(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년09월29일
(11) 등록번호 10-0984440
(24) 등록일자 2010년09월20일

(51) Int. Cl.
G06F 21/24 (2006.01) *G06F 17/00* (2006.01)
(21) 출원번호 10-2004-0009028
(22) 출원일자 2004년02월11일
심사청구일자 2008년12월29일
(65) 공개번호 10-2004-0073356
(43) 공개일자 2004년08월19일
(30) 우선권주장
10/364,627 2003년02월11일 미국(US)
(56) 선행기술조사문헌
US20020184515 A1
WO0068763 A
US20020112171 A1
전체 청구항 수 : 총 22 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
나린아틸라
미국98011워싱턴주보텔엔이144번코트8741
벤캐테시찬드라모울리
미국98074워싱턴주삼마미시213 번플레이스에스이414
(뒷면에 계속)
(74) 대리인
주성민, 이중희, 백만기

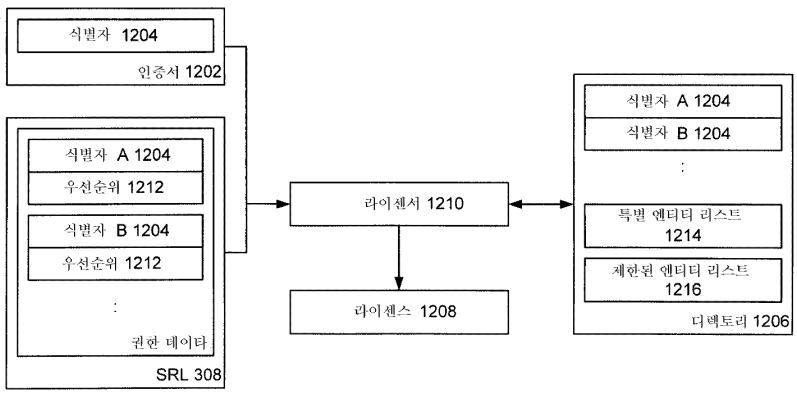
심사관 : 안지현

(54) 디지탈 라이센스 발행 방법 및 컴퓨터 판독 가능 기록 매체

(57) 요 약

라이센서는 요청자를 식별하는 식별자, 및 디지탈 콘텐트와 연관된 권한 데이타를 포함하는 요청자로부터의 요청을 수신하고, 권한 데이타는 적어도 하나의 식별자 및 그것과 연관된 권한을 리스트한다. 그 다음, 라이센서는 디렉토리 내에 요청자의 식별자를 위치시키고, 그것에 기초하여 요청자가 그 구성원인 각 그룹의 식별자를 디렉토리 내에 위치시킨다. 각각의 위치된 요청자 식별자 및 각각의 위치된 그룹 식별자는 권한 데이타 내에 리스트된 각 식별자와 비교되어 부합을 찾으며, 콘텐트를 렌더하기 위한 디지탈 라이센스는 부합 식별자와 연관된 권한을 갖는 요청자에게 발행된다.

대 표 도



(72) 발명자

비럼프랭크디.

미국98101워싱턴주시애틀넘버1210웨스턴애비뉴1200

데멜로마르코에이.

미국98052워싱턴주레드몬드152번애비뉴6606

왁스맨피터데이비드

미국98004워싱턴주벨레뷰엔이28번플레이스10008

말릭프래산트

미국98007워싱턴주벨레뷰디-228154
번애비뉴엔이1820

말라비아래치치루시미유.

미국98007워싱턴주벨레뷰엔이154번애비뉴500

보우네스티브

미국98122워싱턴주시애틀넘버602
이.파이크스트리트303

크리스나스와미비나이

미국98072워싱턴주우딘빌엔이142번플레이스23319

로젠펠드에브게니(유진)

미국98007워싱턴주벨레뷰넘버2714엔이13
번플레이스15202

특허청구의 범위

청구항 1

클라이언트 장치로 하여금 대응하는 디지탈 콘텐트를 렌더(render)하게 할 수 있도록 DRM(digital rights management) 서버(320)가 상기 클라이언트 장치(300)에게 디지탈 라이센스(license)를 발행하기 위한 방법 - 상기 DRM 서버는 상기 클라이언트 장치에 대한 리스트(listing)를 포함하는 디렉토리에 액세스할 수 있고, 상기 리스트는 상기 클라이언트 장치의 식별자, 및 상기 클라이언트 장치가 그 구성원인 각각의 그룹의 식별자를 포함함 - 에 있어서,

상기 클라이언트 장치로부터 요청을 수신하는 단계(602) - 상기 요청은 i) 상기 클라이언트 장치를 식별하는 식별자를 포함하는 송신된 인증서, 및 ii) 상기 콘텐트와 연관된 권한 데이타를 포함하는 서명된 권한 레이블(308)을 포함하고, 상기 권한 데이타는 복수의 식별자를 리스트하고, 각각의 리스트된 식별자에 대하여 권한들이 연관됨 -;

상기 클라이언트 장치의 식별자를 상기 디렉토리 내에 위치시키는(locating) 단계;

상기 디렉토리 내에 위치된 상기 클라이언트 장치의 식별자로부터, 상기 클라이언트 장치가 그 구성원인 각각의 그룹의 식별자를 상기 디렉토리 내에 위치시키는 단계;

부합(match)을 찾기 위해, 위치된 상기 클라이언트 장치의 식별자 각각 및 위치된 상기 그룹의 식별자 각각을, 상기 권한 데이타 내에 리스트된 복수의 식별자 각각과 비교하는 단계; 및

부합하는 식별자(matching identifier)와 연관된 권한 데이터로부터의 권한을 갖는 상기 클라이언트 장치에게 상기 라이센스를 발행하는 단계(618)

를 포함하는 디지탈 라이센스 발행 방법.

청구항 2

제1항에 있어서,

상기 클라이언트 장치로부터, 상기 클라이언트 장치를 식별하는 식별자를 갖는 디지탈 인증서를 포함하는 요청을 수신하는 단계를 포함하는 디지탈 라이센스 발행 방법.

청구항 3

제1항에 있어서,

상기 클라이언트 장치로부터, 디지탈 서명을 갖는 권한 데이타를 포함하는 요청을 수신하는 단계를 포함하고, 상기 디지탈 서명은 상기 권한 데이터에 기초하는 디지탈 라이센스 발행 방법.

청구항 4

제3항에 있어서,

상기 디지탈 서명을 검증하는(verify) 단계를 더 포함하는 디지탈 라이센스 발행 방법.

청구항 5

제1항에 있어서,

위치된 상기 클라이언트 장치의 식별자 각각 및 위치된 상기 그룹의 식별자 각각에 대해, 적어도 2개의 부합하는 식별자를 생기게 하기 위해(to result in),

이러한 식별자를 상기 권한 데이타 내에 리스트된 각각의 식별자와 비교하는 단계; 및

비교된 상기 식별자가 부합하는 식별자인지 여부를 표시하는(noting) 단계

를 포함하고,

상기 부합하는 식별자들 중의 하나의 식별자를 선택하는 단계; 및

선택된 상기 부합 식별자와 연관된 권한들을 갖는 상기 클라이언트 장치에게 상기 라이센스를 발행하는 단계

를 포함하는 디지탈 라이센스 발행 방법.

청구항 6

제5항에 있어서,

상기 부합하는 식별자들 중에서 가장 많은 양의 권한들을 상기 클라이언트 장치에게 전달하는 상기 부합하는 식별자를 선택하는 단계를 포함하는 디지탈 라이센스 발행 방법.

청구항 7

제5항에 있어서,

상기 권한 데이타 내의 각각의 식별자는 대응하는 우선순위 표시(priority indicia)를 가지며,

상기 방법은,

가장 큰 우선순위 표시를 갖는 상기 부합하는 식별자를 선택하는 단계를 포함하는 디지탈 라이센스 발행 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항의 방법을 행하기 위한 컴퓨터 실행 가능 명령어들이 저장되어 있는 컴퓨터 판독 가능 기록 매체.

청구항 9

그룹의 구성원인 클라이언트 장치로 하여금 대응하는 디지탈 콘텐트를 렌더하게 할 수 있도록 DRM 서버(320)가 상기 클라이언트 장치(300)에게 디지탈 라이센스를 발행하기 위한 방법에 있어서,

상기 클라이언트 장치로부터 요청을 수신하는 단계(602) - 상기 요청은 i) 상기 그룹을 식별하는 식별자를 포함하는 송신된 인증서, 및 ii) 상기 콘텐트와 연관된 권한 데이타를 포함하는 서명된 권한 레이블(308)을 포함하고, 상기 권한 데이타는 복수의 식별자를 리스트하고, 각각의 리스트된 식별자에 대하여 권한들이 연관됨 -;

부합을 찾기 위해, 상기 요청으로부터의 상기 그룹의 식별자를 상기 권한 데이타 내에 리스트된 복수의 식별자 각각과 비교하는 단계; 및

부합하는 상기 그룹의 식별자와 연관된 상기 권한 데이터로부터의 권한을 갖는 상기 클라이언트 장치에게 상기 라이센스를 발행하는 단계(618) - 발행된 상기 라이센스는 상기 그룹의 공개 키에 따라 암호화된 상기 콘텐트에 대응하는 콘텐트 키를 포함함으로써, 상기 클라이언트 장치가, 그 공개 키에 대응하는 그룹의 개인 키를 이용하여 상기 콘텐트 키를 얻을 수 있음 -

를 포함하는 디지탈 라이센스 발행 방법.

청구항 10

제9항에 있어서,

상기 클라이언트 장치로부터, 상기 그룹을 식별하는 식별자를 갖는 디지탈 인증서를 포함하는 요청을 수신하는 단계를 포함하는 디지탈 라이센스 발행 방법.

청구항 11

제9항에 있어서,

상기 클라이언트 장치로부터, 디지탈 서명을 갖는 권한 데이타를 포함하는 요청을 수신하는 단계를 포함하고, 상기 디지탈 서명은 상기 권한 데이타에 기초하는 디지탈 라이센스 발행 방법.

청구항 12

제11항에 있어서,

상기 디지탈 서명을 검증하는 단계를 더 포함하는 디지탈 라이센스 발행 방법.

청구항 13

제9항에 있어서,

상기 DRM 서버는 그룹에 대한 리스트를 포함하는 디렉토리에 액세스할 수 있고, 상기 리스트는 상기 그룹의 식별자, 및 상기 클라이언트 장치를 포함하는 그룹의 각각의 구성원의 식별자를 포함하며,

상기 방법은,

상기 클라이언트 장치로부터 그 식별자를 수신하는 단계;

상기 그룹에 대한 리스트를 상기 그룹의 식별자에 기초하여 상기 디렉토리 내에 위치시키는 단계; 및

상기 디렉토리 내의 상기 그룹에 대해 위치된 상기 리스트가 상기 클라이언트 장치의 식별자를 포함하는 것을 검증하는 단계

를 더 포함하는 디지탈 라이센스 발행 방법.

청구항 14

제9항 내지 제13항 중 어느 한 항의 방법을 행하기 위한 컴퓨터 실행 가능 명령어들이 저장되어 있는 컴퓨터 판독 가능 기록 매체.

청구항 15

그룹의 구성원인 클라이언트 장치로 하여금 대응하는 디지탈 콘텐트를 렌더하게 할 수 있도록 DRM 서버(320)가 상기 클라이언트 장치(300)에게 디지탈 라이센스를 발행하기 위한 방법 - 상기 DRM 서버는 상기 그룹에 대한 리스트를 포함하는 디렉토리에 액세스할 수 있고, 상기 리스트는 상기 클라이언트 장치를 포함하는 그룹의 각각의 구성원의 식별자를 포함함 - 에 있어서,

상기 클라이언트 장치로부터 요청을 수신하는 단계(602) - 상기 요청은 i) 상기 그룹을 식별하는 식별자 및 상기 클라이언트 장치를 식별하는 식별자를 포함하는 송신된 인증서, 및 ii) 상기 콘텐트와 연관된 권한 데이타를 포함하는 서명된 권한 레이블(308)을 포함하고, 상기 권한 데이타는 복수의 식별자를 리스트하고, 각각의 리스트된 식별자에 대하여 권한들이 연관됨 -;

부합을 찾기 위해, 상기 요청으로부터의 그룹의 식별자를 상기 권한 데이터에 리스트된 복수의 식별자 각각과 비교하는 단계;

상기 그룹에 대한 리스트를 상기 그룹의 식별자에 기초하여 상기 디렉토리 내에 위치시키는 단계;

위치된 상기 리스트로부터, 상기 클라이언트 장치 식별자가 그 안에 포함된다는 것을 검증하는 단계; 및

부합하는 상기 그룹의 식별자와 연관된 권한 데이터로부터의 권한을 갖는 상기 클라이언트 장치에게 상기 라이센스를 발행하는 단계 - 발행된 상기 라이센스는 상기 클라이언트 장치의 공개 키에 따라 암호화된 콘텐트에 대응하는 콘텐트 키를 포함함으로써, 상기 클라이언트 장치가 그 공개 키에 대응하는 상기 클라이언트 장치의 개인 키를 이용하여 상기 콘텐트 키를 얻을 수 있음 -

를 포함하는 디지탈 라이센스 발행 방법.

청구항 16

제15항에 있어서,

상기 클라이언트 장치로부터, 상기 그룹을 식별하는 식별자를 갖는 디지탈 인증서를 포함하는 요청을 수신하는 단계를 포함하는 디지탈 라이센스 발행 방법.

청구항 17

제15항에 있어서,

상기 클라이언트 장치로부터, 상기 클라이언트 장치를 식별하는 식별자를 갖는 디지탈 인증서를 포함하는 요청을 수신하는 단계를 포함하는 디지탈 라이센스 발행 방법.

청구항 18

제17항에 있어서,

상기 디지탈 인증서로부터 상기 클라이언트 장치의 공개 키를 얻는 단계를 더 포함하는 디지탈 라이센스 발행 방법.

청구항 19

제15항에 있어서,

상기 클라이언트 장치로부터, 디지탈 서명을 갖는 상기 권한 데이타를 포함하는 요청을 수신하는 단계를 포함하고, 상기 디지탈 서명은 상기 권한 데이타에 기초하는 디지탈 라이센스 발행 방법.

청구항 20

제19항에 있어서,

상기 디지탈 서명을 검증하는 단계를 더 포함하는 디지탈 라이센스 발행 방법.

청구항 21

제15항에 있어서,

파일 상의 디지탈 인증서로부터 상기 클라이언트 장치의 공개 키를 얻는 단계를 더 포함하고, 상기 디지탈 인증서는 상기 클라이언트 장치의 식별자를 포함하는 디지탈 라이센스 발행 방법.

청구항 22

제15항 내지 제21항 중 어느 한 항의 방법을 행하기 위한 컴퓨터 실행 가능 명령어들이 저장되어 있는 컴퓨터 판독 가능 기록 매체.

<첨부 1>

Sample Rights Data

```
<?xml version="1.0" ?>
<XrML version="1.2">
  <BODY type="Rights Template">
    <DESCRIPTOR>
      <OBJECT>
        <ID type="GUID">c43...</ID>
        <NAME>$$411$411name$411desc</NAME>
      </OBJECT>
    </DESCRIPTOR>
    <WORK>
      <OBJECT>
        <ID />
      </OBJECT>
      <RIGHTSGROUP name="MAIN RIGHTS">
        <RIGHTSLIST>
          <VIEW>
            <CONDITIONLIST>
              <ACCESS>
                <PRINCIPAL>
                  <OBJECT>
                    <ID />
                    <NAME>test@company.com</NAME>
                  </OBJECT>
                </PRINCIPAL>
              </ACCESS>
            </CONDITIONLIST>
          </VIEW>
          <RIGHT name="generic">
            <CONDITIONLIST>
              <ACCESS>
                <PRINCIPAL>
                  <OBJECT>
                    <ID />
                    <NAME>test@company.com</NAME>
                  </OBJECT>
                </PRINCIPAL>
              </ACCESS>



            </CONDITIONLIST>
          </RIGHT>
        </RIGHTSLIST>
      </RIGHTSGROUP>
    </WORK>
  </BODY>
  <SIGNATURE>
    <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
    <DIGEST>
      <ALGORITHM>SHA1</ALGORITHM>
      <PARAMETER name="codingtype">
        <VALUE encoding="string">surface-coding</VALUE>
      </PARAMETER>
      <VALUE encoding="base64” size="160">MwI...=</VALUE>
    </DIGEST>
    <VALUE encoding="base64" size="1024">Msi...=</VALUE>
  </SIGNATURE>
</XrML>
```

<첨부 2>

Sample Signed Rights Label (SRL) 308

```
<?xml version="1.0" ?>
<XrML version="1.2">
  <BODY type="Rights Label" version="3.0">
    <ISSUEDTIME>2002-01-01_12:00:00</ISSUEDTIME>
    <DESCRIPTOR>
      <OBJECT>
        <ID />
        <NAME>$$409$...</NAME>
      </OBJECT>
    </DESCRIPTOR>
    <ISSUER>
      <OBJECT type="DRM-Server">
        <ID type="GUID">{d81...}</ID>
        <NAME>Test DRM Server</NAME>
        <ADDRESS type="URL">http://licensing.dev.com</ADDRESS>
      </OBJECT>
      <PUBLICKEY>
        <ALGORITHM>RSA</ALGORITHM>
        <PARAMETER name="public-exponent">
          <VALUE encoding="integer32">65537</VALUE>
        </PARAMETER>
        <PARAMETER name="modulus">
          <VALUE encoding="base64" size="1024">NcO...=</VALUE>
        </PARAMETER>
      </PUBLICKEY>
      <ENABLINGBITS type="sealed-key">
        <VALUE encoding="base64" size="1024">tFg...=</VALUE>
      </ENABLINGBITS>
      <SECURITYLEVEL name="Server-Version" value="2.0" />
      <SECURITYLEVEL name="Server-SKU" value="22222-3333" />
    </ISSUER>
    <DISTRIBUTIONPOINT>
      <OBJECT type="LICENSE ACQUISITION URL">
        <ID type="GUID">{0F4...}</ID>
        <NAME>DRM Server Cluster</NAME>
        <ADDRESS type="URL">http://localhost/Licensing</ADDRESS>
      </OBJECT>



      </DISTRIBUTIONPOINT>
      <WORK>
        <OBJECT type="TEST-FORMAT">
          <ID type="MYID">FDB-1</ID>
        </OBJECT>
        <METADATA>
          <SKU type="PIDTYPE">PID</SKU>
        </METADATA>
        <PRECONDITIONLIST>
          <TIME />
        </PRECONDITIONLIST>
      </WORK>
      <AUTHDATA name="Encrypted Rights data">PAB... </AUTHDATA>
    </BODY>
    <SIGNATURE>
      <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
      <DIGEST>
        <ALGORITHM>SHA1</ALGORITHM>
        <PARAMETER name="codingtype">
          <VALUE encoding="string">surface-coding</VALUE>
        </PARAMETER>
        <VALUE encoding="base64" size="160">Prc...=</VALUE>
      </DIGEST>
      <VALUE encoding="base64" size="1024">EHd...=</VALUE>
    </SIGNATURE>
  </XrML>
```

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0028] <연관된 출원에 대한 참조>

[0029] 이하의 미국특허출원들은 본 출원과 관련된 주제에 관하여 개시하고 있으며, 본 명세서에 참고로서 포함되어 있다:

[0030] 미국 특허출원 제_____호, 대리인 도켓번호 MSFT-1569 하에서 본 출원과 동일자로 출원되었으며, 제목은 "디지탈 권한 관리(DRM) 시스템에 따른, 조직과 같은 규정된 집단 내에서의 디지탈 콘텐트 출판"이며;

[0031] 미국 특허출원 제10/185,527호, 대리인 도켓번호 MSFT-1330 하에서 2002년 6월 28일자로 출원되었으며, 제목은 "디지탈 콘텐트를 위한 서명된 권한 레이블(SRL) 획득 및 디지탈 권한 관리 시스템의 SRL에 기초하여 콘텐트에 대응하는 디지탈 라이센스 획득"이며;

[0032] 미국 특허출원 제10/185,278호, 대리인 도켓번호 MSFT-1333 하에서 2002년 6월 28일자로 출원되었으며, 제목은 "권한 템플릿을 사용하여 디지탈 권한 관리 시스템의 디지탈 콘텐트를 위한 서명된 권한 레이블(SRL) 획득"이며;

[0033] 미국 특허출원 제10/185,511호, 대리인 도켓번호 MSFT-1343 하에서 2002년 6월 28일자로 출원되었으며, 제목은 "디지탈 콘텐트 및 서비스를 위한 이용 라이센스 발행 시스템 및 방법"이다.

[0034] <기술 분야>

[0035] 본 발명은 디지탈 권한 관리(DRM) 시스템에 관한 것이다. 더욱 구체적으로, 본 발명은 조직체, 사무실, 회사 등과 같은 규정된 집단(universe) 내에서의 콘텐트의 렌더링(rendering) 및 사용이 대응하는 사용 또는 라이센스 기간에 따라 제한될 수 있도록 상기와 같은 규정된 집단 내에서 디지탈 콘텐트를 출판하는 데에 DRM 시스템을 사용하는 것에 관한 것이다.

발명이 이루고자 하는 기술적 과제

[0036] 디지탈 권한 관리 및 시행은 디지탈 오디오, 디지탈 비디오, 디지탈 텍스트, 디지탈 데이타, 디지탈 멀티미디어 등과 같은 디지탈 콘텐트와 관련하여 매우 바람직한 것으로, 이러한 디지탈 콘텐트는 한 사람 이상의 사용자에게 배포될 수 있다. 디지탈 콘텐트는 예를 들어, 텍스트 문서와 같이 정적(static)일 수 있거나, 또는 라이브 이벤트의 스트림식(streamed) 오디오/비디오와 같이 스트림될 수 있다. 전형적인 배포 모드는 자기(플로피) 디스크, 자기 테이프, 광(컴팩트) 디스크(CD) 등과 같은 유형의(tangible) 장치, 및 전자 게시판, 전자 네트워크, 인터넷 등과 같은 무형의 매체를 포함한다. 사용자에 의해 수신되고 있는 중에, 이러한 사용자는 퍼스널 컴퓨터 상의 미디어 플레이어 등과 같은 적절한 렌더링 장치의 도움으로 디지탈 콘텐트를 렌더(render)하거나 '플레이(play)'한다.

[0037] 하나의 시나리오에 있어서, 작성자(author), 발행자(publisher), 방송자 등과 같은 콘텐트 소유자 또는 권한 소유자는 이러한 디지탈 콘텐트를 라이센스 요금이나 소정의 다른 대가와 교환하여 많은 사용자들 또는 수신인들 각각에게 배포하고자 한다. 이러한 시나리오에서, 콘텐트는 노래, 노래 앨범, 영화 등이 될 수 있으며, 배포 목적은 라이센스 요금을 발생시키기 위한 것이다. 이러한 콘텐트 소유자는, 선택권이 주어지면, 사용자가 이러한 배포된 디지탈 콘텐트를 가지고 할 수 있는 것을 제한하고자 할 것이다. 예를 들어, 콘텐트 소유자는 적어도 제2 사용자로부터의 라이센스 요금을 콘텐트 사용자에게 주지않는 방식으로, 사용자가 제2 사용자에게 이러한 콘텐트를 복사 및 재배포하는 것을 제한하고자 한다.

