(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년12월10일
(11) 등록번호 10-2054444
(24) 등록일자 2019년12월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/3268 (2013.01)
H04L 9/321 (2013.01)
(21) 출원번호 10-2017-7018303
(22) 출원일자(국제) 2015년12월14일
심사청구일자 2017년07월03일
(85) 번역문제출일자 2017년07월03일
(65) 공개번호 10-2017-0094276
(43) 공개일자 2017년08월17일
(86) 국제출원번호 PCT/US2015/065634
(87) 국제공개번호 WO 2016/140724
국제공개일자 2016년09월09일
(30) 우선권주장
14/570,867 2014년12월15일 미국(US)
(56) 선행기술조사문헌
US20100268942 A1*
US20130254535 A1*
US20130275750 A1
US20030046544 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
아마존 테크놀로지스, 인크.
미국 98108-1226 워싱턴주 시애틀 피오 박스 81226
(72) 발명자
보웬, 피터 자카리
미국 98109-5210 워싱턴주 시애틀 테리 애비뉴 노스 410
(74) 대리인
양영준, 백만기

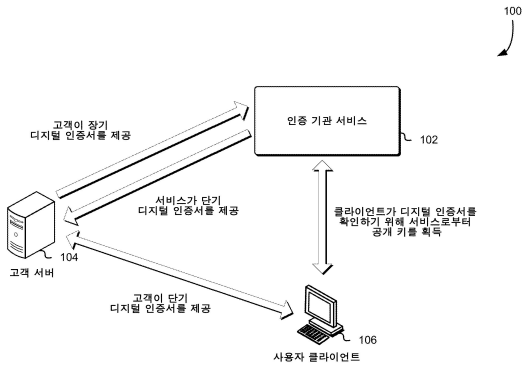
전체 청구항 수 : 총 15 항 심사관 : 양종필

(54) 발명의 명칭 **장기 디지털 인증서 검증에 기초한 단기 디지털 인증서 발급**

(57) 요 약

인증 기관 서비스는 엔티티 및 서비스 간 검증 목적들을 위해 엔티티로부터 장기 디지털 인증서를 발급하기 위한 요청을 수신한다. 장기 디지털 인증서의 발급 시, 엔티티는 장기 디지털 인증서보다 짧은 유효 기간을 포함하는 단기 디지털 인증서의 발급에 대한 요청을 서비스에 제출한다. 서비스는 엔티티를 검증하기 위해 장기 디지털 인증서를 이용할 수 있고, 엔티티를 검증 시, 단기 디지털 인증서를 엔티티에 발급할 수 있다. 그 후 엔티티는 사용자 클라이언트가 엔티티를 인증하고 엔티티와 안전하게 통신하게 하기 위해 단기 디지털 인증서를 이용할 수 있다.

대 표 도



명 세 서

청구범위

청구항 1

컴퓨터-구현 방법으로서,

실행가능한 명령들로 구성된 하나 이상의 컴퓨터 시스템의 제어 하에,

제1 디지털 인증서를 엔티티에 발급하는 단계로서, 상기 제1 디지털 인증서는 인증 기관 서비스에 상기 엔티티의 검증을 가능하게 하는 중요 확장(critical extension)을 지정하고, 상기 제1 디지털 인증서는:

상기 엔티티에 특유한 적어도 하나의 주체 필드를 지정하고;

제1 공개 암호화 키를 지정하고;

제1 비밀 암호화 키에 대응하며; 그리고

상기 제1 디지털 인증서에 대한 제1 유효 기간을 지정하는, 상기 제1 디지털 인증서를 엔티티에 발급하는 단계;

상기 엔티티로부터, 제2 디지털 인증서의 발급에 대한 요청을 수신하는 단계로서, 상기 요청은 상기 제1 디지털 인증서 및 디지털 서명을 포함하고, 상기 제2 디지털 인증서는 상기 엔티티의 서버의 인증을 위해 사용가능한 것인, 상기 제2 디지털 인증서의 발급에 대한 요청을 수신하는 단계;

상기 제1 디지털 인증서 내에 지정된 유효 기간 및 상기 제1 공개 암호화 키에 적어도 부분적으로 기초하여, 상기 제2 디지털 인증서를 발급할지 여부를 결정하는 단계; 및

상기 적어도 하나의 주체 필드 및 상기 제1 유효 기간보다 짧은 제2 유효 기간을 갖기 위한 제2 디지털 인증서를 발급하는 단계

를 포함하고, 상기 제2 유효 기간은 상기 제2 디지털 인증서 내에 지정되는, 컴퓨터-구현 방법.

청구항 2

청구항 1에 있어서, 인증 기관 서비스에 상기 엔티티의 검증을 가능하게 하는 상기 중요 확장은 또한 상기 제1 디지털 인증서가 상기 엔티티의 상기 서버의 인증을 위해 사용될 수 없도록 만드는, 컴퓨터-구현 방법.

청구항 3

청구항 1에 있어서, 상기 중요 확장은 상기 제1 디지털 인증서의 발급 이전 상기 인증 기관 서비스에 의한 상기 엔티티의 검증 날짜, 상기 엔티티를 검증하기 위해 상기 인증 기관 서비스에 의해 이용된 하나 이상의 표준, 및 상기 엔티티에 대응하는 식별자를 지정하는, 컴퓨터-구현 방법.

청구항 4

청구항 1에 있어서, 상기 제2 디지털 인증서는 상기 제1 디지털 인증서에 지정된 상기 제1 공개 암호화 키와 별개의 제2 공개 암호화 키를 더 포함하는, 컴퓨터-구현 방법.

청구항 5

하나 이상의 서비스를 구현하도록 구성된 적어도 하나의 컴퓨팅 디바이스를 포함하는 시스템으로서, 상기 하나 이상의 서비스는:

제1 디지털 인증서를 엔티티에 발급하되, 상기 제1 디지털 인증서는:

상기 하나 이상의 서비스에 상기 엔티티의 검증을 가능하게 하고;

상기 제1 디지털 인증서에 대한 제1 유효 기간을 지정하고; 그리고

상기 엔티티에 특유한 적어도 하나의 주체 필드를 지정하며;

상기 엔티티로부터, 제2 디지털 인증서의 발급에 대한 요청을 수신하되, 상기 요청은 상기 제1 디지털 인증서를 포함하는 것이고, 상기 제2 디지털 인증서는 상기 엔티티의 인증을 위해 사용가능한 것이고;

상기 제1 디지털 인증서 내에 지정된 정보에 적어도 부분적으로 기초하여, 상기 제2 디지털 인증서를 발급할지 여부를 결정하며; 그리고

상기 제1 디지털 인증서 내에 지정된 상기 정보에 적어도 부분적으로 기초한 정보를 갖게끔, 그리고 상기 엔티티에 특유한 상기 적어도 하나의 주체 필드, 및 상기 제1 유효 기간보다 짧고 상기 제2 디지털 인증서 내에 지정되는 제2 유효 기간을 갖게끔, 상기 제2 디지털 인증서를 발급하도록 구성된, 시스템.

청구항 6

청구항 5에 있어서,

상기 제2 디지털 인증서의 발급에 대한 상기 요청은 디지털 서명을 포함하며; 그리고

상기 하나 이상의 서비스는 상기 제1 디지털 인증서 내에 지정된 공개 암호화 키를 사용하여 상기 디지털 서명을 확인하도록 더 구성된, 시스템.

청구항 7

청구항 5에 있어서,

상기 하나 이상의 서비스는 상기 제1 디지털 인증서가 만료되지 않았고 상기 제2 디지털 인증서의 발급을 위해 이용될 수 있음을 확인하기 위해 상기 제1 디지털 인증서에 대한 상기 유효 기간을 이용하도록 더 구성된, 시스템.

청구항 8

청구항 7에 있어서, 상기 하나 이상의 서비스는 상기 제2 유효 기간이 상기 제1 유효 기간을 넘어서 확장되지 않게끔 보장하도록 더 구성된, 시스템.

청구항 9

청구항 5에 있어서, 상기 제2 디지털 인증서 내에 포함되는 상기 정보는 또한 상기 제2 디지털 인증서의 발급에 대한 상기 요청 내에 상기 엔티티에 의해 지정된 유효 기간에 적어도 부분적으로 기초하는, 시스템.

청구항 10

청구항 5에 있어서, 상기 제2 디지털 인증서는 또한 상기 제1 디지털 인증서 내에 포함되지 않은 하나 이상의 추가 주체 필드를 갖도록 발급되는, 시스템.

청구항 11

청구항 5에 있어서, 상기 제1 디지털 인증서는 상기 제1 디지털 인증서가 인증을 위해 사용되지 않아야 함을 나타내는 중요 확장을 지정하는, 시스템.

청구항 12

청구항 11에 있어서, 상기 중요 확장은 상기 제1 디지털 인증서의 발급 이전 상기 하나 이상의 서비스에 의한 상기 엔티티의 검증 날짜, 상기 엔티티를 검증하기 위해 상기 하나 이상의 서비스에 의해 이용되는 하나 이상의 표준, 및 상기 엔티티에 대응하는 식별자를 포함하는, 시스템.

청구항 13

하나 이상의 서비스를 구현하도록 구성된 적어도 하나의 컴퓨팅 디바이스를 포함하는 시스템으로서, 상기 하나 이상의 서비스는:

엔티티로부터, 상기 엔티티의 인증을 위해 사용가능한 디지털 인증서의 발급에 대한 요청을 수신하되, 상기 요청은 인증 기관 서비스에 상기 엔티티를 검증하기 위해 사용가능한 이전에 발급된 디지털 인증서를 포함하고 상기 엔티티에 특유한 적어도 하나의 주체 필드, 및 상기 이전에 발급된 디지털 인증서에 대한 유효 기간을 지정

하는 것이고;

상기 이전에 발급된 디지털 인증서 내에 지정된 정보에 적어도 부분적으로 기초하여, 상기 디지털 인증서를 발급할지 여부를 결정하며; 그리고

상기 이전에 발급된 디지털 인증서 내에 지정된 상기 정보에 적어도 부분적으로 기초한 정보를 갖게끔, 그리고 상기 엔티티에 특유한 상기 적어도 하나의 주체 필드, 및 상기 이전에 발급된 디지털 인증서에 대한 상기 유효 기간보다 짧고 상기 디지털 인증서 내에 지정되는 유효 기간을 갖게끔, 상기 디지털 인증서를 발급하도록 구성된, 시스템.

청구항 14

청구항 13에 있어서, 상기 하나 이상의 서비스는 상기 디지털 인증서를 발급할지 여부를 결정하기 위해 상기 요청 내에 상기 엔티티에 의해 정의된 원하는 유효 기간을 획득하도록 더 구성된, 시스템.

청구항 15

청구항 13에 있어서,

상기 하나 이상의 서비스는 상기 이전에 발급된 디지털 인증서가 만료되지 않았고 상기 디지털 인증서의 발급을 위해 이용될 수 있음을 확인하기 위해 상기 유효 기간을 이용하도록 더 구성되고,

상기 디지털 인증서의 발급에 대한 상기 요청은 상기 이전에 발급된 디지털 인증서에 지정된 공개 암호화 키에 대응하는 비밀 암호화 키를 이용하여 상기 엔티티에 의해 디지털 방식으로 서명되는, 시스템.

발명의 설명

기 술 분 야

[0001] 관련 출원에 대한 상호-참조

[0002] 본 출원은 2014년 12월 15일에 출원된, "장기 디지털 인증서 검증에 기초한 단기 디지털 인증서 발급"이라는 명칭의, 동시 계류중인 미국 특허 출원 제14/570,867호로부터의 우선권을 주장하며, 이의 내용은 그 전체가 본 출원에 참조로 원용된다.

배 경 기 술

[0003] 인증 기관은 일반적으로 고객들이 다른 엔티티들과의 보안 통신을 설정할 수 있게 하기 위해 그리고 이러한 다른 엔티티들이 이러한 고객들을 인증하는 것을 가능하게 하기 위해 이러한 고객들에게 디지털 인증서들을 발급한다. 고객에게 디지털 인증서를 발급하기 위해, 인증 기관은 정부 데이터베이스,들 제3자 데이터베이스들 및 서비스들, 및 다른 고객 기술들을 검사함으로써 고객에 관한 정보를 검증할 필요가 있을 수 있다. 고객에 관한 정보가 인증 기관에 의해 검증될 수 있는 경우, 인증 기관은 디지털 인증서를 생성하고 이를 고객에게 발급할 수 있다. 그러나, 그러한 검증 기술들은 시간 및 자원이 광범위한 활동일 수 있다. 따라서, 이러한 디지털 인증서들을 획득하는 데 요구되는 비용 및 시간이 상당할 수 있기 때문에, 다수의 디지털 인증서에 대한 요청들은 바람직하지 않을 수 있다.

도면의 간단한 설명

[0004] 본 발명에 따른 다양한 실시예는 다음 첨부 도면들을 참조하여 설명될 것이다:

도 1은 다양한 실시예가 구현될 수 있는 환경의 예시적인 예를 도시한다;

도 2는 적어도 하나의 실시예에 따라 인증 기관 서비스의 다양한 구성요소가 고객에게 장기 디지털 인증서들 및 단기 디지털 인증서들을 발급하도록 총괄하여 구성된 환경의 예시적인 예를 도시한다;

도 3은 적어도 하나의 실시예에 따라 인증 기관 서비스가 유효한 장기 디지털 인증서의 수신 시 고객에게 단기 디지털 인증서를 발급하는 환경의 예시적인 예를 도시한다;

도 4는 적어도 하나의 실시예에 따라 사용자 클라이언트가 고객 서버로부터 수신된 장기 디지털 인증서를 거부하는 환경의 예시적인 예를 도시한다;

도 5는 적어도 하나의 실시예에 따라 사용자 클라이언트가 고객 서버를 인증하기 위해 고객 서버로부터 수신된 단기 디지털 인증서를 이용할 수 있는 환경의 예시적인 예를 도시한다;

도 6은 적어도 하나의 실시예에 따라 장기 디지털 인증서들 및 단기 디지털 인증서들을 수신하기 위한 프로세스의 예시적인 예를 도시한다;

도 7은 적어도 하나의 실시예에 따라 장기 디지털 인증서의 발급에 대한 고객 요청에 응답하여 장기 디지털 인증서를 생성하고 발급하기 위한 프로세스의 예시적인 예를 도시한다;

도 8은 적어도 하나의 실시예에 따라 고객 요청에 응답하여 고객을 인증하고 하나 이상의 단기 디지털 인증서를 발급하기 위해 장기 디지털 인증서를 이용하기 위한 프로세스의 예시적인 예를 도시한다;

도 9는 적어도 하나의 실시예에 따라 고객 서버를 인증하기 위해 디지털 인증서를 이용하기 위한 프로세스의 예시적인 예를 도시한다; 그리고

도 10은 다양한 실시예가 구현될 수 있는 환경의 예시적인 예를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0005] 다음 설명에서, 다양한 실시예가 설명될 것이다. 설명의 목적들로, 실시예들에 대한 충분한 이해를 제공하기 위해 구체적인 구성들 및 세부사항이 제시된다. 그러나, 또한 해당 기술분야의 통상의 기술자에게 실시예들이 구체적인 세부사항들 없이 실시될 수 있다는 것이 분명할 것이다. 뿐만 아니라, 주지의 특징들은 설명되는 실시예가 모호하지 않게 하기 위해 생략 또는 간략화될 수 있다.

[0006] 본 출원에 설명되고 제안된 기술들은 서버 인증을 위해 단기 디지털 인증서들을 요청 및 획득하기 위해 이용될 수 있는 장기 인증서의 발급에 관한 것이다. 실시예에서, 엔티티(예를 들어, 조직의 컴퓨팅 디바이스)는 장기 디지털 인증서의 발급을 요청하기 위해, 이를테면 인증 기관 서비스에 대한 하나 이상의 응용 프로그램 인터페이스(API) 호를 통해, 인증 기관 서비스와 통신한다. 엔티티는 인증 기관 서비스의 고객과 연관될 수 있으며, 이는 이들 다양한 고객이 다른 엔티티들과의 보안 통신을 설정할 수 있게 하기 위해 그리고 이들 다른 엔티티가 발급된 디지털 인증서들을 사용하여 이들 다양한 고객을 인증하는 것을 가능하게 하기 위해 다양한 고객에게 디지털 인증서들을 발급하도록 구성될 수 있다. 장기 디지털 인증서는 긴 검증 주기(예를 들어, 1년 이상)를 갖게 발급될 수 있고 중요한 것으로 표시될 수 있는 확장을 포함할 수 있다. 이러한 중요 확장은 사용자 클라이언트들(예를 들어, 사용자 컴퓨팅 디바이스 상에 설치된 브라우저 애플리케이션들)이 중요 확장을 인식하도록 구성되지 않을 수 있거나 이러한 중요 확장을 거부하도록 구성됨에 따라, 이러한 사용자 클라이언트들이 이러한 장기 디지털 인증서를 채택할 수 없도록 만들 수 있다.

[0007] 인증 기관 서비스가 엔티티를 검증하여 장기 디지털 인증서가 해당 엔티티에 발급될 수 있음을 보장하면, 인증 기관 서비스는 엔티티 또는 엔티티의 서버들에 이러한 장기 디지털 인증서를 발급할 수 있다. 장기 디지털 인증서의 수신 시, 엔티티는 사용자 클라이언트와의 보안 통신 채널을 설정하기 위해 이용될 수 있는 단기 디지털 인증서들을 요청할 수 있다. 예를 들어, 실시예에서, 인증 기관 서비스는 엔티티로부터, 장기 디지털 인증서 및 단기 디지털 인증서의 발급에 대한 요청을 수신한다. 인증 기관 서비스는 엔티티를 인증하기 위해 장기 디지털 인증서 내에 지정된 정보를 확인할 수 있고, 검증 시, 단기 디지털 인증서를 엔티티에 발급할 수 있다. 단기 디지털 인증서는 장기 디지털 인증서에 관하여 보다 짧은 유효 기간을 가질 수 있다(예를 들어, 수 일, 수 개월 등). 나아가, 인증 기관 서비스는 장기 디지털 인증서의 남아 있는 유효 기간에 기초하여 단기 디지털 인증서 유효 기간을 결정한다. 예를 들어, 장기 디지털 인증서에 대해 남아 있는 유효 기간이 3개월인 경우, 인증 기관 서비스는 3개월을 초과하지 않는 유효 기간을 갖는 단기 디지털 인증서를 발급할 수 있다.

[0008] 실시예에서, 엔티티가 인증 기관 서비스로부터 단기 디지털 인증서를 획득하면, 엔티티는 보안 통신 채널을 설정하기 위해 이 단기 디지털 인증서를 사용자 클라이언트에 제공할 수 있다. 사용자 클라이언트는 단기 디지털 인증서의 수신 시, 단기 디지털 인증서의 평가를 통해 엔티티의 식별 정보를 확인할 수 있고, 인증 기관 서비스로부터 획득된 공개 암호화 키를 통해 단기 디지털 인증서 내에 포함된 디지털 서명을 확인할 수 있다. 이는 사용자 클라이언트가 단기 디지털 인증서가 인증 기관 서비스에 의해 발급되었고 그에 따라 유효함을 확인하게 할 수 있다. 이러한 단기 디지털 인증서를 이용하여, 사용자 클라이언트는 엔티티의 공개 암호화 키를 획득하고 데이터를 암호화하고 보안 통신 채널을 통해 엔티티에 송신기 위해 이러한 공개 암호화 키를 이용할 수 있다.

