(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년09월01일
(11) 등록번호 10-1548753
(24) 등록일자 2015년08월25일

(51) 국제특허분류(Int. Cl.)
G06Q 50/10 (2012.01)
(21) 출원번호 10-2009-7027149
(22) 출원일자(국제) 2008년08월04일
심사청구일자 2013년07월31일
(85) 번역문제출일자 2009년12월28일
(65) 공개번호 10-2010-0050442
(43) 공개일자 2010년05월13일
(86) 국제출원번호 PCT/KR2008/004503
(87) 국제공개번호 WO 2009/022802
국제공개일자 2009년02월19일
(30) 우선권주장
60/955,125 2007년08월10일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
KR1020050029723 A*
KR1020060102686 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
엘지전자 주식회사
서울특별시 영등포구 여의대로 128 (여의도동)
(72) 발명자
박구용
서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)
조성현
서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)
(뒷면에 계속)
(74) 대리인
에스앤아이피특허법인

전체 청구항 수 : 총 10 항 심사관 : 장지혜

(54) 발명의 명칭 **컨텐츠 공유 방법**

(57) 요 약

컨텐츠 공유 방법이 개시되어 있다. 컨텐츠 공유 방법은 수신 디바이스를 사용하여, 서비스 제공자로부터 컨텐츠를 수신하고, 타겟 디바이스에서 지원되는 컨텐츠 보호 솔루션을 검출하고, 그 검출된 컨텐츠 보호 솔루션에 기반하여 상기 컨텐츠를 상기 타겟 디바이스 및 상기 수신 디바이스 중 어느 하나에서 지원되는 컨텐츠 보호 솔루션에 적합하도록 변환한다. 상기 수신 디바이스는 상기 수신 디바이스의 인증서에 상기 수신 디바이스의 보안 특성을 나타내는 보안 솔루션 레벨을 포함할 수 있다. 따라서, 수신 디바이스를 이용하여 서비스 제공자로부터 송신되는 컨텐츠를 홈 디바이스의 보안 솔루션에 부합되게 재분해함으로써 컨텐츠를 효율적으로 공유할 수 있다.

(72) 발명자

박일곤

서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)

정만수

서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)

키란, 쿠마 케이

서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)

김수정

서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)

정민규

서울특별시 서초구 바우뫼로 38, LG R&D Campus DM Lab NAS Group (우면동)

(30) 우선권주장

60/957,708 2007년08월23일 미국(US)
60/971,548 2007년09월11일 미국(US)
60/981,815 2007년10월22일 미국(US)
60/981,816 2007년10월22일 미국(US)

특허청구의 범위

청구항 1

수신 디바이스를 이용한 컨텐츠 공유 방법에 있어서,

서비스 제공자로부터 컨텐츠를 수신하는 단계;

타겟 디바이스에서 지원되는 컨텐츠 보호 솔루션을 검출하는 단계; 및

상기 검출된 컨텐츠 보호 솔루션에 기반하여 상기 컨텐츠를 상기 타겟 디바이스 및 상기 수신 디바이스 중 어느 하나에서 지원되는 컨텐츠 보호 솔루션에 적합하도록 변환하는 단계를 포함하며,

상기 수신 디바이스는 상기 수신 디바이스의 인증서에 상기 수신 디바이스의 보안 특성을 나타내는 보안 솔루션 레벨을 포함하고,

상기 보안 솔루션 레벨은 비보안 수행 환경(Non-Secured Execution Environment)에서 보안 솔류션 인증 프로세스의 인증(Authentication) 및 무결성(Integrity) 체크를 수행하지 않는 보안 수준을 나타내는 제로 레벨, 비보안 수행 환경에서 디바이스의 소프트웨어 엘리먼트(Element)를 사용하여 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 보안 수준을 나타내는 제 1 레벨, 비보안 수행 환경에서 디바이스의 하드웨어 엘리먼트를 사용하여 직접적으로 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 보안 수준을 나타내는 제 2 레벨, 보안 수행 환경(Secured Execution Environment)에서 디바이스의 소프트웨어 엘리먼트를 사용하여 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 보안 수준을 나타내는 제 3 레벨, 및 보안 수행 환경에서 디바이스의 하드웨어 엘리먼트를 사용하여 직접적으로 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 보안 수준을 나타내는 제 4 레벨 중 어느 하나인 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 2

제 1 항에 있어서, 상기 보안 솔루션 레벨은 상기 수신 디바이스의 보안 솔루션 인증 프로세스의 보안 특성 정보에 의하여 분류되는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 3

제 2 항에 있어서, 상기 보안 솔루션 레벨은 상기 보안 솔루션 인증 프로세스에 의한 것이거나, 소프트웨어 또는 하드웨어 엘리먼트를 사용한 인증 및 무결성 체크 여부에 따라 다수의 등급으로 분류되는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 4

제 2 항에 있어서, 상기 보안 솔루션 인증 프로세스의 보안성이 높을 수록 상기 보안 솔루션 레벨은 높은 레벨로 지정되는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 5

제 1 항에 있어서, 상기 변환 단계는,

상기 타겟 디바이스에서 지원되는 타겟 컨텐츠 보호 솔루션이 상기 수신 디바이스에서 지원되는 컨텐츠 보호 솔루션과 동일할 경우, 상기 컨텐츠를 상기 수신 디바이스에서 지원되는 컨텐츠 보호 솔루션에 부합되도록 변환하는 단계; 및

상기 타겟 디바이스에서 지원되는 타겟 컨텐츠 보호 솔루션이 상기 수신 디바이스에서 지원되는 컨텐츠 보호 솔루션과 상이할 경우, 상기 컨텐츠를 타겟 컨텐츠 보호 솔루션에 부합되도록 변환하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 6

제 1 항에 있어서, 상기 서비스 제공자로부터 컨텐츠를 수신하는 단계는, 상기 서비스 제공자로부터 전송되는 컨텐츠를 서비스 보호 솔루션 및 컨텐츠 보호 솔루션 중 어느 하나를 사용하여 수신하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 7

제 1 항에 있어서, 상기 변환된 컨텐츠를 상기 타겟 디바이스로 재분배하는 단계를 더 포함하는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 8

제 1 항에 있어서, 홈 디바이스의 인증서에 상기 홈 디바이스의 보안 특성을 나타내는 보안 솔루션 레벨을 포함하는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 9

제 8 항에 있어서, 상기 수신 디바이스 보안 솔루션 레벨 또는 상기 홈 디바이스의 보안솔루션 레벨에 기반하여 상기 홈 디바이스로의 컨텐츠 전송을 제한할 수 있는 것을 특징으로 하는 컨텐츠 공유 방법.

청구항 10

제 8 항에 있어서, 상기 검출된 컨텐츠 보호 솔루션에 적합하도록 상기 컨텐츠의 사용에 필요한 정보를 변환하는 단계; 및

상기 변환된 정보를 상기 홈 디바이스로 전송하는 단계를 더 포함하는 것을 특징으로 하는 컨텐츠 공유 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 컨텐츠 공유 방법에 관한 것으로, 좀더 상세하게는 IPTV 수신 디바이스를 이용하여 서비스 제공자로부터 제공되는 컨텐츠를 홈 디바이스로 재분해함으로써 컨텐츠를 공유할 수 있는 컨텐츠 공유 기술과 관련된 것이다.

배 경 기 술

[0002] 최근 들어, 유선 또는 무선 통신망을 이용한 디지털 TV 서비스가 보편화되고 있다. 디지털 TV 서비스는 기존의 아날로그 방송 서비스에서는 제공할 수 없었던 다양한 서비스를 제공할 수 있다. 예를 들어 디지털 TV 서비스의 한 종류인 IPTV(Internet Protocol Television) 서비스의 경우 사용자로 하여금 시청 프로그램의 종류, 시청 시간 등을 능동적으로 선택할 수 있도록 하는 양방향성을 제공한다. IPTV 서비스는 이러한 양방향성을 기반으로 하여 다양한 부가 서비스, 예컨대 인터넷 검색, 홈쇼핑, 온라인 게임 등을 제공할 수도 있다.

[0003] 이러한 IPTV 서비스를 위해서는 사용자 측은 IPTV 셋톱박스를 구비하여야 한다. IPTV 셋톱박스는 양방향 서비스를 지원하는 소프트웨어를 탑재하고 그 소프트웨어를 기반으로 서비스 클라이언트로서의 기능을 수행할 수 있다. 예를 들어 IPTV 셋톱박스는 IP 네트워크를 통해 서비스 제공자와 정보를 송수신하면서 서비스 제공자에게 방송 컨텐츠의 전송을 요청하고 서비스 제공자로부터 수신되는 방송 신호를 표준 TV 신호로 변환하여 TV 수상기로 송신할 수 있다.

[0004] 한편, 최근에는 IPTV 서비스를 가정 내의 홈 네트워크 환경과 연계시켜 IPTV 컨텐츠의 제공 영역을 확장하려는 노력이 시도되고 있다. 그 예로, 컨텐츠 공유 서비스가 있다. 컨텐츠 공유 서비스는 IPTV 호환 단말기인 IPTV 셋톱박스를 홈 네트워크에 접속된 디바이스를과 연동시킨 뒤, IPTV 셋톱박스에 저장된 컨텐츠를 연동된 디바이스로 재분배한다. 따라서 컨텐츠 공유 서비스는 IPTV 컨텐츠를 사용자가 원하는 다양한 디바이스에서 재생할 수 있도록 한다.

[0005] 이러한 컨텐츠 공유 서비스를 위한 시스템의 구현에 있어서 가장 중요한 관건 중의 하나는 컨텐츠의 저장 또는 재분배 시에 발생할 수 있는 불법 행위들, 예컨대 컨텐츠의 불법적인 유출이나 복사 등으로부터 컨텐츠를 안전하게 보호하는 것이다. 따라서 컨텐츠의 공유 서비스에서는 컨텐츠의 보호를 위한 보안 수단 및 절차 등이 반드시 요구되며, 이러한 요구에 따라 관련 기술의 개발이 시급히 요구되고 있다.

발명의 상세한 설명

[0006] **기술적 과제**

[0007] 본 발명이 해결하고자 하는 기술적 과제는 디바이스에 보안 솔루션 레벨을 연계시키고, 디바이스의 보안 정보에 기반하여 컨텐츠를 재분배할 수 있는 컨텐츠 공유 방법을 제공하는데 있다.

[0008] **기술적 해결방법**

[0009] 이러한 기술적 과제를 해결하기 위하여 본 발명은 일 측면(Aspect)에서 컨텐츠 공유 방법을 제공한다. 상기 컨텐츠 공유 방법은, 수신 디바이스를 이용한 컨텐츠 공유 방법에 있어서, 서비스 제공자로부터 컨텐츠를 수신하는 단계와; 타겟 디바이스에서 지원되는 컨텐츠 보호 솔루션을 검출하는 단계; 및 상기 검출된 컨텐츠 보호 솔루션에 기반하여 상기 컨텐츠를 상기 타겟 디바이스 및 상기 수신 디바이스 중 어느 하나에서 지원되는 컨텐츠 보호 솔루션에 적합하도록 변환하는 단계를 포함한다. 상기 수신 디바이스는 상기 수신 디바이스의 인증서에 상기 수신 디바이스의 보안 특성을 나타내는 보안 솔루션 레벨을 포함할 수 있다.

[0010] 상기 보안 솔루션 레벨은 상기 수신 디바이스의 보안 솔루션 인증 프로세스의 보안 특성 정보에 의하여 분류(Classify)된다. 상기 보안 솔루션 레벨은 상기 보안 솔루션 인증 프로세스의 수행 환경, 소프트웨어 또는 하드웨어 엘리먼트를 사용한 인증 및 무결성 체크 여부에 따라 다수의 등급으로 분류될 수 있다. 상기 보안 솔루션 인증 프로세스의 보안성이 높을 수록 상기 보안 솔루션 레벨은 높은 레벨로 지정될 수 있다.