[0038] 또한, 콘텐트 소유자는 사용자에게 실제로 구매되는 모든 종류의 라이센스의 기간을 지키게 하는 동시에, 사용자에게 다른 유형의 사용 라이센스를 다른 라이센스 요금으로 구매하는 융통성을 제공하고자 할 수 있다. 예를 들어, 콘텐트 소유자는 배포된 디지탈 콘텐트가 제한된 횟수만, 소정의 총 시간동안만, 소정 종류의 기계 상에서만, 소정 종류의 미디어 플레이어 상에서만, 소정 종류의 사용자 등에 의해서만 플레이될 수 있게 하고자 할

수 있다.

[0039] 다른 시나리오에 있어서, 한 조직체 내의 피고용인 또는 구성원과 같은 콘텐트 개발자는 이러한 디지탈 콘텐트를 그 조직체 내의 한 사람 이상의 다른 피고용인들 또는 구성원들에게, 또는 그 조직체 외부의 다른 개인들에게 배포하고자 하지만, 다른 사람들은 그 콘텐트의 렌더링은 못하게 하고자 한다. 여기에서, 콘텐트의 배포는 라이센스 요금 또는 소정의 다른 대가와의 교환으로, 광역 기반의(broad-based) 배포와 대조적으로, 비밀의 또는 제한된 방식으로 공유하는 조직 기반의(organization-based) 콘텐트에 더 가깝다.

[0040] 이러한 시나리오에서, 콘텐트는 사무실 세팅 내에서 교체될 수 있는 것과 같은 문서 프리젠테이션, 스프레드시트, 데이타베이스, 이메일 등이 될 수 있으며, 콘텐트 개발자는 콘텐트가 조직체 또는 사무실 세팅 내에서 유지될 수 있고, 예를 들어 경쟁자들 또는 적들과 같이 권한이 없는 개인들에게는 렌더될 수 없게 하고자 할 수 있다. 다시, 이러한 콘텐트 개발자는 수신인이 이러한 배포된 디지탈 콘텐트로 할 수 있는 것을 제한하고자 한다. 예를 들어, 콘텐트 소유자는 적어도 콘텐트를 렌더하도록 허용되어야 하는 개인들의 범위를 벗어난 콘텐트를 노출시키는 방식으로, 사용자가 제2 사용자에게 이러한 콘텐트를 복사 및 재배포하는 것을 제한하고자 한다.

[0041] 또한, 콘텐트 개발자는 다양한 수신인들에게 다른 레벨의 렌더링 권한을 제공하고자 할 수 있다. 예를 들어, 콘텐트 개발자는 보호된 디지탈 콘텐트를 한 클래스의 개인에 대해서는 볼 수 있지만 프린트할 수 없게 하고, 다른 클래스의 개인에 대해서는 볼 수 있으면서 프린트할 수 있게 하고자 할 수 있다.

[0042] 그러나, 둘 중 어느 시나리오에서는, 배포가 발생된 후, 이러한 콘텐트 소유자/개발자는 디지탈 콘텐트에 관한 제어를 거의 하지 않는다. 이것은 실질적으로 모든 퍼스널 컴퓨터가 이러한 디지탈 콘텐트의 정확한 디지탈 복사를 행하여, 그 정확한 디지탈 복사를 기입가능한 자기 또는 광 디스크로 다운로드하거나, 또는 그 정확한 디지탈 복사를 인터넷과 같은 네트워크를 통해 소정의 목적지로 보내는데 필요한 소프트웨어 및 하드웨어를 포함한다는 사실로 보아 특히 문제가 된다.

[0043] 물론, 콘텐트가 배포되는 거래의 일부로서, 콘텐트 소유자/개발자는 디지탈 콘텐트의 사용자/수신인에게 달갑지 않은 방식으로 이러한 디지탈 콘텐트를 재배포하지 않기로 약속할 것을 요구할 수 있다. 그러나, 이러한 약속은 쉽게 이루어지고, 쉽게 파기된다. 콘텐트 소유자/개발자는 일반적으로 암호화 및 복호화를 수반하는 소정의 몇몇 공지된 보안 장치를 통해 이러한 재배포를 방지하려고 시도할 수 있다. 그러나, 가볍게 결정된 사용자가 암호화된 디지탈 콘텐트를 복호화하고, 이러한 디지탈 콘텐트를 비암호화 형태로 보관한 다음, 그것을 재배포하는 것을 금지하게 하는 것은 거의 불가능하다.

[0044] 그러므로, 임의의 형태의 디지탈 콘텐트의 제어된 렌더링 또는 플레잉을 허용하는 디지탈 권한 관리(DRM) 및 시행 아키텍처 및 방법을 제공할 필요성이 있으며, 상기 제어는 융통성이 있어서 디지탈 콘텐트의 콘텐트 소유자/개발자에 의해 융통성있으며 규정가능하다. 더욱 구체적으로, 특히 규정된 그룹의 개인들 또는 클래스의 개인들 사이에서 문서가 공유될 사무실 또는 조직체 등의 안에서, 그 제어된 렌더링을 허용하고 용이하게 하는 아키텍처에 대한 필요성이 있다.

발명의 구성 및 작용

[0045] 상술된 필요성은 요청자가 대응하는 디지탈 콘텐트를 렌더할 수 있도록 라이센서가 요청자에게 디지탈 라이센스를 발행하는 본 발명에 의해 적어도 부분적으로 충족된다. 본 발명에서, 라이센서는 요청자에 대한 리스트를 포함하는 디렉토리에 액세스하는데, 상기 리스트는 요청자의 식별자, 및 그 요청자가 구성원인 각 그룹의 식별자를 포함한다.

[0046] 라이센서는 요청자로부터 요청을 수신하여, 상기 요청은 요청자를 식별하는 식별자, 및 콘텐트와 연관된 권한 데이타를 포함하고, 권한 데이타는 적어도 하나의 식별자 및 그것과 연관된 권한을 리스트한다. 그 후, 라이센서는 디렉토리 내에 요청자의 식별자를 위치시키고, 디렉토리 내에 위치된 요청자 식별자로부터, 요청자가 그 구성원인 각 그룹의 식별자를 디렉토리 내에 위치시킨다. 각각의 위치된 요청자 식별자 및 각각의 위치된 그룹 식별자는 권한 데이타 내에 리스트된 각 식별자와 비교되어 부합을 찾고, 라이센스는 부합 식별자와 연관된 권한을 갖는 요청자에게 발행된다.

[0047] 상기 설명, 및 본 발명의 실시예에 관한 다음의 상세한 설명은 첨부된 도면을 참조하면 더욱 잘 이해될 수 있을 것이다. 본 발명의 설명을 위해, 양호한 실시예가 도시된다. 그러나, 본 발명은 도시된 정밀한 구성 및 수단에 제한되는 것은 아니다.

[0048] **컴퓨터 환경**

[0049] 도 1 및 다음 설명은 본 발명이 실현될 수 있는 적절한 컴퓨팅 환경에 관한 간단한 설명을 제공하고자 하는 것이다. 그러나, 핸드헬드, 포터블, 및 모든 종류의 다른 컴퓨팅 장치들이 본 발명과 관련하여 사용이 고려될 수 있다는 것을 이해해야 한다. 범용 컴퓨터가 후술되지만, 그것은 단지 한 예이고, 본 발명은 단지 네트워크 서버 상호운용성(interoperability) 및 상호작용을 갖는 씬(thin) 클라이언트를 필요로 한다. 그러므로, 본 발명은 거의 없거나 극미한 클라이언트 자원이 관련되는 네트워크화 호스티드 서비스의 환경, 즉 클라이언트 장치가 단지 월드 와이드 웹에 대한 브라우저 또는 인터페이스로서 작용하는 네트워크 환경에서 실현될 수 있다.

[0050] 요구되지는 않지만, 본 발명은 개발자에 의한 사용을 위한 응용 프로그래밍 인터페이스(API)를 통해 실현될 수 있고, 및/또는 클라이언트 워크스테이션, 서버 또는 기타의 장치들과 같은 하나 이상의 컴퓨터들에 의해 실행되고 있는 프로그램 모듈과 같은 컴퓨터 실행가능한 명령어의 일반적인 문맥으로 기술될 수 있는 네트워크 브라우징 소프트웨어 내에 포함될 수 있다. 일반적으로, 프로그램 모듈은 특정 태스크를 수행하거나 특정 추상 데이타 유형을 실행하는 루틴, 프로그램, 오브젝트, 컴포넌트, 데이타 구조 등을 포함한다. 전형적으로, 프로그램 모듈의 기능성은 여러 실시예에서 요구된 바와 같이 결합되거나 분포될 수 있다. 게다가, 본 분야에 숙련된 기술자들은 본 발명이 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 이해할 수 있을 것이다. 본 발명과 사용하기에 적절하게 될 수 있는 그밖의 다른 널리 공지된 컴퓨팅 시스템, 환경 및/또는 구성들은 퍼스널 컴퓨터(PC), 현금자동 입출금기(ATM), 서버 컴퓨터, 핸드-헬드 또는 랩탑 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 시스템, 프로그램가능 소비자 전자제품, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터 등을 포함하지만, 이것에 제한되는 것은 아니다. 본 발명은 또한 통신망 또는 다른 데이타 전송 매체를 통해 링크되는 원격 프로세싱 장치에 의해 태스크가 실행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 메모리 저장 장치를 포함하는 로컬 및 원격 컴퓨터 저장 매체 내에 위치될 수 있다.

[0051] 그러므로, 도 1은 본 발명이 실현될 수 있는 적절한 컴퓨팅 환경(100)의 한 예를 도시한 것으로, 위에서 명백해지긴 했지만, 컴퓨팅 시스템 환경(100)은 적절한 컴퓨팅 환경의 한 예일 뿐이며, 본 발명의 사용범위 또는 기능에 관해 소정의 제한을 제안하고자 하는 것은 아니다. 컴퓨팅 환경(100)은 예시적인 동작 환경(100)에 도시된 구성요소의 임의의 하나 또는 조합에 관련하여 어떠한 종속성이나 요구사항을 갖는 것으로 해석되어서는 안된다.

[0052] 도 1을 참조하면, 본 발명을 실현하는 예시적인 시스템은 컴퓨터(100) 형태의 범용 컴퓨팅 장치를 포함한다. 컴퓨터(100)의 구성요소는 프로세싱 유닛(120), 시스템 메모리(130), 및 시스템 메모리를 포함하는 다양한 시스템 구성요소를 프로세싱 유닛(120)에 연결하는 시스템 버스(121)를 포함할 수 있으며, 이것에 제한되는 것은 아니다. 시스템 버스(121)는 메모리 버스 또는 메모리 제어기, 주변 버스, 및 다양한 버스 아키텍처 중의 임의의 것을 사용하는 로컬 버스를 포함하는 몇몇 형태의 버스 구조들 중의 어떤 구조로 될 수 있다. 예를 들어, 이러한 아키텍처는 ISA(Industry Standard Architecture) 버스, MCA(Micro Channel Architecture) 버스, EISA(Enhanced ISA) 버스, VESA(Video Electronics Standards Association) 로컬 버스, 및 PCI(Peripheral Component Interconnect) 버스(Mezzanine 버스라고도 공지됨)를 포함하며, 이에 제한되는 것은 아니다.

[0053] 컴퓨터(110)는 전형적으로 다양한 컴퓨터 판독가능한 매체를 포함한다. 컴퓨터 판독가능한 매체는 컴퓨터(110)에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있고, 휘발성 및 불휘발성 매체, 착탈가능 및 착탈불가능 매체를 모두 포함한다. 예로서, 컴퓨터 판독가능한 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있으며, 이에 제한되는 것은 아니다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이타 구조, 프로그램 모듈 또는 그밖의 다른 데이타와 같은 정보의 저장을 위해 임의의 방법 또는 기술로 실현된 휘발성 및 불휘발성, 착탈 가능 및 착탈불가능 매체를 모두 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 그밖의 다른 메모리 기술, CDROM, DVD(Digital Versatile Disks) 또는 그밖의 다른 광 디스크 저장장치, 자기 카세트, 자기 테이프, 자기 디스크 저장장치 또는 그밖의 다른 자기 저장 장치, 또는 원하는 정보를 저장하기 위해 사용될 수 있고 컴퓨터(110)에 의해 액세스될 수 있는 임의의 다른 매체를 포함하지만, 이것에 제한되지는 않는다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이타 구조, 프로그램 모듈, 또는 반송파 또는 다른 전송 메카니즘과 같은 변조된 디지탈 신호 내의 다른 데이타를 구현하고, 임의의 정보 전달 매체를 포함한다. "변조된 데이타 신호"라는 용어는 하나 이상의 자체 특성 세트를 갖거나 또는 신호 내의 정보를 인코드하는 것과 같은 방식으로 변화된 신호를 의미한다. 예를 들어, 통신 매체는 유선 네트워크 또는 직접-유선 접속과 같은 유선 매체, 및 음향, RF, 적외선 및 다른 무선 매체와 같은 무선 매체를 포함하며, 이에 제한되는 것은 아니다. 상기의 임의의 결합은 또한 컴퓨터 판독가능한 매체의 범위 내에 포함되어야 한다.

[0054] 시스템 메모리(130)는 판독 전용 메모리(ROM)(131) 및 랜덤 액세스 메모리(RAM)(132)와 같은 휘발성 및/또는 불휘발성 메모리 형태의 컴퓨터 저장 매체를 포함한다. 예를 들어 스타트-업(start-up) 동안에 컴퓨터(110) 내의 소자들 간의 정보 전달을 돕는 베이직 루틴을 포함하는 기본 입/출력 시스템(133)(BIOS)은 전형적으로 ROM(131)에 저장된다. RAM(132)은 전형적으로 프로세싱 유닛(120)에 즉시 액세스가능하거나 및/또는 프로세싱 유닛(120)에 의해 현재 동작되고 있는 데이타 및/또는 프로그램을 포함한다. 예를 들어, 도 1은 운영 체계(134), 응용 프로그램(135), 기타의 프로그램 모듈(136) 및 프로그램 데이타(137)를 도시한 것이고, 이에 제한되는 것은 아니다.

[0055] 컴퓨터(110)는 또한 그밖의 다른 착탈가능/착탈불가능, 휘발성/불휘발성 컴퓨터 저장 매체를 포함할 수 있다. 단지 예를 들어보면, 도 1은 착탈불가능 불휘발성 자기 매체로부터 판독하거나 기입하는 하드 디스크 드라이브(141), 착탈가능 불휘발성 자기 디스크(152)로부터 판독하거나 기입하는 자기 디스크 드라이브(151), 및 CD ROM 또는 그밖의 광 매체와 같은 착탈가능 불휘발성 광 디스크(156)로부터 판독하거나 기입하는 광 디스크 드라이브(155)를 도시한 것이다. 예시적인 동작 환경에서 사용될 수 있는 그밖의 다른 착탈가능/착탈불가능, 휘발성/불휘발성 컴퓨터 저장 매체는 자기 테이프 카세트, 플래시 메모리 카드, DVD, 디지탈 비디오 테이프, 고체상태 RAM, 고체상태 ROM 등을 포함하지만, 이것에 제한되지는 않는다. 하드 디스크 드라이브(141)는 전형적으로, 인터페이스(140)와 같은 착탈불가능 메모리 인터페이스를 통해 시스템 버스(121)에 접속되고, 자기 디스크 드라이브(151) 및 광 디스크 드라이브(155)는 전형적으로, 인터페이스(150)와 같은 착탈가능 메모리 인터페이스에 의해 시스템 버스(121)에 접속된다.

[0056] 상술되고 도 1에 도시된 드라이브 및 이와 연관된 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이타 구조, 프로그램 모듈 및 컴퓨터(110)용의 다른 데이타의 저장을 제공한다. 도 1에서, 예를 들어, 하드 디스크 드라이브(141)는 운영 체계(144), 응용 프로그램(145), 다른 프로그램 모듈(146) 및 프로그램 데이타(147)를 저장하는 것으로 도시된다. 이들 구성요소들은 운영 체계(134), 응용 프로그램(135), 다른 프로그램 모듈(136) 및 프로그램 데이타(137)와 동일하거나 다르게 될 수 있다는 것을 유의한다. 운영 체계(144), 응용 프로그램(145), 다른 프로그램 모듈(146) 및 프로그램 데이타(147)는 적어도 이들이 서로다른 카피인 것을 나타내기 위해 여기에서 서로다른 번호로 주어진다. 사용자는 일반적으로 마우스, 트랙볼 또는 터치패드로 언급되는 포인팅 장치(161) 및 키보드(162)와 같은 입력 장치를 통해 컴퓨터(110) 내로 커맨드 및 정보를 입력시킬 수 있다. 다른 입력 장치(도시되지 않음)는 마이크로폰, 조이스틱, 게임 패드, 위성 접시, 스캐너 등을 포함할 수 있다. 이들 및 그밖의 입력 장치들은 시스템 버스(121)에 연결되는 사용자 입력 인터페이스(160)를 통해 프로세싱 유닛(120)에 자주 접속되지만, 병렬 포트, 게임 포트 또는 유니버셜 시리얼 버스(USB)와 같은 그밖의 인터페이스 및 버스 구조에 의해 접속될 수도 있다.

[0057] 모니터(191) 또는 다른 유형의 디스플레이 장치는 또한 비디오 인터페이스(190)와 같은 인터페이스를 통해 시스템 버스(121)에 접속된다. 노스브리지(Northbridge)와 같은 그래픽 인터페이스(182)가 또한 시스템 버스(121)에 접속될 수 있다. 노스브리지는 CPU 또는 호스트 프로세싱 유닛(120)과 통신하는 칩셋으로서, AGP(Accelerated Graphics Port) 통신에 대한 책임을 맡고 있다. 하나 이상의 그래픽 프로세싱 유닛(GPU)(184)는 그래픽 인터페이스(182)와 통신할 수 있다. 이와 관련하여, GPU(184)는 레지스터 저장장치와 같은 온칩(on-chip) 메모리 저장장치를 일반적으로 포함하고, GPU(184)는 비디오 메모리(186)와 통신한다. 그러나, GPU(184)는 코프로세서(coprocessor)의 한 예일 뿐이므로, 다양한 코프로세싱 장치가 컴퓨터(110) 내에 포함될 수 있다. 모니터(191) 또는 다른 유형의 디스플레이 장치는 또한, 비디오 메모리(186)와 교대로 통신할 수 있는 비디오 인터페이스(190)와 같은 인터페이스를 통해 시스템 버스(121)에 접속된다. 모니터(191) 이외에, 컴퓨터는 출력 주변 인터페이스(195)를 통해 접속될 수 있는 스피커(197) 및 프린터(196)와 같은 다른 주변 출력 장치들을 마찬가지로 포함할 수 있다.

[0058] 컴퓨터(110)는 원격 컴퓨터(180)와 같은 하나 이상의 원격 컴퓨터들로의 논리적인 접속을 사용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(180)는 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어(peer) 장치, 또는 그밖의 통상의 네트워크 노드일 수 있으며, 도 1에 메모리 저장 장치(181)만이 도시되었지만, 전형적으로 컴퓨터(110)와 관련하여 상술된 다수의 또는 모든 소자들을 포함할 수 있다. 도 1에 도시된 논리적 접속은 근거리 통신망(LAN)(171) 및 광역 통신망(WAN)(173)을 포함하지만, 다른 네트워크를 포함할 수도 있다. 이러한 네트워킹 환경은 사무실, 기업체 전반의 컴퓨터 네트워크, 인트라넷 및 인터넷에서 통상적인 것이다.

[0059] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(110)는 네트워크 인터페이스 또는 어댑터(170)를 통해 LAN(171)에 접속된다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(110)는 전형적으로, 모뎀(172), 및 인터넷과 같은 WAN(173)을 통해 통신을 설정하는 다른 수단을 포함한다. 내부 또는 외부에 있을 수 있는 모뎀(172)은 사용자 입력

인터페이스(160) 또는 다른 적절한 메카니즘을 통해 시스템 버스(121)에 접속될 수 있다. 네트워크 환경에서, 컴퓨터(110)와 관련하여 묘사된 프로그램 모듈, 또는 그것의 일부분은 원격 메모리 저장 장치 내에 저장될 수 있다. 예를 들어, 도 1은 메모리 장치(181)에서 상주하는 원격 응용 프로그램(185)을 도시하고 있으며, 이에 제한되는 것은 아니다. 도시된 네트워크 접속은 예시적인 것이고, 컴퓨터들 사이의 통신 링크를 설정하는 다른 수단이 사용될 수 있다는 것을 이해할 수 있을 것이다.

[0060] 본 분야에 숙련된 기술자라면 컴퓨터(110) 또는 다른 클라이언트 장치가 컴퓨터 네트워크의 일부로서 전개될 수 있다는 것을 이해할 수 있다. 이와 관련하여, 본 발명은 임의 수의 메모리 또는 저장 유닛을 갖고 있고, 임의 수의 저장 유닛 또는 볼륨을 교차하여 발생하는 임의 수의 어플리케이션 및 프로세스를 갖고 있는 소정의 컴퓨터 시스템에 속한다. 본 발명은 원격 또는 로컬 저장 장치를 갖고 있는 네트워크 환경에서 전개된 서버 컴퓨터 및 클라이언트 컴퓨터를 갖는 환경에 적용할 수 있다. 본 발명은 또한 프로그래밍 언어 기능, 번역 및 실행 능력을 갖고 있는 단독형(standalone) 컴퓨터 장치에 적용할 수 있다.

[0061] 분산 컴퓨팅은 컴퓨팅 장치와 시스템 간의 직접 교환에 의해 컴퓨터 자원 및 서비스의 공유를 용이하게 한다. 이들 자원 및 서비스는 정보 교환, 캐시 저장장치, 및 파일용 디스크 저장장치를 포함한다. 분산 컴퓨팅은 네트워크 접속성을 이용하여, 클라이언트가 전체 기업에게 이익이 되는 그들의 집합적인 능력을 발휘할 수 있게 한다. 이와 관련하여, 여러가지 장치는 신뢰된 그래픽 파이프라인(들)에 대한 본 발명의 인증 기술을 관련시키기 위해 상호작용할 수 있는 어플리케이션, 오브젝트 또는 자원을 가질 수 있다.

[0062] 도 2는 예시적인 네트워크 또는 분산된 컴퓨팅 환경의 개략도를 제공한다. 분산 컴퓨팅 환경은 컴퓨팅 오브젝트(10a, 10b 등) 및 컴퓨팅 오브젝트 또는 장치(110a, 110b, 110c 등)를 포함한다. 이들 오브젝트들은 프로그램, 방법, 데이타 저장, 프로그램가능한 로직 등을 포함할 수 있다. 오브젝트들은 PDA, 텔레비젼, MP3 플레이어, 퍼스널 컴퓨터 등과 같은 동일하거나 상이한 장치들의 일부를 포함할 수 있다. 각 오브젝트는 통신 네트워크(14)에 의해 다른 오브젝트와 통신할 수 있다. 이 네트워크는 도 2의 시스템에 서비스를 제공하는 다른 컴퓨팅 오브젝트 및 컴퓨팅 장치를 포함할 수 있다. 본 발명의 실시양상에 따라, 각 오브젝트(10 또는 110)는 신뢰된 그래픽 파이프라인(들)에 대한 본 발명의 인증 기술을 요청할 수 있는 어플리케이션을 포함할 수 있다.

[0063] 또한, 오브젝트(110c)는 다른 컴퓨팅 장치(10 또는 110) 상에 호스팅될 수 있다는 것을 이해할 수 있다. 그러므로, 묘사된 물리적인 환경이 컴퓨터와 같은 접속된 장치를 도시할 수 있지만, 이러한 도시는 예시적일 뿐이며, 물리적 환경은 대안적으로 PDA, TV, MP3 플레이어 등과 같은 다양한 디지탈 장치, 인터페이스, COM 오브젝트 등과 같은 소프트웨어 오브젝트를 포함하는 것으로 묘사되거나 설명될 수 있다.

