



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0036529  
(43) 공개일자 2011년04월07일

(51) Int. Cl.

G06F 21/24 (2006.01) G06Q 50/00 (2006.01)

G06F 21/00 (2006.01)

(21) 출원번호 10-2010-7026838

(22) 출원일자(국제출원일자) 2009년06월01일

심사청구일자 **없음**

(85) 번역문제출일자 2010년11월29일

(86) 국제출원번호 PCT/US2009/045857

(87) 국제공개번호 WO 2009/149019

국제공개일자 2009년12월10일

(30) 우선권주장

12/134,360 2008년06월06일 미국(US)

(71) 출원인

마이크로소프트 코포레이션

미국 위싱턴주 (우편번호 : 98052) 레드몬드 원  
마이크로소프트 웨이

(72) 벌명자

스치넬, 패트릭

미국 98052-6399 위싱턴주 레드몬드 원 마이크로  
소프트 웨이 마이크로소프트 코포레이션 국제 특  
허부 내

알코베, 제임스, 엠.

미국 98052-6399 위싱턴주 레드몬드 원 마이크로  
소프트 웨이 마이크로소프트 코포레이션 국제 특  
허부 내

(74) 대리인

양영준, 백만기

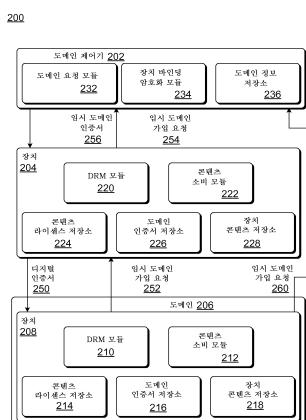
전체 청구항 수 : 총 20 항

(54) 콘텐츠 공유를 위한 임시 도메인 멤버십

### (57) 요 약

하나 이상의 측면들에 따르면, 제1 장치는 제2 장치의 디지털 인증서를 수신한다. 제1 장치는 디지털 서명된 임시 도메인 가입 요청을 생성하고, 이 요청을 도메인 제어기로 보낸다. 도메인 제어기는, 제1 장치를 위하여, 제1 장치가 도메인에 바인딩되어 있는 콘텐츠를 임시로 소비하는 것을 가능하게 해주는 임시 도메인 인증서를 생성한다. 임시 도메인 인증서는 제1 장치로 보내지고, 그에 따라 제1 장치가 도메인에 바인딩되어 있는 콘텐츠를 임시로 소비할 수 있게 된다.

**대 표 도** - 도2



## 특허청구의 범위

### 청구항 1

임시 도메인 멤버십을 허용하는 방법으로서,

제1 장치가 도메인에 임시로 가입하기 위한 요청을 수신하는 단계(602) - 상기 요청은 도메인의 멤버인 제2 장치에 의해 디지털 서명되어 있음 -,

상기 요청이 유효한지 여부를 검사하는 단계(604, 608),

상기 요청이 유효하지 않은 경우, 상기 요청을 거부하는 단계(606),

상기 요청이 유효한 경우,

상기 제1 장치에 대한 임시 도메인 인증서를 생성하는 단계(610) - 상기 임시 도메인 인증서는 상기 제1 장치가 상기 도메인에 임시로 가입할 수 있게 해줌 -, 및

상기 임시 도메인 인증서를 상기 제1 장치로 전송하는 단계(612)를 포함하는 방법.

### 청구항 2

제1항에 있어서, 상기 요청이 유효한지 여부를 검사하는 단계가,

상기 제1 장치의 인증서가 해지되었는지 여부를 검사하는 단계,

상기 요청에 디지털 서명했던 상기 제2 장치로부터의 디지털 서명을 검증하는 단계,

상기 제1 장치의 인증서가 해지되지 않은 경우와 상기 디지털 서명이 검증된 경우 둘다일 때, 요청이 유효한 것으로 결정하는 단계, 및

상기 제1 장치의 인증서가 해지된 경우와 상기 디지털 서명이 검증되지 않은 경우 중 어느 하나 또는 둘 다일 때, 상기 요청이 유효하지 않은 것으로 결정하는 단계를 포함하는 것인 방법.

### 청구항 3

제1항에 있어서, 상기 임시 도메인 인증서가 상기 제1 장치가 멤버로 있는 제2 도메인에 바인딩되어 있는 것인 방법.

### 청구항 4

제1항에 있어서, 상기 임시 도메인 인증서가 상기 제1 장치에 바인딩되어 있는 것인 방법.

### 청구항 5

제1항에 있어서, 상기 요청이 상기 제1 장치의 공개/개인 키 쌍의 공개 키를 포함하고, 상기 제1 장치의 공개 키를 사용하여 암호화된, 도메인의 공개/개인 키 쌍의 도메인 개인 키를 상기 제1 장치로 전송하는 단계를 더 포함하는 방법.

### 청구항 6

제5항에 있어서, 상기 제1 장치의 공개/개인 키 쌍의 공개 키가 상기 요청에 포함되어 있는 디지털 인증서에 포함되어 있고, 상기 디지털 인증서가 상기 제2 장치에 의해 상기 제1 장치로부터 수신되는 것인 방법.

### 청구항 7

제1항에 있어서, 상기 임시 도메인 인증서가 상기 제1 장치가 상기 도메인에 바인딩되어 있는 콘텐츠를 소비할 수 있는 기간을 정의하는 만기를 포함하는 것인 방법.

### 청구항 8

제1항에 있어서, 상기 요청을 수신하는 단계가 상기 제1 장치로부터의 요청을 수신하는 단계를 포함하는 것인

방법.

### 청구항 9

제1항에 있어서, 상기 요청을 수신하는 단계가 상기 제2 장치로부터의 요청을 수신하는 단계를 포함하는 것인 방법.

### 청구항 10

제1항에 있어서, 상기 도메인에 임시 장치들을 추가하는 것에 관한 하나 이상의 조건들을 검사하는 단계, 및 상기 하나 이상의 조건들이 만족되는 경우에만 상기 임시 도메인 인증서를 생성하여 전송하는 단계를 더 포함하는 방법.

### 청구항 11

제10항에 있어서, 상기 하나 이상의 제약조건들이 몇개의 만료되지 않은 임시 도메인 인증서들이 언제라도 발급될 수 있는지에 대한 제한을 포함하는 것인 방법.

### 청구항 12

제1 장치의 하나 이상의 프로세서들에 의해 실행될 때, 상기 하나 이상의 프로세서들로 하여금

제2 장치로부터, 상기 제2 장치의 디지털 인증서 및 디지털 서명된 임시 도메인 가입 요청에 대한 요청을 수신하고(502),

디지털 인증서가 해지되었는지 여부를 검사하며(504),

상기 제1 장치의 사용자가 상기 제1 장치가 멤버로 있는 도메인에 상기 제2 장치가 임시로 가입할 수 있도록 승인하였는지 여부를 검사하고(508),

상기 디지털 인증서가 해지되지 않았고 상기 제1 장치의 사용자가 상기 제2 장치가 상기 도메인에 임시로 가입할 수 있도록 승인한 경우,

상기 제2 장치의 공개 키를 포함하는 임시 도메인 가입 요청을 생성하고 디지털 서명하며(510),

상기 디지털 서명된 임시 도메인 가입 요청을 수신자에게 전송하고(512, 514),

상기 디지털 인증서가 해지되었거나 상기 제1 장치의 사용자가 상기 제2 장치가 상기 도메인에 임시로 가입할 수 있도록 승인하지 않은 경우, 상기 디지털 서명된 임시 도메인 가입 요청에 대한 요청을 거부하게(506) 하는 다수의 명령어들이 저장되어 있는 하나 이상의 컴퓨터 저장 매체.

### 청구항 13

제12항에 있어서, 상기 제2 장치의 디지털 인증서가 상기 제2 장치가 멤버로 있는 제2 도메인에 특유한 디지털 인증서인 하나 이상의 컴퓨터 저장 매체.

### 청구항 14

제12항에 있어서, 상기 제2 장치의 디지털 인증서가 상기 제2 장치에 특유한 디지털 인증서인 하나 이상의 컴퓨터 저장 매체.

### 청구항 15

제12항에 있어서, 상기 수신자가 상기 제2 장치를 포함하는 하나 이상의 컴퓨터 저장 매체.

### 청구항 16

제12항에 있어서, 상기 수신자가 상기 도메인을 관리하는 도메인 제어기를 포함하는 하나 이상의 컴퓨터 저장 매체.

### 청구항 17

제1 장치의 하나 이상의 프로세서들에 의해 실행될 때, 하나 이상의 프로세서들로 하여금

상기 제1 장치를 대신하여 제2 장치가 디지털 서명된 임시 도메인 가입 요청을 생성하도록, 상기 제1 장치의 디지털 인증서를 상기 제2 장치로 전송하고(402),

상기 제2 장치가 멤버로 있는 도메인을 관리하는 도메인 제어기로부터, 상기 제1 장치가 상기 도메인에 임시로 가입하는 것을 가능하게 해주는 임시 도메인 인증서를 수신하게(408) 하는 다수의 명령어들이 저장되어 있는 하나 이상의 컴퓨터 저장 매체.

### 청구항 18

제17항에 있어서, 상기 명령어들이 또한 하나 이상의 프로세서들로 하여금, 상기 제2 장치로 상기 디지털 인증서를 전송한 것에 응답하여, 상기 제2 장치로부터 디지털 서명된 임시 도메인 가입 요청을 수신하고 - 상기 디지털 서명된 임시 도메인 가입 요청은 상기 제2 장치에 의해 디지털 서명되어 있음 -,

상기 디지털 서명된 임시 도메인 가입 요청을 상기 도메인 제어기로 전송하게 하며,

디지털 서명된 임시 도메인 가입 요청에 응답하여, 상기 임시 도메인 인증서가 상기 도메인 제어기로부터 수신되는 것인 하나 이상의 컴퓨터 저장 매체.

### 청구항 19

제18항에 있어서, 상기 제1 장치의 디지털 인증서와 상기 디지털 서명된 임시 도메인 가입 요청 둘 다가 상기 제1 장치의 공개/개인 키 쌍의 공개 키를 포함하고 있으며, 명령어들이 또한 상기 하나 이상의 프로세서들로 하여금, 상기도메인의 공개/개인 키 쌍의 도메인 개인 키를 수신하게 하고, 상기 도메인 개인 키가 상기 제1 장치의 공개/개인 키 쌍의 공개 키를 사용하여 암호화되어 있는 것인 하나 이상의 컴퓨터 저장 매체.

### 청구항 20

제17항에 있어서, 상기 제1 장치의 디지털 인증서가 상기 제1 장치가 멤버로 있는 제2 도메인의 디지털 인증서를 포함하며, 상기 도메인과 상기 제2 도메인이 2개의 서로 다른 도메인인 하나 이상의 컴퓨터 저장 매체.

## 명세서

### 배경기술

[0001] 휴대용 음악 플레이어, 데스크톱 및 랩톱 컴퓨터, 핸드헬드 컴퓨터 또는 PDA(personal digital assistant), 휴대폰 등과 같은 디지털 미디어 재생 장치들이 점점 흔해지고 있다. 이러한 장치들에 있는 디지털 콘텐츠의 예술가 및/또는 저작권 소유자의 권리를 보호하기 위하여, 이러한 장치들은 빈번하게 DRM(digital rights management) 기술들을 이용한다. 그러나, 이러한 DRM 기술들을 이용하는 것은 일반적으로 사용자가 다른 사용자의 장치에서 디지털 콘텐츠를 재생할 수 있는 것을 제한하고 있다. 이것이 문제가 되는데, 그 이유는 사용자들이 자신의 책, CD 및 DVD를 자기의 친구들에게 빌려주는 데 익숙해져 있고 이 DRM 기술들이 일반적으로 사용자들이 구입한 디지털 미디어를 자기의 친구들에게 빌려줄 수 있는 것을 제한하기 때문이다.

### 발명의 내용

#### 과제의 해결 수단

##### 개요

[0003] 이 요약은 이하에서 상세한 설명에 더 기술되는 일련의 개념들을 간략화된 형태로 소개하기 위해 제공된 것이다. 이 요약은 청구된 발명 대상의 주요 특징들 또는 필수적인 특징들을 확인하기 위한 것이 아니며, 청구된 발명 대상의 범위를 제한하는 데 사용되기 위한 것도 아니다.

[0004] 콘텐츠 공유를 위한 임시 도메인 멤버십의 하나 이상의 측면들에 따르면, 제1 장치가 도메인에 임시로 가입하기 위한 요청이 수신되고, 이 요청은 도메인의 멤버인 제2 장치에 의해 디지털 서명되어 있다. 요청이 유효한지 여부에 대한 검사가 이루어진다. 요청이 유효하지 않은 경우, 요청은 거부된다. 그러나, 요청이 유효한 경우, 제1

장치에 대해 임시 도메인 인증서가 생성되어 - 임시 도메인 인증서는 제1 장치가 도메인에 임시로 가입하는 것을 가능하게 해줌 -, 제1 장치로 보내진다.