[0011] 상기 변환 단계는, 상기 검출된 컨텐츠 보호 솔루션이 상기 수신 디바이스에서 지원되는 컨텐츠 보호 솔루션과 동일할 경우, 상기 컨텐츠를 상기 수신 디바이스에서 지원되는 컨텐츠 보호 솔루션에 부합되도록 변환하는 단계; 및 상기 검출된 컨텐츠 보호 솔루션이 상기 수신 디바이스에서 지원되는 컨텐츠 보호 솔루션과 상이할 경우, 상기 컨텐츠를 상기 검출된 컨텐츠 보호 솔루션에 부합되도록 변환하는 단계를 포함할 수 있다.

[0012] 상기 서비스 제공자로부터 컨텐츠를 수신하는 단계는, 상기 서비스 제공자로부터 전송되는 컨텐츠를 서비스 보호 솔루션 및 컨텐츠 보호 솔루션 중 어느 하나를 사용하여 수신하는 단계를 포함할 수 있다.

[0013] 상기 컨텐츠 공유 방법은, 상기 변환된 컨텐츠를 상기 타겟 디바이스로 재분배하는 단계를 더 포함할 수 있다. 또한, 상기 컨텐츠 공유 방법은, 상기 검출된 컨텐츠 보호 솔루션에 적합하도록 상기 컨텐츠의 사용에 필요한 정보를 변환하는 단계; 및 상기 변환된 정보를 상기 홈 디바이스로 전송하는 단계를 더 포함할 수도 있다.

[0014] 상기 홈 디바이스는 상기 홈 디바이스의 인증서에 상기 홈 디바이스의 보안 특성을 나타내는 보안 솔루션 레벨을 포함할 수도 있다. 상기 수신 디바이스 보안 솔루션 레벨 또는 상기 홈 디바이스의 보안솔루션 레벨에 기반하여 상기 홈 디바이스로의 컨텐츠 전송을 제한할 수도 있다.

[0015] **유리한 효과**

[0016] 이상 설명한 바와 같이, 본 발명에 따르면 수신 디바이스를 이용하여 서비스 제공자로부터 송신되는 컨텐츠를 홈 디바이스의 보안 솔루션에 부합되게 재분해함으로써 컨텐츠를 효율적으로 공유할 수 있다. 또한 디바이스, 예컨대 수신 디바이스 또는 홈 디바이스에 해당 디바이스의 보안 특성을 나타내는 보안 솔루션 레벨을 연계시키고 이를 기반으로 컨텐츠의 전송을 제어할 수도 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 바람직한 실시예에 따른 컨텐츠 공유 방법을 위한 도메인 시스템의 구성을 도시하는 블록도이다.

[0018] 도 2는 컨텐츠 공유 방법을 실현하기 위한 시스템의 전체적인 구성을 개략적으로 도시하는 블록도이다.

[0019] 도 3은 도 2에 도시되어 있는 IPTV 수신 디바이스의 구성을 도시하는 블록도이다.

[0020] 도 4는 디바이스의 보안 솔루션 레벨을 지정하는 기준이 되는 보안 솔루션 레벨 테이블을 나타내는 예시도이다.

[0021] 도 5는 본 발명의 바람직한 실시예에 따른 컨텐츠 저장 방법의 절차를 설명하기 위한 예시도이다.

[0022] 도 6은 본 발명의 바람직한 실시예에 따른 컨텐츠 공유 방법을 실현하기 위한 시스템 구성을 도시하는 블록도이다.

[0023] 도 7은 본 발명의 바람직한 실시예에 따른 컨텐츠 공유 방법을 설명하기 위한 흐름도이다.

[0024] 도 8은 본 발명의 바람직한 다른 실시예에 따른 컨텐츠 공유 방법을 실현하기 위한 시스템 구성을 도시하는 블록도이다.

[0025] 도 9는 본 발명의 바람직한 다른 실시예에 따른 컨텐츠 공유 방법을 설명하기 위한 흐름도이다.

[0026] <도면의 주요 부분에 대한 부호 설명>

[0027] 20 : 서비스 제공자

[0028] 40 : IPTV 수신 디바이스

[0029] 44 : 컨텐츠 보호 솔루션

[0030] 45a : IPTV 수신 디바이스의 컨텐츠 보호 솔루션 'A'

[0031] 50 : 홈 디바이스

[0032] 55a : 홈 디바이스의 컨텐츠 보호 솔루션 'A'

[0033] **발명의 실시를 위한 형태**

[0034] 이하, 본 발명이 속하는 분야에 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 본 발명의 바람직한 실시예를 첨부된 도면을 참조하여 상세히 설명한다. 이하에 설명할 본 발명의 바람직한 실시예에서는 내용의 명료성을 위하여 특정한 기술 용어를 사용한다. 하지만 본 발명은 그 선택된 특정 용어에 한정되지는 않으며, 각각의 특정 용어가 유사한 목적을 달성하기 위하여 유사한 방식으로 동작하는 모든 기술 동의어를 포함함을 미리 밝혀둔다.

[0035] 도 1은 본 발명의 바람직한 실시예에 따른 컨텐츠 공유 방법을 위한 도메인 시스템의 구성을 도시하는 블록도이다.

[0036] 도 1에 도시된 바와 같이, 도메인 시스템(10)은 도메인(7)을 구성한다. 도메인(7)이란 허가된(Authorized) 디바이스인 도메인 디바이스(5)의 집합으로서, 도메인 서비스가 적용되는 범위를 의미할 수 있다. 도메인(7) 내에 포함된 도메인 디바이스(5) 간에는 허용된 권한에 따라 콘텐츠를 공유하고 사용할 수 있다.

[0037] 도메인(7)은 디바이스의 물리적인 위치를 고려하여 구성할 수 있다. 즉 특정한 물리적 영역 내에 존재하는 디바이스들로 도메인(7)을 구성하는 것이다. 이러한 도메인(7)을 구성하기 위해서는 로컬 환경이 요구된다. 이때 로컬 환경이란 특정한 로컬 영역 내에 속한 디바이스들이 상호 연동될 수 있는 물리적인 네트워크가 마련되어 있고, 이 물리적인 네트워크가 외부의 네트워크와도 연동할 수 있는 환경을 의미할 수 있다.

[0038] 이와 같은 로컬 환경을 제공할 수 있는 예로서, 홈 네트워크 시스템을 들 수 있다. 홈 네트워크 시스템은 유선 또는 무선 로컬 네트워크를 통하여 가정 내의 가전기기, 각종 센서들, 보안 기기 등의 상호 연동이 가능하며, 홈 게이트웨이와 같은 통신 노드를 통하여 인터넷 등과 같은 외부 네트워크와도 연동할 수 있다. 상기 로컬 환경은 이러한 홈 네트워크 시스템뿐만 아니라 상호 연동 가능한 2개 이상의 네트워크 디바이스가 존재한다면 구성 가능하다.

[0039] 이하에서는 이러한 로컬 환경이 마련된 영역을 도메인 영역이라 칭하기로 한다. 도메인 영역 내에는 다수의 디바이스가 존재할 수 있다. 사용자는 이러한 디바이스들을 이용하여 도메인(7)을 구성하고 도메인 디바이스(5) 간에 컨텐츠를 공유하며 사용할 수 있다. 도메인(7)으로의 등록을 위하여 디바이스는 도메인 관리자(1)에게 도메인 등록 요청을 송신하고 이를 수신한 도메인 관리자(1)는 상기 도메인 등록 요청이 정당한 요청인지 등을 판단한 뒤 디바이스를 도메인(7)에 등록한다. 도메인(7)에 등록된 도메인 디바이스(5) 간에는 허용된 조건에 따라 콘텐츠를 공유하고 사용할 수 있다. 한편 경우에 따라서는 도메인 영역 밖의 디바이스, 예컨대 인터넷 등을 통해 접속하는 외부 영역의 디바이스 등도 리모트 상태로 도메인에 등록될 수도 있다.

[0040] 한편 도메인(7)은 도메인 대표 디바이스(3)를 포함할 수 있다. 도메인 대표 디바이스(3)는 도메인 내에서 도메인 관리를 위한 마스터의 역할을 수행하는 디바이스를 의미할 수 있다. 예를 들어, 도메인 대표 디바이스(3)는 도메인 관리자(1)를 도와 도메인 관리 기능, 도메인 디바이스 관리 기능, 도메인 디바이스 인증 기능 등을 수행할 수도 있다. 또한, 상기 도메인 대표 디바이스는 도메인 영역 내의 디바이스의 근접도(Proximity) 측정을 수행하여 해당 디바이스가 도메인 영역 내에 포함되는 지의 여부를 검증할 수도 있다. 즉 도메인 대표 디바이스(3)는 도메인(7)의 물리적인(예컨대, 홉수, 반응시간, TTL 등) 범위를 결정하는 기능을 수행할 수 있다. 상기 근접도 측정 정보는 도메인 디바이스(5)를 도메인으로 등록할 때 도메인 관리자(1)에서 해당 도메인 디바이스(5)의 인증 가능 여부를 판단할 수 있는 정보로 사용될 수도 있고, 도메인 디바이스(5)가 로컬 엑세스 상태(즉, 도메인 영역 내에서 도메인에 엑세스한 상태) 인지 리모트 엑세스 상태(즉, 도메인 영역 밖에서 도메인에 엑세

스한 상태) 인지를 관리하기 위한 정보로 사용될 수도 있다.

[0041] 이러한 도메인 대표 디바이스(3)는 특정 시점(예컨대 도메인의 구성 초기, 사용자로부터의 요청 시, 기존의 도메인 대표 디바이스에 에러가 발생했을 경우 등)에 도메인 디바이스 중에서 선출될 수 있다. 예를 들어, 도메인 디바이스들 간에 디바이스 커패빌리티(Capability) 정보를 송수신하면서 디바이스 커패빌리티를 서로 비교하고 디바이스 커패빌리티가 높은 디바이스는 생존하고 디바이스 커패빌리티가 낮은 디바이스는 탈락하는 선출 경쟁(Election Competition)을 수행하여, 가장 디바이스 커패빌리티가 높은 도메인 디바이스(예컨대, 최종적으로 선출 경쟁에서 생존한 디바이스)가 도메인 대표 디바이스(3)로 선출될 수도 있으며, 또는 도메인 디바이스들이 도메인 관리자(1) 또는 특정 디바이스에게 디바이스 커패빌리티 정보를 송신하고 이를 수신한 도메인 관리자(1) 또는 특정 디바이스가 디바이스 커패빌리티가 높은 도메인 디바이스를 도메인 대표 디바이스(3)로 선출할 수도 있다.

[0042] 상기 디바이스 커패빌리티란 해당 디바이스가 가지는 하드웨어적 또는 소프트웨어적 능력(예를 들어, 배터리 용량, 하드웨어 사양, 소프트웨어 종류, 특정 소프트웨어의 탑재 여부 등)을 의미할 수 있다. 한편 선출된 도메인 디바이스는 도메인 대표 디바이스(3)로 지정되어 상기 언급되었던 기능들을 수행하게 된다.

[0043] 이상 도메인 시스템의 구성을 살펴보았다. 이러한 도메인의 개념을 IPTV 서비스 시스템에 도입하면 IPTV 서비스 컨텐츠를 다수의 디바이스에서 공유하여 사용할 수 있는 컨텐츠 공유 시스템을 구성할 수 있다.

[0044] 도 2는 컨텐츠 공유 방법을 실현하기 위한 시스템의 전체적인 구성을 개략적으로 도시하는 블록도이다.