[0064] 분산 네트워크 환경을 지원하는 여러가지 시스템, 구성요소 및 네트워크 구성이 있다. 예를 들어, 컴퓨팅 시스템은 유선 또는 무선 시스템에 의해, 로컬 네트워크 또는 널리 분산된 네트워크에 의해 함께 접속될 수 있다. 현재, 다수의 네트워크들은 널리 분산된 컴퓨팅을 위한 기반구조를 제공하고 다수의 상이한 네트워크를 망라하는 인터넷에 연결된다.

[0065] 홈 네트워킹 환경에는, 전원선, 데이타(무선 및 유선), 음성(예를 들어, 전화) 및 엔터테인먼트 매체와 같은 고유의 프로토콜을 각각 지원할 수 있는 적어도 4개의 별도의 네트워크 전송 매체가 있다. 조명 스위치 및 전기 기구와 같은 대부분의 홈 제어 장치는 접속을 위해 전원선을 사용할 수 있다. 데이타 서비스는 홈에 광대역(예를 들어, DSL 또는 케이블 모뎀)으로서 들어갈 수 있으며, 무선(예를 들어, HomeRF 또는 802.11b) 또는 유선(예를 들어, Home PNA, Cat5, 심지어 전원선) 접속을 사용하여 홈 내에 액세스할 수 있다. 음성 트래픽은 홈에 유선(예를 들어, Cat3) 또는 무선(예를 들어, 셀 폰)으로 들어갈 수 있으며, Cat3 유선을 사용하여 홈 내에 분산될 수 있다. 엔터테인먼트 매체는 위성 또는 케이블을 통해 홈에 들어갈 수 있으며, 전형적으로 동축 케이블을 사용하여 홈 내에 분산된다. IEEE 1394 및 DVI는 또한 매체 장치의 클러스터용 디지탈 상호접속으로서 대두되고 있다. 이러한 모든 네트워크 환경들, 및 프로토콜 표준으로서 대두될 수 있는 기타의 것들은 인터넷에 의해 외부 세계에 접속될 수 있는 인트라넷을 형성하기 위해 상호접속될 수 있다. 간략하게 말하면, 여러가지 개별적인 소스들이 데이타의 저장 및 전송을 위해 존재하고, 따라서, 더 나아가, 컴퓨팅 장치는 데이타 프로세싱 파이프라인의 모든 부분에서 콘텐트를 보호하는 방법을 요구할 것이다.

[0066] '인터넷'은 일반적으로, 컴퓨터 네트워킹 분야에 널리 알려진 프로토콜의 TCP/IP 슈트를 이용하는 네트워크 및 게이트웨이의 집합을 칭한다. TCP/IP는 "Transport Control Protocol/Interface Program"의 약어이다. 인터넷은 사용자가 네트워크를 통해 상호작용할 수 있게 하고 정보를 공유할 수 있게 하는 네트워킹 프로토콜을 실행하는 컴퓨터에 의해 상호접속된 지리적으로 분산된 원격 컴퓨터 네트워크의 시스템으로서 설명될 수 있다. 이러한 광범위한 정보 공유 때문에, 인터넷과 같은 원격 네트워크는 개발자들이 기본적으로 제한없이 특별화된

동작 또는 서비스를 실행하기 위한 소프트웨어 어플리케이션을 설계할 수 있는 오픈 시스템으로 상당히 발전되었다.

[0067] 그러므로, 네트워크 기반구조는 클라이언트/서버, 피어-투-피어(peer-to-peer), 또는 하이브리드 아키텍처와 같은 네트워크 토폴로지의 호스트를 가능하게 한다. "클라이언트"는, 관련되지 않은 다른 클래스 또는 그룹의 서비스를 사용하는 클래스 또는 그룹의 멤버이다. 그러므로, 컴퓨팅에서, 한 클라이언트는 한 프로세스이고, 즉 대체로 다른 프로그램에 의해 제공된 서비스를 요청하는 한 세트의 명령어 또는 태스크이다. 클라이언트 프로세스는 다른 프로그램 또는 서비스 자체에 관한 소정의 작업 상세를 "알(know)" 필요없이 요청된 서비스를 사용한다. 클라이언트/서버 아키텍처, 특히 네트워크 시스템에서, 클라이언트는 보통 다른 컴퓨터, 예를 들어 서버에 의해 제공된 공유된 네트워크 자원을 액세스하는 컴퓨터이다. 도 2의 예에서, 컴퓨터(110a, 110b 등)는 클라이언트로 생각될 수 있고, 컴퓨터(10a, 10b 등)는 서버로 생각될 수 있으며, 서버(10a, 10b 등)는 다음에 클라이언트 컴퓨터(110a, 110b 등)에 복제되는 데이타를 유지한다.

[0068] 서버는 전형적으로 인터넷과 같은 원격 네트워크를 통해 액세스가능한 원격 컴퓨터 시스템이다. 클라이언트 프로세스는 제1 컴퓨터 시스템 내에서 동작될 수 있고, 서버 프로세스는 제2 컴퓨터 시스템 내에서 동작될 수 있으며, 통신 매체를 통해 서로 통신함으로써, 분산된 기능을 제공하고, 다수의 클라이언트가 서버의 정보-수집 능력을 이용할 수 있게 한다.

[0069] 클라이언트 및 서버는 프로토콜 층에 의해 제공된 기능을 사용하여 서로 통신한다. 예를 들어, HTTP(Hypertext-Transfer Protocol)는 WWW(World Wide Web)과 함께 사용되는 공통 프로토콜이다. 전형적으로, URL(Universal Resource Locator) 또는 IP(Internet Protocol) 어드레스와 같은 컴퓨터 네트워크 어드레스는 서버 또는 클라이언트 컴퓨터를 서로 식별하기 위해 사용된다. 네트워크 어드레스는 URL 어드레스로 언급될 수 있다. 예를 들어, 통신은 통신 매체를 통해 제공될 수 있다. 특히, 클라이언트 및 서버는 고용량 통신을 위한 TCP/IP 접속을 통해 서로 연결될 수 있다.

[0070] 그러므로, 도 2는 본 발명이 사용될 수 있는, 네트워크/버스를 통해 클라이언트 컴퓨터와 통신하는 서버를 갖는 예시적인 네트워크 또는 분산된 환경을 도시한 것이다. 더욱 상세하게, 다수의 서버(10a, 10b 등)는 본 발명에 따라, LAN, WAN, 인트라넷, 인터넷 등이 될 수 있는 통신 네트워크/버스(14)를 통해, 포터블 컴퓨터, 핸드헬드 컴퓨터, 씬 클라이언트, 네트워크화된 전기기구, 또는 VCR, TV, 오븐, 조명, 히터 등과 같은 그밖의 장치들과 같은 다수의 클라이언트 또는 원격 컴퓨팅 장치(110a, 110b, 110c, 110d, 110e 등)와 상호접속된다. 그러므로, 본 발명은 신뢰된 소스로부터 안전한 콘텐트를 바람직하게 처리, 저장 또는 렌더하는 것이 바람직한 것과 관련된 임의의 컴퓨팅 장치에 적용할 수 있다.

[0071] 통신 네트워크/버스(14)가 인터넷인 네트워크 환경에서, 예를 들어, 서버(10)는 HTTP와 같은 다수의 공지된 프로토콜 중의 어느 것을 통해 클라이언트(110a, 110b, 110c, 110d, 110e 등)가 통신하는 웹 서버일 수 있다. 서버(10)는 또한 분산 컴퓨팅 환경의 특성일 수 있는 바와 같이 클라이언트(110)로서도 작용할 수 있다. 통신은 적절하게 유선 또는 무선으로 될 수 있다. 클라이언트 장치(110)는 통신 네트워크/버스(14)를 통해 통신하거나 통신하지 않을 수 있고, 이와 연관된 독립된 통신을 할 수도 있다. 예를 들어, TV 또는 VCR인 경우에는, 그것의 제어에 대해 네트워크된 양상일 수도 있고 아닐 수도 있다. 각 클라이언트 컴퓨터(110) 및 서버 컴퓨터(10)에는 다양한 어플리케이션 프로그램 모듈 또는 오브젝트(135)가 구비될 수 있고, 파일이 저장될 수 있거나 또는 파일의 일부분(들)이 다운로드되거나 이동될 수 있는 여러가지 종류의 저장 소자 또는 오브젝트에의 접속 또는 액세스가 이루어질 수 있다. 그러므로, 본 발명은 컴퓨터 네트워크/버스(14)와 액세스 및 상호작용할 수 있는 클라이언트 컴퓨터(110a, 110b 등), 클라이언트 컴퓨터(110a, 110b 등)와 상호작용할 수 있는 서버 컴퓨터(10a, 10b 등), 및 그밖의 장치(111) 및 데이타베이스(20)를 갖고 있는 컴퓨터 네트워크 환경에서 활용될 수 있다.

[0072] **디지탈 권한 관리(DRM) 개요**

[0073] 이제 도 11을 참조하면, 공지된 바와 같이, 디지탈 권한 관리(DRM) 및 시행은 디지탈 오디오, 디지탈 비디오, 디지탈 텍스트, 디지탈 데이타, 디지탈 멀티미디어 등과 같은 디지탈 콘텐트(12)와 관련하여 매우 바람직한 것으로, 이러한 디지탈 콘텐트(12)는 사용자에게 배포될 수 있다. 사용자에 의해 수신되고 있는 중에, 이러한 사용자는 퍼스널 컴퓨터(14) 상의 미디어 플레이어 등과 같은 적절한 렌더링 장치의 도움으로 디지탈 콘텐트를 렌더하거나 '플레이'한다.

[0074] 전형적으로, 이러한 디지탈 컨텐를 배포하는 콘텐트 소유자 또는 개발자(이후 '소유자')는 사용자가 이러한 디

지털 콘텐트(12)를 가지고 할 수 있는 것을 제한하고자 한다. 예를 들어, 콘텐트 소유자는 사용자가 제2 사용자에게 이러한 콘텐트(12)를 복사 및 재배포하는 것을 제한하고자 하거나, 또는 배포된 디지털 콘텐트(12)가 제한된 횟수만, 소정의 총 시간동안만, 소정 종류의 기계 상에서만, 소정 종류의 미디어 플레이어 상에서만, 소정 종류의 사용자 등에 의해서만 플레이될 수 있게 하고자 할 수 있다.

[0075] 그러나, 배포가 발생된 후, 이러한 콘텐트 소유자는 디지털 콘텐트에 관한 제어를 거의 하지 않는다. 그 다음, DRM 시스템(10)은 디지털 콘텐트(12)의 임의의 형태의 제어된 렌더링 또는 플레잉을 허용하고, 이러한 제어는 그 디지털 콘텐트의 콘텐트 소유자에 의해 융통성이 있으며 규정가능하다. 전형적으로, 콘텐트(12)는 임의의 적절한 배포 채널에 의해 패키지(13)의 형태로 사용자에게 배포된다. 배포된 디지털 콘텐트 패키지(13)는 콘텐트, 이러한 콘텐트의 라이센스를 획득하는 방법 등을 식별하는 다른 정보뿐만 아니라, 대칭 암호화/복호화 키(KD)(즉, (KD(CONTENT))로 암호화된 디지털 콘텐트(12)를 포함할 수 있다.

[0076] 신뢰-기반의 DRM 시스템(10)은 디지털 콘텐트(12)의 소유자가 이러한 디지털 콘텐트(12)가 사용자의 컴퓨팅 장치(14) 상에 렌더되도록 허용되기 전에 충족되어야 하는 라이센스 규칙을 지정할 수 있게 한다. 이러한 라이센스 규칙은 상술된 일시적 요구사항을 포함할 수 있고, 사용자/사용자의 컴퓨팅 장치(14)(이후, 이러한 용어는 상황이 다른 것을 필요로 하지 않는한 교체가능함)가 콘텐트 소유자 또는 대리인으로부터 얻어야 하는 디지털 라이센스 또는 사용 문서(이후, '라이센스') 내에 구체화될 수 있다. 이러한 라이센스(16)는 또한 사용자의 컴퓨팅 장치에 의해 해독가능한 키에 따라서 가능하다면 암호화된 디지털 콘텐트를 해독하기 위한 암호해독 키(KD)를 포함한다.

[0077] 디지털 콘텐트(12)에 대한 콘텐트 소유자는, 사용자의 컴퓨팅 장치(14)가 라이센스(16)의에 이러한 콘텐트 소유자에 의해 지정된 규칙 및 요구사항을 지킬 것이라는 것을, 즉 라이센스(16) 내의 규칙 및 요구사항이 만족되지 않으면 디지털 콘텐트(12)가 렌더되지 않을 것이라는 것을 신뢰해야 한다. 그 다음, 양호하게, 사용자의 컴퓨팅 장치(14)는 디지털 콘텐트(12)와 연관되고 사용자에 의해 얻어진 라이센스(16)에 구현된 라이센스 규칙에 따르는 것을 제외하고는 디지털 콘텐트(12)를 렌더할 수 없는 신뢰된 구성요소 또는 메카니즘(18)이 구비된다.

[0078] 신뢰된 구성요소(18)는 전형적으로, 라이센스(16)가 유효한 지를 판정하고, 이러한 유효 라이센스(16) 내의 라이센스 규칙 및 요구사항을 리뷰하며, 리뷰된 라이센스 규칙 및 요구사항에 기초하여 요청 사용자가 그 중에서도 특히 탐색된 방식으로 요청 디지털 콘텐트(12)를 렌더할 권리를 가지는지를 판정하는 라이센스 평가기(20)를 갖는다. 이해될 수 있는 바와 같이, 라이센스 평가기(20)는 라이센스(16)의 규칙 및 요구사항에 따라 디지털 콘텐트(12) 소유자의 희망사항을 실행하기 위해 DRM 시스템(10) 내에서 신뢰되며, 사용자는 임의의 목적, 음모 또는 그 반대에 대해 이러한 신뢰 구성요소를 용이하게 변경할 수 없어야만 한다.

[0079] 이해될 수 있는 바와 같이, 라이센스(16) 내의 규칙 및 요구사항은 사용자가 누구인지, 사용자가 어디에 위치되는지, 사용자가 어떤 종류의 컴퓨팅 장치를 사용하는지, 어떤 렌더링 어플리케이션이 DRM 시스템을 호출하고 있는지, 날짜, 시간 등을 포함하는, 소정의 몇가지 요인에 기초하여 사용자가 디지털 콘텐트(12)를 렌더할 권리를 가졌는지의 여부를 지정할 수 있다. 또한, 라이센스(16)의 규칙 및 요구사항은 라이센스(16)를, 예를 들어 소정 수의 플레이, 또는 소정 플레이 시간으로 제한할 수 있다.

[0080] 규칙 및 요구사항은 임의의 적절한 언어 및 신택스(syntax)에 따라 라이센스(16)에 지정될 수 있다. 예를 들어, 언어는 만족되어야 하는 속성 및 값을 단순히 지정하거나(예를 들어, DATE는 X보다 더 늦어야 된다), 또는 지정된 스크립트(예를 들어, IF DATE greater than X, THEN DO...,)에 따른 기능의 성능을 요구할 수 있다.

[0081] 라이센스(16)가 유효하고, 사용자가 그 안의 규칙 및 요구사항을 만족시키는지를 라이센스 평가기(20)가 판정하면, 디지털 콘텐트(12)는 렌더될 수 있다. 특히, 콘텐트(12)를 렌더하기 위해, 암호해독 키(KD)는 라이센스(12)로부터 얻어지고, 콘텐트 패키지(13)로부터 (KD(CONTENT))에 인가되어 실제 콘텐트(12)를 생성하고, 그 다음 실제 콘텐트(12)는 실제로 렌더된다.

[0082] **디지털 콘텐트 출판**

[0083] 도 3은 디지털 콘텐트를 출판하기 위한 본 발명에 따른 시스템 및 방법의 일 실시예의 기능 블록도이다. 여기에서 사용되는 "출판(publishing)"이란 용어는 권한 및 조건의 세트가 누구에게 발행될 수 있을지 뿐만 아니라, 신뢰된 엔티티로 이 엔티티가 그 콘텐트에 대해 발행할 수 있는 권한 및 조건의 세트를 설정하도록 어플리케이션 또는 서비스가 뒤따르는 프로세스를 칭하는 것이다. 본 발명에 따르면, 출판 프로세스는 디지털 콘텐트를 암호화하는 단계, 및 콘텐트의 작성자가 콘텐트의 가능한 모든 사용자용으로 준비한 계속적인 시행가능 권한의 리스트를 연관시키는 단계를 포함한다. 이 프로세스는 콘텐트의 작성자에 의해 의도되지 않으면 임의의 권한으

로의 액세스 또는 콘텐트로의 액세스를 금지하는 안전한 방식으로 실행될 수 있다.

[0084] 본 발명의 일 실시예에서, 특히 3개의 엔티티들이 안전한 디지탈 콘텐트를 출판하기 위해 사용될 수 있다: 즉, 클라이언트(300) 상에서 실행하고 출판하기 위한 콘텐트를 준비하는 콘텐트 준비 어플리케이션(302), 또한 클라이언트 장치(300)에 상주하는 디지탈 권한 관리(DRM) 어플리케이션 프로그램 인터페이스(API)(306), 통신 네트워크(330)를 통해 클라이언트(300)에 통신 결합되는 DRM 서버(320). 본 발명의 일 실시예에서, 통신 네트워크(330)가, 예를 들어 독점적인 인트라넷과 같은 임의의 근거리 통신망 또는 광역 통신망일 수 있다는 것을 이해할 수 있긴 하지만, 통신 네트워크(330)는 인터넷을 포함한다.

[0085] 콘텐트 준비 어플리케이션(302)은 디지탈 콘텐트를 생성하는 임의의 어플리케이션일 수 있다. 예를 들어, 어플리케이션(302)은 디지탈 텍스트 파일, 디지탈 뮤직, 비디오 또는 기타의 콘텐트를 생성하는 다른 출판자 또는 워드 프로세서일 수 있다. 콘텐트는 또한 예를 들어, 라이브 또는 테이프식 이벤트의 스트림된 오디오/비디오와 같은 스트림된 콘텐트를 포함할 수 있다. 본 발명에 따르면, 콘텐트 준비 어플리케이션은 그것의 사용자에게 그 사용자가 제공하는 키를 사용하여 콘텐트를 암호화하게 한다. 어플리케이션(302)은 디지탈 콘텐트를 암호화하는 키를 사용하므로, 암호화된 디지탈 콘텐트 파일(304)을 형성한다. 클라이언트 어플리케이션은 또한 사용자에게 디지탈 콘텐트 파일(304)용 권한 데이타를 제공하게 한다. 권한 데이타는 디지탈 콘텐트의 권한을 갖는 각각의 엔티티에 대한 각각의 아이덴티티(identity)를 포함한다.

[0086] 이러한 엔티티는 예를 들어, 개인, 한 클래스의 개인들, 또는 장치일 수 있다. 각각의 이러한 엔티티마다, 권한 데이타는 또한 그 엔티티가 콘텐트 내에 갖고 있는 권한의 리스트, 및 임의의 또는 이들 모든 권한에 부과될 수 있는 임의의 조건을 포함한다. 이러한 권한은 디지탈 콘텐트를 판독, 편집, 카피, 프린트 등을 할 권리를 포함할 수 있다. 부수적으로, 권한은 포함적 또는 배타적일 수 있다. 포함적 권한은 특정 사용자가 콘텐트의 특정 권한을 갖는다는 것을 나타낸다(예를 들어, 사용자는 디지탈 콘텐트를 편집할 수 있다). 배타적 권한은 특정 사용자가 지정된 것을 제외하고 콘텐트 내의 모든 권한을 갖는다는 것을 나타낸다(예를 들어, 사용자는 디지탈 콘텐트로, 그것을 카피하는 것을 제외한 모든 것을 행할 수 있다).

[0087] 본 발명의 일 실시예에 따르면, 클라이언트 API(306)는 암호화된 디지탈 콘텐트 및 권한 데이타를 DRM 서버(320)에 보낼 수 있다. 후술되는 프로세스를 사용하여, DRM 서버(320)는 사용자가 부여받은 권한을 시행할 수 있는 지를 판정하고, 그렇다면, DRM 서버(320)는 서명된 권한 레이블(SRL)(308)을 형성하기 위해 권한 데이타에 서명한다. 그러나, 일반적으로, 임의의 신뢰된 엔티티는 양호하게 DRM 서버(320)에 의해 신뢰된 키를 사용하여 권한 데이타에 서명할 수 있다. 예를 들어, 클라이언트는 DRM 서버(320)에 의해 클라이언트에게 제공된 키를 사용하여 권한 데이타에 서명할 수 있다.

[0088] 권한 레이블(308)은 권한 설명, 암호화된 콘텐트 키, 및 권한 설명과 암호화된 콘텐트 키를 통한 디지탈 서명을 나타내는 데이타를 포함할 수 있다. DRM 서버가 권한 레이블에 서명하고 있으면, DRM 서버는 서명된 권한 레이블(308)을 클라이언트 장치(300) 상에 저장하는 클라이언트 API(306)를 통해 서명된 권한 레이블(308)을 클라이언트에게 다시 보낸다. 그 다음, 콘텐트 준비 어플리케이션(302)은 서명된 권한 레이블(308)을 암호화된 디지탈 콘텐트 파일(304)과 연관시킨다. 예를 들어, SRL(308)은 암호화된 디지탈 콘텐트와 연결되어 권한 관리된 콘텐트 파일(310)을 형성할 수 있다.

[0089] 그러나, 일반적으로, 권한 데이타는 디지탈 콘텐트와 결합될 필요는 없다. 예를 들어, 권한 데이타는 알려진 위치에 저장될 수 있고, 저장된 권한 데이타에 대한 레퍼런스(reference)는 암호화된 디지탈 콘텐트와 결합될 수 있다. 레퍼런스는 권한 데이타가 저장되는 곳(예를 들어, 권한 데이타를 포함하는 데이타 저장소)을 나타내는 식별자, 및 그 특정 저장 위치에서의 그 특정 권한 데이타에 대응하는(예를 들어, 관심있는 특정 권한 데이타를 포함하는 파일을 식별하는) 식별자를 포함한다. 그 다음, 권한 관리 콘텐트(310)는 임의의 장소의 임의의 사람에게 전달될 수 있고, 콘텐트를 소비할 권한을 갖는 그 엔티티들만이 이들이 할당받은 권한에 따라서만 콘텐트를 소비할 수 있다.

[0090] 도 4는 권한 관리 디지탈 콘텐트를 출판하기 위한 본 발명에 따른 예시적인 방법(400)의 플로우차트로서, 권한 레이블은 DRM 서버에 의해 서명된다. 그러나, 이 실시예는 단지 예시적일 뿐이며, 권한 레이블은 일반적으로 임의의 신뢰된 엔티티에 의해 서명될 수 있다는 것을 이해할 수 있을 것이다. 일반적으로, 디지탈 콘텐트를 출판하기 위한 본 발명에 따른 방법은, 콘텐트 키(CK)를 사용하여 디지탈 콘텐트를 암호화하는 단계, 디지탈 콘텐트와 연관된 권한 설명을 생성하는 단계, (PU-DRM(CK))를 생기게 하기 위해 DRM 서버(PU-DRM)용 공개 키에 따라 콘텐트 키(CK)를 암호화하는 단계, 및 권한 설명과 (PU-DRM(CK))의 결합을 통해 (PU-DRM)에 대응하는 개인 키(private key)에 기초하여 디지탈 서명을 생성하는 단계를 포함한다.