[0009] 이러한 방식으로, 엔티티는 광범위한 검증 프로세스들이 각 단기 디지털 인증서의 발급 이전에 수행될 필요 없이 이전에 발급된 장기 디지털 인증서에 기초하여 인증 기관 서비스로부터 다수의 단기 디지털 인증서를 획득할

수 있을 수 있다. 덧붙여, 본 출원에 설명되고 제안된 기술들은 추가 기술적 이점들을 가능하게 한다. 예를 들어, 몇몇 실시예에서, 장기 디지털 인증서가 인식 불가능하고/거나 사용자 클라이언트가 장기 디지털 인증서를 거부하게 하는 확장을 포함하기 때문에, 엔티티는 장기 디지털 인증서가 손상될 경우 더 이상 새로운 장기 디지털 인증서의 발급을 취소 및 요청하도록 요구되지 않을 수 있다. 나아가, 단기 디지털 인증서가 손상되는 경우, 엔티티는 이러한 단기 디지털 인증서를 취소할 수 있고 전체 검증 프로세스를 한 번 더 거치지 않고도 인증 기관 서비스로부터 새로운 단기 디지털 인증서를 획득하기 위해 발급된 장기 디지털 인증서를 이용할 수 있다.

[0010] 도 1은 다양한 실시예가 구현될 수 있는 환경(100)의 예시적인 예를 도시한다; 환경(100)에서, 인증 기관 서비스(102)는 인증 기관 서비스(102)의 고객들이 하나 이상의 디지털 인증서의 발급을 요청하게 하는 인증 기관 시스템을 제공할 수 있으며, 이는 고객(디지털 인증서 내에서 식별될 때, 지명된 주체)의 공개 암호화 키의 소유를 증명할 수 있다. 이러한 하나 이상의 디지털 인증서는 다른 엔티티, 이를테면 사용자 클라이언트(106)(예를 들어, 브라우저 애플리케이션)가 고객의 식별 정보를 확인하는 것을 가능하게 할 수 있고, 고객과의 보안 통신 채널을 설정할 수 있으며, 이에 의해 암호화된 데이터의 송신 및 비-암호화된 데이터의 송신이 이루어질 수 있다. 실시예에서, 인증 기관 서비스(102)는 고객으로부터, 장기 디지털 인증서가 계속해서 유효인 한 나중에 단기 디지털 인증서의 발급을 위해 이용될 수 있는 장기 디지털 인증서에 대한 요청을 수신한다.

[0011] 인증 기관 서비스(102)는 고객으로부터 장기 인증서의 발급에 대한 요청을 수신 시, 고객이 인증 기관 서비스(102)로부터 신뢰될 수 있고 인증 기관 서비스(102)로부터 디지털 인증서를 획득하기 위해 인증됨을 보장하기 위해 하나 이상의 검증 프로세스를 수행할 수 있다. 예를 들어, 인증 기관 서비스(102)는 고객을 평가하고, 고객이 그것이 표방하는 것임을, 그리고 고객이 디지털 인증에 대해 정당하게 조사되었음을 보장하기 위해 하나 이상의 정부 관계 기관, 제3자 데이터베이스 또는 임의의 다른 신뢰 정보 저장소에 액세스할 수 있다. 고객이 인증 기관 서비스(102)에 의해 정당하게 조사된 경우, 인증 기관 서비스(102)는 보다 짧은 기간의 단기 디지털 인증서들을 획득하는 데 사용하기 위한 장기 디지털 인증서를 고객에게 발급할 수 있다. 장기 디지털 인증서는, 몇몇 실시예에서, X.509 인증서이며, 이는 디지털 인증서의 발급자, 인증서에 대한 유효 기간, 주체(예를 들어, 고객), 주체의 공개 암호화 키, 및 인증 기관 서비스(102)의 디지털 서명을 지정할 수 있다. 그러나, 이러한 장기 디지털 인증서는 장기 디지털 인증서가 단지 검증 목적들만을 위해 이용될 것임을 나타낼 수 있는 중요 확장을 더 지정할 수 있다. 이러한 중요 확장은 일부 사용자 클라이언트(106)에 의해서는 인식되지 않을 수 있고, 그 결과, 이러한 사용자 클라이언트들(106)에 의해 자동으로 거부될 수 있다. 대안적으로, 사용자 클라이언트들(106)은 이러한 중요 확장을 포함하는 임의의 디지털 인증서들을 거부하도록 구성될 수 있다.

[0012] 고객이 인증 기관 서비스(102)로부터 이러한 장기 디지털 인증서를 수신하면, 고객은 하나 이상의 고객 서버(104)를 통해 사용자 클라이언트(106)와의 보안 통신 채널을 설정하고 사용자 클라이언트(106)가 고객 서버(104)를 인증하게 하기 위해 사용가능한 하나 이상의 단기 디지털 인증서를 획득하기 위한 요청을 인증 기관 서비스(102)에 제출할 수 있다. 인증 기관 서비스(102)에 대한 요청은 앞서 언급한 장기 디지털 인증서를 포함할 수 있다. 하나 이상의 고객 서버(104)로부터의 요청을 수신 시, 인증 기관 서비스(102)는 고객의 식별 정보를 확인하고 장기 디지털 인증서가 여전히 유효함을 보장하기 위해 장기 디지털 인증서를 평가할 수 있다. 실시예에서, 요청은 인증 기관 서비스(102)가 그것이 장기 디지털 인증서를 초기에 발급한 동일한 엔티티에 하나 이상의 단기 디지털 인증서를 발급하고 있음을 인증 기관 서비스(102)에 보장하기 위해 장기 디지털 인증서 내에 지정된 공개 암호화 키에 대응하는 고객의 비밀 암호화 키를 사용하여 디지털 방식으로 서명될 수 있다. 인증 기관 서비스(102)는 디지털 서명을 확인하기 위해 장기 디지털 인증서의 공개 암호화 키를 사용할 수 있다.

[0013] 인증 기관 서비스(102)는 요청을 제공한 고객의 식별 정보를 확인 시, 이러한 디지털 인증서에 대한 남아 있는 유효 기간을 결정하기 위해 장기 디지털 인증서를 평가할 수 있다. 인증 기관 서비스(102)는 이러한 정보를 하나 이상의 단기 디지털 인증서 내에 지정될 수 있는 유효 기간을 설정하기 위해 이용할 수 있다. 예를 들어, 장기 디지털 인증서에 대해 남아 있는 유효 기간이 3개월인 경우, 인증 기관 서비스(102)는 장기 디지털 인증서에 정의된 남아 있는 3개월의 기간을 초과하지 않는 유효 기간을 갖는 단기 디지털 인증서를 발급할 수 있다. 대안적으로, 고객은 요청을 통해, 원하는 유효 기간이 제공된 장기 디지털 인증서의 남아 있는 유효 기간을 초과하지 않는 한, 단기 디지털 인증서에 대해 원하는 유효 기간을 지정할 수 있다.

[0014] 인증 기관 서비스(102)는 내에 장기 디지털 인증서 내에 지정된 동일한 공개 암호화 키를 포함하기 위한 단기 디지털 인증서를 생성할 수 있다. 이는 단기 디지털 인증서가 장기 디지털 인증서에 대한 프록시로서의 역할을 하게 할 수 있고, 사용자 클라이언트(106) 또는 다른 엔티티에 대한 액세스를 가능하게 할 수 있다. 예를 들어, 장기 디지털 인증서는 물리적 구현, 이를테면 스마트 카드, 뱃지 또는 그것 내에 장기 디지털 인증서를 저장할 수 있는 다른 디바이스를 통해 고객에게 발급될 수 있다. 고객은 스마트 카드, 뱃지 또는 다른 디바이스를 원격

위치의 컴퓨팅 디바이스를 통해 인증 기관 서비스(102)에 제시할 수 있다. 스마트 카드 또는 다른 디바이스 내 장기 디지털 인증서의 분석에 적어도 부분적으로 기초하여, 고객은 보다 짧은 시간 기간 동안 유효할 수 있는 단기 디지털 인증서를 발급받을 수 있다. 이는 고객이, 원격 위치에서 단지 그/그녀의 시간 동안 유효할 수 있는 이 새롭게 발급된 단기 디지털 인증서를 이용하여 이 원격 위치에 액세스하게 할 수 있다. 대안적인 실시예에서, 단기 디지털 인증서는 장기 디지털 인증서 내에 지정된 것과 상이한 고객 암호화 키를 더 지정할 수 있다. 이는 손상된 경우 장기 디지털 인증서 내에 지정된 고객 암호화 키를 노출하지 않고도 단기 디지털 인증서를 취소하게 할 수 있다.

[0015] 고객이 하나 이상의 고객 서버(104)를 통해, 인증 기관 서비스(102)로부터 하나 이상의 단기 디지털 인증서를 수신하면, 고객 서버들(104)은 이제 데이터를 수신된 하나 이상의 단기 디지털 인증서와 함께 하나 이상의 사용자 클라이언트(106)에 송신할 수 있다. 사용자 클라이언트(106)는 인증 기관 서비스(102)로부터, 하나 이상의 단기 디지털 인증서 내에 지정된 인증 기관 서비스(102)의 디지털 서명을 확인하기 위해 사용될 수 있는 암호화 키 쌍의 공개 암호화 키를 획득할 수 있다. 인증 기관 서비스(102)의 디지털 서명이 인증된 것으로 확인되는 경우, 사용자 클라이언트(106)는 하나 이상의 단기 디지털 인증서가 유효함을 결정할 수 있고 그에 따라 이들을 하나 이상의 고객 서버(104)의 식별 정보를 확인하기 위해 사용할 수 있으며, 확인되는 경우, 단기 디지털 인증서들 내에 지정된 고객의 공개 암호화 키를 이용할 수 있다. 예를 들어, 고객 서버들(104)이 디지털로 서명된 (예를 들어, 고객의 비밀 암호화 키를 이용) 데이터를 사용자 클라이언트(106)에 송신하기 위해 이용되는 경우, 사용자 클라이언트(106)는 고객의 디지털 서명을 확인하고 송신된 데이터가 유효한지 여부를 결정하기 위해 단기 디지털 인증서 내에 지정된 고객의 공개 암호화 키를 이용할 수 있다. 이렇게 하여, 사용자 클라이언트(106)는 고객 서버들(104)에 정보를 안전하게 송신하기 위해 이용될 수 있다.

[0016] 위에서 언급된 바와 같이, 고객은 단기 디지털 인증서들을 획득하는 데 있어서 검증 목적들을 위해 이용될 수 있는 장기 디지털 인증서의 발급을 요청하기 위해 인증 기관 서비스와 통신할 수 있다. 나아가, 고객은 하나 이상의 고객 서버를 통해, 인증 기관 서비스로부터의 이러한 단기 디지털 인증서들을 요청할 수 있으며, 이것들은 그 다음 사용자 클라이언트들이 하나 이상의 고객 서버를 인증하게 하기 위해 사용될 수 있다. 이러한 단기 디지털 인증서들에 대한 요청은, 인증 기관 서비스가 고객을 인증하기 위해 이용할 수 있는 장기 디지털 인증서를 포함할 수 있다. 따라서, 도 2는 적어도 하나의 실시예에 따라 인증 기관 서비스(202)의 다양한 구성요소가 고객(212)에게 장기 디지털 인증서들 및 단기 디지털 인증서들을 발급하도록 총괄하여 구성된 환경(200)의 예시적인 예를 도시한다.

[0017] 인증 기관 서비스(202)는 고객들(212)이 인증 기관 서비스(202)에 액세스하게 할 수 있는 인터페이스(204)를 이들 고객(212)에 제공할 수 있다. 고객(212)은 하나 이상의 통신 네트워크, 이를테면 인터넷을 통해 인터페이스(204)를 이용할 수 있다. 인터페이스(204)는 고객(212)이 인증 기관 서비스(202)에 액세스하기 위한 인가를 가짐을 보장하기 위해 특정 보안 조치를 포함할 수 있다. 예를 들어, 인증 기관 서비스(202)에 액세스하기 위해, 고객은 인터페이스(204)를 사용할 때 사용자 이름 및 대응하는 비밀번호 또는 암호 키를 제공해야 할 수 있다. 추가적으로, 인터페이스(204)에 제출된 요청들(예를 들어, API 호출들)은 전자 서명이 인증 기관 서비스(202)에 의해, 이를테면 인증 시스템(미도시)에 의해 확인가능하도록 암호화 키를 사용하여 생성된 전자 서명을 필요로 할 수 있다.

[0018] 인터페이스(204)를 통해, 고객(212)은 하나 이상의 고객(212) 서버에 장기 디지털 인증서의 발급에 대한 요청을 제출할 수 있을 수 있다. 위에서 언급된 바와 같이, 장기 디지털 인증서는 나중에, 인증 기관 서비스(202)가 고객(212)을 인증하게 하고 단기 디지털 인증서들을 고객(212) 서버들에 발급하기 위해 이용될 수 있다. 장기 디지털 인증서의 발급에 대한 요청은 고객(212)에 관한 정보, 이를테면 고객(212)의 이름, 주소, 소득 정보 기타 같은 종류의 것을 포함할 수 있다. 나아가, 인터페이스(204)를 통해, 고객(212)은, 그 다음 장기 디지털 인증서 내에 지정될 수 있는 장기 디지털 인증서에 대한 유효 기간을 지정하도록 허용될 수 있다.

[0019] 인증 기관 서비스(202)가 장기 디지털 인증서의 발급에 대한 고객(212)의 요청을 수신하면, 인터페이스(204)는, 요청을 프로세싱하고 고객(212)이 장기 디지털 인증서를 발급받을 수 있는지 여부를 결정하도록 구성될 수 있는 관리 서브-시스템(206)에 요청을 송신할 수 있다. 예를 들어, 관리 서브-시스템(206)은 요청과 함께 제공된 고객(212) 정보에 적어도 부분적으로 기초하여, 고객(212)이 장기 디지털 인증서를 발급받을 수 있는지 여부를 결정하기 위해 정부 관계 기관 데이터베이스들 및 다른 제3자 데이터베이스들에 액세스하도록 구성될 수 있다. 예를 들어, 관리 서브-시스템(206)은 제3자 데이터베이스 내에 명시된 정보에 적어도 부분적으로 기초하여, 고객(212)이 신뢰될 수 없다고 결정하는 경우, 관리 서브-시스템(206)은 장기 디지털 인증서에 대한 고객(212)의 요청을 거부할 수 있다. 관리 서브-시스템(206)이 고객(212)이 장기 디지털 인증서를 발급받을 수 있다고 결정하

는 경우, 관리 서브-시스템(206)은 고객 프로필 저장소(210) 내에 고객(212)의 정보를 저장할 수 있다. 나아가, 관리 서브-시스템(206)은 장기 디지털 인증서를 생성하기 위해 이용될 수 있는 인증서 템플릿을 획득하기 위해 인증서 데이터 저장소(208)에 액세스할 수 있다. 예를 들어, 관리 서브-시스템(206)은 인증서 데이터 저장소(208)로부터 X.509 디지털 인증서 템플릿을 획득할 수 있고 이러한 템플릿을 고객(212)에 대한 장기 X.509 디지털 인증서를 생성하기 위해 이용할 수 있다. 관리 서브-시스템(206)은 인터페이스(204)를 통해, 새롭게 생성된 장기 디지털 인증서를 고객(212)에게 제공할 수 있다.

[0020] 실시예에서, 관리 서브-시스템(206)은 장기 디지털 인증서 내에, 사용자 클라이언트에 의해 인식가능하지 않을 수 있거나 사용자 클라이언트에 의해 거부될 수 있는 중요 확장을 지정한다. 예를 들어, 중요 확장은 "검증-전용" 확장일 수 있으며 이는 디지털 인증서가 고객(212)을 인증하기 위해서는 이용되지 않을 수 있음을 사용자 클라이언트에 시그널링할 수 있다. 이러한 중요 확장은 고객(212)을 인증하기 위해 수행되는 하나 이상의 검증에 대한 정보, 이를테면 검증이 수행된 날짜, 고객(212) 검증을 위해 사용된 표준들 또는 요건들, 및/또는 검증이 수행된 인증 기관 서비스(202)의 고객(212)의 식별자를 포함할 수 있다.

[0021] 나중에, 고객(212)은 하나 이상의 고객(212) 서버를 통해, 사용자 클라이언트와의 보안 통신 채널을 설정하고 사용자 클라이언트가 고객(212)를 인증하게 하기 위해 사용될 수 있는 하나 이상의 단기 디지털 인증서의 생성을 요청하기 위해 다시 인터페이스(204)에 액세스할 수 있다. 요청은 고객(212)에게 이전에 발급된 장기 디지털 인증서를 포함할 수 있다. 나아가, 몇몇 실시예에서, 요청은, 원래 장기 디지털 인증서 내에 지정된 공개 암호화 키에 대응할 수 있는 고객(212)의 비밀 암호화 키를 사용하여 고객(212)에 의해 디지털 방식으로 서명될 수 있다. 요청의 수신 시, 관리 서브-시스템(206)은 장기 디지털 인증서에 대한 남아 있는 유효 기간을 결정하기 위해 장기 디지털 인증서를 평가할 수 있다. 예를 들어, 장기 디지털 인증서는 장기 디지털 인증서에 대한 시작 날짜 및 만료 날짜를 지정하는 유효 기간 필드를 포함할 수 있다. 지정된 만료 날짜에 적어도 부분적으로 기초하여, 관리 서브-시스템(206)은 장기 디지털 인증서에 대한 남아 있는 유효 기간을 계산할 수 있을 수 있다.

[0022] 추가적으로, 요청이 고객(212)에 의해 디지털 방식으로 서명된 경우, 관리 서브-시스템(206)은 요청과 함께 포함된 디지털 서명을 확인하고 수신된 요청이 유효함을 보장하기 위해 사용될 수 있는 이러한 특정 고객(212)에 대응하는 암호화 키를 획득하기 위해 고객 프로필 저장소(210)에 액세스할 수 있다. 관리 서브-시스템(206)이 장기 디지털 인증서 내에 지정된 정보에 적어도 부분적으로 기초하여, 고객(212)이 그것이 주장하는 것이라고 결정하는 경우, 관리 서브-시스템(206)은 요청된 하나 이상의 단기 디지털 인증서를 생성하기 위해 사용될 수 있는 디지털 인증서 템플릿을 획득하기 위해 인증서 데이터 저장소(208)에 액세스할 수 있다. 하나 이상의 단기 디지털 인증서는 지정된 특정 정보를 제외하고는 장기 디지털 인증서와 유사할 수 있다. 예를 들어, 단기 디지털 인증서는 장기 디지털 인증서에 대해 남아 있는 유효 기간 이하인 유효 기간을 지정할 수 있다. 예를 들어, 장기 디지털 인증서에 대해 남아 있는 유효 기간이 3개월인 경우, 관리 서브-시스템(206)은 단기 디지털 인증서 내에, 단기 디지털 인증서에 대한 유효 기간이 3개월 이하의 임의의 값임을 지정할 수 있다. 그에 따라 단기 디지털 인증서에 대한 만료 날짜는 장기 디지털 인증서의 만료 날짜와 일치하거나 장기 디지털 인증서의 만료 날짜보다 빠를 수 있다.

