(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04N 7/16 (2006.01)
H04L 12/22 (2006.01)
H04L 12/18 (2006.01)

(11) 공개번호 10-2006-0116967
(43) 공개일자 2006년11월16일

(21) 출원번호 10-2005-0039627
(22) 출원일자 2005년05월12일

(71) 출원인 에스케이 텔레콤주식회사
서울 중구 을지로2가 11번지

(72) 발명자 김도완
경기도 고양시 일산구 백석동 1300 현대밀라트 2차 B동 813호
오현준
서울특별시 강남구 일원동 629-15번지
김종호
서울특별시 종로구 무악동 82번지 현대아파트 111동 1003호
박재범
서울특별시 서초구 우면동 동양고속아파트 102동 505호
임재철
서울특별시 동작구 상도4동 경향렉스빌 101동 902호
최진승
서울특별시 노원구 월계3동 한진그랑빌아파트 120동 402호
나동원
경기도 성남시 분당구 구미동 무지개마을LG아파트 214동 804호
임종태
경기도 성남시 분당구 이매동 동신아파트 304-502호
이명성
서울특별시 강남구 도곡동 964번지 현대그린아파트 1605호

(74) 대리인 남상선

심사청구 : 있음

(54) 방송 컨텐츠 보호 시스템 및 그 방법

요약

수신제한 시스템 및 디지털 권한 관리시스템을 이용하여 방송 컨텐츠를 보호하는 방송 컨텐츠 보호 시스템 및 그 방법이 개시된다. 이를 위하여, CAS(Conditional Access System)서버가 방송 컨텐츠를 스크램블 한 후 ECM과 함께 IB로 브로드캐스팅 또는 멀티캐스팅 하고, EMM을 대역 내/외 채널을 통해 브로드캐스팅 또는 유니캐스팅 하는 단계; 제1클라이언트 단말기가 상기 방송 컨텐츠를 수신하여 디스크램블한 후, 상기 방송 컨텐츠를 재생/저장하는 단계; 상기 제1클라이언트가 합법적 배포(Super-distribution)를 위하여 DRM(Digital Rights Management)패키징을 수행하여, DRM컨텐츠로 변환하는 단계; 상기 제1클라이언트 단말기가 유/무선 망을 통해 상기 DRM컨텐츠를 적어도 하나 이상의 제2 클라이언트 단

말기로 합법적으로 배포(super-distribution)하는 단계; 및 상기 제2클라이언트 단말기가 DRM서버로부터 RO(Rights Object)를 구매하여 상기 DRM컨텐츠를 재생하는 단계를 포함함으로써, 상기 방송 컨텐츠를 무분별하게 배포되더라도 방송사 측의 허가 없는 재생(Play)을 방지할 수 있다.

대표도

도 3

색인어

CAS, DRM, 방송 컨텐츠, DCP

명세서

도면의 간단한 설명

도1 은 본 발명에 따른 방송 컨텐츠 보호 시스템의 개략적인 구성을 나타내는 도면.

도2는 본 발명의 바람직한 실시예에 따른 클라이언트 단말기의 구성을 나타내는 도면.

도3은 본 발명의 바람직한 실시예에 따른 방송 컨텐츠의 상태 천이(transition)과정을 나타내는 도면.

도4는 본 발명의 바람직한 실시예에 따른 방송 컨텐츠 보호 시스템을 나타내는 구성도.

도5는 본 발명의 바람직한 실시예에 따른 방송 컨텐츠 보호 방법을 설명하기 위한 도면.

도6은 본 발명의 바람직한 실시예에 따른 CID의 구성을 나타내는 도면.

도7및 도8은 본 발명의 바람직한 실시예에 따른 CEK생성방법을 나타내는 도면.

도9는 본 발명의 바람직한 실시예에 따라 DCP에서 DCF를 형성하기 위한 헤더정보를 나타내는 도면.

도10은 본 발명의 바람직한 실시예에 따른 CEK, 컨텐츠 정보, 과금정보 요청/전달 과정을 나타내는 도면.

* 도면의 주요부분에 대한 부호설명*

100, 100A: 방송사서버 110: CIP서버

120: CAS서버 200, 300: 클라이언트 단말기

250: DCP 270: DRM 에이전트

400: CP/PP 500: DRM서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 컨텐츠 보호 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 수신제한 시스템 및 디지털 권한 관리시스템을 이용하여 방송 컨텐츠를 보호하는 방송 컨텐츠 보호 시스템 및 그 방법에 관한 것이다.

최근, 유/무선을 통해 자기 자신이 보유하는 디지털 컨텐츠를 다른 사용자에게 제공하고, 자기 자신이 보유하고 있지 않은 디지털 컨텐츠를 다른 사용자로부터 제공받음으로써, 복수의 사용자가 무료로 디지털 컨텐츠를 서로 교환/공유하는 시스템의 실현으로 인하여, 상기 디지털 컨텐츠 제작자와는 관련없이 무분별하게 유통되고 있다. 이에 따라, 상기 무분별한 유통을 차단하는 방안으로 DRM(Digital Rights Management)기술이 급속히 주목을 받고 있다.

일반적으로, 상기 디지털 컨텐츠는 제작/가공, 관리, 보호/보안, 전달/유통/결재/과금, 이용 등과 같은 라이프 사이클을 갖으며, 방송 컨텐츠의 경우에는 제작/가공, 전달, 과금에 사업자들의 초점이 맞추어져 있었으나, 방송 컨텐츠가 디지털화 되면서 보호/보안, 유통, 이용등에도 고려해야 하는 상황이다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 방송 컨텐츠에 수신제한 시스템(CAS) 및 디지털 권한관리(DRM) 시스템을 적용하여 상기 방송 컨텐츠의 무분별한 유통을 방지할 수 있는 방송 컨텐츠 보호 시스템 및 그 방법을 제공하는 데 있다.

또한, 본 발명의 다른 목적은 방송 컨텐츠에 수신제한 시스템(CAS) 및 디지털 권한관리(DRM) 시스템을 적용하여 상기 방송 컨텐츠를 무분별한 복제를 방지할 수 있는 방송 컨텐츠 보호를 위한 저장 방법을 제공하는 데 있다.

또한, 본 발명의 또 다른 목적은 상기 보호된 방송 컨텐츠를 정당한 권한을 얻어 언패키징할 수 있는 방송 컨텐츠 재생 방법을 제공하는 데 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여, 본 발명의 바람직한 실시예에 따른 방송 컨텐츠 보호 방법은, A) CAS서버가 방송 컨텐츠를 스크램블한 후 ECM과 함께 IB로 브로드캐스팅 또는 멀티캐스팅 하고EMM을 대역 내/외 채널을 통해 브로드캐스팅 또는 유니캐스팅 하는 단계; B) 제1클라이언트 단말기가 상기 방송 컨텐츠를 수신하여 디스크램블한 후, 상기 방송 컨텐츠를 재생/저장하는 단계; C) 상기 제1클라이언트가 합법적 배포(Super-distribution)를 위하여 DRM(Digital Rights Management)패키징을 수행하여, DRM컨텐츠로 변환하는 단계; D) 상기 제1클라이언트 단말기가 유/무선 망을 통해 상기 DRM컨텐츠를 적어도 하나 이상의 제2 클라이언트 단말기로 배포하는 단계; 및 E) 상기 제2클라이언트 단말기가 DRM 서버로부터 RO를 구매하여 상기 DRM컨텐츠를 재생하는 단계를 포함하는 것을 특징으로 한다.

또한, 본 발명의 바람직한 실시예에 따라, CAS서버가 방송 컨텐츠를 스크램블한 후 ECM과 함께IB로 브로드캐스팅 또는 멀티캐스팅 하고, EMM을 대역 내/외 채널을 통해 브로드캐스팅 또는 유니캐스팅 한 후, 제1클라이언트 단말기가 상기 방송 컨텐츠를 수신하여 상기 방송 컨텐츠를 저장하는 방법은, a) 상기 CAS서버로부터 전송된 방송 컨텐츠를 수신하여, 미리 저장된 가입자 키등를 통해 중간 키를 재생성하고, 상기 중간 키를 통해 CW(Control Word)를 복호한 후, 상기 CW를 통해 상기 방송 컨텐츠를 디스크램블 하는 단계; b) 상기 방송 컨텐츠의 EID(Event ID)를 기반으로 CID(Content ID)를 생성하는 단계; c) CAS서버로부터 전송된CW(Control Word) 및 중간 키를 기반으로 CEK(Content Encryption Key)를 생성하는 단계; d) 상기 CID와 CEK를 상기 EID를 기준으로 맵핑하는 단계; 및 e) 상기 CW 또는 CEK를 토대로 상기 방송 컨텐츠를 암호화하여 저장하는 단계를 포함하는 것을 특징으로 한다.

