(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월22일
(11) 등록번호 10-1122842
(24) 등록일자 2012년02월24일

(51) 국제특허분류(Int. Cl.)
G06F 15/00 (2006.01) *G06F 17/00* (2006.01)
(21) 출원번호 10-2005-0011665
(22) 출원일자 2005년02월11일
심사청구일자 2010년02월03일
(65) 공개번호 10-2006-0041882
(43) 공개일자 2006년05월12일
(30) 우선권주장
10/779,248 2004년02월13일 미국(US)
(56) 선행기술조사문헌
WO2003039155 A1
US5990883 A
US20030126086 A1
US20030051149 A1
전체 청구항 수 : 총 15 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
로버트, 아나우드
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
프리체트, 사더스 씨.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
(74) 대리인
제일특허법인

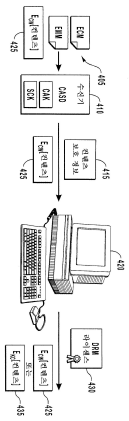
심사관 : 권오성

(54) 발명의 명칭 **디지털 권한 관리 변환에 대한 조건부 액세스**

(57) 요 약

본 발명은 두개의 외관상 비호환적이고 상이한 컨텐츠 보호 시스템 사이에 인터페이스를 제공한다. 따라서, 보호 컨텐츠는 조건부 액세스(CA)와 디지털 권한 관리(DRM) 시스템의 개별 보안 커널 사이에 전송되면서 컨텐츠 및 임의의 관련 보호 정보를 보안을 유지할 수 있다. 보호 컨텐츠 및 관련 컨텐츠 보호 정보의 전송 및 소비는 CA 및 DRM 시스템의 개별 보안 커널을 일시 또는 영구 결합하고, 컨텐츠 보호 정보를 전사하고, 상기 컨텐츠를 잠재적으로 전사하여 달성될 수 있다.

대 표 도 - 도4a



특허청구의 범위

청구항 1

엔터테인먼트 매체 환경에서, 컨텐츠가 상이한 컨텐츠 보호 방식으로부터 발생(originated)하더라도, 컨텐츠 보호 방식에 의해 한정되는 사용 권한에 따라 컨텐츠를 소비하는 데 사용되는 컨텐츠 라이센스를 생성하는 방법으로서,

복수의 수신기에 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화되는 조건부 액세스 보호 컨텐츠를 수신하는 동작;

상기 조건부 액세스 보호 컨텐츠에 관련된 사용 권한을 결정, 관리, 및 행사하는 데 사용되는 정보를 포함하는 조건부 액세스 컨텐츠 보호 정보를 수신하는 동작;

상기 컨텐츠가 데스티네이션(destination) 장치에서 소비될 수 있는 조건 및 방식을 규정하는, 컨텐츠 제공자에 의해 정의되는 상기 사용 권한을 결정하기 위해 상기 조건부 액세스 컨텐츠 보호 정보를 해석하는 동작;

상기 복수의 간헐 갱신 키를 사용하여 상기 조건부 액세스 보호 컨텐츠를 복호화하여 소비가능한 컨텐츠를 생성하는 동작;

상기 해석된 조건부 액세스 컨텐츠 보호 정보에 기초하여, 상기 사용 권한에 따라 하나 이상의 디지털 권한 관리 키를 제공하여 상기 데스티네이션 장치 내에서 디지털 권한을 행사하는 데 사용되는 컨텐츠 라이센스를 생성하는 동작; 및

상기 하나 이상의 디지털 권한 관리 키를 사용하여 상기 소비가능한 컨텐츠를 암호화하는 동작 - 상기 하나 이상의 디지털 권한 관리 키는 상기 소비가능한 컨텐츠 내에 포함되지 않음 -

을 포함하는 컨텐츠 라이센스 생성 방법.

청구항 2

제1항에 있어서,

상기 데스티네이션 장치는 상기 조건부 액세스 보호 컨텐츠의 수신기와 상기 데스티네이션 장치 간의 보안 통신 채널을 설정하기 위한 신뢰 장치임을 인증하는 동작을 더 포함하는 컨텐츠 라이센스 생성 방법.

청구항 3

제2항에 있어서,

상기 수신기는 조건부 액세스 보안 장치이며, 상기 조건부 액세스 컨텐츠 보호 정보와 상기 조건부 액세스 보호 컨텐츠를 상기 데스티네이션 장치에 전송하고,

상기 데스티네이션 장치는 상기 조건부 액세스 컨텐츠 보호 정보를 해석하고 상기 컨텐츠 라이센스를 생성하는 컨텐츠 라이센스 생성 방법.

청구항 4

제2항에 있어서,

상기 수신기는, 상기 복수의 간헐 갱신 키를 사용하여 상기 조건부 액세스 보호 컨텐츠를 복호화하여 소비가능한 컨텐츠를 생성하고, 상기 조건부 액세스 컨텐츠 보호 정보를 상기 데스티네이션 장치에 전송하고,

상기 데스티네이션 장치는 상기 조건부 액세스 컨텐츠 보호 정보를 해석하고 상기 컨텐츠 라이센스를 생성하는 컨텐츠 라이센스 생성 방법.

청구항 5

제1항에 있어서,

상기 수신기는 상기 복수의 간헐 갱신 키를 사용하여 상기 조건부 액세스 보호 컨텐츠를 복호화하여 소비가능한 컨텐츠를 생성하고, 상기 조건부 액세스 컨텐츠 보호 정보를 상기 데스티네이션 장치에 전송하고,

상기 데스티네이션 장치는, 상기 컨텐츠 보호 정보와 상기 컨텐츠 라인센스 요청을, 상기 조건부 액세스 컨텐츠 보호 정보를 해석하여 상기 컨텐츠 라이센스를 생성하는 라이센스 서버에 전송하는 컨텐츠 라이센스 생성 방법.

청구항 6

제1항에 있어서,

상기 수신기는, 상기 컨텐츠 라이센스를 생성하고, 상기 컨텐츠 라이센스와 상기 조건부 액세스 보호 컨텐츠를 상기 데스티네이션 장치에 전송하는 컨텐츠 라이센스 생성 방법.

청구항 7

엔터테인먼트 매체 환경에서, 컨텐츠가 상이한 컨텐츠 보호 방식으로부터 발생하더라도, 컨텐츠 보호 방식에 의해 정의되는 사용 권한에 따라 컨텐츠를 소비하는 데 사용되는 컨텐츠 라이센스를 생성하는 방법으로서,

복수의 수신기에 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화되는 조건부 액세스 보호 컨텐츠를 수신하는 동작;

상기 조건부 액세스 보호 컨텐츠에 관련된 사용 권한을 결정, 관리, 및 행사하는 데 사용되는 정보를 포함하는 조건부 액세스 컨텐츠 보호 정보를 수신하는 동작;

상기 조건부 액세스 컨텐츠 보호 정보의 해석을 통해, 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 조건 및 방식을 규정하는 상기 사용 권한을 결정하는 동작;

상기 복수의 간헐 갱신 키를 사용하여 상기 조건부 액세스 보호 컨텐츠를 복호화하여 소비가능한 컨텐츠를 생성하는 동작;

상기 해석된 조건부 액세스 컨텐츠 보호 정보에 따라, 하나 이상의 디지털 권한 관리 키를 포함하는 컨텐츠 라이센스를 생성하여 상기 데스티네이션 장치 내에서 디지털 권한을 행사하는 동작; 및

상기 하나 이상의 디지털 권한 관리 키를 사용하여 상기 소비가능한 컨텐츠를 암호화하는 동작 - 상기 하나 이상의 디지털 권한 관리 키는 상기 소비가능한 컨텐츠 내에 포함되지 않음 -

을 포함하는 컨텐츠 라이센스 생성 방법.

청구항 8

제7항에 있어서,

상기 데스티네이션 장치는 상기 조건부 액세스 보호 컨텐츠의 수신기와 상기 데스티네이션 장치 간의 보안 통신 채널을 설정하기 위한 신뢰 장치임을 인증하는 동작을 더 포함하는 컨텐츠 라이센스 생성 방법.

청구항 9

제7항에 있어서,

상기 데스티네이션 장치는 상기 소비가능한 컨텐츠를 복호화하고, 상기 컨텐츠 라이센스에 정의된 사용 권한에 따라 제2 컨텐츠 라이센스를 생성하며, 하나 이상의 제2 디지털 권한 관리 키를 사용하여 상기 복호화된 소비가능한 컨텐츠를 암호화하는 컨텐츠 라이센스 생성 방법.

청구항 10

제7항에 있어서,

상기 수신기는 상기 복수의 간헐 갱신 키를 사용하여 상기 조건부 액세스 보호 컨텐츠를 복호화하여 소비가능한 컨텐츠를 생성하고, 상기 조건부 액세스 컨텐츠 보호 정보를 해석하여 상기 컨텐츠 라이센스를 생성하며, 상기 컨텐츠 라이센스와 소비가능한 컨텐츠를 상기 데스티네이션 장치에 전송하고,

상기 데스티네이션 장치는 상기 하나 이상의 디지털 권한 관리 키를 사용하여 상기 소비가능한 컨텐츠를 암호화하는 컨텐츠 라이센스 생성 방법.

청구항 11

엔터테인먼트 매체 환경에서, 컨텐츠가 상이한 컨텐츠 보호 방식으로부터 발생하더라도, 컨텐츠 보호 방식에 의해 정의되는 사용 권한에 따라 컨텐츠를 소비하는 데 사용되는 컨텐츠 라이센스를 생성하는 방법을 구현하기 위한 프로그램을 기록한 하나 이상의 컴퓨터 판독가능 기록 매체로서,

상기 방법은,

복수의 수신기에 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화되는 조건부 액세스 보호 컨텐츠를 수신하는 동작;

상기 조건부 액세스 보호 컨텐츠에 관련된 사용 권한을 결정, 관리, 및 행사하는 데 사용되는 정보를 포함하는 조건부 액세스 컨텐츠 보호 정보를 수신하는 동작;

상기 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 조건 및 방식을 규정하는, 컨텐츠 제공자에 의해 정의되는 상기 사용 권한을 결정하기 위해 상기 조건부 액세스 컨텐츠 보호 정보를 해석하는 동작;

상기 복수의 간헐 갱신 키를 사용하여 상기 데스티네이션 장치에서 상기 조건부 액세스 보호 컨텐츠를 복호화하여 소비가능한 컨텐츠를 생성하는 동작;

상기 조건부 액세스 컨텐츠 보호 정보를 원격 컨텐츠 라이센스 서버에 전송하는 동작 - 상기 컨텐츠 라이센스 서버는, 상기 사용 권한에 따라 하나 이상의 디지털 권한 관리 키를 제공하여 상기 데스티네이션 장치 내에서 디지털 권한을 행사하는 데 사용되는 컨텐츠 라이센스를 생성함 - ; 및

상기 컨텐츠 라이센스를 상기 원격 라이센스 서버로부터 수신하는 동작; 및

상기 하나 이상의 디지털 권한 관리 키를 사용하여 상기 소비가능한 컨텐츠를 암호화하는 동작 - 상기 하나 이상의 디지털 권한 관리 키는 상기 소비가능한 컨텐츠 내에 포함되지 않음 -

을 포함하는 하나 이상의 컴퓨터 판독가능 기록 매체.

청구항 12

제11항에 있어서,

상기 데스티네이션 장치는 상기 조건부 액세스 보호 컨텐츠의 수신기와 상기 데스티네이션 장치 간의 보안 통신 채널을 설정하기 위한 신뢰 장치임을 인증하는 동작을 더 포함하는 하나 이상의 컴퓨터 판독가능 기록 매체.

청구항 13

제12항에 있어서,

상기 수신기는 데이터의 패키지를 상기 데스티네이션 장치에 전송하고,

상기 데스티네이션 장치는 패키지된 데이터를 해석하여 상기 컨텐츠 라이센스를 생성하는 하나 이상의 컴퓨터 판독가능 기록 매체.

청구항 14

엔터테인먼트 매체 환경에서, 초기의(originating) 보호 방식과 상이한 컨텐츠 보호 방식 내에서 사용 권한을 정의하는 라이센스를 사용하여 보호 컨텐츠를 소비하는 방법으로서,

복수의 수신기에 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화된 조건부 액세스 보호 컨텐츠를 수신하는 동작;

상기 조건부 액세스 보호 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 방식 및 조건을 규정하는 정보를 포함하고, 또한 상기 복수의 간헐 갱신 키 중 적어도 일부를 포함하는 디지털 권한 라이센스를 수신하는 동작;

디지털 권한 보호 방식을 사용하는 데스티네이션 장치에서 상기 조건부 액세스 보호 컨텐츠를 복호화하기 위한 상기 디지털 권한 라이센스를 사용하여 컨텐츠를 소비하는 동작; 및

사용 권한에 따라 하나 이상의 디지털 권한 관리 키를 사용하여 복호화된 조건부 액세스 보호 컨텐츠를 암호화하는 동작 - 상기 하나 이상의 디지털 권한 관리 키는 상기 복호화된 조건부 액세스 보호 컨텐츠 내에 포함되지 않으며, 컨텐츠가 상기 데스티네이션 장치에서 소비될 수 있는 방식 및 조건을 정의함 -

을 포함하는 보호 컨텐츠 소비 방법.

