에 등록되어 있는지의 여부를 조사한다(단계 S2002).
그 결과, 의뢰 대상의 공개 키 증명서를 발행한 단말기 수용 인증국 CA에 대응된 패스 및 의뢰주의 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA에 대응된 패스의 양방이 패스 데이터 베이스(31)에 등록되어 있지 않은 것이 판명되었으면, 유효성 확인부(35)는 공개 키 증명서가 유효가 아님을 통신부(36)를 통해 의뢰주의 엔드 엔티티 EE에 통지한다(단계 S2003).
한편, 의뢰 대상의 공개 키 증명서를 발행한 단말기 수용 인증국 CA에 대응된 패스 및 의뢰주의 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA에 대응된 패스의 양방이 패스 데이터 베이스(31)에 등록되어 있는 것이 확인할 수 있었으면, 유효성 확인부(35)는 이들 두 개의 패스 중 어느 하나에 대응되어 패스 데이터 베이스(31)에 등록되어 있는 각 공개 키 증명서 중에, 신뢰하지 않은 다른 인증국의 명칭이나 해당 공개 키 증명서의 유효성 확인을 위해 허용되는 최대 패스 길이(패스 상의 허용 최대 인증국 수) 등의 제한 기술이 있는지의 여부를 더 조사한다(단계 S2004).
그와 같은 제한 기술이 없는 경우, 단계 S2006으로 이행한다. 한편, 그와 같은 제한 기술이 있는 경우에는 단계 S2005로 이행하고, 이들 두 개의 패스가 그 제한을 만족하고 있는지의 여부, 즉 각 공개 키 증명서 중, 이들 두 개의 패스 상의 어느 하나의 인증국을 신뢰하지 않은 취지가 기술되어 있는지의 여부 및 최대 패스 길이로서, 이들 두 개의 패스 상의 인증국 수보다 적은 인증국 수가 기술되어 있는지의 여부를 조사한다.

그리고, 그와 같은 기술이 있는 경우, 유효성 확인부(35)는 이들 두 개의 패스가 그 제한을 만족하고 있지 않은 것으로 판단하여, 공개 키 증명서가 유효성이 아님을 통신부(36)를 통해 의뢰주의 엔드 엔티티 EE에 통지한다(단계 S2003). 한편, 그와 같은 기술이 없는 경우에는 이들 두 개의 패스가 그 제한을 만족하고 있는 것으로 판단하여 단계 S2006으로 이행한다.

단계 S2006에서는 유효성 확인부(35)는 엔드 엔티티 EE로부터 수취한 확인 의뢰에, 해당 엔드 엔티티 EE가 행하고자 하는 전자 수속의 거래액 등으로 나타난 신뢰도(폴리시)가 포함되어 있는지의 여부를 조사한다. 전자 수속의 신뢰도가 포함되어 있는 경우에는 이들 두 개의 패스 중 어느 하나에 대응되어 패스 데이터 베이스 (31)에 등록되어 있는 각 공개 키 증명서 중, 상기 전자 수속의 신뢰도를 만족하지 않은 신뢰도의 기술이 있는지의 여부를 더 조사한다(단계 S2007).

그리고, 그와 같은 기술이 있는 경우에는 이들 두 개의 패스를 의뢰주의 엔드 엔티티 EE가 행하고자 하고 있는 전자 수속을 위한 공개 키 증명서의 유효성 확인에 이용할 수 없는 것으로 판단하여, 공개 키 증명서가 유효가 아님을 통신부 (36)를 통해 의뢰주의 엔드 엔티티 EE에 통지한다(단계 S2003).

한편, 엔드 엔티티 EE로부터 수취한 확인 의뢰에 해당 엔드 엔티티 EE가 행하고자 하는 전자 수속의 신뢰도가 포함되어 있지 않은 경우, 또는 포함되어 있더라도 이들 두 개의 패스 중 어느 하나에 대응되어 패스 데이터 베이스(31)에 등록되어 있는 각 공개 키 증명서 중에 기술되어 있는 신뢰도가 상기 전자 수속의 신뢰도보다 높은 경우에는 공개 키 증명서는 유효하다고 판단하여, 공개 키 증명서가 유효하다는 취지를 통신부(36)를 통해 의뢰주의 엔드 엔티티 EE에 통지한다(단계 S 2008).

발명의 효과

이상, 본 발명의 일 실시예에 대하여 설명하였다.

본 실시예에서는 브릿지 인증국 CA_{bridge}로부터 각 단말기 수용 인증국 CA까지의 패스의 검색 및 검증을 엔드 엔티티 EE로부터의 공개 키 증명서의 유효성 확인 의뢰와는 독립하여 정기적으로 행하도록 하고 있다. 그리고, 어떤 엔드 엔티티 EE로부터 공개 키 증명서의 유효성 확인 의뢰를 받은 경우, 사전에 검색, 검증한 패스를 이용하여, 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA와 의뢰 대상의 공개 키 증명서를 발행한 단말기 수용 인증국 CA 사이에 브릿지 인증국 CA_{bridge}를 통한 패스를 구축할 수 있는지의 여부를 조사함으로써, 해당 공개 키 증명서가 유효한지의 여부를 판단하도록 하고 있다. 따라서, 공개 키 증명서의 유효성 확인 의뢰를 받고 나서, 해당 유효성을 확인하기까지 걸리는 시간을 단축할 수 있다.

또한, 본 실시예에서는 어떤 엔드 엔티티 EE로부터 공개 키 증명서의 유효성 확인 의뢰를 받은 경우, 사전에 검색, 검증한 패스를 이용하고, 해당 엔드 엔티티 EE를 수용하는 단말기 수용 인증국 CA와 의뢰 대상의 공개 키 증명서를 발행한 단말기 수용 인증국 CA 사이에 브릿지 인증국 CA_{bridge}를 통한 패스를 구축할 수 있을지의 여부를 조사하여, 할 수 있는 경우, 해당 패스 상의 인증국이 발행한 공개 키 증명서 중에 기술된 제한[신뢰하지 않은 다른 인증국의 명칭이나 최대 패스 길이(패스 상의 허용 최대 인증국 수)나 신뢰도(폴리시) 등]을 고려하여, 의뢰 대상의 공개 키 증명서가 유효한지의 여부를 최종적으로 판단하도록 하고 있다. 따라서, 공개 키 증명서의 유효성 확인의 판단을 보다 정확하게 행할 수 있다.

또, 본 발명은 상기한 실시예에 한정되는 것이 아니라, 그 요지의 범위 내에서 수많은 변형이 가능하다.