[0045] 도 2에 도시된 바와 같이, IPTV 수신 디바이스(40)는 IP 통신망을 통하여 서비스 제공자(20)와 연동할 수 있다. 이때, 상기 IPTV 수신 디바이스(40)는 IPTV 서비스 기능을 구비하는 단말기, 예컨대 IPTV 셋톱박스 등을 의미할 수 있다. IPTV 수신 디바이스(40)는 도메인 대표 디바이스일 수도 있다. 이러한 IPTV 수신 디바이스(40)는 다른 한편으로 홈 디바이스(50)와 연동할 수 있다. 이때 홈 디바이스(50)는 유선 또는 무선 네트워킹 기능을 구비하는 고정형 또는 포터블 단말기들, 예컨대 가전기기, 휴대폰, PC(Personal Computer), 노트북(Notebook), PDA(Personal Digital Assistance), PMP(Portable Multimidea Player), 리모컨 등일 수 있다.

[0046] IPTV 수신 디바이스(40) 및 홈 디바이스(50)는 컨텐츠의 공유를 위하여 도메인(30)에 조인(Join)할 수 있다. 즉, IPTV 수신 디바이스(40) 및 홈 디바이스(50)는 도메인 디바이스일 수 있다. 도메인에 조인하기 위하여 IPTV 수신 디바이스(40) 및 홈 디바이스(50)는 각각 서비스 제공자(20)에게 도메인(30)으로의 조인을 요청하고, 서비스 제공자(20)는 해당 디바이스(40, 50)을 인증한 후 그 디바이스로 인증서(Certificate)를 발급하고 디바이스(40, 50)를 도메인(30)에 등록할 수 있다.

[0047] 상기 도메인(30)으로의 등록 요청 시에 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)는 각각 자신의 보안 커패빌리티 정보를 서비스 제공자(20)에게 제공할 수 있다. 이때 보안 커패빌리티 정보는 해당 디바이스에 적용되어 있는 보안 솔루션(예컨대, CAS(Conditional Access System) 모듈, DRM(Digital Rights Management) 모듈 등)들의 정보, 보안 솔루션 레벨 등을 포함할 수 있다. 상기 보안 솔루션 레벨은 디바이스에 적용된 보안 솔루션 인증 프로세스의 보안 수준을 나타내는 보안 솔루션 프로파일 정보를 의미할 수 있다. 바람직하기로는 보안 솔루션 레벨은 보안 솔루션 인증 프로세스의 보안 수준을 정해진 테이블에 근거하여 분류(Classify)한 정보를 의미할 수 있다. 이러한 보안 솔루션 레벨에 대해서는 차후에 상세히 설명할 것이다.

[0048] 서비스 제공자(20)는 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)로부터 수신된 보안 커패빌리티 정보를 저장할 수도 있고, 보안 커패빌리티 정보(예컨대 보안 솔루션들의 정보, 보안 솔루션 레벨 등) 중 적어도 어느 하나를 디바이스(40, 50)의 인증서에 삽입하여 디바이스(40, 50)로 발급할 수도 있다.

[0049] 한편, IPTV 수신 디바이스(40)는 서비스 제공자(20)로부터 컨텐츠 안내 정보를 요청하여 수신할 수 있다. 이때 컨텐츠 안내 정보는 서비스 컨텐츠의 일정, 목록, 부가 정보 등을 안내하는 정보로서, 예컨대 EPG(Electronic Program Guide), CPG(Content Program Guide), VoD 컨텐츠 가이드, IPG(Interactive Program Guide) 등일 수 있다.

[0050] IPTV 수신 디바이스(40)는 서비스 제공자(20)로부터 수신한 컨텐츠 안내 정보를 사용자 인터페이스에 부합하도록 가공하여 표시할 수 있다. 사용자는 표시된 컨텐츠 안내 정보에서 원하는 서비스 컨텐츠를 선택할 수 있다. 그러면 IPTV 수신 디바이스(40)는 선택된 컨텐츠를 서비스 제공자(20)에게 요청할 수 있다.

[0051] IPTV 수신 디바이스(40)로부터의 요청에 따라 서비스 제공자(20)는 해당 컨텐츠를 IPTV 수신 디바이스(40)로 전송한다. 이때 서비스 제공자(20)는 상기 컨텐츠와 더불어 상기 컨텐츠의 사용을 위하여 필요한 컨텐츠 관련 정

보들, 예컨대 보안 정보(Security Information), 유시지 권한 정보(Usage Rights Information), 리보케이션 리스트 정보(Revocation List Information) 등을 IPTV 수신 디바이스(40)로 전송할 수도 있다. 상기 보안 정보는 컨텐츠의 사용 또는 공유가 가능한 보안 수준, 컨텐츠의 사용에 필요한 보안 솔루션 정보 등을 포함할 수 있다. 상기 유시지 권한 정보는 컨텐츠의 사용을 위한 권한 정보, 예컨대 컨텐츠의 라이선스 등을 포함할 수 있다. 리보케이션 리스트 정보는 컨텐츠의 사용이 금지되는 디바이스의 리스트인 리보케이션 리스트 또는 그 리보케이션 리스트를 식별할 수 있는 정보를 포함할 수 있다.

[0052] IPTV 수신 디바이스(40)는 서비스 제공자(20)로부터 전송되는 컨텐츠를 수신한 후 저장 및 재생할 수 있으며, 도메인(30)에 등록된 홈 디바이스(50)로 전송할 수도 있다. 컨텐츠의 저장, 재생 또는 전송 등을 수행하기 위해서는 서비스 제공자(20)로부터 전달된 컨텐츠와 연계되는 정보들, 예컨대 보안 정보, 유시지 권한 정보, 리보케이션 리스트 정보 등을 고려할 수 있으며, 그에 근거하여 컨텐츠의 저장, 재생 또는 전송을 제한할 수도 있다.

[0053] 도 3은 도 2에 도시되어 있는 IPTV 수신 디바이스(40)의 구성을 도시하는 블록도이다.

[0054] 도 3에 도시된 바와 같이, IPTV 수신 디바이스(40)는 IPTV 수신 모듈(41), 보안 컨트롤러(42), 보안 솔루션(43), 컨텐츠 재생기(47), 스토리지(48) 및 출력 포트(46) 등을 포함할 수 있다. 도시되지는 않았지만 IPTV 수신 디바이스(40)는 통산의 IPTV 단말기가 구비하는 기능 모듈들, 예컨대 정보 입력 모듈, 디스플레이 모듈, 전원 모듈 등도 구비할 수 있음은 물론이나, 이들은 본 발명의 요지와 직접적으로 연관되지는 않는 요소들이므로 별도의 도시 및 설명은 생략하기로 한다.

[0055] IPTV 수신 모듈(41)은 서비스 제공자(20)와 데이터를 송수신하는 인터페이스 기능을 수행할 수 있다. 예를 들어, IPTV 수신 모듈(41)은 서비스 제공자(20)로부터 컨텐츠 및 컨텐츠의 사용에 필요한 정보들, 예컨대 보안 정보, 유시지 권한 정보, 리보케이션 리스트 정보 등을 수신할 수 있다. 상기 컨텐츠는 특정 보호 기술, 예컨대 CAS(Conditional Access System) 또는 DRM(Digital Rights Management) 등과 같은 서비스 보호 기술이 또는 컨텐츠 보호 기술이 적용되어 스크램블링(Scrambling) 또는 암호화(Encrytion)되어 있을 수 있다. 한편 IPTV 수신 모듈(41)은 서비스 제공자(20) 또는 특정 서버로부터 보안 솔루션(43)과 관련한 데이터들, 예컨대 DRM 코드, 보안 메시지, 어플리케이션 등을 수신할 수도 있다. IPTV 수신 디바이스는 이러한 데이터들을 TS(Transport Stream) 또는 보안 다운로드(Secure Download)의 형태로 수신할 수 있다.

[0056] 보안 컨트롤러(42)는 컨텐츠 및 디바이스 보안을 위한 보안 제어 기능을 수행할 수 있다. 예를 들어, 보안 컨트롤러(42)는 서비스 제공자(20)에게 IPTV 수신 디바이스(40)를 도메인에 등록해줄 것을 요청하고, 도메인에 등록되었음을 증명하는 인증서를 수신하여 저장할 수 있다. 도메인 등록 요청 시 보안 컨트롤러(42)는 IPTV 수신 디바이스(40)에 구비된 보안 솔루션(43)을 검사하여 IPTV 수신 디바이스(40)에 적용되어 있는 보안 솔루션(예컨대, CAS 모듈, DRM 모듈 등)들의 정보를 서비스 제공자(20)로 제공할 수 있으며, IPTV 수신 디바이스(40)의 보안 솔루션 레벨을 서비스 제공자(20)에게 제공할 수도 있다.

[0057] 보안 컨트롤러(42)는 서비스 제공자(20)로부터 전송되는 컨텐츠 및 그 컨텐츠의 사용에 필요한 컨텐츠 관련 정보를 IPTV 수신 모듈(41)을 제어하여 수신하고, 보안 솔루션(43), 예컨대 서비스 보호 솔루션(44)을 제어하여 스크램블링되어 있는 컨텐츠를 클린 타입의 컨텐츠로 변환할 수 있다. 또 보안 컨트롤러(42)는 보안 솔루션(43), 예컨대 컨텐츠 보호 솔루션(45)을 제어하여 클린 타입으로 변환된 컨텐츠 및 그 컨텐츠의 유시지 권한 정보를 컨텐츠 재생기(47)에서 지원 가능한 타입으로 변환하여 스토리지(48)에 저장하거나 또는 컨텐츠 재생기(47)에서 재생 가능하도록 한다.

[0058] 또한, 보안 컨트롤러(42)는 사용자로부터 홈 디바이스(50)로의 컨텐츠 공유 요청이 있을 경우, 홈 디바이스(50)에 어떠한 컨텐츠 보호 솔루션 적용되어 있는지를 검출하고, 해당 컨텐츠 보호 솔루션이 지원하는 형태로 컨텐츠를 변환한 후 변환한 컨텐츠를 출력 포트(46)를 통해 홈 디바이스(50)로 전송할 수 있다. 이때, 만약 검출된 홈 디바이스(50)의 컨텐츠 보호 솔루션(미도시)과 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45)이 동일할 경우, 보안 컨트롤러(42)는 별도의 변환 없이 상기 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45)에서 지원 가능한 타입으로 변환한 컨텐츠를 홈 디바이스(50)로 전송할 수도 있다.

[0059] 한편, 보안 컨트롤러(42)는 IPTV 수신 디바이스(40)의 보안 솔루션 레벨 또는 홈 디바이스(50)의 보안 솔루션 레벨에 근거하여 컨텐츠의 공유를 제한할 수도 있다. 예를 들어 보안 컨트롤러(42)는 컨텐츠와 연계된 보안 정보를 확인하여 컨텐츠의 전송에 필요한 보안 수준을 추출하고, IPTV 수신 디바이스(40) 또는 홈 디바이스(50)의 보안 솔루션 레벨에서 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)의 보안 수준을 확인한 뒤, 컨텐츠의 사용에 필요한 보안 수준을 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)의 보안 수준이 만족하지 못할 경우 컨텐

츠의 사용 또는 전송을 제한할 수도 있다.

[0060] 보안 솔루션(43)은 보안 컨트롤러(42)의 제어에 따라 컨텐츠를 보호하기 위한 기능을 수행할 수 있다. 보안 솔루션(43)은 서비스 보호 솔루션(44), 컨텐츠 보호 솔루션(45) 등을 포함할 수 있다.

[0061] 서비스 보호 솔루션(44)은 컨텐츠에 서비스 보호 기술을 적용하거나 적용을 해지하는 기능을 수행하는 모듈을 의미할 수 있다. 서비스 보호 솔루션(44)은 CAS 솔루션 등일 수 있다. 서비스 보호 모듈(44)은 보안 컨트롤러(42)의 제어에 따라 서비스 제공자(20)로부터 전송되는 컨텐츠를 수신하여 처리한다. 예를 들면, 서비스 보호 솔루션(44)은 서비스 제공자(20)로부터 수신되는 TS에서 디스크램블링(Descrambling) 키를 추출하고 그 디스크램블링 키를 이용하여 스크램블링되어 있는 수신 컨텐츠 디스크램블링하여 클린 타입의 컨텐츠로 변환할 수 있다.