청구항 15

제14항에 있어서,

상기 디지털 권한 라이센스는 상기 브로드캐스트된 조건부 액세스 보호 컨텐츠와 함께 병렬 경로에서 수신되고,

상기 디지털 권한 라이센스는 상기 조건부 액세스 보호 컨텐츠의 수신 이전, 이후, 또는 그 동안 수신되고,

상기 디지털 권한 라이센스는 조건부 액세스 메시지를 통해 연결되거나 식별자에 의해 상기 조건부 액세스 보호 컨텐츠에 링크되는 보호 컨텐츠 소비 방법.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

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

청구항 39

삭제

청구항 40

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0015] 본 발명은 두개의 상이한 컨텐츠 보호 방식의 인터페이스에 관한 것이다. 보다 구체적으로는, 본 발명은 컨텐츠의 보안 및 임의의 관련 컨텐츠 보호 정보를 유지하면서, 조건부 액세스 방식에서 발생된 보호된 컨텐츠를 소비하기 위한 디지털 권한 관리 라이센스의 생성을 제공한다.

[0016] 광범위한 매체(예를 들어, 자기 디스크, 자기 테이프, 광 디스크, 위성, 케이블, 지상파 등)를 통한 저작권있는 컨텐츠(오디오, 비디오, 텍스트, 데이터, 멀티미디어 등)의 배포에 대한 관심의 증가로 인해 여러 다양한 컨텐츠 보호 방법이 제공되어 왔다. 통상, 이들 방식은 컨텐츠가 수신된 후(예를 들어, 셋탑 박스, 개인용 컴퓨터,

텔레비전, 이동 전화 등) 뿐만 아니라 전송 동안 컨텐츠를 보호하도록 설계된다. 두개의 흔한 보호 방식 유형은 조건부 액세스(CA)와 디지털 권한 관리(DRM) 시스템이다.

[0017] 조건부 액세스(CA) 시스템(예를 들면, 도 2 및 도 3을 참조하여 이하 보다 상세히 설명됨)은 위성 또는 케이블 공급자 등의 서비스 운영자로부터 개별 수신자에게 컨텐츠를 보안 전송하기 위해 브로드캐스트 플랫폼에서 사용된다. 대부분의 네트워크 운영자는 이들의 유료-TV 운영을 보호하기 위해서 이들의 서비스 중 적어도 일부를 스크램블할 것이다. 조건부 액세스 시스템은 암호화된 데이터 뿐만 아니라, 스크램블된 프로그램과 함께 또는 이와 병행하여 전송 스트림에 통상 브로드캐스트되는, CA 메시지(CAM)로 알려진 두개의 추가 데이터 유형을 포함하는 보안 원리를 이용한다. CAM은 두개의 개별 및 독립 메시지 스트림으로 이루어지며, 하나는 일련의 간헐적이고 연속적으로 갱신된 암호화 키를 포함하고 다른 하나는 특정 프로그램을 관측하는 가입자 권한을 포함한다. 양자의 CA 메시지는 관련 액세스 조건을 포함한다.

[0018] 컨텐츠의 브로드캐스트 전송을 위한 CA 시스템(예를 들어, 도 2 및 도 3을 참조하여 이하 보다 상세히 설명됨)과는 달리, DRM 시스템은 개인용 컴퓨터 및 다른 전자 품목 등의 장치 상에 다른 유형의 컨텐츠(예를 들면, CD, MPEG 파일, DVD, 오디오/비디오 스트림 등)의 안전한 소비를 위해 개발되어 왔다. 다수의 간헐적으로 갱신된 키와 CA 방식에서 사용된 여러 메시지 스트림 대신, DRM 시스템은 통상, 컨텐츠 사용 권한을 포함하는 단일 라이센스 뿐만 아니라 보호 컨텐츠를 소비하기 위한 복호화 키를 사용한다. 또한, 라이센스는 컨텐츠에 독립적으로 전달될 수 있지만, 이 컨텐츠를 라이센스 및 특정 장치 또는, 가능하게는, 장치 그룹에 결합시킬 수 있다.

[0019] 상이한 전달 메커니즘과 상이한 보안 위험을 염두해 두고 상이한 유형의 컨텐츠를 보호하기 위해 CA 및 DRM 기술이 개발되었다. 예를 들어, CA 보호 시스템은 스트리밍 방식, 예를 들어, 실시간 재생으로, 복수의 장치에 브로드캐스트되는 유료-TV 매체를 위한 CA 보호 시스템이 개발되었다. 따라서, 컨텐츠가 브로드캐스트되고 스트리밍되기 때문에, 다양한 보호 레벨(간헐 갱신 키와 상이한 시점에서의 암호화 및 상이한 메시지에서 은폐됨)이 중요하고, 가능하고, 실용적이라고 간주되었다.

[0020] 한편, 컨텐츠의 단일 부분(즉, 반드시 실시간 브로드캐스트는 아니지만, 저장되고 추후 재생/소비될 수 있는 디지털 데이터)을 통상 단일 장치(또는 작은 장치 그룹)에 전송하기 위한 DRM 시스템이 개발되었다. 따라서, 컨텐츠의 단일 라이센스로의 결합과 라이센스의 특정 장치(또는 장치 그룹)로의 결합은 컨텐츠가 수신 및 소비되는 방식에 어느 정도 조정되는 적절한 보호 레벨을 제공한다.

발명이 이루고자 하는 기술적 과제

[0021] 그러나, 신생 네트워크 기술, 예를 들어, 홈 네트워킹은 이들 대안적인 컨텐츠 보호 방법들 간의 현재의 비호환성을 노출하기 시작한다. 특히, 모든(또는 적어도 대부분의) 기기 및 가정 내의 다른 장치가 서로 통신할 수 있게 하고 가정 네트워크 내의 임의의 장치 상에서 각 장치의 고유 성능을 이용하고자 하는 요구로 인해, 이들 두 컨텐츠 보호 시스템의 통합이 이롭게 된다.

발명의 구성 및 작용

[0022] 본 발명의 실시예에 따라, 두개의 상이한 보호 방식을 인터페이스하고자 하는 상술한 요구가 달성된다. 예를 들면, 본 발명은 하나의 컨텐츠 보호 방식을 다른 컨텐츠 보호 방식으로 변환할 수 있는 엔터테인먼트 매체 환경을 제공한다. 특히, 본 발명은, 컨텐츠가 상이한 컨텐츠 보호 방식에서 발생하더라도, 컨텐츠 보호 방식에 의해 한정된 사용 권한에 따라 컨텐츠를 소비하는 데 사용되는 컨텐츠 라이센스를 생성하는 방법, 시스템 및 컴퓨터 프로그램 제품을 제공한다.

[0023] 복수의 수신기에 의해 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화되는 조건부 액세스 보호 컨텐츠를 수신하는 실시예가 제공된다. 또한 조건부 액세스 보호 컨텐츠와 관련된 사용 권한을 결정, 관리, 및 행사하는 데 사용되는 정보를 포함하는 조건부 액세스 컨텐츠 보호 정보가 제공된다. 조건부 액세스 컨텐츠 보호 정보는 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 방식 및 조건을 규정하는, 컨텐츠 제공자에 의해 한정되는 사용 권한을 결정하기 위해 해석된다. 해석된 조건부 액세스 컨텐츠 보호 정보에 기초하여, 컨텐츠 라이센스가 생성되고, 사용 권한에 따라 하나 이상의 디지털 권한 관리 키를 제공함으로써 데스티네이션 장치 내에서 디지털 권한을 행사하는 데 사용된다.

[0024] 다른 실시예는 복수의 수신기에 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화되는 조건부 액세스 보호 컨텐츠를 수신하는 엔터테인먼트 매체 환경에 대하여 제공된다. 조건부 액세스 보호 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 조건 및 방식을 규정하는 정보를 포함하는 디지털 권한 라이센스가 수신된다. 또한, 디

지털 권한 라이센스는 복수의 간헐 갱신 키 중 적어도 일부를 포함한다. 조건부 액세스 보호 컨텐츠는 그 후 디지털 권한 보호 방식을 사용하여 컨텐츠를 소비하는 데스티네이션 장치에서 디지털 권한 라이센스를 사용하여 복호화될 수 있다.

[0025] 본 발명의 추가 특징 및 이점은 후술하는 상세한 설명 부분에서 설명되며 이로부터 일부 명백해 질 것이며 본 발명의 실시에 의해 습득될 수 있다. 본 발명의 특징 및 이점은 첨부된 청구항에서 특히 지적된 도구 및 조합으로 실현 및 획득될 수 있다. 본 발명의 이들 및 다른 특징은 후술하는 설명 및 첨부된 청구항으로부터 보다 완전하게 명백하게 될 것이며, 이하 후술하는 본 발명의 실시에 의해 습득될 수 있다.

[0026] 본 발명의 상기 및 다른 이점이 획득될 수 있는 방법을 설명하기 위해서, 위에서 간략하게 설명된 본 발명의 보다 구체적인 설명이 첨부 도면에 도시된 특정 실시예를 참조하여 행해질 것이다. 이들 도면은 단지 본 발명의 통상의 실시예를 도시하며 본 발명의 범위를 한정하는 것으로 이해되어서는 안되며, 본 발명은 첨부한 도면을 통해 구체적이고 세부적으로 설명될 것이다.

[0027] <실시예>

[0028] 본 발명은 발생하는 컨텐츠 보호 방식과 상이한 컨텐츠 보호 방식에 의해 한정되는 사용 권한에 따라 컨텐츠를 소비하는 데 사용되는 컨텐츠 라이센스를 생성하는 방법, 시스템 및 컴퓨터 프로그램 제품으로 확장된다. 본 발명의 실시예는 이하 상세히 후술하는 바와 같이 다양한 컴퓨터 하드웨어 등의 특수 목적 또는 범용 컴퓨터를 포함할 수 있다.

[0029] 실시예들은 두개의 상이한 보호 방식을 인터페이스하는 상술한 요구를 달성하는 방법, 시스템 및 컴퓨터 프로그램 제품을 제공한다. 특히, 홈 네트워크 내에서 상이한 장치들 사이에 정보를 공유하고자 하는 요구로 인해, 본 발명은 컨텐츠 및 임의의 관련 보호 정보의 보안을 유지하면서, 조건부 액세스(CA) 및 디지털 권한 관리(DRM) 시스템의 개별 보안 커널들 간의 보호 컨텐츠 전송을 제공한다. 다음 설명에서, 컨텐츠 보호 정보(CPI)는 컨텐츠 관련 사용 규칙을 결정, 관리 또는 행사하는 데 사용되는 임의의 정보를 포함하는 일반 용어로서 사용될 수 있다. 보다 구체적으로는, CPI는 컨텐츠 암호화 키, 사용 권한, 라이센스 기간, 액세스 조건, 다른 보안 키, 및 컨텐츠 보호에 유용한 다른 정보를 의미할 수 있다. 보호 컨텐츠 및 관련 컨텐츠 보호 정보의 전송 및 소비는 CA 및 DRM 시스템의 개별 보안 커널을 일시 또는 영구적으로 결합시키고, 컨텐츠 보호 정보를 전사하며, 컨텐츠를 잠재적으로 전사하여 달성될 수 있다.

[0030] 도 1은 네트워크 운영자(110)가 유료 TV 또는 다른 동작을 보호하기 위해 그들의 서비스 중 일부를 스크램블하려는 통상의 CA 시스템(100)을 나타낸다. 물론, 이는 여기서 셋탑 박스(STB; 135a-f)로 도시된 수신기가 이들 서비스를 액세스하기 위한 몇몇 디스크램블링 소프트웨어를 포함할 수 있다. 스크램블 또는 암호화된 컨텐츠(122)는 여러 방송 수단 중 임의의 것, 예를 들어, 위성, 케이블, 지상파 등을 통해 전송 스트림으로 브로드캐스트되어 사용자(130a-f)에 의해 수신된다. 따라서, 동일한 정보가 모든 사용자(130a-f)에 의해 수신되지만, 후술하는 적절한 키가 없는 경우, 비인가된 사용자는 보호 컨텐츠(122)를 복호화할 수 없다.

[0031] 암호화 컨텐츠(122)에 더하여, CA 시스템은 전송 스트림에 두 유형의 데이터를 추가한다. 이들은 CA 메시지(CAM)로 알려져 있으며, 자격 제어 메시지(ECM; 123)와 자격 관리 메시지(EMM; 126)로 이루어진다. 또한, 이들은 개별 사용자(130a-f)(또는 사용자 그룹)의 보호 컨텐츠를 볼 수 있는 기능을 제어한다. 암호화(및 복호화)는 3개의 정보에 의존한다: (1) 제어 워드; (2) 서비스 키; 및 (3) 사용자 키.

[0032] 제어 워드(CW)는 서비스 키(SK)를 사용하여 암호화되어 제1 레벨의 암호화를 제공한다. 이러한 SK는 사용자 그룹에게는 흔할 수 있으며, 통상 각 암호화된 서비스가 하나의 SK를 가질 수 있다. 이러한 암호화된 CW는 대략 매 2초마다 ECM(123)에 브로드캐스트되고 디코더 또는 수신기(135a-f)가 실제 서비스를 디스크램블하기 위해 실제 요구하는 것이다.