예를 들면, 상기한 실시예에서는 증명서 유효성 확인 센터 VC는 브릿지 인증국 CA_{bridge}를 기점 인증국으로 하여, 브릿지 인증국 CA_{bridge}로부터 각 단말기 수용 인증국 CA까지의 패스 검색 및 검증을 행하도록 하고 있다. 그러나, 본 발명은 이에 한정되지 않는다. 다른 임의의 인증국 CA를 기점 인증국으로서, 각 단말기 수용 인증국 CA까지의 패스 검색 및 검증을 행할 수도 있다. 예를 들면, 각 인증국 CA가 도 2에 도시한 관계에 있는 경우, 각 시큐리티 도메인 SD의 루트 인증국 CA_{11}, CA_{21}, CA_{31} 중 어느 하나를 기점 인증국으로서, 각 단말기 수용 인증국 CA까지의 패스 검색 및 검증을 행하도록 하더라도 좋다.

또한, 상기한 실시예에서는 설명을 알기 쉽게 하기 위해서, 도 2에 도시한 바와 같이 단말기 수용 인증국 CA는 엔드 엔티티 EE에 대해서만 공개 키 증명서를 발행하고, 그 밖의 인증국 CA는 인증국 CA에 대해서만 공개 키 증명서를 발행하는 것으로 하고 있지만, 본 발명은 엔드 엔티티 EE와 인증국 CA의 양방에 대하여 공개 키 증명서를 발행하는 인증국 CA를 포함하는 경우라도 마찬가지로 적용할 수 있다.

또한, 상기한 실시예에서는 인증국 CA의 구성으로서 각 시큐리티 도메인의 루트 인증국 CA끼리 상호 인증을 하는 것으로서 설명하였지만, 루트 인증국 CA에 한하지 않고 다른 인증국 CA가 상호 인증을 행하더라도 상관없다.

이상 설명한 바와 같이 본 발명에 따르면, 공개 키 증명서의 유효성 확인을 의뢰하고 나서, 해당 유효성이 확인될 때까지 걸리는 시간을 단축할 수 있다.

(57) 청구의 범위

청구항 1.

단말기로부터의 의뢰에 따라, 해당 단말기가 신뢰하는 인증국과는 다른 인증국이 발행한 공개 키 증명서의 유효성을 확인하는 증명서의 유효성 확인 방법에 있어서,

임의의 인증국을 기점 인증국으로 하여 해당 기점 인증국이 발행한 공개 키 증명서의 피발행처를 조사하고, 해당 피발행처에 인증국이 포함되는 경우에는 해당 인증국이 발행한 공개 키 증명서의 피발행처를 더 조사하는 처리를, 해당 공개 키 증명서의 피발행처가 전부 단말기가 될 때까지 계속함으로써, 상기 기점 인증국에서 임의의 단말기에 대하여

공개 키 증명서를 발행한 단말기 수용 인증국까지의 패스를 검색하는 패스 검색 단계,
상기 패스 검색 단계에 의해 검출된 패스에 대하여 상기 기점 인증국을 상류로 하여, 해당 패스 상의 단말기 수용 인증국이 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하여, 검증이 성립한 경우에는 하나 상류측의 인증국이 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하는 처리를, 해당 하나 상류측의 인증국이 상기 기점 인증국이 될 때까지 계속함으로써, 해당 패스를 검증하는 패스 검증 단계,
상기 패스 검증 단계에 의해 검증이 성립한 패스를 데이터 베이스에 등록하는 패스 등록 단계, 및
단말기로부터 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있었던 경우, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있을 때, 상기 공개 키 증명서의 유효성이 확인된 것으로 판단하는 유효성 확인 단계
를 포함하는 증명서의 유효성 확인 방법.

청구항 2.

제1항에 있어서, 상기 패스 검색 단계는 정기적으로 실행되고, 상기 패스 검증 단계는 상기 패스 검색 단계에 의해 검색된 최신 패스에 대하여 실행되며, 상기 패스 등록 단계는 상기 데이터 베이스의 등록 내용을 상기 패스 검증 단계에서 검증이 성립한 최신의 패스에 갱신하는 증명서의 유효성 확인 방법.

청구항 3.

제1항에 있어서,
상기 패스 등록 단계에 의해 상기 데이터 베이스에 등록되어 있는 각 패스에 대하여 해당 패스 상의 각 인증국이 발행한 하나 하류측의 인증국(발행처가 단말기 수용 인증국의 경우에는 해당 인증국이 수용하는 단말기)에 대한 공개 키 증명서 각각의 유효 기한을 조사하는 유효 기한 조사 단계, 및
상기 유효 기한 조사 단계에 의해 유효 기한이 경과한 것이 확인된 공개 키 증명서의 발행처으로부터 해당 공개 키 증명서의 피발행처에 대한 새로운 공개 키 증명서를 입수하고, 적어도 해당 새로운 공개 키 증명서의 서명을 상기 발행처보다 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하는 패스 재검증 단계
를 더 포함하고,
상기 패스 등록 단계는,
상기 패스 재검증 단계에서 상기 새로운 공개 키 증명서의 서명 검증이 성립하지 않는 경우, 또는 상기 새로운 공개 키 증명서를 입수할 수 없는 경우에는, 상기 유효 기한 조사 단계에 의해 유효 기한이 경과한 것이 확인된 공개 키 증명서의 발행처와 피발행처를 포함하는 패스를 상기 데이터 베이스에서 삭제하는 증명서의 유효성 확인 방법.

청구항 4.

제1항에 있어서,
상기 패스 등록 단계에 의해 상기 데이터 베이스에 등록되어 있는 각 패스에 대하여 해당 패스 상의 각 인증국이 발행한 공개 키 증명서의 실효 정보를 조사하는 실효 정보 조사 단계
를 더 포함하고,
상기 패스 등록 단계는,
상기 실효 정보 조사 단계에 의해 효력이 상실한 것이 확인된 공개 키 증명서의 발행처와 피발행처를 포함하는 패스가 상기 데이터 베이스에 등록되어 있는 경우에는, 이를 상기 데이터 베이스에서 삭제하는 증명서의 유효성 확인 방법.

청구항 5.

제1항에 있어서,
상기 유효성 확인 단계는,
단말기로부터 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있었던 경우, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스, 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있는 경우라도, 상기 두 개의 패스 상의 어느 하나의 인증국이 발행한 해당 인증국이 위치하는 패스 상의 하나 하류측의 인증국(발행처가 단말기 수용 인증국의 경우에는, 해당 인증국이 수용하는 단말기)에 대한 공개 키 증명서 중에, 상기 두 개의 패스 상의 어느 하나의 인증국을 신뢰하지 않는다는 취지의 제한이 기술되어 있는 경우에는, 상기 공개 키 증명서의 유효성이 확인되지 않은 것으로 판단하는 증명서의 유효성 확인 방법.