[0091] 단계 402에서, 어플리케이션(302)은 디지탈 콘텐트를 암호화하는데 사용되는 콘텐트 키(CK)를 생성한다. 일반적으로, 디지탈 콘텐트를 암호화하기 위해 임의의 키가 사용될 수 있음에도 불구하고, 양호하게는 콘텐트 키(CK)는 대칭 키이다. 때로 "비밀 키(secret key)" 알고리즘으로 언급되는 대칭 키 알고리즘은 동일한 키를 사용하여 이들이 메시지를 암호화하기 위해 행하는 것처럼 메시지를 암호해독한다. 그러한 이유로, (CK)가 비밀로 유지되는 것이 바람직하다. 송신자와 수신자 사이에서 (CK)를 공유하는 것은 권한없이 이러한 (CK)를 가로채는 것을 막기 위해 매우 신중하게 행해져야 된다. (CK)가 암호화기와 암호해독기 사이에서 공유되기 때문에, (CK)는 임의의 암호화된 메시지가 전송되기 전에 통신되는 것이 바람직하다.

[0092] 몇가지 대칭 키 생성 알고리즘은 본 기술분야에 잘 알려져 있다. 임의의 대칭 알고리즘이 사용될 수 있다는 것을 이해할 수 있지만, 일 실시예에서는 데이타 암호화 표준(DES)이 채용된다. 이러한 대칭 키 알고리즘의 예는 AES, Triple-DES, IDEA(International Data Encryption Algorithm), Cast, Cast-128, RC4, RC5 및 SkipJack을 포함하는데, 이것에 제한되지는 않는다.

[0093] 단계 404에서, 어플리케이션(302)은 표기(CK(content))를 사용하여 기입될 수 있는 암호화된 디지탈 콘텐트(304)를 형성하기 위해 대칭 콘텐트 키(CK)로 디지탈 콘텐트를 암호화한다. 어플리케이션(302)을 사용하는 작성자는 또한 디지탈 콘텐트와 연관된 권한 데이타를 생성할 수 있다. 권한 데이타는 콘텐트를 소비할 권리가 있을 수 있는 엔티티의 리스트, 및 특정 권한에 부과될 수 있는 임의의 조건과 함께, 각 엔티티가 콘텐트와 관련하여 소유하는 특정 권한을 포함한다. 이러한 권한은 예를 들어, 콘텐트의 뷰잉, 콘텐트의 프린팅 등을 포함할 수 있다. 어플리케이션(302)은 권한 데이타를 API(306)에 제공한다. XML/XrML 포맷의 권한 데이타의 한 예는 첨부 1로서 본 명세서에 첨부된다.

[0094] 단계 406에서, API(306)는 콘텐트 키(CK)를 암호화하는데 사용되는 제2 암호화 키(DES1)를 생성한다. 양호하게, (DES1)도 대칭 키이다. 단계 408에서, API(306)는 (CK)를 (DES1)로 암호화하여 (DES1(CK))를 생기게 한다. 단계 410에서, API(306)는 (CK)를 버리고, 그 결과 (CK)는 이제 (DES1(CK))를 암호해독함으로써만 얻어질 수 있게 된다. (CK(content))가 중앙 DRM 서버(320)에 대해 보호될 수 있게 하고, 콘텐트에 대한 모든 "라이센스 요청"이 권한 데이타에 따라 중심적으로 행해질 수 있게 하는 것을 보증하기 위해 위해, API(306)는 단계 412에서, 제공된 DRM 서버(320)와 접촉하여 그것의 공개 키(PU-DRM)을 검색한다. 단계 414에서, API(306)는 (DES1)을 (PU-DRM)으로 암호화하여 (PU-DRM(DES1))을 생기게 한다. 그러므로, (CK(content))를 암호해독하기 위해 요구되는 바와 같이, DRM 서버(320)가, (CK)로의 액세스를 행할 수 있는 유일한 엔티티임을 보증하기 위해, (CK)는 (PU-DRM)에 대해 보호될 수 있다. 단계 416에서, API(306)는 권한 데이타(즉, 권한부여된 엔티티의 리스트, 및 그 리스트 내의 각각의 권한부여된 엔티트와 연관된 각각의 권한 및 조건)를 (DES1)로 암호화하여 (DES1(rightsdata))를 생기게 한다.

[0095] 대안적인 실시예에서, (CK)는 권한 데이타를 직접 암호화하는데 사용되어 (CK(rightsdata))를 생기게 할 수 있고, (PU-DRM)은 (CK)를 직접 암호화하는데 사용되어 (PU-DRM(CK))를 생기게 할 수 있으며, 이로 인해 (DES1)의 사용이 완전히 보류된다. 그러나, 권한 데이타 및 (CK)를 암호화하기 위해 (DES1)을 사용하는 것은, 그 (DES1)이 DRM 서버를 따를 수 있는 임의의 특정 알고리즘을 따를 수 있게 하는 반면에, (CK)는 DRM 서버와는 독립된 엔티티에 의해 지정될 수 있고, 거기에 따르지 않을 수도 있다.

[0096] 단계 418에서, 콘텐트 보호 어플리케이션(302)은 서명을 위한 권한 레이블로서 (PU-DRM(DES1)) 및 (DES1(rightsdata))를 DRM 서버(320)에 제출할 수 있다. 대안적으로, 클라이언트 자신이 권한 데이타에 서명할 수 있다. 권한 데이타가 서명을 위해 서버에 제출되고 있으면, 단계 420에서, DRM 서버(320)는 권한 데이타를 액세스하고, 제출된 권한 레이블의 권한 및 조건을 시행할 수 있음을 검증한다. 권한 데이타를 시행할 수 있음을 검증하기 위해, DRM 서버(320)는 (PR-DRM)을 (PU-DRM(DES1))에 적용하여 (DES1)을 생기게 한 다음에, (DES1)을 (DES1(rightsdata))에 적용하여 빈곳에 권한 데이타를 생기게 한다. 그 다음, 서버(320)는 권한 데이타 내에 지정된 사용자, 권한 및 조건이 서버(320)에 의해 시행된 임의의 정책 내에 있는 지를 검증하기 위해 임의의 정책 체크를 할 수 있다. 서버(320)는 (PU-DRM(DES1)) 및 (DES1(rightsdata))를 포함하는 원래 제출된 권한 레이블에 서명하여, 서명된 권한 레이블(SRL)(308)을 생기게 하고(여기에서, 서명은 DRM 서버(320)의 개인 키(PR-DRM)에 기초한 것임), SRL(308)을 API(306)로 다시 복귀시키며, 그 다음 복귀된 SRL(308)을 클라이언트 어플리케이션(302)에 제공한다.

[0097] SRL(308)은 변경이 방지된 디지탈 서명된 문서이다. 부수적으로, SRL(308)은 콘텐트를 암호화하는데 사용된 실제 키 형태 및 알고리즘에 관계없지만, 이것이 보호하고 있는 콘텐트에 대해 강한 1-1 관계를 유지한다. 이제 도 4a를 참조하면, 본 발명의 일 실시예에서, SRL(308)은 그중에서도 특히; 아마도 콘텐트의 ID를 포함하는,

SRL(308)의 기본인 콘텐트 상의 정보; (PU-DRM(DES1)), 및 DRM 서버를 네트워크 상에 위치시키기 위한 URL과 같은 참고(referral) 정보 및 URL 고장시의 대처 정보를 포함하는, SRL(308)에 서명하는 DRM 서버 상의 정보; SRL(308) 자체를 설명하는 정보; (DES1(rightsdata)):(DES1(CK)); 및 S(PR-DRM)을 포함할 수 있다. XML/XrML의 샘플 SRL(308)은 본 명세서에 첨부 2로서 첨부된다.

[0098] 신뢰된 엔티티가 권한 데이타에 서명하여 서명된 권한 레이블(308)을 생성하는 것을 확실하게 하기 위해, DRM 서버는, 권한 레이블(308)의 권한 데이타에 설명된 바와 같이 발행자에 의해 발표된 기간에 따라 콘텐트에 대한 라이센스를 발행할 것이라는 것을 표명하고 있다. 알 수 있는 바와 같이, 사용자는, 특히 라이센스가 콘텐트 키(CK)를 포함하기 때문에, 콘텐트를 렌더하기 위해서는 라이센스를 취득하록 요구된다. 사용자가 암호화된 콘텐트에 대한 라이센스를 얻고 싶을 때, 그 사용자는 콘텐트용 SRL(308)을 포함하는 라이센스 요청, 및 사용자의 신임장을 검증하는 증명서를 DRM 서버(320) 또는 다른 라이센스 발행 엔티티에게 제시할 수 있다. 그 다음, 라이센스 발행 엔티티는 (PU-DRM(DES1)) 및 (DES1(rightsdata))를 암호해독하여 권한 데이타를 생성하고, 라이센스 요청 엔티티에게 작성자(있다면) 에 의해 승인된 모든 권한을 리스트하며, 이들 지정된 권한만으로 라이센스를 구성할 수 있다.

[0099] 바람직하게는, 어플리케이션(302)이 SRL(308)을 수신시에, 이러한 어플리케이션(302)은 서명된 권한 레이블(308)을 대응하는 (CK(content))(304)와 연결시켜 관리된 디지탈 콘텐트를 형성한다. 대안적으로, 권한 데이타는 암호화된 디지탈 콘텐트가 제공된 알려진 위치에 대한 레퍼런스를 갖고 알려진 위치에 저장될 수 있다. 그러므로, DRM-가능 렌더링 어플리케이션은 렌더링 어플리케이션이 렌더하기 위해 시도하고 있는 콘텐트의 일부를 통해 서명된 권한 레이블(308)을 발견할 수 있다. 이 발견은 DRM 라이센싱 서버(320)에 대한 라이센스 요청을 시작하기 위해 렌더링 어플리케이션을 트리거한다. 예를 들어, 출판 어플리케이션(302)이 DRM 라이센싱 서버(320)에 대한 URL을 저장할 수 있거나, DRM 라이센싱 서버(320)가 디지탈식 서명 이전에 권한 레이블 내로 메타데이타의 일부로서 자신의 URL을 포함할 수 있으므로, 렌더링 어플리케이션에 의해 호출된 DRM 클라이언트 API(306)는 올바른 DRM 라이센싱 서버(320)를 식별할 수 있다. 예를 들어 GUID(globally unique identifier)와 같은 유일한 식별자는 서명되기 전에 권한 레이블 내로 삽입되는 것이 바람직하다.

[0100] 본 발명의 일 실시예에서, 단순한 오브젝트 액세스 프로토콜(SOAP)은 콘텐트 보호 어플리케이션(302) 또는 렌더링 어플리케이션과 DRM 서버(320) 사이의 통신에 사용될 수 있다. 부가적으로, API(306)와 같은 API 라이브러리는 어플리케이션(302)과 같은 어플리케이션이 DRM 프로토콜의 클라이언트측을 구현하도록 요구되지 않고, 단지 로컬 API 호출을 생성할 수 있도록 제공될 수 있다. 임의의 적절한 포맷이 권한 설명 및 다른 데이타를 위해 사용될 수 있다는 것을 이해할 수 있지만, 디지탈 콘텐트에 대한 권한 설명, 라이센스 및 권한 레이블을 설명하는데 XrML, XML 언어를 사용하는 것이 바람직하다.

[0101] **출판된 콘텐트용 라이센스 획득**

[0102] 도 5는 권한 관리 디지탈 콘텐트를 라이센싱하기 위한 본 발명에 따른 시스템 및 방법의 일 실시예의 기능 블록도이다. "라이센싱(licensinh)"이라는 용어는 여기에서, 라이센스 내에 명명된 엔티티가 라이센스 내에 지정된 조건에 따라 콘텐트를 소비할 수 있게 할 수 있는 라이센스를 요청하여 수신하도록 어플리케이션 또는 서비스가 뒤따르는 프로세스를 칭하는 것이다. 라이센싱 프로세스로의 입력은 라이센스가 요청되고 있는 콘텐트와 연관된 서명된 권한 레이블(SRL), 및 라이센스가 요청되고 있는 엔티티(들)의 공개 키 증명서(들)을 포함할 수 있다. 라이센스를 요청하는 엔티티는 라이센스가 요청되고 있는 엔티티일 필요는 없다는 것을 알기 바란다. 전형적으로, 라이센스는 SRL(308)로부터의 권한 설명, 암호화된 콘텐트를 암호해독할 수 있는 암호화된 키, 및 권한 설명 및 암호화된 키를 통한 디지탈 서명을 포함한다.

[0103] 어플리케이션(302)이 권한 관리 콘텐트(310)를 소비하는 한가지 방식은 클라이언트 API(306)가 권한 관리 콘텐트(310)의 서명된 권한 레이블(308)을 통신 네트워크(330)를 통해 DRM 서버(320)로 전송하는 것이다. DRM 서버(320)의 위치는 예를 들어, SRL(308) 내의 참조 정보에서 발견될 수 있다. 이러한 실시예에서, 후술되는 프로세스를 통해 DRM 라이센싱 서버(320)는 권한 레이블 내의 권한 설명을 사용하여 라이센스를 발행할 것인 지를 판정하고, 그렇다고 하면 그 라이센스로 포함하기 위한 권한 설명을 이끌어낼 수 있다.

[0104] 상술된 바와 같이, 권한 레이블(308)은 DRM 서버(320)(PU-DRM)의 공개 키(즉, PU-DRM(CK))에 따라 암호화된 콘텐트 키(CK)를 포함한다. 라이센스를 발행하는 프로세스에서, DRM 서버(320)는 이 값을 확실하게 암호해독하여 (CK)를 얻는다. 그 다음, 이것은 (CK)(즉, (PU-ENTITY(CK))를 다시 암호화하기 위해 라이센스 요청 시에 간과된 공개키 인증서 내의 공개 키(PU-ENTITY)를 사용한다. 새로 암호화된 (PU-ENTITY(CK))는 서버(320)가 라이센스 내로 배치하는 것이다. 그러므로, 연관된 개인 키(PR-ENTITY)의 소유자만이 (PU-ENTITY(CK))로부터 (CK)를

복구할 수 있기 때문에, 라이센스는 (CK)를 노출시킬 위험없이 호출자에게 복귀될 수 있다. 그 다음, 클라이언트 API(306)는 (CK)를 사용하여 암호화된 콘텐트를 암호해독해서, 해독된 디지탈 콘텐트(312)를 형성한다. 그 다음, 클라이언트 어플리케이션(302)은 라이센스 내에 제공되는 권한에 따라 암호해독된 디지탈 콘텐트(312)를 사용할 수 있다.

[0105] 대안적으로, 예를 들어, 출판 클라이언트와 같은 클라이언트는 콘텐트를 소비하기 위해 자신의 라이센스를 발행할 수 있다. 이러한 실시예에서, 안전한 프로세스는 적절한 환경 하에서 디지탈 콘텐트를 암호해독하기 위해 필요한 키(들)을 클라이언트에게 제공하는 클라이언트 컴퓨터 상에서 실행될 수 있다.

[0106] 도 6a 및 도 6b는 권한 관리 디지탈 콘텐트를 라이센싱하기 위한 본 발명에 따른 방법(600)의 일 실시예의 플로우차트를 제공한다. 본 발명에 따르면, 요청 엔티티는 하나 이상의 잠재적 라이센시(licensee)를 대신하여 라이센스 요청을 제출할 수 있다. 요청 엔티티는 잠재적 라이센시 중의 하나이거나 그렇지 않을 수도 있다. 잠재적 라이센시는 사람, 그룹, 장치, 또는 어떤 방식으로든 콘텐트를 소비할 수 있는 소정의 다른 엔티티일 수 있다. 방법(600)이 DRM 서버가 라이센스 요청을 프로세스하는 일 실시예와 관련하여 이제 설명될 것이나, 라이센스 요청 프로세싱은 또한 클라이언트 상에서 실행되고 직접 클라이언트에 의해 라이센스가 발행될 수도 있다는 것을 이해해야 한다.

[0107] 단계 602에서, 예를 들어 DRM 서버와 같은 라이센스 발행 엔티티는 라이센스 요청을 수신한다. 바람직하게는, 라이센스 요청은 공개 키 인증서, 또는 하나 이상의 요청된 라이센시 각각의 아이덴티티를 포함한다.

[0108] 단계 604에서, 요청 엔티티(즉, 라이센스 요청을 생성하는 엔티티)가 인증된다. 본 발명의 일 실시예에 따르면, 라이센스 발행 엔티티는 프로토콜(예를 들어, 시도-응답) 인증을 사용하여 요청 엔티티의 아이덴티티를 판정하도록 구성될 수 있고, 또는 요청 엔티티의 인증을 요구하지 않도록(즉, "익명 인증 허용"이라고도 함) 구성될 수 있다. 인증이 요구되는 경우, 소정 형태의 인증 스킴이 사용될 수 있다(예를 들어, 상술된 시도-응답 스킴, MICROSOFT.NET, PASSPORT, WINDOWS 인증, x509 등과 같은 사용자 아이디 및 패스워드 스킴 등). 양호하게, 통합된 정보 시스템에 의해 지원되는 소정의 프로토콜 인증 스킴을 지원할 뿐만 아니라. 익명 인증이 허용된다. 인증 단계의 결과는 예를 들어 "익명" 아이덴티티(익명 인증시), 또는 개인 어카운트 아이덴티티과 같은 아이덴티티일 수 있다. 라이센스 요청이 어떠한 이유로 인증될 수 없으면, 에러가 복귀되어 라이센스가 허여되지 않는다.

[0109] 단계 606에서, 인증된 엔티티는 권한을 부여받는다 - 즉, 단계 608에서 인증된 엔티티가 (스스로 또는 다른 엔티티를 대신하여) 라이센스 요청을 허가받았는지 판정된다. 양호하게, 라이센스 발행 엔티티는 라이센스 요청이 허가된(또는 허가되지 않은) 엔티티의 리스트를 저장한다. 일 실시예에서, 이 아이덴티티 리스트 내의 아이덴티티는 양자가 다 될 수 있지만, 라이센스가 요청되고 있는 엔티티의 아이덴티티가라기 보다는, 요청을 행하는 엔티티의 아이덴티티가다. 예를 들어, 개인 어카운트 아이덴티티는 라이센스 요청을 직접 행하는 것이 금지될 수 있지만, 신뢰된 서버 프로세스는 이러한 엔티티 대신에 라이센스 요청을 행할 수 있다.

[0110] 본 발명에 따르면, 라이센스 요청은 공개 키 인증서 또는 각각의 잠재적 라이센시에 대한 아이덴티티를 포함할 수 있다. 라이센스가 하나의 라이센시에 대해서만 요청되면, 하나의 인증서 또는 아이덴티티만이 명명된다. 라이센시가 다수의 라이센스에 대해 요청되면, 인증서 또는 아이덴티티는 각각의 잠재적 라이센시에 대해 명명될 수 있다.

[0111] 바람직하게, 라이센스 발행 엔티티는 각각의 유효 라이센시에 대한 공개 키 인증서를 가질 수 있다. 그러나, 어플리케이션(302)은 주어진 사용자에게 라이센스를 생성하고 싶지만, 어플리케이션(302)은 그 사용자에 대한 공개 키 인증서로 액세스할 수 없을 수 있다. 이러한 상황에서, 어플리케이션(302)은 라이센스 요청시에 사용자 아이덴티티를 지정할 수 있고, 그 결과 라이센스 발행 엔티티는 디렉토리 서비스 내에서의 조사를 실행하여 적절한 사용자의 공개 키 인증서를 복귀시키는 등록된 인증서 플러그-인 모듈을 호출할 수 있다.

[0112] 단계 608에서, 공개 키 인증서가 라이센스 요청에 포함되지 않았다고 발행 엔티티가 판정하면, 발행 엔티티는 특정 아이덴티티를 이용하여 적절한 공개 키 인증서에 대한 디렉토리 서비스 또는 데이타베이스 내에서의 조사를 실행하기 위해 지정된 아이덴티티를 사용한다. 단계 610에서, 발행 엔티티가 인증서가 디렉토리 내에 있다고 판정하면, 단계 612에서 인증서가 검색된다. 일 실시예에서, 인증서 플러그-인은 디렉토리 액세스 프로토콜에 의해 디렉토리 서비스로부터 공개 키 인증서를 검색하는데 사용된다. 인증서가 주어진 잠재적 라이센시에 대해 발견되지 않으면, 요청 또는 디렉토리 내에서, 라이센스 서버는 그 잠재적 라이센시에 대한 라이센스를 생성하지 않고, 단계 614에서, 에러가 요청 엔티티로 복귀된다.

[0113] 라이센스 발행 엔티티가 적어도 하나의 잠재적 라이센시에 대해 공개 키 인증서를 갖는다고 하면, 단계 616에서 발행 엔티티는 라이센시 인증서의 신용을 확인한다. 양호하게, 발행 엔티티는 한 세트의 신뢰된 인증서 발행인 인증서로 구성되고, 라이센시 인증서의 발행인이 신뢰된 발행인 리스트 내에 있는 지를 판정한다. 단계 616에서, 라이센시 인증서의 발행인이 신뢰된 발행인 리스트 내에 없다고 발행 엔티티가 판정하면, 그 라이센시에 대해 요청은 실패하고, 단계 614에서 에러가 발생된다. 그러므로, 신뢰된 발행인에 의해 인증서가 발행되지 않은 소정의 잠재적 라이센시는 라이센스를 수신할 수 없다.

[0114] 부수적으로, 발행 엔티티는 양호하게, 신뢰된 발행인 인증서로부터 개인 라이센시 공개 키 인증서로 진행하는 인증서 체인 내의 모든 엔티티에 관해 디지탈 서명 확인을 실행한다. 체인 내의 디지탈 서명을 확인하는 프로세스는 잘 알려진 알고리즘이다. 주어진 잠재적 라이센시에 대한 공개 키 인증서가 확인되지 않거나 체인 내의 인증서가 확인되지 않으면, 잠재적 라이센시는 신뢰받지 못하므로, 라이센스는 그 잠재적 라이센시에게 발행되지 않는다. 그렇지 않으면, 단계 618에서, 라이센스가 발행될 수 있다. 이 프로세스는 단계 620에서, 라이센스가 요청된 모든 엔티티가 처리될 때까지 반복된다.

[0115] 도 6b에 도시된 바와 같이, 라이센스 발행 엔티티는 라이센스 요청 시에 수신된 서명된 권한 레이블(308)을 확인하도록 진행한다. 일 실시예에서, 발행 엔티티는 권한 레이블 플러그-인, 및 후위 데이타베이스를 사용하여, 발행 엔티티에 의해 서명된 모든 권한 레이블의 마스터 카피를 서버에 저장한다. 권한 레이블은 출판 시에 이 레이블 내에 배치된 GUID에 의해 식별된다. 라이센스 시기에(단계 622에서), 발행 엔티티는 라이센스 요청에 입력된 권한 레이블을 분석하여 그 GUID를 검색한다. 그 다음에, 이 GUID를 권한 레이블 플러그-인으로 보내서, 데이타베이스에 대한 질의를 발행하여, 마스터 권한 레이블의 카피를 검색한다. 마스터 권한 레이블은 라이센스 요청 시에 보내진 권한 레이블의 카피보다 더욱 최신의 것일 수 있고, 이하의 단계에서 요청 시에 사용된 권한 레이블일 수 있다. GUID에 기초하여 데이타베이스 내에서 권한 레이블이 발견되지 않으면, 발행 엔티티는 그 정책을 체크하여, 단계 624에서 요청 시의 권한 레이블에 기초하여 라이센스의 발행이 여전히 허가되었는 지를 판정한다. 이 정책이 이것을 허가하지 않았으면, 단계 626에서 라이센스 요청은 실패하고, 단계 628에서 에러가 API(306)로 복귀될 수 있다.