[0005] 콘텐츠 공유를 위한 임시 도메인 멤버십의 하나 이상의 측면들에 따르면, 제1 장치에서, 제2 장치의 디지털 인증서 및 디지털 서명된 임시 도메인 가입 요청에 대한 요청 둘다가 제2 장치로부터 수신된다. 디지털 인증서가 해지되었는지 여부 및 제1 장치의 사용자가 제1 장치가 멤버로 있는 도메인에 제2 장치가 임시로 가입할 수 있도록 승인하였는지 여부에 대한 검사가 이루어진다. 만일 디지털 인증서가 해지되지 않았고 제1 장치의 사용자가 제2 장치가 도메인에 임시로 가입할 수 있도록 승인하였으면, 제2 장치의 공개 키를 포함하는 임시 도메인 가입 요청이 생성되어 디지털 서명되고, 디지털 서명된 임시 도메인 가입 요청이 수신자에게 보내진다. 그러나, 만일 디지털 인증서가 해지되었거나 제1 장치의 사용자가 제2 장치가 도메인에 임시로 가입할 수 있도록 승인하지 않았으면, 디지털 서명된 임시 도메인 가입 요청에 대한 요청은 거부된다.

[0006] 콘텐츠 공유를 위한 임시 도메인 멤버십의 하나 이상의 측면들에 따르면, 제1 장치는, 제2 장치가 제1 장치를 대신하여 디지털 서명된 임시 도메인 가입 요청을 생성하도록, 제1 장치의 디지털 인증서를 제2 장치로 보낸다. 제1 장치는, 제2 장치가 멤버로 있는 도메인을 관리하는 도메인 제어기(domain controller)로부터, 제1 장치가 도메인에 임시로 가입하는 것을 가능하게 해주는 임시 도메인 인증서를 수신한다.

### 도면의 간단한 설명

[0007] 유사한 특징들을 참조하기 위해 도면 전체에 걸쳐 동일한 번호가 사용된다.

도 1은 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십이 이용될 수 있는 예시적인 시스템을 나타낸 도면.

도 2는 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 구현하는 보다 상세한 예시적인 시스템을 나타낸 도면.

도 3은 하나 이상의 실시예들에 따른 예시적인 임시 도메인 인증서를 나타낸 도면.

도 4는 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 위한 예시적인 프로세스를 나타낸 플로우차트.

도 5는 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 위한 다른 예시적인 프로세스를 나타낸 플로우차트.

도 6은 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 위한 다른 예시적인 프로세스를 나타낸 플로우차트.

도 7은 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 구현하도록 구성될 수 있는 예시적인 컴퓨팅 장치를 나타낸 도면.

### 발명을 실시하기 위한 구체적인 내용

[0008] 콘텐츠 공유를 위한 임시 도메인 멤버십이 본 명세서에 기술되어 있다. 특정 도메인의 멤버가 아닌 제1 장치를 위한 임시 도메인 멤버십이 요청될 수 있다. 특정 도메인의 멤버인 제2 장치는 제1 장치를 대신하여 임시 도메인 가입 요청에 디지털 서명을 하며, 이 요청은 특정 도메인의 도메인 제어기로 보내진다. 도메인 제어기는, 제1 장치가 그 특정 도메인에 임시로 가입하는 것을 가능하게 해주는 임시 도메인 인증서를 제1 장치에게 발급한다.

[0009] 도 1은 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십이 이용될 수 있는 예시적인 시스템(100)을 나타낸 것이다. 시스템(100)은 도메인 제어기(102), 콘텐츠 공급자(104), 라이센스 서버(license server)(106), 하나 이상의(x개) 도메인들[108(1), ..., 108(x)], 하나 이상의(y개) 장치들[110(1), ..., 110(y)] 및 신뢰 기관(trust authority)(120)을 포함한다. 비록 단지 하나의 도메인 제어기(102), 콘텐츠 공급자(104), 라이센스 서버(106) 및 신뢰 기관(120)이 나타내어져 있지만, 구성요소들(102, 104, 106 및 120) 중 다수가 시스템(100)에 포함될 수 있음을 잘 알 것이다.

[0010] 도메인 제어기(102), 콘텐츠 공급자(104), 라이센스 서버(106) 및 신뢰 기관(120) 각각은 하나 이상의 컴퓨팅 장치 상에서 구현될 수 있는 서비스를 나타낸다. 이를 서비스들 중 2개 이상은, 선택적으로, 동일한 컴퓨팅 장치 상에서 구현될 수 있다. 그에 부가하여, 도메인 제어기(102), 콘텐츠 공급자(104), 라이센스 서버(106) 및

신뢰 기관(120) 중 하나 이상이 결합되어 단일 서비스로 될 수 있거나, 또는 다른 대안으로서 각각이 별도의 서비스일 수 있다.

[0011] 이 구성요소들(102, 104, 106, 108, 110, 116, 및 120) 각각은 네트워크(110)를 통해 서로 통신할 수 있다. 네트워크(110)는, 인터넷, LAN(local area network), 휴대폰 또는 기타 무선 전화 네트워크, 기타 공중 및/또는 독점 네트워크, 이들의 조합, 기타 등등과 같은 다양한 네트워크들 중 하나 이상을 포함할 수 있다.

[0012] 각각의 도메인(108)은 장치들[112(1), ..., 112(a) 및 114(1), ..., 114(b)]로 나타낸 하나 이상의 장치들을 포함하고 있다. 도메인에 포함된 이 장치들(112와 114) 각각은 또한 그 도메인의 멤버라고 말해진다. 그에 부가하여, 하나 이상의 디지털 미디어 장치들[116(1), ..., 116(y)]은 임의의 도메인(108)의 일부가 아닐 수도 있다. 장치들(112, 114, 및 116)은 각각, 데스크톱 컴퓨터, 랩톱 컴퓨터, 핸드헬드 컴퓨터 또는 PDA, 자동차 컴퓨터, 휴대용 음악 플레이어, 휴대용 영화 플레이어, 휴대폰 또는 기타 무선 전화 등등과 같은 다양한 서로 다른 유형의 디지털 미디어 장치들일 수 있다. 서로 다른 장치들(112, 114 및 116)이 동일하거나, 다른 대안으로서, 서로 다른 유형의 디지털 미디어 장치일 수 있다.

[0013] 장치들(112, 114 및 116) 각각은 디지털 콘텐츠를 소비할 수 있는 디지털 미디어 장치이다. 본 명세서에서 사용되는 바와 같이, 디지털 콘텐츠는, 오디오 콘텐츠(예를 들어, 노래), 오디오/비디오 콘텐츠(예를 들어, TV 프로그램, 영화, 다큐멘터리, 만화, 기타), 이미지 콘텐츠(예를 들어, 디지털 사진), 그래픽 콘텐츠, 텍스트 콘텐츠(예를 들어, 전자책), 컴파일된 또는 컴파일되지 않은 컴퓨터 프로그램 또는 그 일부분, 자바 게임, zip 압축된(zipped) 또는 다른 방식으로 압축된 파일, 전자메일 메시지 및 첨부 파일 등등은 물론 이들의 조합과 같은 다양한 서로 다른 디지털 또는 전자 콘텐츠를 말하고 있다. 디지털 콘텐츠의 소비는, 디지털 콘텐츠를 재생하는 것, 디지털 콘텐츠를 다른 장치로 전송하는 것, 디지털 콘텐츠를 CD(compact disc) 또는 기타 광 디스크에 굽는 것, 디지털 콘텐츠의 하드 카피를 인쇄하는 것, 디지털 콘텐츠를 전자 메일로 보내는 것 등등과 같은 여러 형태들을 취할 수 있다.

[0014] 각각의 도메인(108)은 특정 사용자 또는 사용자 그룹과 연관되어 있다. 디지털 콘텐츠는 사용자의 도메인과 연관되고(바인딩된다고도 함), 그에 따라 그 사용자의 도메인의 일부인 장치들(112, 114) 중 어떤 것이라도 사용자의 도메인에 바인딩되어 있는 디지털 콘텐츠를 소비할 수 있게 된다. 특정 도메인(108) 내의 서로 다른 장치들(112, 114)은 서로 다른 유형들의 디지털 미디어 장치일 수 있거나, 다른 대안으로서, 장치들(112, 114) 중 하나 이상이 동일한 유형의 장치일 수 있다. 일례로, 사용자는 자신의 데스크톱 컴퓨터, 휴대용 음악 플레이어, 휴대폰 및 자동차 컴퓨터(모두가 사용자의 도메인의 일부임)을 가질 수 있으며, 이 장치들 전부는 사용자의 도메인에 바인딩되어 있는 디지털 콘텐츠를 소비할 수 있다. 특정 장치(112, 114)는 하나 이상의 도메인들(108)의 멤버일 수 있다. 게다가, 도메인(108) 내의 장치들(112, 114)은 그 동일한 도메인 내에 있는 다른 장치들(112, 114)을 알고 있을 필요가 없다는 것에 주목해야 한다.

[0015] 도메인의 일부가 아닌 장치들(116)의 경우, 디지털 콘텐츠는 그 특정 장치(116)와 연관(또는 바인딩)되어 있다. 장치(116)는 장치(116)에 바인딩되어 있는 디지털 콘텐츠를 소비할 수 있다.

[0016] 도메인 제어기(102)는 도메인들(108)을 관리한다. 도메인의 관리는, 도메인에서 멤버십을 관리하는 것 및 도메인의 멤버들에 제한을 부과하는 것(도메인에 장치들을 추가하는 것, 도메인으로부터 장치들을 제거하는 것, 도메인 멤버십 인증서들을 생성하여 배포하는 것, 임시 도메인 인증서들의 생성하여 배포하는 것 등을 포함함)을 말한다. 장치(112, 114)가 도메인에 가입할 때, 장치(112, 114)는 도메인 제어기(102)로부터 그 도메인에 대한 도메인 멤버십 인증서를 제공받는다. 이하에서 상세히 기술하는 바와 같이, 이 도메인 멤버십 인증서는, 콘텐츠 라이센스와 함께, 장치가 그 도메인에 바인딩되어 있는 보호된 콘텐츠를 소비하는 것을 가능하게 해준다. 장치(112, 114, 및/또는 116)는 또한 도메인에 임시로 가입할 수 있고, 이 경우 장치(112, 114, 116)는 도메인 제어기(102)로부터 그 도메인에 대한 임시 도메인 인증서를 제공받는다. 이하에서 상세히 기술하는 바와 같이, 이 임시 도메인 인증서는, 콘텐츠 라이센스와 함께, 장치가 그 도메인에 바인딩되어 있는 콘텐츠를 일시적으로 소비하는 것을 가능하게 해준다.

[0017] 콘텐츠 공급자(104)는 장치들(112, 114 및 116)에게 콘텐츠를 제공한다. 장치들(112, 114 및 116)에게 제공되는 콘텐츠는 일반적으로 보호된 콘텐츠이다. 보호된 콘텐츠는 암호화를 통해 보호되고, 복호화 키들은 보호된 콘텐츠와 연관한 콘텐츠 라이센스에 포함되어 있다. 각각의 콘텐츠 라이센스는 특정 도메인(108) 또는 특정 장치(116)에 바인딩되어 있고, 따라서 이하에서 보다 상세히 기술되는 바와 같이, 콘텐츠 라이센스가 바인딩되어 있는 특정 도메인(108)의 일부인 그 장치를 또는 콘텐츠 라이센스가 바인딩되어 있는 특정 장치만이 콘텐츠를 소비할 수 있다.