[0062] 컨텐츠 보호 솔루션(45)은 컨텐츠에 컨텐츠 보호 기술을 적용하거나 적용을 해지하는 기능을 수행하는 모듈을 의미할 수 있다. 컨텐츠 보호 모듈(45)은 DRM 모듈, 카피 보호(Copy Protection) 모듈, ASD(Authorized Service Domain) 모듈 등일 수 있다. 컨텐츠 보호 솔루션(45)은 보안 컨트롤러(42)의 제어에 따라 컨텐츠의 변환을 수행할 수 있다. 예를 들면, 컨텐츠 보호 솔루션(45)은 컨텐츠를 저장하거나 또는 홈 디바이스(50)로 재분배하기 위하여 컨텐츠를 DRM 기술에 따라 암호화하거나, 재생 등을 위하여 암호화된 컨텐츠를 복호화할 수 있다. 한편, 서비스 제공자(20)에서는 컨텐츠에 컨텐츠 보호 기술을 적용하여 IPTV 수신 디바이스(40)로 전송할 수도 있은데, 이 경우 컨텐츠 보호 솔루션(45)은 앞서 언급한 서비스 보호 솔루션(44)의 기능과 같은 개념으로 컨텐츠를 수신하여 저장하거나 처리할 수도 있다.

[0063] 컨텐츠 재생기(47)는 컨텐츠, 예컨대 멀티미디어 등을 재생하는 기능을 수행할 수 있다. 예를 들면, 컨텐츠 재생기(47)는, 사용자의 요청에 따라, 보안 솔루션(43)에 의하여 변환된 컨텐츠를 수신하여 재생하는 기능을 수행할 수 있다. 예컨대 컨텐츠 재생기(47)는 컨텐츠 보호 솔루션(45)과 연계되어 컨텐츠 보호 솔루션(45)에 의하여 변환되는 컨텐츠를 재생할 수 있다. 스토리지(48)는 보안 솔루션(43)에 의해 처리된 컨텐츠를 저장할 수 있다. 출력 포트(46)는 홈 디바이스(50)와 연동하는 기능을 수행한다. 예를 들어, 출력 포트(46)는 보안 컨트롤러(42)의 제어에 따라 컨텐츠를 홈 디바이스(50)로 전송하는 기능을 수행할 수 있다.

[0064] 이상 IPTV 수신 디바이스(40)의 구성을 살펴보았다. 한편, 도시하지는 않았지만 홈 디바이스(50)의 경우, 서비스 제공자(20)와 직접적으로 연동하는데 필요한 구성, 예컨대 IPTV 수신 모듈(41) 또는 서비스 보호 솔루션(44) 등을 가지지 않아도 된다는 점 이외에는 상술한 IPTV 수신 디바이스(40)와 거의 동일한 구성을 가질 수 있다. 그러나 이는 한정된 사항은 아니며, 홈 디바이스(50)가 서비스 제공자(20)와 직접 연동할 수도 있다. 이러한 홈 디바이스(50)는 또 다른 홈 디바이스로 컨텐츠를 전송할 수도 있다.

[0065] 한편, 디바이스, 예컨대 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)는 서비스 제공자(20) 또는 특정 서버로부터 보안 솔루션을 위한 DRM 코드, 보안 메시지, 어플리케이션 등을 다운로드 또는 수신할 때 이를 인증하기 위한 보안 솔루션 인증 프로세스를 수행할 수 있다. 보안 솔루션 인증 프로세스는 보안 솔루션의 보안 기능 수행 시 신뢰성에 영향을 미친다. 즉, 보안 솔루션 인증 프로세스가 엄격할 수록 보안 솔루션의 신뢰성은 높아진다. 이러한 보안 솔루션 인증 프로세스의 보안 수준을 나타내는 정보로서 보안 솔루션 레벨의 개념을 도입할 수 있다.

[0066] 보안 솔루션 레벨은 디바이스의 보안 특성을 미리 정해진 기준에 따라 등급화한(Classify) 정보를 의미할 수 있다. 상기 보안 솔루션 레벨은 디바이스의 보안 솔루션 프로파일일 수 있다. 디바이스는 그 디바이스의 보안 솔루션 인증 프로세스의 보안 수준에 따라 지정되는 보안 솔루션 레벨과 연계될 수 있다. 상기 미리 정해진 기준이란 보안 솔루션 레벨 테이블일 수 있다.

[0067] 도 4는 디바이스의 보안 솔루션 레벨을 지정하는 기준이 되는 보안 솔루션 레벨 테이블을 나타내는 예시도이다.

[0068] 도 4에 도시된 바와 같이, 보안 솔루션 레벨 테이블(SSLT)은 예시적으로 5개의 등급의 보안 솔루션 레벨을 정의할 수 있다.

[0069] 레벨 0은 비보안 수행 환경(Non-Secured Execution Environment)에서 보안 솔루션 인증 프로세스의 인증(Authentication) 및 무결성(Integrity) 체크를 수행하지 않는 보안 수준을 의미할 수 있다. 보안 솔루션 레벨이 레벨 0인 디바이스는 보안 솔루션 인증 프로세스를 인증하지 않고 보안 솔루션 인증 프로세스를 개시(Initiats)한다. 따라서 디바이스의 보안 솔루션 레벨이 레벨 0라면 그 디바이스는 보안이 상당히 취약한 디바이스라 할 수 있다. 레벨 0은 정의된 보안 솔루션 레벨 중 가장 신뢰도가 낮은 레벨이다.

[0070] 레벨 1은 비보안 수행 환경에서 디바이스의 소프트웨어 엘리먼트(Element)를 사용하여 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 수준의 보안 솔루션 레벨을 의미할 수 있다. 레벨 1에서의 보안 솔루션 인증 프로세스는 디바이스의 소프트웨어 엘리먼트에 의하여 인증된 후 개시될 수 있다. 이러한 레벨 1은 앞서 언급한 레벨 0보다는 보안성 높다고 할 수 있다.

[0071] 레벨 2는 비보안 수행 환경에서 디바이스의 하드웨어 엘리먼트를 사용하여 직접적으로 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 레벨을 의미할 수 있다. 레벨 2에서의 보안 솔루션 인증 프로세스는 디바이스의 하드웨어 엘리먼트에 의하여 인증된 후 개시될 수 있다. 이러한 레벨 2는 앞서 언급한 레벨 1보다는 보안성 높다고 할 수 있다.

[0072] 레벨 3은 보안 수행 환경(Secured Execution Environment)에서 디바이스의 소프트웨어 엘리먼트를 사용하여 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 보안 솔루션 레벨을 의미할 수 있다. 레벨 3에서의 보안 솔루션 인증 프로세스는 보안 수행 환경 하에서 디바이스의 소프트웨어 엘리먼트에 의하여 인증된 후 개시될 수 있다. 이러한 레벨 3은 앞서 언급한 레벨 2보다는 보안성 높다고 할 수 있다.

[0073] 레벨 4는 보안 수행 환경에서 디바이스의 하드웨어 엘리먼트를 사용하여 직접적으로 보안 솔루션 인증 프로세스의 인증 및 무결성 체크를 검증하는 보안 솔루션 레벨을 의미할 수 있다. 레벨 4에서의 보안 솔루션 인증 프로세스는 보안 수행 환경 하에서 디바이스의 하드웨어 엘리먼트에 의하여 인증된 후 개시될 수 있다. 이러한 레벨 4는 앞서 언급한 레벨 3보다 보안성 높으며, 정의된 보안 솔루션 레벨 등급 중 가장 신뢰도가 높다고 할 수 있다.

[0074] 디바이스, 예컨대 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)는 해당 디바이스의 보안 수준에 따라 상술한 기준에 해당하는 보안 솔루션 레벨을 가질 수 있다. 이러한 보안 솔루션 레벨은 디바이스의 인증서 내의 특정 필드에 삽입됨으로써, 해당 디바이스와 연계될 수 있다. 즉 디바이스의 인증서는 그 디바이스의 보안 솔루션 레벨을 포함할 수 있다.

[0075] 디바이스는 자신 또는 컨텐츠를 공유하고자 하는 디바이스(즉 타겟 디바이스)의 보안 솔루션 레벨에 근거하여 컨텐츠의 사용 또는 전송을 제한할 수도 있다. 예를 들어, 컨텐츠의 사용 또는 공유 시에 요구되는 보안 수준을 자신 또는 타겟 디바이스의 보안 수준(즉, 해당 디바이스의 보안 솔루션 레벨) 만족하지 못할 경우 컨텐츠의 사용 또는 공유를 제한할 수도 있다. 컨텐츠에서 요구되는 보안 수준과 관련한 정보는 컨텐츠와 연계된 보안 정보에 포함될 수 있다. 상기 컨텐츠와 연계된 보안 정보는 해당 컨텐츠의 사용 또는 공유 시에 요구되는 보안 솔루션 레벨을 나타내는 정보를 포함할 수 있다.

[0076] 도 5는 본 발명의 바람직한 실시예에 따른 컨텐츠 저장 방법의 절차를 설명하기 위한 예시도로서, IPTV 수신 디바이스(40)가 서비스 제공자(20)로부터 컨텐츠를 수신하여 저장하는 절차를 보여주고 있다.

[0077] 도 5에 도시된 바와 같이, IPTV 수신 디바이스(40)는 서비스 보호 솔루션(44) 및 컨텐츠 보호 솔루션(45)을 구비한다. 먼저, 사용자는 컨텐츠를 시청하기 위하여 IPTV 수신 디바이스(40)에 컨텐츠의 다운로드 및 저장을 요청할 수 있다. IPTV 수신 디바이스(40)는 이에 응답하여 서비스 제공자(20)에게 해당 컨텐츠를 전송해줄 것을 요청한다(단계:S1). 한편 사용자가 다른 디바이스(예컨대 홈 디바이스, 또는 제 3의 단말기)를 통하여 IPTV 수신 디바이스(40)로의 컨텐츠 전송을 요청할 수도 있다.

[0078] 서비스 제공자(20)는 서비스 제공자(20)의 서비스 보호 솔루션을 사용하여 컨텐츠를 보호한 뒤 IPTV 수신 디바이스(40)로 그 보호된 컨텐츠를 전송한다. 예를 들어, 서비스 제공자(20)는 컨텐츠를 상기 서비스 보호 솔루션을 사용하여 스크램블링하고, 스크램블링된 컨텐츠 및 그 컨텐츠와 연계된 유시지 권한 정보 등을 IPTV 수신 디바이스(40)로 전송할 수 있다.

[0079] IPTV 수신 디바이스(40)는 IPTV 수신 디바이스(40)에 구비된 서비스 보호 솔루션(44)을 이용하여 서비스 제공자(20)로부터 전송되는 컨텐츠를 다운로드한다(단계:S2). 다운로드 시에 IPTV 수신 디바이스(40)의 서비스 보호 솔루션(44)은 서비스 제공자(20)로부터 수신되는 스크램블링된 컨텐츠를 내부에서 처리할 수 있는 형태의 컨텐츠, 예컨대 클린 타입의 컨텐츠로 변환할 수 있다.

[0080] 이어서 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45)은 다운로드된 컨텐츠를 컨텐츠 재생기를 지원하는 컨텐츠 보호 솔루션(45)에 부합되도록 변환하고, 변환한 컨텐츠를 스토리지에 저장할 수 있다(단계:S3). 또한 상기 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45)은 상기 컨텐츠와 연계된 유시지 권한 정보 등을 상기 컨텐츠 보호 솔루션(45)에 부합되는 형태로 변환하여 저장할 수 있다. 한편 컨텐츠의 사용 시에는 IPTV 수신 디바

이스(40)의 보안 솔루션 레벨에 따라 컨텐츠의 사용을 제한될 수도 있다.