청구항 6.

제1항에 있어서,
상기 유효성 확인 단계는,
단말기로부터 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있었던 경우, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스, 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있는 경우라도, 상기 두 개의 패스 상의 어느 하나의 인증국이 발행한 해당 인증국이 위치하는 패스 상의 하나 하류측의 인증국(발행처가 단말기 수용 인증국의 경우에는, 해당 인증국이 수용하는 단말기)에 대한 공개 키 증명서 중에 기술되어 있는 패스 길이(패스 상의 허용 최대 인증국 수)를 상기 두 개의 패스 상의 인증국의 합계 수가 넘는 경우에는, 상기 공개 키 증명서의 유효성이 확인되지 않은 것으로 판단하는 증명서의 유효성 확인 방법.

청구항 7.
제1항에 있어서,
상기 유효성 확인 단계는,
단말기로부터 해당 단말기가 행하고자 하는 전자 수속에 요구되는 신뢰도의 제시를 따른, 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있는 경우, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스, 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있는 경우라도, 상기 두 개의 패스 상의 어느 하나의 인증국이 발행한, 해당 인증국이 위치하는 패스 상의 하나 하류측의 인증국(발행처가 단말기 수용 인증국의 경우에는, 해당 인증국이 수용하는 단말기)에 대한 공개 키 증명서 중에 기술되어 있는 신뢰도(policy)가 상기 전자 수속에 요구될 수 있는 신뢰도보다 낮은 경우에는, 상기 공개 키 증명서의 유효성이 확인되지 않은 것으로 판단하는 증명서의 유효성 확인 방법

청구항 8.
제1항에 있어서, 상기 기점 인증국은 적어도 두 개의 시큐리티 도메인의 루트 인증국 각각과 상호 인증을 행하고 있는 브릿지 인증국인 증명서의 유효성 확인 방법.

청구항 9.
단말기로부터의 의뢰에 따라 해당 단말기가 신뢰하는 인증국과는 다른 인증국이 발행한 공개 키 증명서의 유효성을 확인하는 증명서의 유효성 확인 장치에 있어서,
임의의 인증국을 기점 인증국으로 하여, 해당 기점 인증국이 발행한 공개 키 증명서의 피발행처를 조사하고, 해당 피발행처에 인증국이 포함되는 경우에는 해당 인증국이 발행한 공개 키 증명서의 피발행처를 더 조사하는 처리를, 해당 공개 키 증명서의 피발행처가 전부 단말기가 될 때까지 계속함으로써, 상기 기점 인증국에서 임의의 단말기에 대하여 공개 키 증명서를 발행한 단말기 수용 인증국까지의 패스를 검색하는 패스 검색 수단,
상기 패스 검색 수단에 의해 검출된 패스에 대하여 상기 기점 인증국을 상류로 하여, 해당 패스 상의 단말기 수용 인증국이 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하여, 검증이 성립한 경우에는 하나 상류측의 인증국이 발행한 공개 키 증명서의 서명을 더 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하는 처리를, 하나 상류측의 인증국이 상기 기점 인증국이 될 때까지 계속함으로써, 해당 패스를 검증하는 패스 검증 수단,
상기 패스 검증 수단에 의해 검증이 성립한 패스를 데이터 베이스에 등록하는 패스 등록 수단, 및
단말기로부터 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있었던 경우, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스, 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있을 때, 상기 공개 키 증명서의 유효성이 확인된 것으로 판단하는 유효성 확인 수단
을 포함하는 증명서의 유효성 확인 장치.

청구항 10.
단말기로부터의 의뢰에 따라 해당 단말기가 신뢰하는 인증국과는 다른 인증국이 발행한 공개 키 증명서의 유효성을 확인하기 위한 프로그램이 기억된 기억 매체에 있어서,
상기 프로그램은 컴퓨터에서 판독되어 실행됨으로써,
임의의 인증국을 기점 인증국으로 하여 해당 기점 인증국이 발행한 공개 키 증명서의 피발행처를 조사하고, 해당 발행처에 인증국이 포함되는 경우에는 해당 인증국이 발행한 공개 키 증명서의 피발행처를 더 조사하는 처리를, 해당 공개 키 증명서의 피발행처가 전부 단말기가 될 때까지 계속함으로써, 상기 기점 인증국에서 임의의 단말기에 대하여 공개 키 증명서를 발행한 단말기 수용 인증국까지의 패스를 검색하는 패스 검색 수단,
상기 패스 검색 수단에 의해 검출된 패스에 대하여 상기 기점 인증국을 상류로 하고, 해당 패스 상의 단말기 수용 인증국이 발행한 공개 키 증명서의 서명을 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하여, 검증이 성립한 경우에는 하나 상류측의 인증국이 발행한 공개 키 증명서의 서명을 더 하나 상류측의 인증국이 발행한 공개 키 증명서로 검증하는 처리를, 하나 상류측의 인증국이 상기 기점 인증국이 될 때까지 계속함으로써, 해당 패스를 검증하는 패스 검증 수단,
상기 패스 검증 수단에 의해 검증이 성립한 패스를 데이터 베이스에 등록하는 패스 등록 수단, 및
단말기로부터 해당 단말기가 신뢰하는 인증국과는 다른 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성 확인 의뢰가 있는 경우, 상기 단말기가 신뢰하는 인증국과 상기 기점 인증국 사이의 패스 및 상기 다른 단말기 수용 인증국과 상기 기점 인증국 사이의 패스가 상기 데이터 베이스에 등록되어 있을 때, 상기 공개 키 증명서의 유효성이 확인된 것으로 판단하는 유효성 확인 수단
을 해당 컴퓨터 상에 구축하는 프로그램이 기억된 기억 매체.