또한, 본 발명의 바람직한 실시예에 따라 DRM패키징된 방송 컨텐츠를 클라이언트 단말기에서 재생하는 방법은, 1) 상기 클라이언트 단말기가 CIP(Content Information Provider)에 RO(Rights Object)의 구매를 요구하는 단계; 2) 상기 CIP가 상기 클라이언트 단말기로부터 요청된 RO의 CID(Content ID)를 분석하여 EID(Event ID)를 추출한 후, 상기 EID에 따른 CEK(Content Encryption Key) 및 컨텐츠 정보를 상기 CAS(Conditional Access System)서버로 요청하는 단계; 3) 상기 CAS 서버가 상기 EID를 토대로 CEK, 컨텐츠 정보를 추출하여 상기 CIP를 통해 DRM(Digital Rights Management)서버로 전송하는 단계; 4) 상기 CIP가 상기 DRM서버와 클라이언트 단말기 사이에 ROAP(Rights Object Acquisition Protocol)를 기반으로 하는 세션을 설정해주는 단계; 및 5) 상기 클라이언트 단말기가 상기 설정된 세션을 통해 DRM서버로 RO를 요청/전송 받아 상기 방송 컨텐츠를 재생하는 단계를 포함하는 것을 특징으로 한다.

한편, 본 발명의 제1 실시예에 따른 방송 컨텐츠 보호 시스템은, 방송 컨텐츠를 브로드캐스팅 또는 멀티캐스팅 하고 CAS를 통해 시청권한을 제어하며, 합법적으로 배포(Super-distribution)된 상기 방송 컨텐츠의 재생을 위한 권리(Right)구매 요청이 있으면 해당 방송 컨텐츠에 대한 재생 권리를 발급하는 방송사서버; 및 상기 CAS를 통해 제어된 방송 컨텐츠를 재생하며, 상기 방송 컨텐츠를 DRM컨텐츠로 저장하고, 합법적 배포를 위한 DRM(Digital Rights Management) 패키징을

수행하며, 상기 방송사서버로 상기 DRM컨텐츠에 대한 권리(Right)구매를 요청한 후, 해당 DRM컨텐츠에 대한 권리(Right)를 발급받아 상기 DRM컨텐츠에 대응되는 방송 컨텐츠를 재생하는 클라이언트 단말기를 포함하는 것을 특징으로 한다.

또한, 본 발명의 제2 실시예에 따른 방송 컨텐츠 보호 시스템은, EMM(Entitlement Management Message)을 대역 내 및/또는 OOB을 통해 전송하고, 중간 키를 생성하여 CW(Control Word)를 암호화한 후 상기 CW를 ECM(Entitlement Control Message)에 포함시켜 IB을 통해 브로드캐스팅 또는 멀티캐스팅 하는 CAS(Conditional Access System)서버; 합법적으로 배포(super-distribution)된 방송 컨텐츠에 대한 RO(Rights Object)의 CID(Content ID)를 분석하여 EID(Event ID)를 추출하고, 상기 EID에 따른 CEK(Content Encryption Key) 및 컨텐츠 정보를 상기 CAS서버로 수신한 후, ROAP(Rights Object Acquisition Protocol) 설정을 위한 ROAP트리거 중계역할을 수행하는 CIP(Contents Information Provider); 브로드캐스팅 또는 멀티캐스팅된 방송 컨텐츠를 수신하여 디스플레이하고, 상기 방송 컨텐츠를 합법적 배포를 수행하기 위한 저장 및 DRM패키징을 수행하는 제1클라이언트 단말기; 상기 DRM패키징된 방송 컨텐츠를 합법적으로 배포 받아 저장하거나, RO를 구매하여 상기 방송 컨텐츠를 화면에 디스플레이 하는 제2클라이언트 단말기; 및 상기 제2클라이언트 단말기로부터의 RO 구매 요청에 대하여 소정 인증과정을 거친 후 RO를 발급 또는 다운로드해주는 DRM 서버를 포함하는 것을 특징으로 한다.

이하에서는, 첨부도면 및 바람직한 실시예를 참조하여 본 발명을 상세히 설명한다. 도면상에서 동일 또는 유사한 구성요소에 대하여는 동일한 참조번호를 부여하였으며, 이하에서 자주 설명될 약어들은 다음과 같은 풀 네임을 갖는다.

CAS(Conditional Access System) CEK(Content Encryption Key)

CI(Contents Issuer) CID(Contents ID)

CIP(Contents Information Provider) CP(Content Provider)

CW(Control Word) DCF(DRM Content Format)

PDCF(Packetized DCF) DCP(DRM Client Packager)

DRM(Digital Rights Management)

ECM(Entitlement Control Message): 가입자 자격 제어 메시지

ECMG(ECM Generator): 가입자 자격 제어 메시지 발생기

EID(Event ID)

EMM(Entitlement Management Message): 가입자 자격 관리 메시지

EMMG(EMG Generator): 가입자 자격 관리 메시지 발생기

ES(Elementary Stream)

IB(In Band): 대역 내 채널 OMA(Open Mobile Alliance)

OOB(Out of Band): 대역 외 채널

PES(Packetised Elementary Stream) RO(Rights Object)

ROAP(Rights Object AcquisitionProtocol)

RI(Rights Issuer) STK(Short-Term Key)

TS(Transport Stream) PS(Program Stream)

UID(User ID)

도1은 본 발명에 따른 방송 컨텐츠 보호 시스템의 개략적인 구성을 나타내는 도면이다.

도1에 도시한 바와 같이, 상기 시스템은, 방송사서버(100); 및 적어도 하나 이상의 클라이언트 단말기(200, 300)를 포함한다.

방송사서버(100)는 보도, 뮤직비디오, 스포츠, 영화, 드라마, 가요, 외국어, 증권, 교통, 날씨 등과 같이 다양하게 구성된 방송 컨텐츠를 IB를 통해 클라이언트 단말기(200)로 브로드캐스팅 또는 멀티캐스팅 하거나, 유선 또는 무선 망을 통해 클라이언트 단말기(200)로 유니캐스팅 한다. 이때, 방송사서버(100)는 CAS를 통해 상기 클라이언트 단말기(200)의 시청권한을 제어한다.

또한, 방송사서버(100)는 클라이언트 단말기(300)에서 상기 방송 컨텐츠를 구매요청 하거나, 합법적으로 배포(Super-distribution)된 방송 컨텐츠의 재생을 위한 권리(Right)구매 요청이 있으면, 해당 방송 컨텐츠를 다운로드해 주거나 해당 권리를 발급해준다.

이에 따라, 상기 방송 컨텐츠는 상기 방송사서버(100)의 CAS에 의해 암호화된 방송 컨텐츠 형태로 IB을 통해 클라이언트 단말기(200)로 전송되고, 상기 클라이언트 단말기(200)에서 저장 시 디지털 권한관리(DRM)를 위해 필요한 정보를 헤더로서 부가 시켜 DRM컨텐츠 형태로 암호화된다. 이때, DRM컨텐츠는 OMA의 DCF/PDCF가 그 대표적인 예이다.

클라이언트 단말기(200)는, 도2에 도시한 바와 같이, CAS에 대응되는 스마트카드(260); 상기 방송 컨텐츠를 수신하여 DRM패키징을 수행하는 DCP(250); 상기 방송사서버(100)로부터RO를 전송받아 상기 RO를 이용하여 상기 DRM패키징된 방송 컨텐츠를 재생하는 DRM에이전트(270); 및 상기 DCP(250)를 통해 DRM 패키징된 방송 컨텐츠를 저장하는 메모리(280)를 포함한다.