- [0018] 라이센스 서버(106)는 장치들(112, 114 및 116)에게 콘텐츠 라이센스를 제공한다. 장치들(112, 114 및 116)이 콘텐츠 공급자(104)로부터 획득한 콘텐츠는 보호되어 있다. 장치들(112, 114 및 116)은 보호된 콘텐츠에 대한 콘텐츠 라이센스를 획득하기 위해 라이센스 서버(106)에 액세스한다. 콘텐츠 라이센스가 특정 도메인 또는 장치에 바인딩될 수 있다.
- [0019] 신뢰 기관(120)은 디지털 인증서를 디지털 서명하여 발급한다. 신뢰 기관(120)은 엔터티로서, 통상적으로 도메인 제어기(102), 콘텐츠 공급자(104) 및 라이센스 서버(106)가 신뢰하고 있는 하나 이상의 컴퓨팅 장치들 상에 구현되는 서비스이다. 신뢰 기관(120)은, 장치들(112, 114 및 116)의 신뢰성(authenticity)을 입증하는 디지털 인증서를 장치들(112, 114 및 116)에게 발급할 수 있는, 신뢰할 수 있는 제3자로서 기능한다. 신뢰기관(120)은 또한, 다른 엔터티(장치 제조업체 등)가 장치들(112, 114 및 116)에게 이러한 디지털 인증서를 발급하는 것을 가능하게 해주는 인증서를 발급할 수 있으며, 그로써 디지털 인증서 발급을 이 다른 엔터티에게 위임할 수 있다.
- [0020] 본 명세서에서는 대칭 키 암호화, 공개 키 암호화 및 공개/개인 키 쌍에 대해 언급하고 있다. 비록 이러한 키 암호화는 당업자들에게 잘 알려져 있더라도, 읽는 사람을 돋기 위하여 이러한 암호화에 대한 간략한 개요가 여기에 포함되어 있다. 공개 키 암호화에서, 엔터티(하드웨어 또는 소프트웨어 구성요소, 장치, 도메인, 기타 등등)는 공개/개인 키 쌍과 관련되어 있다. 공개 키는 공개적으로 이용 가능하도록 되어 있을 수 있지만, 엔터티는 개인 키를 비밀로 유지한다. 개인 키 없이, 공개 키를 사용하여 암호화된 데이터를 복호화하는 것은 계산이 매우 어렵다. 따라서, 데이터가 공개 키를 가진 어떤 엔터티에 의해서라도 암호화될 수 있고, 대응하는 개인 키를 가진 엔터티에 의해서만 복호화될 수 있다. 그에 부가하여, 데이터에 대한 디지털 서명은 데이터와 개인 키를 사용하여 생성될 수 있다. 개인 키 없이, 공개 키를 사용하여 검증될 수 있는 서명을 생성하는 것은 계산이 매우 어렵다. 공개 키를 가진 어떤 엔터티라도, 공개 키를 사용하여 획득한 검증값을 원본 데이터와 비교하여 디지털 서명을 검증하기 위해, 공개 키를 사용할 수 있으며, 만일 2개가 같다면, 누구도 디지털 서명된 데이터를 무단으로 변조하거나 변경하지 않은 것으로 안심할 수 있다.
- [0021] 한편, 대칭 키 암호화에서는, 공유 키가 두 엔터티에게 알려지고 비밀로 유지된다. 공유 키를 가지는 엔터티는 일반적으로 그 공유 키로 암호화된 데이터를 복호화할 수 있다. 공유 키 없이, 공유 키로 암호화된 데이터를 복호화하는 것은 계산이 매우 어렵다. 그래서, 만일 두 엔터티 모두가 공유 키를 알고 있다면, 각각은 상대방에 의해 복호화될 수 있는 데이터를 암호화할 수는 있으나, 만일 다른 엔터티가 공유 키를 알지 못하면, 그 다른 엔터티는 데이터를 복호화할 수 없다.
- [0022] 본 명세서에서는 또한 디지털 인증서에 대해서도 말하고 있다. 디지털 인증서는 당업자들에게 잘 알려져 있다. 그럼에도 불구하고, 읽는 사람에게 도움을 주기 위하여 디지털 인증서에 대한 간략한 개요가 여기에 포함되어 있다. 특정 엔터티의 신뢰성을 입증하는 디지털 인증서는 신뢰 기관에 의해 생성될 수 있다. 디지털 인증서는 일반적으로 생성되는 디지털 인증서를 받을 특정 엔터티의 공개 키를 포함하고 있으며, 디지털 인증서는 신뢰 기관의 개인 키를 이용하여 신뢰 기관에 의해 디지털 서명된다. 엔터티 A가 엔터티 B의 신뢰성을 검증하고자 하는 경우, 엔터티 A는 신뢰 기관(몇몇 실시예에서, 엔터티 A일 수 있음)의 공개 키를 획득하여 엔터티 B의 디지털 인증서의 디지털 서명을 검증할 수 있다. 신뢰 기관이 엔터티 A에 의해 신뢰되고 있기 때문에, 엔터티 B의 디지털 인증서의 디지털 서명이 올바른 것으로 검증되면, 엔터티 B는 신뢰할 수 있는 것으로 검증될 수 있다.
- [0023] 일반적으로, 시스템(100)의 동작 동안에, 장치들은 특정 도메인(108)에 가입하기 위하여 도메인 제어기(102)와 통신할 수 있다. 특정 도메인(108)에 가입할 때, 도메인 제어기(102)는 장치가 도메인(108)에 바인딩되어 있는 콘텐츠를 소비할 수 있게 해준다. 그 도메인(108)에 있는 장치들은 그 도메인(108) 내의 콘텐츠 공급자(104) 또는 다른 장치들(112)(또는 114)로부터 암호화된 콘텐츠를 획득할 수 있고 라이센스 서버(106)로부터 콘텐츠에 대응하는 라이센스를 획득할 수 있다. 라이센스는 특정 도메인(108)에 바인딩되어 있고, 일반적으로 암호화된 콘텐츠를 복호화하는 콘텐츠 키를 포함하고 있다. 특정 도메인(108)의 멤버인 장치들은 그 특정 도메인(108)에 바인딩된 라이센스들로부터 콘텐츠 키들을 복호화할 수 있고, 차례로 암호화된 콘텐츠를 복호화하기 위해 콘텐츠 키를 사용할 수 있다. 이어서, 이러한 장치들은 라이센스에 포함되어 있는 정책들에 따라 콘텐츠를 소비할 수 있다. 특정 도메인(108)에 바인딩되어 있지 않은 장치들은 그 특정 도메인(108)에 바인딩된 라이센스들로부터 콘텐츠 키들을 복호화할 수 없으며, 따라서 암호화된 콘텐츠를 복호화할 수 없다.
- [0024] 그러나, 어떤 환경 하에서는, 그 특정 도메인(108)의 멤버가 아닌 장치가 그 특정 도메인(108)에 대한 임시 도메인 멤버십을 획득할 수 있다. 특정 도메인(108)에 대한 임시 도메인 멤버십을 획득하기 위하여, 특정 도메인

(108)의 멤버는 장치를 대신하여 임시 도메인 가입 요청에 디지털 서명을 하고, 임시 도메인 가입 요청은 장치의 디지털 인증서를 포함한다. 도메인 제어기(102)는 임시 도메인 가입 요청을 수신하고, 임시 도메인 멤버십을 발급할지 여부를 결정한다. 도메인 제어기(102)가 임시 도메인 멤버십을 발급하기로 결정한 경우, 도메인 제어기(102)는 장치에 대한 임시 도메인 인증서를 발급한다. 임시 도메인 인증서는 장치가 특정 도메인(108)에 임시로 가입하는 것을 가능하게 해주며, 그로써 장치는 마치 도메인의 멤버인 것처럼 특정 도메인(108)에 바인딩되어 있는 콘텐츠를 일시적으로 소비할 수 있게 된다. 그러나, 콘텐츠의 이러한 소비는 콘텐츠에 대응하는 라이센스 및/또는 기타 제한들(예를 들어, 임시 도메인 인증서에 포함되어 있는 제한들)에 기초하여 제한될 수 있다. 이러한 제한들은 일반적으로 임시 도메인 멤버십이 유효한 기간을 포함하며, 이 기간은 일반적으로 임시가 아닌 도메인 멤버십의 기간보다 짧다.

[0025] 도 2는 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 구현하는 보다 상세한 예시적인 시스템(200)을 나타낸 것이다. 도 2는, 일례로, 각자가 도 1의 도메인 제어기(102), 장치(116) 및 도메인(108)일 수 있는 도메인 제어기(202), 장치(204) 및 도메인(206)을 나타내고 있다. 이 구성요소들(202, 204 및 206) 간의 통신은 도 1의 네트워크(110)와 같은 네트워크를 통해 수행될 수 있다.

[0026] 도메인(206)은 멤버 장치(208)를 가지고 있는 것으로 나타내어져 있다. 설명의 편의상, 하나의 장치(208)가 도메인(206)의 멤버인 것으로 예시되어 있지만, 도메인(206)이 2개 이상의 장치들(208)을 포함할 수 있다는 것을 잘 알 것이다. 장치(208)는 DRM(digital rights management) 모듈(210), 콘텐츠 소비 모듈(212), 콘텐츠 라이센스 저장소(214), 도메인 인증서 저장소(216), 및 장치 콘텐츠 저장소(218)를 포함하고 있다. 개별적인 것으로 나타내어져 있지만, 다른 대안으로서, 모듈(210), 모듈(212), 저장소(214), 저장소(216) 및 저장소(218) 중 하나 이상이 결합될 수 있다.

[0027] DRM 모듈(210)은 장치(208)에 대한 DRM(digital rights management) 기술들을 구현하고 있다. DRM은 디지털 콘텐츠의 예술가, 출판업자, 및/또는 저작권 소유자의 권리의 보호를 말한다. 콘텐츠 라이센스 및/또는 도메인 또는 장치의 인증서에 포함되어 있는 콘텐츠 사용에 대한 제한들은 DRM 모듈(210)에 의해 시행된다. 일반적으로, DRM은 조건부 액세스, 복사 보호, 콘텐츠 보호, 기타 등등과 같은 콘텐츠의 소비를 제한하는 다양한 기술들을 이용할 수 있다. 이러한 기술들이 구현되는 구체적인 방식은 DRM 시스템에 의해 달라질 수 있다.

[0028] 디지털 콘텐츠는 일반적으로, 적합한 복호화 키(들)이 알려져 있는 경우, 콘텐츠가 알기 쉬운 방식으로 재생만 될 수 있도록 암호화됨으로써 보호된다. DRM 모듈(210)은 언제 콘텐츠를 복호화하는 것을 허용할지를 결정하는 다양한 DRM 기술들을 이용할 수 있으며, 이러한 DRM 기술들은 다양한 서로 다른 방식들로 구현될 수 있다. 일례로, DRM 기술들은 장치(208) 상에서 실행되는 운영 체제 및/또는 기타 소프트웨어들이 신뢰할 수 있다는 점을, 콘텐츠 저작권 소유자 및/또는 콘텐츠 배급업자에 의해 좌우되는 제약 조건이 만족되었다는 점을, 도메인 멤버십 인증서가 유효하다는 점(예를 들어, 만료되지 않음), 기타 등을 포함할 수 있다. 다양한 서로 다른 DRM 기술들이 당업자들에게 알려져 있으며, 이러한 어떠한 기술이라도 DRM 모듈(210)에 의해 사용될 수 있다.

[0029] 장치 콘텐츠 저장소(218)는 도 1의 콘텐츠 공급자(104)와 같은 콘텐츠 공급자로부터 획득된 콘텐츠를 저장하고 있다. 콘텐츠 공급자는 일반적으로 보호된(예를 들어, 암호화된) 콘텐츠를 획득할 수 있는 원격 장치 또는 서비스이다. 다른 대안으로서, 콘텐츠 공급자가 다른 로컬 장치[예를 들어, 도 1의 다른 장치(112, 114, 또는 116)], 로컬 미디어 장치[예를 들어, 컴팩트 디스크(CD) 또는 DVD(digital versatile disc)], 기타 등등일 수 있다. 비록, 다른 대안으로서, 장치 콘텐츠 저장소(218)의 전부 또는 일부가 별도의 장치 상에 구현될 수도 있지만, 장치 콘텐츠 저장소(218)는 일반적으로 장치(208)의 일부로서 구현된다. 그에 부가하여, 장치 콘텐츠 저장소(218)는 적어도 일부가 플레이시 메모리 카드, 휴대용 하드 드라이브, 기타 등등의 이동식 매체 상에 구현될 수 있다.

[0030] 콘텐츠 라이센스 저장소(214)는 콘텐츠 저장소(218)에 있는 보호된 콘텐츠에 대응하는 콘텐츠 라이센스들을 저장하고 있다. 라이센스는 도 1의 라이센스 서버(106)와 같은 라이센스 서버, 또는 다른 대안으로서, 다른 서비스 또는 장치[예를 들어 도 1의 장치(112, 114, 또는 116)]로부터 획득될 수 있다. 콘텐츠 라이센스는 도메인(206)의 멤버들에게만 콘텐츠를 복호화할 수 있게 해줌으로써 특정 콘텐츠를 도메인(206)에 바인딩한다. 하나 이상의 실시예들에서, 이 바인딩은 콘텐츠에 대한 콘텐츠 키(예를 들어 대칭 키)를 도메인(206)의 공개 키로 암호화하고, 암호화된 콘텐츠 키를 라이센스에 포함시킴으로써 달성된다. 도메인(206)의 멤버들이 도메인(206)의 개인 키를 알고 있기 때문에, 이 멤버들은 콘텐츠 키를 복호화할 수 있고, 따라서 콘텐츠도 복호화할 수 있다. 다른 대안으로서, 이러한 바인딩은, 콘텐츠 키를 도메인(206)의 대칭 키로 암호화하는 것, 콘텐츠 키를 장치

(208)의 공개 키로 암호화하는 것, 기타 등등과 같은 다른 방식으로 달성될 수 있다.

[0031] 도메인 인증서 저장소(216)는 장치(208)에게 발급되었던 도메인 인증서를 저장하고 있다. 도메인 인증서는 장치(208)가 콘텐츠 라이센스에 있는 정보에 액세스할 수 있게 해주고, 장치(208)가 관련된 콘텐츠를 소비할 수 있도록 콘텐츠 라이센스로부터 적절한 정보를 추출할 수 있게 해준다. 저장소(216)에 있는 도메인 인증서는, 일례로, 장치(208)의 공개 키로 암호화된 도메인(206)의 개인 키, 또는 장치(208)의 공개 키로 암호화된 다른 도메인[장치(208)가 임시 멤버로 되어 있음]의 개인 키를 포함하고 있다. 장치(208)가 장치(208)의 개인 키를 알고 있기 때문에, 장치(208)는 인증서에 있는 도메인(206)의 개인 키를 복호화할 수 있다. 다른 대안으로서, 이 도메인 키는 대칭 키일 수 있다.

[0032] 장치(208)는 또한 콘텐츠 소비 모듈(212)을 포함하고 있다. 콘텐츠 소비 모듈(212)은 DRM 모듈(210)의 영향을 받는 장치(208) 상의 디지털 콘텐츠에 액세스하고 이 콘텐츠를 소비한다. 콘텐츠 소비 모듈(212)은, 디지털 콘텐츠를 재생하는 것, 디지털 콘텐츠를 다른 장치로 전송하는 것, 디지털 콘텐츠를 CD 또는 기타 광 디스크에 굽는 것, 디지털 콘텐츠의 하드 카피를 인쇄하는 것, 디지털 콘텐츠를 전자메일로 전송하는 것, 기타 등등과 같이, 다양한 서로 다른 종류의 디지털 콘텐츠 소비를 가능하게 해줄 수 있다. 콘텐츠 소비 모듈(212)은 도시된 바와 같이 별도의 모듈일 수 있거나, 다른 대안으로서, 다른 모듈[DRM 모듈(210) 등]에 포함되어 있을 수 있다.