청구항 11.
컴퓨터가 공개 키 증명서의 유효성을 확인하는 공개 키 증명서의 유효성 확인 방법에 있어서,
상기 컴퓨터는,
기점이 되는 임의의 인증국 및 단말기에 공개 키 증명서를 발행하는 단말기 수용 인증국간의 패스를 검색하는 패스 검색 단계와,
상기 패스 검색 단계에 의해 검색된 패스를 검증하는 패스 검증 단계와,
상기 패스 검증 단계에 의해 검증된 패스를 데이터베이스에 등록하는 패스 등록 단계와,
공개 키 증명서의 유효성 확인 의뢰를 수신하여 상기 데이터베이스에 등록되어 있는 검증된 패스에 관한 정보를 이용

하여, 상기 단말기 수용 인증서가 발행한 공개 키 증명서의 유효성을 확인하는 유효성 확인 단계를 행하며,
상기 컴퓨터는, 상기 패스 검색 단계에서,
상기 기점이 되는 임의의 인증국을 발행처 인증국으로 하는 제1 단계와,
상기 발행처 인증국의 장치가 발행한 모든 공개 키 증명서의 피발행처를 입수하는 제2 단계와,
상기 제2 단계에서 입수한 피발행처 각각에 대해, 해당 피발행처가 인증국인 경우는, 해당 피발행처의 인증국과 상기 발행처 인증국 간에 패스를 설정하여, 해당 피발행처의 인증국을 새로운 발행처 인증국으로 하고, 해당 피발행처가 단말기인 경우는, 상기 발행처 인증국을 단말기 수용 인증국으로 하여, 적어도 하나의 상기 설정된 패스로 이루어지는, 상기 기점이 되는 임의의 인증국과 상기 단말기 수용 인증국 간의 패스를 상기 검색된 패스로 하는 제3 단계와,
상기 제2 단계에서 입수한 피발행처에 인증국이 포함되는 경우는, 상기 제2 단계로 복귀하는 제4 단계를 행하며,
상기 컴퓨터는, 상기 패스 검증 단계에서,
상기 단말기 수용 인증국을 피발행처 인증국으로 하는 제5 단계와,
상기 피발행처 인증국이 발행한 공개 키 증명서의 서명을, 상기 검색된 패스 상의 상기 발행처 인증국이 발행한 공개 키 증명서로 검증하는 제6 단계와,
상기 서명을 검증한 경우이고, 또한 상기 패스 상의 상기 발행처 인증국이 상기 기점이 되는 임의의 인증국이 아닌 경우는, 해당 발행처 인증국을 상기 패스 상의 새로운 피발행처 인증국으로 하여, 제6 단계로 복귀하고, 상기 서명을 검증을 한 경우이며, 또한 상기 패스 상의 상기 발행처 인증국이 상기 기점이 되는 임의의 인증국인 경우는, 상기 검색된 패스를 검증된 패스로 하는 제7 단계를 행하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 12.

제11항에 있어서,
상기 컴퓨터는, 상기 유효성 확인 단계에서, 상기 기점이 되는 임의의 인증국과 상기 유효성 확인 의뢰처가 신뢰하는 인증국 간의 패스, 및 상기 기점이 되는 임의의 인증국과 상기 단말기 수용 인증국 간의 패스가 상기 데이터베이스에 등록되어 있는 패스에 포함되어 있을 때, 상기 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성이 확인된 것으로 판단하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 13.

제12항에 있어서,
상기 컴퓨터는, 상기 유효성 확인 단계에서, 상기 유효성 확인 의뢰처가 신뢰하는 인증국이 상기 기점이 되는 임의의 인증국인 경우, 상기 기점이 되는 임의의 인증국과 상기 단말기 수용 인증국 간의 패스가 상기 데이터베이스에 등록되어 있을 때, 상기 단말기 수용 인증국이 발행한 공개 키 증명서의 유효성이 확인된 것으로 판단하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 14.

제11 내지 제13항 중 어느 한 항에 있어서,
상기 컴퓨터는, 상기 제3 단계에서, 상기 제2 단계에서 입수한 피발행처 각각에 대해, 해당 피발행처가 인증국이며, 또한 해당 인증국이 이미 설정되어 있는 패스에 포함되어 있는 경우, 해당 인증국을 피발행처 인증국으로 하지 않는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 15.

제11항에 있어서,
상기 컴퓨터는, 상기 패스 검색 단계를 상기 유효성 확인 단계와는 독립적으로 실행하고, 상기 패스 검증 단계를 상기 패스 검색 단계에 의해 검색된 패스에 대해 실행하고,
상기 컴퓨터는, 상기 패스 등록 단계에서, 상기 데이터베이스의 등록 내용을 상기 패스 검증 단계에서 검증된 패스로 갱신하는 단계를 포함하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 16.

제11항에 있어서,
상기 컴퓨터는, 또한
상기 패스 등록 단계에 의해 상기 데이터베이스에 등록되어 있는 각각의 패스에 대해, 상기 패스 상의 각 인증국이 발행한 공개 키 증명서 각각의 유효 기한을 조사하는 유효 기한 조사 단계와,
상기 유효 기한 조사 단계에 의해 유효 기한을 초과하고 있는 것이 확인된 공개 키 증명서의 발행처 인증국의 장치로부터, 해당 공개 키 증명서의 피발행처에 대한 새로운 공개 키 증명서의 입수를 시도하는 입수 단계와,
입수한 새로운 공개 키 증명서의 서명을, 상기 발행처 인증국을 상기 패스 상에서 피발행처의 인증국으로 하는 인증국의 장치가 발행한 공개 키 증명서로 검증하는 패스 재검증 단계를 행하고,
상기 컴퓨터는, 상기 패스 등록 단계에서, 상기 패스 재검증 단계에서 상기새로운 공개 키 증명서의 서명이 검증되지 않은 경우, 또는 상기 입수 단계에서 상기 새로운 공개 키 증명서를 입수할 수 없는 경우는, 상기 유효 기한을 초과하고 있는 것이 확인된 공개 키 증명서를 포함한, 패스를 상기 데이터베이스로부터 삭제하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 17.

제11항에 있어서,
상기 컴퓨터는, 또한, 상기 패스 등록 단계에 의해 상기 데이터베이스에 등록되어 있는 각각의 패스에 대해, 상기 패스 상의 각 인증국이 발행한 공개 키 증명서의 실효 정보를 조사하는 실효 정보 조사 단계를 행하고,
상기 패스 등록 단계는, 상기 실효 정보 조사 단계에서 얻은 상기 실효 정보에 의해 실효되어 있는 것이 확인된 공개

키 증명서를 포함하는 패스를 상기 데이터베이스로부터 삭제하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 18.

제11항에 있어서,

상기 컴퓨터는, 상기 제6 단계에서의 공개 키 증명서를 실효 정보로 검증하는 실효 정보 조사 단계를 행하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 19.

제18항에 있어서,

상기 컴퓨터는, 상기 실효 정보 조사 단계에서, 상기 패스 등록 단계에 의해 상기 데이터베이스에 등록되어 있는 각각의 패스에 대해,

상기 패스 상의 각 인증국이 발행한 공개 키 증명서의 실효 정보 각각의 작성 예정 일시를 넘기고 있는지를 조사하는 실효 정보 예정 일시 조사 단계와,

상기 실효 정보 예정 일시 조사 단계에 의해, 작성 일시가 초과한 것이 확인된 실효 정보의 발행처 인증국의 장치로부터, 해당 실효 정보에 대한 새로운 실효 정보를 입수하는 입수 단계와,

입수한 새로운 실효 정보에 기술되어 있는 공개 키 증명서가, 상기 데이터베이스에 등록되어 있는지의 여부를 조사하는 실효 증명서 조사 단계를 행하고,

상기 컴퓨터는, 상기 패스 등록 단계에서, 상기 실효 증명서 길이 조사 단계에 의해 실효되어 있는 것이 확인된 공개 키 증명서를 포함하는 패스를 상기 데이터베이스로부터 삭제하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 20.