[0081] 이상 설명한 바와 같이, IPTV 수신 디바이스(40)는 IPTV 수신 디바이스(40)에 구비된 서비스 보호 솔루션(44)을 이용하여 서비스 제공자(20)로부터 전송되는 컨텐츠를 다운로드하고, 컨텐츠 보호 솔루션(45)을 이용하여 컨텐츠를 IPTV 수신 디바이스(40)에서 보안 재생 가능한 형태로 변환할 수 있다.

[0082] 한편, 도시되지는 않았지만, 컨텐츠 저장 방법의 다른 실시예로 서비스 제공자(20)가 IPTV 수신 디바이스(40)에 구비된 컨텐츠 보호 솔루션(45)에 부합되도록 컨텐츠를 보호하여 IPTV 수신 디바이스(40)로 컨텐츠를 전송할 수도 있다. 예를 들어, IPTV 수신 디바이스(40)가 컨텐츠의 전송을 요청하면, 서비스 제공자(20)는 IPTV 수신 디바이스(40)에서 지원하는 컨텐츠 보호 솔루션(45)과 호환 가능하도록(Compitible) 컨텐츠 보호 테크닉을 사용하여 컨텐츠를 보호하고 이를 IPTV 수신 디바이스(40)로 전송한다. 그러면 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45)은 이를 수신하여 저장할 수 있다.

[0083] 서비스 제공자(20)는 IPTV 수신 디바이스(40)가 도메인에 등록 할 때, 또는 서비스 제공자(20)의 요청에 따라 IPTV 수신 디바이스(40)로부터 IPTV 수신 디바이스(40)의 보안 커패빌리티 정보를 수신하여 저장 및 관리함으로써, IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45)을 파악할 수 있다. 상기 보안 커패빌리티 정보는 앞서도 언급했듯이, IPTV 수신 디바이스(40)에 구비된 보안 솔루션의 정보, 보안 솔루션 레벨 등을 포함할 수 있다. 상기 보안 솔루션의 정보, 보안 솔루션 레벨 등은 IPTV 수신 디바이스(40)의 인증서에 포함될 수도 있다.

[0084] 도 6은 본 발명의 바람직한 실시예에 따른 컨텐츠 공유 방법을 실현하기 위한 시스템 구성을 도시하는 블록도이다. 또한, 도 7은 본 발명의 바람직한 실시예에 따른 컨텐츠 공유 방법을 설명하기 위한 흐름도로서, 서비스 제공자(20)로부터 다운로드한 컨텐츠를 홈 디바이스(50)로 재분배함으로써 컨텐츠를 공유하는 절차를 보여주고 있다.

[0085] 도 6에 도시된 바와 같이, 서비스 제공자(20)는 서비스 보호 테크닉을 사용하여 컨텐츠를 전송하며, IPTV 수신 디바이스(40)는 서비스 보호 솔루션(44) 및 컨텐츠 보호 솔루션 'A'(45a)를 구비한다. 또한 IPTV 수신 디바이스(40)와 컨텐츠를 공유할 홈 디바이스(50)는 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션(45a)과 동일한 컨텐츠 보호 솔루션 'A'를 구비한다. 즉 홈 디바이스는(50)는 IPTV 수신 디바이스(40)와 동일한 컨텐츠 보호 솔루션을 지원한다.

[0086] 도 6 내지 도 7을 참조하면, 먼저, 사용자는 원하는 컨텐츠를 홈 디바이스(50)로 다운로드받아 시청하기 위하여 홈 디바이스(50) 또는 디스커버리 프로세스를 통하여 홈 디바이스(50)를 발견(Discover)할 수 있는 IPTV 수신 디바이스(40), 또는 제 3의 디바이스를 이용하여 컨텐츠를 홈 디바이스(50)로 다운로드할 것을 요청할 수 있다. 그러면 해당 디바이스는 서비스 제공자(20)에게 사용자에 의해 요청된 컨텐츠를 전송할 것을 요청한다(단계:S11).

[0087] 서비스 제공자(20)는 상기 요청에 응답하여 서비스 제공자(20)의 서비스 보호 솔루션을 사용하여 상기 컨텐츠를 스크램블링하고, 스크램블링된 컨텐츠 및 그 컨텐츠의 사용에 필요한 정보들, 예컨대 유시지 권한 정보, 보안 정보, 리보케이션 리스트 정보 등을 IPTV 수신 디바이스(40)로 전송한다. 이에 따라 서비스 보호 테크닉에 의하여 보호되는 컨텐츠가 IPTV 수신 디바이스(40)로 전송된다.

[0088] IPTV 수신 디바이스(40)는 IPTV 수신 디바이스(40)에 구비된 서비스 보호 솔루션(44)을 이용하여 서비스 제공자(20)로부터 컨텐츠를 수신하여 처리할 수 있다(단계:S12). 예컨대 서비스 보호 솔루션(44)은 수신되는 스크램블링된 컨텐츠를 서비스 보호 테크닉에 따라 클린 타입의 컨텐츠로 변환할 수 있다. 또한 컨텐츠의 사용에 필요한 정보들을 IPTV 수신 디바이스(40)의 내부에서 사용 가능한 형태로 변환할 수도 있다.

[0089] 이어서 IPTV 수신 디바이스(40)는 컨텐츠를 전송하고자 하는 홈 디바이스(50)에 구비된 컨텐츠 보호 솔루션을 검출(detecting)한다(단계:S13). 이때 홈 디바이스(50)에서 지원하는 컨텐츠 보호 솔루션과 IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션이 동일할 경우(본 실시예에서는 홈 디바이스(50) 및 IPTV 수신 디바이스(40)가 동일한 컨텐츠 보호 기술을 지원하는 컨텐츠 보호 솔루션 'A'(44a 및 55a)를 각각 구비함), IPTV 수신 디바이스(40)의 컨텐츠 보호 솔루션 'A'(45a)는 상기 컨텐츠를 컨텐츠 보호 솔루션 'A'(45a)에 적합한 형태로 변환(Convert)한다(단계:S14). 예를 들어, 컨텐츠 보호 솔루션 'A'(45a)는 컨텐츠를 약속된 형태로 암호화하고, 컨텐츠의 유시지 권한 등을 컨텐츠 보호 솔루션 'A'(45a)에 적합한 형태로 번역(Translates)한다.

[0090] 다음으로, IPTV 수신 디바이스(40)는 변환된 컨텐츠 및 그 컨텐츠를 사용하는데 필요한 정보들을 컨텐츠 보호 솔루션 'A'(45a)에서 지원되는 기술을 사용하여 홈 디바이스(50)로 전송함으로써 컨텐츠를 재분배한다(단계:S15). 이때 IPTV 수신 디바이스(40)는 컨텐츠의 유시지 권한에 의하여 컨텐츠의 전송을 제한할 수 있다. 즉

컨텐츠의 공유는 해당 컨텐츠와 연계된 유시지 권한에서 허용하는 범위 내에서 수행될 수 있다.

[0091] 또한 IPTV 수신 디바이스(40)는 홈 디바이스(50) 또는 IPTV 수신 디바이스(40)의 보안 솔루션 레벨에 근거하여 컨텐츠의 공유를 제한할 수도 있다. 예를 들어, IPTV 수신 디바이스(40)는 컨텐츠의 공유 시에 요구되는 보안 수준을 IPTV 수신 디바이스(40) 또는 홈 디바이스(50)의 보안 수준(즉, 해당 디바이스의 보안 솔루션 레벨) 만족하지 못할 경우 컨텐츠의 공유를 제한할 수도 있다. 이때 IPTV 수신 디바이스(40)의 보안 솔루션 레벨 및 홈 디바이스(50)의 보안 솔루션 레벨은 각각 IPTV 수신 디바이스(40)의 인증서 및 홈 디바이스(50)의 인증서 내에서 포함되며, 컨텐츠의 공유 시 요구되는 보안 수준은 컨텐츠와 연계된 보안 정보에 포함될 수 있다. IPTV 수신 디바이스(40)는 자신의 보안 솔루션 레벨을 확인하기 위하여 자신의 인증서를 검사할 수 있으며, 홈 디바이스(50)의 보안 솔루션 레벨을 확인하기 위하여 홈 디바이스(50)에 인증서를 요청하거나 별도로 보안 솔루션 레벨의 정보를 요청할 수도 있다.

[0092] 다른 한편으로, IPTV 수신 디바이스(40)는 상기 홈 디바이스(50)와의 인증을 수행하여, 상기 홈 디바이스(50)가 IPTV 수신 디바이스(40)와 동일한 도메인에 등록된 도메인 디바이스인지를 확인할 수도 있다. 만약 홈 디바이스(50)가 IPTV 수신 디바이스(40)와 동일한 도메인에 속하지 않았다면 IPTV 수신 디바이스(40)는 홈 디바이스(50)로의 컨텐츠 공유를 제한할 수도 있다.

[0093] IPTV 수신 디바이스(40)로부터 홈 디바이스(50)로 컨텐츠 및 그 컨텐츠를 사용하는데 필요한 정보들이 전송되면, 홈 디바이스(50)의 컨텐츠 보호 솔루션 'A'(55a)는 이를 수신하여 저장하고 재생할 수 있다. 재생 시 홈 디바이스(50)의 컨텐츠 보호 솔루션 'A'(55a)는, 컨텐츠의 유시지 권한 정보에서 허용하는 범위 내에서, 컨텐츠를 재생할 수 있도록 컨텐츠의 암호화를 해제하여 컨텐츠 재생기(미도시)로 제공할 수 있다.

[0094] 한편, 도 6에 점선으로 표시된 바와 같이, 서비스 제공자(20)와 컨텐츠 보호 솔루션 'A'(45a)가 직접 연동할 수도 있다. 예를 들면, 서비스 제공자(20)는 IPTV 수신 디바이스(40)에 구비된 컨텐츠 보호 솔루션 'A'(45a)에 부합되는 컨텐츠 보호 기술을 사용하여 컨텐츠를 보호하고, 이를 IPTV 수신 디바이스(40)로 전송할 수 있다. 이 경우 IPTV 수신 디바이스(40)는, 별도의 서비스 보호 솔루션(44)의 동작 없이, 서비스 제공자(20)로부터 컨텐츠 보호 솔루션 'A'(45a)에 의해 보호된 컨텐츠를 다운로드하여 홈 디바이스(50)로 재분배할 수도 있다.

[0095] 도 8은 본 발명의 바람직한 다른 실시예에 따른 컨텐츠 공유 방법을 실현하기 위한 시스템 구성을 도시하는 블록도이다. 또한, 도 9는 본 발명의 바람직한 다른 실시예에 따른 컨텐츠 공유 방법을 설명하기 위한 흐름도로서, 서비스 제공자(60)로부터 다운로드한 컨텐츠를 홈 디바이스(80)로 재분배함으로써 컨텐츠를 공유하는 절차를 보여주고 있다.

[0096] 도 8에 도시된 바와 같이, 서비스 제공자(60)는 컨텐츠 보호 테크닉에 따라 컨텐츠를 전송하며, IPTV 수신 디바이스(70)는 컨텐츠 보호 솔루션 'A'(75a)를 구비한다. 또한 IPTV 수신 디바이스(70)와 컨텐츠를 공유할 홈 디바이스(80)는 IPTV 수신 디바이스(70)의 컨텐츠 보호 솔루션 'A'(75a)와는 다른 종류의 컨텐츠 보호 기술을 지원하는 컨텐츠 보호 솔루션 'B'(85b)를 구비한다.

[0097] 도 8 내지 도 9를 참조하면, 먼저 사용자는 원하는 컨텐츠를 홈 디바이스(80)로 다운로드받아 시청하기 위하여 홈 디바이스(80) 또는 디스커버리 프로세스를 통하여 홈 디바이스(80)를 발견(Discover)할 수 있는 IPTV 수신 디바이스(70), 또는 제 3의 디바이스를 이용하여 컨텐츠를 홈 디바이스(80)로 다운로드할 것을 요청할 수 있다. 그러면 해당 디바이스는 서비스 제공자(60)에게 사용자에 의해 요청된 컨텐츠를 전송할 것을 요청한다(단계:S21).