[0033] 다음으로, 방송자 또는 네트워크 운영자는 단지 인가된 사용자(즉, 유료 교객)이 CW를 복호화할 수 있게 보장할 필요가 있다. 이를 위해서, SK는 사용자 키(UK), 예를 들어, UK1-6를 사용하여 암호화될 수 있다. 각 사용자 키는 단일 사용자에게는 고유하므로, 서비스 키는 컨텐츠를 관람할 수 있도록 인가된 각 사용자에 대하여 UK로 암호화될 수 있다. SK가 암호화되면, EMM(126)의 일부로서 브로드캐스트된다. 브로드캐스트해야 할 많은 정보가 있기 때문에(예를 들어, 암호화된 SK는 각각의 인가된 사용자에 대하여 브로드캐스트되어야 한다), 이들은 ECM(123) 보다 덜 흔하게 브로드캐스트된다. 다음은 상술한 CA 프로세스의 일 예를 제공한다.

[0034] 암호화된 컨텐츠(122)와 ECM(123) 및 EMM(126)으로 이루어진 CAM 메시지는 네트워크 제공자로부터 위성(120)을 통해 다수의 사용자(130a-f)에게 브로드캐스트된다. 암호화된 컨텐츠(122)는 제어 워드(CW)를 사용하여 암호화

되며, 이는 추후 사용자 키(SK)를 사용하여 암호화되고 ECM(123)에서 전송 스트림으로 브로드캐스트된다. EMM(126)은 또한 전송 스트림으로 브로드캐스트되고 , 이 전송 스트림은 서비스에 비용을 지불한 인가된 사용자에 대한 사용자 키(UK)로 암호화된 SK를 포함한다. 예를 들면, 도 1에 도시한 바와 같이, 사용자(130a 및 130e)는 네트워크 제공자(110)로부터의 서비스에 지불했으므로, SK는 130a 및 130e에 대응하고 EMM(126)에 포함되는 UK1과 UK5를 사용하여 암호화된다. 따라서, 모든 사용자(130a-f)가 동일 브로드캐스트 신호를 수신하더라도, 단지 수신기(135a 및 135e) 만이 SK를 복호화하고, 추후 이 SK를 사용하여 CW를 복호화하여, 이는 보호 컨텐츠(122)를 복호화하는데 사용될 수 있다.

[0035] 상술한 CA 시스템과는 달리, DRM 시스템은 보호 컨텐츠를 암호화 및 복호화하는데 상이한 프로세스를 사용한다. 도 2는 DRM(200)의 일 예를 나타내며, 이는 컨텐츠 소유자가 자치(230)에 보호 컨텐츠(205)를 배포할 수 있게 한다. 통상, 컨텐츠를 암호화하고 이 컨텐츠를 패키지하여 고객에게 인터넷, CD 또는 다른 통상의 수단을 통해 배포하는 라이센싱 프로세스는 컨텐츠 소유자에 의해 개시된다. 고객은 그 후 컨텐츠 소유자에 의해 한정된 비즈니스 규칙(210)에 따라 컨텐츠를 소비하기 위한 라이센스를 수신할 수 있다. 다음은 DRM 모델에서 보호 컨텐츠(205)를 복호화하기 위해서 라이센스(225)가 수신되어 사용되는 방식에 대한 통상의 프로세스를 나타낸다.

[0036] 컨텐츠 소유자는 통상 임의 개수의 공지된 프로세스에 따라 컨텐츠(205)를 암호화 및 패키지한다. 그러나, 통상, 컨텐츠는 암호화된 컨텐츠(205)와 컨텐츠를 소비할 때 장치(230)를 보조하는 정보를 포함하는 헤더부를 포함하도록 패키지될 수 있다. 또한, 패키지된 컨텐츠는 라이센스(225)가 획득된 위치를 나타내도록 라이센스 획득 URL을 사용할 수 있다. 더욱이, 패키지된 파일 내에 포함될 수 있는 다수의 다른 선택적 그리고 주요 데이터, 예를 들어, 컨텐츠 헤더를 사인하는데 사용되는 사적 사인 키, 컨텐츠 소유자와 라이센스 발행자 간에 공유된 키를 생성하는데 사용될 수 있는 라이센스 키 시드 등이 포함될 수 있다.

[0037] 보호 컨텐츠(205)는 컨텐츠 배포자(240)에 전송되어 배포를 위한 스트리밍 서버 또는 웹 서버 상에 배치될 수 있다. 그 컨텐츠를 수신한 장치(230)는 그 후 파일 헤더 내에 매립된 라이센스 획득 URL에게 컨텐츠(205) 소비를 위한 적절한 라이센스(225)를 획득하도록 지시할 수 있다. 라이센스(225)가 라이센스 발행자(215)에 의해 배포되기 전에, 컨텐츠 소유자는 라이센스 발행자(215)에게, 시드, 공개 키 및 라이센스(225)가 허여되는 비즈니스 규칙을 포함할 수 있는, 비즈니스 규칙과 비밀 공유(210)를 전송하여야 한다. 이 규칙(210)은 라이센스가 사용자에게 배포되는 방식 및 조건을 한정한다. 예를 들면, 규칙은 디지털 컨텐츠의 배포가 한정된 횟수만큼, 특정 총 시간 동안, 특정 유형의 머신 상에서만, 특정 유형의 미디어 플레이어에서만, 특정 유형의 사용자에게만 실행되도록 할 수 있다. 어느 경우이든, 라이센스 발행자(215)는 라이센스(225)가 적절한 비즈니스 규칙 또는 컨텐츠 소유자에 의해 규정된 요건에 따라 발생되도록 보장하기 위해 인증되어야 한다.

[0038] 컨텐츠(205)가 컨텐츠 배포자(240)에게 전송된 경우 컨텐츠 소유자에 의해 한정되는 고려사항(235)을 지불한 후에, 장치(230)는 컨텐츠 배포자(240)로부터 컨텐츠(205)를 획득할 수 있다. 상술한 바와 같이, 암호화된 컨텐츠(205)를 실행하기 위해서, 장치(230)는 라이센스 발행자(215)로부터 라이센스(225)를 우선 획득하여야 한다. 장치(230)는, 라이센스(225)에 대한 요청(220)을 행하기 위해서, 암호화된 컨텐츠(205)의 헤더 내에서 라이센스 획득 URL을 사용하여 라이센스 발행자(215)가 누구인지를 결정할 수 있다. 그 후, 컨텐츠 헤더, 클라이언트 컴퓨터(230)에 대한 정보 및 다른 선택적 정보를 교환하는 것을 포함하는 등의 요청 프로세스가 개시될 수 있다. 수신된 정보에 기초하여, 라이센스 발행자(215)는 적절한 라이센스(225)에 응답하여, 장치(230)가 암호화된 컨텐츠(205)를 소비할 수 있게 한다. 이러한 라이센스(225)는 통상 단일 암호화된 키(KC)만을 포함하여 컨텐츠, 특정 권한, 장치에 대한 정보 및 다른 컨텐츠 보호 정보를 복호화할 수 있다.

[0039] CA 및 DRM 시스템에 대한 상기 설명에 기초하여, 두개의 시스템은 컨텐츠 보호를 위해 상이한 메커니즘을 사용할 수 있음을 쉽게 알 수 있다. 도 3은 DRM 패키지 시스템을 사용하여 CA 패키징 방식의 일대일 비교를 나타낸다. CA와 DRM 간의 지적해야 할 주요 차이점 중 하나는, DRM 시스템이 단일 암호화된 키로 단일 라이센스를 사용하여 컨텐츠(340)를 복호화하는 반면, CA 시스템은 여러 간헐 갱신 키를 사용하여 컨텐츠를 관람 또는 소비한다는 점이다. 예를 들면, DRM 시스템으로 암호화된 2시간짜리 영화는 암호화 컨텐츠(340)에 관련하여 하나의 라이센스(350)를 갖고, 통상 컨텐츠(340)를 복호화하는데 사용되는, 라이센스(350) 내에 하나의 암호화 키를 가질 수 있다.

[0040] 반면에, CA 시스템은 두개의 상이한 메시징 메커니즘 내에서 임베디드되는 동적으로 또는 연속적으로 변경하는 암호화 키와 여러 암호화 층을 제공한다. 특히, 컨텐츠를 복호화하는데 사용되는 연속 갱신 제어 워드는 서비스 키를 사용하여 암호화되고, 이 서비스키 또한 주기적으로 변경하여 ECM(320) 내에서 임베디드된다. 또한, SK는 여러 사용자 키를 사용하여 암호화되고 EMM(30) 내에 포함된다. 따라서, 여러 SK 및 가능하게는 수백 또

는 수천의 CW가 DRM 시스템이 단지 하나의 라이센스와 하나의 암호화 키를 가질 수 있는 동일한 2시간 짜리의 영화를 관람 또는 소비하기 위해서 요구될 수 있다.

[0041] 상술한 바와 같이, 홈 네트워킹 대중성의 증가에 따라, CA 보호 시스템을 DRM 보호 시스템에 관련시키는 충족되지 않은 요구가 있다. 따라서, 본 발명은 CA와 DRM 시스템을 안전하게 인터페이스하는 방법, 시스템 및 컴퓨터 프로그램 제품을 제공하여 개별 보안 커널 간의 컨텐츠 보호 정보를 전송하면서 컨텐츠와 임의의 관련 보호 컨텐츠 정보(예를 들어, 사용 권한, 액세스 조건, 암호화 키 등)의 보안을 유지할 수 있다. 본 발명은 각각의 CA 및 DRM 보안 커널을 일시 또는 영구적으로 결합하고, CA 구문에서 DRM 구문으로 컨텐츠 보호 정보를 전사하며, 가능하게는, 보호 컨텐츠를 전사한다.

[0042] 이해할 수 있는 바와 같이, 디지털 권한 관리 시스템에 대한 조건부 액세스로부터 컨텐츠 보호 정보의 전사가 달성될 수 있는 많은 방식이 있다. 예를 들면, 도 3에서 CA 패키징 방식과 DRM 패키징 시스템의 일대일 비교에서 도시한 바와 같이, CA 방식에 따라 컨텐츠(310)를 암호화하는데 사용되는 다수의 CW는 라이센스(350)에 포함되어 전사될 수 있으므로, 라이센스(340)가 인코딩된 조건부 액세스 컨텐츠를 복호화하는데 사용될 수 있게 한다. 다르게는, 또는, 이에 더하여, 라이센스는 CW를 암호화하는데 사용되는 서비스 키를 포함하여 DRM 시스템에 전사될 때 라이센스(350) 내에 추가 보호 층을 가질 수 있다. 다른 예로서, 암호화된 컨텐츠(310)는 ECM(330)과 ECM(320)을 사용하여 종래의 CA 방법에 따라 복호화될 수 있으며, 라이센스(350)는 그 후 종래의 DRM 방법을 사용하여 생성 및 컨텐츠 암호화될 수 있다. 실제로, CA 및 DRM 구문 간의 임의의 조합 및 개수의 가능한 매핑이 가능하며, 이에 따라, CA 및 DRM 구문을 전사하는 상술한 그리고 후술하는 예는 단지 예시적인 것으로서 본 발명의 범위를 한정하려는 것은 아니다. 또한, 이하 보다 상세히 설명하는 바와 같이, CA 구문에서 DRM 구문으로 컨텐츠 보호 정보의 전사는 다수의 상이한 장치 중 임의의 것에서 뿐만 아니라 변환 프로세스 동안 상이한 시점에서 발생할 수 있다. 따라서, 다음 구현 세부사항은 본 발명의 범위를 한정하거나 좁히려는 것은 아니다.

[0043] 상술한 바와 같이, 본 발명은, 컨텐츠 보호 방식에 의해 한정되는 사용 권한에 따라 컨텐츠를 소비하는데 사용되는 컨텐츠 라이센스 생성 프로세스를 기술하엿지만, 상이한 컨텐츠 보호 방식으로 컨텐츠를 생성할 수 있다. 조건부 액세스와 디지털 권한 관리 시스템의 보안 커널 들 간의 결합 메커니즘을 통신할 때 두개의 보안 커널을 인증함으로써 설정하는 실시예가 제공된다. 이하 보다 상세히 설명하는 바와 같이, 도 4a 내지 도 4l에 따른 예에서, 사용자 권한 정보의 전송 및 보호 컨텐츠의 전송이 여러 상이한 방식 중 임의의 하나로 구현될 수 있다.

[0044] 결합 기능은 상이한 방식으로 저장될 수 있는 비밀 정보에 의존한다. 바람직한 실시예에서, 결합 정보는 믿을 수 있고, 침해되지 않는 보안 장치, 예를 들어, 스마트 카드 또는 다른 보안 침 내에 저장된다. 다른 실시예는 결합 정보가 이상적으로는 DRM 시스템의 보안 커널로부터 판독하기 위해서만 액세스가능한 보안 라이브러리에 저장될 수 있다. 다르게는, 또는 이에 더하여, 결합 정보는 애플리케이션의 보안 커널에 단지 이용가능한 보안 파일 내에 저장될 수 있다.

[0045] 이해될 수 있는 바와 같이, 다수의 실현이 CA와 DRM 보안 커널 간의 결합을 위해 가능하다. 예를 들면, 보안 커널은 공통 비밀을 공유할 수 있고, 이 비밀을 사용하여 컨텐츠를 암호화함으로써 정보의 교환을 보안할 수 있다. 비밀은 정적(즉, 인스톨 시 또는 개별화 시에 커널 내에 로딩됨) 또는 동적(즉, 비밀이 시간 경과에 따라 소프트웨어 다운로드가능한 메커니즘을 사용하여 또는 내부 자동화 갱신 프로세스를 사용하여 변경)일 수 있다. 공통 비밀은 또한 공개 키 암호 및/또는 인증의 사용에 의해 보안 커널에 제공될 수 있다.