[0033] 장치(208)가 획득한 콘텐츠 중 일부가 보호된 콘텐츠가 아닐 수도 있다는 것에 주목해야 한다. 일례로, 일부 무료로 배포된 콘텐츠가 장치(208)에 의해 획득될 수 있고, 콘텐츠가 아무런 보호 없이 CD로부터 장치(208)로 복사될 수 있으며, 기타 등등이 있을 수 있다. 이러한 보호되지 않은 콘텐츠가 어떻게 처리되는지는, DRM 모듈(210)을 관여시킬 필요 없이, 콘텐츠 소비 모듈(212)에 의해 결정된다.

[0034] 장치(204)는 도메인(206)의 멤버가 아닌 것으로 나타내어져 있다. 장치(204)는 어떤 도메인의 멤버도 아닌 별도의 장치일 수 있거나, 다른 대안으로서, 하나 이상의 도메인들[도메인(206)은 제외]의 멤버일 수 있다. 장치(204)는 장치(208)의 DRM 모듈(210)과 비슷하게 동작하는 DRM 모듈(220)과, 장치(208)의 콘텐츠 소비 모듈(212)과 비슷하게 동작하는 콘텐츠 소비 모듈(222)을 포함하고 있다. 마찬가지로, 장치(204)는 장치(208)의 콘텐츠 라이센스 저장소(214)와 비슷하게 동작하는 콘텐츠 라이센스 저장소(224), 장치(208)의 도메인 인증서 저장소(216)와 비슷하게 동작하는 도메인 인증서 저장소(226), 및 장치(208)의 장치 콘텐츠 저장소(218)와 비슷하게 동작하는 장치 콘텐츠 저장소(228)를 포함하고 있다.

[0035] 도메인 제어기(102)는 도메인 요청 모듈(232), 장치 바인딩 암호화 모듈(234), 및 도메인 정보 저장소(236)를 포함하고 있다. 모듈(232), 모듈(234), 및 저장소(236)는 동일한 장치 상에 구현될 수 있거나, 다른 대안으로서, 다수의 장치들 상에 구현될 수 있다.

[0036] 도메인 요청 모듈(232)은 도메인(206)을 관리하며, 따라서 어느 장치들이 도메인(206)에 가입할 수 있는지를 제어한다. 이러한 관리는 장치들이 도메인(206)에 임시로 가입할 수 있는지 여부를 제어하는 것을 포함한다. 도메인 요청 모듈(232)은 다양한 서로 다른 조건에 기초하여 장치들이 도메인(206)에 가입하는 것을 허용하거나 금지할 수 있다. 이러한 조건들의 일례들은, 몇개의 장치가 도메인(206)에 가입할 수 있는지에 대한 제한들, 어떤 유형들의 장치들[예를 들어, 장치들 상의 DRM 모듈들(210)]이 도메인(206)에 가입할 수 있는지에 대한 제한들, 도메인(206)에 가입하기 위해 장치의 사용자에 의해 제공되어야 하는 사용자 자격증명, 기타 등등을 포함한다. 도메인 요청 모듈(232)은, 몇개의 장치들이 도메인(206)에 임시로 가입할 수 있는지에 대한 제한들, 어떤 유형들의 장치들[예를 들어, 장치들상의 DRM 모듈들(220)]이 도메인(206)에 임시로 가입할 수 있는지에 대한 제한들, 장치의 디지털 인증서가 도메인(206)의 멤버에 의해 디지털 서명되었는지 여부, 기타 등등과 같은, 동일하거나 서로 다른 조건들 중 하나 이상에 기초하여 장치가 도메인(206)에 임시로 가입할 수 있게 해줄 수 있다.

[0037] 도메인 정보 저장소(236)는 도메인 제어기(202)에 의해 관리되는 다양한 도메인들과 관련한 정보를 저장하고 있다. 이 도메인 정보는, 몇개의 장치들이 도메인의 일부일 수 있는지에 대한 제한들을 기술하는 정보, 얼마나 자주 사용자가 장치들을 도메인에 추가할 지에 대한 제한들을 기술하는 정보, 기타 등등과 같이, 장치들이 도메인(206)에 가입할 수 있게 해줄지 여부(일시적으로인지 비일시적으로인지)를 결정할 시에 도메인 요청 모듈(232)에 의해 사용되는 정보를 포함할 수 있다. 이 도메인 정보는 또한, 도메인(206)의 멤버인 각각의 장치에 대한 장치 ID, 도메인(206)과 연관된 권한, 도메인(206)의 공개/개인 키 쌍, 도메인(206)의 멤버인 장치들의 공개 키, 기타 등등을 포함할 수 있다.

[0038] 장치 바인딩 암호화 모듈(234)은 라이센스(따라서, 이상에서 논의된 바와 같이 콘텐츠)를 도메인(206)에 바인딩

하는 도메인 인증서를 생성한다. 도메인 인증서는 서로 다른 방식으로 라이센스를 도메인(206)에 바인딩할 수 있다. 하나 이상의 실시예들에서, 이 바인딩은 장치(208)의 공개 키로 암호화된 적어도 일부분[예를 들어, 도메인(206)의 개인 키]를 포함하는 도메인 인증서를 생성함으로써 달성된다. 다른 대안으로서, 이 바인딩은, 키로 암호화된 적어도 일부분[예를 들어, 도메인(206)의 개인 키]를 포함하는 도메인 인증서를 생성하고 이 키를 도메인 내의 장치에게 안전하게 발급하는 것, 보안 키 교환 프로토콜을 이용하여 도메인 제어기(202)와 도메인(206) 내의 장치 간에 대칭 키를 설정하고 대칭 키로 암호화된 적어도 일부분[예를 들어, 도메인(206)의 개인 키]를 포함하는 도메인 인증서를 생성하는 것, 기타 등등과 같은 다른 방식들로 달성될 수 있다.

[0039] 임시 도메인 멤버십은 사용자가 장치를 자신의 도메인에 임시로 가입시키는 것을 바라는 많은 서로 다른 시나리오들에서 유용하다. 일례로, 사용자는 사용자의 휴대용 장치 상에 있는 영화를 보기로 결정한 친구의 집을 방문할 수 있다. 친구는 영화 재생 장치를 가지고 있지만, 그 장치는 사용자의 휴대용 장치와 동일한 도메인의 멤버가 아니다. 따라서, 본 명세서에서 논의된 콘텐츠 공유를 위한 임시 도메인 멤버십을 사용하여, 친구의 장치는 사용자의 도메인에서의 임시 멤버십을 친구의 장치에게 부여하는 임시 도메인 인증서를 제공받을 수 있다. 이어서, 사용자의 휴대용 장치로부터의 콘텐츠가 친구의 장치에 의해 재생될 수 있고, 따라서 사용자는 자기의 친구와 콘텐츠를 공유할 수 있다.

[0040] 시스템(200)에서, 장치(204)가 도메인(206)의 멤버는 아니지만, 장치(204)는 장치(204)가 도메인(206)에 임시로 가입할 수 있게 해주는 임시 도메인 인증서를 제공받을 수 있다. 이 임시 도메인 인증서를 획득하기 위해, 장치(204)는 장치(204)의 디지털 인증서(250)를 장치(208)와 같은 도메인(206) 내의 장치로 보낸다. 장치(204)의 디지털 인증서(250)는 장치(204)에 특유한 디지털 인증서 또는 장치(204)가 멤버로 있는 다른 도메인[도메인(206) 제외]에 특유한 디지털 인증서일 수 있다.

[0041] 디지털 인증서(250)를 보내는 것은 장치(204)에 의해 또는, 다른 대안으로서, 장치(208)에 의해 시작될 수 있다. 일례로, 장치(204)는 장치(204)가 도메인(206)에 임시로 가입할 수 있도록 요청할 수 있거나, 장치(208)는 장치(204)가 도메인(206)에 임시로 가입할 수 있도록 요청할 수 있다. 이러한 요청이 장치들(204 또는 208) 중 하나의 사용자에 의해 시작될 수 있거나, 다른 대안으로서, 장치들(204 또는 208) 중 하나의 모듈 또는 구성요소에 의해 자동으로 생성될 수 있다.

[0042] 디지털 인증서(250)의 수신 시에, DRM 모듈(210)은, 장치(204)를 대신하여, 임시 도메인 가입 요청을 생성할지 여부를 결정한다. 임시 도메인 가입 요청을 생성할지 여부를 결정할 시에 다양한 다른 조건들이 사용될 수 있다. 하나 이상의 실시예들에서, DRM 모듈(210)은 디지털 인증서(250)가 유효한지 여부를 검사한다. 이러한 실시예들에서, 장치(208)는 해지된 디지털 인증서들의 목록 또는 기타 기록을 유지하거나 그에 액세스한다. DRM 모듈(210)은 디지털 인증서(250)가 이 목록에 있는지, 따라서 해지되었는지 여부를 검사한다. 디지털 인증서(250)가 해지된 경우, DRM 모듈(210)은 임시 도메인 요청을 생성하지 않고, 그렇지 않은 경우, DRM 모듈(210)은 임시 도메인 요청을 생성할 수 있다(선택적으로, 다른 조건이 만족되는지에 따라).

[0043] 하나 이상의 다른 실시예들에서, DRM 모듈(210)은 장치(204)가 도메인(206)에 임시로 가입하는 것을 장치(208)의 사용자가 승인하는지 여부를 검사한다. 이 검사는 디지털 인증서(250)가 유효한지 여부의 검사에 부가하여 또는 그 대신에 수행될 수 있다. 장치(204)가 도메인(206)에 임시로 가입하는 것을 장치(208)의 사용자가 승인하는지 여부에 대한 이 검사는, 장치(204)가 도메인(206)에 임시로 가입하는 것의 승인 또는 거부를 입력하도록 사용자에게 요청하는 프롬프트를 장치(208)의 사용자 인터페이스(UI) 상에 디스플레이하는 것과 같이, 여러 방식으로 수행될 수 있다. 다른 대안으로서, 도메인(206)에 임시로 가입하도록 승인되는 하나 이상의 장치들(또는 사용자들)을 식별해주는 장치(208) 상의 기본 설정(preferences) 또는 옵션들을 사용자가 이미 설정해 두는 것과 같이, 검사가 다른 방식으로 수행될 수 있다. 다른 대안에서, 장치(208)의 사용자는, 장치(204)에게 디지털 인증서(250)를 요청함으로써, 장치(204)가 도메인(206)에 임시로 가입하는 것을 기본적으로 승인한다.

[0044] DRM 모듈(210)이 장치(204)를 대신하여 임시 도메인 가입 요청을 생성하지 않기로 결정하면, 임시 도메인 가입 요청이 생성되지 않으며, 장치(204)는 선택적으로 이 결정을 통보받는다. 그러나, DRM 모듈(210)이 장치(204)를 대신하여 임시 도메인 가입 요청을 생성하기로 결정하면, DRM 모듈(210)은 디지털 인증서(250)를 포함하는 임시 도메인 가입 요청을 생성한다. DRM 모듈(210)은 또한 임시 도메인 가입 요청에 디지털 서명을 하며, 따라서 이하에서 상세히 논의되는 바와 같이, 도메인 제어기(202)는 요청이 도메인(206)의 멤버에 의해 생성되었다는 것을 검증할 수 있다. DRM 모듈(210)은 임시 도메인 가입 요청 전체 또는 다른 대안으로서 요청의 일부만[예를 들어, 적어도 디지털 인증서(250)]에 디지털 서명할 수 있다. DRM 모듈(210)은, 장치(208)의 개인 키, DRM 모듈(210)의 개인 키, 도메인(206)의 개인 키, 기타 등등과 같은 개인 키를 사용하여 임시 도메인 가입 요청(또는

그 일부분)에 디지털 서명할 수 있다.

[0045] 다른 대안으로서, 디지털 인증서(250)의 단지 일부분만이 디지털 서명된 임시 도메인 가입 요청에 포함된다. 일례로, 장치(204)의 공개 키[장치(204)에 특유한 또는 장치(204)가 멤버로 있는 도메인에 특유한 공개 키]가 디지털 인증서(250)로부터 추출되고, 나머지 디지털 인증서(250) 없이, 디지털 서명된 임시 도메인 가입 요청에 포함될 수 있다. 다른 대안으로서, 인증서를 장치(204)[또는 장치(204)가 멤버로 있는 도메인]에 바인딩하는 데 사용될 수 있는, 장치(204)[또는 장치(204)가 멤버로 있는 도메인]와 연관된 다른 키들 또는 메커니즘들이, 디지털 인증서(250) 대신에, 디지털 서명된 임시 도메인 가입 요청에 포함될 수 있다.

[0046] 하나 이상의 실시예들에서, 디지털 서명된 임시 도메인 가입 요청은 임시 도메인 가입 요청(252)이다. 요청(252)은 장치(204)에게 반환되며, 이 장치는 차례로 요청을 임시 도메인 가입 요청(254)으로서 도메인 제어기(202)로 보낸다. 하나 이상의 다른 실시예들에서, 디지털 서명된 임시 도메인 가입 요청은, DRM 모듈(210)이 도메인 제어기(202)로 보내는 임시 도메인 가입 요청(260)이다. 따라서, 디지털 서명된 임시 도메인 가입 요청은, 장치(204)를 통하여나, 장치(208)로부터 직접, 기타 등등과 같은 다른 방식들로, 도메인 제어기(202)로 전달될 수 있다.