제11항에 있어서,

상기 컴퓨터는, 상기 유효성 확인 단계에서, 상기 기점이 되는 임의의 인증국과 상기 유효성 확인 의뢰처 간의 패스가 상기 데이터베이스에 등록되어 있는 경우라도, 상기 패스 상의 어느 한 인증국이 발행한 공개 키 증명서 중에, 상기 패스 상의 어느 다른 인증국을 신뢰하지 않는다는 취지가 기술되어 있는 경우는, 상기 공개 키 증명서의 유효성이 확인되지 않은 것으로 판단하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 21.

제11항에 있어서,

상기 컴퓨터는, 상기 유효성 확인 단계에서, 상기 기점이 되는 임의의 인증국과 상기 유효성 확인 의뢰처 간의 패스가 상기 데이터베이스에 등록되어 있는 경우라도, 상기 패스 상의 어느 한 인증국이 발행한, 상기 패스 상의 피발행처 인증국에 대한 공개 키 증명서 중에 기술되어 있는 상기 패스 상의 허용 최대 인증국수가 상기 패스 상의 합계 인증국수를 초과하는 경우에는, 상기 공개 키 증명서의 유효성이 확인되지 않은 것으로 판단하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 22.

제11항에 있어서,

상기 공개 키 증명서의 유효성 확인 의뢰가 전자 수속에 요구되는 신뢰도의 제시를 수반하는 경우, 상기 컴퓨터는, 상기 유효성 확인 단계에서,

상기 기점이 되는 임의의 인증국과 상기 유효성 확인 의뢰처 간의 패스가 상기 데이터베이스에 등록되어 있는 경우라도, 상기 패스 상의 어느 한 인증국이 발행한, 상기 패스 상의 피발행처 인증국에 대한 공개 키 증명서 중에 기술되어 있는 신뢰도가, 상기 전자 수속에 요구되는 신뢰도보다 낮은 경우는, 상기 공개 키 증명서의 유효성이 확인되지 않은 것으로 판단하는 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

청구항 23.

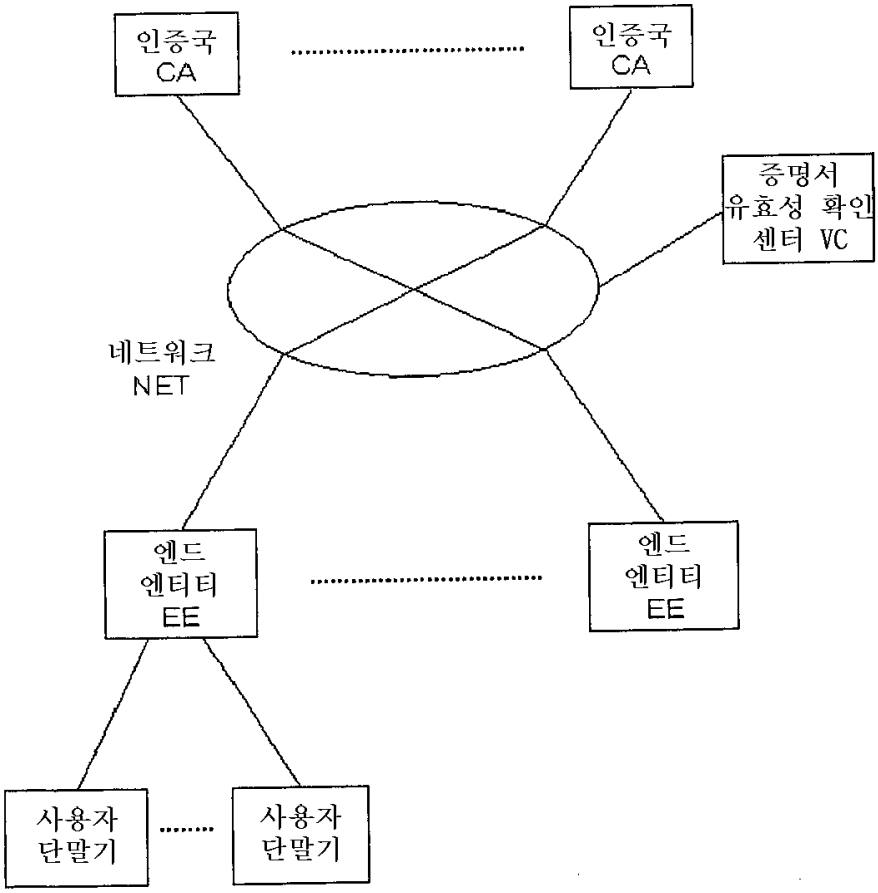
제11항에 있어서,

상기 기점이 되는 임의의 인증국은 적어도 2개의 시큐리티 도메인의 루트 인증국 각각과 상호 인증을 행하고 있는 브릿지 인증국인 것을 특징으로 하는 공개 키 증명서의 유효성 확인 방법.