여기서, DCP(250)는 CAS에 의해 보호된 방송 컨텐츠를 저장할 경우, 다른 클라이언트 단말기(300)로 DRM아키텍처(Architecture) 내에서 합법적 배포(Super-distribution)될 수 있도록 DRM 패키징을 수행한다.

상술한 바와 같이 합법적으로 배포된 DRM컨텐츠를 수신받은 클라이언트 단말기(300)는, DRM에이전트(270)를 통해 방송사서버(100)로 해당 DRM컨텐츠에 대한 RO 구매를 요청하고, 상기 방송사서버(100)로부터 해당 RO를 발급받아 상기 DRM컨텐츠에 대응되는 방송 컨텐츠를 재생한다. 이때, 상기 클라이언트 단말기(200, 300)는 DRM에이전트(270)를 보유해야 하나 외부 메모리장치(미도시) 등은 자체적으로 가질 필요가 없다.

도3은 본 발명의 바람직한 실시예에 따른 방송 컨텐츠의 상태 천이과정을 나타내는 도면으로서, 상기 방송사서버(100)에서 생성된 방송 컨텐츠가 클라이언트 단말기(200)에서 재생된 후, 합법적 배포를 통해 다양한 클라이언트 단말기(300)에 의해 다시 재생되는 과정을 설명한다.

먼저, CP(400)에 의해 생성된 방송 컨텐츠는 스크램블된 후 IB로 전송된다. 이를 수신한 클라이언트 단말기(200)가 디스크램블한 후, 상기 방송 컨텐츠를 재생한다(S310-S330).

이어, 상기 방송 컨텐츠는 클라이언트 단말기(200)의 메모리나 저장장치에 저장된다. 이때, 상기 방송 컨텐츠는 CAS에 의해 암호화된 방송 컨텐츠 형태로 저장되며, CAS로부터 전송받은 EMM/ECM을 통해 재생할 수 있다(S340).

이후, 합법적 배포를 위하여 DCP(250)에 의해DRM패키징이 수행되어 DCF 파일 포맷으로 변환된다(S350).

그런 다음, 상기 DCF가 유/무선 망을 통해 적어도 하나 이상의 클라이언트 단말기(300)로 배포되면(S360), 해당 클라이언트 단말기(300)는 DRM에이전트(270)를 통해 RO를 방송사서버(100)로부터 구매하여 재생할 수 있다(S370).

이하, 본 발명을 구체적인 실시예를 통해 보다 상세히 설명한다.

도4는 본 발명의 바람직한 실시예에 따른 방송 컨텐츠 보호 시스템을 나타내는 구성도이다.

도4에 도시한 바와 같이, 상기 시스템은, CP(400), 방송사서버(100A), 적어도 하나 이상의 클라이언트 단말기(200, 300) 및 DRM서버(500)를 포함한다.

CP(400)는 방송 컨텐츠를 생성/가공한다. 여기서, 프로그램 공급자(Program Provider, PP) 역시 CP(400)의 한 예이다.

방송사서버(100A)는 상기 CP(400)로부터 제공된 방송 컨텐츠를 각각 비디오 ES 및 오디오 ES로 변환하고, 상기 비디오 ES 및 오디오 ES를 비디오 PES 및 오디오 PES로 변환하며, 상기 비디오 PES 및 오디디 PES를 TS/PS로 변환한 후, 상기 TS/PS를 스크램블하여 IB로 브로드캐스팅 또는 멀티캐스팅 한다. 본 실시예의 방송사서버(110A)는 상기 도1에 도시한 방송사서버(100)와는 RO발급 또는 다운로드 권한이 없는 점에서 다르다.

이러한 방송사서버(100A)는 CAS서버(120) 및 CIP(110)를 포함하며, 상기 구성요소에 대한 상세한 설명은 다음과 같다.

CAS서버(120)는EMM을 발생하는 EMMG(미도시); ECM을 발생하는 ECMG(미도시); 및 가입자 정보 및 과금정보를 관리하거나 방송 컨텐츠의 정보를 관리하는 BIS/PMS(미도시)를 포함하며, EMM을 IB 또는 OOB를 통해 전송하고, 소정 중간 키(예컨대, Short Term Key, 이하 STK)를 생성하여 CW를 암호화한 후 상기 CW를 ECM에 포함시켜 IB을 통해 브로드캐스팅 또는 멀티캐스팅 한다.

이때, 상기 CAS서버(120)는, 클라이언트 단말기(200)로 전송되는 데이터와 DCF로 패키징 하는데 필수적인 데이터(예컨대, STK, EID등)를 분석한 후, 상기 클라이언트 단말기(200)에서 DCF를 형성하기에 부족한 데이터(예컨대, STK 등)를 추출한 후, 추출된 데이터 중 CAS서버(120)에서 전송 가능한 데이터는 ECM 및 EMM을 통해 전송하며, 전송 불가능하거나 비효율적인 데이터는 미리 DCP(250)의 디폴트 값으로 설정하고, 향후 OOB를 통해 변경할 수 있도록 한다.

또한, CAS 서버(120)는, CIP(110)로부터 전송된 EID를 토대로 CEK 및 컨텐츠 정보 및 클라이언트 단말기(300)의 권한(Permission/Constraint)정보를 생성하여 상기 CIP(110)를 통해 상기 DRM서버(500)로 전송한다.

CIP(110)는 사용자에 대한 프리젠테이션 서버 역할을 수행하며, 클라이언트 단말기(300)의 RO구매 요청 시 결재기능도 수행한다. 본 발명에 따른 CIP(110)는 OMA DRMv2.0에서의 CI와 비슷한 역할을 수행하지만, 실제 컨텐츠를 전송하지 않는 점에서 그 차이가 있다.

또한, CIP(110)는 클라이언트 단말기(300)로부터 RO구매요청과 함께 전송된 CID를 분석하여 EID, 녹화시간(시작시간, 종료시간), 보상을 위한 UID를 추출한다. 또한, CIP(110)는 EID를 CAS서버(120)로 전송하여 상기 EID에 해당하는 CEK, 컨텐츠 정보, 과금정보 등을 제공받는다. 이 방식을 풀 방식이라고 하나, 상기 풀 방식이외에도 CAS서버(120)의 방송 프로그램 스케줄에 따라 푸쉬 방식으로 CEK, 컨텐츠 정보, 과금정보 등을 제공 받을 수 도 있다.

그리고, CIP(110)는 CAS서버(120)로부터 전송된 상기 권한정보를 이용하여 권리제안(Rights Offer)을 생성하여 클라이언트 단말기(300)로 제공하며, CIP(110)는 DRM서버(500)와 클라이언트 단말기(300) 사이에 ROAP 설정을 위한 ROAP 트리거 중계역할을 수행한다. 이에 따라 DRM서버(500)는 ROAP를 통해 클라이언트 단말기(300)로 RO를 제공할 수 있다.

클라이언트 단말기(200)는, 도2에 도시한 바와 같은 구성 및 기능을 포함하며, 상기 브로드캐스팅 또는 멀티캐스팅된 방송 컨텐츠를 수신하여 화면에 디스플레이하고, 상기 방송 컨텐츠를 합법적 배포를 수행하기 위한 DRM패키징을 수행한다. 이때, DRM패키징을 위하여 필요한 정보들은 클라이언트 단말기(200)의 보안 수준에 따라 USIM(Universal Subscriber Identification Module)이나 스마트카드(260)를 이용하여 관리할 수 도 있다.

상기 DRM패키징된 방송 컨텐츠에 대한 권리(Rights)는, ECM내의 AC(Access Criteria)정보를 기반으로 구성되며, 합법적 배포가 이루어진 후에 DRM서버(500)를 통해 RO를 획득하여 상기 RO을 이용하여 상기 방송 컨텐츠를 재생할 수 있다.

이와 같은 클라이언트 단말기(200)는, CAS에 의해 보호된 방송 컨텐츠를 재생하는 기능을 구비한 단말기(200)이며, PDA(Personal Digital Assistant), 핸드 헬드 PC(Hand-Held PC), CDMA(Code Division Multiple Access)폰, GSM(Global System for Mobile)폰, WCDMA(Wideband CDMA)폰 및 MBS(Mobile Broadband System)폰 등을 포함할 수 있다.