[0047] 도메인 제어기(202)는 요청(254) 또는 요청(260)과 같은 임시 도메인 가입 요청들을 수신하고, 도메인 요청 모듈(232)은, 요청에 응답하여, 임시 도메인 인증서(256)를 발급할지 여부를 결정한다. 도메인 요청 모듈(232)은, 몇개의 장치들이 도메인(206)에 임시로 가입할 수 있는지에 대한 제한들, 어떤 유형들의 장치들[예를 들어, 장치들상의 DRM 모듈들(220)]이 도메인(206)에 임시로 가입할 수 있는지에 대한 제한들, 기타 등등과 같은, 하나 이상의 서로 다른 조건들에 기초하여, 임시 도메인 인증서(256)를 발급할지 여부를 결정할 수 있다. 이러한 제한들은, 일례로, 도메인 제어기(202)의 관리자 또는 다른 사용자에 의해 설정될 수 있고, 도메인 정보 저장소(236)에 유지될 수 있다.

[0048] 하나 이상의 실시예들에서, 도메인 제어기(202)는 단지 임계값 개수의 만료되지 않은 임시 도메인 인증서들이 언제라도 발급될 수 있는 것으로 제한되고 있다. 따라서, 임계값 개수의 만료되지 않은 임시 도메인 인증서가 발급된 후에 수신되는 임시 도메인 가입 요청은 도메인 요청 모듈(232)에 의해 거부될 것이다. 발급된 임시 도메인 인증서들 중 하나 이상이 만료되면, 임시 도메인 가입 요청들은 그것에 기초하여 더 이상 거부되지 않을 것이다.

[0049] 하나 이상의 실시예들에서, 임시 도메인 멤버십이 요청되는 도메인은, 임시 도메인 가입 요청에 디지털 서명하는 장치가 멤버로 있는 도메인이다. 이 도메인 멤버는, 일례로, 임시 도메인 가입 요청에 포함된 데이터에 의해, 도메인 정보 저장소(236)에 있는 데이터에 의해, 기타 등등에 의해 식별될 수 있다.

[0050] 임시 도메인 멤버십이 요청되는 도메인을 임시 도메인 가입 요청이 식별해주는 실시예들에서, 임시 도메인 가입 요청 또는 적어도 임시 도메인 가입 요청에 포함된 디지털 인증서(250)가 요청되는 도메인의 멤버에 의해 디지털 서명되었는지 여부를 도메인 요청 모듈(232)이 검사한다. 디지털 서명은 일반적으로 디지털 인증서 또는 디지털 서명을 생성하는 엔터티를 식별해주는 기타 데이터에 동반된다. 도메인(206)의 멤버들의 식별자들이 도메인 정보 저장소(236)에서 유지되기 때문에, 도메인(206)의 멤버에 의해 디지털 서명된 요청이 즉각 확인될 수 있다.

[0051] 디지털 서명이 검증될 수 없는 경우[또는 디지털 서명이 도메인(206)의 멤버가 아닌 장치에 의해 생성된 경우], 도메인 요청 모듈(232)은 임시 도메인 가입 요청을 거부하고, 임시 도메인 인증서(256)를 생성하지 않는다. 이러한 거부의 표시는, 선택적으로, 임시 도메인 가입 요청의 발신자로 반환될 수 있다. 그러나, 디지털 서명이 검증되고 도메인(206)의 멤버인 장치에 의해 생성된 경우, 도메인 요청 모듈(232)은 임시 도메인 인증서(256)를 생성한다(선택적으로, 다른 조건이 만족되는지에 따라).

[0052] 그에 부가하여, 하나 이상의 실시예들에서, 도메인 요청 모듈(232)은 수신된 임시 도메인 가입 요청에 포함된 디지털 인증서(250)가 유효한지 여부를 검사한다. 이 검사는, 이상에서 논의된 바와 같이, DRM 모듈(210)에 의해 수행되는 이러한 검사에 부가하여 또는 그 대신에 수행될 수 있다. 이러한 실시예들에서, 도메인 제어기(202)는 해지된 디지털 인증서들의 목록 또는 기타 기록을 유지하거나 그에 액세스한다. 도메인 요청 모듈(232)은 디지털 인증서(250)가 이 목록에 있는지, 따라서 해지되었는지 여부를 검사한다. 디지털 인증서(250)가 해지된 경우, 도메인 요청 모듈(232)은 임시 도메인 가입 요청을 거부하며, 그렇지 않은 경우, 도메인 요청 모듈(232)은 임시 도메인 인증서(256)를 생성한다(선택적으로, 기타 조건이 만족되는지에 따라).

[0053] 도메인 요청 모듈(232)이, 임시 도메인 가입 요청에 응답하여, 임시 도메인 인증서(256)를 발급하기로

결정하면, 장치 바인딩 암호화 모듈(234)은 임시 도메인 인증서(256)를 생성한다. 장치 바인딩 암호화 모듈(234)은 임시 도메인 인증서(256)를 장치(204)에 바인딩하거나, 다른 대안으로서, 장치(204)가 멤버로 있는 도메인에 바인딩한다. 이상에서 논의된 바와 같이, 장치(208)에 의해 생성된, 디지털 서명된 임시 도메인 가입 요청은 장치(204)의 공개 키 또는 장치(204)[또는 장치(204)가 멤버로 있는 도메인]와 연관된 기타 키 또는 메커니즘을 포함하고 있다. 디지털 서명된 임시 도메인 가입 요청에 포함된 키 또는 기타 메커니즘은 장치 바인딩 암호화 모듈(234)에서 임시 도메인 인증서(256)를 장치(204)[또는 장치(204)가 멤버로 있는 도메인]에 바인딩하는 데 사용된다.

[0054] 하나 이상의 실시예들에서, 암호화 모듈(234)은, 도메인 제어기(202)가 수신한 임시 도메인 가입 요청에 포함된 디지털 인증서(250)를 사용하여, 임시 도메인 인증서(256)를 장치 및/또는 도메인에 바인딩한다. 도메인 제어기(202)가 수신한 임시 도메인 가입 요청에 포함된 디지털 인증서(250)는 장치(204)의 공개 키[장치(204) 또는 장치(204)가 멤버로 있는 도메인에 특유한 공개 키]를 포함하고 있다. 임시 도메인 인증서(256)는 도메인(206)의 개인 키를 포함하고 있으며, 도메인(206)의 적어도 이 개인 키는 장치(204)의 공개 키를 사용하여 암호화되어 있다. 임시 도메인 인증서(256)의 부가적인 부분들이 또한 장치(204)의 공개 키를 사용하여 암호화될 수 있다.

[0055] 장치(204)는 임시 도메인 인증서(256)를 수신하고, 임시 도메인 인증서(256)를 도메인 인증서 저장소(226)에 저장한다. 임시 도메인 인증서(256)는 장치(204)[또는 장치(204)가 멤버로 있는 도메인]에 바인딩되어 있으며, 그로써 장치(204)는 장치(204)의 개인 키[예를 들어, 장치(204)에 특유한 또는 장치(204)가 멤버로 있는 도메인에 특유한 개인 키]를 사용하여 도메인(206)의 개인 키를 복호화하고 따라서 도메인(206)에 바인딩되어 있는 콘텐츠를 소비할 수 있다.

[0056] 다른 대안으로서, 도메인 제어기(202)는, 임시 도메인 인증서(256)에 개인 키를 포함시키는 것보다는, 다른 방식들로 도메인(206)의 개인 키를 장치(204)로 전달할 수 있다. 일례로서, 도메인(206)의 개인 키는 장치(204)[또는 장치(204)가 멤버로 있는 도메인]에 바인딩될 수 있으며, 임시 도메인 인증서(256)와 별도로 장치(204)로 보내진다. 이 바인딩은, 도메인(206)의 개인 키를 장치(204)[또는 장치(204)가 멤버로 있는 도메인]의 공개 키를 사용하여 암호화하는 것, 보안 키 교환 프로토콜을 이용하여 도메인 제어기(202)와 장치(204) 간의 대칭 키를 설정하고 대칭 키를 사용하여 도메인(206)의 개인 키를 암호화하는 것, 기타 등등과 같은 다양한 서로 다른 방식들로 달성될 수 있다.

[0057] 하나 이상의 실시예들에서, 본 명세서에서 논의된 콘텐츠 공유를 위한 임시 도메인 멤버십이 장치(204)와 장치(208) 간의 근접성(proximity)에 대해서는 어떠한 제한도 두지 않는다. 일례로, 장치들(204와 208)은 동일한 방에, 서로 다른 도시에, 서로 다른 국가에, 기타 등등에 위치할 수 있다. 다른 대안으로서, 하나 이상의 실시예들에서, 근접성 제한이 시행될 수 있다. 일례로, DRM 모듈(210)에서 인증서(250)에 디지털 서명할지 여부를 결정할 시에 이용되는 한 조건은 장치(204)가 장치(208)의 근접성 임계값 내에 있는 것이다. 다른 일례로서, 도메인 요청 모듈(232)에서 임시 도메인 인증서(256)를 발급할지 여부를 결정할 시에 이용되는 한 조건은 장치(204)가 장치(208)의 근접성 임계값 내에 있는 것이다.

[0058] 장치들(204 및 208)의 서로에 대한 근접성은 서로 다른 방식들로 식별될 수 있다. 하나 이상의 실시예들에서, 장치들(204 및 208)의 지리적 위치들이 식별되어 근접성을 결정하는 데 사용된다. 이 지리적 위치들은, 장치들(204 및 208)이 위치하는 우편번호(예를 들어, 장치의 사용자에 의해 식별됨)에 기초하여, 장치들(204 및 208)의 전화번호(예를 들어, 장치의 사용자에 의해 식별됨)에 기초하여, 장치들(204 및 208)의 GPS(Global Positioning System) 좌표(예를 들어, 장치에 포함되거나 연결된 GPS 모듈 또는 구성요소에 의해 식별됨)에 기초하여, 장치들(204 및 208)과 통신하고 있는 셀 사이트(cell site) 또는 기지국(base station)(예를 들어, 장치에 내에 있거나 장치에 연결되어 있는 모듈 또는 구성요소에 의해 식별됨)에 기초하여, 기타 등등과 같이 서로 다른 방식으로 식별될 수 있다. 이러한 지리적 위치들이 식별될 수 있고, 장치들의 지리적 위치들 사이의 거리가 계산될 수 있으며, 이 거리가 임계값 미만인지 여부에 대한 검사가 행해질 수 있다.

[0059] 다른 대안으로서, 장치들(204 및 208)의 근접성이 다른 방식으로 확인될 수 있다. 일례로, 장치들(204와 208)이 특정의 프로토콜들 또는 기술들을 사용하여 통신하고 있는 경우, 장치들(204와 208)이 서로 근접성 임계값 내에 있는 것으로 가정될 수 있다. 이러한 프로토콜들 및 기술들의 일례로서, 장치들(204 및 208)이 적외선(IR, infrared) 연결을 사용하여, 전용 유선 연결을 사용하여, 무선 USB(Wireless USB) 연결을 사용하여, 몇몇 다른 개인 영역 네트워크(PAN, personal area network) 통신 프로토콜을 통하여, 기타 등등으로 서로 통신하고 있는 경우, 장치들(204 및 208)은 서로 근접성 임계값 내에 있는 것으로 가정될 수 있다.

[0060] 도 3은 하나 이상의 실시예들에 따른 임시 도메인 인증서(300)의 일례를 나타내고 있다. 임시 도메인 인증서

(300)는, 일례로, 도 2의 임시 도메인 인증서(256)일 수 있다. 임시 도메인 인증서(300)는 다수의 필드들 또는 부분들, 즉 장치 ID(302), 도메인 ID(304), 도메인 개인 키(306), 도메인 인증서(308), 무결성 검증값(310), 권한 목록(312), 및 만기(314)를 포함하고 있다. 임시 도메인 인증서(300)는 특정의 장치 및/또는 특정의 도메인[예를 들어, 도 2의 장치(204) 및/또는 장치(204)가 멤버로 있는 도메인]에 바인딩되어 있다.

[0061] 장치 ID(302)는 임시 도메인 인증서(300)가 바인딩되어 있는 장치[예를 들어, 도 2의 장치(204)], 또는 다른 대안으로서, 임시 도메인 인증서(300)가 바인딩되어 있는 도메인[예를 들어, 도 2의 장치(204)가 멤버로 있는 도메인]의 식별자이다. 이 식별자는 수신된 임시 도메인 가입 요청에 응답하여 임시 도메인 인증서(300)를 생성하는 모듈 또는 구성요소에 의해 수신될 수 있다. 도메인 ID(304)는 임시 멤버십을 위한 임시 도메인 인증서(300)가 주어지는 도메인[예를 들어, 도 2의 도메인(206)]의 식별자이다.

[0062] 도메인 개인 키(306)는 도메인 ID(304)에 의해 식별되는 도메인의 공개/개인 키 쌍의 개인 키이다. 각각의 도메인은 그 자신의 공개/개인 키 쌍을 가지며, 이 키 쌍은, 일례로, 도 2의 도메인 정보 저장소(236)에 저장될 수 있다. 도메인 개인 키(306)는 임시 도메인 인증서(300)에 암호화되어 있다. 임시 도메인 인증서의 하나 이상의 부분들이 또한 선택적으로 암호화될 수 있다.

[0063] 도메인 인증서(308)는 도메인 ID(304)에 의해 식별되는 도메인과 연관된 디지털 인증서이다. 이 디지털 인증서는, 도메인의 공개/개인 키 쌍의 공개 키와 같이 도메인을 기술하는 다양한 정보들을 포함할 수 있으며, 도메인 제어기(202)의 개인 키를 사용하여 [예를 들어, 도 2의 장치 바인딩 암호화 모듈(234)에 의해] 디지털 서명된다. 이 디지털 서명에 의해, 다른 모듈 또는 구성요소는, 원하는 경우, 인증서가 실제로 도메인 제어기(202)에 의해 생성되었고 변조되지 않았다는 것을 검증할 수 있다.