[0023] 나아가, 단기 디지털 인증서는 장기 디지털 인증서 내에 지정된 중요 확장을 포함하지 않을 수 있다. 이는 사용자 클라이언트들이 고객(212)을 인증하기 위해 단기 디지털 인증서를 이용하게 하고 사용자 클라이언트들이 고객(212)과 안전하게 통신하게 할 수 있다. 몇몇 실시예에서, 관리 서브-시스템(206)은 원래의, 장기 디지털 인증서 내에 지정된 암호화 키에 대안적인 고객(212) 암호화 키를 지정하는 단기 디지털 인증서를 생성할 수 있다. 이는 장기 디지털 인증서 및, 그에 따라, 원래 고객(212) 암호화 키가 단기 디지털 인증서 위반의 결과로서 손상될 수 있는 가능성을 감소시키는 것을 도울 수 있다.

[0024] 관리 서브-시스템(206)이 고객(212) 요청에 응답하여 하나 이상의 단기 디지털 인증서를 생성하면, 관리 서브-시스템(206)은 발급된 단기 디지털 인증서들의 수, 대응하는 고객(212) 암호화 키들, 및 나중에 고객(212)을 대신하여 디지털 인증서들을 생성하는 데 유용할 수 있는 임의의 다른 정보를 지정하기 위해 고객 프로필 저장소(210) 내 고객(212)의 프로필에 액세스할 수 있다. 관리 서브-시스템(206)은 인터페이스(204)를 통해, 사용자 클라이언트들이 고객(212)을 인증하고 데이터를 보안 통신 채널을 통해 안전하게 고객(212)에게 송신하게 하기 위해 이러한 사용자 클라이언트들에 이러한 단기 디지털 인증서들을 제공할 수 있는 고객(212)에게 이러한 단기 디지털 인증서들을 발급할 수 있다. 나아가, 이러한 단기 디지털 인증서들은 고객(212)이 그/그녀의 데이터에 디지털로 서명하고 사용자 클라이언트들에 송신되어야 할 데이터를 암호화하게 할 수 있다.

[0025] 위에서 언급된 바와 같이, 고객은 사용자 클라이언트들이 고객을 인증하기 위해 단기 디지털 인증서들을 이용할

수 있도록 이러한 사용자 클라이언트에 송신될 수 있는 하나 이상의 단기 디지털 인증서를 획득하기 위해 이전에 발급된 장기 디지털 인증서를 포함한 요청을 인증 기관 서비스에 송신할 수 있다. 따라서, 도 3은 적어도 하나의 실시예에 따라 인증 기관 서비스(304)가 유효한 장기 디지털 인증서(306)의 수신 시 고객(302)에게 단기 디지털 인증서(308)를 발급하는 환경(300)의 예시적인 예를 도시한다. 환경(300)에서, 고객(302)은 하나 이상의 단기 디지털 인증서(308)의 발급을 위한 인증 기관 서비스(304)에 대한 요청의 부분으로서, 인증 기관 서비스(304)에 의해 고객(302)에게 이전에 발급된 장기 디지털 인증서(306)를 제공할 수 있다. 위에서 언급된 바와 같이, 장기 디지털 인증서(306)는 유효 기간을 지정할 수 있는, 이는 시작 날짜(예를 들어, 도 3에 예시된 "이후" 필드) 및 만료 날짜(예를 들어, 도 3에 예시된 "이전" 필드)를 포함할 수 있다. 이러한 유효 기간은 장기 디지털 인증서(306)가 유효한 지속 기간을 정의할 수 있다. 나아가, 이러한 유효 기간은 인증 기관 서비스(304)이 장기 디지털 인증서(306)에 대한 남아 있는 유효 기간을 결정하게 할 수 있다. 예를 들어, 인증 기관 서비스(304)는 장기 디지털 인증서(306)에 대해 남아 있는 유효 기간을 계산하기 위해 만료 날짜 및 현재 날짜 및 시간을 이용할 수 있다.

[0026] 장기 디지털 인증서(306)는 또한 중요 확장을 포함할 수 있으며 이는 사용자 클라이언트들이 고객(302)을 인증하기 위해 장기 디지털 인증서(306)를 사용할 수 없도록 만들기 위해 이용될 수 있다. 예를 들어, 도 3에 예시된 바와 같이, 장기 디지털 인증서(306)는 식별자 "검증-전용 유형 - 1.01."을 갖는 확장을 지정할 수 있다. 이러한 특정 확장은 중요한 것으로 표시되어, 사용자 클라이언트(404)가 중요 확장을 인식하지 않는 경우 그것은 장기 디지털 인증서(306)를 거부해야 함을 의미할 수 있다. 나아가, 사용자 클라이언트들이 이러한 중요 확장을 인식하도록 업데이트될 때, 사용자 클라이언트들은 이러한 중요 확장을 포함하는 어떤 장기 디지털 인증서(306)도 수용하지 않도록 구성될 수 있다. 이렇게 하여, 고객(302)은 단순히 이러한 장기 디지털 인증서(306) 이용하여 그것의 식별 정보를 사용자 클라이언트에 주장할 수 없을 수 있다.

[0027] 위에서 언급된 바와 같이, 고객(302)이 하나 이상의 단기 디지털 인증서(308)를 획득하기 위한 요청을 인증 기관 서비스(304)에 제출할 때, 고객(302)은 이전에 발급된 장기 디지털 인증서(306)를 인증 기관 서비스(304)에 제공할 수 있다. 인증 기관 서비스(304)는 장기 디지털 인증서(306)가 여전히 유효함을 보장하기 위해 장기 디지털 인증서(306)를 평가할 수 있다. 나아가, 인증 기관 서비스(304)는 고객(302)이 그것이 주장하는 것임을 확인하기 위해 하나 이상의 주체 필드(미제시)를 평가할 수 있다. 예를 들어, 하나 이상의 주체 필드는 고객(302)의 소정의 성 및 이름, 고객(302)의 단체 이름 및/또는 부서, 단체가 위치될 수 있는 나라, 구, 및 주, 고객(302) 또는 다른 엔티티에 대한 속칭(예를 들어, URL) 기타 같은 종류의 것을 지정할 수 있다. 실시예에서, 고객(302)은 단기 디지털 인증서들(308)이 장기 디지털 인증서(306)를 발급한 동일한 고객(302)에 발급될 것임을 인증 기관 서비스(304)에 보장하기 위해 인증 기관 서비스(304)에 대한 요청에 디지털로 서명하기 위해 장기 디지털 인증서(306) 내에 포함된 암호화 키를 이용한다.

[0028] 인증 기관 서비스(304)가 장기 디지털 인증서(306)를 사용하여 고객(302)을 인증하면, 인증 기관 서비스(304)는 하나 이상의 단기 디지털 인증서(308)를 생성하고 그것들을 고객(302)에게 발급할 수 있다. 하나 이상의 단기 디지털 인증서(308)는 몇몇 대안적인 엔트리를 제외하고는 장기 디지털 인증서(306)와 유사할 수 있다. 예를 들어, 도 3에 예시된 바와 같이, 단기 디지털 인증서(308)에 대한 유효 기간은 장기 디지털 인증서(306) 내에 지정된 유효 기간보다 짧다. 예를 들어, 인증 기관 서비스(304)는 단기 디지털 인증서(308)가 생성된 날짜와 동일한 시작 날짜를 지정할 수 있다. 대안적으로, 단기 디지털 인증서(308)에 대한 시작 날짜는 장기 디지털 인증서(306) 내에 지정된 만료 날짜 이전 그리고 단기 디지털 인증서(308)가 고객(302)에 발급된 날짜에서 차후 날짜로서 정의될 수 있다.

[0029] 실시예에서, 단기 디지털 인증서(308)는 장기 디지털 인증서(306)의 동일한 주체 필드 내에 지정된 고객(302) 또는 다른 엔티티에 특유한 적어도 하나의 주체 필드를 포함하도록 생성된다. 예를 들어, 단기 디지털 인증서(308)는 장기 디지털 인증서(306) 내에 지정된 것들과동일한 단체 이름, 단체 장소(예를 들어, 나라, 구, 주), 및 속칭(예를 들어, URL)을 지정할 수 있다. 몇몇 실시예에서, 단기 디지털 인증서(308)는 장기 디지털 인증서(306) 내에 지정되지 않은 추가 주체 필드들을 더 포함할 수 있다. 예를 들어, 단기 디지털 인증서(308)는 이러한 추가 주체 필드들 중 하나 이상을 통해, 단기 디지털 인증서(308)가 생성된 고객(302)과 연관된 위임 엔티티의 식별 정보를 지정할 수 있다. 추가적으로, 단기 디지털 인증서(308) 내에 포함된 하나 이상의 추가 주체 필드는 단기 디지털 인증서(308)가 이용될 수 있는 제2 위치(예를 들어, 나라, 구, 주)를 지정할 수 있다.

[0030] 단기 디지털 인증서(308)의 만료 날짜는 장기 디지털 인증서(306) 및/또는 고객(302) 요청 내에 지정된 만료 날짜에 적어도 부분적으로 기초하여 인증 기관 서비스(304)에 의해 정의될 수 있다. 예를 들어, 도 3에 예시된 바와 같이, 단기 디지털 인증서(308) 내에 지정된 만료 날짜는 장기 디지털 인증서(306) 내에 지정된 만료 날짜보

다 빠르다. 단기 디지털 인증서(308)에 대한 유효 기간은 단기 디지털 인증서(308)에 대한 유효 기간이 장기 디지털 인증서(306)에 대해 남아 있는 유효 기간을 초과하지 않는 한, 요청을 통해 고객(302)에 의해 또는 인증 기관 서비스(304)에 의해 정의될 수 있다.

[0031] 단기 디지털 인증서(308)는 사용자 클라이언트들이 디지털 인증서를 사용할 수 없도록 만드는 장기 디지털 인증서(306) 내에 포함된 중요 확장을 포함하지 않을 수 있다. 예를 들어, 도 3에 예시된 바와 같이, 단기 디지털 인증서(308)는 확장 "검증-전용 유형 - 1.01."을 포함하지 않는다. 대신, 단기 디지털 인증서(308) 내에 지정된 확장은 사용자 클라이언트들이 고객(302)을 인증하기 위해 그리고 다른 목적들로(예를 들어, 날짜 검증, 날짜 해독 등) 단기 디지털 인증서(308)를 이용하게 할 수 있다. 단기 디지털 인증서(308)가 만료될 때, 고객(302)은 새로운 단기 디지털 인증서(306)를 획득하기 위한 요청을 장기 디지털 인증서(306)와 함께 인증 기관 서비스(304)에 다시 제출할 수 있다.

[0032] 위에서 언급된 바와 같이, 인증 기관 서비스에 의해 고객에게 발급된 장기 디지털 인증서는 고객의 그/그녀의 식별 정보 주장의 인증을 확인하기 위해 이용되지 않을 수 있다. 예를 들어, 장기 디지털 인증서는 하나 이상의 사용자 클라이언트에 의해 인식되지 않을 수 있는 중요 확장을 포함할 수 있고, 이러한 하나 이상의 사용자 클라이언트에게 장기 디지털 인증서가 고객 인증을 위해 수용되지 않을 수 있음을 나타낼 수 있다. 따라서, 도 4는 적어도 하나의 실시예에 따라 사용자 클라이언트(404)가 고객 서버(402)로부터 수신된 장기 디지털 인증서(406)를 거부하는 환경(400)의 예시적인 예를 도시한다.

[0033] 장기 디지털 인증서(406)는 정기적인 디지털 인증서들에 포함된 유사한 필드들 중 많은 필드를 포함할 수 있다. 예를 들어, 장기 디지털 인증서(406)는 인증서에 대한 유효 기간, 장기 디지털 인증서(406)가 발급된 고객, 고객 암호화 키, 및 인증 기관 서비스 디지털 서명을 지정할 수 있으며, 이것들은 장기 디지털 인증서(406)가 유효함을 확인하기 위해 사용될 수 있다. 그러나, 장기 디지털 인증서(406)는 장기 디지털 인증서(406)가 단지 검증을 위한 것임을 지정하기 위해 이용될 수 있는 하나 이상의 중요 확장을 포함할 수 있다. 예를 들어, 도 4에 예시된 바와 같이, 장기 디지털 인증서(406)는 식별자 "검증-전용 유형 - 1.01."을 갖는 확장을 지정할 수 있다. 이러한 특정 확장은 중요한 것으로 표시되어, 사용자 클라이언트가 중요 확장을 인식하지 않는 경우 그것은 장기 디지털 인증서(406)를 거부해야 함을 의미할 수 있다. 나아가, 사용자 클라이언트들(404)이 이러한 중요 확장을 인식하도록 업데이트될 때, 사용자 클라이언트들(404)은 이러한 중요 확장을 포함하는 어떤 장기 디지털 인증서(406)도 수용하지 않도록 구성될 수 있다.

[0034] 사용자 클라이언트(404)가 이러한 장기 디지털 인증서(406)를 고객 서버(402)로부터 수신하는 경우, 사용자 클라이언트(404)는 고객 서버(402)로부터 수신된 데이터를 폐기하고 고객 서버(402)와의 통신 채널을 종료할 수 있다. 이렇게 하여, 고객은 단지 인증 기관 서비스와 함께 검증 목적들을 위해서만 장기 디지털 인증서(406)를 이용하도록 허용될 수 있다. 나아가, 이는 많은 청중에 장기 디지털 인증서(406)의 노출을 제한할 수 있고, 그렇게 함으로써 장기 디지털 인증서(406) 및 그로 인해 고객의 공개 암호화 키가 손상될 수 있는 위험을 가능성 있게 감소시킬 수 있다.

[0035] 위에서 언급된 바와 같이, 고객은 하나 이상의 고객 서버를 통해, 인증 기관 서비스로부터의 하나 이상의 단기 디지털 인증서를 요청할 수 있다. 요청은, 인증 기관 서비스가 고객을 인증하고 고객에게 발급될 하나 이상의 단기 디지털 인증서에 대한 유효 기간을 정의하기 위해 장기 디지털 인증서 내에 지정된 정보를 이용하게 할 수 있는 장기 디지털 인증서를 포함할 수 있다. 이러한 하나 이상의 단기 디지털 인증서는 고객에 의해 그/그녀의 식별 정보를 사용자 클라이언트에 주장하고 사용자 클라이언트가 고객을 인증하게 하기 위해 이용될 수 있다. 따라서, 도 5는 적어도 하나의 실시예에 따라 사용자 클라이언트(504)가 고객 서버(502)를 인증하기 위해 고객 서버(502)로부터 수신된 단기 디지털 인증서(506)를 이용할 수 있는 환경(500)의 예시적인 예를 도시한다. 사용자 클라이언트(504) 및 고객 서버(502)는 도 4에 예시된 사용자 클라이언트 및 고객 서버와 유사할 수 있다.

[0036] 환경(500)에서, 고객 서버(502)는 데이터 및 단기 디지털 인증서(506)를 사용자 클라이언트(504)에 송신할 수 있다. 사용자 클라이언트(504)는 사용자가 고객 서버(502)에 액세스하기 위해 상호작용할 수 있는 브라우저 애플리케이션일 수 있다. 사용자 클라이언트(504)가 고객 서버(502)와 통신을 시작할 때, 고객 서버(502)는 특정 데이터 및 단기 디지털 인증서(506)를 사용자 클라이언트(504)에 제공함으로써 응답할 수 있다. 단기 디지털 인증서(506)는 고객의 식별 정보, 단기 디지털 인증서(506)에 대한 유효 기간, 고객 공개 암호화 키, 및 고객 서버(502)에 단기 디지털 인증서를 발급한 인증 기관 서비스의 디지털 서명을 지정할 수 있다. 이러한 정보에 더하여, 단기 디지털 인증서(506)는, 단기 디지털 인증서(506)가 특정 목적들을 위해 이용될 수 있음을 지정하기 위해 사용될 수 있는 하나 이상의 확장을 지정할 수 있다. 예를 들어, 도 5에 예시된 바와 같이, 단기 디지털

인증서(506)는, 특정 사슬에 대한 경로 길이를 제한하기 위해 사용될 수 있는 "기초적 제약" 확장을 포함할 수 있다. 예시의 목적을 위해 본 발명 전체에 걸쳐 "기초적 제약" 확장이 광범위하게 사용되지만, 추가적인 및/또는 대안적인 확장들이 단기 디지털 인증서(506) 내에 지정될 수 있다.

[0037] 그러나, 도 4에 예시된 장기 디지털 인증서에 반해, 단기 디지털 인증서(506)는 중요 "검증-전용" 확장, 이를테면 도 4에 예시된 장기 디지털 인증서 내에 지정된 "검증_전용 유형 - 1.01" 확장을 지정하지 않을 수 있다. 이렇게 하여, 단기 디지털 인증서(506)는 사용자 클라이언트(504)에 의해 인식될 수 있고, 고객 서버(502)를 인증하기 위해, 그리고 인증 기관 서비스의 공개 암호화 키를 사용하여, 단기 디지털 인증서(506) 내에 지정된 인증 기관 서비스 디지털 서명을 검증하기 위해 사용자 클라이언트(504)가 단기 디지털 인증서(506)를 이용하게 할 수 있다. 그에 따라, 사용자 클라이언트(504)가 고객 서버(502)를 인증하고 단기 디지털 인증서(506)가 유효함을 확인할 수 있는 경우, 사용자 클라이언트(504)는 보안 통신 채널을 통해 고객 서버(502)와의 그 이상의 통신에 참여할 수 있다.

[0038] 위에서 언급된 바와 같이, 고객은 고객 및 인증 기관 서비스 간 단지 검증 목적들을 위해서만 이용될 수 있는 장기 디지털 인증서의 발급을 요청하기 위한 요청을 인증 기관 서비스에 제출할 수 있다. 나아가, 장기 디지털 인증서가 고객에게 발급되면, 고객은 고객을 인증하기 위해 사용자 클라이언트들에 의해 사용될 수 있고 고객 및 이러한 사용자 클라이언트들 간 보안 통신을 가능하게 할 수 있는 하나 이상의 단기 디지털 인증서의 발급을 위한 요청들을 인증 기관 서비스에 제출할 수 있다. 하나 이상의 단기 디지털 인증서의 발급에 대한 새로운 요청들은, 인증 기관 서비스가 고객을 인증하기 위해 그리고 단기 디지털 인증서들의 파라미터들을 정의하는 데 필요한 정보를 획득하기 위해 이용할 수 있는 앞서 언급한 장기 디지털 인증서를 포함할 수 있다. 따라서, 도 6은 적어도 하나의 실시예에 따라 장기 디지털 인증서들 및 단기 디지털 인증서들을 수신하기 위한 프로세스(600)의 예시적인 예를 도시한다. 프로세스(600)는, 고객 및 인증 기관 서비스 간 통신을 가능하게 하도록 구성될 수 있는 하나 이상의 고객 서버를 통해 고객에 의해 수행될 수 있다.

[0039] 고객이 장기 디지털 인증서를 획득하기 위해, 고객은 인증 기관 서비스가 장기 디지털 인증서를 위임받을 수 있는 신뢰할 수 있는 엔티티로서 고객을 정당하게 조사하기 위해 이용할 수 있는 특정 정보를 인증 기관 서비스에 제공하도록 요구될 수 있다. 예를 들어, 인증 기관 서비스는 고객이 신뢰될 수 있는지 여부를 결정하기 위해 정부 관계 기관, 신뢰된 제3자 데이터베이스들 및 다른 신뢰 정보 저장소들에 의해 유지되는 하나 이상의 데이터베이스에 액세스할 수 있다. 그에 따라, 고객은 장기 인증서를 획득하기 위해 하나 이상의 인증 기관 서비스 검증 요건을 만족하도록 요구될 수 있다(602).