한편, 클라이언트 단말기(300)는 상기 DRM컨텐츠를 배포 받아 저장한 후, RO를 구매하여 상기 방송 컨텐츠를 화면에 디스플레이 한다. 상기 클라이언트 단말기(300)는 메모리, PDA(Personal Digital Assistant), 핸드 헬드 PC(Hand-Held PC), CDMA(Code Division Multiple Access)폰, GSM(Global System for Mobile)폰, WCDMA(Wideband CDMA)폰 및 MBS(Mobile Broadband System)폰 등을 포함할 수 있다.

DRM서버(500)는 적어도 하나 이상으로 이루어지며, 상기 클라이언트 단말기(300)로부터의 RO 구매요청에 대하여 소정 인증과정을 거친 후 RO를 발급 또는 다운로드 한다. 그리고, DRM서버(500)는 OMA DRMv2.0에서의 RI기능을 포함함으로써, ROAP트리거를 클라이언트 단말기(300)로 전송한다.

상기 ROAP는 요청-응답(Request-Response) 프로토콜이고, 상기 ROAP 트리거는 상기 클라이언트 단말기(300)로 하여금 ROAP세션을 DRM서버(500)와 설정하도록 지시한다.

이하, 첨부된 도5내지 도10을 참고하여 본 발명의 바람직한 실시예에 따른 방송 컨텐츠 보호 방법을 설명한다.

도5는 본 발명의 바람직한 실시예에 따른 방송 컨텐츠 보호 방법을 설명하기 위한 도면으로서, 방송사서버(100A)에서 브로드캐스팅 또는 멀티캐스팅된 방송 컨텐츠가 클라이언트 단말기(200)에서 수신/DRM패키징된 후, 합법적 배포되어 클라이언트 단말기(300)에서 DRM서버(500)로부터 RO의 구매를 통해 재생하기까지의 과정을 나타낸다.

이를 분류하면 크게, 1) 방송 송출 과정, 2) 방송 수신하여 DRM컨텐츠화 과정 3) DRM 컨텐츠 배포과정 4) 배포된 DRM컨텐츠를 RO 구매를 통해 재생하는 과정으로 나눌 수 있다.

1) 방송 컨텐츠 송출 과정

먼저, 방송사서버(100A)가 방송 컨텐츠 및 제어정보(CW가 포함된 ECM)를 IB을 통해 브로드캐스팅 또는 멀티캐스팅 하고, 가입자 정보(EMM)를 IB 또는 OOB을 통해 브로드캐스팅 또는 유니캐스팅 한다(S501). 이때, 방송사서버(100A)에 포함된 CAS서버(120)에서 상기 가입자 자격 제어정보 및 가입자 자격 관리정보를 생성한다.

2) 방송 컨텐츠를 수신하여 DRM컨텐츠화 과정

이어, 클라이언트 단말기(200) 가 상기 방송 컨텐츠를 수신하여 재생하거나 저장(Recording)한 후, DRM 아키텍쳐 내에서 합법적으로 배포(super-distribution)될 수 있도록 DRM 패키징 한다(S502-S503).

상기 방송 컨텐츠는 상기 단계502 내지 단계 503을 통해 헤더정보, CID, CEK, 상기 CID 와 CEK의 맵핑정보가 생성된 후 CEK로 암호화된다. 이때, 클라이언트 단말기(200)의 성능 및 노출정도(Open platform 또는 Proprietary platform)에 따라 클라이언트 단말기(200) 내에서 방송 컨텐츠를 CEK로 암호화 시키지 않고, 합법적 배포가 이루어지는 시점에서 CEK로 암호화 시킬 수도 있다.

CAS에 의해 보호된 방송 컨텐츠는 DCP(250)에 의해 메모리(280)에 저장된다. 상기 DCP(250)는 클라이언트 단말기(200)와 별도로 구성될 수 있으며, DCP(250)에 의해 곧 바로 DCF(또는 PDCF) 형태로 저장된다. 이러한 DCP(250)가 상기 방송 컨텐츠를 저장하는 시점은, TS/PS형태, 중간 단계인 PES 혹은 마지막 단계인 ES형태인 시점이다.

상술한 바와 같이 수신한 방송 컨텐츠를 통해 CID, CEK를 생성하고, 상기 CID와 CEK를 맵핑한 후, 상기 방송 컨텐츠를 CEK로 암호화한다. 이때, CID 및 CEK 생성은 상기 단계502 또는 단계 503 중 어느 시점에서 수행하더라도 상관없다.

2-1) CID 생성

상술한 바와 같은 CAS에 의해 보호된 방송 컨텐츠가 클라이언트 단말기(200)에 저장될 때, 프로그램 전체가 저장되거나, 프로그램의 일부가 저장될 수 있다. 이에 따라, 상기 DCP(250)는, 도6에 도시한 바와 같은 CID를 생성한다.

도6은 본 발명의 바람직한 실시예에 따른 CID의 구성을 나타내는 도면으로서, CID는 URI로 표현되며, 다음과 같은 두 가지로 구분된다.

먼저, 프로그램 전체가 DRM패키징 될 경우, DCP(250)는 방송 컨텐츠의 EID와 함께 CP(400)의 도메인 네임, 상기 DRM 컨텐츠를 저장하는 클라이언트 단말기(200)의 UID를 포함하는 CID를 생성한다.

다음으로, 프로그램 일부가 DRM패키징 될 경우, DCP(250)는 방송 컨텐츠의 EID와 함께 녹화시작시간, 녹화종료시간, 컨텐츠 공급자의 도메인 네임, 상기 DRM컨텐츠를 저장하는 UID를 포함하는 CID를 생성한다.

여기서, 상기 UID는, DRM컨텐츠가 배포된 후 클라이언트 단말기(300)에서 최초로 RO요청이 이루어지면 해당 DRM컨텐츠의 등록이 이루어지며, 이처럼 등록된 UID에 대한 보상을 통해 방송 컨텐츠의 유통시장의 활성화를 가져올 수 있는 부수적 효과가 있다.

이때, 상기 녹화시작시간, 녹화종료시간 및 UID는 CID에 포함시키지 않고, 차후에 생성될 DRM컨텐츠의 확장헤더(Extended Header)에 부가시킬 수도 있다.

2-2) CEK 생성

또한, DCP(250)는 도7 및 도8에 도시한 CEK를 생성한 후, 상기 CEK를 이용하여 방송 컨텐츠를 암호화한다.

도7및 도8는 본 발명의 바람직한 실시예에 따른 CEK생성방법을 나타내는 도면으로서, CAS서버(120)의 스크램블 방식에 따라 다음과 같이 두 가지로 구분된다.

먼저, CW가 프로그램별로 바뀌는 경우(One Key per One Program), 해당 프로그램에 대한 DRM컨텐츠의 CEK로 CW를 그대로 사용하거나(랜덤숫자와 함께) 일방향 함수를 통해 변경된 값을 사용한다. 이에 따라, CEK는 다음 수학식 1과 같이 표현될 수 있다.

CEK = CW 또는 CEK = f(CW, random number)

다음으로, CW가 한 프로그램내에서 여러 번 바뀌는 경우(Many Keys per One Program)에는, CAS서버(120)에 대한 가입자가 달라져도 상관없는 키를 이용하여 CEK를 유도하여 사용한다. 즉, CAS서버(120)는 서버와 클라이언트가 공유하는 키가 다양하게 존재하며, 그 중에서 가입자가 달라져도 상관없는 중간 키, 예컨대 STK라 하면, 해당 프로그램에 대한 DRM컨텐츠의 CEK로 STK와 해당프로그램의 EID를 다음 수학식 2와 같은 특정한 함수(예컨대, 해쉬함수)에 넣어 도출된 결과값을 이용할 수 있다. 이때, 특정한 함수의 입력값으로 브로드캐스팅 되는 랜덤숫자를 함께 넣을 수도 있다.

CEK = f(STK, EID) 또는 CEK = f(STK, EID, random number)

한편, 상술한 바와 같은 CEK는 CAS서버(120)에서 전송되는 CW 또는 방송 컨텐츠 내에 포함된EID를 이용하여 생성되나, 자체적으로 랜덤하게 생성한 후 서버(예컨대, CIP(110))쪽으로 전송할 수 있다.