[0116] 단계 630에서, 라이센스 발행 엔티티는 권한 레이블(308)을 확인한다. 권한 레이블 상의 디지탈 서명이 확인되고, 라이센스 발행 엔티티가 권한 레이블의 발행인(서명한 엔티티)이 아니면, 라이센스 발행 엔티티는 권한 레이블의 발행인이 다른 신뢰된 엔티티(예를 들어, 라이센스 발행 엔티티가 키 재료를 공유할 수 있게 된 엔티티)인지 판정한다. 권한 레이블이 확인되지 않거나, 신뢰된 엔티티에 의해 발행되지 않으면, 단계 626에서 라이센스 요청은 실패하고, 단계 628에서 에러가 API(306)에 복귀될 수 있다.

[0117] 모든 확인이 발생된 후에, 라이센스 발행 엔티티는 권한 레이블(308)을 각각의 승인된 라이센시에 대한 라이센스로 변환한다. 단계 632에서, 라이센스 발행 엔티티는 각 라이센시에게 발행될 라이센스에 대한 각각의 권한 설명을 생성한다. 각 라이센시마다, 발행 엔티티는 권한 레이블 내의 권한 설명 내에 명명된 아이덴티티에 대하여 그 라이센시의 공개 키 인증서 내에 명명된 아이덴티티를 확인한다. 권한 설명은 모든 권한 또는 권한 세트, 및 라이센스 내의 그 권한 또는 권한 세트를 실행할 수 있는 아이덴티티 세트에 할당된다. 라이센시의 아이덴티티가 연관되는 모든 권한 또는 권한 세트에 대해, 그 권한 또는 권한 세트는 라이센스의 새로운 데이타 구조 내로 카피된다. 이렇게 얻어진 데이타 구조는 특정 라이센시에 대한 라이센스 내의 권한 설명이다. 이 프로세스의 일부로서, 라이센스 발행 엔티티는 권한 레이블의 권한 설명 내의 소정의 권한 또는 권한 세트와 연관될 수 있는 소정의 전제조건을 검토한다. 예를 들어, 권한은 지정된 시간 후에 라이센스의 발행으로부터 라이센스 발행 엔티티를 제한하는 권한과 연관된 시간 전제조건을 가질 수 있다. 발행 엔티티가 현재의 시간을 체크할 필요가 있는 경우에, 전제조건에서 내에 지정된 시간이 경과되면, 발행 엔티티는 라이센시의 아이덴티티가 그 권한과 연관되었다고 하더라도 라이센시에게 그 권한을 발행할 수 없다.

[0118] 단계 636에서, 발행 엔티티는 권한 레이블(308)로부터 (PU-DRM(DES1)) 및 (DES1(CK))를 획득하고, (PR-DRM)을 적용하여, (CK)를 얻는다. 그 다음, 발행 엔티티는 라이센시의 공개 키 인증서 (PU-ENTITY)를 사용하여 (CK)를 다시 암호화해서, (PU-ENTITY(CK))를 생기게 한다. 단계 638에서, 발행 엔티티는 생성된 권한 설명을 (PU-ENTITY(CK))와 연결시키고, (PR-DRM)을 사용하여 최종 데이타 구조를 디지탈 서명한다. 이 서명된 데이타 구조는 이 특정 라이센시에 대한 라이센스이다.

[0119] 단계 640에서, 발행 엔티티가 특정 요청에 대해 생성할 라이센스가 더 없다고 판정하면, 발행 엔티티는 생성된 0개 이상의 라이센스를 가질 수 있다. 생성된 라이센스는 단계 642에서, 이들 라이센스와 연관된 인증서 체인(예를 들어, 그것의 인증서를 발행한 인증서뿐만 아니라 서버 자신의 공개 키 인증서 등등)과 함께, 요청 엔티

티에 복귀된다.

[0120] 본 발명에 따른 시스템의 일 실시예에서는, 다수의 라이센서 키가 사용될 수 있다. 이러한 실시예에서, 권한 레이블(308)을 통하여 라이센스 내로 들어가는 암호화된 콘텐트 키(CK)는 실제로 어떤 임의의 데이타일 수 있다. 특히 유용한 한가지 변형은 권한 설명 내의 상이한 권한 또는 상이한 본인과 각각 연관된 다수의 분리되고 암호화된 콘텐트 키(CK)를 사용하는 것이다. 예를 들어, 앨범의 디지탈 버전의 노래는 모두 상이한 키(CK)로 암호화될 수 있다. 이들 키(CK)는 동일한 권한 레이블 내에 포함될 수 있지만, 한 본인은 한 노래를 플레이할 권리를 가질 수 있고(예를 들어, 그는 자기의 라이센스 내에서 하나의 키를 얻을 권리만을 가질 수 있고), 제2의 본인은 모든 노래를 플레이할 권리를 가질 수 있다(예를 들어, 그녀는 자기의 라이센스 내에서 모든 키를 얻을 권리를 가질 수 있다).

[0121] 양호하게, 본 발명에 따른 시스템은 출판 어플리케이션/사용자가 권한 레이블(308) 내의 라이센시의 그룹 또는 클래스를 명명할 수 있게 한다. 이러한 실시예에서, 라이센스 발행 엔티티는 권한 레이블 내에 명명된 임의의 그룹/클래스를 검토하여, 현재의 라이센시 아이덴티티가 그 그룹/클래스의 구성원인지를 판정한다. 명명된 그룹/클래스 내에서 구성원이 발견되면, 발행 엔티티는 그룹/클래스와 연관된 권한 또는 권한 세트를 라이센스에 사용된 권한 설명 데이타 구조에 추가할 수 있다.

[0122] 본 발명의 일 실시예에서, DRM 서버 내의 출판 및 라이센스 프로토콜 인터페이스는 호출하는 어플리케이션 또는 사용자의 인증 및 권한부여를 지원하고, DRM 서버용 관리 콘솔은 관리자가 라이센싱 및 출판 인터페이스에 대한 액세스 제어 리스트를 생성할 수 있게 한다. 이것은 서버의 고객이 사용자/어플리케이션이 출판, 라이센스, 또는 이 둘 다를 하도록 허가하는 정책을 적용할 수 있게 한다.

[0123] **서명된 권한 레이블(308)의 변경 또는 재판(republishing)**

[0124] 본 발명의 일 실시예에서, SRL(308)은 콘텐트의 사용자가 그와 같이 하도록 충분한 약속을 부여받게 되었으면 "재판"될 수 있다. 즉, 허가받은 경우, 사용자는 SRL(308) 내의 권한 데이타를 변경할 수 있다. 특히, 권한 데이타를 변경할 허가를 받은 사용자는 연관된 콘텐트와 관련하여 기본적으로 스스로 광범위한 권리를 허여할 수 있는 만큼, 권한 데이타를 변경하기 위한 허가는 드물고 현명하게 부여되어야 된다. 생각건대, 이러한 사용자는 심지어, 콘텐트를 노출시켜 그것을 세상에 보내도록 권한을 부여할 수도 있다.

[0125] 여기에서, 변경을 위한 허가는 특정 사용자 또는 사용자 클래스가 권한 데이타 및 권한 레이블(308)을 실제로 변경 또는 '재판'할 수 있다는 표시를 SRL(308)내의 권한 데이타 내에 포함함으로써 나타낸다. DRM 서버(320)가 라이센스 요청과 관련하여 이러한 약속이 있는 SRL(308)을 수신할 때, DRM 서버(320)는 사용자의 공개키(즉, PU-ENTITY)에 따라 암호화된 대칭 키(DES1)를 사용자의 요청된 라이센스 내에 포함시켜 (PU-ENTITY(DES1))를 생기게 한다.

[0126] 그러므로, SRL(308) 내의 권한 데이타를 편집하기 위해, 이제 도 7을 참조하면, 사용자는 라이센스로부터 (PU-ENTITY(DES1))을 검색하고(단계 701), 이것에 (PR-ENTITY)를 적용하여 (DES1)을 생기게 하며(단계 703), (DES1(rightsdata))를 SRL(308)로부터 검색하고(단계 705), 거기에 (DES1)을 적용하여 권한 데이타를 생기게 한다(단계 707). 그 다음, 사용자는 원하는 대로 권한 데이타를 변경하고(단계 709), 서명된 권한 레이블(308)를 얻기 위해 도 4와 관련하여 설명된 방식으로 DRM 서버(320)에 변경된 권한 데이타를 제출한다(단계 711). 물론, 여기서, 서명된 권한 레이블(308)은 실제로 재판된 SRL(308)이고, 따라서 그 SRL(308)이 수신되기만 하면(단계 713), 사용자는 연관된 콘텐트에 연결된 원래의 SRL(308)을 분리하고(단계 715), 그 다음에 재판된 SRL(308)을 이러한 콘텐트에 연결시킨다(단계 717).

[0127] 그러므로, 알 수 있는 바와 같이, SRL(308)을 재판하면 사용자가 연관된 콘텐트를 변경할 필요없이 권한, 조건 및 사용자를 포함하는 SRL(308) 내의 권한 데이타를 갱신할 수 있게 한다. 특히, 재판은 연관된 콘텐트를 새로운 (CK)로 다시 암호화할 것을 필요로 하지 않는다. 또한, 재판은 특히 새로운 SRL(308)에 카피될 수 있는 다수의 아이템을 원래의 SRL(308)이 갖고 있기 때문에 새로운 SRL을 생성할 것을 필요로 하지 않는다.

[0128] **서명된 권한 레이블(308)의 자체-출판**

[0129] 본 발명의 일 실시예에서, SRL(308)은 요청 사용자 자신에 의해 서명될 수 있다. 따라서, 사용자는 콘텐트의 연관된 부분에 대한 SRL(308)을 얻기 위해 DRM 서버(320)에 접촉할 필요가 없다. 그 결과, 자체-출판은 또한 오프-라인 출판이라고도 한다. 이러한 실시예에서, 사용자는 이러한 자체-출판된 SRL(308)에 기초하여 라이센스를 요청하기 위해 DRM 서버(320)에 접촉하도록 요구될 수 있다. 또한, 출판 엔티티가 그 자신의 라이센스를

발행할 수 있게 될 수 있다는 것을 이해해야 한다.

[0130] 특히, 이제 도 8을 참조하면, 이 실시예에서, 사용자는 (PU-ENTITY(PR-CERT))를 생기게 하기 위해 사용자의 공개 키(PU-ENTITY)에 따라 암호화된 공개 키(PU-CERT) 및 대응하는 개인 키(PR-CERT)를 포함하는 DRM 인증서(810)를 DRM 서버(320)로부터 수신함으로써 자체-출판하도록 먼저 준비된다. 이 인증서는 더욱 상세하게 후술되는 바와 같이, DRM 서버(320)가 검증할 수 있도록 DRM 서버(320)의 개인 키(PR-DRM)에 의해 서명되어야 된다. 알 수 있는 바와 같이, DRM 인증서(810)는 사용자에게 자체-출판하도록 권한을 부여한다. 알 수 있는 바와 같이, 키 쌍(PU-CERT, PR-CERT)은 (PU-ENTITY, PR-ENTITY)로부터 분리되고, 구체적으로 자체-출판을 위해 사용된다. 키 쌍(PU-CERT, PR-CERT)은 DRM 인증서(810)가 사용자의 공개 키(PU-ENTITY)만을 포함하고, DRM 서버(320)가 그것을 검증할 수 있도록 DRM 서버(320)의 개인 키(PR-DRM)에 의해 서명되는 경우에는 사용되지 않을 수 있다.

[0131] 자체-출판은 수행된 단계와 관련하여 사용자가 기본적으로 DRM 서버(320)를 대신한다는 점에서 도 4에 도시된 출판과 다르다. 중요하게는, 사용자는 DRM 증명서(810)(즉, S(PR-CERT))로부터 얻어진 (PR-CERT)와 더불어 (PU-DRM(DES1)) 및 (DES1(rightsdata))를 포함하는 제출된 권한 레이블에 서명하여 (PU-ENTITY(PR-CERT))를 생기게 한다. 알 수 있는 바와 같이, 사용자는 이러한 DRM 인증서(810)로부터 (PU-ENTITY(PR-CERT))를 얻고 거기에 (PR-ENTITY)를 적용함으로써 DRM 인증서(810)로부터 (PR-CERT)를 얻는다. 그러나, 특히 사용자가 (PU-DRM(DES1))에 적용하기 위한 (PR-DRM)을 갖지 않기 때문에, 사용자는 DRM 서버(320)가 제출된 권한 레이블 내의 권한들을 실행할 수 있음을 검증할 수 없다는 것을 알기 바란다. 따라서, DRM 서버(320) 자체는 자체-출판된 SRL(308)에 기초하여 라이센스가 요청될 때 검증을 실행해야 한다.

[0132] 일단 사용자가 SRL(308)을 자체-출판하면, 사용자는 자체-출판된 SRL(308) 및 이것을 생성하기 위해 사용된 DRM 인증서(810)를 콘텐트에 연결시키고, SRL(308) 및 DRM 인증서(810)를 갖는 이러한 콘텐트는 다른 사용자에게 배포된다. 그 다음, 다른 사용자는 도 6a 및 6b에 도시된 것과 실질적으로 동일한 방식으로 DRM 서버(320)로부터 그 콘텐트의 라이센스를 요청하여 얻는다. 그러나, 여기에서, 라이센스-요청 사용자는 콘텐트에 연결되는 것과 같이 자체-출판된 SRL(308) 및 DRM 인증서(810) 둘 다를 DRM 서버(320)에 제출한다. 그 다음, DRM 서버(320)는 대응하는 (PU-DRM)에 기초하여 DRM 인증서(810) 내의 S(PR-DRM)을 검증하고, DRM 인증서(810)로부터 (PU-CERT)를 얻는다. 그 다음, DRM 서버(320)는 얻어진 (PU-CERT)에 기초하여 SRL(308) 내의 S(PR-CERT)를 검증하고, 이전과 같은 것을 계속한다. 그러나, DRM 서버(320)가 SRL(308) 내의 권한을 시행할 수 있음을 사용자가 검증할 수 없기 때문에, 상술된 바와 같이, DRM 서버(320) 스스로 이때 검증을 실행해야 한다는 것을 주목해야 한다.

[0133] **권한 템플릿**

[0134] 상술된 바와 같이, 사용자는 사용자 또는 사용자의 클래스를 정하고, 각각의 정해진 사용자 또는 사용자 클래스에 대한 권한을 정한 다음에, 임의의 사용 조건을 정함으로써 권한 레이블 내의 권한 데이타의 대부분의 임의의 종류를 생성할 자유가 주어진다. 그러나, 특히 동일한 사용자 또는 사용자 클래스, 권한 및 조건이 콘텐트의 상이한 부분에 대해서 반복적으로 정해질 때, 다수의 권한 레이블에 대해 권한 데이타를 반복적으로 정하는 것은 상당히 부담이 되고 반복적인 것이 될 수 있다. 이러한 상황은 예를 들어 회사나 사무실 환경에서 발생할 수 있으며, 사용자는 특별히 정해진 사용자 팀과 공유될 콘텐트의 상이한 부분들을 반복적으로 출판한다. 이러한 상황에서, 본 발명의 일 실시예에서는, 사용자가 권한 레이블 생성과 관련하여 반복적으로 사용할 수 있는 권한 템플릿이 생성되는데, 이 권한 템플릿은 이미 그 안에 소정의 사용자 또는 사용자 클래스, 각각의 정해진 사용자 또는 사용자 클래스에 대한 선정된 권한, 및 소정의 사용 조건을 포함한다.

[0135] 본 발명의 일 실시예에서, 이제 도 9을 참조하면, 권한 템플릿(900)은 권한 레이블에서와 실질적으로 동일한 권한 데이타를 갖는다. 그러나, 콘텐트가 출판될 때까지 (DES1)이 알려지지 않기 때문에, 권한 데이타는 권한 레이블에서처럼 이 (DES1)에 따라 암호화될 수 없다. 본 발명의 일 실시예에서, 그러면 암호화되지 않은 권한 데이타를 갖는 권한 템플릿(900)은 도 4의 단계 416에서 권한 데이타를 (DES1)로 암호화하는 과정에서 제출되어 (DES1(rightsdata))를 생성한다. 물론, 권한 데이타는 그렇게 암호화되기 이전에 제출된 권한 템플릿(900)으로부터 검색된다.

[0136] 권한 템플릿이 구성될 때 DRM 서버(320) 및 그것의 공개 키(PU-DRM)가 알려지는 경우가 되거나 되지 않을 수 있다. 더욱이, 알려졌더라도, 각각 자신의 (PU-DRM)을 갖고 있는 2개 이상의 DRM 서버(320)가 있는 경우가 되거나 되지 않을 수 있다. 그럼에도 불구하고, 권한 템플릿이 구성될 때 DRM 서버(320) 및 그것의 공개 키(PU-DRM)이 알려지는 경우, 및 하나의 DRM 서버(320)만이 사용되거나, 또는 하나의 DRM 서버(320)만이 권한 템플릿

(900)과 관련하여 사용될 것인 경우에, 이러한 권한 템플릿은 또한 그의 공개 키(PU-DRM)을 포함하는 권한 템플릿(900)으로 인해 권한 레이블에 서명하기 위한 DRM 서버 상의 정보를 포함할 수 있다. 이러한 (PU-DRM)은 (DES1)을 암호화하여 (PU-DRM(DES1))을 생기게 할 때 SRL(308) 내에 나타나지만, 콘텐트가 출판될 때까지 (DES1)이 알려지지 않으므로, 권한 템플릿(900) 내의 (PU-DRM)이 권한 레이블에서처럼 이러한 (DES1)을 암호화할 수 없다는 것을 다시 알 수 있을 것이다. 그 다음, 본 발명의 일 실시예에서, 암호화되지 않은 (PU-DRM)을 갖는 권한 템플릿(900)은 도 4의 단계 414에서 (PU-DRM)으로 (DES1)을 암호화하는 도중에 제출되어 (PU-DRM(DES1))을 생성한다. 물론, (PU-DRM)은 사용되기 이전에 제출된 권한 템플릿(900)으로부터 검색된다.

[0137] 또한, 상술된 경우에, 권한 템플릿 내에 포함될 수 있는 DRM 서버 상의 다른 정보는 네트워크 상의 DRM 서버를 위치시키기 위한 URL과 같은 참조 정보, 및 URL 고장 시의 대처 정보를 포함할 수 있다. 어떤 경우에, 권한 템플릿은 또한 무엇보다도 권한 템플릿(900) 자체를 설명하는 정보를 포함할 수 있다. 권한 템플릿(900)은 또한, 권한 템플릿의 설명이 실제로 권한 레이블로 변환되지 않는다면 필요하지 않겠지만, 콘텐트 및/또는 암호화 키(CK) 및 (DES1)에 관련된 권한 레이블 내에 나타나는 정보와 같은, 출판될 콘텐트에 관련된 정보를 위한 공간을 제공할 수 있다.

[0138] 이제까지 개시된 권한 템플릿(900)은 주로 사용자의 편의를 위한 것이지만, 어떤 경우에, 사용자는 권한 레이블 내의 권한 데이타를 규정하는 무제한적인 자유를 가질 수 없으며, 권한 템플릿(900)은 생성될 수 있는 권한 레이블의 범위 또는 형태를 제한하도록 사용될 수 있다는 것을 또한 알 수 있을 것이다. 예를 들어, 특히 회사 또는 사무실 환경에서, 특정 사용자가 항상 특정 사용자 클래스에게만 콘텐트를 출판해야 하거나, 사용자가 특정 사용자 클래스에게 콘텐트를 전혀 출판할 수 없다는 것이 정책으로서 선정될 수 있다. 어떤 경우에, 본 발명의 일 실시예에서, 이러한 정책은 하나 이상의 권한 템플릿(900) 내에 선정된 권한 데이타로서 구현되고, 사용자는 콘텐트 출판 시에 권한 레이블을 생성하기 위해 이러한 권한 템플릿을 사용하는 것이 제한될 수 있다. 특히, 사용자를 위한 출판 정책을 지정하기 위해 사용자에게 이용가능하게 된 하나의 권한 템플릿(900) 또는 한 그룹의 권한 템플릿(900)은 본 발명의 정신 및 범위를 벗어나지 않고 임의의 특정 형태의 출판 정책을 지정할 수 있다.

[0139] 제한된 사용자 등을 위한 권한 템플릿(900)을 지정하기 위해, 이제 도 10을 참조하면, 관리자 등은 실제로 선정된 권한 데이타를 규정하고(단계 1001), 특정 DRM 서버(320)에 관련된 정보와 같은, 필요하고 적절한 임의의 다른 데이타를 규정함으로써(단계 1003) 권한 템플릿(900)을 구성한다. 중요하게, 제한된 사용자 등에 의해 사용자용 권한 템플릿을 실행하게 하기 위해, 권한 템플릿(900)은 공식적이 되어야 한다. 즉, 권한 템플릿(900)은 제한된 사용자 등이 사용할 수 있는 권한 템플릿으로 인식될 수 있게 되어야 한다. 따라서, 본 발명의 일 실시예에서, 관리자 등에 의해 구성된 권한 템플릿은 서명을 위한 DRM 서버(320)에 제출되는데, 이러한 서명은 권한 템플릿을 공식적으로 만든다(단계 1005).

[0140] 실제로 권한 템플릿(900) 내에 정보가 존재한다면, 서명 DRM 서버(320)는 정보가 권한 템플릿 내에 있는 DRM 서버(320)라는 것을 알아야 한다. 또한, DRM 서버(320)는 임의의 필요한 체크를 행할 때만 권한 템플릿(900)에 서명하거나, 또는 전혀 체크하지 않고 서명할 수 있다는 것을 알기 바란다. 마지막으로, DRM 서버(320)로부터의 템플릿 서명 S(PR-DRM-T)(여기서, -T는 서명이 ORT(900)에 대한 것임을 나타냄)는 적어도 권한 템플릿(900) 내의 선정된 권한 데이타에 기초하여야 되지만, 본 발명의 정신과 범위를 벗어나지 않는 한 다른 정보에 기초하게 될 수도 있다는 것을 알기 바란다. 후술되는 바와 같이, 서명 S(PR-DRM-T)는 권한 레이블 내에 포함될 수 있고, 이와 관련하여 검증될 수 있으므로, 서명이 기초로 하는 것은 무엇이든 변경된 형태의 권한 테이블 내로 포함될 수 있어야 한다.

[0141] DRM 서버(320)가 권한 템플릿(900)에 서명하여 이것을 관리자 등에게 돌려보내면, 관리자는 S(PR-DRM-T)로 서명되고 이제 공식적인 권한 템플릿(900)을 수신하고(단계 1007), 이 공식적인 권한 템플릿(ORT)(900)를 하나 이상의 사용자에게 보낸다(1009). 따라서, 사용자가 ORT(900)에 기초하여 콘텐트를 출판하기 위해, 사용자는 ORT(900)를 검색하고(단계 1011), 콘텐트 상의 정보, 적절한 키 정보, (DES1(rightsdata))를 생기게 하기 위해 (DES1)에 의해 암호화된 ORT(900)로부터의 권한 데이타, 및 ORT(900)로부터의 임의의 다른 정보와 같은 임의의 필요한 정보를 제공함으로써 ORT(900)에 기초하여 권한 레이블을 구성한다(단계 1013). 중요하게, 사용자는 또한 ORT(900)로부터의 서명 S(PR-DRM-T)를 권한 레이블과 함께 포함한다.