[0046] 다르게는, CA 및 DRM 보호 방법은 공개 키 암호 기반 정보를 포함하는 인증서를 교환하는 수단을 가질 수 있다. 예를 들면, 데스티네이션 장치 커널, 즉, DRM 시스템은 그 인증을 수신 커널, 즉, CA 커널에 정보 요청시 전송할 수 있다. 수신 커널은 그 후 인증성을 유효화하고, 이의 유효성에 기초하여 데스티네이션 커널의 공개 키를 사용하여 요청된 정보를 암호화하고 암호화된 정보를 전송한다. 그 후, 데스티네이션 장치는 그 개인 키를 사용하여 정보를 검색할 수 있다. 물론, 커널들을 서로 인증하는 다른 수단, 예를 들어, 딜페 헬만(Dilfe-Hellmann) 또는 다른 공개 키 암호화 알고리즘이 구현될 수 있다.

[0047] 두개의 보안 커널들 간의 결합 기간은 무한 또는 특정 기간 동안 지속할 수 있다. 결합이 만료되지 않으면(또는 오래 지정된 기간의 경우), 결합 메커니즘은 상술한 바와 같이 민감한 정보를 교환하는데 사용되는 비밀의 동적 갱신에 관련될 수 있다. 결합이 만료되면, 보안 커널은 새로운 결합 프로세스를 단독으로 또는 신뢰있는 기관을 통해 트리거할 수 있다.

[0048] 데스티네이션 커널, 즉, DRM 장치의 성공적인 인증인 경우, 결합 정보의 변경은 수신 및 데스티네이션 커널을 모두 트리거하여 모든 후속 민감 정보의 교환에서 새로운 결합 정보를 사용한다. 실시예는 데스티네이션 커널에 대한 결합 메커니즘을 관리할 수 있다. 이러한 동적 결합은, 이로서 동작할 수 있는 모든 보안 커널에 공통인, 보다 높은 레벨의 비밀(대칭 또는 비대칭)을 사용하여 새로운 결합 정보를 데스티네이션 장치에 전송한다. 보다 높은 레벨의 비밀은 비침해 간주되는 위치, 예를 들어, 스마트 카드, 임베드 칩 또는 비간섭 위치에서 상주하여야 한다. 결합 정보의 변경은 수신 장치에 의해 임의의 시점에서 프로그래밍되거나 트리거될 수 있다.

[0049] 두개의 보안 커널들 간의 신뢰는 수신 및 데스티네이션 보안 커널과 독립적으로 임의의 시점에서 도전받을 수 있다. 이러한 경우, 도전받는 커널은 다른 커널에 결합 관련 정보, 예를 들어, 인증서를 요청할 수 있다. 도전이 성공하면, 민감한 정보는 전후로 다시 전송될 수 있으며, 그렇지 않은 경우, 통신이 정지될 수 있다. 도전 응답은 소정의 시간 내에서, 임의로 선택된 시간에서 발생할 수 있거나 수신 또는 데스티네이션 보안 커널에 의해 트리거될 수 있거나 그렇지 않을 수 있다. 다수의 다른 도전 응답 프로토콜이 보안 커널의 인증여부를 우발적으로 검증하는데 사용될 수 있다.

[0050] 다른 예는 사용 권한 또는 컨텐츠 보호 정보의 전송을 위한 다수의 구현을 제공한다. 예를 들면, 수신 장치(즉, CA 장치)는 CPI를 데스티네이션 장치(즉, DRM 장치)에 전송하며, 데스티네이션 장치는 그 후 적절한 DRM 컨텐츠 라이센스를 국부적으로 또는 이에 연결된 원격 서버를 사용하여 생성할 수 있다. 다른 실시예는 수신기간 데스티네이션 장치에 의해 인식되는 포맷 또는 구문으로 적절한 라이센스를 생성할 수 있다. 컨텐츠 라이센스의 생성은 수신기가 접속하는 원격 서버를 사용하거나 국부적으로 행해질 수 있다. 또다른 실시예에서, DRM 보호 방식에 관련된 라이센스는 수신기 또는 CA 구문 장치에 의해 수신되는 컨텐츠로 전달된다. 예를 들면, DRM 라이센스는 CA 보호된 (또는 CA 비보호된) 전송 시스템의 사적 디스크립터를 통해 전달 될 수 있다.

[0051] 컨텐츠 보호 정보의 전송의 변화와 유사하게, 보호 컨텐츠 자체의 전송에 대한 다수의 실현이 가능하다. 예를 들면, 보호 컨텐츠는 수신 장치에서 데스티네이션 장치로 "있는 그대로" 전송될 수 있다. 다르게는, 실시예에 따라, 수신기 또는 CA 장치는 컨텐츠를 복호화하고 이를 데스티네이션 장치에 압축 또는 비압축으로 전송하며, 데스티네이션 장치는 DRM 라이센스와 CPI에 따라 컨텐츠를 추후 암호화할 수 있다. CA 장치와 DRM 장치 간의 통신 채널은 통상 - 하지만, 필수는 아닌 -, 예를 들면, 하드웨어 또는 링크 보호 메커니즘으로 보안될 수 있다. 어느 경우이든, DRM 장치는 암호화 키를 보안 생성하고 컨텐츠를 암호화할 뿐만 아니라 컨텐츠 라이센스 내의 CPI 정보를 갱신하여 새로운 암호화 키 세트를 나타내는 수단을 구비하여야 한다. 또다른 실시예는 CA 장치가 DRM 장치에 암호화된 컨텐츠를 전송하고, DRM 장치가 컨텐츠에 관련된 CPI를 사용하여 컨텐츠를 복호화하고 이 컨텐츠를 국부적으로 다시 암호화한다.

[0052] 다른 실시예는 데스티네이션 장치 또는 DRM 장치가 수신 장치 또는 CA 장치에 의해 보호되지 않지만 CPI를 포함하는 컨텐츠를 수신하는 경우, DRM 장치는 CPI의 해석에 가장 가까운 디폴트 컨텐츠 보호 정책을 적용할 수 있다.

[0053] 또다른 실시예에서, 수신 장치는 컨텐츠(가능하게는, 라이센스)를 링크 암호화 메커니즘에 전사하고, 링크 암호화 메커니즘은 그 후 DRM 메커니즘으로 변환될 수 있다. 통상, 컨텐츠는 링크 암호화에서 사용되는 키(가능하게는, CA 보호에서 사용되는 것과 동일한 키)로 암호화된 상태를 유지하고 단지 라이센스만이 링크 보호에서 DRM 보호로 전사될 수 있다.

[0054] 도 4a 내지 도 41 및 이의 후술하는 설명은 컨텐츠 보호 정보가 DRM 라이센스를 생성하여 후에 CA 보호 컨텐츠를 보여주는 데 사용될 수 있는 방식의 다양한 구현예를 나타낸다. 다음 예시 및 설명은 상기 실시예의 단지 구현예일 뿐이며 본 발명의 범위를 한정 또는 좁히려는 것은 아니다. 또한, 도 4a 내지 도 41은 DRM 라이센스를 생성하고 추후 이 라이센스를 사용하여 보호 컨텐츠를 소비하는 경우에 CA에서 DRM으로 전사하는 다양한 장치를 나타낸다. 그러나, 유사한 기능을 수행할 수 있는 다수의 상이한 유형의 장치가 가능하다. 예를 들면, 상술한 바와 같이, 수신기(410) 또는 데스티네이션 장치(420)는 DRM 라이센스를 생성하는데 사용될 수 있다. 다르게는, 수신기(410) 또는 데스티네이션 장치(420)는 신뢰있는 원격 장치에 접속하고, 이 원격 장치가 DRM 라이센스를 생성할 수 있다. 더욱이, 수신기 또는 데스티네이션 커널은 스마트 카드, 조건부 액세스 커널, 비간섭 칩, 보안 라이브러리 중 임의의 것일 수 있다. 따라서, 다음 구현예는 CA 컨텐츠 보호 정보를 사용하여 DRM 라이센스를 생성하지만, 이 리스트는 단지 일 예로서 이해되어야 한다.

[0055] 도 4a는 수신기(410) 또는 CA 보안 장치(CASD)가 조건부 액세스 메시지(CAM; 405), 즉, ECM과 EMM을 보호 컨텐츠(425)와 함께 수신하는 일 구현예를 나타낸다. 상술한 바와 같이, 수신기(410)는 조건부 액세스 커널(CAK), 스마트 카드 커널(SCK) 등과 같이 다수의 보안 장치 중 임의의 것을 포함할 수 있다. 수신기(410)는 컨텐츠 보

호 정보(415) 뿐만 아니라 수신된 CA 보호 컨텐츠(425)를 데스티네이션 장치(420)에 전송한다. 데스티네이션 장치는 CPI(415)에 기초하여 DRM 라이센스(430)를 생성하는 보안 메커니즘을 포함하는 DRM 시스템일 수 있다. 데스티네이션 장치(420)는 보안 라이브러리 또는 DRM 라이센스(430)를 보안 생성할 수 있는 다른 유사 DLL의 형태일 수 있는 보안 커널을 포함할 수 있다. CA 보호 컨텐츠(425)는 "있는 그대로" 남겨질 수 있으며, 이에 따라, DRM 라이센스(430)는 CAM(405)에 제공된 것과 유사한 키의 리스트를 포함할 수 있다. 다르게는, 데스티네이션 장치(420)는 CA 보호 컨텐츠(425)를 복호화하고 이 컨텐츠를 다시 암호화하여 DRM 보호 컨텐츠(435)를 생성하고 CPI(415)와 보호 컨텐츠(435)에 관련된 키로부터 해석된 적절한 사용 권한을 사용하여 DRM 라이센스(430)를 갱신한다.

[0056] 도 4b는 도 4a에 대하여 상술한 바와 유사한 방식으로 CPI(415)에 따라 컨텐츠 라이센스(430)를 생성하는 다른 구현예를 나타낸다. 여기서 조건부 액세스 커널(CAK)로서 도시한 수신기(410)는 CAM(405)와 CA 보호 컨텐츠(425)를 위성, 케이블 또는 다른 지상파 수단을 통해 대응하는 네트워크 운영자로부터 수신한다. 물론, 수신기(410)는 상술한 바와 같이 임의 개수의 CASD, 예를 들면, 스마트 카드 커널일 수 있다. 수신기(410)는 DRM 데스티네이션 장치(420)에 CPI(415)를 전송한다. 또한, 수신기(410)는 종래의 CA 방식과 CAM(405) 내에 제공된 정보를 사용하여 CA 보호 컨텐츠(425)를 복호화한다. 따라서, 수신기(410)는 비암호화된 컨텐츠를 데스티네이션 장치에 전송하거나 데스티네이션 장치(420)에 의해 인식된 DRM 방식에 따라 컨텐츠를 재암호화하고 데스티네이션 장치(420)에 암호화된 컨텐츠(435)를 전송할 수 있다. 어느 경우이든, 데스티네이션 장치(420)는 DRM 라이센스(430)를 생성하여 비암호화되어 수신된 경우 컨텐츠(440)를 암호화하거나, 수신된 암호화 컨텐츠(435)를 단순히 사용하여 적절한 키로 DRM 라이센스(430)를 갱신할 수 있다.

[0057] 도 4c는 CA 시스템에서 CPI에 의해 한정되는 사용 권한에 따라 컨텐츠(425, 435)를 소비하는데 사용되는 컨텐츠 라이센스(430)를 생성하는 다른 구현예를 나타낸다. 또한, CASD, 예를 들어, CAK, SCK인 수신기(410)는 CAM(405)과 CA 보호 컨텐츠(425)를 수신한다. 그러나, 이 구현예에서, 수신기(410)는 DRM 라이센스(430)를 생성 또는 발생시켜 이러한 라이센스(430)를 데스티네이션 DRM 장치(420)에 전송할 수 있다. 이러한 특정 구현예에서, 수신기(410)는 또한 CA 보호 컨텐츠(425) 있는 그대로를 데스티네이션 장치(420)에 전송한다. 데스티네이션 장치(420)는 그 후 보호 컨텐츠 (425)를 복호화하고, DRM 방식에 따라 컨텐츠를 재암호화하여 보호 컨텐츠(435)를 생성하고, 적절한 컨텐츠 보호 키를 사용하여 DRM 라이센스(430)를 갱신한다. 다르게는, 수신기(410)는 DRM 라이센스(430)를 데스티네이션 장치(420)에 전송할 때 DRM 라이센스(430) 내에 적절한 키(예를 들어, CW 리스트)를 포함시켜, 데스티네이션 장치(420)가 DRM 라이센스(430)를 사용하여 CA 보호 컨텐츠(425)를 그 본래의 형태로서 복호화한다. 다른 실시예에서는 데스티네이션 장치(420) 또는, 물론, 일부 미도시된 원격 장치가 CA 보호 컨텐츠(425)를 소비하기 위해서 적절한 CA 키로 컨텐츠 라이센스(430)를 갱신할 수 있다.