2-3) CID 및 CEK 맵핑

또한, DCP(250)는 상기에서 생성된 CID 및 CEK를 맵핑한다. CID 와 CEK의 맵핑은 EID를 기준으로 이루어지며, 동일한 프로그램에 대한 전체 DRM패키징 및 부분 DRM패키징 모두 EID는 동일하므로, CEK는 일관성 있게 유지된다.

지금까지 설명한 EID는 CEK의 유니크(unique)를 위하여, 서비스ID, 날짜정보 및 방송프로그램 ID를 토대로 이루어진다. 상기 서비스ID, 날짜정보 및 방송프로그램 ID는 일 실시예이며, EID가 유니크하게 형성된다면 다른 정보를 토대로 형성하여도 무방하다.

2-4) 헤더 형성

도9는 본 발명의 바람직한 실시예에 따라 DCP에서 DCF를 형성할 때 부가되는 헤더를 나타내는 도면으로서, DCP(250)가 CAS에 의해 암호화된 방송 컨텐츠를 DCF로 변환할 때 ECM 및 EMM을 통해 전송된 정보를 기반으로 형성하는 헤더의 구성을 나타낸다. 이에 따라 DCP(250)는 상기 CEK를 통해 암호화된 방송 컨텐츠에 상기 헤더가 부가한다.

상기 헤더는, 도9에 도시한 바와 같이, 컨텐츠 객체(Content Object), 권리 객체(Rights Object, RO), 암호화정보(Encryption Information), 컨텐츠 정보(Content Information), 권리발생기(Rights Issuer, RI)정보 또는 컨텐츠 발생기(Content Issuer, CI)정보, ROAP정보, 트랜잭션 트랙킹 정보(Transaction Tracking Information), 기록정보(Recording Information), 유저 데이터(User Data)등과 같은 정보를 포함한다.

여기서, 상기 RI정보는 본 실시예에서의 DRM서버(500)의 정보를 의미하고, CI정보는 CIP(110) 정보를 의미한다.

3) DRM 컨텐츠 배포과정

상술한 과정을 통해 방송 컨텐츠가 DRM컨텐츠화 되어 클라이언트 단말기(200)에 저장된다. 이에 따라 상기 단계 503이후, 상기 DRM컨텐츠는 적어도 하나 이상의 클라이언트 단말기(300)로 합법적으로 배포(Super-distribution)된다(S504).

4) 배포된 DRM컨텐츠를 RO 구매를 통해 재생하는 과정

클라이언트 단말기(300)가 상기 DRM컨텐츠를 이용하기 위하여 CIP(110)에 RO를 요구한다(S505). 여기서, 상기 클라이언트 단말기(300)는 상기 RO요청메시지와 함께 CID를 전송한다. 이때, 상기 클라이언트 단말기(300)가 CIP(110)에 등록되지 않은 경우에는, 클라이언트 단말기(300)의 디바이스 등록절차를 수행한 후에 RO요청에 따른 해당 방송 컨텐츠에 대한 권리(Rights)를 제공한다.

그러면, CIP(110)는 클라이언트 단말기(300)로부터 전송된 CID를 분석하여 EID, 녹화시간(시작시간, 종료시간), 보상을 위한 UID를 추출한 후(S506), CAS서버(120)에 상기 EID에 따른 CEK 및 컨텐츠 정보(과금정보 포함)를 요청한다(S507).

이에 따라, 상기 CAS서버(120)는 상기CIP(110)로부터 요청된 CEK, 컨텐츠 정보(과금내역 포함)와 상기 RO구매 요청한 클라이언트 단말기(300)에 대한 권한정보를 상기 CIP(110)로 전송한다(S508). 이때, 상기 컨텐츠 정보에 따른 최초 RO에 따른 DRM컨텐츠의 등록을 수행한다.

여기서, 상기 단계 507과 단계 508을 첨부된 도10을 참고하여 보다 더 상세히 설명한다.

도10은 본 발명의 바람직한 실시예에 따른 CEK, 컨텐츠 정보, 과금정보 요청/전달 과정을 나타내는 도면으로서, 상기 CAS서버(120)와 CIP(110)사이에서 일어나는 CEK, 컨텐츠 정보, 과금정보 요청/전달 과정을 요청/전달 방법을 나타낸다.

도10에 도시한 바와 같이, CIP(110)는 ECMG(123), EMMG(122), 또는 BIS/PMS(121)를 통해 상기 EID에 해당하는 CEK를 얻을 수 있다. 예컨대, EMMG(122)에서 상기 EID에 해당하는 CEK 유도방법을 설명한다.

먼저, CW가 프로그램별로 바뀌는 경우에는, 상기 EID에 해당하는 CW가 CEK이거나 수학식 1에 표현된 일방향 함수를 통해 CEK를 얻을 수 있다.

한편, CW가 한 프로그램내에서 여러 번 바뀌는 경우에는, 상기 EID 및 STK 를 이용하여 상기 수학식 2에 표현된 일방향 함수를 토대로 CEK를 얻을 수 있다.

여기서, 상기 EMMG(122)에서 STK와 EID를 이용하여 CEK를 유도할 경우, 하나의 EID가 두개의 STK에 걸쳐 발생할 수도 있다. 이러한 경우는 한 프로그램이 방송되는 상황에서 STK가 바뀌는 경우이다. 이때에는 STK가 바뀌는 타임정보를 두개의 CEK와 함께 전달하여 해결한다. 추후, 클라이언트 단말기(300)의 RO요청이 들어올 때 마다 아래 수학식3에 나타난 CID의 저장시작 시간정보를 이용하여 해당 CEK를 선택한다.

CEK1 = f(STK(j), EID), 저장 시작시간이 STK(j)보다 작거나 같은 경우,

CEK2 = f(STK(j+ 1), EID), 저장 시작시간이 STK(j)보다 큰 경우,

한편, CIP(110)는 CEK, 컨텐츠 정보, 과금정보 등을 CAS서버(120)로부터 풀 방식(2-way)으로 얻을 수 있으나, ECMG(123), EMMG(122), PMS/BIS(121) 등과 같은 CAS서버(120)내 각 시스템들의 프로그램 스케줄에 따라 자동으로 푸쉬 방식(1-way)으로 얻을 수 있다.

이후, CIP(110)는 상기 권한정보(Permission/Constraint)를 이용하여 권리 제안(Rights Offer)을 생성하여 클라이언트 단말기(300)로 제공한 후, 상기 클라이언트 단말기(300)로부터 상기 권리 제안을 토대로 선택된 권리내역(예컨대, 3회 복사 가능)을 전송 받는다(S509-S510).

이어, CIP(110)는 CEK, 컨텐츠 정보, 권리동의서(Rights Agreement)를 DRM서버(500)로 전송한 후 상기 DRM서버(500)에 ROAP트리거(Trigger)를 요청하면, 상기 DRM서버(500)는 해당 ROAP트리거를 CIP(110)로 전송한다(S511-S513). 그러면, CIP(110)는 상기 ROAP트리거를 클라이언트 단말기(300)로 전송한다(S514). 이때, 상기 ROAP트리거에는 상기 클라이언트 단말기(300)가 RO를 획득할 수 있는 적어도 하나 이상의DRM서버 가운데 해당 DRM서버(500)의 주소정보(URL)를 포함한다. 상기 ROAP는 요청-응답(Request-Response) 프로토콜로서, DRM서버(500)에서 상기 CIP(110)를 통해 클라이언트 단말기(300)로 ROAP트리거를 전송한다. 상기 ROAP트리거는 상기 클라이언트 단말기(300)로 하여금 ROAP세션을 DRM서버(500)와 설정하도록 지시한다.

따라서, 클라이언트 단말기(300)는 ROAP트리거에 따라 ROAP세션을 설정한 후 DRM서버(500)로 RO(Rights Object)를 요청하고, DRM서버(500)는 RO를 클라이언트 단말기(300)로 전송한다(S515-S517).

이후, 클라이언트 단말기(300)는 상기 RO를 통해 해당 방송 컨텐츠를 재생할 수 있다.