[0064] 무결성 검증값(310)은 임시 도메인 인증서(300)의 무결성을 검증하는 데 사용될 수 있는 값이다. 이 값은, 임시 도메인 인증서(300)의 부분들[선택적으로, 값(310) 제외]에 대한 체크섬(checksum), 임시 도메인 인증서(300)의 하나 이상의 부분들[선택적으로, 값(310) 제외]에 대한 디지털 서명, 기타 등등과 같은 다양한 서로 다른 검증 기술들에 따라 생성될 수 있다.

[0065] 권한 목록(312)은 임시 도메인 인증서(300)에 의해 부여된 임시 도메인 멤버십에 대한 권한들 및/또는 제한들의 집합이다. 이상에서 논의된 바와 같이, 콘텐츠 소비에 대한 다양한 제한들이 도메인의 멤버들에게 부과될 수 있으며, 그러한 제한들이 권한 목록(312)에서 식별될 수 있다. 재생은 허용하지만 CD에 복사하거나 굽는 것은 허용하지 않는 것, 콘텐츠가 오직 한번만 재생되거나 전자메일로 전송될 수 있게 하는 것, 도메인에서의 임시 멤버십을 얻기 위한 기타 장치들을 대신해서 장치가 디지털 서명된 임시 도메인 멤버십 요청을 생성하는 것을 허용하지 않는 것, 기타 등등과 같은 부가적인 제한들이 임시 도메인 멤버십을 부여받은 멤버들에게 선택적으로 부과될 수 있다.

[0066] 다른 대안으로서, 또는 권한 목록(312)에 부가하여, 임시 도메인 인증서(300)에 의해 부여되는 임시 도메인 멤버십에 대한 권한들 및/또는 제한들을 설정하는 데 기타 메커니즘들이 사용될 수 있다. 일례로, 이러한 권한들 및/또는 제한들은, 선택적으로, 장치의 DRM 모듈[예를 들어, 도 2의 DRM 모듈(220)]에 포함될 수 있다.

[0067] 만기(314)는 임시 도메인 인증서(300)가 사용될 수 있는 기간을 나타낸다. 만기(314)는 일반적으로 임시 도메인 인증서(300)가 만료되어 관련 콘텐츠를 소비하기 위해 콘텐츠 라이센스들로부터 정보를 추출하는 데 더 이상 사용될 수 없는 날짜 및/또는 시간을 포함한다. 다른 대안으로서, 임시 도메인 인증서(300)는 관련된 발급 날짜 및/또는 시간[임시 도메인 인증서(300)의 일부로서 포함되거나, 다른 대안으로서, 별도로 유지됨]을 가질 수 있으며, 만기(314)는, 임시 도메인 인증서(300)의 발급 날짜 및/또는 시간 이후 관련 콘텐츠를 소비하기 위해 콘텐츠 라이센스로부터의 정보를 추출하는 데 인증서(300)가 사용될 수 있는 기간을 나타내는 기간일 수 있다. 이상에서 논의된 바와 같이, 만료되지 않는 동안, 임시 도메인 인증서(300)는 콘텐츠 키를 복호화하기 위하여 장치[예를 들어, 도 2의 장치(204)]에 의해 사용될 수 있다. 만료된 후에, 임시 도메인 인증서는 콘텐츠 키를 복호화하기 위하여 장치에 의해 사용될 수 없다[예를 들어, 장치의 DRM 모듈은 임시 도메인 인증서(300)가 만료되었음을 인식할 것이며, 콘텐츠 키를 복호화하는 데 인증서(300)를 사용하지 않을 것이다].

[0068] 도 4는 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 예시적인 프로세스(400)를 나타낸 플로우차트이다. 프로세스(400)는, 도 2의 장치(204)와 같은, 도메인에서 임시 멤버십을 얻고자 하는 장치에 의해 수행되며, 소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합으로 구현될 수 있다. 프로세스(400)는 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 예시적인 프로세스이며, 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 부가적인 논의는 다른 도면들을 참조하여 본 명세서에 포함되어 있다.

- [0069] 처음에, 도메인 내의 임시 멤버십을 얻으려고 하는 장치의 디지털 인증서가, 임시 멤버십을 얻으려고 하는 도메인의 멤버로 전송된다[동작(402)]. 이상에서 논의된 바와 같이, 이 인증서는 장치에 특유한 인증서이거나, 다른 대안으로서, 프로세스(400)를 구현하는 장치가 멤버로 있는 도메인에 특유한 인증서일 수 있다.
- [0070] 동작(402)에서의 인증서의 전송은 프로세스(400)를 구현하는 장치에 의해, 또는 다른 대안으로서, 인증서를 전송받을 도메인의 멤버로부터의 요청에 응답하여 시작될 수 있다. 일례로, 프로세스(400)를 구현하는 장치의 사용자에게 UI가 디스플레이될 수 있고, 그에 따라 사용자가 임시 도메인 멤버십에 대한 요청을 입력할 수 있으며, 이로부터 사용자는 그 도메인에 있는 장치 상의 특정 콘텐츠에 대한 요청을 입력할 수 있고, 기타 등을 할 수 있다. 다른 일례로, 인증서를 전송받을 장치의 사용자에게 UI가 디스플레이될 수 있고, 그에 따라 프로세스(400)를 구현하는 장치가 임시 도메인 멤버십을 부여받아야 한다는 요청, 프로세스(400)를 구현하는 장치로 특정 콘텐츠가 전송되어야 한다는 요청, 기타 등의 요청을 사용자가 입력할 수 있게 된다.
- [0071] 하나 이상의 실시예들에서, 이상에서 논의한 바와 같이, 동작(402) 후에, 디지털 서명된 임시 도메인 가입 요청이 도메인 멤버로부터 수신되고[동작(404)], 도메인 제어기로 전송된다[동작(406)]. 다른 대안으로서, 도메인 멤버가 프로세스(400)를 구현하는 장치를 대신하여 디지털 서명된 임시 도메인 가입 요청을 생성하지 않기로 결정하는 경우, 또는 이상에서 논의된 바와 같이 디지털 서명된 임시 도메인 가입 요청이 도메인 멤버에 의해 도메인 제어기로 전송되는 경우, 이러한 요청이 수신될 수 없다.
- [0072] 디지털 서명된 임시 도메인 가입 요청이 도메인 제어기로 전송되는 방식에 관계없이, 그 요청의 전송 이후에, 도메인 멤버가 멤버로 있는 도메인에 대한 임시 도메인 인증서가 수신된다[동작(408)]. 이 도메인에 대한 도메인 키는 임시 도메인 인증서에 포함되어 있으며, 도메인 멤버의 도메인에 바인딩되어 있는 콘텐츠를 소비하는데 사용된다 [동작(410)]. 이상에서 논의된 바와 같이, 하나 이상의 실시예들에서, 이 도메인 키는 콘텐츠를 복호화하기 위해 콘텐츠 키를 복호화하는 데 사용될 수 있다. 이 소비는, 콘텐츠와 연관된 하나 이상의 라이센스들에 따라, 임시 도메인 인증서가 만료될 때까지 계속될 수 있다.
- [0073] 도메인 제어기가, 임시 도메인 가입 요청에 응답하여, 임시 도메인 인증서를 발급하기로 결정하는 경우, 임시 도메인 인증서가 프로세스(400)를 구현하는 장치에 의해 수신된다는 것에 주목해야 한다. 도메인 제어기가, 임시 도메인 가입 요청에 응답하여, 임시 도메인 인증서를 발급하지 않기로 결정하는 경우, 이러한 인증서가 동작(408)에서 수신되지 않고 동작(410)에서 사용되지 않는다.
- [0074] 도 5는 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 예시적인 프로세스(500)를 나타낸 플로우차트이다. 프로세스(500)는, 도 2의 장치(208)와 같은, 도메인의 멤버인 장치에 의해 수행되며, 소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합으로 구현될 수 있다. 프로세스(500)는 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 예시적인 프로세스이며, 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 부가적인 논의는 다른 도면들을 참조하여 본 명세서에 포함되어 있다.
- [0075] 처음에, 장치의 디지털 인증서가, 디지털 서명된 임시 도메인 가입 요청에 대한 요청과 함께, 요청측 장치로부터 수신된다[동작(502)]. 인증서와 요청이 별도로 있을 수 있거나, 다른 대안으로서, 요청이 내재되어 있을 수 있다. 일례로, 프로세스(500)를 구현하는 장치에 의한 인증서 요청에 응답하여 인증서가 수신될 수 있고, 이 경우 디지털 서명된 임시 도메인 가입 요청에 대한 요청은 바로 그 인증서의 수신에 내재되어 있을 수 있다. 그에 부가하여, 이상에서 논의된 바와 같이, 요청측 장치에 대한 인증서는 요청측 장치에 특유한 것이거나 요청측 장치가 멤버로 있는 도메인에 특유한 것일 수 있다.
- [0076] 이어서, 동작(502)에서 수신된 요청측 장치의 디지털 인증서가 유효한지 여부에 대한 검사가 이루어진다[동작(504)]. 유효성에 대한 이 검사는, 이상에서 논의된 해지 목록 또는 기록의 검사와 같이, 서로 다른 방식들로 수행될 수 있다. 동작(502)에서 수신된 인증서가 디지털 서명되어 있는 경우, 유효성에 대한 이 검사는 또한 인증서의 디지털 서명을 검증하는 것을 포함할 수 있다. 다른 대안으로서, 동작(504)이 수행되지 않을 수 있다. 이상에서 논의된 바와 같이, 장치의 디지털 인증서는 장치에 특유한 것이거나 장치가 멤버로 있는 도메인에 특유한 것일 수 있다.
- [0077] 요청측 장치의 디지털 인증서가 유효하지 않은 경우, 동작(502)에서 수신된 요청이 거부된다[동작(506)]. 이 거부의 표시는, 선택적으로, 요청측 장치에게 반환될 수 있다.
- [0078] 그러나, 장치의 디지털 인증서가 유효한 경우, 프로세스(500)를 구현하는 장치의 사용자가 요청측 장치가 도메인에 임시로 가입하는 것을 승인할지 여부에 대한 검사가 이루어진다[동작(508)]. 이상에서 논의된 바와 같이, 사용자 승인의 결정은 다양한 서로 다른 방식들로 수행될 수 있다. 다른 대안으로서, 동작(508)이 수행되지 않

을 수 있다.

[0079] 요청측 장치가 도메인에 임시로 가입할 수 있게 해주는 것을 사용자가 승인하지 않는 경우, 동작(502)에서 수신된 요청이 거부된다[동작(506)]. 이 거부의 표시는, 선택적으로, 요청측 장치에게 반환될 수 있다.

[0080] 그러나, 요청측 장치가 도메인에 임시로 가입하는 것을 사용자가 승인하는 경우, 요청측 장치의 키를 포함하는 디지털 서명된 임시 도메인 가입 요청이 생성된다[동작(510)]. 하나 이상의 실시예들에서, 이 디지털 서명된 임시 도메인 가입 요청은 [동작(502)에서 수신된 디지털 인증서로부터의] 요청측 장치의 공개 키를 포함한다. 디지털 서명된 임시 도메인 가입 요청은 동작(502)에서 수신된 요청측 장치의 인증서(요청측 장치의 공개 키를 포함함), 또는, 다른 대안으로서, 임시 도메인 인증서가 요청측 장치에 바인딩될 수 있게 해주는 몇몇 다른 키 또는 메커니즘을 포함할 수 있다.

[0081] 디지털 서명된 임시 도메인 가입 요청이 요청측 장치 또는 도메인 제어기와 같은 수신자로 전송된다. 하나 이상의 실시예들에서, 디지털 서명된 임시 도메인 가입 요청이 요청측 장치에게 반환된다[동작(512)]. 디지털 서명된 임시 도메인 가입 요청을 요청측 장치로 전송하는 대신에, 또는, 다른 대안으로서, 디지털 서명된 임시 도메인 가입 요청을 요청측 장치로 전송하기는 것에 부가하여, 디지털 서명된 임시 도메인 가입 요청이 도메인 제어기로 전송된다[동작(514)].

[0082] 도 6은 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 예시적인 프로세스(600)를 나타낸 플로우차트이다. 프로세스(600)는 도 2의 도메인 제어기(202) 등의 도메인 제어기에 의해 수행되고, 소프트웨어, 펌웨어, 하드웨어, 또는 이들의 조합으로 구현될 수 있다. 프로세스(600)는 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 예시적인 프로세스이며, 콘텐츠 공유를 위한 임시 도메인 멤버십에 대한 부가적인 논의는 다른 도면들을 참조하여 본 명세서에 포함되어 있다.

[0083] 처음에, 디지털 서명된 임시 도메인 가입 요청이 수신된다[동작(602)]. 이어서, 임시 도메인 가입 요청 상의 디지털 서명이 유효한지 여부에 대한 검사가 이루어진다[동작(604)]. 임시 도메인 가입 요청 상의 디지털 서명이 검증될 수 있다면, 임시 도메인 가입 요청 상의 디지털 서명은 유효하다. 임시 도메인 가입 요청 상의 디지털 서명이 유효하지 않은 경우, 임시 도메인 가입 요청이 거부된다[동작(606)]. 이 거부의 표시는, 선택적으로, 동작(602)에서 수신된 요청을 보낸 장치에게 반환될 수 있다.