[0058] 도 4d에 도시한 바와 같은 또다른 구현예에서, 여기서 SCK로 도시된 수신기(410)는 CAM(405)와 보호 컨텐츠(425)를 수신하고, CA 보호 컨텐츠(425)를 복호화하고, DRM 방식에 따라 컨텐츠를 재암호화하여 암호화된 컨텐츠(435a)를 생성한다. 또한, 수신기(410)는 또한 CPI를 사용하여 DRM 컨텐츠 라이센스 #1(430a)을 생성한다. DRM 라이센스 #1(430a)과 보호 컨텐츠(435a)는 데스티네이션 장치(420)에 전송될 수 있다. 그 후, 데스티네이션 장치(420)는 DRM 라이센스 #1(430a)을 사용하여 재암호화된 컨텐츠(435a)를 소비할 수 있거나, 또는 DRM 라이센스 #1(430a) 내의 사용 권한 정보를 사용하여 제2 DRM 라이센스 #2(430b)를 생성하고 또한 원래의 재암호화된 컨텐츠(435a)를 복호화하여 라이센스 #2(430b)가 관련되는 다른 암호화 버전(435b)를 생성한다.

[0059] 도 4e는 수신기(410)가 CA 정보(405)와 보호 컨텐츠(425)를 수신하는 다른 구현예를 나타낸다. 수신기(410)는, 여기서 CAK로 나타내는, 보안 커널과 CPI를 사용하여 DRM 라이센스(430)를 생성한다. 또한, 이 구현예는 컨텐츠를 복호화하여 컨텐츠(440)를 생성하는 수신기(410)를 나타내며, 컨텐츠(440)는 DRM 라이센스(430)와 함께 데스티네이션 장치(420)에 전송될 수 있다. 그 후, 데스티네이션 장치(420)는 컨텐츠(440)를 암호화하여 암호화된 컨텐츠(435)를 생성하고 수신된 DRM 라이센스(430)를 적절한 암호화 키로 갱신한다.

[0060] 도 4f는 수신기(410)가 CAM(405)와 CA 암호화 컴포넌트(425) 뿐만 아니라 DRM 라이센스(430)를 전송 스트림 또는, 이와 병행하여, 네트워크 운영자 또는 다른 신뢰있는 소스로부터 수신하는 또다른 실시예 및 구현예를 나타낸다. 이 라이센스(430)는 보호 컨텐츠(425)의 수신 동안, 이전, 이후에 수신될 수 있다. 그러나, DRM 라이센스(430)는 컨텐츠에 어느 정보 링크되어야 한다. 예를 들면, 컨텐츠는 둘 모두에 관련된 공통 식별자에 의해 DRM 라이센스(430)에 링크될 수 있다. 다르게는, 둘은 브리지 메커니즘 또는 메시지, 예를 들어, CAM(405)에 의해 링크될 수 있으며, 이는 라이센스(430)와 컨텐츠(425) 모두에 대한 식별자이다. 어느 경우에든, 일단 수신되면, 수신기(410)는 DRM 라이센스(430)와 보호 컨텐츠(425)를 데스티네이션 장치(420)에 전달한다. 이 구현예에서, 데스티네이션 장치(420)는 DRM 라이센스(430)를 사용하여 그 원래의 형태 대로 조건부 액세스 보호 컨

텐츠(425)를 소비한다.

[0061] 다른 예에서, CAM(405)은 수신기(410)에서 수신되고 데스티네이션 장치(420)에 전달될 수 있다. 이러한 경우, 데스티네이션 장치는 CAM(405)을 DRM 라이센스 서버 또는 서비스(미도시)에 제공할 수 있으며, 이 서버 또는 서비스는 그 후 DRM 라이센스(430; 한정된 사용 권한에 따라)를 생성하여 다시 데스티네이션 장치(420)에 전달할 수 있다. DRM 라이센스(430)는 DRM 서비스에서 DRM 라이센스를 생성할 때 조건부 액세스 컨텐츠와 사용 권한에 기초하여 조건부 액세스 컨텐츠(425) 또는 추후 생성된 보호 컨텐츠를 복호화하는데 사용될 수 있다. DRM 라이센스(430, 그리고 보호 컨텐츠)는 여기서 설명된 임의의 가능한 방법을 통해 직접 또는 간접으로 데스티네이션 장치(420)에 배포될 수 있다.

[0062] 도 4g는 전송 스트림을 통해 DRM 라이센스의 상술한 수신시에 대한 다른예를 나타낸다. 이 실시예에서, 수신기(410)는 ECM 및 EMM(405), CA 보호 컨텐츠(425) 및 제1 DRM 라이센스(430a)를 전송 스트림을 통해 수신하고, 그 후 전송 스트림은 데스티네이션 장치(420)에 전송된다. 그 후, 데스티네이션 장치는 그 보안 커널과 제1 DRM 라이센스(430a)를 사용하여 CA 보호 컨텐츠(425)를 복호화한다. 이 비암호화 컨텐츠는 그 후 재암호화되어 암호화 컨텐츠(435)를 생성한다. 따라서, 제1 DRM 라이센스(430a)에서의 CPI는 제2 DRM 라이센스(430b)를 생성하는데 사용될 수 있으며, 제2 DRM 라이센스(430b)는 제1 DRM 라이센스(430a)로부터 적어도 사용 권한을 포함할 수 있다. 또한, 제2 DRM 라이센스(430b)는 적절한 암호화 키로 갱신될 수 있다.

[0063] 도 4h는 도 4g에 대하여 상술한 바와 유사한 구현예를 나타낸다; 그러나, 수신기(410)는 CA 보호 컨텐츠(425)를 복호화하여 비암호화 컨텐츠(440)를 생성하고, 이 비암호화 컨텐츠(440)는 그 후 제1 DRM 라이센스(430a)와 함께 데스티네이션 장치(420)에 전송된다. 그 후, 데스티네이션 장치(420)는 암호화 컨텐츠(435)를 생성하고 또한 제2 DRM 라이센스(430b)를 대응 갱신 키를 사용하여 생성한다.

[0064] 또다른 실시예에서, 도 4i는 CA 정보가 패키지되어 데스티네이션 장치(420)에 전송되는 방식을 나타낸다. 이 구현예와 실시예에서, 수신기(410)는 CAM(405)과 보호 컨텐츠(425)를 수신하고, 이를 패키지 데이터(445)로서 패키지하며, 그 후, 데스티네이션 장치(420)에 전송된다. 이 패키지된 데이터는, 예를 들어, CPI 정보와 적절한 DRM 라이센스(430)를 생성하기에 충분한 데스티네이션 장치(420)에 의해 이해되는 다른 정보를 포함할 수 있다.

[0065] 다음은 데스티네이션 장치(420)가 패키지 데이터(445)를 사용하여 적절한 DRM 컨텐츠 라이센스(430)를 생성하고 그 후 컨텐츠(425, 435)를 소비하는 방식을 나타낸다. 예를 들면, 도 4j에서 나타낸 바와 같이, 데스티네이션 장치(420)는 다른 데이터 중에서 ECM 및 EMM(405)을 포함하는 패키지 데이터(445)를 수신한다. CA 보호 컨텐츠(435)는 수신기(410)에 의해 데스티네이션 장치(420)에 전송될 수 있다. 그 후, 데스티네이션 장치(420)는 패치지 데이터(445)에 전송되거나 원격 소스(미도시)로부터 수신되어, 또는 데스티네이션 장치(420)에 알려진 CPI 정보를 사용하여 컨텐츠 라이센스(430)를 생성한다. 또한, 데스티네이션 장치(420)는 CA 보호 컨텐츠(425)를 복호화하는데 사용되는 CW 키로 DRM 컨텐츠 라이센스(430)를 갱산할 수 있으며, 또는 다르게는, 보호 컨텐츠(425)를 복호화하고 DRM 키를 사용하여 재암호화하여 암호화된 컨텐츠(435)를 생성하고 이에 따라 DRM 라이센스(430)를 갱신한다.

[0066] 도 4k는 수신기(425)와, 다른 정보 중에서 CAM(405)과 CA 보호 컨텐츠(425)를 포함하는 패키징 데이터(445)의 다른 예를 나타낸다. 데스티네이션 장치(420)는 패키지 데이터(445)의 처리 방식을 인지하며 이와 CPI 등의 다른 정보를 사용하여 DRM 라이센스(430)와 적절한 DRM 보호 컨텐츠(435)를 생성할 수 있다. 유사하게, 도 4l은 조건부 액세스 보안 장치(410)가 적절한 ECM 및 EMM(405)과 CA 보호 컨텐츠(425)를 수신하여 적절한 CPI(415)와 CA 보호 컨텐츠(425)를 포함하는 패키지 데이터(445)를 생성하고, 이를 데스티네이션(420)에 전송하며, 데스티네이션 장치(420)는 그 후 적절한 컨텐츠 라이센스(430)를 생성하고 상술한 다양한 방식에 따라 컨텐츠를 소비한다.

[0067] 또한, 본 발명은 평션 단계 및/또는 비평션 동작을 포함하는 방법으로 나타낼 수 있다. 다음은 본 발명을 실시할 때 수행될 수 있는 동작 및 단계의 설명이다. 통상, 평션 단계는 달성될 수 있는 결과로 본 발명을 나타내지만, 비평션 동작은 특정 결과를 달성하는 보다 구체적인 동작을 나타낸다. 평션 단계 및 비평션 동작이 설명되고 특정 순서로 청구되지만, 본 발명은 임의의 특정 순서 또는 동작 및/또는 단계의 조합에 반드시 한정되는 것은 아니다.

[0068] 도 5는, 컨텐츠가 상이한 컨텐츠 보호 방식으로 발생되었지만, 컨텐츠 보호 방식에 의해 한정된 사용 권한에 따라 컨텐츠를 소비하기 위해 컨텐츠 라이센스를 생성하는데 사용되는 단계 및 동작의 일 예를 나타낸다. 도시한

바와 같이, 조건부 액세스 보호 컨텐츠와 컨텐츠 보호 정보는 동작 510 및 520에서 각각 수신된다. 조건부 액세스 보호 컨텐츠는 복수의 수신기에 브로드캐스트되어 복수의 간헐 갱신 키에 의해 복호화된다. 또한, 컨텐츠 보호 정보는 조건부 액세스 보호 컨텐츠에 관련된 사용 권한을 결정, 관리 및 행사하는데 사용되는 정보를 포함한다.

[0069] 도 5에 도시한 바와 같이, 사용 권한을 결정하는 단계(535)는 CA 컨텐츠 보호 정보를 해석하는 동작(530)을 포함한다. 사용 권하는 컨텐츠 제공자에 의해 한정되며 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 조건 및 방식을 규정한다.

[0070] 디지털 권한 관리 키를 제공하는 단계(545)는 데스티네이션 장치 내에서 디지털 권한을 행사하는 데 사용되는 컨텐츠 라인센스를 제공하는 동작(540)을 포함할 수 있다. 물론, 라이센스 내의 정보는 해석된 조건부 액세스 컨텐츠 보호 정보에 기초하고 사용 권한에 따른다.

[0071] 상술한 바와 같이, 두개의 보안 커널, 즉, 수신 장치와 데스티네이션 장치는, 여러 방식으로 저장될 수 있는 비밀 정보를 통해 결합될 수 있다. 이와 같이, 상술한 단계 및 동작은 데스티네이션 장치가 조건부 액세스 보호 컨텐츠의 수신기와 데스티네이션 장치 사이에 보안 통신 채널을 설정하는 데 있어 신뢰 장치임을 인증하는 동작을 포함한다. 또한, 상술한 바와 같이, 컨텐츠 보호 정보가 해석되고 수신되며, 컨텐츠 라이센스가 생성되는 위치는 상술한 구현예 중 임의의 하나 이상에 따라 변할 수 있다.

[0072] 본 발명의 다른 실시예에 따라 그리고 도 6에 도시한 바와 같이, 발생한 보호 방식과 상이한 컨텐츠 보호 방식 내에서 사용권한을 한정하는 라이센스를 사용하여 보호 컨텐츠를 소비하는 방법이 이용가능하다. 프로세스는 복수의 수신기에 의해 브로드캐스트되고 복수의 간헐 갱신 키에 의해 암호화되는 조건부 액세스 보호 컨텐츠를 수신한다(610). 또한, 조건부 액세스 보호 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 조건 및 방식을 규정하는 정보를 포함하는 디지털 권한 라이센스를 수신하는 동작(620)이 수행된다. 또한, 디지털 권한 라이센스는 복수의 간헐 갱신 키 중 적어도 일부를 포함한다. 마지막으로, 디지털 권한 라이센스는 디지털 권한 보호 방식을 사용하는 데스티네이션 장치에서 조건부 액세스 보호 컨텐츠를 복호화하여 컨텐츠를 소비하는 데 사용될 수 있다(630).

[0073] 데스티네이션 장치는 추후, 컨텐츠가 데스티네이션 장치에서 소비될 수 있는 조건 및 방식을 한정하는 사용 권한에 따라 하나 이상의 디지털 권하나 관리 키를 사용하여 복호화된 조건부 액세스 보호 컨텐츠를 암호화할 수 있다. 다른 실시예에서는 사용 권한이 수신 장치 내에서 보안 장치에 한정되는 디폴트 값이다. 다르게는, 사용 권하는 데스티네이션 장치 내에서 보안 라이브러리 내에 한정되는 디폴트 값일 수 있다. 또한, 사용 권한은 수신 장치와 데스티네이션 장치로부터 분리된 장치 내에 한정된 디폴트 값일 수 있다.