[0040] 고객이 인증 기관 서비스 검증 요건을 만족할 수 있는 경우, 인증 기관 서비스는 장기 디지털 인증서를 생성할 수 있다. 이러한 장기 디지털 인증서는 장기 유효 기간(예를 들어, 1년 이상) 및 장기 디지털 인증서 인증 기관 서비스에 의해 단지 검증 목적들을 위해서만 사용될 수 있음을 지정할 수 있는 특정 중요 확장을 지정할 수 있다. 그에 따라, 장기 디지털 인증서는 이러한 특정 중요 확장을 인식하도록 구성된 사용자 클라이언트들에 의해 수용되지 않을 수 있다. 대안적으로, 중요 확장은 사용자 클라이언트에 의해 인식되지 않을 수 있으며, 이는 사용자 클라이언트가 장기 디지털 인증서를 거부하게 할 수 있다. 장기 디지털 인증서의 유효 기간은 인증 기관 서비스 또는 고객에 의해 서비스에 대한 그/그녀의 요청을 통해 정의될 수 있다. 장기 디지털 인증서가 생성되면, 인증 기관 서비스는 고객 사용용 장기 디지털 인증서를 발급할 수 있다. 그에 따라, 고객은 인증 기관 서비스로부터 장기 디지털 인증서를 수신할 수 있다(604).

[0041] 인증 기관 서비스로부터 장기 디지털 인증서를 수신한 이후 언제라도, 고객은 하나 이상의 사용자 클라이언트와 통신할 때 인증 목적들을 위해 이용될 수 있는 하나 이상의 단기 디지털 인증서의 발급에 대한 요청을 인증 기관 서비스에 제출할 수 있다(606). 요청은, 인증 기관 서비스가 고객의 식별 정보를 확인하기 위해 그리고 고객이 요청된 하나 이상의 단기 디지털 인증서를 획득하기 위해 인증됨을 보장하기 위해 이용할 수 있는 앞서 언급한 장기 디지털 인증서를 포함할 수 있다. 실시예에서, 인증 기관 서비스에 제출된 요청은 장기 디지털 인증서 내에 지정된 공개 암호화 키에 대응하는 고객의 비밀 암호화 키를 이용함으로써 고객에 의해 디지털 방식으로 서명된다. 인증 기관 서비스는 디지털 서명을 확인하기 위해 장기 디지털 인증서의 공개 키를 사용할 수 있다. 이는 인증 기관 서비스가 단기 디지털 인증서들이 이전에 장기 디지털 인증서를 발급한 동일한 엔티티에 발급될 것을 보장하게 한다.

[0042] 인증 기관 서비스가 장기 디지털 인증서를 사용하여 고객을 검증하면, 인증 기관 서비스는 그것들을 고객에게 발급될 수 있는 하나 이상의 단기 디지털 인증서를 생성할 수 있다. 이러한 단기 디지털 인증서들은 장기 디지털 인증서 보다 짧은 지속기간 또는 유효 기간을 가질 수 있다. 예를 들어, 인증 기관 서비스는 장기 디지털 인

증서에 대해 남아 있는 유효 기간에 적어도 부분적으로 기초하여 단기 디지털 인증서들에 대한 유효 기간을 정의할 수 있다. 대안적으로, 고객은 유효 기간이 장기 디지털 인증서에 대해 남아 있는 유효 기간보다 짧거나 동일인 한, 이러한 단기 디지털 인증서들에 대한 특정 유효 기간을 요청할 수 있다. 이는 인증 기관 서비스가 장기 디지털 인증서의 만료 날짜 이후인 만료 날짜를 갖는 단기 디지털 인증서를 발급할 수 없도록 만들 수 있다. 단기 디지털 인증서는 또한 장기 디지털 인증서 내에 지정된 중요 확장을 생략할 수 있다. 이는 이러한 단기 디지털 인증서들이 고객을 인증하기 위해 사용자 클라이언트들에 의해 이용되게 할 수 있다. 단기 디지털 인증서들이 생성되면, 고객은 인증 기관 서비스로부터 이러한 단기 디지털 인증서들을 수신할 수 있다(608).

[0043] 고객이 인증 기관 서비스로부터 하나 이상의 단기 디지털 인증서를 수신하면, 고객은 인증 목적들을 위해 이러한 하나 이상의 단기 디지털 인증서들을 이용할 수 있다(610). 예를 들어, 고객의 고객 서버는 예를 들어, 사용자 클라이언트들이 그들이 단기 디지털 인증서에 지정된 도메인 네임을 대신하여 가동될 권한이 있는 서버와 통신하고 있다고 결정하게 하기 위해 단기 디지털 인증서의 복사본을 사용자 클라이언트들에 제공할 수 있다. 단기 디지털 인증서는, 인증 기관 서비스로부터 획득되는 공개 암호화 키를 사용하여 사용자 클라이언트에 의해 검증될 수 있고 사용자 클라이언트에 의해 예를 들어, 신뢰된 인증서들에 대한 데이터 저장 장소에 유지될 수 있는 인증 기관 서비스 디지털 서명을 포함할 수 있다. 디지털 서명이 검증되는 경우, 사용자 클라이언트는 단기 디지털 인증서가 인증되고 고객이 그것이 주장하는 것임을 보장하기 위해 사용될 수 있다고 결정할 수 있다.

[0044] 위에서 언급된 바와 같이, 인증 기관 서비스는 장기 디지털 인증서의 발급에 대한 요청을 고객으로부터 수신할 수 있다. 이러한 장기 디지털 인증서는 고객 및 인증 기관 서비스 간 검증 목적들을 위해 이용될 수 있다. 예를 들어, 장기 디지털 인증서는 고객 또는 임의의 다른 엔티티에 의해 사용자 클라이언트들에 제공된 경우 사용자 클라이언트들이 디지털 인증서를 거부하게 할 수 있는 중요 확장을 지정할 수 있다. 그러나, 인증 기관 서비스는 고객을 검증하고 요청 시 인증을 위해 사용될 수 있는 단기 디지털 인증서들을 발급하기 위해 이러한 장기 디지털 인증서를 이용할 수 있다. 따라서, 도 7은 적어도 하나의 실시예에 따라 장기 디지털 인증서의 발급에 대한 고객 요청에 응답하여 장기 디지털 인증서를 생성하고 발급하기 위한 프로세스(700)의 예시적인 예를 도시한다. 프로세스(700)는, 고객들로부터 요청들을 수신하고 고객이 장기 디지털 인증서들을 수탁할 수 있는지 여부를 결정하기 위해 다른 엔티티들과 통신하도록 구성될 수 있는 앞서 언급한 인증 기관 서비스에 의해 수행될 수 있다. 나아가, 인증 기관 서비스는 고객의 요청 및 알려진 디지털 인증서 포맷들 및 표준들에 적어도 부분적으로 기초하여 이러한 장기 디지털 인증서들을 생성하도록 구성될 수 있다.

[0045] 고객은, 고객 및 인증 기관 서비스 간 검증 목적들을 위해 이용될 수 있는 장기 디지털 인증서의 발급을 요청하기 위해 인증 기관 서비스와 통신할 수 있다. 고객은, 사업 과정 동안 다양한 사용자 클라이언트와 통신하기 위해 이용될 수 있는 하나 이상의 서버를 가동할 수 있다. 이러한 하나 이상의 서버가 이러한 사용자 클라이언트들에 의해 인증되기 위해 그리고 이러한 하나 이상의 서버 및 사용자 클라이언트 간 보안 통신을 가능하게 하기 위해, 고객은 고객이 그것이 주장한느 것임을 이러한 사용자 클라이언트들에 보장하기 위해 하나 이상의 디지털 인증서를 획득해야 할 수 있다. 위에서 언급된 바와 같이, 장기 디지털 인증서는 검증 목적들을 위해 이용될 것이다. 추가적으로, 장기 디지털 인증서는 사용자 클라이언트들에 의해 서버 인증을 위해 이용될 수 있는 단기 디지털 인증서들을 획득하기 위해 요구될 수 있다. 그에 따라, 인증 기관 서비스는 장기 디지털 인증서의 발급에 대한 요청을 고객으로부터 수신할 수 있다(702).

[0046] 고객으로부터의 요청은 고객의 경영 활동들에 관한 정보를 포함할 수 있다. 예를 들어, 고객은 그의 이름, 주소, 이-메일 주소, URL(Uniform Resource Locator), 재무 기록 기타 같은 종류의 것을 심사를 위해 인증 기관 서비스에 제공할 수 있다. 이러한 정보는 고객이 하나 이상의 장기 디지털 인증서를 수탁할 수 있는지 여부를 결정하는 데 필요할 수 있다. 이렇게 하여, 인증 기관 서비스는 그것이 고객을 조사하기 위한 정밀 검증 프로세스를 수행하기 위해 고객으로부터 필수 정보를 수신했는지 여부를 결정할 수 있다(704). 고객이 인증 기관 서비스가 요청한 바에 따라, 이러한 필수 정보를 제공하지 않은 경우, 인증 기관 서비스는 장기 디지털 인증서의 발급에 대한 고객의 요청을 거부할 수 있다(706).

[0047] 고객이 고객을 검증하기 위해 요구되는 필수 정보를 인증 기관 서비스에 공급한 경우, 인증 기관 서비스는 요청자(예를 들어, 고객)를 확인 및 검증하기 위한 하나 이상의 엔티티 및 도메인 검증 프로세스를 수행할 수 있다(708). 예를 들어, 몇몇 실시예에서, 인증 기관 서비스는 고객의 도메인에 대한 관리상 책임이 있는 것으로 알려진 주소에 하나 이상의 메일(이-메일) 메시지를 전송할 수 있다. 인증 기관 서비스는 예를 들어, 고객 도메인을 식별하기 위해 "WHOIS" 질의를 이용할 수 있고 고객의 "WHOIS" 엔트리에 포함된 지정된 연락처에 인증 링크를 전송할 수 있다. 추가적으로, 또는 대안적으로, 인증 기관 서비스는 제공된 정보에 적어도 부분적으로 기초하여, 고객이 장기 디지털 인증서를 수탁받을 수 있는지 여부를 결정하기 위해 다양한 정부 관계 기관 데이터베

이스 및 다른 제3자 데이터베이스들 액세스할 수 있다.

[0048] 인증 기관 서비스가 엔티티 및 도메인 검증 프로세스들을 수행하면, 인증 기관 서비스는 이러한 프로세스들이 만족되었는지 여부를 결정할 수 있다(710). 예를 들어, 인증 기관 서비스가 정부 관계 기관 데이터베이스들 및 다른 제3자 데이터베이스들 내에 명시된 고객 정보의 분석에 기초하여, 고객이 장기 디지털 인증서를 수탁할 수 없다고 결정하는 경우, 인증 기관 서비스는 고객의 요청을 거부할 수 있다(706). 그러나, 검증 프로세스들이 충족된 경우, 인증 기관 서비스는 인증 기관 서비스 및 고객 간 검증 목적들을 위해 이용될 수 있는 장기 디지털 인증서를 생성할 수 있다(712).

[0049] 장기 디지털 인증서는 디지털 인증서의 발급자, 인증서에 대한 유효 기간, 주체(예를 들어, 고객), 주체의 공개 암호화 키, 및 인증 기관 서비스의 디지털 서명을 지정할 수 있다. 장기 디지털 인증서는 장기 디지털 인증서가 단지 검증 목적들을 위해서만 이용될 것임을 나타낼 수 있는 중요 확장을 더 지정할 수 있다. 이러한 중요 확장은 일부 사용자 클라이언트에 의해서는 인식되지 않을 수 있고, 그 결과, 이러한 사용자 클라이언트들에 의해 자동으로 거부될 수 있다. 대안적으로, 사용자 클라이언트들은 이러한 중요 확장을 포함하는 임의의 디지털 인증서들을 거부하도록 구성될 수 있다. 인증 기관 서비스가 이러한 장기 디지털 인증서를 생성되면, 인증 기관 서비스는 이러한 인증서를 고객에게 발급할 수 있다(714). 이렇게 하여, 고객은 이제 검증 목적들을 위해 그리고 하나 이상의 사용자 클라이언트와의 통신을 위해 단기 디지털 인증서들을 획득하기 위한 요청의 부분으로서 이러한 장기 디지털 인증서를 이용할 수 있다.

[0050] 위에서 언급된 바와 같이, 인증 기관 서비스는 하나 이상의 단기 디지털 인증서의 발급에 대한 요청을 고객으로부터 수신할 수 있다. 이러한 하나 이상의 단기 디지털 인증서는 이전에 발급된 장기 디지털 인증서와는 대조적으로, 고객을 인증하기 위해 그리고 고객 및 이러한 사용자 클라이언트들 간 보안 통신을 가능하게 위해 사용자 클라이언트들에 의해 이용될 수 있다. 고객으로부터의 요청은, 고객을 검증하기 위해 그리고 요청된 단기 디지털 인증서들을 생성하기 위해 필요한 정보를 획득하기 위해 인증 기관 서비스에 의해 이용될 수 있는 이전에 발급된 장기 디지털 인증서를 포함할 수 있다. 따라서, 도 8은 적어도 하나의 실시예에 따라 고객 요청에 응답하여 고객을 인증하고 하나 이상의 단기 디지털 인증서를 발급하기 위해 장기 디지털 인증서를 이용하기 위한 프로세스(800)의 예시적인 예를 도시한다.

[0051] 위에서 설명된 프로세스(700)와 유사하게, 고객은, 사용자 클라이언트들이 고객을 인증하게 하기 위해 그리고 보안 통신을 고객에게 전달하게 하기 위해 고객에 의해 사용자 클라이언트들에 제공될 수 있는 단기 디지털 인증서의 발급을 요청하기 위해 인증 기관 서비스와 통신할 수 있다. 요청은 인증 기관 서비스에 의해 고객에게 이전에 발급되고 단지 고객 및 인증 기관 서비스 간 검증 목적들을 위해서만 사용가능한 장기 디지털 인증서를 포함할 수 있다. 몇몇 실시예에서, 단기 디지털 인증서들의 발급에 대한 요청은 단기 디지털 인증서들이 고객에게 발급될 것임을 인증 기관 서비스에 보장하기 위해 장기 디지털 인증서 내에 포함된 고객의 비밀 암호화 키를 사용하여 디지털 방식으로 서명될 수 있다. 인증 기관 서비스는 디지털 서명을 확인하기 위해 장기 디지털 인증서의 공개 암호화 키를 사용할 수 있다. 이렇게 하여, 인증 기관 서비스는 하나 이상의 단기 디지털 인증서의 발급에 대한 요청을 수신할 수 있다(802).

[0052] 인증 기관 서비스가 고객으로부터 하나 이상의 단기 디지털 인증서의 발급에 대한 요청을 수신하면, 장기 디지털 인증서 내에 포함된 정보를 검사하여(804) 인증 기관 서비스는 인증서가 유효한지 여부를 결정할 수 있다(806). 예를 들어, 인증 기관 서비스는 요청을 제출한 엔티티가 장기 디지털 인증서 내에 지정된 주체에 매칭하는지 여부를 결정하기 위해 장기 디지털 인증서 내 주체 필드들을 평가할 수 있다. 나아가, 인증 기관 서비스는 장기 디지털 인증서가 인증서의 유효성을 결정하기 위해 포함된 인증 기관 서비스 디지털 서명을 이용함으로써 장기 디지털 인증서가 위조되었는지 여부를 결정할 수 있다. 인증 기관 서비스가 장기 디지털 인증서가 유효하지 않다고 결정하는 경우, 인증 기관 서비스는 단기 디지털 인증서의 발급에 대한 고객의 요청을 거부할 수 있다(808).

[0053] 실시예에서, 장기 디지털 인증서는 단기 디지털 인증서들을 고객에게 발급하도록 구성된 인증 기관 서비스와 상이한 인증 기관 서비스에 의해 발급될 수 있다. 장기 디지털 인증서는 이러한 상이한 인증 기관 서비스에 대응하는 인증 기관 서비스 디지털 서명을 포함할 수 있다. 그에 따라, 인증 기관 서비스는 먼저 그것이 이러한 상이한 인증 기관 서비스로부터의 공개 암호화 키를 갖는지 여부를 결정할 수 있고, 만약 그렇다면, 이러한 공개 암호화 키를 이용하여 장기 디지털 인증서 내에 지정된 디지털 서명을 확인하고 장기 디지털 인증서를 검증할 수 있다. 장기 디지털 인증서가 유효인 경우, 인증 기관 서비스는 계속해서 장기 디지털 인증서를 검사하여 그것이 요청된 단기 디지털 인증서들을 고객에게 발급할 수 있는지 여부를 결정할 수 있다.

[0054] 인증 기관 서비스가 장기 디지털 인증서가 실제로 유효하다고 결정하는 경우, 인증 기관 서비스는 장기 디지털 인증서가 여전히 단기 디지털 인증서들의 발급에 대해 충분히 남아 있는 유효 기간을 갖는지 여부를 결정할 수 있다(810). 예를 들어, 인증 기관 서비스는 인증 기관 서비스가 장기 디지털 인증서에 기초하여 임의의 단기 디지털 인증서들을 발급하기 위해 장기 디지털 인증서가 3개월보다 긴 남아 있는 유효 기간을 가져야 함을 요구할 수 있다. 유사하게, 인증 기관 서비스는 단지 특정 유효 기간을 갖는 단기 디지털 인증서들만을 발급하도록 구성될 수 있다. 이러한 특정 유효 기간이 장기 디지털 인증서의 남아 있는 유효 기간을 초과하는 경우, 인증 기관 서비스는 요청된 하나 이상의 단기 디지털 인증서를 생성하도록 허용되지 않을 수 있다. 이렇게 하여, 인증 기관 서비스가 장기 디지털 인증서가 충분한 남아 있는 유효 기간을 가지지 않는다고 결정하는 경우, 인증 기관 서비스는 고객의 요청을 거부할 수 있다(808).

[0055] 인증 기관 서비스가 장기 디지털 인증서가 하나 이상의 단기 디지털 인증서의 발급에 대한 충분한 남아 있는 유효 기간을 갖는다고 결정하면, 인증 기관 서비스는 발급될 단기 디지털 인증서들의 유효 기간을 결정할 수 있다(812). 위에서 언급된 바와 같이, 인증 기관 서비스는 설정된 유효 기간을 갖는 단기 디지털 인증서들을 생성하도록 구성될 수 있다. 이렇게 하여, 이러한 단기 디지털 인증서들은 이러한 특정 유효 기간을 지정할 수 있다. 다른 실시예들에서, 고객은 요청을 통해, 단기 디지털 인증서들에 대해 원하는 유효 기간을 지정할 수 있다. 원하는 유효 기간이 장기 디지털 인증서에 대해 남아 있는 유효 기간을 초과하지 않는 경우, 인증 기관 서비스는 요청된 하나 이상의 단기 디지털 인증서의 시작 날짜 및 만료 날짜를 계산하기 위해 이러한 원하는 유효 기간을 이용할 수 있다.

[0056] 인증 기관 서비스는 하나 이상의 단기 디지털 인증서를 생성하기 위해 단기 디지털 인증서들의 결정된 유효 기간 및 장기 디지털 인증서로부터 획득된 정보를 이용할 수 있다. 그 후, 인증 기관 서비스는 그/그녀의 요청에 응답하여 하나 이상의 단기 디지털 인증서를 고객에게 발급할 수 있다(814). 이는 다양한 사용자 클라이언트가 고객을 인증하게 하기 위해 그리고 고객와 안전하게 통신하게 하기 위해 고객이 이러한 사용자 클라이언트들에 이러한 하나 이상의 단기 디지털 인증서를 제공하게 할 수 있을 수 있다.