지금까지 본 발명을 바람직한 실시예를 참조하여 상세히 설명하였지만, 당업자는 본 발명의 사상 및 범위를 벗어나지 않고 다양한 변형 또는 수정이 가능하다는 것을 알 것이다.

발명의 효과

이상 설명한 바와 같이, 본 발명에 따르면, 방송 컨텐츠에 CAS와 DRM 기술을 접목시켜 상기 방송 컨텐츠를 보호함으로써, 방송 컨텐츠의 무분별하게 배포되더라도 방송사 측의 허가 없는 재생(Play)을 방지할 수 있는 효과가 있다.

또한, 본 발명에 따르면 방송사측에서는 한번 전송된 방송 컨텐츠가 가입자 망 자원을 통해 유통되면서, 재생 권리(Rights) 발급 만을 통해 추가적인 수익을 얻을 수 있는 효과가 있다.

또한, 본 발명에 있어서, 상기 방송 컨텐츠의 유통에 있어서 주요한 역할을 수행하는 합법적 배포자(super-distributor)에게도 방송사측에서 일정 수익/이익을 지급함으로써, 능동적으로 합법적 배포가 이루어지도록 하는 효과가 있다.

(57) 청구의 범위

청구항 1.

A) CAS(Conditional Access System)서버가 방송 컨텐츠를 스크램블한 후 ECM과 함께 IB로 브로드캐스팅 또는 멀티캐스팅 하고, EMM을 대역 내/외 채널을 통해 브로드캐스팅 또는 유니캐스팅 하는 단계;

B) 제1클라이언트 단말기가 상기 방송 컨텐츠를 수신하여 디스크램블 한 후, 상기 방송 컨텐츠를 저장한 후 DRM(Digital Rights Management)패키징을 수행하여, 상기 방송 컨텐츠를 DRM컨텐츠로 변환하는 단계;

C) 상기 제1클라이언트 단말기가 유/무선 망을 통해 상기 DRM컨텐츠를 적어도 하나 이상의 제2 클라이언트 단말기로 합법적으로 배포(super-distribution)하는 단계; 및

D) 상기 제2클라이언트 단말기가 RO(Rights Object)를 구매하여 상기 DRM컨텐츠를 재생하는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 2.

제1항에 있어서, 상기 B) 단계는,

B1) 상기 방송 컨텐츠의 EID(Event ID)를 기반으로 CID(Content ID)를 생성하는 단계;

B2) CAS서버로부터 전송된CW(Control Word)를 기반으로 CEK(Content Encryption Key)를 생성하는 단계;

B3) 상기 CID와 CEK를 상기 EID를 기준으로 맵핑하는 단계; 및

B4) 상기 CW 또는 CEK를 토대로 상기 방송 컨텐츠를 암호화하는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 3.

제2항에 있어서, 상기 CID는,

상기 방송 컨텐츠의 EID, 컨텐츠 공급자(CP)의 도메인 네임 및 UID를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 4.

제2항에 있어서, 상기 CID는,

상기 방송 컨텐츠의 EID, 컨텐츠 공급자(CP)의 도메인 네임, UID, 녹화시작시간 및 녹화종료시간을 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 5.

제2항에 있어서, 상기 B4) 단계는

상기 녹화시작시간, 녹화종료시간 및 UID를 상기 암호화된 DRM컨텐츠의 확장헤더(Extended Header)에 부가시키는 단계를 더 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 6.

제2항에 있어서, 상기 CEK는,

상기 CW가 방송 프로그램별로 바뀌는 경우에는, 상기 CW를 그대로 사용하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 7.

제2항에 있어서, 상기 CEK는,

상기 CW가 방송 프로그램별로 바뀌는 경우에는, 상기 CW를 소정 함수에 의해 변경된 값을 사용하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 8.

제2항에 있어서, 상기 CEK는,

상기 CW가 한 방송 프로그램내에서 여러 번 바뀌는 경우에는, 소정 키와 해당 프로그램의 EID를 이용하여 특정한 함수에 의해 생성된 결과값을 이용하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 9.

제1항 또는 제2항에 있어서, 상기 B) 단계는,

상기 CAS서버로부터 전송된 EMM 및 ECM을 토대로 헤더를 생성하여 상기 CW 또는 CEK에 의해 암호화된 방송 컨텐츠에 부가하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 10.

제1항 또는 제2항에 있어서, 상기 B) 단계는,

상기 CAS서버에서 전송 불가능하거나 비효율적인 데이터는 미리 DCP의 디폴트 값으로 설정하고, 향후 OOB채널을 통해 변경 가능한 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 11.

제9항에 있어서, 상기 헤더는,

상기 방송 컨텐츠의 컨텐츠 객체(Content Object), 권리 객체(Rights Object, RO), 암호화정보(Encryption Information), 컨텐츠 정보(Content Information), 권리발생기(Rights Issuer) 또는 컨텐츠 발생기(Content Issuer)정보, ROAP(Rights Object Acquisition Protocol)정보, 트랜잭션 트랙킹 정보(Transaction Tracking Information), 기록정보(Recording Information), 유저 데이터(User Data) 중에서 적어도 하나 이상을 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 12.

제1항 또는 제2항에 있어서, 상기 D) 단계는,

D1) 상기 제2클라이언트 단말기가 CIP(Content Information Provider)에 RO(Rights Object)의 구매를 요구하는 단계;.

D2) 상기 CIP가 상기 제2클라이언트 단말기로부터 요청된 RO의 CID를 분석하여 EID를 추출한 후, 상기 EID에 따른 CEK 및 컨텐츠 정보를 상기 CAS서버로 요청하는 단계;

D3) 상기 CAS 서버가 상기 EID를 토대로 CEK, 컨텐츠 정보를 추출하여 상기 CIP를 통해 DRM서버로 전송하는 단계;

D4) 상기 CIP가 상기 DRM서버와 제2클라이언트 단말기 사이에 ROAP(Rights Object Acquisition Protocol)를 기반으로 하는 세션을 설정해주는 단계; 및

D5) 상기 제2클라이언트 단말기가 상기 설정된 세션을 통해 DRM서버로 RO를 요청하여 전송받는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 13.

제12항에 있어서, 상기 D3) 단계는,

D3-1) 상기 CAS 서버가 상기 EID를 토대로 CEK, 컨텐츠 정보를 추출하여 상기 제2클라이언트 단말기에 대한 권한(Permission/Constraint)정보와 함께 상기 CIP로 전송하는 단계;

D3-2) 상기 CIP가 상기 권한정보를 토대로 권리 제안(Rights Offer)을 생성하여 제2클라이언트 단말기로 전송하는 단계;

D3-3) 상기 제2클라이언트 단말기가 상기 권리 제안을 토대로 상기 사용자로부터 선택된 권리내역을 상기 CIP로 전송하는 단계; 및

D3-4) 상기 CIP가 상기 CEK, 컨텐츠 정보 및 권리동의서(Rights Agreement)를 DRM서버로 전송하는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 14.

제13항에 있어서, 상기 D3-2) 단계는,

상기 RO 요청한 제2클라이언트 단말기가 상기 CIP에 등록되지 않은 경우, 상기 제2클라이언트 단말기의 등록을 수행하는 단계를 더 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 15.

제12항에 있어서, 상기 D4) 단계는,

ROAP트리거를 통해 ROAP를 기반으로 하는 세션을 설정하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 16.

제12항에 있어서, 상기 D4) 단계는,

상기 RO요청된 방송 컨텐츠가 최초의 RO요청인 경우, 상기 CIP가 상기 방송 컨텐츠에 대한 DRM컨텐츠 등록을 수행하는 것을 특징으로 하는 방송 컨텐츠 보호 방법.

청구항 17.