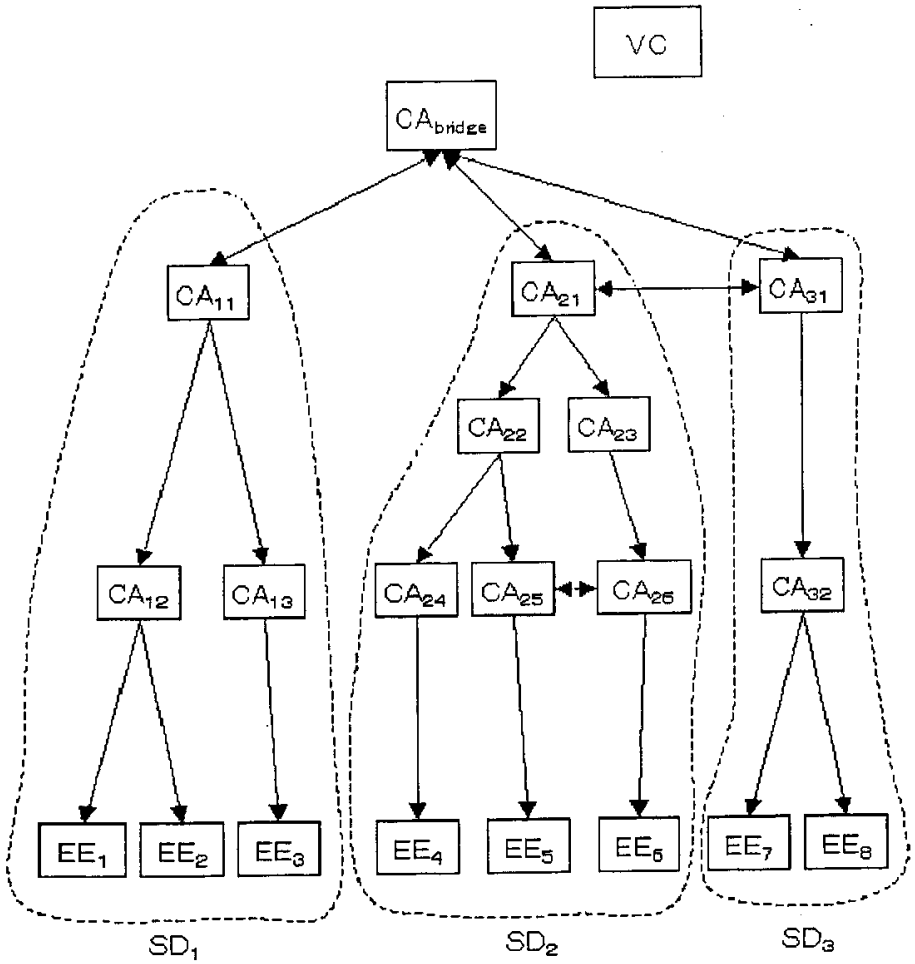
도면

도면1

PKI 시스템


인증국
CA
인증국
CA
증명서
유효성 확인
센터 VC
네트워크
NET
엔드
엔티티
EE
엔드
엔티티
EE
사용자
단말기
사용자
단말기

도면2



→ : 공개키 증명서의 흐름

CA: 인증국

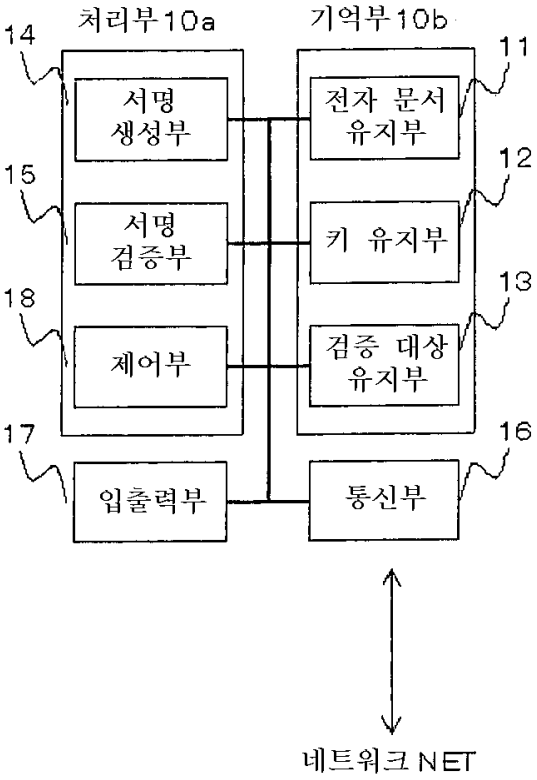
EE: 엔드 엔티티

VC: 증명서 유효성 확인 센터

SD: 시큐리티 도메인

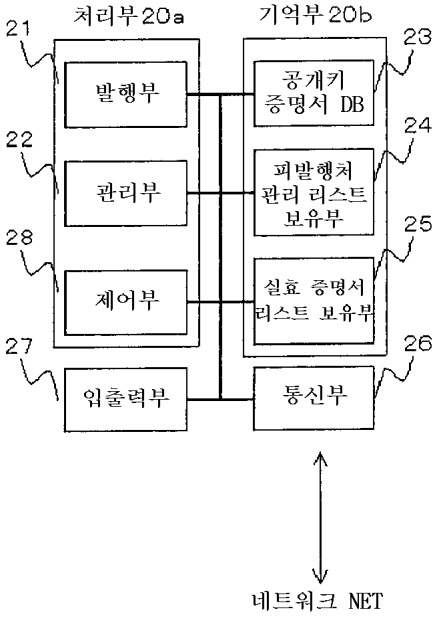
도면3

엔드 엔티티 EE

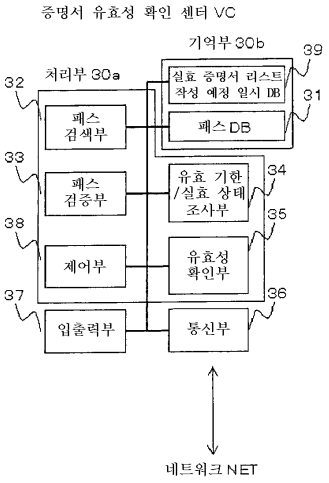


도면4

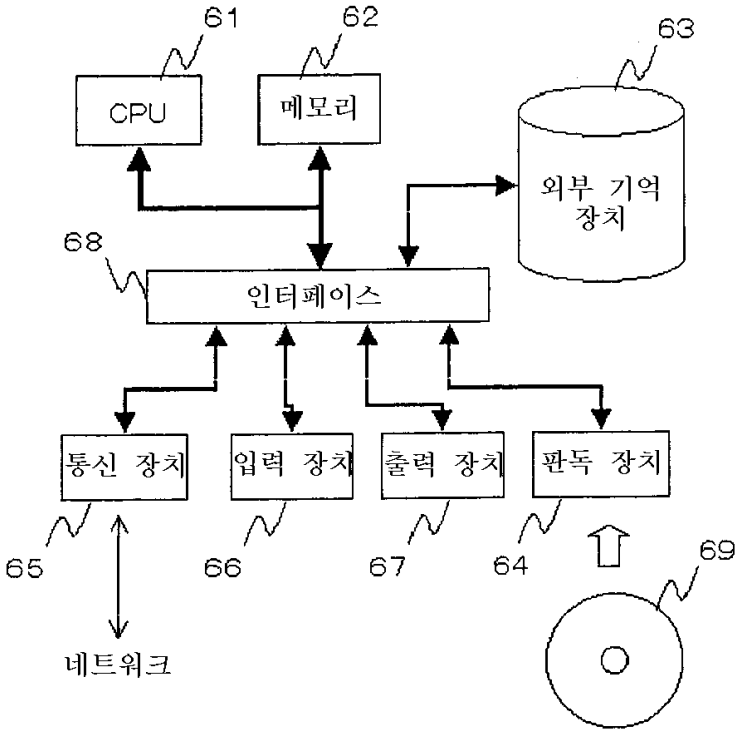
인증국 CA



도면5

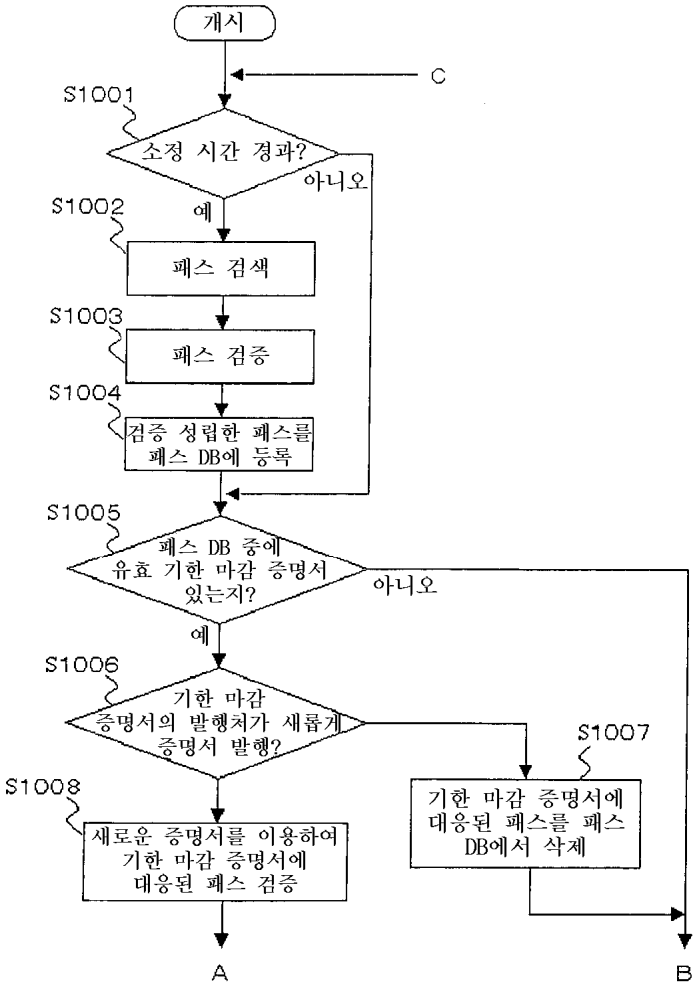

증명서 유효성 확인 센터 VC
기억부 30b
처리부 30a
실효 증명서 리스트 작성 예정 일시 DB
패스 DB
패스 검색부
패스 검증부
유효 기한 /실효 상태 조사부
제어부
유효성 확인부
입출력부
통신부
32
33
38
37
39
31
34
35
36
네트워크 NET

도면6


61
62
63
CPU
메모리
외부 기억 장치
68
인터페이스
통신 장치
입력 장치
출력 장치
판독 장치
65
66
67
64
69
네트워크

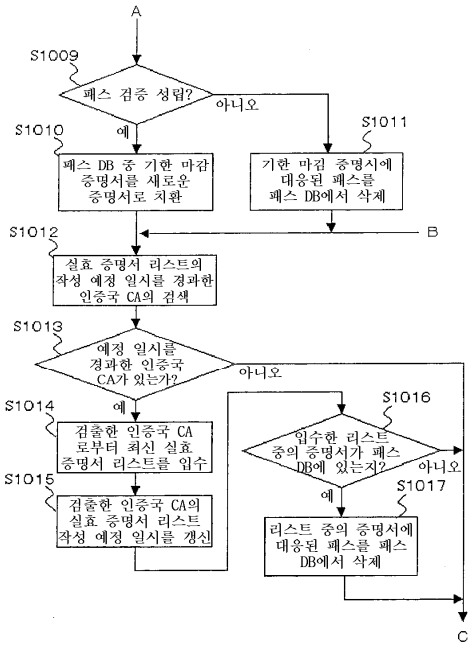
도면7

패스 검색, 검증 및 관리 동작