[0142] 그 다음, 이전과 같이, 사용자는 권한 레이블을 서명을 위한 DRM 서버(320)에 제출한다(단계 1015). 그러나, 여기에서, DRM 서버(320)는 내부의 S(PR-DRM-T)가 검증하지 않으면 제출된 권한 레이블에 서명하지 않을 것이다. 즉, DRM 서버(320)는 제출된 권한 레이블이 ORT(900)으로부터 서명 S(PR-DRM-T)를 포함하지 않으면 제

출된 권한 레이블에 서명하는 것을 거절함으로써 사용자가 ORT(900) 상의 제출된 권한 레이블에 기초해야 한다는 것을 실행한다. 특히, DRM 서버(320)는 이러한 S(PR-DRM-T)를 검색하고, 제출된 권한 레이블로부터 이러한 서명이 기초하고 있는 모든 정보를 검색한 다음에, (PU-DRM)에 기초하여 이러한 서명을 검증한다. 제출된 권한 레이블 내의 권한 데이타는 (DES1)(즉, (DES1(rightsdata))에 따라 암호화된다는 것을 알기 바란다. 따라서, DRM 서버(320)는 제출된 권한 레이블 내의 권한 데이타에 기초하여 서명을 검증할 수 있도록, 도 7과 관련하여 설명된 바와 같이, 먼저 (DES1)을 획득해서, 이것으로 (DES1(rightsdata))를 암호해독한다.

[0143] 검증되면, DRM 서버(320)는 제출된 권한 레이블에 S(PR-DRM-L)로 서명하여, 이전과 같이 SRL(308)을 생성한다(여기서, -L은 서명이 SRL(308)에 대한 것임을 나타낸다). 여기에서, S(PR-DRM-L)은 S(PR-DRM-T)를 대신할 수 있거나, S(PR-DRM-T)에 추가될 수 있다. 또한, S(PR-DRM-L)은 부분적으로 S(PR-DRM-T)에 기초할 수 있다. (PR-DRM)은 S(PR-SRM-T) 및 S(PR-DRM-L)을 생성하기 위해 사용되거나, 또는 상이한 (PR-DRM)이 S(PR-DRM-T) 및 S(PR-DRM-L)의 각각에 사용될 수 있다는 것을 알기 바란다. DRM 서버(320)가 권한 레이블에 서명하여 SRL(308)을 사용자에게 돌려보내면, 사용자는 S(PR-DRM-L)을 갖는 SRL(308)을 수신하고(단계 1017), 이전과 같이 이것을 출판되는 콘텐트에 연결시키는 것을 진행한다.

[0144] ORT(900)의 서명 S(PR-DRM-T)가 적어도 부분적으로 ORT(900) 내의 선정된 권한 데이타에 기초하면, SRL(308) 내에(DES1(rightsdata) 내에) 나타내는 권한 데이타는 수정되거나 변경될 수 없다. 그렇지 않으면, S(PR-DRM-T)는 검증되지 않을 것이다. 그럼에도 불구하고, 본 발명의 일 실시예에서, ORT(900) 내의 권한 데이타는 또한 ORT(900) 내에 포함되는 선정된 규칙 내에서 변화할 수 있다. 예를 들어, SRL(308) 내에 포함될 2세트의 권한 데이타 중 하나를 지정하거나, 대안적인 세트 중에서 선택을 할 수 있게 하는 규칙들이 있을 수 있다. 알 수 있는 바와 같이, 이 규칙들은 본 발명의 사상 및 범위 내에서 임의의 적절한 문맥으로 설명된 임의의 특정 규칙이 될 수 있다. 여기서, 이 규칙들은 권한 레이블이 생성될 때 사용자를 위한 적절한 규칙 해석기에 의해 해석될 수 있다. 권한 데이타가 변할 수 있긴 하지만, 규칙들은 같이 변하지 않으므로, ORT(900)에 대한 템플릿 서명 S(PR-DRM-T)는 적어도 부분적으로 규칙에 기초하고, 권한 데이타 자체에 기초하지 않는다. 그 결과, ORT(900)와 함께 포함된 규칙은 또한 SRL(308)과 함께 포함되어야 한다.

[0145] 본 발명의 일 실시예에서, 상술된 바와 같이, ORT(900) 내의 선정된 권한 데이타는 부분적으로는 고정되어 변화되지 않고, 부분적으로는 변화되어 규칙이 유도된다. 여기에서, ORT(900)의 템플릿 서명 S(PR-DRM-T)는 적어도 부분적으로 고정된 부분의 규칙, 및 변하는 부분의 권한 데이타의 규칙에 기초한다.

[0146] 알 수 있는 바와 같이, 사용자가 소유한 ORT(900)는 오래되었거나 실효된 것일 수 있다. 즉, 내부의 권한 데이타를 통한 ORT(900)는 오래되었거나, 부적절하거나, 또는 더이상 단순히 적용될 수 없는 정책을 반영할 수 있다. 예를 들어, ORT(900)의 권한 데이타 내에 지정된 하나 이상의 사용자 또는 사용자 클래스는 정책 환경내에 더 이상 존재할 수 없거나, 또는 ORT(900)의 권한 데이타 내에 지정된 특정 사용자 또는 사용자 클래스는 정책 환경 내에서 더 이상 동일한 권한을 가질 수 없다. 이러한 경우에, 관리자는 개정된 ORT(900)를 발행할 수 있지만, 사용자는 여전히 이전의 실효된 버전의 ORT(900)를 사용하고 있을 수 있다.

[0147] 그 다음, 이러한 상황에서, 본 발명의 일 실시예에서, ORT(900)를 생성하기 위해 제출된 권한 템플릿(900)에 서명하고 있는 DRM 서버(320)는 ORT(900)의 카피를 보유하고, 각 ORT(900)는 유일한 식별 표시를 가지며, ORT(900)에 기초하여 구성된 각 권한 레이블은 내부에 ORT(900)의 식별 표시를 포함한다. 따라서, 도 10과 관련한 것과 같이 제출된 권한 레이블을 수신 시에, DRM 서버(320)는 권한 레이블 내에서 ORT(900)의 식별 표시를 발견하고, 발견된 식별 표시에 기초하여 ORT(900)의 가장 최신의 카피를 검색하며, 제출된 권한 레이블로부터의 권한 데이타를 제거하고, 검색된 ORT(900)로부터 권한 데이타를 삽입한 다음, 적어도 부분적으로 삽입된 권한 데이타에 기초하여 권한 레이블에 서명한다. 물론, DRM 서버는 또한, (DES1(rightsdata))의 암호해독 및 재암호화를 포함하여, 상술된 프로세스에 필요하고 프로세스에 의무적인 임의의 필요한 암호화 및 복호화를 실행한다. DRM 서버가 제출된 권한 레이블 내의 권한 데이타를 교체하도록 적용되면, 이러한 권한 레이블, 및 이러한 권한 레이블이 구성되는 ORT(900)는 내부에 권한 데이타를 반드시 포함할 필요는 없다. 그 대신, 권한 데이타가 DRM 서버(320)에 상주할 필요만은 없다. 그러나, 권한 레이블 및 이러한 권한 레이블이 구성되는 ORT(900)와 함께 권한 데이타를 포함하는 것은 사용자에게 유용할 수 있으므로, 어떤 경우에는 유용하게 이용될 수 있다.

[0148] **디렉토리를 통한 라이센싱**

[0149] 보호된 콘텐트의 라이센스를 발행할 때, 라이센스 발행 엔티티(이하, '라이센서')는 콘텐트로부터 보내진 SRL(308)을 참고하여, 어떤 사용자/그룹/클러스터/구획/플랫폼/등등(이하, '엔티티')에게 권한, 및 라이센스 요

청자를 식별하기 위해 보내진 인증서가 제공될 것인지를 판정한다. 이것에 기초하여, 라이센서는 SRL(308) 내에 리스트된 것들의 어떤 권한이 요청자에게 발행될 것인지 판정한다. 개념상, 라이센서는 SRL(308) 내에 리스트된 엔티티들을 조사하고, 이러한 엔티티들을 요청자와 비교한다. 그러므로, 특정 그룹이 라이센스를 수신하고, 요청자가 이러한 그룹의 구성원이라는 것을 SRL(308)이 열거하면, 요청자에게는 SRL(308) 내의 그룹을 위해 설명된 권한을 갖는 라이센스가 부여된다. 이와 마찬가지로, 특정 사용자가 라이센스를 수신하고, 요청자가 이러한 사용자라는 것을 SRL(308)이 열거하면, 요청자에게는 SRL(308) 내의 사용자를 위해 설명된 권한을 갖는 라이센스가 부여된다. 알 수 있는 바와 같이, 특정 SRL(308)은 몇가지 엔티티 및 그에 대한 권한을 리스트할 수 있고, 특정 요청자에게는 존재하는 하나 이상의 엔티티의 구성원에 기초하여 라이센스가 부여될 수 있다.

[0150] 본 발명의 일 실시예에서, 도 12에서 알 수 있는 바와 같이, 요청자는 식별자(1204)를 통해 보내진 인증서(1202) 내에서 식별되는데, 식별자(1204)는 예를 들어 요청자가 조직 디렉토리(1206) 내에서 식별되는 대체명일 수 있다. 이에 대응하여, SRL(308)은 이러한 식별자(1204)에 따라 각각의 권한부여 엔티티를 리스트한다. 그러므로, 라이센스(1208)에 대한 요청 처리의 일부분으로서, 라이센서(1210)는 인증서(1202)로부터 요청자의 식별자(1204)를 얻어서, 얻어진 식별자를 보내진 SRL(308) 내에 리스트된 모든 식별자(1204)와 비교한다. 부합되는 것이 발견되면, 라이센서(1210)는 이 요청자의 식별자(1204)용 SRL(308) 내에 지정된 권한을 갖는 요청자에게 라이센스(1208)를 발행한다.

[0151] 또한, 디렉토리의 이용도로, 라이센서(1210)는 또한 요청자가 SRL(308) 내에 리스트된 임의의 다른 엔티티의 구성원인지 판단하여, 디렉토리(1206)가 각각의 다른 엔티티 내의 요청자의 구성원 상태를 반영할 수 있는 적절한 상호참조 정보를 포함한다고 추정한다. 전형적으로, 디렉토리(1206)는 각 요청자에 대해, 그의 식별자(1204)뿐만 아니라, 요청자가 그 구성원인 각 그룹/클러스터/구획/플랫폼/다른 엔티티/등등의 식별자(1208)를 리스트한다. 디렉토리(1206)는 메일 주소, 교체 메일 주소, ID, 교체 ID, 그룹 구성원, 이력 식별자 등과 같은 식별자(1208)를 포함할 수 있다는 것에 주목한다.

[0152] 인증서(1202)가 식별자(1204)를 갖는 요청자로부터 수신되고, SRL(308)로부터의 권한 데이타가 요청자로부터 수신되면, 이제 도 13을 참조하여, 라이센서(1210)는 다음과 같은 방식으로 라이센스(1208)를 요청자에게 발행한다. 임시로, 라이센서(1210)는 수신된 인증서(1202)로부터 요청자의 식별자(1204)를 얻고(단계 1301), 얻어진 식별자(1204)를 디렉토리(1206) 내에 위치시킨다(단계 1303). 그 다음에, 라이센서(1210)는 요청자 식별자(1204)가 구성원인 각 엔티티의 식별자(1204)를 디렉토리(1206) 내에 위치된 식별자(1204)에 기초하여 위치시킨다(단계 1305). 그러므로, 각각의 위치된 요청자 식별자(1204) 및 모든 위치된 엔티티 식별자(1204)에 대해, 라이센서(1210)는 이러한 식별자(1204)를 보내진 SRL(308) 내에 리스트된 모든 식별자(1204)와 비교한다(단계 1307). 다시 부합되는 것이 발견되면, 라이센서(1210)는 부합 식별자(1204)용 SRL(308) 내에 지정된 권한을 갖는 요청자에게 라이센스(1208)를 발행한다.

[0153] 다수의 식별자(1204)가 SRL(308)과 비교되기 때문에, 다수의 부합 식별자(1204)가 SRL(308) 내에서 발견되는 경우가 있을 수 있다는 것을 알기 바란다. 그렇다면, 라이센스(1210)는 SRL(308) 내의 부합 식별자(1204) 중 적절한 것을 선택하여, 선택된 부합 식별자(1204)용 SRL(308) 내에 지정된 권한을 갖는 요청자에게 라이센스(1208)를 발행할 수 있다. 예를 들어, 라이센서는 가장 많은 권한을 요청자에게 전달하는 부합 식별자(1204)를 선택할 수 있다(단계 1309b-1). 부합 식별자(1204)가 가장 많은 권한을 전하거나, SRL(308) 내의 동일한 종류의 우선순위 표시(1212)에 의존해야 되는 지를 라이센서가 판정할 수 있다는 것을 알기 바란다. 후자의 경우, SRL(308) 내의 각 부합 식별자(사용자)(1204)는 대응하는 우선순위 표시(1212)를 가지며, 더 높은 순위의 표시(1212)는 예를 들어 더 넓은 범위의 부여된 권한을 나타낸다. 그러므로, 라이센서(1210)가 SRL(308) 내에서 다수의 부합 식별자(1204)를 발견하면, 이러한 라이센서(1210)는 최고 순위의 표시(1212)를 갖는 부합 식별자(1204)를 선택한다(단계 1309b-2).

[0154] 요청자에 관련된 추가적인 식별자(1204)를 생성하기 위해 디렉토리(1206)를 참조하면, 라이센서(1210)는, 예를 들어 SRL(308)이 생성된 이후 요청자의 메일 주소 또는 ID가 변경된 상황에서 부합이 발견될 수 있는 가능성을 증가시킨다는 것을 알기 바란다. 일반적으로, 디렉토리(1206)는 요청자의 한 식별자(1204)로부터 요청자의 다른 가능한 식별자(1204)로의 맵핑을 제공함으로써, 모든 식별자(1204)는 SRL(308) 내의 식별자(1204)에 대한 부합을 발견하고자 시도할 때 사용될 수 있다.

[0155] **그룹으로의 라이센싱**

[0156] 본 발명의 일 실시예에서, 요청자에 의해 제출된 보내진 인증서(1202)는 그룹, 클러스터, 또는 그룹이 디렉토리(1206) 내에서 적절하게 표현되는 임의의 다른 개인 집단(이후, '그룹')을 나타낼 수 있다. 이러한 그룹은 배

포 리스트 또는 메일 대체명과 같은 메일-가능 그룹, 또는 네트워크 운영 시스템과 접속하여 규정될 수 있는 보안 그룹 등을 포함할 수 있다. 따라서, 보내진 '그룹' 인증서(1202)를 수신 중인 라이센서(1210)는 실질적으로 이전과 같이 진행한다. 그러나, 보내진 인증서(1202)가 특정 그룹을 나타내기 때문에, 라이센서(1210)로부터 발행된 라이센스(1208)가 인증서(1202) 내에 식별된 그룹을 위한 것이지, 구체적으로 요청자를 위한 것이 아니라는 것을 알기 바란다. 대안적으로, 라이센서(1210)는 디렉토리(1206)로부터 요청자가 인증서91202) 내에 식별된 그룹의 일부라는 것을 판정할 수 있으며, 그렇다면 발행된 라이센스(1210)는 요청자를 위한 것이 된다.

[0157] 전자의 경우에, 발행된 라이센스(1208)는 그룹의 공개 키에 따라 암호화된 콘텐트 키를 포함할 수 있고, 따라서 요청자는 그룹의 대응하는 개인키를 얻을 필요가 있다. 따라서, 요청자는 요청자의 공개 키에 따라 암호화되어 요청자의 대응하는 개인 키에 따라 암호해독가능한, 이러한 개인 키를 갖는 그룹 구성원 인증서를 가질 수 있다.

[0158] 후자의 경우, 발행된 라이센스(1208) 내의 요청자의 공개 키에 따라 암호화된 콘텐트 키를 포함하기 위해, 라이센서(1210)는 이러한 공개 키를 갖는 요청자로부터 인증서를 추가로 수신할 수 있다. 대안적으로, 라이센서(1210)는 파일 상에 이러한 인증서를 가질 수 있고(예를 들어, 도 6a 및 6b의 단계 608-612 참조), 요청자가 보내진 그룹 인증서(1202) 내에 식별된 그룹의 일부라는 것을 디렉토리(1206)로부터 판정할 때와 동일하게 공개 키를 사용할 수 있다.

[0159] 특히, SRL(308) 내에 권한을 지정하고 그룹에 따라 라이센스(1208)를 발행하는 것은 기업 또는 조직 세팅 시에 디지탈 권한 관리를 실행하게 한다. 예를 들어, 문서 또는 이메일이 DRM-보호되어, 주어진 부서의 모든 구성원이 문서 또는 이메일을 판독할 권리를 가질 수 있다. 이러한 부서에 대한 그룹(예를 들어, 이메일 대체명)이 가장 흔한 경우인 조직의 디렉토리(1206) 내에 존재한다고 하면, 문서 또는 이메일의 작성자는 개인보다는 그룹 단위로 권한을 부여할 수 있다. 알 수 있는 바와 같이, 이러한 그룹식 권한 부여의 장점은 권한을 갖는 개인의 클래스를 작성자가 지정할 때의 사용의 용이성을 포함한다. 또한, 그룹에 따라 권한을 지정함으로써, 지정된 권한은 그룹에 가입하는 새로운 개인 및 그룹을 떠나는 기존의 개인으로서 '실효'되지 않는다. 그 대신에, 그룹의 모든 현재 구성원은 이러한 그룹의 구성원이 조직 디렉토리(1206) 내에 최신으로 유지되는 한 권한을 발휘할 수 있다.

[0160] **라이센싱 중의 정책 도입**

[0161] 본 발명의 일 실시예에서, 도 9의 ORT(900)와 관련하여 상술된 바와 같이, DRM 서버/라이센서(1210)는 SRL(308)에 기초하여 라이센스(1208)를 발행할 때 제출된 SRL(308)로부터의 권한 데이타를 변경하거나 대체하도록 될 수 있다. 특히, 제출된 SRL(308) 내의 권한 데이타가 명백하게 무시되고, 라이센서(1210)가 그 대신에 SRL(308)에 기초하여 라이센스(1218) 생성시에 택일적인 정책을 대체하거나 또는 '도입'하는 경우에 몇가지 상황이 발생한다. 라이센서(1210)가 라이센스(1208) 내로 정책을 도입하는 몇가지 특정 상황이 여기에서 개시되지만, 라이센서(1210)는 본 발명의 정신 및 범위를 벗어나지 않는 한도에서 임의의 다른 형태의 상황에서 라이센스(1208) 내로 정책을 도입할 수 있다.

[0162] 첫번째 경우에, 이제 도 14를 참조하면, 라이센서(1208)는 특별 권한이 부여된 특별 엔티티(사용자, 그룹 등)의 리스트(1214(도 12))를 관리한다. 예를 들어, 특별 엔티티는 그 중에서도 특히, 조직 내의 임의의 더 높은 레벨의 개인, 어떤 관리인, 모든 콘텐트를 렌더할 수 있는 어떤 개인, 및 상술된 개인의 그룹을 포함할 수 있다. 이러한 리스트(1214)는 실제로 각각의 특별 엔티티에 대해 리스트하는 디렉토리 내의 정보를 식별하거나, 또는 이러한 특별 엔티티의 하나 이상의 그룹을 단순히 작성하여, 조직 디렉토리(1206) 내에 포함될 수 있다. 따라서, 이러한 특별 엔티티는 그것의 SRL(308)이 달리 이러한 렌더링을 금지하더라도 콘텐트를 렌더할 수 있다.

[0163] 라이센스(1208)에 대한 요청의 일부로서 엔티티가 SRL(308)을 제출하면, 이제 도 14를 참조하면, 라이센서(1210)는 적절한 방식으로 디렉토리(1206)와 체크하여 제출 엔티티가 특별 엔티티로서 특징지워질 수 있는 지를 판정하고(단계 1401), 그렇다면 라이센서(1210)는 제출된 SRL(308) 내에 존재하는 권한 데이타와 다른 특별 권한을 갖는 특별 엔티티를 위한 라이센스(1208)를 생성한다(단계 1403). 특별 권한은 본 발명의 정신 및 범위를 벗어나지 않는 임의의 권리일 수 있다는 것을 알기 바란다. 예를 들어, 특별 권한은 모든 특별 엔티티가 대응하는 콘텐트를 완전히 액세스하여 렌더할 수 있는 것, 특정 그룹으로부터의 모든 특별 엔티티가 콘텐트를 완전히 액세스하여 렌더할 수 있는 것, 라이센스(1208)가 만기되기 이전의 더욱 높은 플레이 카운트 또는 더욱 긴 기간과 같은 향상된 권리를 특정된 특별 엔티티가 수신한다는 것 등등일 수 있다. 특별 권한이 개인 또는 그룹에 대해 특정된 경우, 이러한 권리는 디렉토리(1206) 내의 개인 또는 그룹을 위한 디렉토리 엔트리 내에 지정될 수 있고, 이러한 디렉토리 엔트리는 특별 권한이 위치하게 되는 위치에 대한 적절한 레퍼런스를 가질 수

있으며, 라이센서(1210)는 개인 또는 그룹의 식별자(1204)에 기초하여 데이타베이스 내에서 특별 권한을 발견할 수 있다는 것을 알기 바란다.

[0164] 두번째 경우에, 이제 도 15를 참조하면, 라이센서(1208)는 권한이 제한되거나 취소될 제한된 엔티티(사용자, 그룹 등)의 리스트(1216)(도 12)를 유지한다. 예를 들어, 제한된 엔티티는 그중에서도 특히, 조직을 떠난 개인, 유지보수 및 빌딩 직원과 같이 임의의 콘텐트에 대한 임의의 권한을 통상적으로 갖지 않는 조직 내의 개인, 계약자 및 임시 종업원과 같이 조직 내에서 제한된 상태만을 갖는 개인, 및 상술된 개인의 그룹을 포함할 수 있다. 상술된 '특별' 리스트(1214)와 같이, 제한된 리스트(1216)는 또한 각각의 제한된 엔티티에 대해 리스트하는 디렉토리 내의 정보를 식별하거나, 또는 이러한 제한된 엔티티의 하나 이상의 그룹을 단순히 작성함으로써, 조직 디렉토리(1216) 내에 포함될 수 있다. 그러므로, 이러한 제한된 엔티티는 그 SRL(308)이 이러한 렌더링을 다르게 허용하더라도 콘텐트 렌더링으로부터 제한된다.

[0165] 엔티티가 라이센스(1208)에 대한 요청의 일부로서 SRL(308)을 제출하면, 이제 도 14를 참조하면, 라이센서(1210)는 적절한 방식으로 디렉토리(1206)와 체크하여 제출 엔티티가 특별 엔티티로서 특징지워질 수 있는 지를 판정하고(단계 1405), 그렇다면 라이센서(1210)는 제출된 SRL(308) 내에 존재하는 권한 데이타와 다른 제한된 권한을 갖는 제한된 엔티티를 위한 라이센스(1208)를 생성한다(단계 1407). 제한된 권한은 본 발명의 정신 및 범위를 벗어나지 않는 임의의 권리일 수 있다는 것을 알기 바란다. 예를 들어, 제한된 권한은 모든 제한된 엔티티가 대응하는 콘텐트를 임의의 방식으로 액세스 및 렌더할 수 없는 것, 특정 그룹으로부터의 모든 제한된 엔티티가 단명 형태만의 콘텐트를 액세스하여 렌더할 수 있는 것, 특정 제한된 엔티티가 일부분의 콘텐트의 하나의 카피만을 프린트할 수 있는 것 등등일 수 있다. 또한 제한된 권한은 제한된 엔티티가 어떤 라이센스도 전혀 부여받지 못한 다는 것일 수 있다. 특별 권한과 같이, 제한된 권한이 개인 또는 그룹에 특정된 경우, 이러한 권리는 디렉토리(1206) 내의 개인 또는 그룹을 위한 디렉토리 엔트리 내에 지정될 수 있고, 이러한 디렉토리 엔트리는 특별 권한이 위치하게 되는 위치에 대한 적절한 레퍼런스를 가질 수 있으며, 라이센서(1210)는 개인 또는 그룹의 식별자(1204)에 기초하여 데이타베이스 내에서 특별 권한을 발견할 수 있다.