CAS(Conditional Access System)서버가 방송 컨텐츠를 스크램블한 후 IB로 브로드캐스팅 또는 멀티캐스팅 하고, EMM을 대역 내/외 채널을 통해 브로드캐스팅 또는 유니캐스팅 한 후, 클라이언트 단말기가 상기 방송 컨텐츠를 수신하여 상기 방송 컨텐츠를 저장하는 방법에 있어서,

a) 상기 CAS서버로부터 전송된 방송 컨텐츠를 수신하여, 미리 저장된 가입자 키 등을 통해 중간 키를 생성하고, 상기 중간 키를 통해 CW(Control Word)를 복호한 후, 상기 CW를 통해 상기 방송 컨텐츠를 디스크램블 하는 단계;

b) 상기 방송 컨텐츠의 EID(Event ID)를 기반으로 CID(Content ID)를 생성하는 단계;

c) 상기CW(Control Word) 및 중간 키를 기반으로 CEK(Content Encryption Key)를 생성하는 단계; 및

d) 상기 CID와 CEK를 상기 EID를 기준으로 맵핑하는 단계; 및

e) 상기 CW 또는 CEK를 토대로 상기 방송 컨텐츠를 암호화하여 저장하는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 18.

제17항에 있어서, 상기 CID는,

상기 방송 컨텐츠의 EID, 컨텐츠 공급자(CP)의 도메인 네임 및 UID를 포함하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 19.

제17항에 있어서, 상기 CID는,

상기 방송 컨텐츠의 EID, 컨텐츠 공급자(CP)의 도메인 네임, UID, 녹화시작시간 및 녹화종료시간을 포함하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 20.

제17항에 있어서, 상기 e) 단계는

상기 녹화시작시간, 녹화종료시간 및 UID를 상기 암호화된 DRM컨텐츠의 확장헤더(Extended Header)에 부가시키는 단계를 더 포함하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 21.

제17항 내지 제20항 중 어느 한 항에 있어서, 상기 CEK는,

상기 CW가 방송 프로그램별로 바뀌는 경우에는, 상기 CW를 그대로 사용하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 22.

제17항 내지 제20항 중 어느 한 항에 있어서, 상기 CEK는,

상기 CW가 방송 프로그램별로 바뀌는 경우에는, 상기 CW를 소정 함수에 의해 변경된 값을 사용하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 23.

제17항 내지 제20항 중 어느 한 항에 있어서, 상기 CEK는,

상기 CW가 한 방송 프로그램내에서 여러 번 바뀌는 경우에는, 소정 중간 키와 해당 프로그램의 EID를 이용하여 특정한 함수에 의해 생성된 결과값을 이용하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 24.

제17항에 있어서,

상기 CAS서버로부터 전송된 EMM 및 ECM을 토대로 헤더를 생성하여 상기 CW 또는 CEK에 의해 암호화된 방송 컨텐츠에 부가하는 단계를 더 포함하는 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 25.

제24항에 있어서, 상기 헤더는

상기 녹화시작시간정보, 녹화종료시간정보 및 UID정보를 포함하는 것을 특징으로 하는 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 26.

제17항에 있어서,

상기 CAS서버에서 전송 불가능하거나 비효율적인 데이터는 미리 DCP의 디폴트 값으로 설정하고, 향후 OOB채널을 통해 변경 가능한 것을 특징으로 하는 방송 컨텐츠 저장 방법.

청구항 27.

DRM(Digital Rights Management)패키징된 방송 컨텐츠를 클라이언트 단말기에서 재생하는 방법에 있어서,

(a) 상기 클라이언트 단말기가 CIP(Content Information Provider)에 상기 방송 컨텐츠의 RO(Rights Object)의 구매를 요청하는 단계;.

(b) 상기 CIP가 상기 클라이언트 단말기로부터 요청된 RO의 CID(Content ID)를 분석하여 EID(Event ID)를 추출한 후, 상기 EID에 따른 CEK(Content Encryption Key) 및 컨텐츠 정보를 CAS서버로 요청하는 단계;

(c) 상기 CAS 서버가 상기 EID를 토대로 CEK 및 컨텐츠 정보를 추출하여 상기 CIP를 통해 DRM(Digital Rights Management)서버로 전송하는 단계;

(d) 상기 CIP가 상기 DRM서버와 클라이언트 단말기 사이에 ROAP(Rights Object Acquisition Protocol)를 기반으로 하는 세션을 설정해주는 단계; 및

(e) 상기 클라이언트 단말기가 상기 설정된 세션을 통해 상기 DRM서버로 RO를 요청하여 전송받는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 28.

제27항에 있어서, 상기 (c) 단계는,

(c1) 상기 CAS 서버가 상기 EID를 토대로 CEK, 컨텐츠 정보를 추출하여 상기 클라이언트 단말기에 대한 권한(Permission/Constraint)정보와 함께 상기 CIP로 전송하는 단계;

(c2) 상기 CIP가 상기 권한정보를 토대로 권리제안(Rights Offer)을 생성하여 상기 클라이언트 단말기로 전송하는 단계;

(c3) 상기 클라이언트 단말기가 상기 권리제안을 토대로 상기 사용자로부터 선택된 권리내역을 상기 CIP로 전송하는 단계; 및

(c4) 상기 CIP가 상기 CEK, 컨텐츠 정보 및 권리동의서(Rights Agreement)를 상기 DRM서버로 전송하는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 29.

제28항에 있어서, 상기 (c1) 단계는,

CW(Control Word)가 방송 프로그램별로 바뀌는 경우, 상기 EID에 해당하는 CW가 CEK이거나 소정 일방향 함수를 토대로 CEK를 추출하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 30.

제28항에 있어서, 상기 (c1) 단계는,

CW(Control Word)가 한 프로그램내에서 여러 번 바뀌는 경우, 상기 EID및 소정 중간 키를 이용하여 소정 일방향 함수를 토대로 CEK를 추출하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 31.

제28항에 있어서, 상기 (c1) 단계는,

상기 CAS서버에서 소정 중간 키와 EID를 이용하여 CEK를 추출할 경우, 하나의 EID가 두개의 중간 키에 걸쳐 발생하면, 상기 중간 키가 바뀌는 타임정보, 두개의 CEK 및 상기 CID의 저장시작 시간정보를 이용하여 해당 CEK추출하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 32.

제28항 내지 제31항 중 어느 한 항에 있어서, 상기 (c2) 단계는,

상기 RO 요청한 클라이언트 단말기가 상기 CIP에 등록되지 않은 경우, 상기 클라이언트 단말기의 등록을 수행하는 단계를 더 포함하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 33.

제28항 내지 제31항 중 어느 한 항에 있어서, 상기 (c4) 단계는,

ROAP트리거를 통해 ROAP를 기반으로 하는 세션을 설정하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 34.

제28항 내지 제31항 중 어느 한 항에 있어서, 상기 (c4) 단계는,

상기 RO요청된 방송 컨텐츠가 최초의 RO요청인 경우, 상기 CIP가 상기 방송 컨텐츠에 대한 DRM컨텐츠 등록을 수행하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 35.

제28항 내지 제31항 중 어느 한 항에 있어서, 상기 (d) 단계는,

상기 CIP가 상기 DRM서버의 주소정보를 상기 클라이언트 단말기로 전송하는 단계를 포함하는 것을 특징으로 하는 방송 컨텐츠 재생 방법.

청구항 36.

방송 컨텐츠를 브로드캐스팅 또는 멀티캐스팅 하고 CAS(Conditional Access System)를 통해 시청권한을 제어하며, 합법적으로 배포(Super-distribution)된 상기 방송 컨텐츠의 재생을 위한 권리(Right)구매 요청이 있으면 해당 방송 컨텐츠에 대한 재생 권리를 발급하는 방송사서버; 및

상기 CAS를 통해 제어된 방송 컨텐츠를 재생하며, 상기 방송 컨텐츠를 저장하고, 합법적 배포를 위한 DRM(Digital Rights Management) 패키징을 수행하며, 상기 방송사서버로 상기 DRM컨텐츠에 대한 권리(Right)구매를 요청한 후, 해당 DRM 컨텐츠에 대한 권리(Right)를 발급받아 상기 DRM컨텐츠에 대응되는 방송 컨텐츠를 재생하는 클라이언트 단말기를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 37.

제36항에 있어서, 상기 클라언트 단말기는

상기 CAS에 대응되는 스마트카드;

상기 방송 컨텐츠를 수신하여 상기 방송 컨텐츠를 저장 및 DRM패키징을 수행하는 DCP(DRM Client Packager);

상기 방송사서버로부터RO(Rights Object)를 전송받아 상기 RO를 이용하여 상기 DRM패키징된 방송 컨텐츠를 재생하는 DRM에이전트; 및

상기 DCP를 통해 DRM 패키징된 방송 컨텐츠를 저장하는 메모리를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 38.