도면8

패스 검색, 검증 및 관리 동작



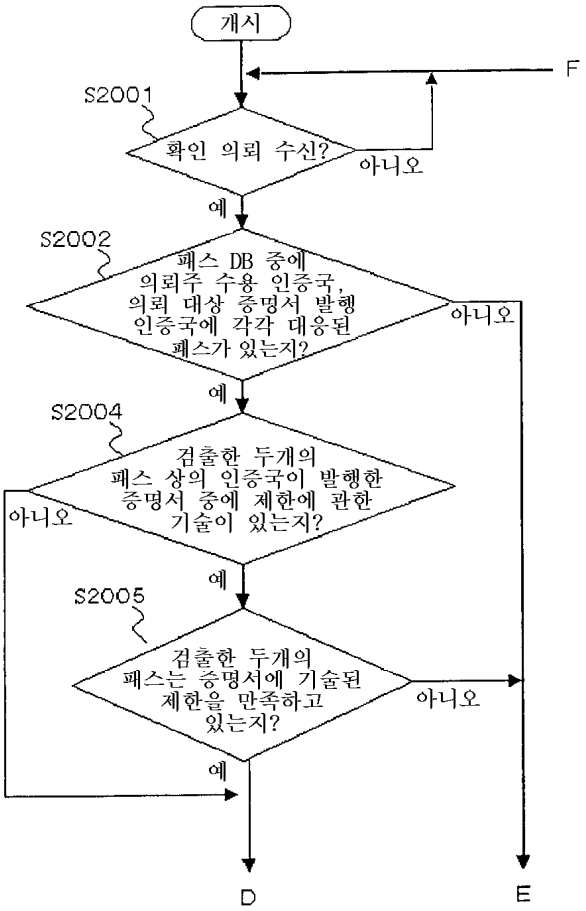
도면9

패스 검색 결과(도 2의 경우)

단말기 수용 인증국	버스
CA_{12}	$CA_{bride}-CA_{11}-CA_{12}$
CA_{13}	$CA_{bride}-CA_{11}-CA_{13}$
CA_{24}	$CA_{bride}-CA_{21}-CA_{22}-CA_{24}$
	$CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{24}$
CA_{25}	$CA_{bride}-CA_{21}-CA_{22}-CA_{25}$
	$CA_{bride}-CA_{21}-CA_{23}-CA_{26}-CA_{25}$
	$CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{25}$
	$CA_{bride}-CA_{31}-CA_{21}-CA_{23}-CA_{25}-CA_{25}$
CA_{26}	$CA_{bride}-CA_{21}-CA_{23}-CA_{26}$
	$CA_{bride}-CA_{21}-CA_{22}-CA_{25}-CA_{26}$
	$CA_{bride}-CA_{31}-CA_{21}-CA_{23}-CA_{26}$
	$CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26}$
CA_{32}	$CA_{bride}-CA_{31}-CA_{32}$
	$CA_{bride}-CA_{21}-CA_{31}-CA_{32}$