[0084] 그러나, 임시 도메인 가입 요청 상의 디지털 서명이 검증되는 경우, 임시 도메인 가입 요청에 포함된 인증서(또는 키 또는 기타 메커니즘)가 유효한지 여부에 대한 검사가 이루어진다[동작(608)]. 유효성에 대한 이 검사는, 이상에서 논의된 해지 목록 또는 다른 기록의 검사와 같이, 서로 다른 방식들로 수행될 수 있다. 다른 대안으로서, 동작(608)이 수행되지 않을 수 있다(예를 들어, 이상에서 논의된 바와 같이, 임시 도메인 가입 요청에 디지털 서명한 장치에 의해 유효성 검사가 이미 수행된 경우).

[0085] 임시 도메인 가입 요청에 포함된 인증서(또는 키 또는 기타 메커니즘)가 유효하지 않은 경우, 임시 도메인 가입 요청이 거부된다[동작(606)]. 이 거부의 표시는, 선택적으로, 동작(602)에서 수신된 요청을 보낸 장치에게 반환될 수 있다.

[0086] 그러나, 임시 도메인 가입 요청에 포함된 인증서(또는 키 또는 기타 메커니즘)가 유효한 경우, 임시 도메인 가입 요청에 포함되어 있는 인증서에 포함된 공개 키에 바인딩되어 있는 임시 도메인 인증서가 생성된다[동작(610)]. 선택적으로, 이상에서 논의된 바와 같이, 임시 도메인 인증서가 생성되기 위해서는, 하나 이상의 다른 조건이 또한 만족될 필요가 있다. 이상에서 논의된 바와 같이, 이 임시 도메인 인증서는 특정의 장치에 또는 특정의 도메인에 바인딩되어 있을 수 있다. 이어서, 생성된 임시 도메인 인증서가 임시 도메인 멤버십을 요청하고 있는 장치로 전송된다[동작(612)]. 이 임시 도메인 인증서는 임시 도메인 가입 요청에 디지털 서명했던 장치가 멤버로 있는 도메인에 대한 것이다.

[0087] 도 7은 하나 이상의 실시예들에 따른, 콘텐츠 공유를 위한 임시 도메인 멤버십을 구현하도록 구성될 수 있는 예시적인 컴퓨팅 장치(700)를 나타낸 것이다. 컴퓨팅 장치(700)는, 일례로, 도 1의 장치(112, 114, 또는 116), 도 2의 장치(204 또는 208)일 수 있거나, 도 1의 도메인 제어기(102) 또는 도 2의 도메인 제어기(202), 도 1의 콘텐츠 공급자(104), 도 1의 라이센스 서버(106), 또는 도 1의 신뢰 기관(120)의 적어도 일부분을 구현할 수 있다.

[0088] 컴퓨팅 장치(700)는 하나 이상의 프로세서들 또는 처리 장치들(702), 하나 이상의 메모리 및/또는 저장 구성요소들(706)을 포함할 수 있는 하나 이상의 컴퓨터-판독가능 매체(704), 하나 이상의 입/출력(I/O) 장치들(708), 및 다양한 구성요소들 및 장치들이 서로 통신할 수 있게 해주는 버스(710)를 포함한다. 컴퓨터-판독가능 매체

(704) 및/또는 하나 이상의 I/O 장치(들)(708)는 컴퓨팅 장치(700)의 일부로서 포함될 수 있거나, 다른 대안으로서 컴퓨팅 장치(700)에 결합되어 있을 수 있다. 버스(710)는 메모리 버스 또는 메모리 제어기, 주변 장치 버스, AGP(accelerated graphics port), 및 각종의 서로 다른 버스 아키텍처들을 사용하는 프로세서 또는 로컬 버스, 기타 등을 비롯한 몇가지 유형의 버스 구조들 중 하나 이상을 나타낸다. 버스(710)는 유선 버스 및/또는 무선 버스를 포함할 수 있다.

[0089] 메모리/저장 구성요소(706)는 하나 이상의 컴퓨터 저장 매체를 나타낸다. 구성요소(706)는 휘발성 매체 [RAM(random access memory) 등] 및/또는 비휘발성 매체[ROM(read only memory), 플래시 메모리, 광 디스크, 자기 디스크, 기타 등등]를 포함할 수 있다. 구성요소(706)는 고정식 매체(fixed media)(예를 들어, RAM, ROM, 고정식 하드 드라이브, 기타)는 물론 이동식 매체(예를 들어, 플래시 메모리 드라이브, 이동식 하드 드라이브, 광 디스크, 기타)도 포함할 수 있다.

[0090] 본 명세서에 기술된 기법들이 소프트웨어로 구현될 수 있고, 명령어들이 하나 이상의 처리 장치들(702)에 의해 실행된다. 서로 다른 명령어들이 컴퓨팅 장치(700)의 서로 다른 구성요소들에[처리 장치(702)에, 처리 장치(702)의 다양한 캐시 메모리들에, 장치(700)의 기타 캐시 메모리들(도시 생략)에, 기타 컴퓨터-판독가능 매체상에, 기타 등등에] 저장될 수 있다는 것을 잘 알 것이다. 그에 부가하여, 컴퓨팅 장치(700)에서 명령어들이 저장되는 위치가 시간에 따라 변할 수 있다는 것을 잘 알 것이다.

[0091] 하나 이상의 입/출력 장치들(708)에 의해 사용자는 컴퓨팅 장치(700)에 명령 및 정보를 입력할 수 있고 또한 정보가 사용자 및/또는 기타 구성요소들 또는 장치들에 제시될 수 있다. 입력 장치의 일례로는 키보드, 커서 제어장치(예를 들어, 마우스), 마이크, 스캐너, 기타 등등이 있다. 출력 장치들의 일례로는 디스플레이 장치(예를 들어, 모니터 또는 프로젝터), 스피커, 프린터, 네트워크 카드, 기타가 있다.

[0092] 다양한 기법들이 일반적으로 소프트웨어 또는 프로그램 모듈들과 관련하여 본 명세서에 기술되어 있을 수 있다. 일반적으로, 소프트웨어는 특정의 작업들을 수행하거나 특정의 추상 데이터 유형들을 구현하는 루틴, 프로그램, 개체, 구성요소, 데이터 구조, 기타 등을 포함한다. 이 모듈들 및 기법들의 구현은 어떤 형태의 컴퓨터-판독가능 매체 상에 저장되거나 그 매체를 통해 전송될 수 있다. 컴퓨터-판독가능 매체는 컴퓨팅 장치에 의해 액세스될 수 있는 이용가능한 매체 또는 매체들이라면 어느 것이라도 될 수 있다. 제한이 아닌 예로서, 컴퓨터-판독가능 매체는 "컴퓨터 저장 매체" 및 "통신 매체"를 포함할 수 있다.

[0093] "컴퓨터 저장 매체"는 컴퓨터-판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등의 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 저장 매체로는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital versatile disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 원하는 정보를 저장하는 데 사용될 수 있고 또 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체가 있지만, 이들로 제한되지 않는다.

[0094] "통신 매체"는 통상적으로 컴퓨터-판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터를 반송과 또는 기타 전송 메카니즘 등의 피변조 데이터 신호에 구현한다. 통신 매체는 또한 모든 정보 전달 매체를 포함한다. "피변조 데이터 신호"라는 용어는 신호의 특성을 중 하나 이상이 정보를 그 신호에 인코딩하는 방식으로 설정 또는 변경된 신호를 의미한다. 제한이 아닌 예로서, 통신 매체는 유선 네트워크 또는 직접 배선 연결(direct-wired connection) 등의 유선 매체와, 음향, RF, 적외선 및 기타 무선 매체 등의 무선 매체를 포함한다. 상기한 것들의 임의의 것의 조합도 역시 컴퓨터-판독가능 매체의 범위 내에 포함된다.

[0095] 일반적으로, 본 명세서에 기술되는 기능들 또는 기법들 중 어느 것이라도 소프트웨어, 펌웨어, 하드웨어(예를 들어, 고정 논리 회로), 수동 처리, 또는 이 구현들의 조합을 사용하여 구현될 수 있다. "모듈"이라는 용어는, 본 명세서에서 사용되는 바와 같이, 일반적으로 소프트웨어, 펌웨어, 하드웨어, 또는 이들의 조합을 나타낸다. 소프트웨어 구현의 경우에, 모듈, 기능, 논리는 프로세서(예를 들어, CPU 또는 CPU들) 상에서 실행될 때 지정된 작업들을 수행하는 프로그램 코드를 나타낸다. 프로그램 코드는 하나 이상의 컴퓨터-판독가능 메모리 장치들에 저장될 수 있으며, 이들에 대한 추가적인 설명은 도 7과 관련하여 찾아볼 수 있다. 본 명세서에 기술된 콘텐츠 공유를 위한 임시 도메인 멤버십 기법들의 특징들이 플랫폼-독립적(platform-independent)이며, 이는 그 기법들이 각종의 프로세서들을 갖는 각종의 상용 컴퓨팅 플랫폼들에서 구현될 수 있다는 것을 의미한다.

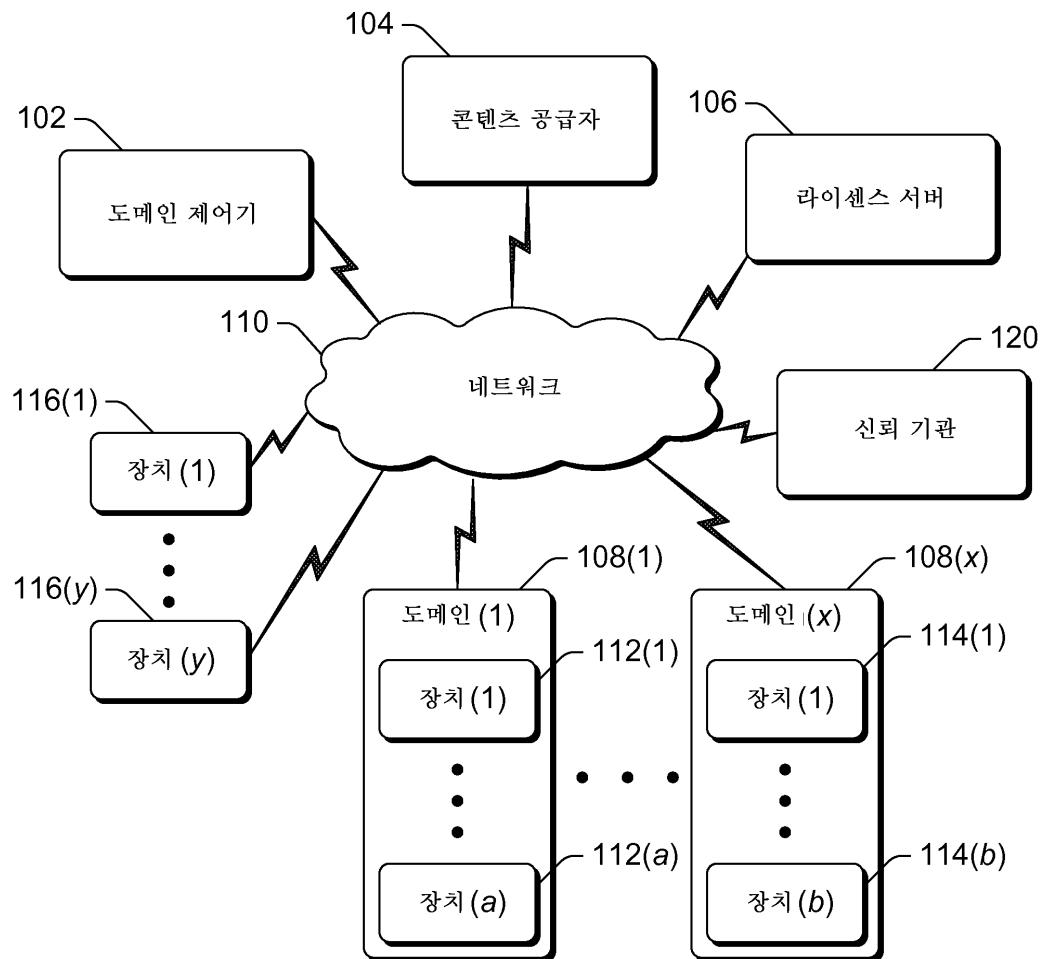
[0096] 발명 대상이 구조적 특징들 및/또는 방법적 동작들과 관련하여 기술되어 있지만, 첨부된 특허청구범위에 정의된 발명 대상이 이상에서 기술한 특정의 특징들 또는 동작들로 반드시 제한되는 것은 아니라는 것을 잘 알 것이다.

오히려, 이상에서 기술한 특정의 특징들 및 동작들은 청구항들을 구현하는 예시적인 형태로서 개시되어 있다.