[0057] 위에서 언급된 바와 같이, 장기 디지털 인증서는 사용자 클라이언트에 의해 인식되지 않을 수 있거나 이러한 확장의 검출 및 인식 시, 사용자 클라이언트가 장기 디지털 인증서를 수용하지 않게 할 수 있는 중요 확장을 포함할 수 있다. 그에 따라, 고객이 사용자 클라이언트에 장기 디지털 인증서를 제공하는 경우, 사용자 클라이언트는 고객을 인증할 수 없을 수 있고 그에 따라 고객과 그 이상 통신하지 않을 수 있다. 따라서, 도 9는 적어도 하나의 실시예에 따라 고객 서버를 인증하기 위해 디지털 인증서를 이용하기 위한 프로세스(900)의 예시적인 예를 도시한다. 프로세스(900)는 임의의 사용자 클라이언트, 이를테면 사용자의 컴퓨팅 디바이스 상에 설치된 브라우저 애플리케이션에 의해 수행될 수 있다.

[0058] 사용자 클라이언트가 고객 서버와 통신 채널을 설정할 때, 고객 서버는 고객 서버의 식별 정보를 설정하기 위해 사용자 클라이언트에 하나 이상의 디지털 인증서를 전송할 수 있다. 이러한 디지털 인증서들은 고객 서버가 그것이 주장하는 것인지 여부를 결정하기 위해 사용될 수 있다. 예를 들어, 디지털 인증서는, 고객의 이름, 주소 및 도메인 및 관련 고객 서버를 지정할 수 있는 주체 필드를 포함할 수 있다. 나아가, 디지털 인증서는 사용자 클라이언트가 디지털 인증서가 신뢰된 인증 기관 서비스에 의해 발급되었음을 그리고 디지털 인증서가 유효함을 확인하기 위해 이용할 수 있는 인증 기관 서비스 디지털 서명을 포함할 수 있다. 나아가, 디지털 인증서는, 디지털 인증서가 사용자 클라이언트에 의해 어떻게 프로세싱되어야 하는지를 지정할 수 있는 다양한 확장을 포함할 수 있다. 이렇게 하여, 고객 서버와 통신을 설정 시, 사용자 클라이언트는 이러한 고객 서버로부터 디지털 인증서를 수신할 수 있고(902), 또한 디지털 인증서 내에 지정된 임의의 확장들을 식별할 수 있다(904).

[0059] 위에서 언급된 바와 같이, 장기 디지털 인증서들은 장기 디지털 인증서가 단지 고객 서버 및 발급 인증 기관 서비스 간 검증 목적들을 위해서만 이용될 수 있음을 지정할 수 있는 중요 확장을 포함할 수 있다. 이러한 중요 확장은 특정 사용자 클라이언트들에 의해서는 인식되지 않을 수 있고, 그 결과, 이러한 사용자 클라이언트들이 장기 디지털 인증서들을 거부하게 할 수 있다. 대안적으로, 몇몇 실시예에서, 사용자 클라이언트는 이러한 중요 확장을 인식하도록, 그리고 그 결과, 고객 서버로부터의 장기 디지털 인증서를 수용하지 않도록 구성될 수 있다. 그에 따라, 사용자 클라이언트는 수신된 디지털 인증서가 이러한 "검증 전용" 중요 확장을 포함하는지 여부를 결정할 수 있다(906). 디지털 인증서가 이러한 중요 확장을 포함하는 경우, 사용자 클라이언트가 고객을 인증할 수 없을 수 있기 때문에, 사용자 클라이언트는 사용자 클라이언트 및 고객 간 통신 채널을 종료할 수 있다(908). 그러나, 중요 확장이 존재하지 않는 경우, 사용자 클라이언트는 고객 서버를 인증하기 위해 계속해서 디지털 인증서를 프로세싱할 수 있다(910).

[0060] 도 10은 본 발명의 다양한 실시예에 따라 측면들을 구현하기 위한 예시적인 환경(1000)의 측면들을 도시한다. 이해될 바와 같이, 웹-기반 환경이 설명의 목적들을 위해 사용되지만, 상이한 환경들이 다양한 실시예를 구현하기 위해 적절하게 사용될 수 있다. 환경은 전자 클라이언트 디바이스(1002)를 포함하며, 이는 적절한 네트워크(1004)를 통해 요청들, 메시지들 또는 정보를 송신 및/또는 수신하도록 동작가능한 임의의 적절한 디바이스를 포함할 수 있고, 몇몇 실시예에서는, 정보를 다시 디바이스의 사용자에게 전달할 수 있다. 그러한 클라이언트 디바이스들의 예들은 개인용 컴퓨터들, 셀 폰들, 핸드헬드 메시징 디바이스들, 랩탑 컴퓨터들, 태블릿 컴퓨터들, 셋-탑 박스들, 개인용 정보 단말기들, 내장형 컴퓨터 시스템들, 전자 북 리더기들 기타 같은 종류의 것을 포함한다. 네트워크는 인트라넷, 인터넷, 셀룰러 네트워크, 근거리 네트워크, 위성 네트워크 또는 임의의 다른 그러한 네트워크 및/또는 이들의 조합을 포함하여 임의의 적절한 네트워크를 포함할 수 있다. 그러한 시스템을 위해 사용되는 구성요소들은 선택된 네트워크 및/또는 환경의 유형에 적어도 부분적으로 따를 수 있다. 그러한 네트워크를 통해 통신하기 위한 프로토콜들 및 구성요소들은 주지되어 있고 본 출원에서 상세하게 논의되지는 않을 것이다. 네트워크를 통한 통신은 유선 연결 또는 무선 연결 및 이들의 조합들에 의해 가능하게 될 수 있다. 이러한 예에서, 네트워크는, 해당 기술분야의 통상의 기술자에게 분명할 바와 같이 다른 네트워크들의 경우 유사한 목적을 제공하는 대안적인 디바이스가 사용될 수 있더라도, 환경이 요청들을 수신하고 그것들에 응답하여 콘텐츠를 제공하기 위한 웹 서버(1006)를 포함하에 따라, 인터넷을 포함한다.

[0061] 예시적인 환경은 적어도 하나의 애플리케이션 서버(1008) 및 데이터 저장소(1010)를 포함한다. 연결되거나 다르게 구성될 수 있는 몇몇 애플리케이션 서버, 계층 또는 다른 요소들, 프로세스들 또는 구성요소들이 있을 수 있으며, 이들은 이를테면 적절한 데이터 저장소로부터 데이터를 획득하는 작업들을 수행하기 위해 상호작용할 수 있다는 것이 이해되어야 한다. 서버들은 본 출원에서 사용될 때, 다양한 방식, 이를테면 하드웨어 디바이스들 또는 가상 컴퓨터 시스템들로 구현될 수 있다. 몇몇 문맥에서, 서버들은 컴퓨터 시스템 상에서 실행되는 프로그래밍 모듈을 지칭할 수 있다. 본 출원에서 사용될 때, 다르게 서술되거나 문맥을 볼 때 분명하지 않는 한, 용어 "데이터 저장소"는 데이터를 저장, 액세스 및 검색할 수 있으며, 임의의 조합 및 수의 데이터 서버, 데이터베이스, 데이터 저장 디바이스 및 데이터 저장 매체를, 임의의 표준, 분산, 가상 또는 클러스터 환경으로 포함할 수 있는 임의의 디바이스 또는 디바이스들의 조합을 지칭한다. 애플리케이션 서버는 클라이언트 디바이스에 대한 하나 이상의 애플리케이션의 측면들을 실행하여, 애플리케이션에 대한 데이터 액세스 및 비즈니스 로직의 일부 또는 전부를 핸들링하기 위해 필요에 따라 데이터 저장소와 통합하기 위한 임의의 적절한 하드웨어, 소프트웨어 및 펌웨어를 포함할 수 있다. 애플리케이션 서버는 데이터 저장소와 협력하여 액세스 제어 서비스들을 제공할 수 있고 이에 한정되는 것은 아니지만, 사용자에게 제공되기 위해 사용가능하며, 웹 서버에 의해 하이퍼텍스트 마크업 언어("HTML"), 확장성 마크업 언어("XML"), 자바스크립트, 연속형 문서 양식("CSS") 또는 다른 적절한 클라이언트-측 구조 언어의 형태로 사용자에게 제공될 수 있는 텍스트, 그래픽, 오디오, 비디오 및/또는 다른 콘텐츠를 포함하여 콘텐츠를 생성할 수 있다. 클라이언트 디바이스에 전달되는 콘텐츠는 이에 한정되는 것은 아니지만, 사용자가 청각적으로, 시각적으로 그리고/또는 촉각, 미각, 및/또는 후각을 포함하는 다음 감각들을 통해 지각할 수 있는 형태들을 포함하여 하나 이상의 형태로 콘텐츠를 제공하도록 클라이언트 디바이스에 의해 프로세싱될 수 있다. 모든 요청 및 응답의 핸들링, 뿐만 아니라 클라이언트 디바이스(1002) 및 애플리케이션 서버(1008) 간 콘텐츠의 전달은 이러한 예에서 PHP: 하이퍼텍스트 프리프로세서("PHP"), 파이톤(Python), 루비(Ruby), 펄(Perl), 자바(Java), HTML, XML, 또는 다른 적절한 서버-측 구조 언어를 사용하여 웹 서버에 의해 핸들링될 수 있다. 본 출원에서 논의된 구조 코드가 본 출원에서의 다른 곳에서 논의된 바와 같이 임의의 적절한 디바이스 또는 호스트 기계 상에서 실행될 수 있기 때문에, 웹 및 애플리케이션 서버들이 필수적인 것은 아니고 단지 예시적인 구성요소들이라는 것이 이해되어야 한다. 나아가, 본 출원에서 단일 디바이스에 의해 수행되는 것으로 설명된 동작들은 문맥을 볼 때 다르게 분명하지 않는 한, 분산 및/또는 가상 시스템을 형성할 수 있는 다수의 디바이스에 의해 총괄하여 수행될 수 있다.

[0062] 데이터 저장소(1010)는 몇몇 별개의 데이터 테이블, 데이터베이스, 데이터 문서, 동적 데이터 저장 기법 및/또는 본 발명의 특정 측면에 관한 데이터를 저장하기 위한 다른 데이터 저장 메커니즘 및 매체를 포함할 수 있다. 예를 들어, 도시된 데이터 저장소는 프로덕션 측에 대한 콘텐츠를 제공하기 위해 사용될 수 있는 프로덕션 데이터(1012) 및 사용자 정보(1016)를 저장하기 위한 메커니즘들을 포함할 수 있다. 데이터 저장소는 또한 보고, 분석 또는 다른 그러한 목적들을 위해 사용될 수 있는 로그 데이터(1014)를 저장하기 위한 메커니즘을 포함하는 것으로 도시된다. 데이터 저장소에 저장되어야 할 수 있는 많은 다른 측면, 이를테면 적절하게 위에서 나열된 메커니즘들 중 임의의 메커니즘 또는 데이터 저장소(1010)에 추가적인 메커니즘들에 저장될 수 있는 페이지 이미지 정보 및 액세스 권한 정보가 있을 수 있다는 것이 이해되어야 한다. 데이터 저장소(1010)는 그것와 연관된 로직을 통해, 애플리케이션 서버(1008)로부터 명령들을 수신하고 그것들에 응답하여 데이터를 획득, 업데이트

또는 다르게 프로세싱하도록 동작가능하다. 애플리케이션 서버(1008)는 수신된 명령들에 응답하여 정적, 동적 또는 정적 및 동적 데이터의 조합을 제공할 수 있다. 동적 데이터, 이를테면 웹 로그들(블로그들), 쇼핑 애플리케이션들, 뉴스 서비스들 및 다른 그러한 애플리케이션들에 사용되는 데이터는 본 출원에 설명된 바와 같은 서버-측 구조 언어들에 의해 생성될 수 있거나 또는 애플리케이션 서버 상에서, 또는 그것의 제어 하에서 동작하는 콘텐츠 관리 시스템("CMS")에 의해 제공될 수 있다. 일례로, 사용자는 사용자에 의해 동작되는 디바이스를 통해, 특정 유형의 아이템에 대한 검색 요청을 제출할 수 있다. 이 경우, 데이터 저장소는 사용자의 식별 정보를 확인하기 위해 사용자 정보에 액세스할 수 있고 해당 유형의 아이템들에 대한 정보를 획득하기 위해 카탈로그 상세 정보에 액세스할 수 있다. 그 다음 정보는 이를테면 사용자 디바이스(1002) 상의 브라우저를 통해 사용자가 볼 수 있는 웹 페이지 상에 나열한 결과들로, 사용자에게 리턴될 수 있다. 특정 관심 아이템에 대한 정보는 브라우저의 전용 페이지 또는 창에 보여질 수 있다. 그러나, 본 발명의 실시예들은 반드시 웹 페이지들의 상황으로 한정되는 것은 아니고, 일반적으로 요청들을 프로세싱하는 것에 보다 일반적으로 적용가능할 수 있으며, 여기서 요청들이 반드시 콘텐츠에 대한 요청들은 아니라는 것이 주의되어야 한다.

[0063] 각 서버는 통상적으로 일반적인 관리 및 해당 서버의 동작을 위한 실행가능한 프로그램 명령들을 제공하는 운영 체제를 포함할 것이고 통상적으로 서버의 프로세서에 의해 실행될 때, 서버가 그것의 의도된 기능들을 수행하게 하는 명령들을 저장한 컴퓨터 판독가능한 저장 매체(예를 들어, 하드 디스크, 랜덤 액세스 메모리, 판독 전용 메모리 등)를 포함할 것이다. 운영 체제 및 서버들의 일반적인 기능에 적합한 구현예들은 알려져 있거나 시판되고 있고 특히 본 출원에서의 본 발명을 고려하여 해당 기술분야의 통상의 기술자들에 의해 용이하게 구현된다.

[0064] 환경은 일 실시예에서, 하나 이상의 컴퓨터 네트워크 또는 직접 연결을 사용하는, 통신 링크들을 통해 상호연결되는 몇몇 컴퓨터 시스템 및 구성요소를 이용하는 분산 및/또는 가상 컴퓨팅 환경이다. 그러나, 해당 기술분야의 통상의 기술자에 의해 그러한 시스템이 도 10에 도시된 것보다 적거나 많은 수의 구성요소를 갖는 시스템에서 똑같이 잘 동작할 수 있음이 이해될 것이다. 그에 따라, 도 10에서의 시스템(1000)의 도면은 사실상 예시적인 것이고 본 발명의 범위를 제한하지 않는 것으로 취해져야 한다.

[0065] 다양한 실시예가 또한 몇몇 경우 다수의 애플리케이션 중 임의의 애플리케이션을 동작하기 위해 사용될 수 있는 하나 이상의 사용자 컴퓨터, 컴퓨팅 디바이스 또는 프로세싱 디바이스를 포함할 수 있는 매우 다양한 동작 환경에서 구현될 수 있다. 사용자 또는 클라이언트 디바이스들은 표준 운영 체제를 실행하는 많은 범용 개인용 컴퓨터, 이를테면 데스크탑, 랩탑 또는 태블릿 컴퓨터, 뿐만 아니라 모바일 소프트웨어를 실행하고 많은 네트워킹 및 메시징 프로토콜을 지원할 수 있는 셀룰러, 무선 및 핸드헬드 디바이스들을 중 임의의 것을 포함할 수 있다. 그러한 시스템은 또한 다양한 시판되고 있는 운영 체제 및 목적들 이를테면 개발 및 데이터베이스 관리를 위한 다른 알려진 애플리케이션들 중 임의의 것을 실행하는 다수의 워크스테이션을 포함할 수 있다. 이러한 디바이스들은 또한 다른 전자 디바이스들, 이를테면 가상 단말기들, 신 클라이언트들, 게이밍 시스템들 및 네트워크를 통해 통신할 수 있는 다른 디바이스들을 포함할 수 있다. 이러한 디바이스들은 또한 가상 디바이스들, 이를테면 가상 기계들, 하이퍼바이저들 및 네트워크를 통해 통신할 수 있는 다른 가상 디바이스들을 포함할 수 있다.

[0066] 본 발명의 다양한 실시예는 다양한 시판되고 있는 프로토콜 , 이를테면 전송 제어 프로토콜/인터넷 프로토콜(“TCP/IP”), 유저 데이터그램 프로토콜(“UDP”), 개방형 시스템 간 상호연결(“OSI”) 모델의 다양한 계층에서 동작하는 프로토콜들, 파일 전송 프로토콜(“FTP”), 유니버셜 플러그 앤 플레이(“UpnP”), 네트워크 파일 시스템(“NFS”), 공통 인터넷 파일 시스템(“CIFS”) 및 애플토크(AppleTalk) 중 임의의 것을 사용하여 통신을 지원하기 위한 해당 기술분야의 통상의 기술자들에게 익숙할 수 있는 적어도 하나의 네트워크를 이용한다. 네트워크는 예를 들어, 근거리 네트워크, 광역 네트워크, 가상 전용 네트워크, 인터넷, 인트라넷, 엑스트라넷, 공중 교환 전화 네트워크, 적외선 네트워크, 무선 네트워크, 위성 네트워크 및 이들의 임의의 조합일 수 있다.

[0067] 웹 서버를 이용하는 실시예들에서, 웹 서버는 하이퍼텍스트 전송 프로토콜("HTTP") 서버들, FTP 서버들, 공통 게이트웨이 인터페이스(“CGI”) 서버들, 데이터 서버들, 자바 서버들, 아파치(Apache) 서버들 및 비지니스 애프릴케이션 서버들을 포함하여, 다양한 서버 또는 중간 애플리케이션 중 임의의 것을 실행할 수 있다. 서버(들)은 또한 이를테면 임의의 프로그래밍 언어, 이를테면 Java®, C, C# 또는 C++, 또는 임의의 스트립팅 언어, 이를테면 루비, PHP, 펄, 파이톤 또는 TCL, 뿐만 아니라 이들의 조합들로 쓰여진 하나 이상의 스크립트 또는 프로그램으로서 구현될 수 있는 하나 이상의 웹 애플리케이션을 실행함으로써, 사용자 디바이스들로부터의 요청들에 응답하여 프로그램들 또는 스크립트들을 실행할 수 있을 수 있다. 서버(들)은 또한 제한 없이 Oracle®, Microsoft®, Sybase® 및 IBM®에서 시판되고 있는 것들 뿐만 아니라 오픈-소스 서버들 이를테면 MySQL, Postgres, SQLite, MongoDB, 및 구조 또는 비구조 데이터를 저장, 검색 및 액세스할 수 있는 임의의 다른 서버

를 포함하는, 데이터베이스 서버들을 포함할 수 있다. 데이터베이스 서버들은 태블릿-기반 서버들, 문서-기반 서버들, 비구조 서버들, 관계형 서버들, 비-관계형 서버들 또는 이들 및/또는 다른 데이터베이스 서버들의 조합들을 포함할 수 있다.