[0098] 서비스 제공자(60)는 상기 요청에 응답하여 서비스 제공자(60)의 컨텐츠 보호 솔루션 'A'를 사용하여 상기 컨텐츠를 암호화하고, 암호화된 컨텐츠 및 그 컨텐츠의 사용에 필요한 정보들, 예컨대 유시지 권한 정보, 보안 정보, 리보케이션 리스트 정보 등을 IPTV 수신 디바이스(70)로 전송한다. 이에 따라 컨텐츠 보호 테크닉에 의하여 보호되는 컨텐츠가 IPTV 수신 디바이스(70)로 전송된다.

[0099] IPTV 수신 디바이스(70)는 컨텐츠 보호 솔루션 'A'(75a)를 이용하여 서비스 제공자(60)로부터 컨텐츠를 수신할 수 있다(단계:S22). 또한 컨텐츠 보호 솔루션 'A'(75a)는 수신되는 암호화된 컨텐츠를 다른 컨텐츠 보호 솔루션으로 변환할 수 있게 하기 위하여 클린 타입의 컨텐츠로 변환할 수도 있다. 또한 컨텐츠의 사용에 필요한 정보들을 IPTV 수신 디바이스(70)의 내부에서 사용 가능한 형태로 변환할 수도 있다.

[0100] 이어서 IPTV 수신 디바이스(70)는 컨텐츠를 전송하고자 하는 홈 디바이스(80)에 구비된 컨텐츠 보호 솔루션을 검출(detecting)한다(단계:S23). 이때 홈 디바이스(80)에서 지원하는 컨텐츠 보호 솔루션과 IPTV 수신 디바이스(70)의 컨텐츠 보호 솔루션이 서로 다를 경우(본 실시예에서는 홈 디바이스(80) 및 IPTV 수신 디바이스(70)가

서로 다른 컨텐츠 보호 기술을 지원하는 예를 듬), IPTV 수신 디바이스(70)는 상기 컨텐츠를 컨텐츠 보호 솔루션 'B'(85b)에 적합한 형태로 변환(Convert)한다(단계:S24). 예를 들어, IPTV 수신 디바이스(70)는 컨텐츠를 약속된 형태로 암호화하고, 컨텐츠의 유시지 권한 등을 컨텐츠 보호 솔루션 'B'(85b)에 적합한 형태로 번역(Translates)한다.

[0101] 이러한 처리를 위하여 IPTV 수신 디바이스(70)는 DRM 상호 호환 솔루션을 구비하거나, 컨텐츠 보호 솔루션 'B'를 구비할 수 있다. 만약 상기 솔루션들을 구비하지 않았을 경우, IPTV 수신 디바이스(70)는 서비스 제공자(60), DRM 서버, 홈 디바이스(80) 등에 요청하여 해당 솔루션을 다운로드 받을 수 있다.

[0102] 다음으로, IPTV 수신 디바이스(70)는 변환된 컨텐츠 및 그 컨텐츠를 사용하는데 필요한 정보들을 상호 호환 재분배(Interoperable Redistribution) 기술 또는 서비스 보호 솔루션 'B'에서 지원되는 기술을 사용하여 홈 디바이스(80)로 전송함으로써 컨텐츠를 재분배한다(단계:S25). 이때 IPTV 수신 디바이스(70)는 컨텐츠의 유시지 권한에 의하여 홈 디바이스(80)로의 컨텐츠 전송을 제한할 수 있다. 즉 컨텐츠의 공유는 해당 컨텐츠와 연계된 유시지 권한에서 허용하는 범위 내에서 수행될 수 있다.

[0103] 또한 IPTV 수신 디바이스(70)는 홈 디바이스(80) 또는 IPTV 수신 디바이스(70)의 보안 솔루션 레벨에 근거하여 컨텐츠의 공유를 제한할 수도 있다. 예를 들어, IPTV 수신 디바이스(70)는 컨텐츠의 공유 시에 요구되는 보안 수준을 IPTV 수신 디바이스(70) 또는 홈 디바이스(80)의 보안 수준(즉, 해당 디바이스의 보안 솔루션 레벨) 만족하지 못할 경우 컨텐츠의 공유를 제한할 수도 있다.

[0104] 이때 IPTV 수신 디바이스(70)의 보안 솔루션 레벨 및 홈 디바이스(80)의 보안 솔루션 레벨은 각각 IPTV 수신 디바이스(70)의 인증서 및 홈 디바이스(80)의 인증서 내에서 포함되며, 컨텐츠의 공유 시 요구되는 보안 수준은 컨텐츠와 연계된 보안 정보에 포함될 수 있다. IPTV 수신 디바이스(70)는 IPTV 수신 디바이스(70)의 보안 솔루션 레벨을 확인하기 위하여 자신의 인증서를 검사할 수 있으며, 홈 디바이스(80)의 보안 솔루션 레벨을 확인하기 위하여 홈 디바이스(80)에 인증서를 요청하거나 별도로 보안 솔루션 레벨의 정보를 요청할 수도 있다.

[0105] 또한 IPTV 수신 디바이스(70)는 상기 홈 디바이스(80)와의 인증을 수행하여, 상기 홈 디바이스(80)가 IPTV 수신 디바이스(70)와 동일한 도메인에 등록된 도메인 디바이스인지를 확인할 수도 있다. 만약 홈 디바이스(80)가 IPTV 수신 디바이스(70)와 동일한 도메인에 속하지 않았다면 IPTV 수신 디바이스(70)는 홈 디바이스(80)로의 컨텐츠 공유를 제한할 수도 있다.

[0106] IPTV 수신 디바이스(70)로부터 홈 디바이스(80)로 컨텐츠 및 그 컨텐츠를 사용하는데 필요한 정보(예컨대 권한 정보 등)들이 전송되면, 홈 디바이스(80)의 컨텐츠 보호 솔루션 'B'(85b)는 이를 수신하여 저장하고 재생할 수 있다. 재생 시 홈 디바이스(80)의 컨텐츠 보호 솔루션 'B'는, 컨텐츠의 유시지 권한 정보에서 허용하는 범위 내에서, 컨텐츠를 재생할 수 있도록 컨텐츠의 암호화를 해제하여 컨텐츠 재생기로 제공할 수 있다.

[0107] 한편, 도 8에 점선으로 표시된 바와 같이, 컨텐츠의 권한 정보를 제공하기 위하여 서비스 제공자(60)와 홈 디바이스(80)가 직접 연동할 수도 있다. 예를 들면, IPTV 수신 디바이스(70)는 컨텐츠를 홈 디바이스(80)로 전송하고, 그 컨텐츠를 사용하는데 요구되는 권한 정보는 홈 디바이스(80)가 직접 서비스 제공자(60)로부터 수신할 수도 있다.

[0108] 이하, 서비스 제공자 간의 컨텐츠 연동 보안 서비스 모델을 설명한다. 서비스 제공자간의 컨텐츠 연동 서비스란 사용자가 한번의 과금으로 2개 이상의 서비스 제공자가 제공하는 컨텐츠를 사용할 수 있는 서비스를 의미할 수 있다. 이하에서 개시할 내용은 이러한 서비스에 안정성을 보안 제공하는 구조를 제공할 수 있다.

[0109] 도 10은 서비스 제공자 간의 컨텐츠 연동 서비스의 개념을 설명하기 위한 예시도이다.

[0110] 도 10에 도시된 바와 같이, 서비스 제공자 1은 서비스 A 및 서비스 B를 제공하고, 서비스 제공자 2는 서비스 C 및 서비스 D를 제공한다고 가정하면, 종래의 경우 사용자는 서비스 제공자 1 및 서비스 제공자 2가 각각 제공하는 서비스 A 및 서비스 C 형태의 서비스를 각 서비스 제공자를 통해서 과금하고 이용할 수 있다. 그러나, 본 발명에서는 단일 과금으로 '서비스 A - 서비스 C'를 자유롭게 이용하는 새로운 개념의 서비스를 제공할 수 있다.

[0111] 도 11은 서비스 제공자 간의 컨텐츠 연동 서비스를 위한 시스템 구조를 나타내는 예시도이다. 또한, 도 12는 서비스 제공자 간의 컨텐츠 연동 서비스의 절차를 설명하기 위한 예시도이다.

[0112] 도 11 내지 도 12를 참조하면, 서비스 제공자 1과 서비스 제공자 2는 각각의 서비스를 위한 도메인을 형성할 수 있다. 이때, 서비스 제공자 간의 컨텐츠 연동 서비스를 위하여 컨텐츠 DRM 상호 호환 매니저(Content DRM Interoperability Manager), 도메인 매니저(Domain Manager) 및 인증서 허가 서버(Certificate Authority) 등

을 구비할 수 있다.

[0113] 컨텐츠 DRM 상호 호환 매니저는 서비스 사업자 간 상이한 DRM으로 보호되는 컨텐츠를 호환시키기 위하여 정보를 제공하는 서버를 의미할 수 있다. 도메인 매니저는 사용자가 제공받기 원하는 서비스 사업자 간 상이한 서비스들을 묶어 서비스 통합 도메인을 제공하는 서비스 도메인 기능 및 사용자가 보유한 단말들이 서비스 도메인에 속한 서비스들을 이용할 수 있도록 묶어주는 사용자/디바이스 도메인 기능을 제공할 수 있다. 인증서 허가 서버는 컨텐츠 연동 서비스와 관련한 서버, 사용자, 사용자 장치들의 인증서를 관리하는 서버를 의미할 수 있다.

[0114] 도 12에 도시된 바와 같이, 서비스 제공자 간의 컨텐츠 연동 서비스는 먼저, 인증서 발급 단계(단계:S31)를 거친다. 인증서 허가 서버 인증서 발급 단계(단계:S31)에서는 표준화(예컨대 X.509 v3 등)된 인증서 허가 서버가 서비스를 위한 인증서(Certificate a)를 발급하여 도메인 매니저, 서비스 제공자, 디바이스A(Device a)로 전달할 수 있다.

[0115] 컨텐츠 연동 서비스 가입 단계(단계:S32)는, 사용자가 디바이스A를 통하여 컨텐츠 연동 서비스를 제공받기 위하여, 디바이스A가 도메인 매니저에게 서비스 가입을 요청하는 단계를 의미할 수 있다.

[0116] 디바이스A로부터 요청 메시지를 수신하는 도메인 매니저 내의 서비스 도메인 구성자는 사용자가 요청하는 서비스를 하나의 가상 도메인으로 묶고 해당 가상 도메인에 속하는 컨텐츠를 보호하기 위한 도메인 키 A(Domain key a)를 생성할 수 있다. 또한 도메인 매니저의 사용자 도메인 구성자는 사용자가 보유한 디바이스들(예컨대 디바이스 A를 포함한 다수의 사용자 디바이스)을 또 다른 가상 도메인으로 묶어 서비스 가상 도메인에 속한 컨텐츠들을 이용할수 있는 환경을 구성할 수 있다.

[0117] 다음으로 도메인 정보 제공 단계(단계:S33)가 수행될 수 있다. 도메인 정보 제공 단계(단계:S33)에서는 앞선 컨텐츠 연동 서비스 가입 단계(단계:S32)를 통하여 생성된 도메인 키 A(Domain key a)와 서비스 도메인 정보, 사용자 도메인 정보를 제공하고, 도메인 키 A(Domain key a)의 생성 정보는 서비스 도메인에 속한 서비스 제공자와 공유한다.

[0118] 컨텐츠 다운로드 단계(단계:S34)에서는, 서비스 가입 후, 사용자는 사용자 도메인에 속한 디바이스A로 서비스 도메인에 속한 서비스 제공자로부터 컨텐츠를 다운로드한다. 다운로드되는 컨텐츠는 기본적으로 각 서비스 제공자가 정한 DRM으로 보호되어 있으며, DRM으로 보호된 컨텐츠는 도메인 키 A(Domain key a)로 다시한번 보호되어서 사용자 장치로 전달된다.