[0074] 또한, 본 발명의 실시예들은 컴퓨터 실행가능 명령 또는 데이터 구조를 갖거나 반송하는 컴퓨터 판독가능 매체를 포함한다. 이러한 컴퓨터 판독가능 매체는 범용 컴퓨터 또는 특정 목적 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 예를 들면 -한정하는 것이 아님-, 이러한 컴퓨터는 RAM, ROM, EEPROM, CD-ROM, 또는 다른 광 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기 스트로지 장치, 또는 컴퓨터 실행가능 명령 의 형태로서 원하는 프로그램 코드 수단을 반송하거나 저장하는데 사용될 수 있고 범용 또는 특정 목적 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 정보가 네트워크 또는 다른 통신 접속(유선, 무선, 또는 유선과 무선의 조합) 상으로 전송 또는 제공되는 경우, 컴퓨터는 이러한 접속은 컴퓨터 판독가능 매체로서 적절하게 간주한다. 따라서, 임의의 이러한 접속은 컴퓨터 판독가능 매체로 적절하게 지정된다. 상기의 것의 조합은 컴퓨터 판독가능 매체의 범위 내에서 또한 포함되어야 한다. 컴퓨터 실해가능 명령은, 예를 들면, 범용 컴퓨터, 특정 목적 컴퓨터, 또는 특정 목적 처리 장치가 특정 펑션 또는 펑션 그룹을 수행하게 하는 명령 및 데이터를 포함한다.

[0075] 도 7과 이하의 설명은 본 발명이 구현될 수 있는 적절한 컴퓨팅 장치의 간단하고 일반적인 예를 제공하려는 것이다. 비록 필수적인 것은 아니지만, 본 발명은 네트워크 환경에서 컴퓨터에 의해 실행되는 프로그램 모듈 등의 컴퓨터 실행가능 명령의 일반적인 경우에 대하여 나타낸다. 통상, 프로그램 모듈은 특정 작업을 수행하거나 특정 추상 데이터형을 구현하는 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조를 포함한다. 데이터 구조와 결합된 컴퓨터 실행가능 명령과 프로그램 모듈은 여기서 개시된 방법의 단계를 실행하는 프로그램 코드 수단의 예를 나타낸다. 이러한 실행가능 명령 또는 관련 데이터 구조의 특정 시퀀스는 이러한 단계로 기재된 펑션을 구현하는 대응 동작의 예를 나타낸다.

[0076] 본 발명은 개인용 컴퓨터, 핸드헬드 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 또는 프로그래머블 소

비자 전자제품, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터 등을 포함하는 많은 유형의 컴퓨터 시스템 구성으로 네트워크 컴퓨팅 환경에서 실시될 수 있다. 본 발명은 또한 통신 링크를 통해 연결(유선 링크, 무선 링크, 또는 유선 및 무선 링크의 조합에 의해)되는 로컬 및 원격 처리 장치에 의해 작업이 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 스토리지 장치에 위치할 수 있다.

[0077] 도 7을 참조하면, 본 발명을 구현하는 예시적인 시스템은, 처리부(720), 시스템 메모리(722), 및 시스템 메모리(722)를 포함하는 여러 시스템 컴포넌트를 처리부(721)에 결합하는 시스템 버스(723)를 포함하는 종래의 컴퓨터(720)의 형태의 범용 컴퓨팅 장치를 포함한다. 시스템 버스(723)는 메모리 버스 또는 메모리 컨트롤러, 주변 버스, 및 임의의 다양한 버스 구조를 사용하는 로컬 버스 중 임의 유형의 것일 수 있다. 시스템 메모리는 판독 전용 메모리(ROM; 724)와 랜덤 액세스 메모리(RAM; 725)를 포함한다. 기본 입출력 시스템(BIOS; 726)은 시동시와 같이 컴퓨터(720) 내에서 요소들 간의 정보 전송을 지원하는 기본 루틴을 포함하며 ROM(724) 내에 저장될 수 있다.

[0078] 컴퓨터(720)는 또한 자기 하드 디스크(739)로부터 판독하고 이에 기입하는 자기 하드 디스크 드라이브(727), 분리형 자기 디스크(729)로부터 판독하고 이에 기입하는 자기 디스크 드라이브(728), 및 CD-ROM 또는 다른 광 매체 등과 같이 분리형 광 디스크(731)로부터 판독하고 이에 기입하는 광 디스크 드라이브(730)를 포함할 수 있다. 자기 하드 디스크 드라이브(727), 자기 디스크 드라이브(728), 및 광 디스크 드라이브(730)는 하드 디스크 드라이브 인터페이스(732), 자기 디스크 드라이브 인터페이스(733), 및 광 드라이브 인터페이스(734)에 의해 각각 접속된다. 이 드라이브 및 관련 컴퓨터 판독가능 매체는 컴퓨터(720)에 대한 컴퓨터 실행가능 명령, 데이터 구조, 프로그램 모듈 및 기타 데이터의 비휘발성 스토리지를 제공한다. 여기서 설명한 예시적인 환경은 자기 하드 디스크(739)를 사용하지만, 분리형 자기 디스크(729) 및 분리형 광 디스크(731), 및 자기 카세트, 플래시 메모리 카드, 디지털 다기능 디스크, 베르누이 카트리지, RAM, ROM, 등의 다른 유형의 컴퓨터 판독가능 매체가 데이터 저장을 위해 사용될 수 있다.

[0079] 운영 체계(735), 하나 이상의 애플리케이션 프로그램(736), 다른 프로그램 모듈(737), 및 프로그램 데이터(738)를 비롯하여 하나 이상의 프로그램 모듈을 포함하는 프로그램 코드 수단이 하드 디스크(739), 자기 디스크(729), 광 디스크(731), ROM(724) 또는 RAM(725) 상에 저장될 수 있다. 사용자는 키보드(740), 포인팅 장치(742), 또는 마이크로폰, 조이 스틱, 게임 패드, 위성 접시, 스캐너 등과 같은 다른 입력 장치(미도시)를 통해 컴퓨터(720)에 명령 및 정보를 입력할 수 있다. 이들 및 다른 입력 장치는 종종 시스템 버스(723)에 결합된 병렬 포트 인터페이스(746)를 통해 처리부(721)에 접속된다. 다르게는, 입력 장치는 병렬 포트, 게임 포트 또는 범용 직렬 버스(USB) 등의 다른 인터페이스에 의해 접속될 수 있다. 모니터(747) 또는 다른 디스플레이 장치가 또한 비디오 어댑터(748) 등의 인터페이스를 통해 시스템 버스(723)에 접속된다. 모니터에 더하여, 개인용 컴퓨터는 스피커와 프린터 등의 다른 주변 출력 장치(미도시)를 통상 포함한다.

[0080] 컴퓨터(720)는 원격 컴퓨터(749a 및 749b)와 같이 하나 이상의 원격 컴퓨터에 대한 논리적 접속을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(749a 및 749b)는 다른 개인용 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 다른 공통 네트워크 노드일 수 있으며, 단지 메모리 스토리지 장치(750a 및 750b)와 관련 애플리케이션 프로그램(736a 및 736b)이 도 7에 도시되었지만 통상 컴퓨터(720)에 대하여 상술한 많은 또는 모든 요소를 포함한다. 도 7에 도시된 논리적 접속은 한정이 아닌 예를 들면 여기에 제공된 근거리 네트워크(LAN; 751)와 광역 네트워크(WAN; 752)를 포함한다. 이러한 네트워킹 환경은 사무실 또는 범사내망 컴퓨터 네트워크, 인트라넷 및 인터넷에서 흔히 볼 수 있다.

[0081] LAN 네트워킹 환경에서 사용되는 경우, 컴퓨터(720)는 네트워크 인터페이스 또는 어댑터(753)를 통해 로컬 네트워크(751)에 접속된다. WAN 네트워킹 환경에서 사용되는 경우, 컴퓨터(720)는 모뎀(754), 무선 링크, 또는 인터넷 등과 같이 광역 네트워크(752)를 통해 통신을 설정하는 다른 수단을 포함할 수 있다. 모뎀(754)은 내장형이거나 외장형일 수 있으며, 직렬 포트 인터페이스(746)를 통해 시스템 버스(723)에 접속된다. 네트워크 환경에서, 컴퓨터(720)에 대하여 도시된 프로그램 모듈 또는 그 일부는 원격 메모리 스토리지 장치 내에 저장될 수 있다. 도시된 네트워크 접속은 예시적이며 광역 네트워크(752) 상에서 통신을 설정하는 다른 수단이 사용될 수 있음이 이해될 것이다.

[0082] 본 발명은 그 취지 및 기본 특성에서 벗어나지 않으면서 다른 특정 형태로 구현될 수 있다. 설명된 실시예는 모든 측면에서 단지 예시이며 한정하려는 것은 아니다. 따라서, 본 발명의 범위는 상기 설명이 아닌 첨부한 청구항으로 나타낸다. 청구항의 균등한 의미 및 범위에 속하는 모든 변화가 이 범위 내에 포함되어야 한다.

발명의 효과

[0083] 상술한 본 발명에 따르면, 두개의 상이한 보호 방식을 인터페이스할 수 있으며, 특히, 컨텐츠가 상이한 컨텐츠 보호 방식에서 발생하더라도, 컨텐츠 보호 방식에 의해 한정되는 사용 권한에 따라 컨텐츠을 소비할 수 있다.

도면의 간단한 설명

[0001] 도 1은 종래의 조건부 액세스 컨텐츠 보호 방식의 일 예를 나타내는 도면.

[0002] 도 2는 종래의 디지털 권한 관리 시스템 컨텐츠 보호 방식의 일 예를 나타내는 도면.

[0003] 도 3은 조건부 액세스 패키징 방식 대 디지털 권한 관리 패키징 방식의 일대일 비교를 나타내는 도면.

[0004] 도 4a 내지 도 41은 실시예들에 따라 조건부 액세스 컨텐츠 보호 방식에서 디지털 권한 관리 컨텐츠 보호 방식으로 변환하는 다양한 구현을 나타내는 도면.

[0005] 도 5는 실시예들에 따라 컨텐츠 라이센스를 생성하는 방법에 대한 동작 및 단계의 예를 나타내는 도면.

[0006] 도 6은 본 발명의 실시예들에 따라 디지털 권한 라이센스를 사용하여 조건부 액세스 보호 컨텐츠를 소비하는 방법에 대한 동작의 예를 나타내는 도면.

[0007] 도 7은 본 발명의 적합한 운영 환경을 제공하는 예시적인 시스템을 나타내는 도면.