[0068] 환경은 위에서 논의된 바와 같이 다양한 데이터 저장소 및 다른 메모리 및 저장 매체를 포함할 수 있다. 이들은 다양한 위치에, 이를테면 컴퓨터들 중 하나 이상에 로컬이거나(그러고/또는 상주하거나) 네크워크를 거쳐 임의의 또는 모든 컴퓨터에서 원격인 저장 매체 상에 상주할 수 있다. 실시예들의 특정 집합에서, 정보는 해당 기술분야의 통상의 기술자들에게 익숙한 저장-영역 네트워크("SAN")에 상주할 수 있다. 유사하게, 컴퓨터들, 서버들 또는 다른 네트워크 디바이스들에 기인하는 기능들을 수행하기 위한 임의의 필요한 파일들이 적절하게, 로컬로 그리고/또는 원격에 저장될 수 있다. 시스템이 컴퓨터화된 디바이스들을 포함하는 경우, 각 그러한 디바이스는 버스를 통해 전기적으로 결합될 수 있는 하드웨어 요소들을 포함할 수 있으며, 요소들은 예를 들어, 적어도 하나의 중앙 처리 장치(CPU" 또는 "프로세서"), 적어도 하나의 입력 디바이스(예를 들어, 마우스, 키보드, 컨트롤러, 터치 스크린 또는 키패드) 및 적어도 하나의 출력 디바이스(예를 들어, 디스플레이 디바이스, 프린터 또는 스피커)를 포함한다. 그러한 시스템은 또한 하나 이상의 저장 디바이스, 이를테면 디스크 드라이브, 광 저장 디바이스 및 고체-상태 저장 디바이스 이를테면 랜덤 액세스 메모리("RAM") 또는 판독-전용 메모리("ROM"), 뿐만 아니라 착탈가능한 미디어 디바이스, 메모리 카드, 플레시 카드 등을 포함할 수 있다.

[0069] 그러한 디바이스들은 또한 위에서 설명된 바와 같은 컴퓨터-판독가능한 저장 매체 판독기, 통신 디바이스(예를 들어, 모뎀, 네트워크 카드(무선 또는 유선), 적외선 통신 디바이스 등) 및 작업 메모리를 포함할 수 있다. 컴퓨터 판독가능한 저장 매체 판독기는 원격, 로컬, 고정 및/또는 착탈가능한 저장 디바이스들 뿐만 아니라 컴퓨터 판독가능한 정보를 일시적으로 그리고/또는 보다 영구적으로 포함, 저장, 전송 및 검색하기 위한 저장 매체를 대표하여, 컴퓨터 판독가능한 저장 매체와 연결되거나, 또는 이를 수용하도록 구성될 수 있다. 시스템 및 다양한 디바이스는 또한 통상적으로 운영 체제 및 애플리케이션 프로그램, 이를테면 클라이언트 애플리케이션 또는 웹 브라우저를 포함하여, 다수의 소프트웨어 애플리케이션, 모듈, 서비스 또는 적어도 하나의 작업 메모리 디바이스 내에 위치된 다른 요소들을 포함할 것이다. 대안적인 실시예들이 위에서 설명된 것으로부터 많은 변경예를 가질 수 있다는 것이 이해되어야 한다. 예를 들어, 맞춤형 하드웨어가 또한 사용될 수 있고/거나 특정 요소들은 하드웨어, 소프트웨어(휴대용 소프트웨어, 이를테면 애플릿들을 포함함) 또는 양자로 구현될 수 있다. 나아가, 다른 컴퓨팅 디바이스들 이를테면 네트워크 입력/출력 디바이스들에 대한 연결이 채용될 수 있다.

[0070] 코드, 또는 코드의 부분들을 포함하기 위한 저장 매체 및 컴퓨터 판독가능한 매체는 RAM, ROM, 전자적으로 소거가능한 프로그램가능한 판독 전용 메모리("EEPROM"), 플래시 메모리 또는 다른 메모리 기술, 콤팩트 디스크 판독 전용 메모리(("CD-ROM"), 디지털 다목적 디스크(DVD) 또는 다른 광 저장장치, 자기 카셋트들, 자기 테이프, 자기 디스크 저장장치 또는 다른 자기 저장 디바이스들 또는 원하는 정보를 저장하기 위해 사용될 수 있고 시스템 디바이스에 의해 액세스될 수 있는 임의의 다른 매체를 포함하여, 저장 매체 및 통신 매체, 이에 한정되는 것은 아니지만, 이를테면, 정보 이를테면 컴퓨터 판독가능한 명령들, 데이터 구조들, 프로그램 모듈들 또는 다른 데이터의 저장 및/또는 전송을 위해 임의의 방법 또는 기술로 구현되는 휘발성 및 비-휘발성, 착탈가능한 및 비-착탈가능한 매체를 포함하여, 해당 기술분야에 알려지거나 사용되는 임의의 적절한 매체를 포함할 수 있다. 본 출원에 제공된 개시 및 교시들에 기초하여, 해당 기술분야의 통상의 기술자는 다양한 실시예를 구현하기 위한 다른 방식들 및/또는 방법들을 이해할 것이다.

[0071] 그에 따라, 명세서 및 도면들은 제한적인 의미가 아니라 예시적인 의미로 여겨져야 한다. 그러나, 청구항들에 제시된 바와 같은 본 발명의 광범위한 사상 및 범위에서 벗어나지 않고 그것에 대한 다양한 변형 및 변경이 이루어질 수 있다는 것이 분명할 것이다.

[0072] 다른 변형들이 본 발명의 사상 내에 있다. 그에 따라, 개시된 기술들이 다양한 변형 및 대안적인 구성을 허용하지만, 그것들의 특정 예시된 실시예들이 도면들에 도시되고 위에서 상세하게 설명되었다. 그러나, 본 발명을 개시된 특정 형태 또는 형태들로 제한하도록 의도되지 않고, 오히려 그와는 반대로, 첨부된 청구항들에 정의되는 바와 같은 본 발명의 사상 및 범위 내에 들어가는 모든 변형, 대안적인 구성 및 등가물을 커버하도록 의도된다는 것이 이해되어야 한다.

[0073] 용어들 "단수 표현" 및 "상기" 및 개시된 실시예들을 설명하는 문맥에서(특히 다음 청구항들의 문맥에서)의 유사한 지시 대상의 사용은 다르게 본 출원에 표시되거나 문맥에 의해 명백히 부인되지 않는 한 단수 및 복수 양자를 커버하도록 간주되어야 한다. 용어 "구성하는", "갖는", "포함하는" 및 "함유하는"은 다르게 언급되지 않는 한 개방형 용어들(즉, "이에 한정되지는 않지만, 포함하는"을 의미함)인 것으로 간주되어야 한다. 용어 "연

결된"은 변형되지 않고 물리적 연결들을 지칭할 때, 개재하는 것이 있더라도, 부분적으로 또는 전체적으로 ~내에 포함되는, ~에 부착되는 또는 함께 연결되는 것으로 간주되어야 한다. 본 출원에서의 값들의 범위의 열거는 단지 각 개별적인 값이 그것이 본 출원에 개별적으로 열거된 것처럼 명세서에 포함되도록 그리고 다르게 본 출원에서 표시되지 않는 한, 범위 내에 들어가는 각각 별개의 값을 개별적으로 지칭하는 약칭법으로서의 역할을 하도록 의도된다. 용어 "집합"의 사용(예를 들어, "아이템들의 집합") 또는 "부분집합"은 문맥에 의해 다르게 언급 또는 부정되지 않는 한, 하나 이상의 멤버를 포함하는 비공집합으로서 간주되어야 한다. 나아가, 문맥에 의해 다르게 언급되거나 부정되지 않는 한, 용어 대응하는 집합의 "부분집합"은 반드시 대응하는 집합의 진 부분집합을 나타내는 것은 아니고, 부분집합 및 대응하는 집합이 동일할 할 수 있다.

[0074] 연어, 이를테면 형태 "A, B, 및 C 중 적어도 하나", 또는 "A, B 및 C 중 적어도 하나"의 구들은 구체적으로 다르게 언급되거나 문맥에 의해 분명히 다르게 부정되지 않는 한, 아이템, 용어 등이 A 또는 B 또는 C 중 어느 하나, 또는 A 및 B 및 C의 집합의 임의의 비공 부분집합일 수 있음을 나타내기 위해 일반적으로 사용되는 바에 따라 문맥과 다르게 이해된다. 예를 들어, 세 개의 멤버를 갖는 집합의 예시적인 예에서, 연결 구들 "A, B, 및 C 중 적어도 하나" 및 "A, B 및 C 중 적어도 하나"는 다음 집합들: {A}, {B}, {C}, {A, B}, {A, C}, {B, C}, {A, B, C} 중 임의의 집합을 지칭한다. 따라서, 그러한 연어는 일반적으로 특정 실시예들이 각각 A의 적어도 하나, B의 적어도 하나 및 C의 적어도 하나가 나타나도록 요구함을 암시하도록 의도되지 않는다.

[0075] 본 출원에 설명된 프로세스들의 동작들은 다르게 본 출원에서 표시되거나 문맥에 의해 분명히 다르게 부정되지 않는 한 임의의 적합한 순서로 수행될 수 있다. 본 출원에 설명된 프로세스들(또는 변형들 및/또는 이들의 조합들)은 실행가능한 명령들로 구성된 하나 이상의 컴퓨터 시스템의 제어 하에서 수행될 수 있고 하드웨어 또는 이들의 조합들에 의해, 하나 이상의 프로세서 상에서 총괄하여 실행되는 코드(예를 들어, 실행가능한 명령들, 하나 이상의 컴퓨터 프로그램 또는 하나 이상의 애플리케이션)로서 구현될 수 있다. 코드는 예를 들어, 하나 이상의 프로세서에 의해 실행가능한 복수의 명령을 포함하는 컴퓨터 프로그램의 형태로, 컴퓨터 판독가능한 저장 매체 상에 저장될 수 있다. 컴퓨터 판독가능한 저장 매체는 비-일시적일 수 있다.

[0076] 본 출원에 제공되는 임의의 그리고 모든 예, 또는 대표적인 언어(예를 들어, "이를테면") 의 사용은 단지 본 발명의 실시예들을 보다 양호하게 밝히도록 의도되고 다르게 주장되지 않는 한 본 발명의 범위에 대한 제한을 지우지 않는다. 명세서에서의 어떠한 언어도 임의의 주장되지 않은 요소를 본 발명의 실시에 필수적인 것으로 나타내는 것으로 간주되지 않아야 한다.

[0077] 본 발명의 실시예들은 본 발명을 수행하기 위해 발명자들에게 알려진 최상의 모드를 포함하여, 본 출원에서 설명된다. 그러한 실시예들의 변형들은 앞서 말한 설명을 읽을 때 해당 기술분야의 통상의 기술자들에게 분명해질 수 있다. 발명자들은 숙련된 기술자들이 그러한 변형들을 적절하게 채용하기를 기대하고 발명자들은 본 발명의 실시예들이 본 출원에 구체적으로 설명된 것과 다르게 실시되는 것을 의도한다. 그에 따라, 본 발명의 범위는 준거법에 의해 허용되는 바에 따라 첨부된 청구항들에 열거된 주제의 모든 변형 및 등가물을 포함한다. 게다가, 본 출원에서 표시되거나 문맥에 의해 분명히 다르게 부정되지 않는 한, 가능한 변형에서의 위에서 설명된 요소들의 임의의 조합이 본 발명의 범위에 의해 망라된다.

[0078] 본 출원에서 인용된 간행물, 특허 출원 및 특허를 포함하는 모든 참조 문헌은 이에 의해 각 참조 문헌이 개별적으로 그리고 구체적으로 참조로 원용되는 것으로 표시되는 것처럼 그리고 그 전체가 본 출원에 제시되는 것처럼 동일한 정도로 원용된다.

[0079] 본 발명의 실시예들은 다음 조항들을 고려해서 설명될 수 있다:

[0080] 1. 컴퓨터-구현 방법으로서,

[0081] 실행가능한 명령들로 구성된 하나 이상의 컴퓨터 시스템의 제어 하에,

[0082] 제1 디지털 인증서를 엔티티에 발급하는 단계로서, 상기 제1 디지털 인증서는 인증 기관 서비스에 상기 엔티티의 검증을 가능하게 하는 중요 확장(critical extension)을 지정하고, 상기 제1 디지털 인증서는:

[0083] 상기 엔티티에 특유한 적어도 하나의 주체 필드를 지정하고;

[0084] 제1 공개 암호화 키를 지정하고;

[0085] 제1 비밀 암호화 키에 대응하며; 그리고

[0086] 상기 제1 디지털 인증서에 대한 제1 유효 기간을 지정하는, 상기 제1 디지털 인증서를 엔티티에 발급하

는 단계;

[0087] 상기 엔티티로부터, 제2 디지털 인증서의 발급에 대한 요청을 수신하는 단계로서, 상기 요청은 상기 제1 디지털 인증서 및 디지털 서명을 포함하고, 상기 제2 디지털 인증서는 상기 엔티티의 서버의 인증을 위해 사용가능한 것인, 상기 제2 디지털 인증서의 발급에 대한 요청을 수신하는 단계;

[0088] 상기 제1 디지털 인증서 내에 지정된 유효 기간 및 상기 제1 공개 암호화 키에 적어도 부분적으로 기초하여, 상기 제2 디지털 인증서를 발급할지 여부를 결정하는 단계; 및

[0089] 상기 적어도 하나의 주체 필드 및 상기 제1 유효 기간보다 짧은 제2 유효 기간을 갖기 위한 제2 디지털 인증서를 발급하는 단계를 포함하는, 컴퓨터-구현 방법.

[0090] 2. 조항 1에 있어서, 인증 기관 서비스에 상기 엔티티의 검증을 가능하게 하는 상기 중요 확장은 또한 상기 제1 디지털 인증서가 상기 엔티티의 상기 서버의 인증을 위해 사용될 수 없도록 만드는, 컴퓨터-구현 방법.

[0091] 3. 조항 1 또는 2에 있어서, 상기 중요 확장은 상기 제1 디지털 인증서의 발급 이전 상기 인증 기관 서비스에 의한 상기 엔티티의 검증 날짜, 상기 엔티티를 검증하기 위해 상기 인증 기관 서비스에 의해 이용된 하나 이상의 표준, 및 상기 엔티티에 대응하는 식별자를 지정하는, 컴퓨터-구현 방법.

[0092] 4. 조항 1 내지 3 중 어느 한 조항에 있어서, 상기 제2 디지털 인증서는 상기 제1 디지털 인증서에 지정된 상기 제1 공개 암호화 키와 별개의 제2 공개 암호화 키를 더 포함하는, 컴퓨터-구현 방법.

[0093] 5. 하나 이상의 서비스를 구현하도록 구성된 적어도 하나의 컴퓨팅 디바이스를 포함하는 시스템으로서, 상기 하나 이상의 서비스는:

[0094] 제1 디지털 인증서를 엔티티에 발급하되, 상기 제1 디지털 인증서는:

[0095] 상기 하나 이상의 서비스에 상기 엔티티의 검증을 가능하게 하는 것; 및

[0096] 상기 엔티티에 특유한 적어도 하나의 주체 필드를 지정하는 것이고;

[0097] 상기 엔티티로부터, 제2 디지털 인증서의 발급에 대한 요청을 수신하되, 상기 요청은 상기 제1 디지털 인증서를 포함하는 것이고, 상기 제2 디지털 인증서는 상기 엔티티의 인증을 위해 사용가능한 것이고;

[0098] 상기 제1 디지털 인증서 내에 지정된 정보에 적어도 부분적으로 기초하여, 상기 제2 디지털 인증서를 발급할지 여부를 결정하며; 그리고

[0099] 상기 제1 디지털 인증서 내에 지정된 상기 정보에 적어도 부분적으로 기초한 정보를 갖기 위한 그리고 상기 엔티티에 특유한 상기 적어도 하나의 주체 필드를 갖기 위한 상기 제2 디지털 인증서를 발급하도록 구성된, 시스템.

[0100] 6. 조항 5에 있어서,

[0101] 상기 제2 디지털 인증서의 발급에 대한 상기 요청은 디지털 서명을 포함하며; 그리고

[0102] 상기 하나 이상의 서비스는 상기 제1 디지털 인증서 내에 지정된 공개 암호화 키를 사용하여 상기 디지털 서명을 확인하도록 더 구성된, 시스템.

[0103] 7. 조항 5 또는 6에 있어서,

[0104] 상기 제1 디지털 인증서 내에 지정된 상기 정보는 상기 제1 디지털 인증서에 대한 유효 기간을 포함하며; 그리고

[0105] 상기 하나 이상의 서비스는 상기 제1 디지털 인증서가 만료되지 않았고 상기 제2 디지털 인증서의 발급을 위해 이용될 수 있음을 확인하기 위해 상기 제1 디지털 인증서에 대한 상기 유효 기간을 이용하도록 더 구성되는, 시스템.

[0106] 8. 조항 7에 있어서, 상기 제2 디지털 인증서의 정보는 상기 제1 디지털 인증서에 대한 상기 유효 기간보다 짧은 유효 기간을 지정하는, 시스템.

[0107] 9. 조항 5 내지 8 중 어느 한 조항에 있어서, 상기 제2 디지털 인증서 내에 포함되는 상기 정보는 또한 상기 제2 디지털 인증서의 발급에 대한 상기 요청 내에 상기 엔티티에 의해 지정된 유효 기간에 적어도 부분적으로 기초하는, 시스템.

[0108] 10. 조항 5 내지 9 중 어느 한 조항에 있어서, 상기 제2 디지털 인증서는 또한 상기 제1 디지털 인증서 내에 포함되지 않은 하나 이상의 추가 주체 필드를 갖도록 발급되는, 시스템.

[0109] 11. 조항 5 내지 10 중 어느 한 조항에 있어서, 상기 제1 디지털 인증서는 상기 제1 디지털 인증서가 인증을 위해 사용되지 않아야 함을 나타내는 중요 확장을 지정하는, 시스템.

[0110] 12. 조항 11에 있어서, 상기 중요 확장은 상기 제1 디지털 인증서의 발급 이전 상기 하나 이상의 서비스에 의한 상기 엔티티의 검증 날짜, 상기 엔티티를 검증하기 위해 상기 하나 이상의 서비스에 의해 이용되는 하나 이상의 표준, 및 상기 엔티티에 대응하는 식별자를 포함하는, 시스템.

[0111] 13. 실행가능한 명령들을 저장한 비-일시적 컴퓨터-판독가능한 저장 매체로서, 상기 명령들은 컴퓨터 시스템의 하나 이상의 프로세서에 의해 실행될 때, 상기 컴퓨터 시스템이 적어도:

[0112] 엔티티로부터, 상기 엔티티의 인증을 위해 사용가능한 디지털 인증서의 발급에 대한 요청을 수신하되, 상기 요청은 인증 기관 서비스에 상기 엔티티를 검증하기 위해 사용가능한 이전에 발급된 디지털 인증서를 포함하고 상기 엔티티에 특유한 적어도 하나의 주체 필드를 지정하는 것이고;

[0113] 상기 이전에 발급된 디지털 인증서 내에 지정된 정보에 적어도 부분적으로 기초하여, 상기 디지털 인증서를 발급할지 여부를 결정하며; 그리고

[0114] 상기 이전에 발급된 디지털 인증서 내에 지정된 상기 정보에 적어도 부분적으로 기초한 정보를 갖기 위한 그리고 상기 엔티티에 특유한 상기 적어도 하나의 주체 필드를 갖기 위한 상기 디지털 인증서를 발급하게 하는, 비-일시적 컴퓨터-판독가능한 저장 매체.

[0115] 14. 조항 13에 있어서, 상기 명령들은 상기 컴퓨터 시스템의 상기 하나 이상의 프로세서에 의해 실행될 때 상기 컴퓨터 시스템이 상기 제2 디지털 인증서를 발급할지 여부를 결정하기 위해 상기 요청 내에 상기 엔티티에 의해 정의된 원하는 유효 기간을 획득하게 하는 명령들을 더 포함하는, 비-일시적 컴퓨터-판독가능한 저장 매체.

[0116] 15. 조항 13 또는 14에 있어서, 상기 이전에 발급된 디지털 인증서는 상기 이전에 발급된 디지털 인증서의 발급을 위한 상기 엔티티로부터의 요청에 응답하여 상기 컴퓨터 시스템에 의해 발급된 것인, 비-일시적 컴퓨터-판독가능한 저장 매체.