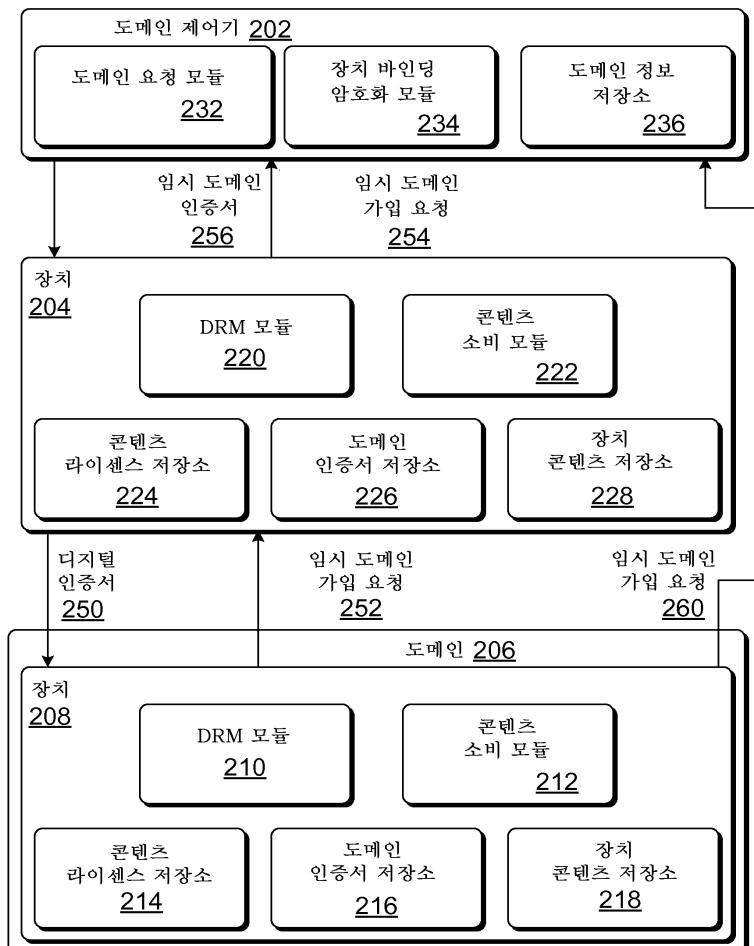
## 도면

### 도면1

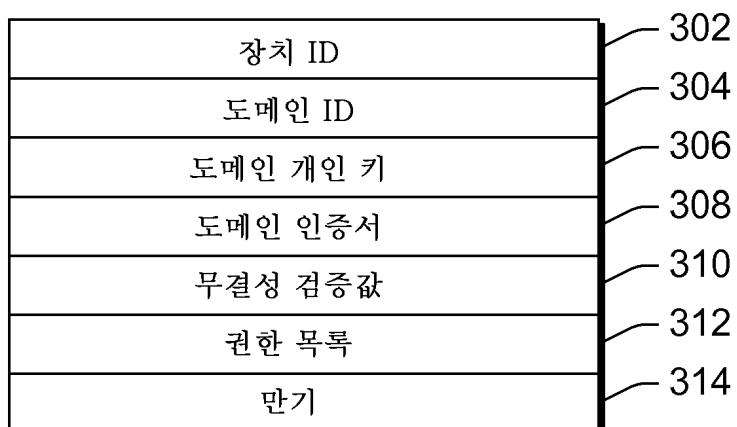
100



## 도면2

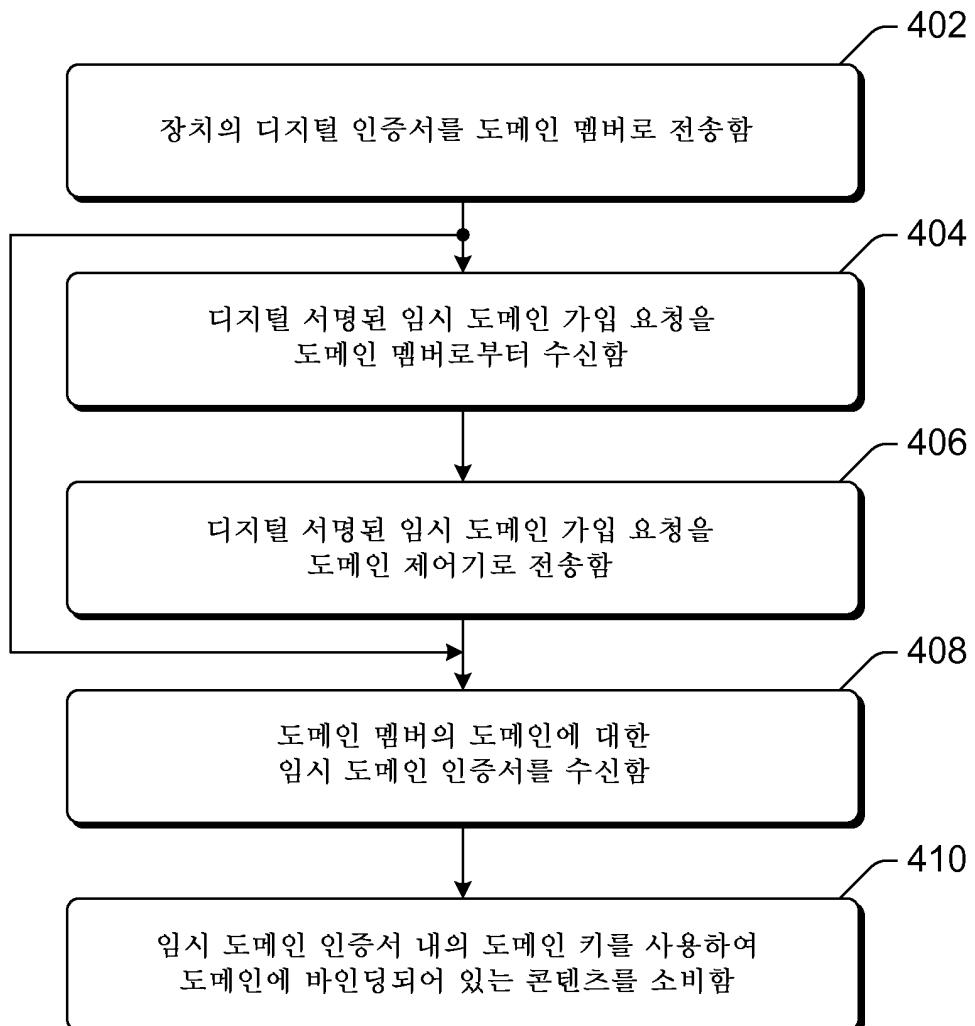
200

## 도면3

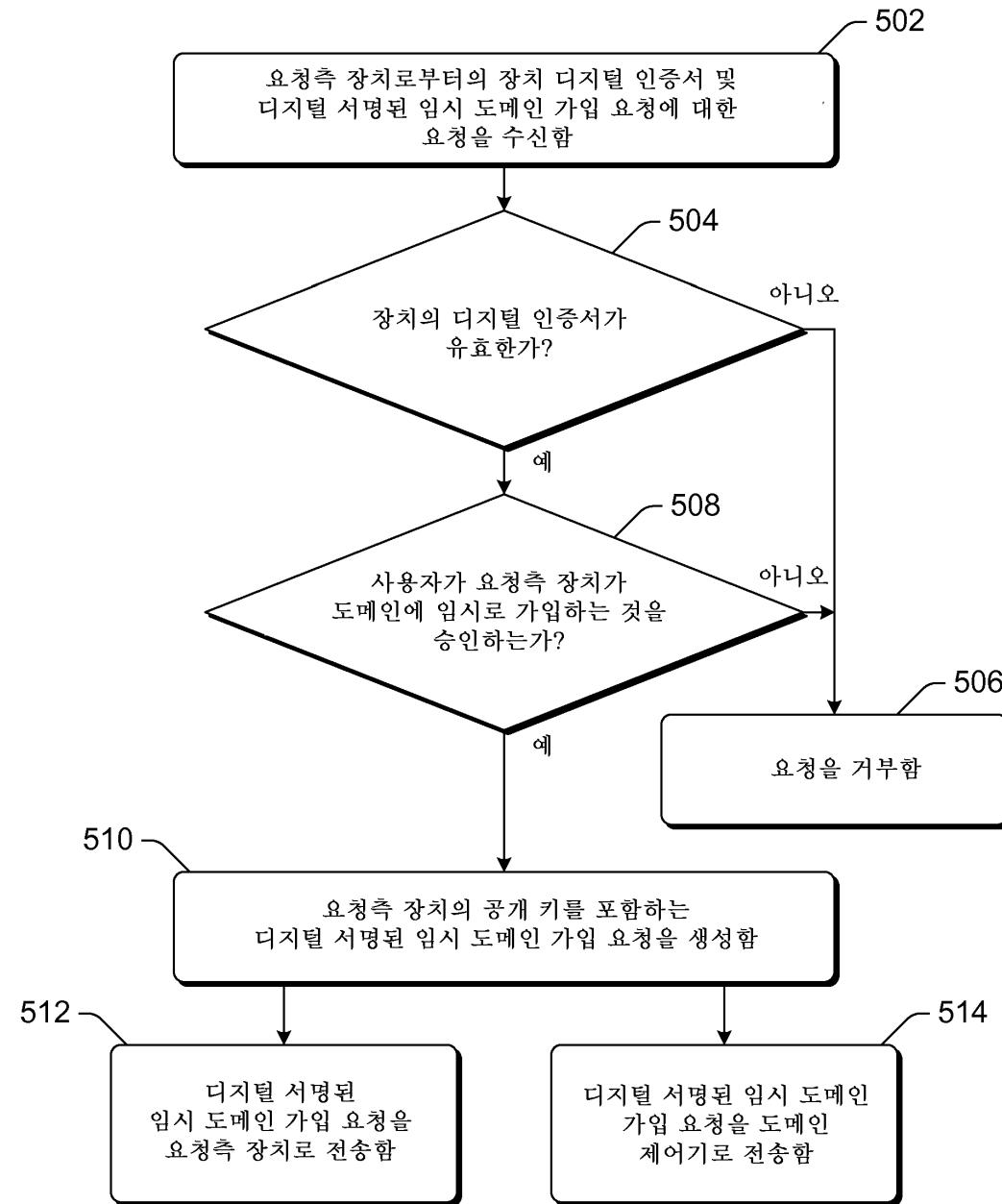
300

## 도면4

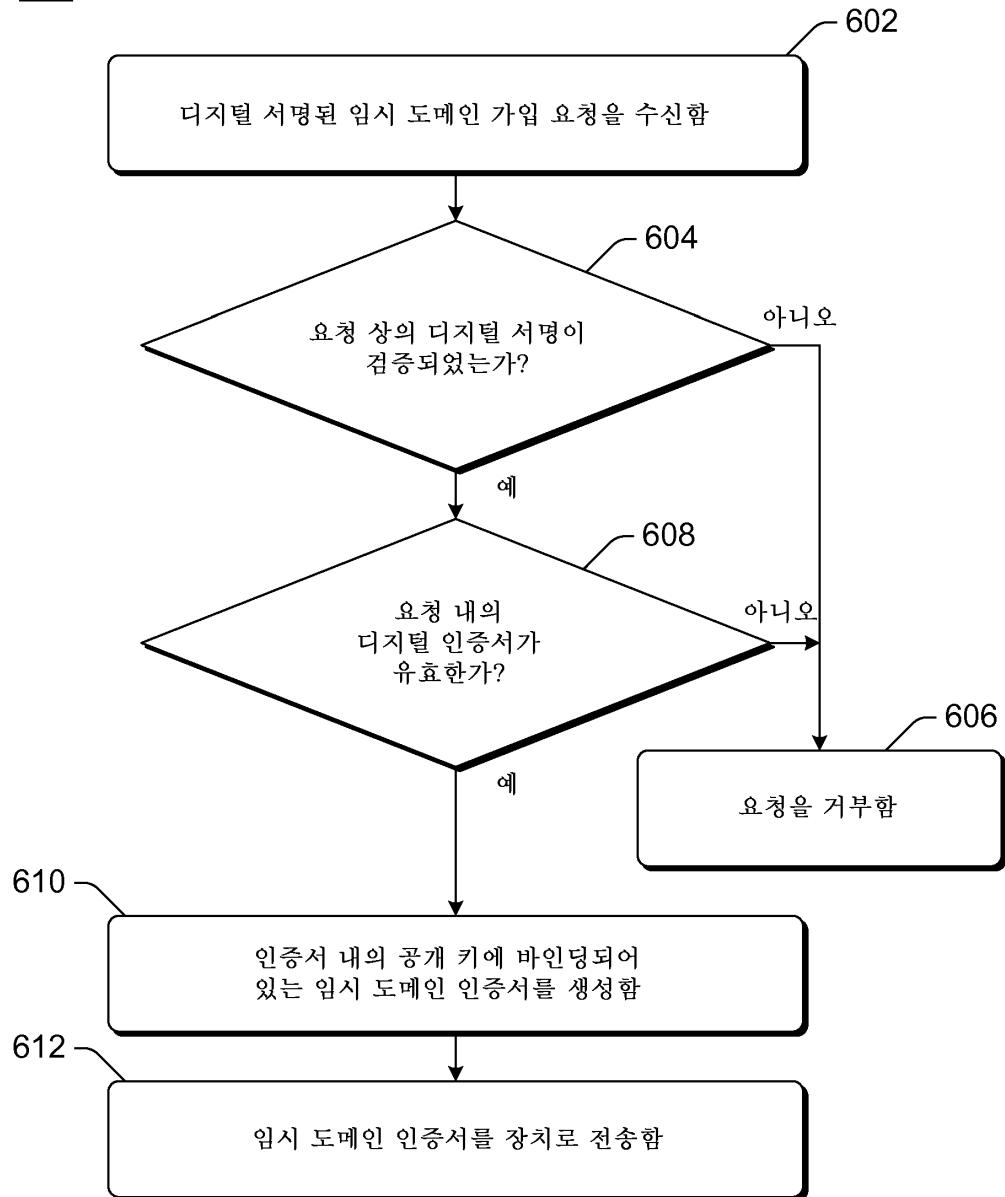
400



## 도면5

500

## 도면6

600

도면7

700