[0119] 사용자가 생성한 서비스 도메인에 속한 컨텐츠들은 서비스 제공자가 상이하더라도 동일한 도메인 키 A(Domain key a)로 보호될 수 있다. 보호되는 형태는 DRM에서 사용되는 컨텐츠 암호화 키(CEK : Content Encrytion Key)를 도메인 키 A(Domain key a)로 암호화하여 각 DRM의 라이선스(License) 파일에 저장하는 형태와, 각 DRM의 라이선스 파일을 도메인 키 A(Domain key a)로 암호화하여 사용자에게 전달하는 방법이 있을 수 있다.

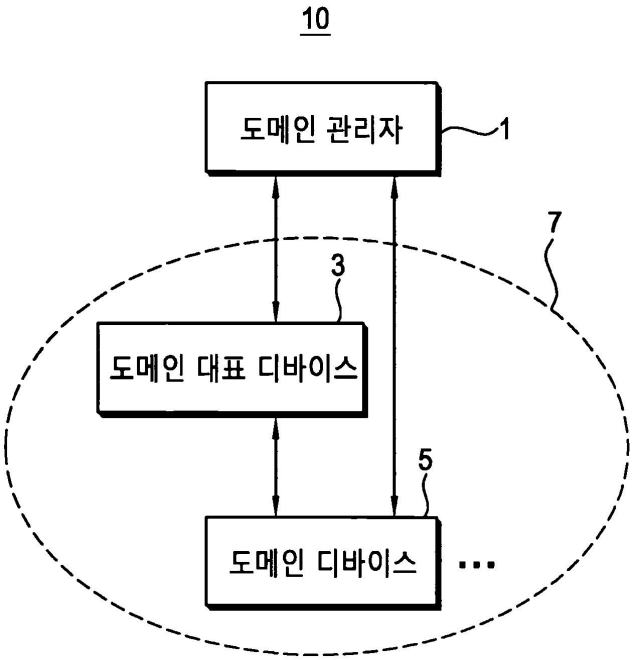
[0120] 다음으로, 컨텐츠 실행 및 변환 단계(단계:S35)가 수행될 수 있다. 컨텐츠 실행 및 변환 단계(단계:S35)는 실제 사용자가 소유한 디바이스에서 상기 컨텐츠 다운로드 단계(단계:S34)에서 다운로드된 컨텐츠를 실행하는 단계로서, 디바이스A가 상기 컨텐츠 연동 서비스 가입 단계(단계:S32)에서 취득한 도메인 키 A(Domain key a)와 다운로드된 컨텐츠를 보호하는 DRM의 언패키징 에이전트(Unpacking Agent)를 보유하고 있으면 컨텐츠를 실행할 수 있다.

[0121] 만약, 디바이스A가 상기 DRM 언패키징 에이전트를 보유하고 있지 않을 경우, DRM 컨버터(Converter)를 통한 DRM 변환을 수행함으로써 컨텐츠의 사용이 가능해질 수 있다. 그러나 이때 변환이 성공적으로 수행되더라도 도메인 키 A(Domain key a)가 없으면 컨텐츠의 사용은 불가능하다.

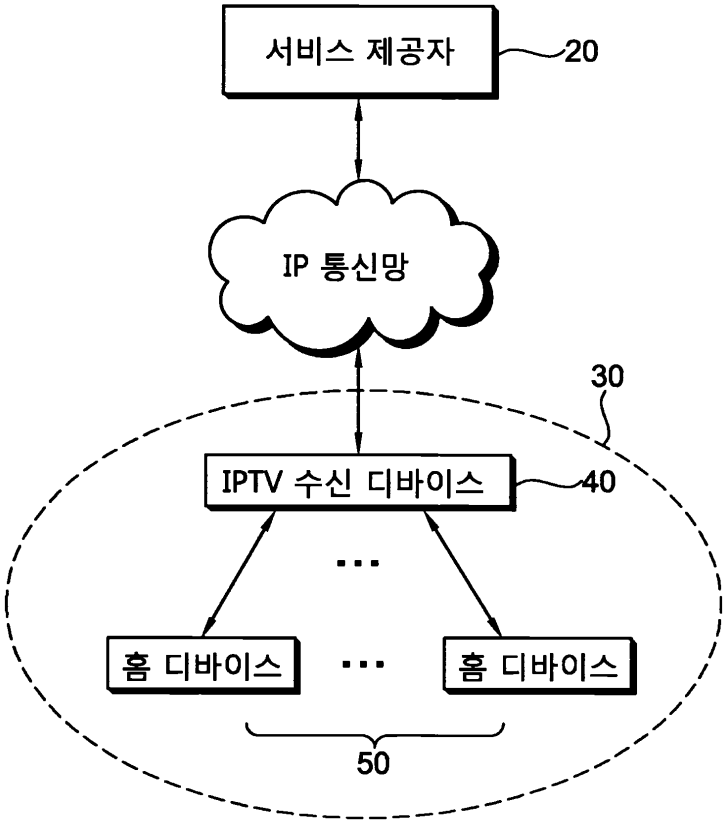
[0122] 이상 본 발명에 대하여 그 바람직한 실시예들을 도면을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 기술적 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시켜 실시할 수 있음을 이해할 수 있을 것이다. 따라서, 본 발명의 앞으로의 실시예들의 변경은 본 발명의 기술을 벗어날 수 없을 것이다.

도면

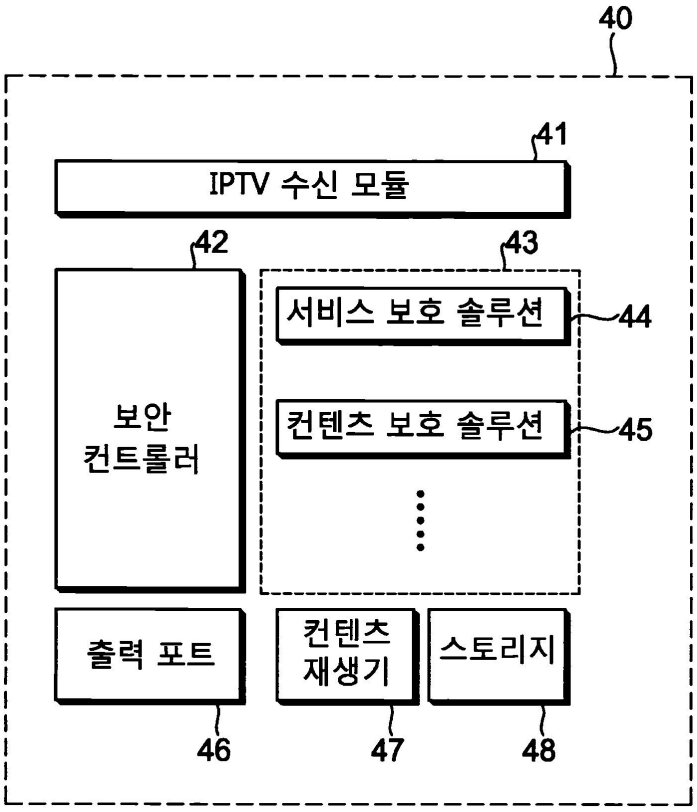
도면1


10
도메인 관리자
1
7
3
도메인 대표 디바이스
5
도메인 디바이스

도면2


서비스 제공자
20
IP 통신망
30
IPTV 수신 디바이스
40
홈 디바이스
홈 디바이스
50

도면3

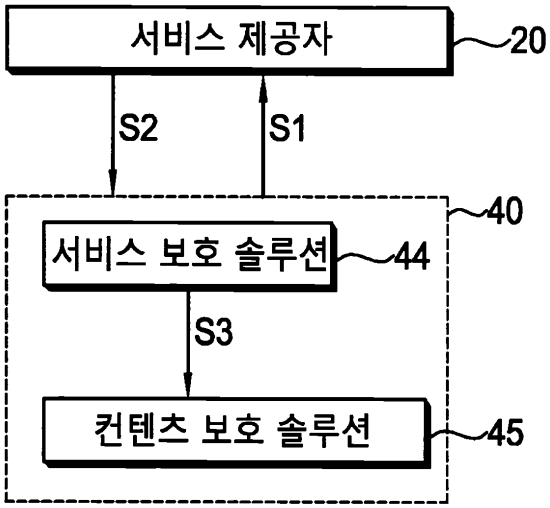

40
41
IPTV 수신 모듈
42
43
서비스 보호 솔루션
44
보안
컨트롤러
컨텐츠 보호 솔루션
45
출력 포트
컨텐츠
재생기
스토리지
46
47
48

도면4

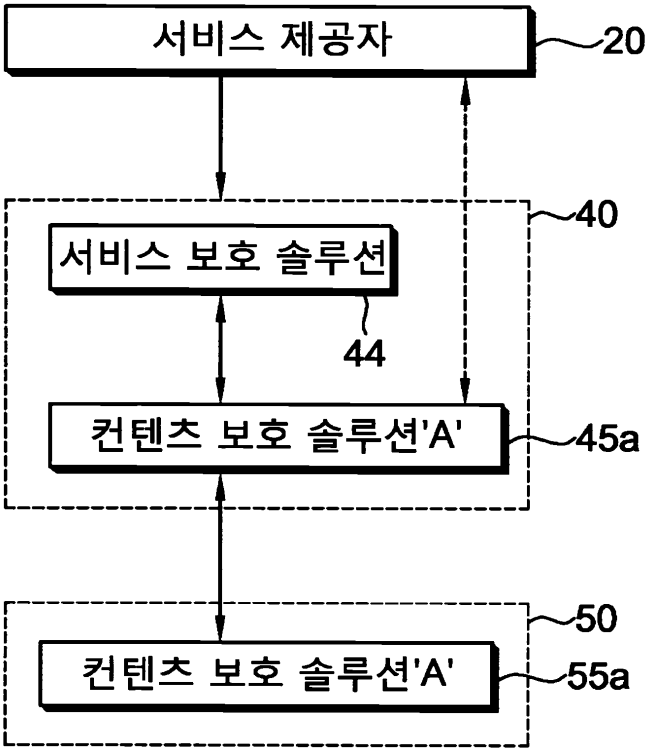
SSLT

SSL	Exeution environent	Definition
0	Non-Secured	-No Authentication and no integrity check
1	Non-Secured	-Authentication and integrity are verified by software
2	Non-Secured	-Authentication and integrity are verified by hardware
3	Secured	-Authentication and integrity are verified by software
4	Secured	-Authentication and integrity are verified by hardware