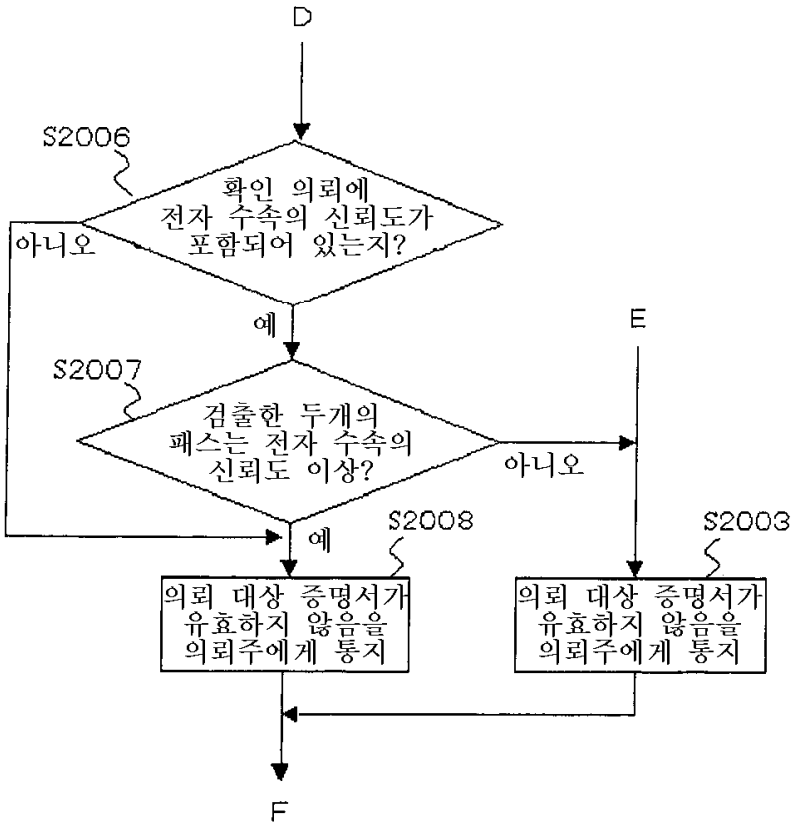
도면10

공개키 증명서의 유효성 확인 동작

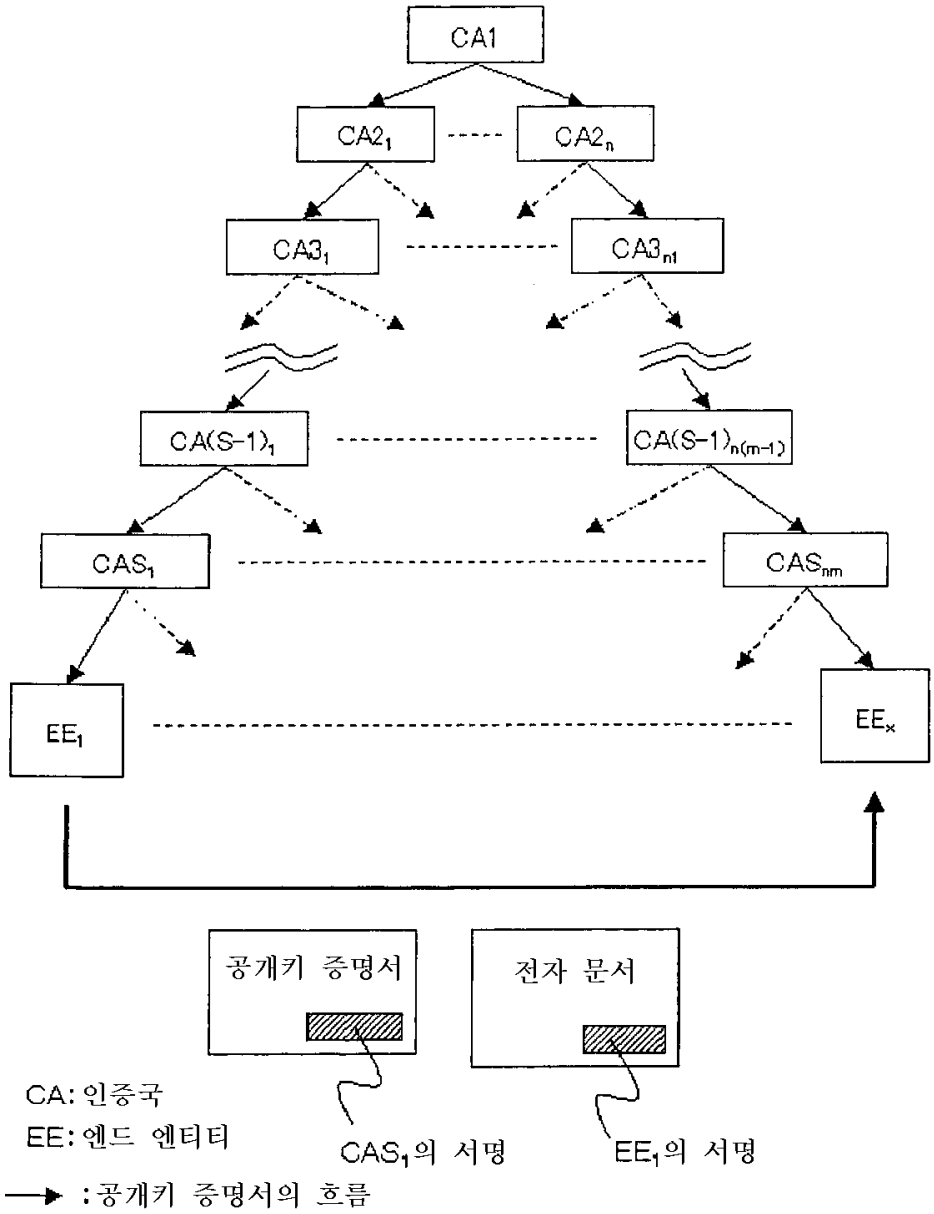


도면11

공개키 증명서의 유효성 확인 동작



도면12


CA1
CA2₁
CA2ₙ
CA3₁
CA3ₙ₁
CA(S-1)₁
CA(S-1)ₙ₍ₘ₋₁₎
CAS₁
CASₙₘ
EE₁
EEₓ
공개키 증명서
전자 문서
CA: 인증국
EE: 엔드 엔티티
CAS₁의 서명
EE₁의 서명
: 공개키 증명서의 흐름