[0008] <도면의 주요 부분에 대한 부호의 설명>

[0009] 205: 컨텐츠 소유자

[0010] 210: 비밀 및 규칙

[0011] 215: 라이센스 발행자

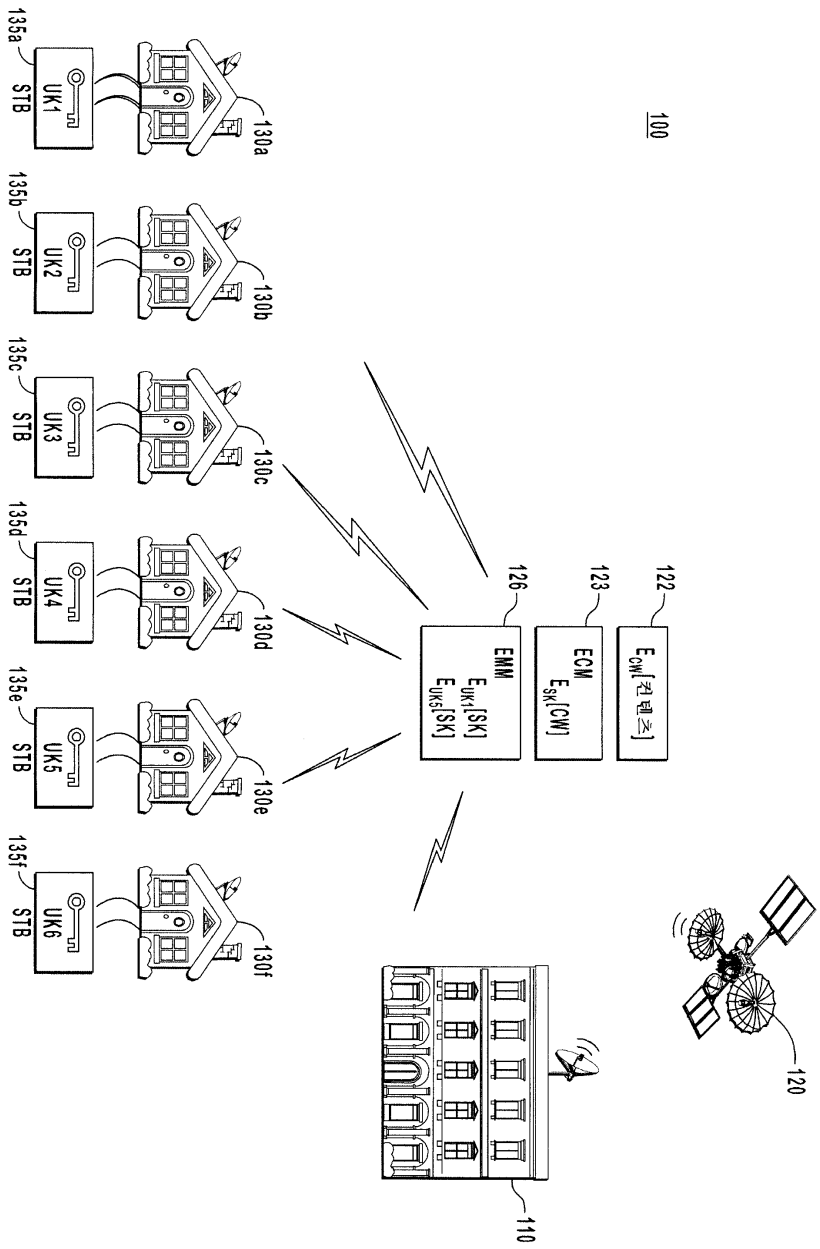
[0012] 220: 컨텐츠 요청/ID 토큰

[0013] 230: 고객 장치

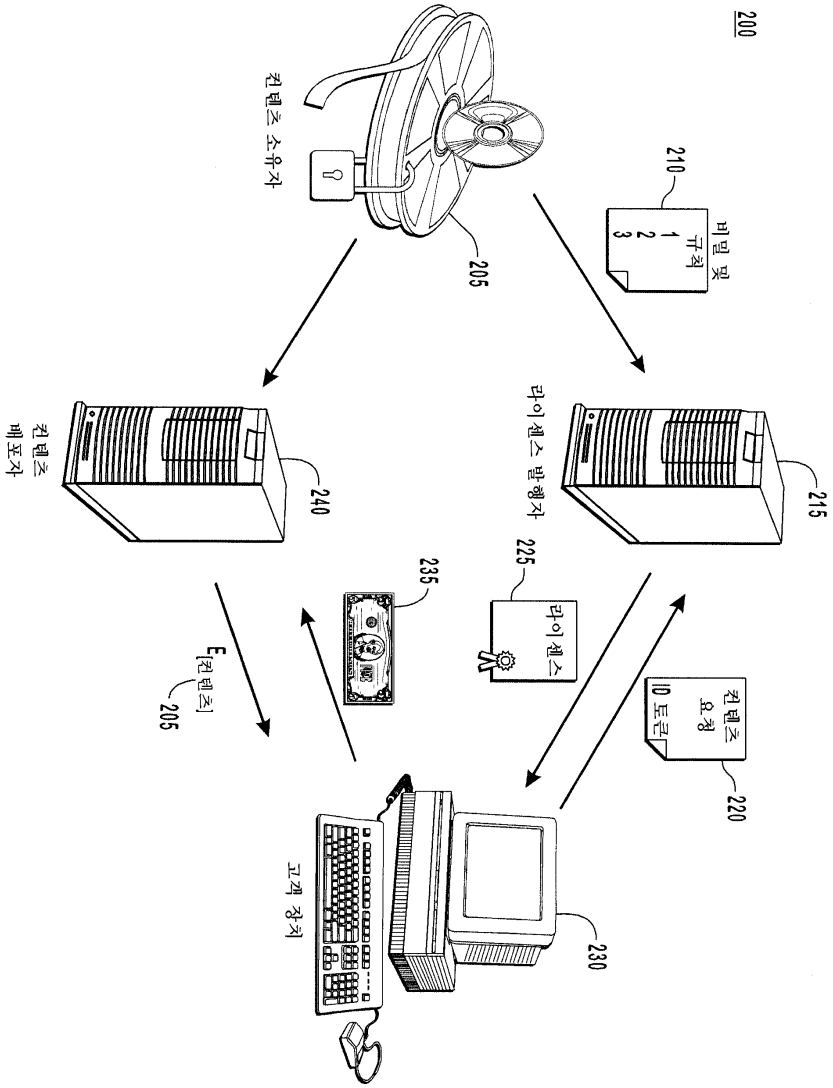
[0014] 240: 컨텐츠 배포자

도면

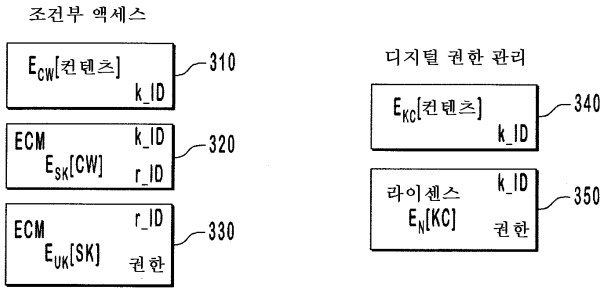
도면1


100
135a
STB
UK1
130a
135b
STB
UK2
130b
135c
STB
UK3
130c
135d
STB
UK4
130d
135e
STB
UK5
130e
135f
STB
UK6
130f
126
EMM
$E_{UK1}[SK]$
$E_{UK6}[SK]$
123
ECM
$E_{SK}[CW]$
122
E_{CW}[컨텐츠]
110
120

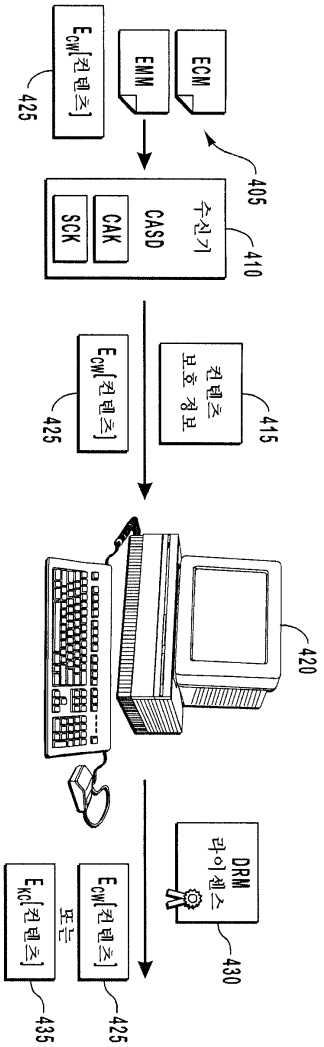
도면2


200
컨텐츠 소유자
205
210
비밀 및 규칙
1
2
3
컨텐츠 배포자
240
라이센스 발행자
215
235
225
라이센스
E[컨텐츠]
205
컨텐츠 요청 ID 토큰
220
고객 장치
230

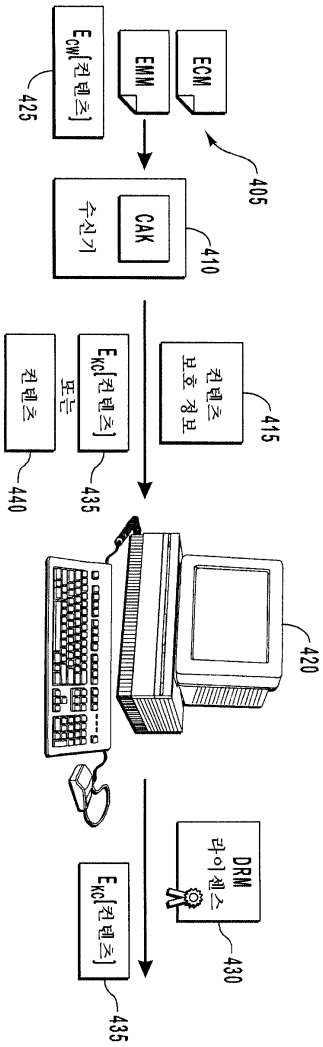
도면3


조건부 액세스
E_{CW}[컨텐츠]
k_ID
310
ECM
E_{SK}[CW]
k_ID
r_ID
320
ECM
E_{UK}[SK]
r_ID
권한
330
디지털 권한 관리
E_{KC}[컨텐츠]
k_ID
340
라이센스
E_N[KC]
k_ID
권한
350

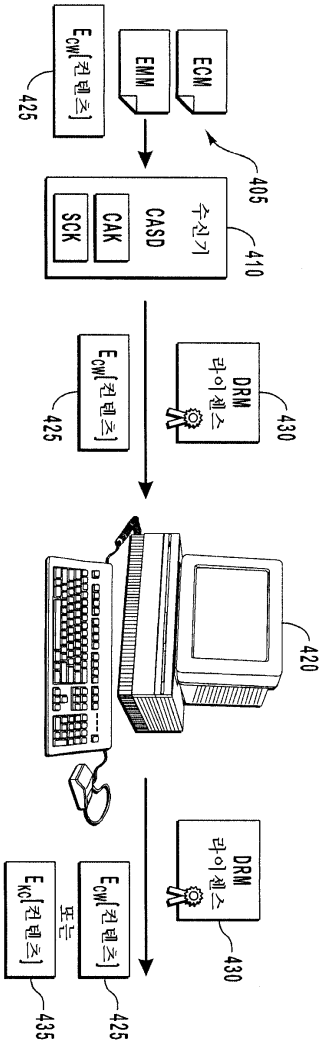
도면4a


ECM
EMM
E_{CW}[컨텐츠]
425
405
수신기
CASD
CAK
SCK
410
컨텐츠 보호 정보
415
E_{CW}[컨텐츠]
425
420
DRM 라이센스
430
E_{CW}[컨텐츠]
425
또는
E_{KC}[컨텐츠]
435

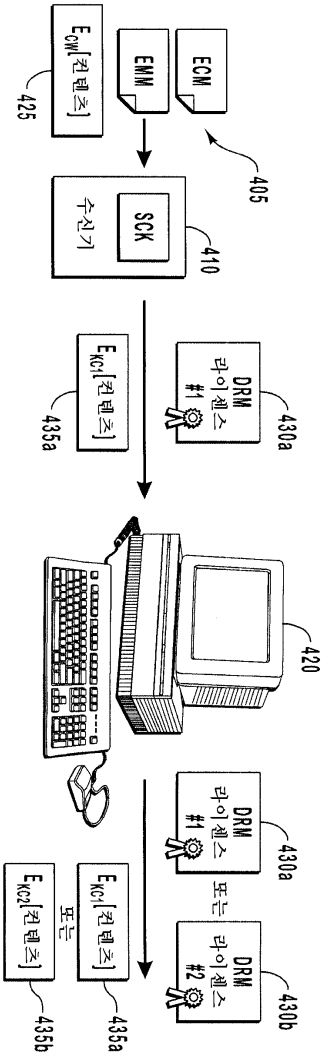
도면4b


ECM
EMM
E_{CW}[컨텐츠]
405
CAK
수신기
410
컨텐츠
보호 정보
415
E_{KC}[컨텐츠]
또는
컨텐츠
435
440
420
DRM
라이센스
430
E_{KC}[컨텐츠]
435

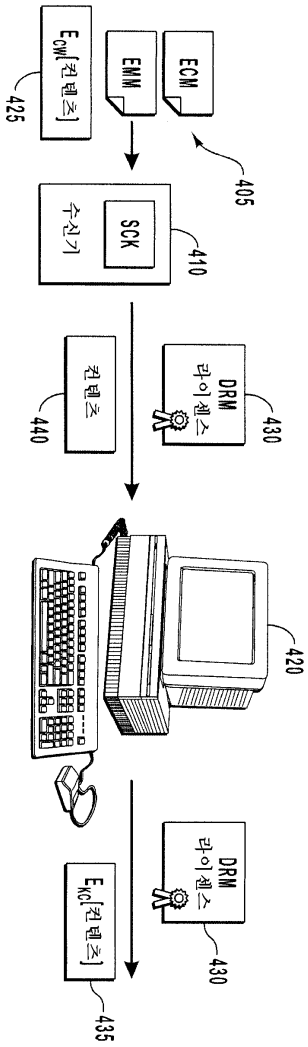
도면4c


ECM
EMM
E_{CW}[컨텐츠]
405
수신기
CASD
CAK
SCK
410
DRM
라이센스
430
E_{CW}[컨텐츠]
425
420
DRM
라이센스
430
E_{CW}[컨텐츠]
425
또는
E_{KC}[컨텐츠]
435

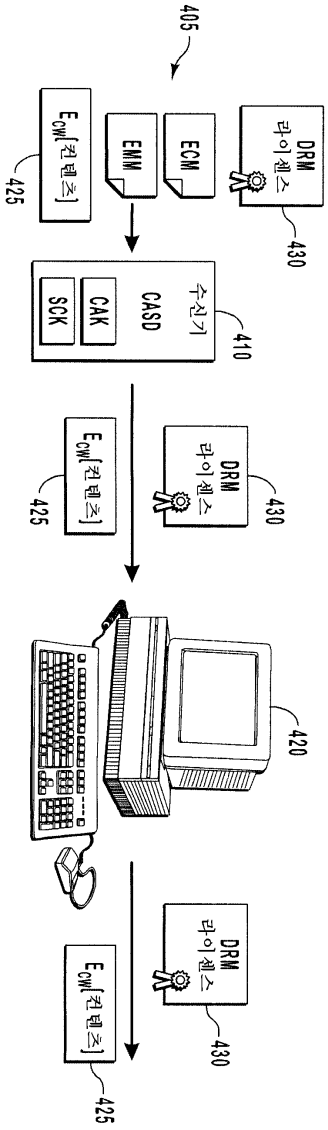
도면4d


ECM
EMM
405
SCK
수신기
410
DRM
라이센스
#1
430a
DRM
라이센스
#2
430b
또는
420
435a
435b
425

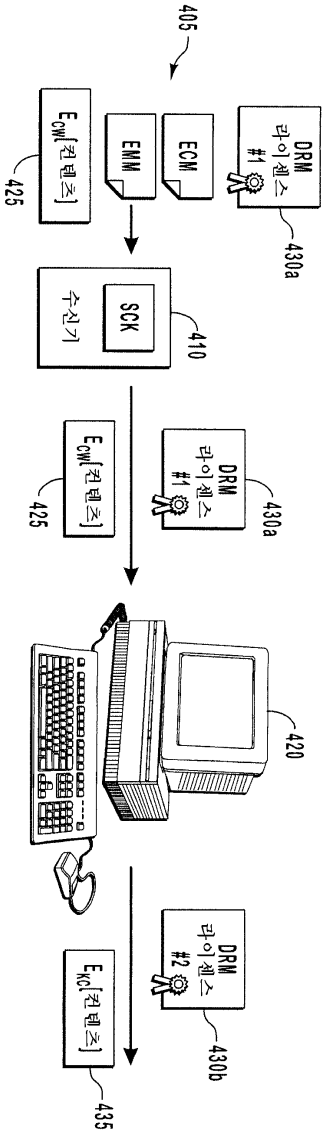
도면4e


ECW[컨텐츠]
425
EMM
ECM
405
수신기
SCK
410
컨텐츠
440
DRM
라이센스
430
420
DRM
라이센스
430
EKC[컨텐츠]
435