[0117] 16. 조항 13 내지 15 중 어느 한 조항에 있어서,

[0118] 상기 이전에 발급된 디지털 인증서는 비밀 암호화 키에 대응하는 공개 암호화 키를 더 지정하고;

[0119] 상기 이전에 발급된 디지털 인증서 내에 지정된 상기 정보는 상기 이전에 발급된 디지털 인증서에 대한 유효 기간을 포함하며; 그리고

[0120] 상기 명령들은 상기 하나 이상의 프로세서에 의해 실행될 때 상기 컴퓨터 시스템이 상기 이전에 발급된 디지털 인증서가 만료되지 않았고 상기 디지털 인증서의 발급을 위해 이용될 수 있음을 확인하기 위해 상기 유효 기간을 이용하게 하는 명령들을 더 포함하는, 비-일시적 컴퓨터-판독가능한 저장 매체.

[0121] 17. 조항 16에 있어서, 상기 발급된 디지털 인증서 내에 포함된 정보는 상기 이전에 발급된 디지털 인증서에 대한 상기 유효 기간보다 짧은 유효 기간을 지정하는, 비-일시적 컴퓨터-판독가능한 저장 매체.

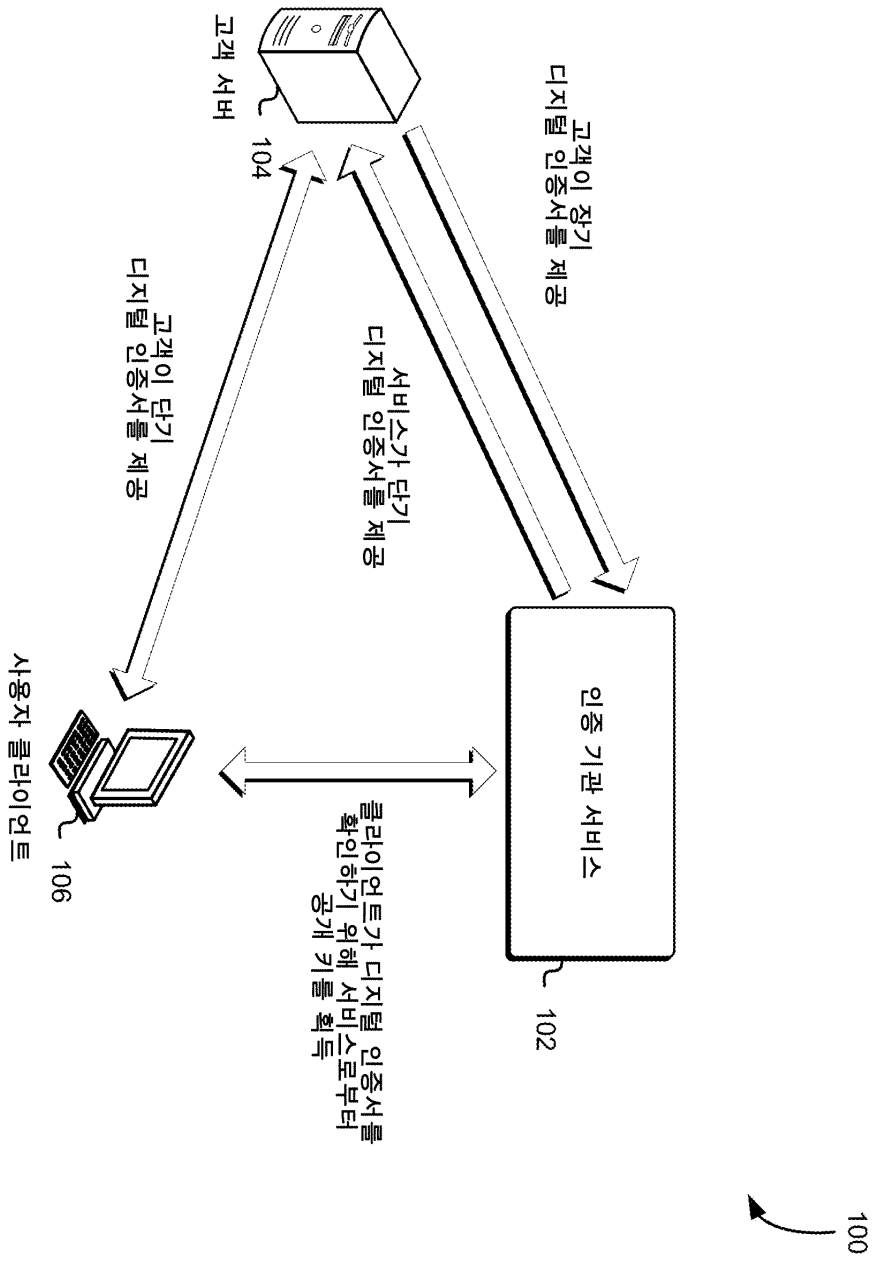
[0122] 18. 조항 16 또는 17에 있어서, 상기 디지털 인증서의 발급에 대한 상기 요청은 상기 공개 암호에 대응하는 상기 비밀 암호화 키를 이용하여 상기 엔티티에 의해 디지털 방식으로 서명되는, 비-일시적 컴퓨터-판독가능한 저장 매체.

[0123] 19. 조항 13 내지 18 중 어느 한 조항에 있어서, 상기 이전에 발급된 디지털 인증서는 상기 엔티티를 검증하기 위해 이용되는 하나 이상의 표준을 포함하는 중요 확장을 지정하는, 비-일시적 컴퓨터-판독가능한 저장 매체.

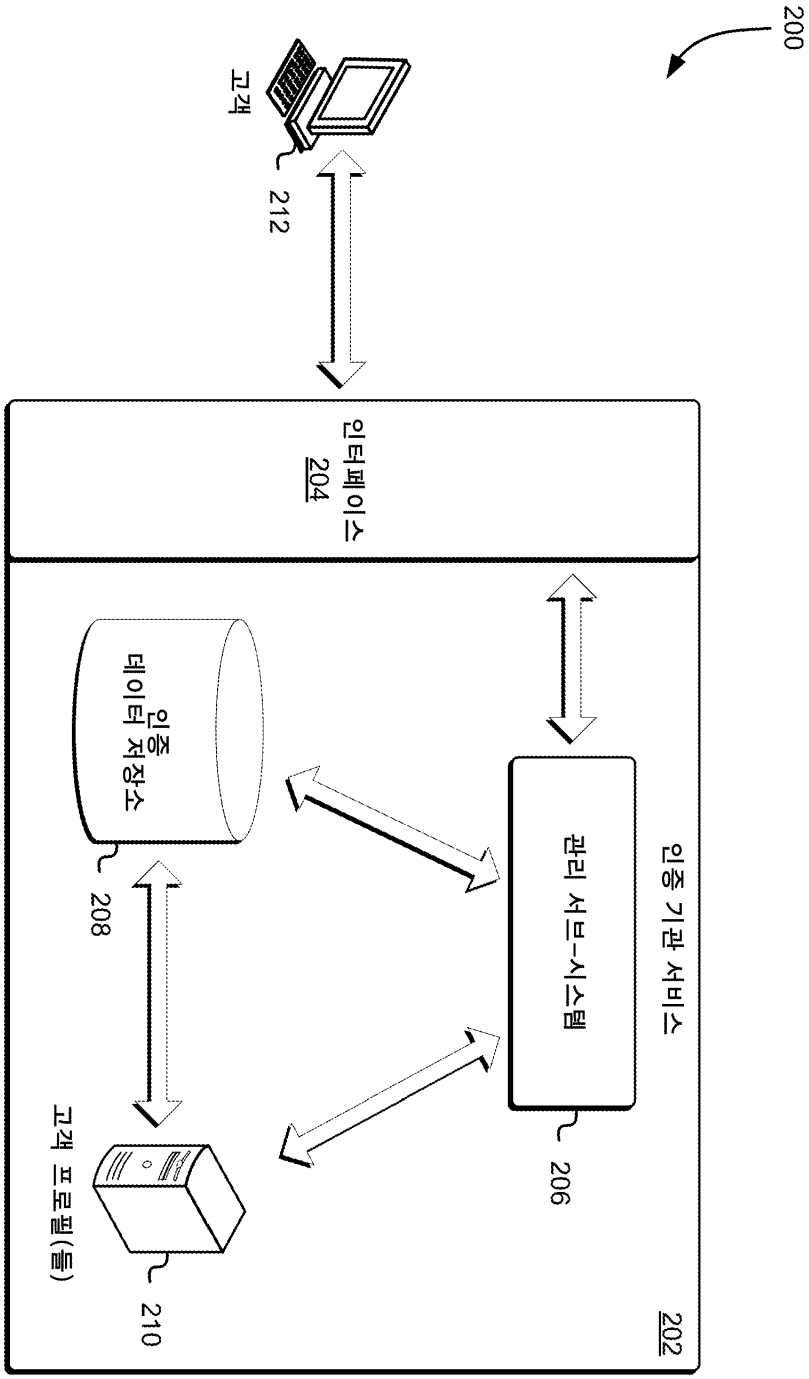
[0124] 20. 조항 19에 있어서, 상기 중요 확장은 상기 이전에 발급된 디지털 인증서가 인증을 위해 사용되지 않아야 함을 더 나타내는 중요 확장을 지정하는, 비-일시적 컴퓨터-판독가능한 저장 매체.

도면

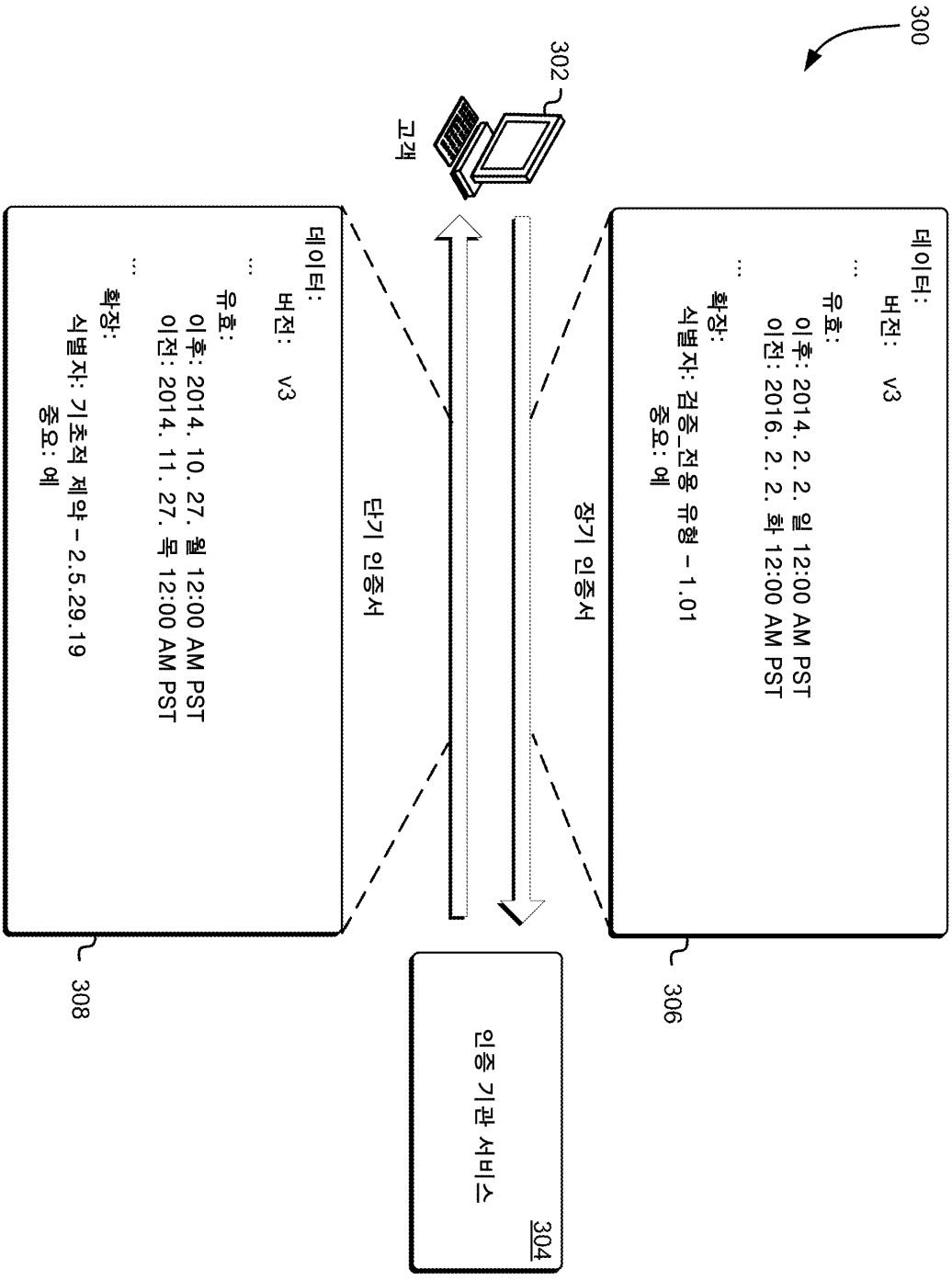
도면1


고객 서버
104
고객이 장기
디지털 인증서를 제공
서비스가 단기
디지털 인증서를 제공
고객이 단기
디지털 인증서를 제공
사용자 클라이언트
106
인증 기관 서비스
102
클라이언트가 디지털 인증서를
확인 하기 위해 서비스로부터
공개 키를 획득
100

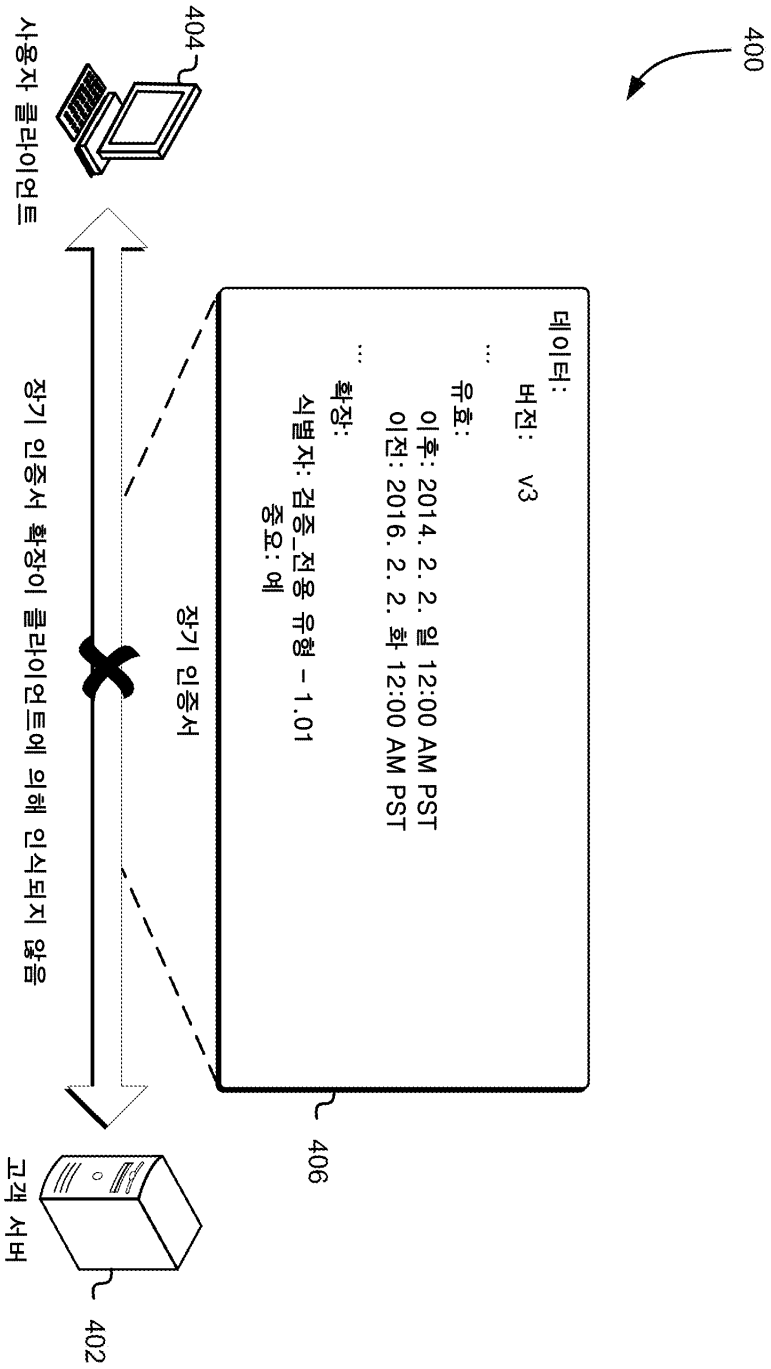
도면2


200
고객
212
인터페이스
204
인증 기관 서비스
관리 서브-시스템
206
인증
데이터 저장소
208
고객 프로필(들)
210
202

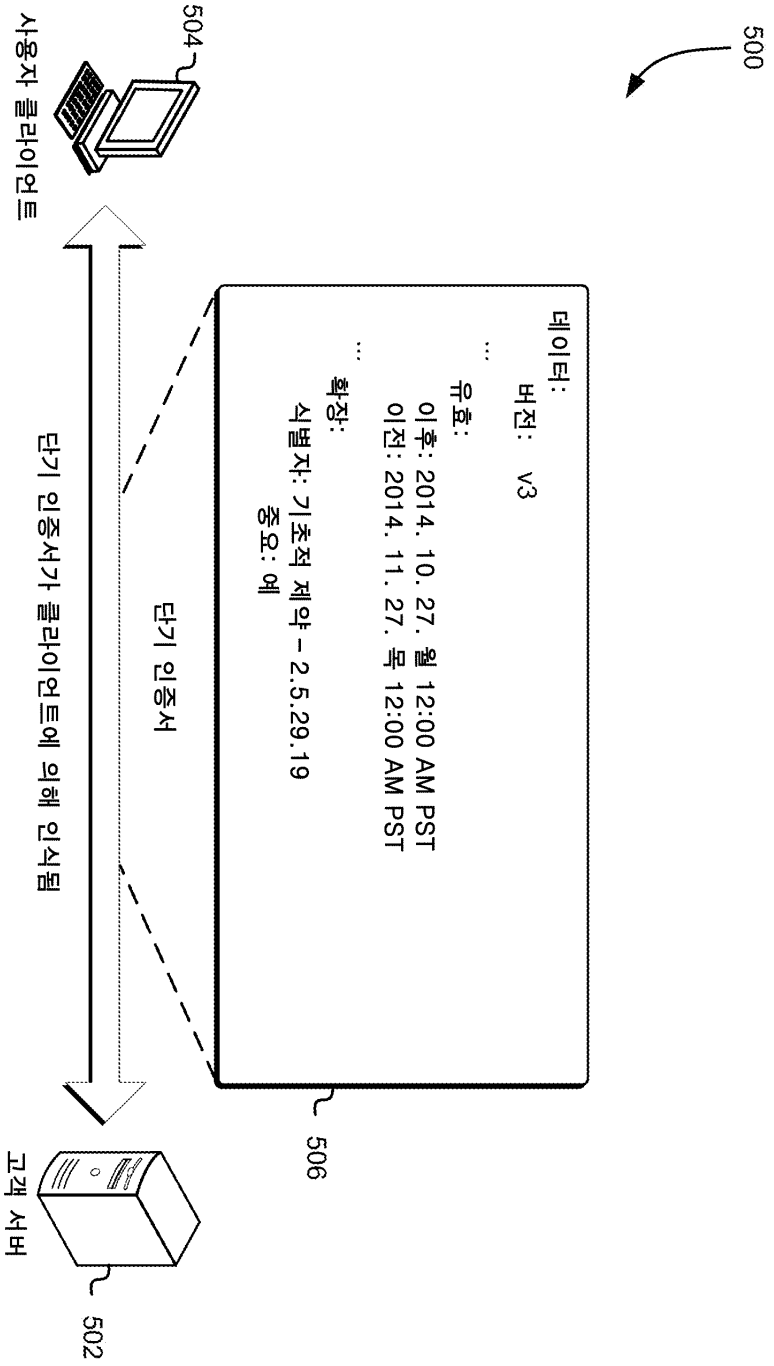
도면3


300
302
고객
데이터:
버전: v3
...
유효:
이후: 2014. 2. 2. 일 12:00 AM PST
이전: 2016. 2. 2. 화 12:00 AM PST
...
확장:
식별자: 검증_전용 유형 - 1.01
중요: 예
306
장기 인증서
단기 인증서
데이터:
버전: v3
...
유효:
이후: 2014. 10. 27. 월 12:00 AM PST
이전: 2014. 11. 27. 목 12:00 AM PST
...
확장:
식별자: 기초적 제약 - 2.5.29.19
중요: 예
308
인증 기관 서비스
304