[0166] 세번째 경우에, 라이센서(1208)는 대응하는 콘텐트를 렌더하기 위한 컴퓨팅 장치(14)(도 11) 상에 필요한 적어도의 시스템 요구사항을 지정하기 위해 라이센스(1208) 내로 정책을 도입할 수 있다(단계 1409). 이러한 적어도의 정책 요구사항은 본 발명의 정신 및 범위를 벗어나지 않는 임의의 다른 사항에 관련될 수도 있지만, 전형적으로 컴퓨팅 장치(14)의 신뢰성 및 보안에 관련된다.

[0167] 라이센서(1210)에 관련될 수 있는 신뢰성 및 보안의 주요한 예는 컴퓨팅 장치(14)의 신뢰된 구성요소(18) 또는 그것의 보안부가 통용되고 있는지의 여부이다. 알 수 있는 바와 같이, 이러한 통용성은 버전 번호, 제조일 등에 의해 표시될 수 있고, 신뢰된 구성요소(18) 또는 그 일부의 연대를 반영한다. 또한 알 수 있는 바와 같이, 신뢰된 구성요소(18) 또는 그 일부는 이러한 신뢰된 구성요소(18) 또는 그 일부의 연대와 같은 나쁜 엔티티에 의한 보안 공격에 더욱 취약하다. 따라서, 라이센서(1210)는 어떤 연대를 초과하는 신뢰된 구성요소(18) 또는 그의 일부가 신뢰되지 않아야 한다고 결정하고, 대응하는 콘텐트가 렌더되기 이전에 이러한 신뢰성이 없는 구성요소(18) 또는 그 일부가 갱신될 것을 요구하는 정책을 발행된 라이센스(1208) 내로 도입할 수 있다.

[0168] 라이센서(1210)에 관련될 신뢰성 및 보안의 다른 예는 콘텐트를 렌더하기 위한 어플리케이션이 실제로 신뢰될 수 있는지의 여부이다. 알 수 있는 바와 같이, 한 어플리케이션은, 예를 들어 콘텐트가 보호되지 않은 형태로 보관될 수 없게 함으로써 라이센스(1208)의 범위 내의 콘텐트를 렌더하도록 신뢰될 수 있지만, 다른 어플리케이션은 마찬가지로 신뢰될 수 없는 경우가 있을 수 있다. 따라서, 라이센서(1210)는 임의의 어플리케이션만이 대응하는 콘텐트를 렌더하도록 사용될 수 있다고 결정하고, 이러한 어플리케이션만이 이러한 콘텐트를 렌더하기 위해 사용될 것을 요구하는 정책을 발행된 라이센스(1208) 내로 도입할 수 있다.

[0169] 물론, 다른 정책 도입 상황도 풍부하다. 일반적으로, 정책 도입은 아마도 요청자에 기초하여 SRL(308) 내의 권한 데이타에 권한을 추가하거나 또는 그 권한 데이타로부터 권한을 제거하도록 실행될 수 있고(단계 1411), 역시 요청자에 기초하여 이러한 권한 데이타로 조건을 추가하거나 또는 그 권한 데이타로부터 조건을 제거하도록 마찬가지로 실행될 수 있다(단계 1413).

발명의 효과

[0170] 결론

[0171] 본 발명과 관련하여 실행된 프로세스를 실행하는데 필요한 프로그래밍은 비교적 간단하고, 공개된 관련 프로그래밍으로 명백해질 수 있다. 따라서, 이러한 프로그래밍은 여기에 첨부하지 않는다. 그리고, 임의의 특정 프

로그래밍이 본 발명의 정신 및 범위를 벗어나지 않고서 본 발명을 실행하는데 사용될 수 있다.

[0172] 본 발명의 개념을 벗어나지 않고서 상술된 실시예에 변경이 이루어질 수 있다는 것을 알 수 있을 것이다. 특히, 본 발명은 조직과 같은 규정된 집단과 관련해서 설명되었지만, 본 발명은 또한, 본 발명의 정신 및 범위를 벗어나지 않고서 조직의 서브셋이나 다수의 조직을 망라하는 규정된 집단 내에서도 사용될 수 있다. 그러므로, 본 발명은 개시된 특정 실시예에 제한되지 않고, 첨부된 청구범위에 의해서만 제한된다는 것을 알 수 있을 것이다.

도면의 간단한 설명

[0001] 도 1은 본 발명이 실현될 수 있는 예시적인 비제한 컴퓨팅 환경을 나타내는 블록도.

[0002] 도 2는 본 발명이 실현될 수 있는 여러가지 컴퓨팅 장치를 갖고 있는 예시적인 네트워크 환경을 나타내는 블록도.

[0003] 도 3은 디지탈 콘텐트를 출판하기 위한 본 발명에 따른 시스템 및 방법의 일 실시예의 기능 블록도.

[0004] 도 4는 권한 관리된 디지탈 콘텐트를 출판하기 위한 본 발명에 따른 방법의 일 실시예의 플로우차트.

[0005] 도 4a는 도 4의 방법에 의해 생성된 것과 같은 서명된 권한 레이블의 구조를 도시한 블록도.

[0006] 도 5는 권한 관리된 디지탈 콘텐트를 라이센싱하기 위한 본 발명에 따른 시스템 및 방법의 일 실시예의 블록도.

[0007] 도 6a 및 도 6b는 권한 관리된 디지탈 내용을 라이센싱하기 위한 본 발명에 따른 방법의 일 실시예의 플로우차트.

[0008] 도 7은 본 발명의 일 실시예에 따라 권한 레이블의 재판(re-publishing)시에 실행된 중요 단계들을 도시한 플로우차트.

[0009] 도 8은 본 발명의 일 실시예에 따라 사용자가 오프라인 출판을 사용할 수 있게 하기 위해 DRM 서버에 의해 사용자에게 발행된 인증서를 도시한 블록도.

[0010] 도 9는 본 발명의 일 실시예에 따라 권한 레이블 내에 편입될 권한 템플릿(template) 지정 정보를 도시한 블록도.

[0011] 도 10은 본 발명의 일 실시예에 따라 도 9의 권한 템플릿을 생성하고, 권한 템플릿에 기초하여 도 4a의 서명된 권한 레이블을 생성할 때 수행되는 중요 단계들을 도시한 플로우차트.

[0012] 도 11은 신뢰 기반 시스템의 한 예의 시행(enforcement) 아키텍처를 도시한 블록도.

[0013] 도 12는 본 발명의 일 실시예에 따라 라이센서가 라이센스에 대한 요청을 처리하는 것을 도시한 블록도.

[0014] 도 13은 라이센스를 발행할 때 디렉토리와 관련하여 도 12의 라이센서에 의해 실행된 단계들을 도시한 흐름도.

[0015] 도 14는 발행될 라이센스 내로 정책을 도입할 때 도 12의 라이센서에 의해 실행된 단계들을 도시한 흐름도.

[0016] <도면의 주요 부분에 대한 부호의 설명>

[0017] 100 : 컴퓨팅 시스템 환경

[0018] 120 : 프로세싱 유닛

[0019] 130 : 시스템 메모리

[0020] 121 : 시스템 버스

[0021] 302 : 콘텐트 준비 어플리케이션

[0022] 304 : 암호화된 디지탈 콘텐트

[0023] 306 : DRM 클라이언트 API

[0024] 308 : 서명된 권한 레이블

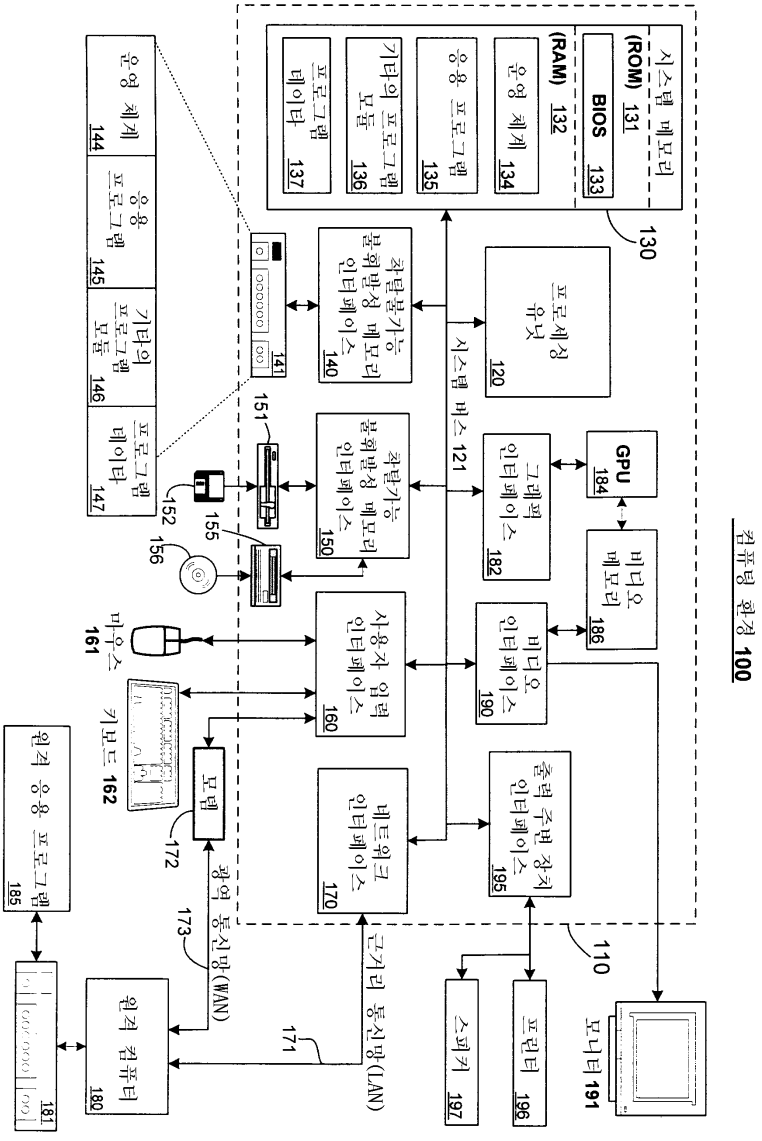
[0025] 310 : 권한 관리된 디지탈 콘텐트

[0026] 320 : DRM 서버

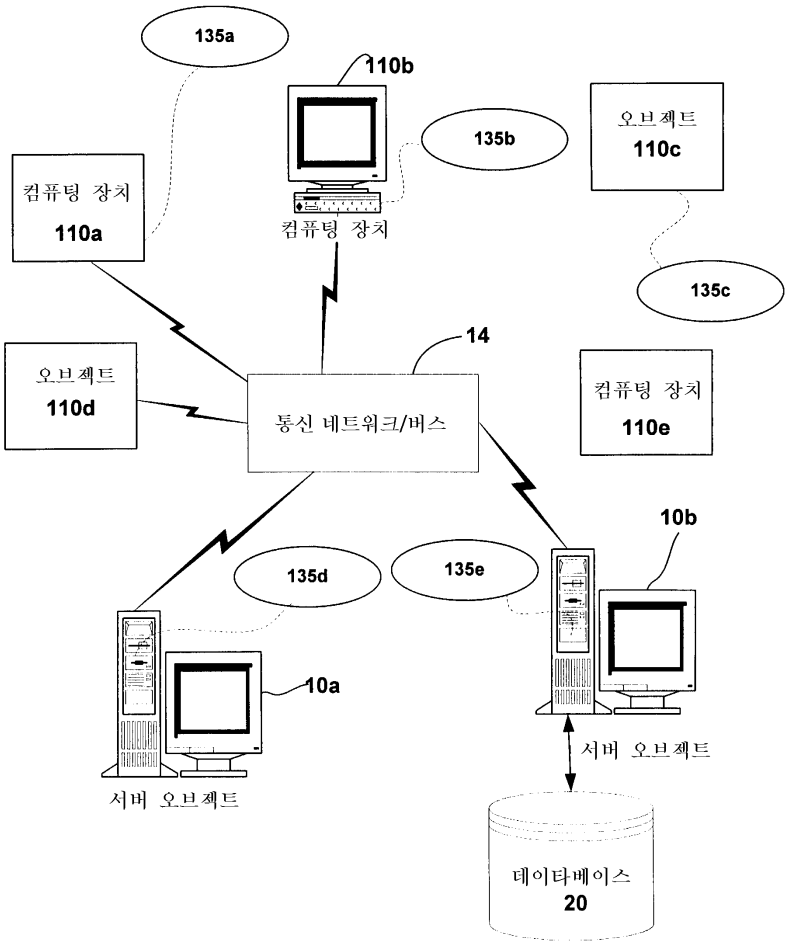
[0027] 330 : 통신 네트워크

도면

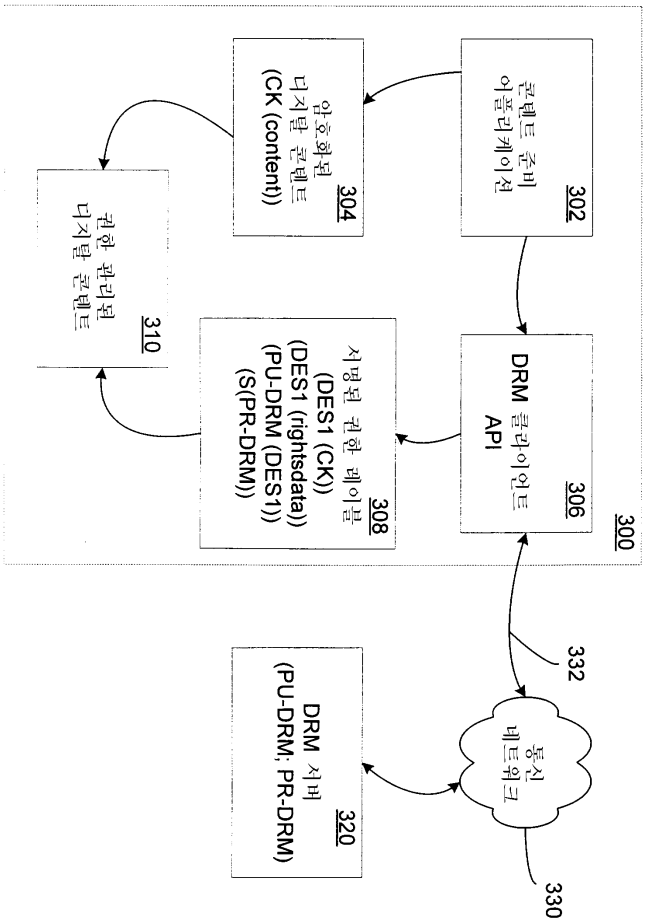
도면1



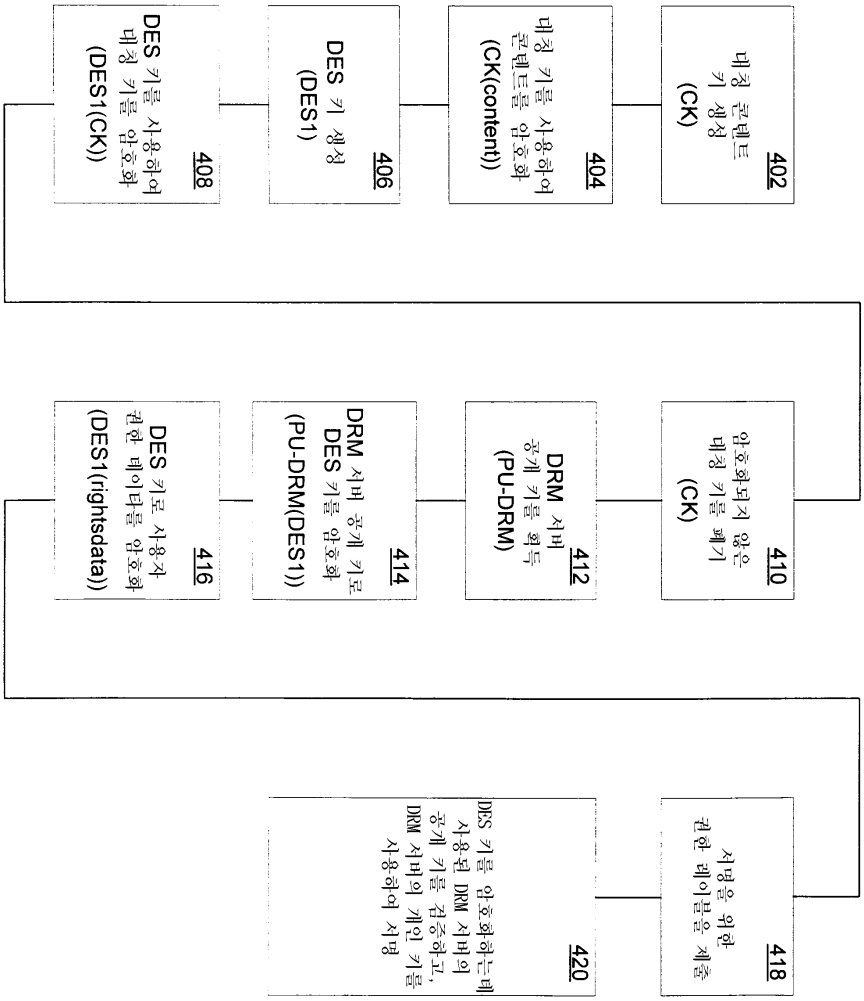
도면2


135a
110b
135b
오브젝트
110c
컴퓨팅 장치
110a
컴퓨팅 장치
135c
14
오브젝트
110d
통신 네트워크/버스
컴퓨팅 장치
110e
10b
135d
135e
10a
서버 오브젝트
서버 오브젝트
데이타베이스
20

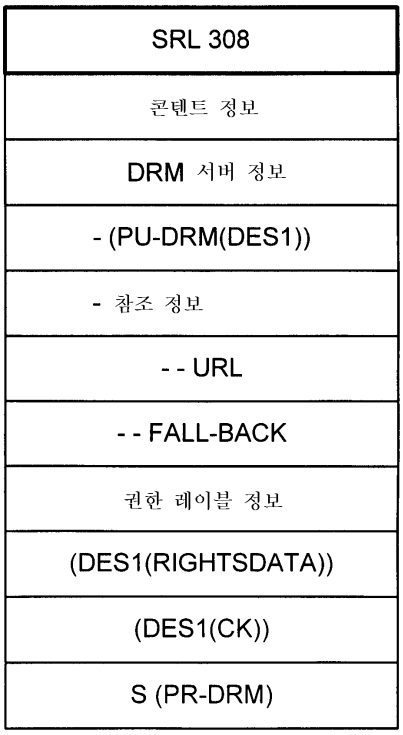
도면3


콘텐트 준비
어플리케이션
302
암호화된
디지털 콘텐트
(CK (content))
304
DRM 클라이언트
API
306
서명된 권한 데이블
(DES1 (CK))
(DES1 (rightsdata))
(PU-DRM (DES1))
(S(PR-DRM))
308
권한 관리된
디지털 콘텐트
310
300
332
통신
네트워크
330
DRM 서버
(PU-DRM; PR-DRM)
320

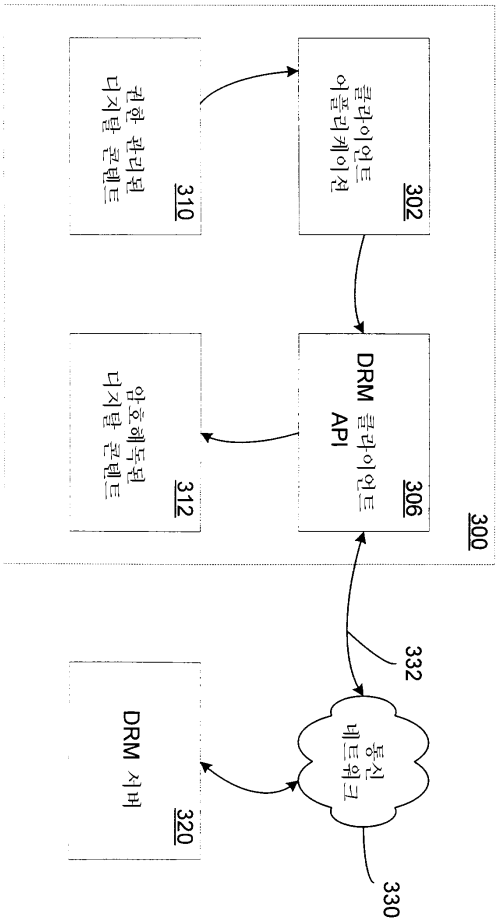
도면4


400
402
대칭 콘텐트 키 생성 (CK)
404
대칭 키를 사용하여 콘텐트를 암호화 (CK(content))
406
DES 키 생성 (DES1)
408
DES 키를 사용하여 대칭 키를 암호화 (DES1(CK))
410
암호화되지 않은 대칭 키를 폐기 (CK)
412
DRM 서버 공개 키를 획득 (PU-DRM)
414
DRM 서버 공개 키로 DES 키를 암호화 (PU-DRM(DES1))
416
DES 키로 사용자 권한 데이터를 암호화 (DES1(rightsdata))
418
서명을 위한 권한 데이블을 제출
420
DES 키를 암호화하는데 사용된 DRM 서버의 공개 키를 검증하고, DRM 서버의 개인 키를 사용하여 서명

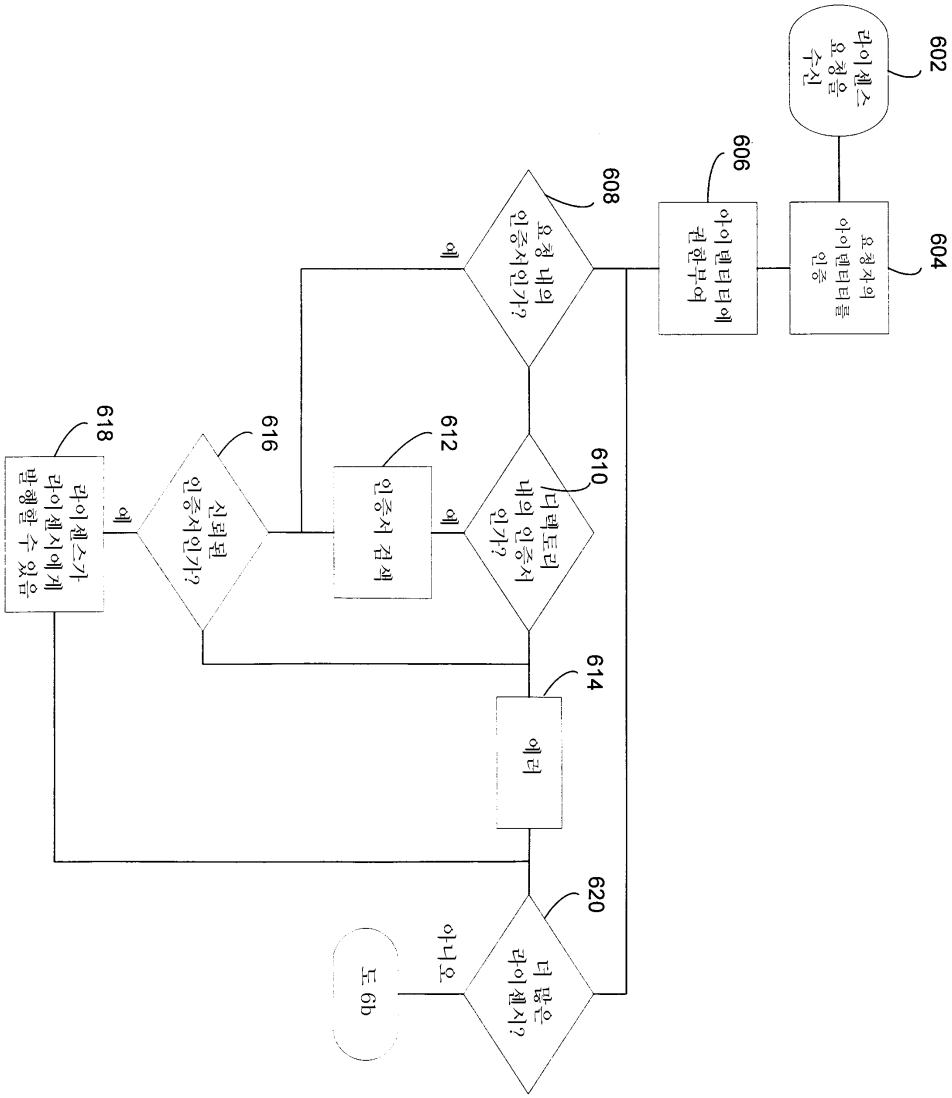
도면4a


SRL 308
콘텐트 정보
DRM 서버 정보
- (PU-DRM(DES1))
- 참조 정보
- - URL
- - FALL-BACK
권한 레이블 정보
(DES1(RIGHTSDATA))
(DES1(CK))
S (PR-DRM)