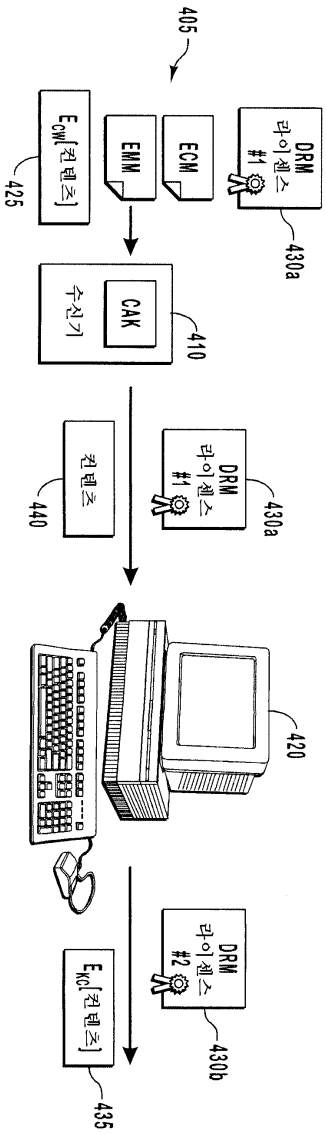
도면4f



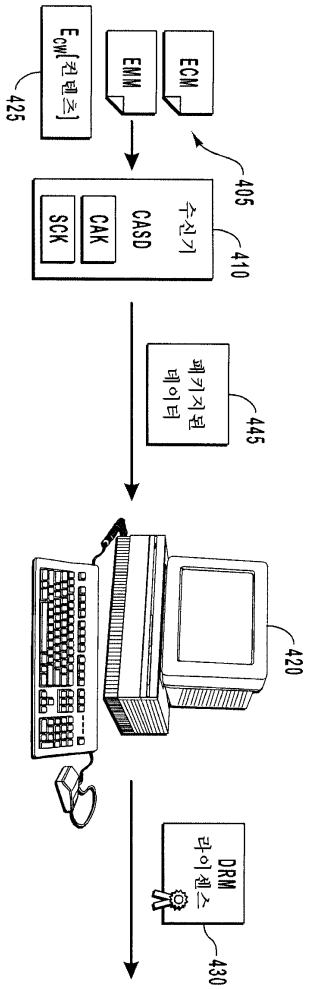
도면4g


405
ECM
EMM
DRM 라이센스 #1
430a
E_{CW}[컨텐츠]
425
수신기
SCK
410
E_{CW}[컨텐츠]
425
DRM 라이센스 #1
430a
420
E_{KCI}[컨텐츠]
435
DRM 라이센스 #2
430b

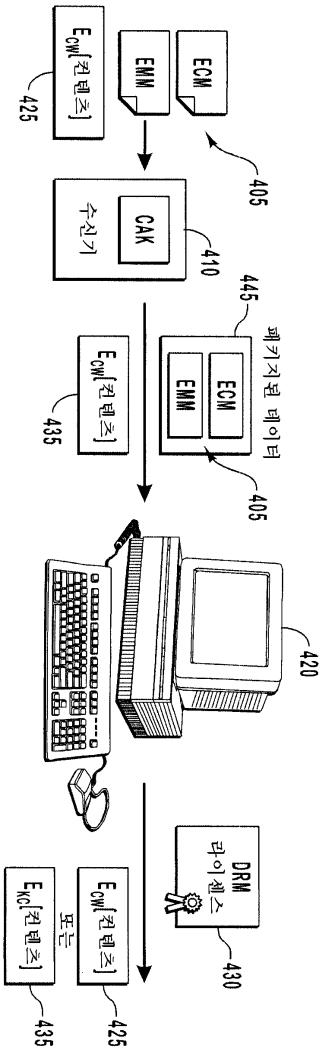
도면4h


405
DRM 라이센스 #1
ECM
EMM
E_{CW}[컨텐츠]
425
430a
수신기
CAK
410
컨텐츠
440
DRM 라이센스 #1
430a
420
DRM 라이센스 #2
E_{KC}[컨텐츠]
430b
435

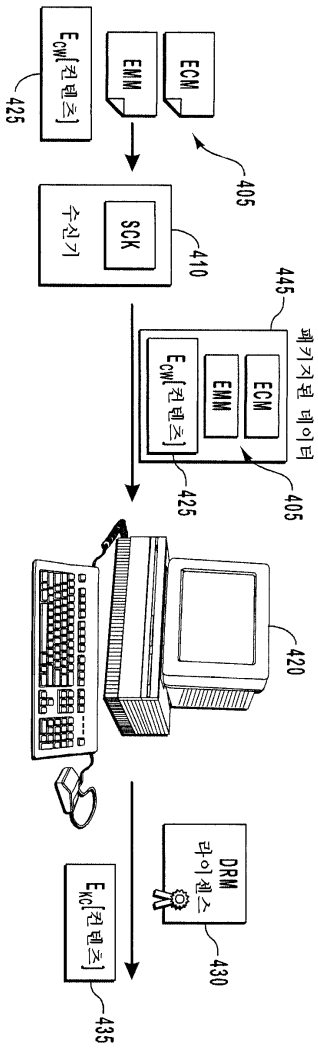
도면4i


ECM
EMM
E_{CW}(컨텐츠)
425
405
수신기
CASD
CAK
SCK
410
패키지된 데이터
445
420
DRM 라이센스
430

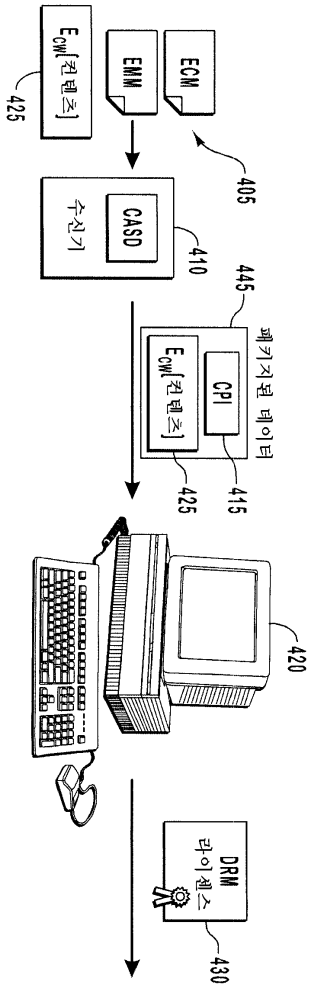
도면4j


ECM
EMM
E_{CW}[컨텐츠]
405
425
CAK
수신기
410
445
패키지된 데이터
ECM
EMM
E_{CW}[컨텐츠]
405
435
420
DRM
라이센스
430
E_{CW}[컨텐츠]
425
E_{KC}[컨텐츠]
또는
435

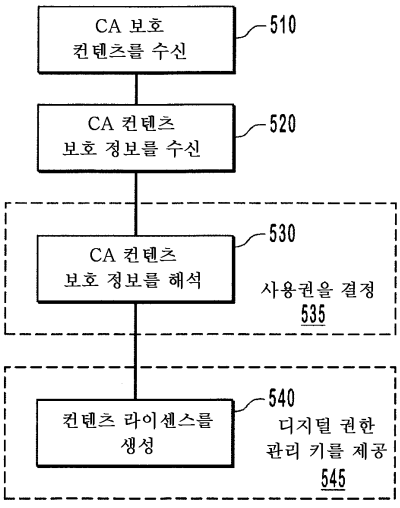
도면4k


E_{CW}[컨텐츠]
425
EMM
ECM
405
수신기
SCK
410
445
패키지된 데이터
E_{CW}[컨텐츠]
EMM
ECM
425
405
420
DRM
라이센스
430
E_{KC}[컨텐츠]
435

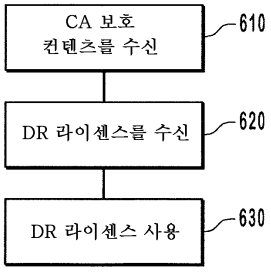
도면41


ECW[컨텐츠]
425
EMM
ECM
405
수신기
CASD
410
445
패키징된 데이터
ECW[컨텐츠]
CPI
425
415
420
DRM
라이센스
430

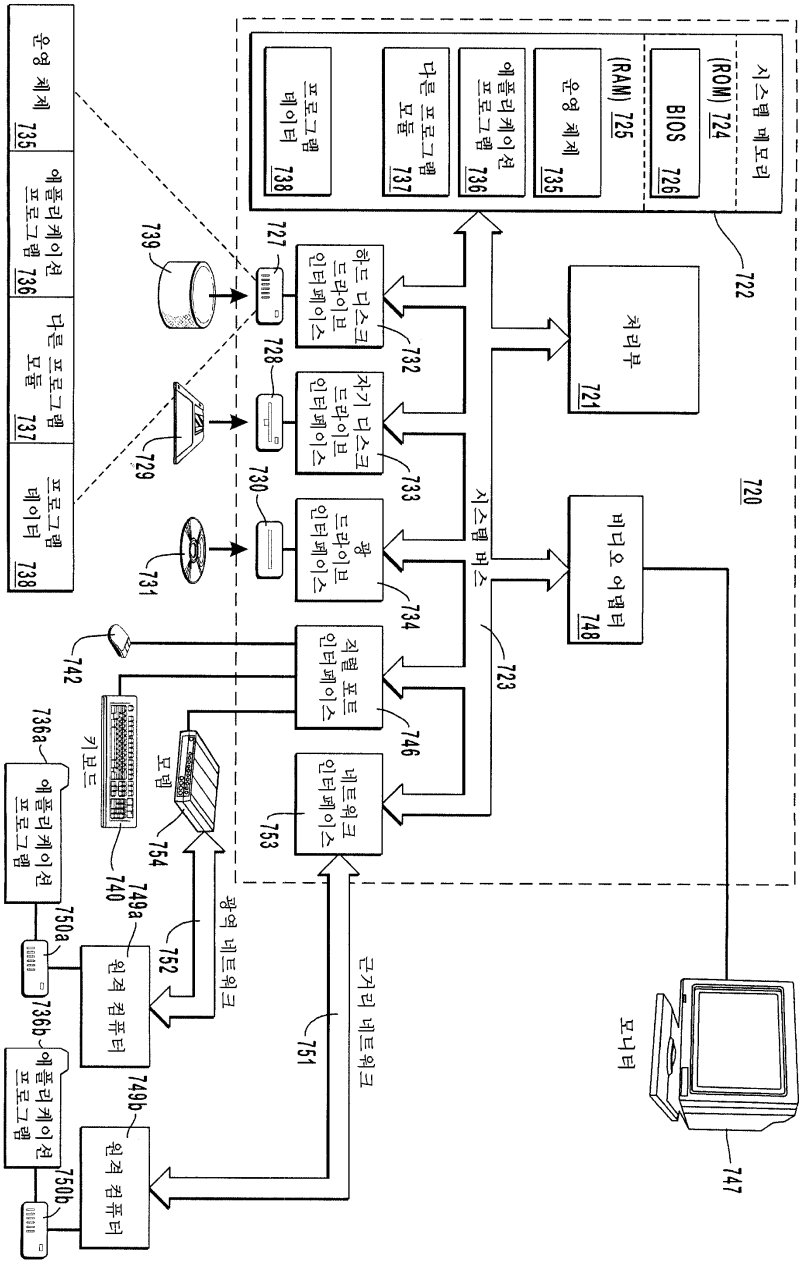
도면5


CA 보호
컨텐츠를 수신
510
CA 컨텐츠
보호 정보를 수신
520
CA 컨텐츠
보호 정보를 해석
530
사용권을 결정
535
컨텐츠 라이센스를
생성
540
디지털 권한
관리 키를 제공
545

도면6


CA 보호
컨텐츠를 수신
610
DR 라이센스를 수신
620
DR 라이센스 사용
630

도면7


운영 체제 735
에플리케이션 프로그램 736
다른 프로그램 모듈 737
프로그램 데이터 738
시스템 메모리 (ROM) 724
BIOS 726
(RAM) 725
운영 체제 735
에플리케이션 프로그램 736
다른 프로그램 모듈 737
프로그램 데이터 738
722
처리부 721
720
비디오 어댑터 748
시스템 버스 723
하드 디스크 드라이브 인터페이스 727
자기 디스크 드라이브 인터페이스 728
광 드라이브 인터페이스 730
직렬 포트 인터페이스 734
네트워크 인터페이스 753
732
733
739
729
731
742
키보드 740
모뎀 754
736a
에플리케이션 프로그램
750a
736b
에플리케이션 프로그램
750b
원격 컴퓨터 749a
원격 컴퓨터 749b
752
광역 네트워크
751
근거리 네트워크
모니터 747
746