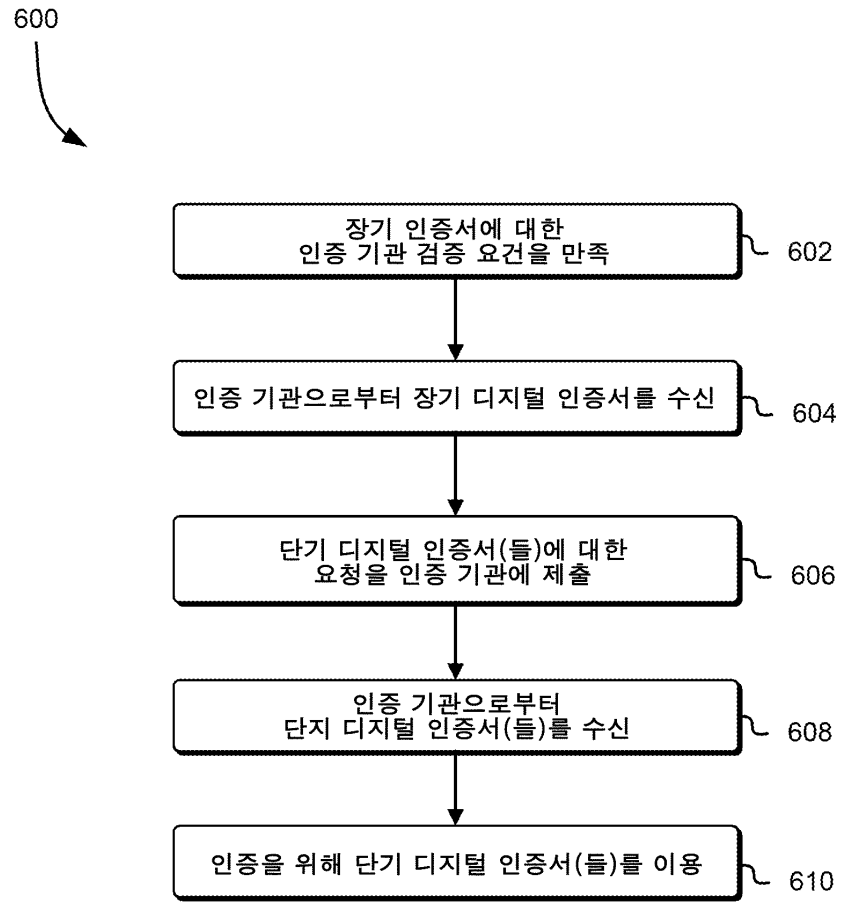
도면4


400
404
사용자 클라이언트
데이터:
버전: v3
...
유효:
이후: 2014. 2. 2. 일 12:00 AM PST
이전: 2016. 2. 2. 화 12:00 AM PST
...
확장:
식별자: 검증_전용 유형 - 1.01
중요: 예
장기 인증서
406
장기 인증서 확장이 클라이언트에 의해 인식되지 않음
고객 서버
402

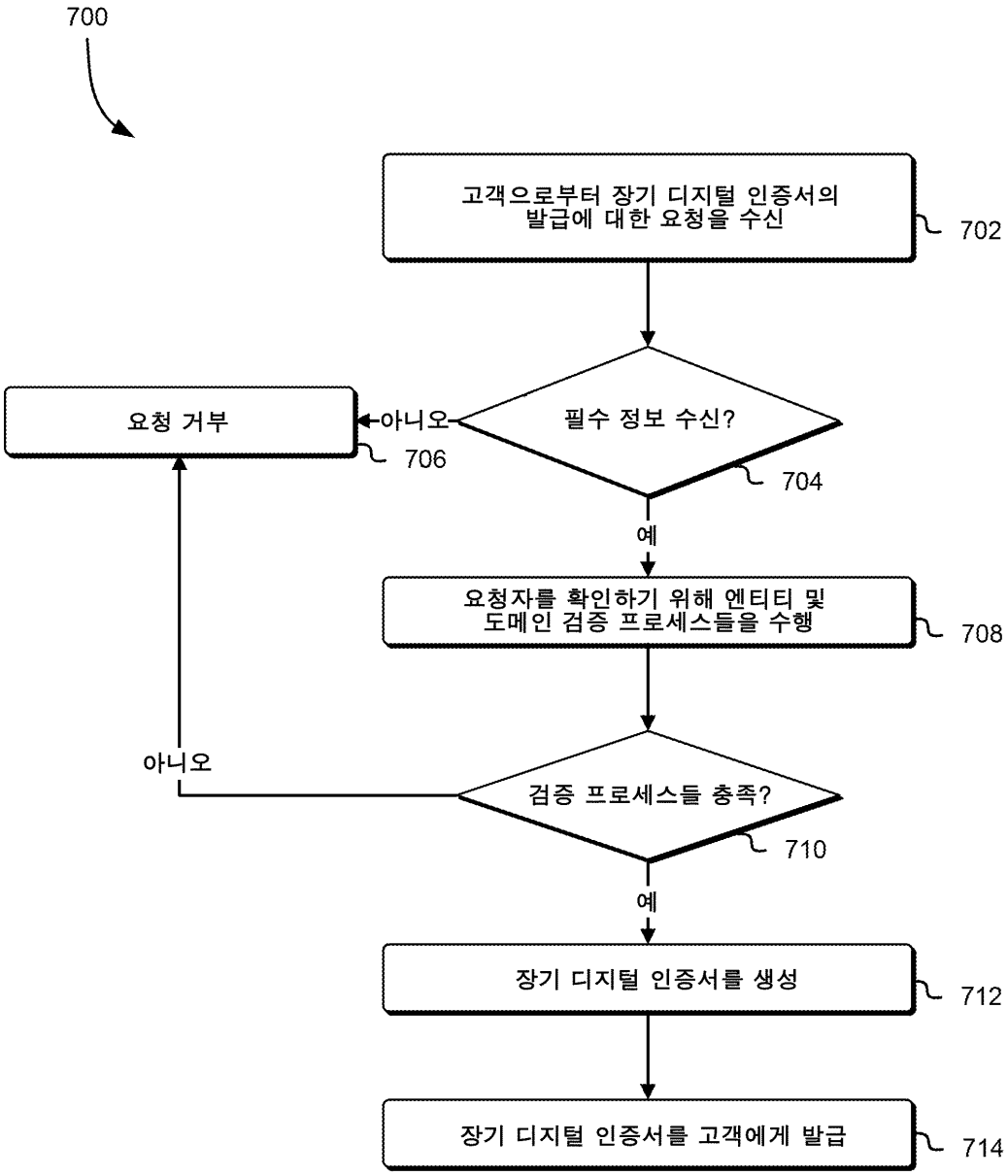
도면5


500
504
사용자 클라이언트
데이터:
버전: v3
...
유효:
이후: 2014. 10. 27. 월 12:00 AM PST
이전: 2014. 11. 27. 목 12:00 AM PST
...
확장:
식별자: 기초적 제약 - 2.5.29.19
중요: 예
506
단기 인증서
단기 인증서가 클라이언트에 의해 인식됨
고객 서버
502

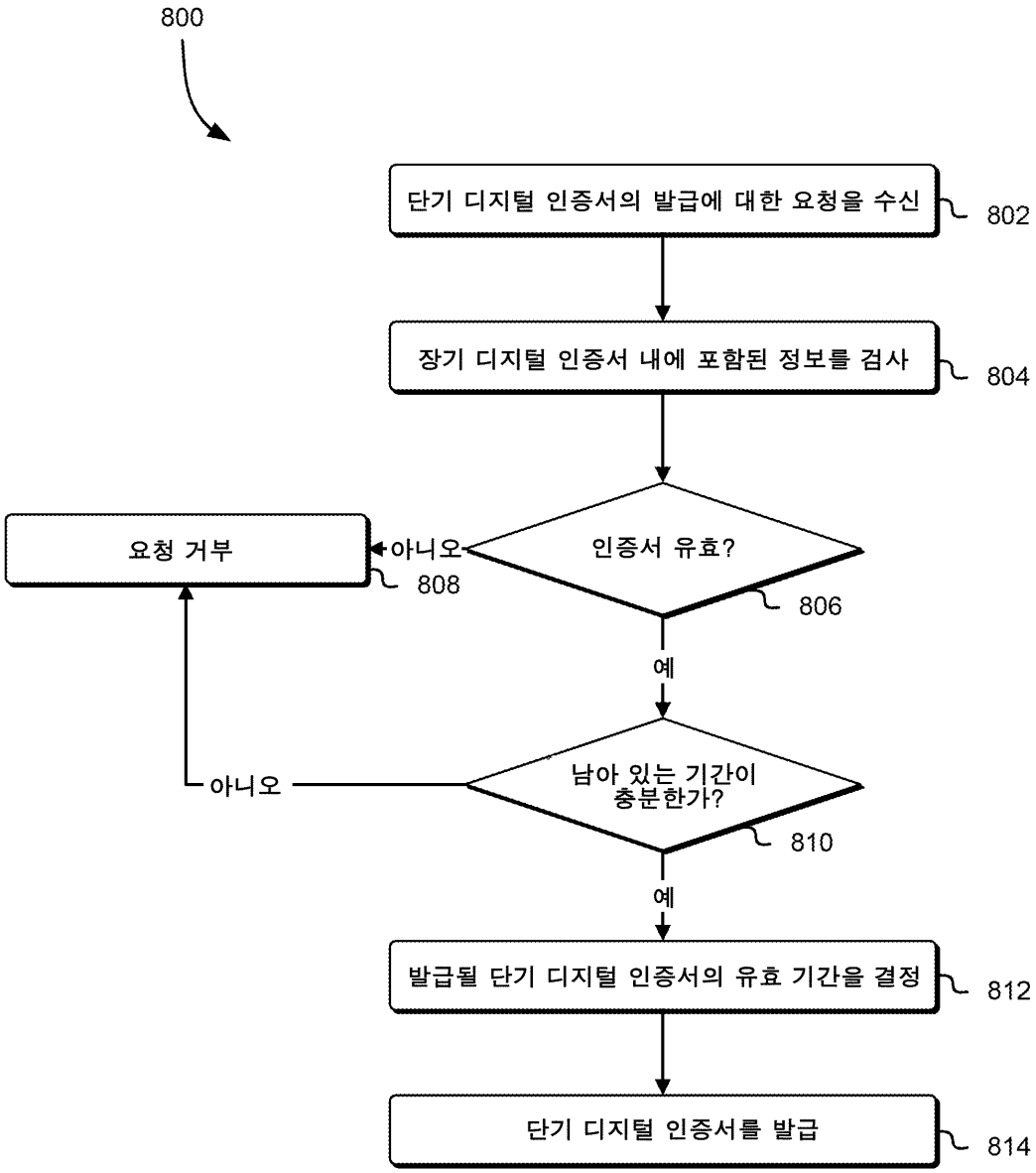
도면6


600
장기 인증서에 대한
인증 기관 검증 요건을 만족
602
인증 기관으로부터 장기 디지털 인증서를 수신
604
단기 디지털 인증서(들)에 대한
요청을 인증 기관에 제출
606
인증 기관으로부터
단지 디지털 인증서(들)를 수신
608
인증을 위해 단기 디지털 인증서(들)를 이용
610

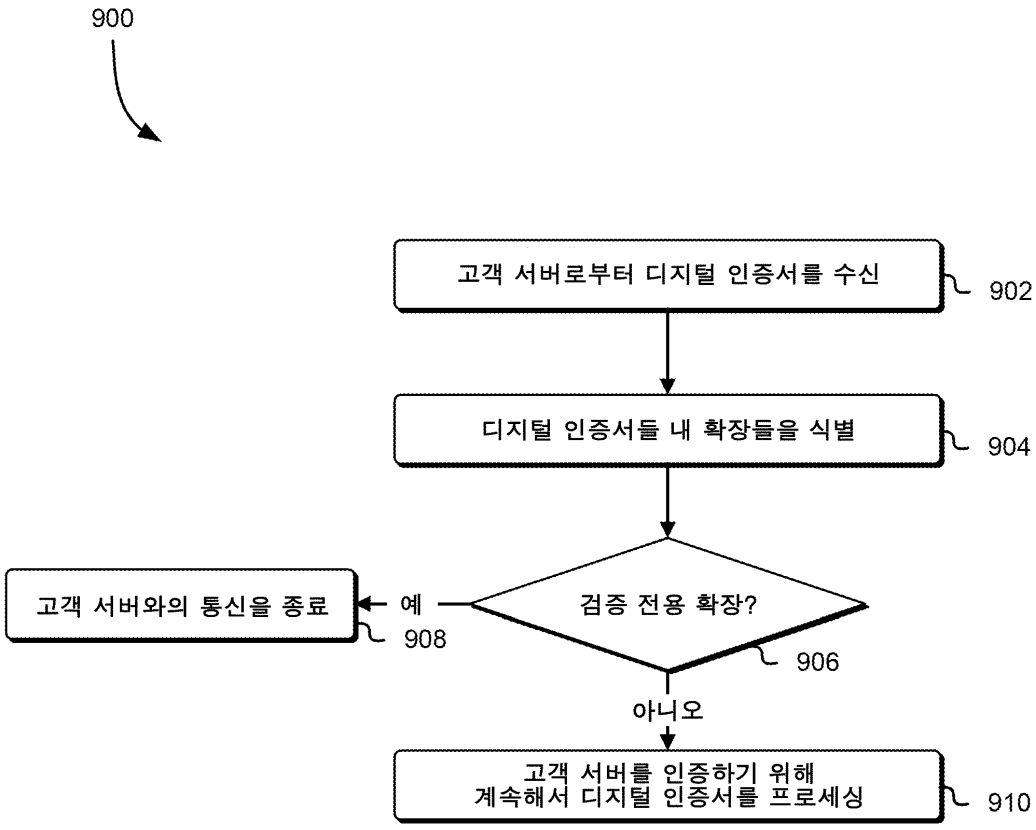
도면7


700
고객으로부터 장기 디지털 인증서의 발급에 대한 요청을 수신
702
필수 정보 수신?
704
아니오
요청 거부
706
예
요청자를 확인하기 위해 엔티티 및 도메인 검증 프로세스들을 수행
708
검증 프로세스들 충족?
710
아니오
예
장기 디지털 인증서를 생성
712
장기 디지털 인증서를 고객에게 발급
714

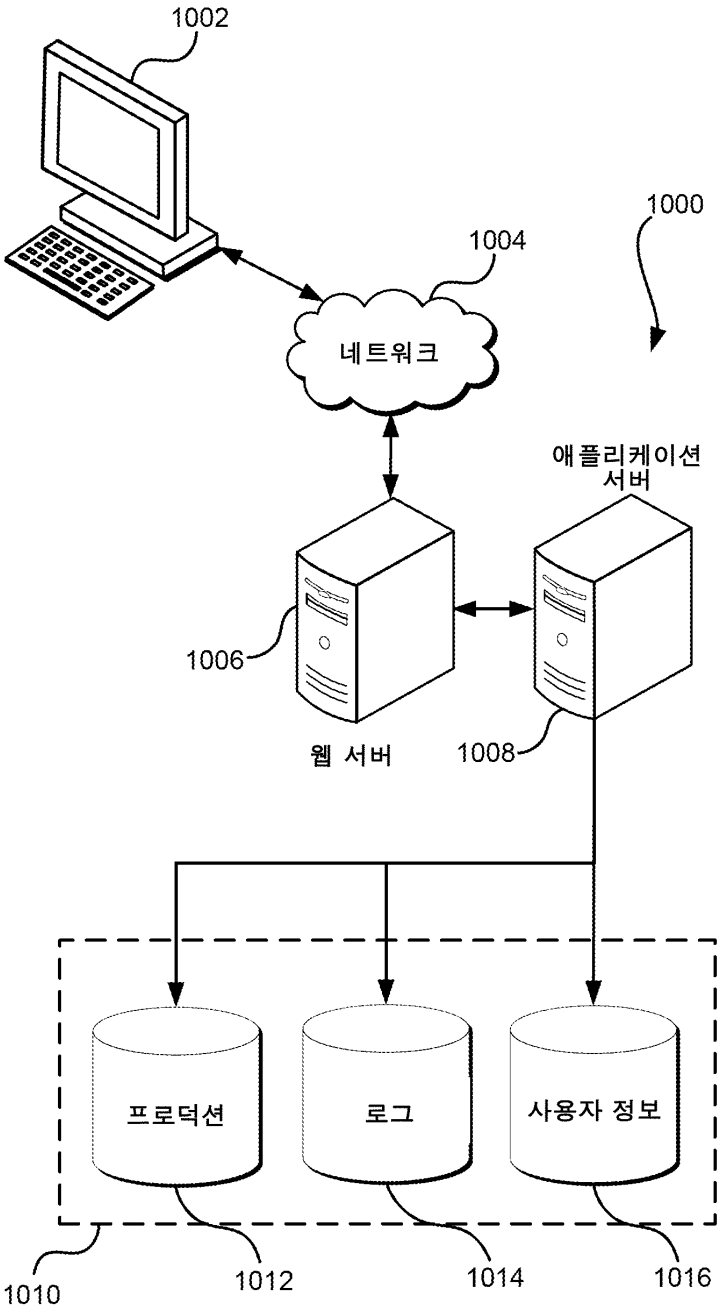
도면8


800
단기 디지털 인증서의 발급에 대한 요청을 수신
802
장기 디지털 인증서 내에 포함된 정보를 검사
804
인증서 유효?
806
아니오
요청 거부
808
예
남아 있는 기간이 충분한가?
810
아니오
예
발급될 단기 디지털 인증서의 유효 기간을 결정
812
단기 디지털 인증서를 발급
814

도면9


900
고객 서버로부터 디지털 인증서를 수신
902
디지털 인증서들 내 확장들을 식별
904
검증 전용 확장?
906
예
고객 서버와의 통신을 종료
908
아니오
고객 서버를 인증하기 위해
계속해서 디지털 인증서를 프로세싱
910

도면10


1002
1000
1004
네트워크
애플리케이션
서버
1006
웹 서버
1008
프로덕션
로그
사용자 정보
1010
1012
1014
1016