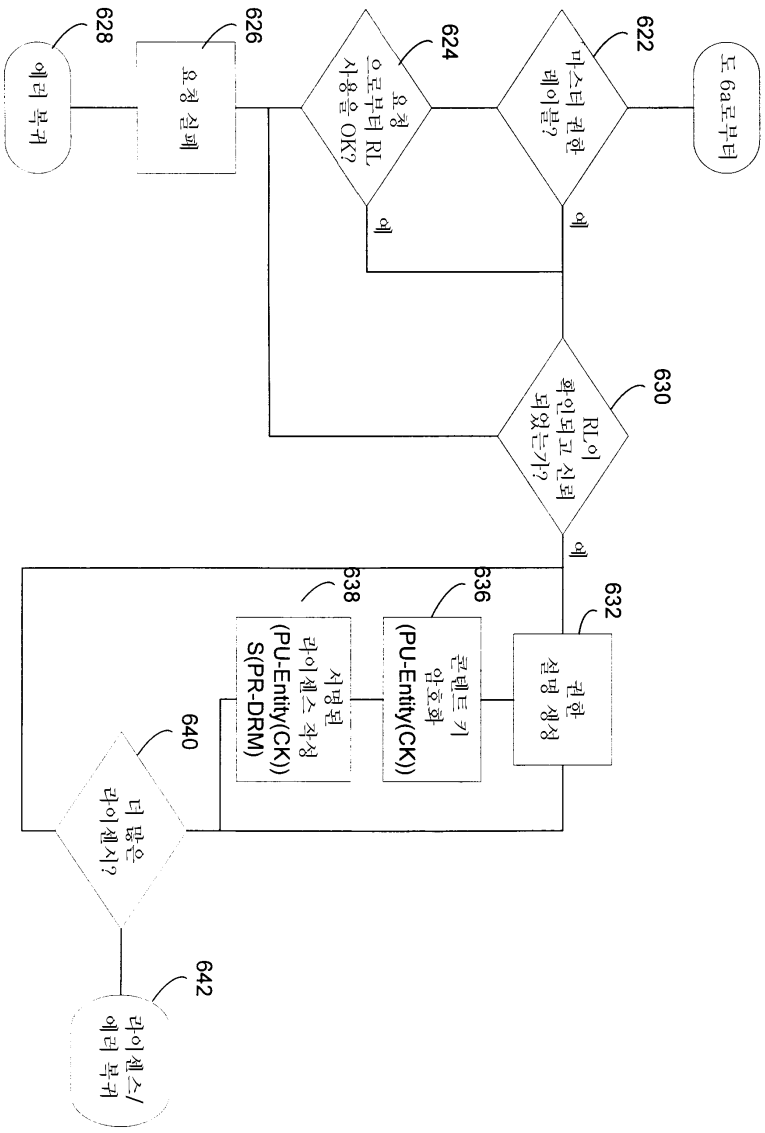
도면5


300
클라이언트 어플리케이션
302
DRM 클라이언트 API
306
권한 관리된 디지탈 콘텐트
310
암호해독된 디지탈 콘텐트
312
통신 네트워크
DRM 서버
320
330
332

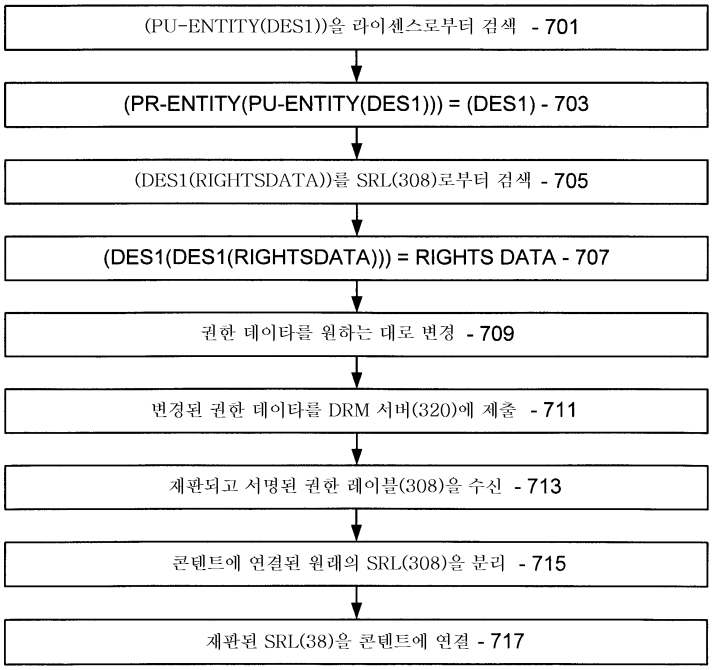
도면6a


라이 셀스 요청을 수신
602
요청자의 아이덴티티를 인증
604
아이덴티티에 권한부여
606
요청 내의 인증서인가?
608
예
/디렉토리 내의 인증서 인가?
610
예
인증서 검색
612
신뢰된 인증서인가?
616
예
라이 셀스가 라이 셀시에게 발행할 수 있음
618
에러
614
더 많은 라이 셀시?
620
아니오
도 6b

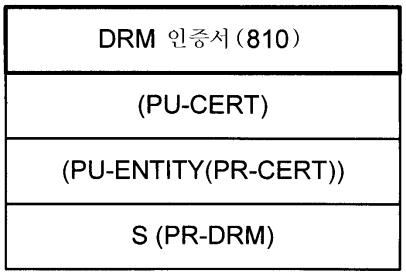
도면6b


도 6a로부터
622
마스터 권한 테이블?
624
요청으로부터 RL 사용을 OK?
626
요청 실패
628
에러 복귀
예
아니오
630
RL이 확인되고 신뢰되었는가?
예
632
권한 설명 생성
636
콘텐트 키 암호화 (PU-Entity(CK))
638
서명된 라이센스 작성 (PU-Entity(CK)) S(PR-DRM)
640
더 많은 라이센스?
642
라이센스/에러 복귀

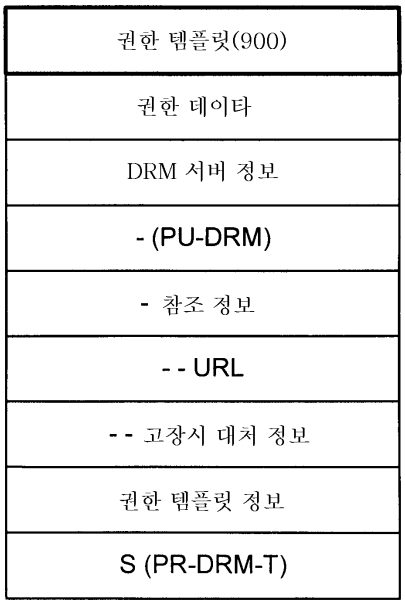
도면7


(PU-ENTITY(DES1))을 라이센스로부터 검색 - 701
(PR-ENTITY(PU-ENTITY(DES1))) = (DES1) - 703
(DES1(RIGHTSDATA))를 SRL(308)로부터 검색 - 705
(DES1(DES1(RIGHTSDATA))) = RIGHTS DATA - 707
권한 데이타를 원하는 대로 변경 - 709
변경된 권한 데이타를 DRM 서버(320)에 제출 - 711
재판되고 서명된 권한 레이블(308)을 수신 - 713
콘텐트에 연결된 원래의 SRL(308)을 분리 - 715
재판된 SRL(38)을 콘텐트에 연결 - 717

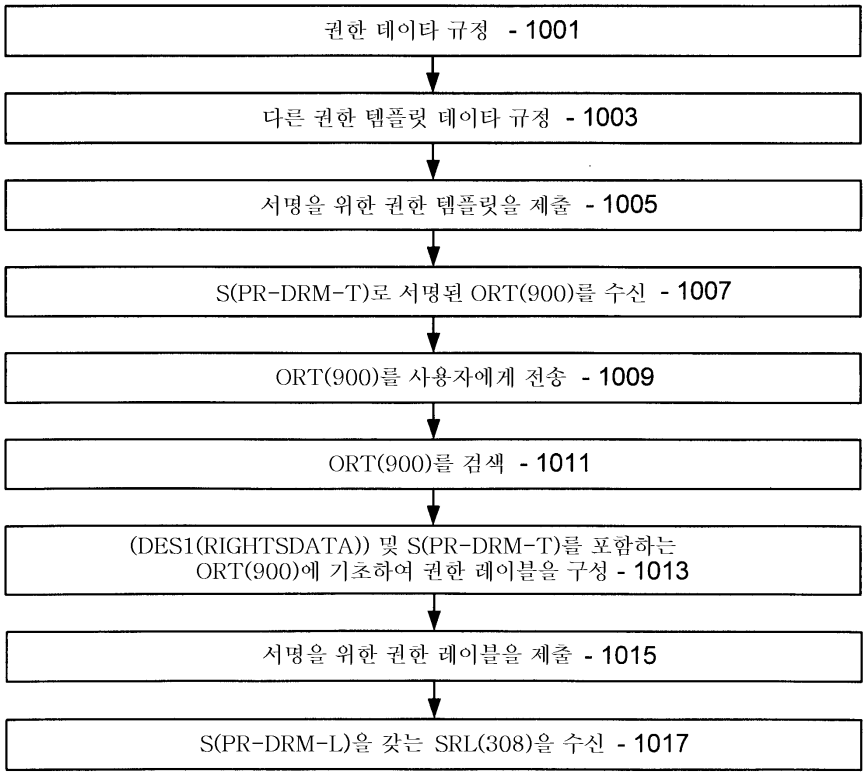
도면8


DRM 인증서 (810)
(PU-CERT)
(PU-ENTITY(PR-CERT))
S (PR-DRM)

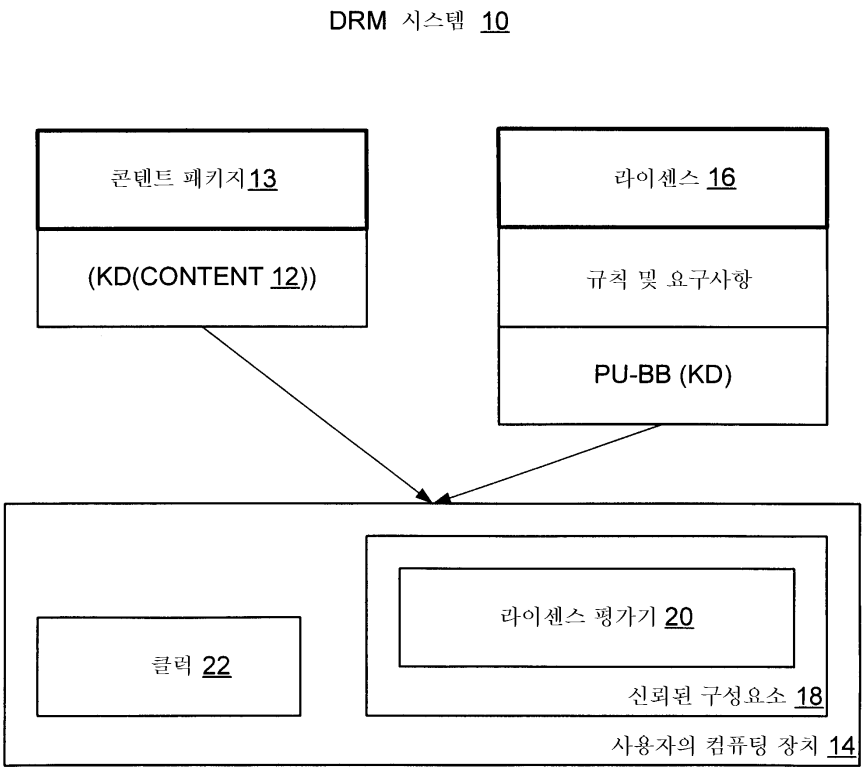
도면9


권한 템플릿(900)
권한 데이타
DRM 서버 정보
- (PU-DRM)
- 참조 정보
- - URL
- - 고장시 대처 정보
권한 템플릿 정보
S (PR-DRM-T)

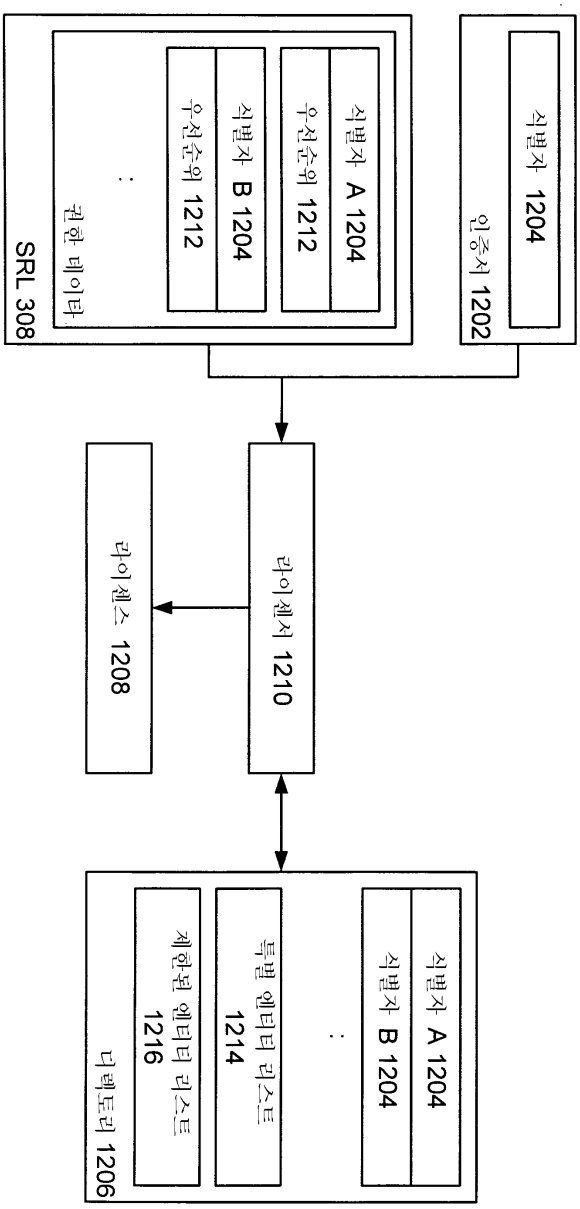
도면10


권한 데이타 규정 - 1001
다른 권한 템플릿 데이타 규정 - 1003
서명을 위한 권한 템플릿을 제출 - 1005
S(PR-DRM-T)로 서명된 ORT(900)를 수신 - 1007
ORT(900)를 사용자에게 전송 - 1009
ORT(900)를 검색 - 1011
(DES1(RIGHTSDATA)) 및 S(PR-DRM-T)를 포함하는
ORT(900)에 기초하여 권한 레이블을 구성 - 1013
서명을 위한 권한 레이블을 제출 - 1015
S(PR-DRM-L)을 갖는 SRL(308)을 수신 - 1017

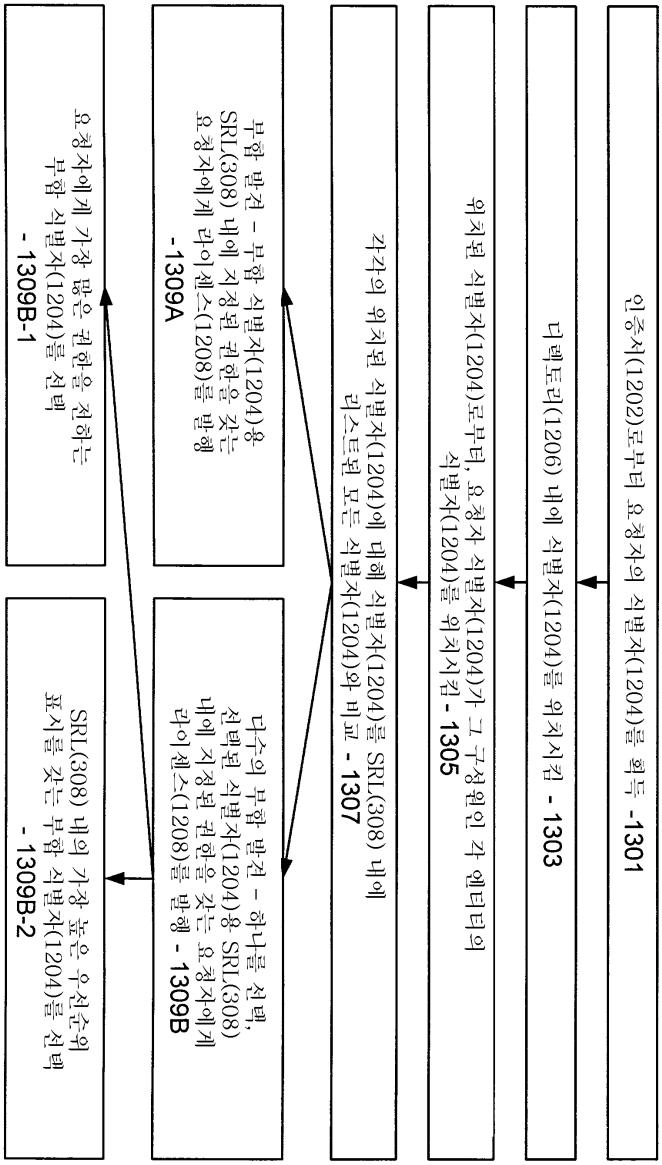
도면11


DRM 시스템 10
콘텐트 패키지 13
(KD(CONTENT 12))
라이센스 16
규칙 및 요구사항
PU-BB (KD)
라이센스 평가기 20
클럭 22
신뢰된 구성요소 18
사용자의 컴퓨팅 장치 14

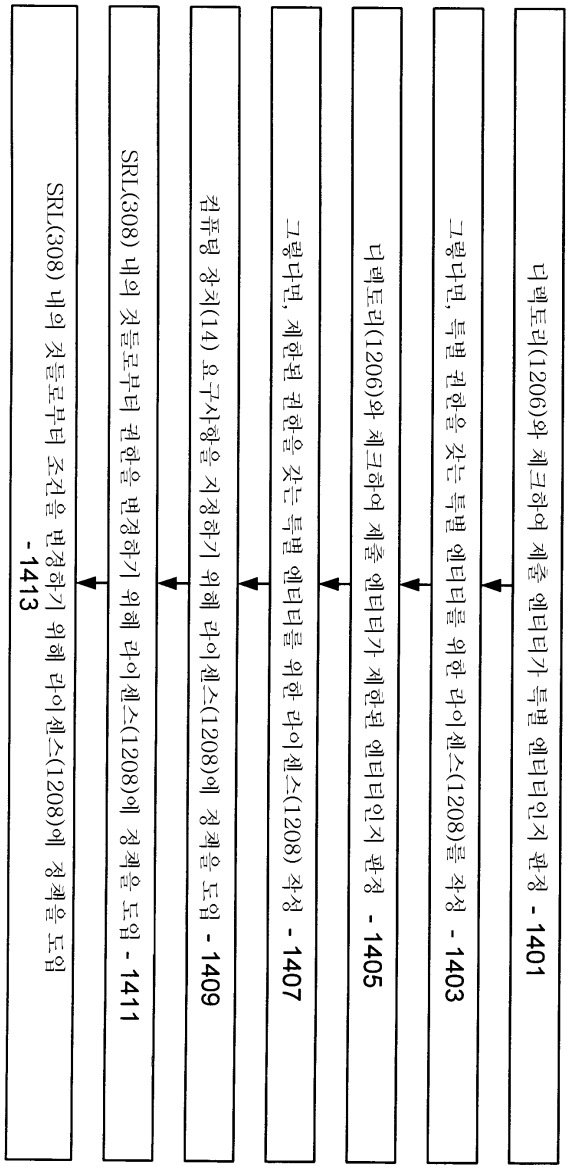
도면12


식별자 1204
인증서 1202
식별자 A 1204
우선순위 1212
식별자 B 1204
우선순위 1212
권한 데이타
SRL 308
라이센스 1208
라이센서 1210
식별자 A 1204
식별자 B 1204
특별 엔티티 리스트 1214
제한된 엔티티 리스트 1216
디렉토리 1206

도면13


인증서(1202)로부터 요청자의 식별자(1204)를 획득 - 1301
디렉토리(1206) 내에 식별자(1204)를 위치시킴 - 1303
위치된 식별자(1204)로부터, 요청자 식별자(1204)가 그 구성원인 각 엔티티의 식별자(1204)를 위치시킴 - 1305
각각의 위치된 식별자(1204)에 대해 식별자(1204)를 SRL(308) 내에 리스트된 모든 식별자(1204)와 비교 - 1307
부합 발견 - 부합 식별자(1204)용 SRL(308) 내에 지정된 권한을 갖는 요청자에게 라이센스(1208)를 발행 - 1309A
다수의 부합 발견 - 하나를 선택, 선택된 식별자(1204)용 SRL(308) 내에 지정된 권한을 갖는 요청자에게 라이센스(1208)를 발행 - 1309B
요청자에게 가장 많은 권한을 전하는 부합 식별자(1204)를 선택 - 1309B-1
SRL(308) 내의 가장 높은 우선순위 표시를 갖는 부합 식별자(1204)를 선택 - 1309B-2

도면14


디렉토리(1206)와 체크하여 제출 엔티티가 특별 엔티티인지 판정 - 1401
그렇다면, 특별 권한을 갖는 특별 엔티티를 위한 라이센스(1208)를 작성 - 1403
디렉토리(1206)와 체크하여 제출 엔티티가 제한된 엔티티인지 판정 - 1405
그렇다면, 제한된 권한을 갖는 특별 엔티티를 위한 라이센스(1208) 작성 - 1407
컴퓨팅 장치(14) 요구사항을 지정하기 위해 라이센스(1208)에 정책을 도입 - 1409
SRL(308) 내의 것들로부터 권한을 변경하기 위해 라이센스(1208)에 정책을 도입 - 1411
SRL(308) 내의 것들로부터 조건을 변경하기 위해 라이센스(1208)에 정책을 도입 - 1413