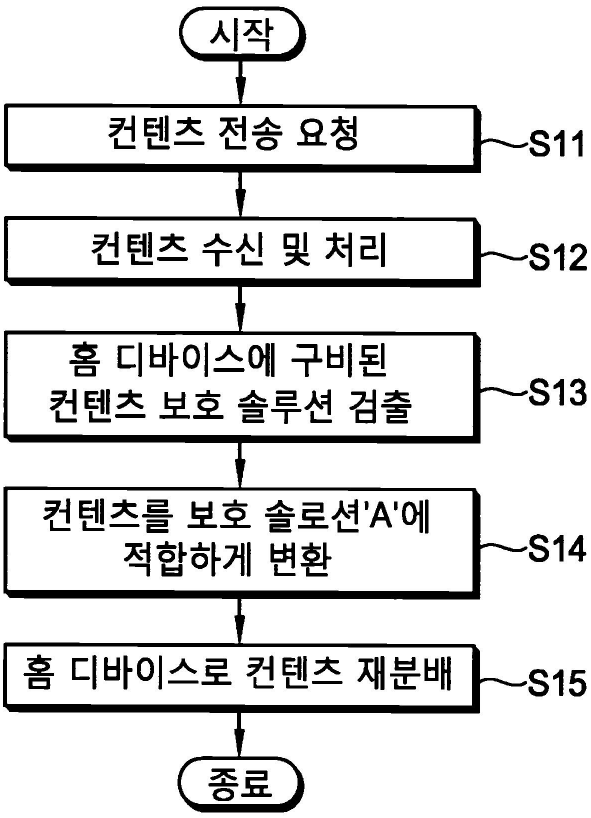
도면5


서비스 제공자
20
S2
S1
40
서비스 보호 솔루션
44
S3
컨텐츠 보호 솔루션
45

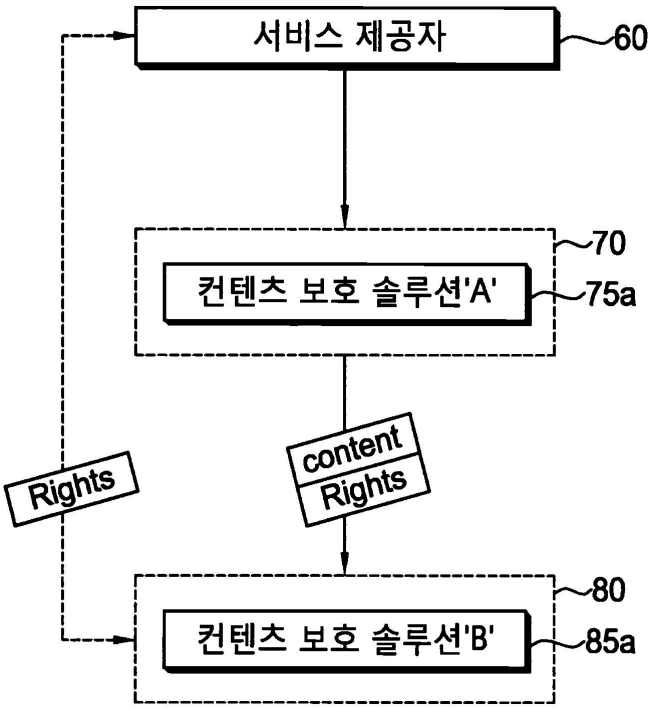
도면6


서비스 제공자
20
40
서비스 보호 솔루션
44
컨텐츠 보호 솔루션'A'
45a
50
컨텐츠 보호 솔루션'A'
55a

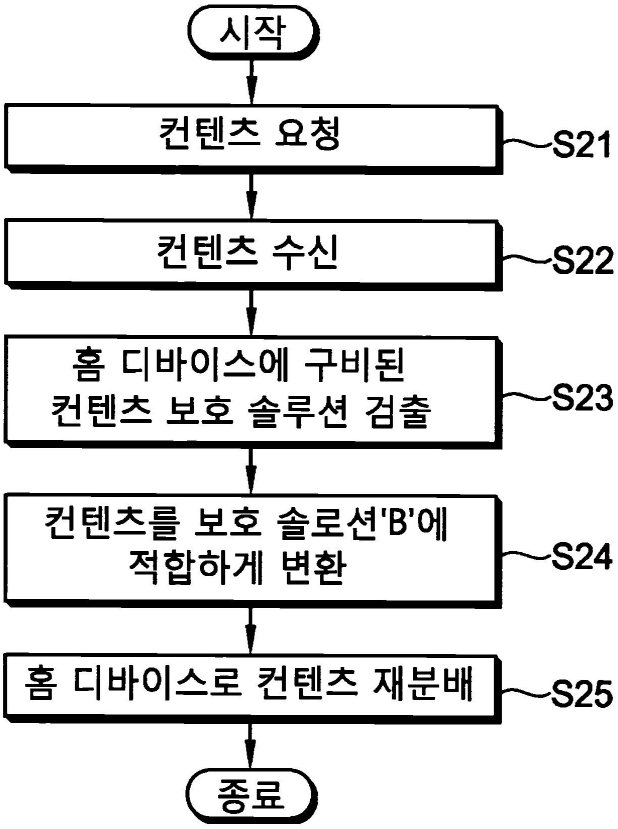
도면7


시작
컨텐츠 전송 요청
S11
컨텐츠 수신 및 처리
S12
홈 디바이스에 구비된
컨텐츠 보호 솔루션 검출
S13
컨텐츠를 보호 솔로션'A'에
적합하게 변환
S14
홈 디바이스로 컨텐츠 재분배
S15
종료

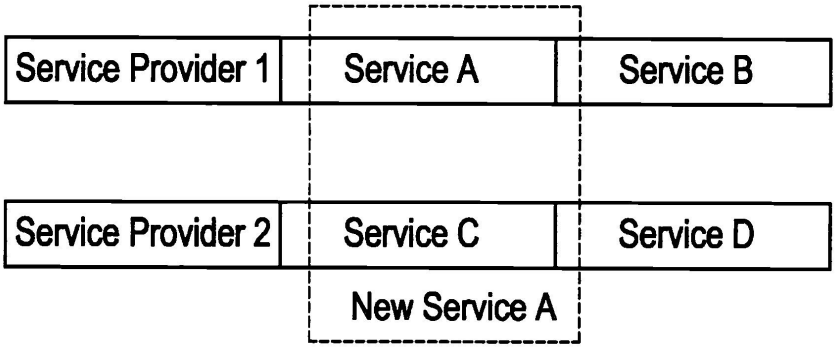
도면8


서비스 제공자
60
70
컨텐츠 보호 솔루션'A'
75a
content
Rights
Rights
80
컨텐츠 보호 솔루션'B'
85a

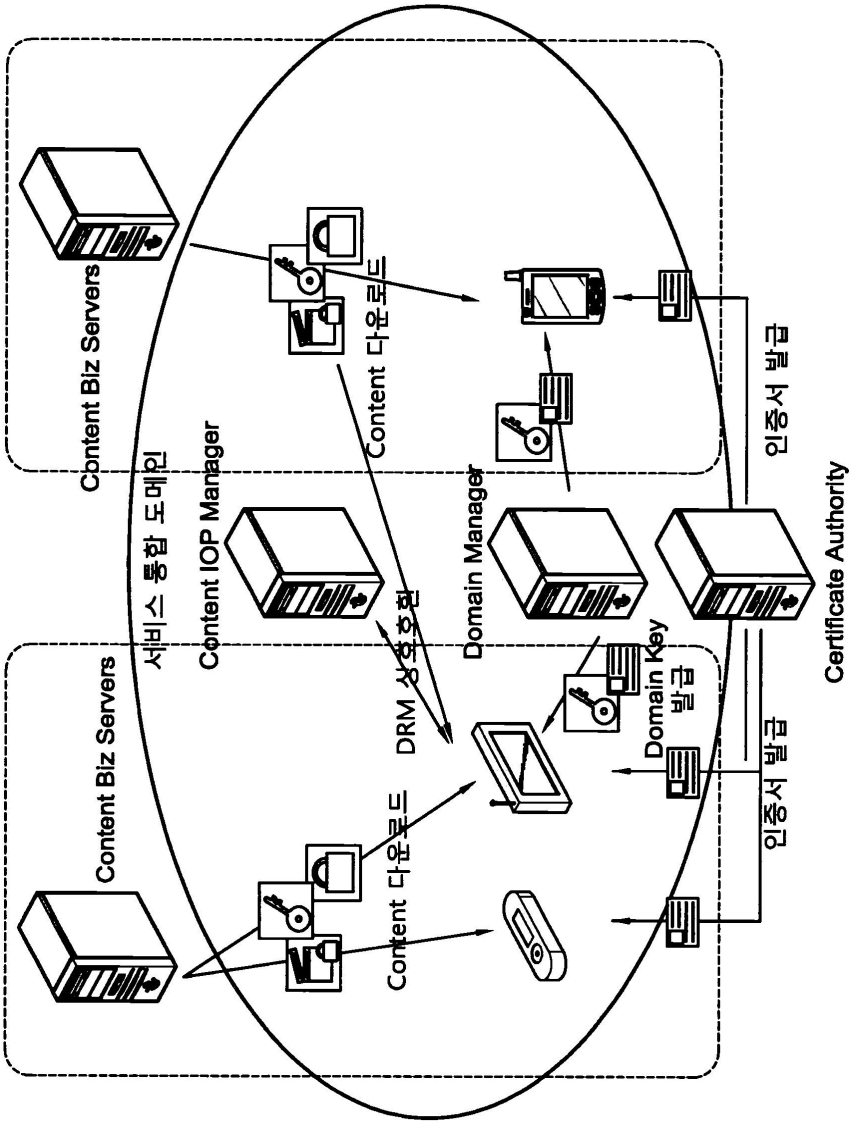
도면9


시작
컨텐츠 요청
S21
컨텐츠 수신
S22
홈 디바이스에 구비된
컨텐츠 보호 솔루션 검출
S23
컨텐츠를 보호 솔로션'B'에
적합하게 변환
S24
홈 디바이스로 컨텐츠 재분배
S25
종료

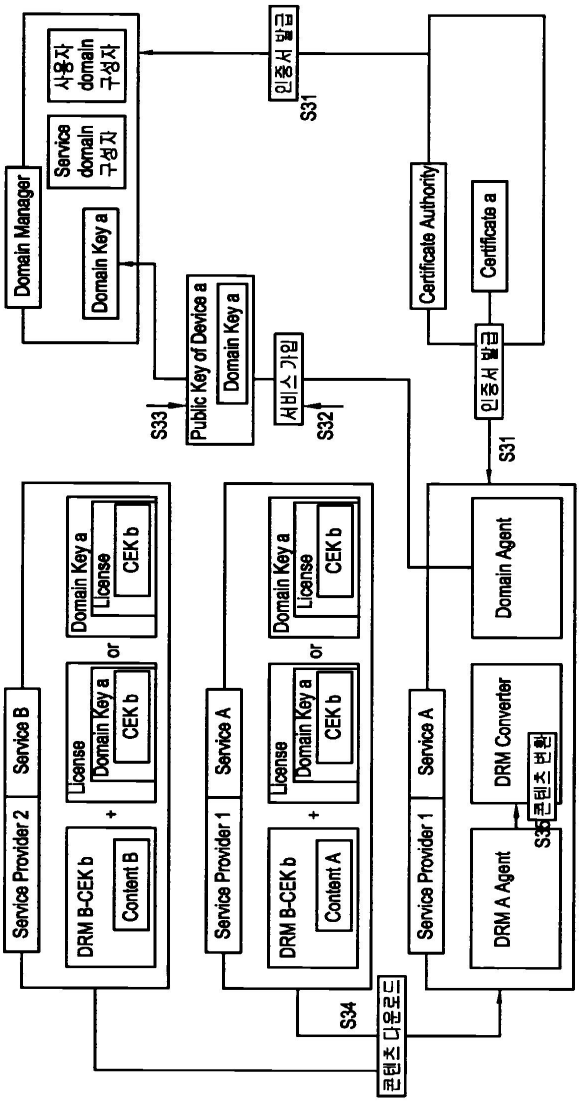
도면10


Service Provider 1
Service A
Service B
Service Provider 2
Service C
Service D
New Service A

도면11


Content Biz Servers
Content Biz Servers
서비스 통합 도메인
Content IOP Manager
Content 다운로드
Content 다운로드
DRM 상호호환
Domain Manager
Domain Key 발급
인증서 발급
인증서 발급
Certificate Authority

도면12


Domain Manager
사용자 domain 구성자
Service domain 구성자
Domain Key a
인증서 발급
S31
Certificate Authority
Certificate a
Public Key of Device a
Domain Key a
S33
서비스 가입
S32
인증서 발급
S31
Service Provider 2
Service B
DRM B-CEK b
Content B
License
Domain Key a
CEK b
or
Service Provider 1
Service A
DRM B-CEK b
Content A
Domain Key a
License
CEK b
Service Provider 1
Service A
DRM A Agent
DRM Converter
콘텐츠 변환
S35
Domain Agent
S34
콘텐츠 다운로드