제37항에 있어서, 상기 DCP는,

상기 방송 컨텐츠의 EID(Event ID)를 기반으로 CID(Content ID)를 생성하는 CID생성기;

상기 CAS서버로부터 전송된CW(Control Word)를 기반으로 CEK(Content Encryption Key)를 생성하는 CEK생성기;

상기 CID와 CEK를 상기 EID를 기준으로 맵핑하는 맵핑기; 및

상기 CW 또는 CEK를 토대로 상기 방송 컨텐츠를 암호화하는 암호화기를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 39.

제37항 또는 제38항에 있어서, 상기 DCP는

상기 방송 컨텐츠의 TS(Transport Stream)/PS(Program Stream)형태; PES(Packetised Elementary Stream)형태 또는 ES(Elementary Stream)형태 중 적어도 하나 이상의 형태를 상기 메모리에 저장하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 40.

EMM(Entitlement Management Message)을 대역 내 및/또는 OOB을 통해 브로드캐스팅 또는 유니캐스팅하고, 소정 중간 키를 생성하여 CW(Control Word)를 암호화한 후 상기 CW를 ECM(Entitlement Control Message)에 포함시켜 IB를 통해 브로드캐스팅 또는 멀티캐스팅 하는 CAS(Conditional Access System)서버;

브로드캐스팅 또는 멀티캐스팅된 방송 컨텐츠를 수신하여 화면에 디스플레이하고, 상기 방송 컨텐츠를 합법적 배포를 수행하기 위하여 DRM(Digital Rights Management)패키징을 수행하는 적어도 하나 이상의 제1클라이언트 단말기;

상기 DRM패키징된 방송 컨텐츠를 배포 받아 저장하거나, RO(Rights Object)를 구매하여 상기 방송 컨텐츠를 화면에 디스플레이 하는 적어도 하나 이상의 제2클라이언트 단말기;

합법적으로 배포(super-distribution)된 방송 컨텐츠에 대한 RO의 CID(Content ID)를 분석하여 EID(Event ID)를 추출하고, 상기 EID에 따른 CEK(Content Encryption Key) 및 컨텐츠 정보를 상기 CAS서버로 수신한 후, ROAP(Rights Object Acquisition Protocol) 설정을 위한 ROAP트리거 중계역할을 수행하는 CIP(Contents Information Provider); 및

상기 제2클라이언트 단말기로부터의 RO 구매 요청에 대하여 소정 인증과정을 거친 후 RO을 발급 또는 다운로드 해주는 적어도 하나 이상의 DRM 서버를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 41.

제40항에 있어서, 상기 CAS서버는,

상기 CIP로부터 전송된 EID를 통해 상기 EID에 따른 CEK, 상기 방송 컨텐츠 정보 및 사용자 권한(Permission/Constraint)정보를 생성하여 상기 CIP를 통해 상기 DRM서버로 전송하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 42.

제40항에 있어서, 상기 CAS서버는

상기 제1클라이언트 단말기로 전송되는 데이터와 상기 방송 컨텐츠를 DRM 패키징 하는데 필수적인 데이터를 분석하고, 상기 제1클라이언트 단말기에서 DRM패키징 하기에 부족한 데이터를 추출한 후, 상기 추출된 데이터 가운데 전송 가능한 데이터를 상기 ECM 및 EMM을 통해 전송하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 43.

제40항에 있어서, 상기 CAS서버는

전송 불가능하거나 비효율적인 데이터는 미리 DCP의 디폴트 값으로 설정하고, 향후 OOB채널을 통해 변경 가능한 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 44.

제40항 내지 43항 중 어느 한 항에 있어서, 상기 CIP는

상기 CAS서버로부터 상기 CEK, 방송 컨텐츠 정보 및 사용자 권한(Permission/Constraint)정보를 풀(Pull) 또는 푸쉬(Push)방식으로 획득하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 45.

제40항 내지 제43항 중 어느 한 항에 있어서, 상기 제1클라언트 단말기는,

상기 CAS에 대응되며, DRM패키징을 위하여 필요한 정보를 저장/관리 하는 스마트카드;

상기 방송 컨텐츠를 수신하여 상기 방송 컨텐츠를 저장 및 DRM패키징을 수행하는 DCP(DRM Client Packager);

상기 방송사서버로부터RO(Rights Object)를 전송받아 상기 RO를 이용하여 상기 DRM패키징된 방송 컨텐츠를 재생하는 DRM에이전트; 및

상기 DCP를 통해 DRM 패키징된 방송 컨텐츠를 저장하는 메모리를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

청구항 46.

제45항에 있어서, 상기 DCP는,

상기 방송 컨텐츠의 EID(Event ID)를 기반으로 CID(Content ID)를 생성하는 CID생성기;

상기 CAS서버로부터 전송된CW(Control Word)를 기반으로 CEK(Content Encryption Key)를 생성하는 CEK생성기;

상기 CID와 CEK를 상기 EID를 기준으로 맵핑하는 맵핑기; 및

상기 CW 또는 CEK를 토대로 상기 방송 컨텐츠를 암호화하는 암호화기를 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

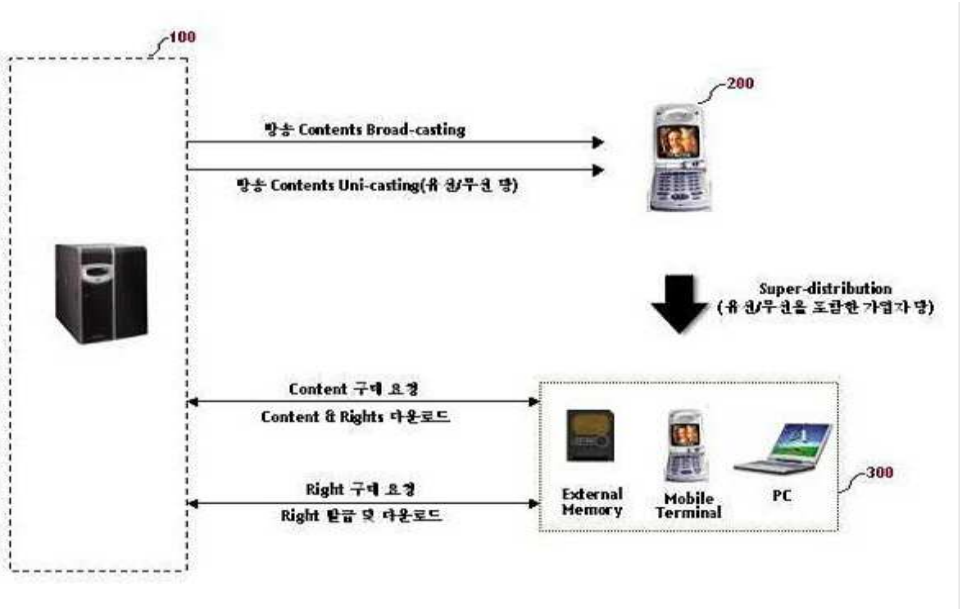
청구항 47.

제45항에 있어서, 상기 스마트카드는

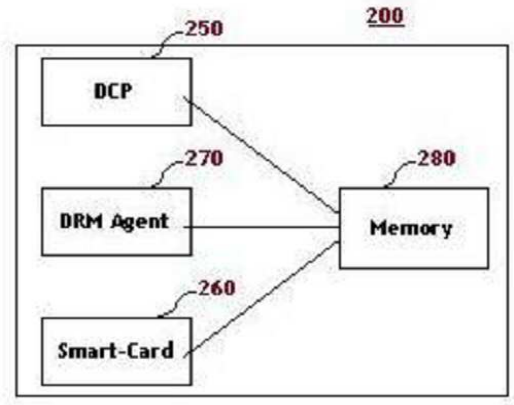
DRM패키징을 위하여 필요한 정보를 저장/관리 하는 USIM(Universal Subscriber Identification Module)을 더 포함하는 것을 특징으로 하는 방송 컨텐츠 보호 시스템.

도면

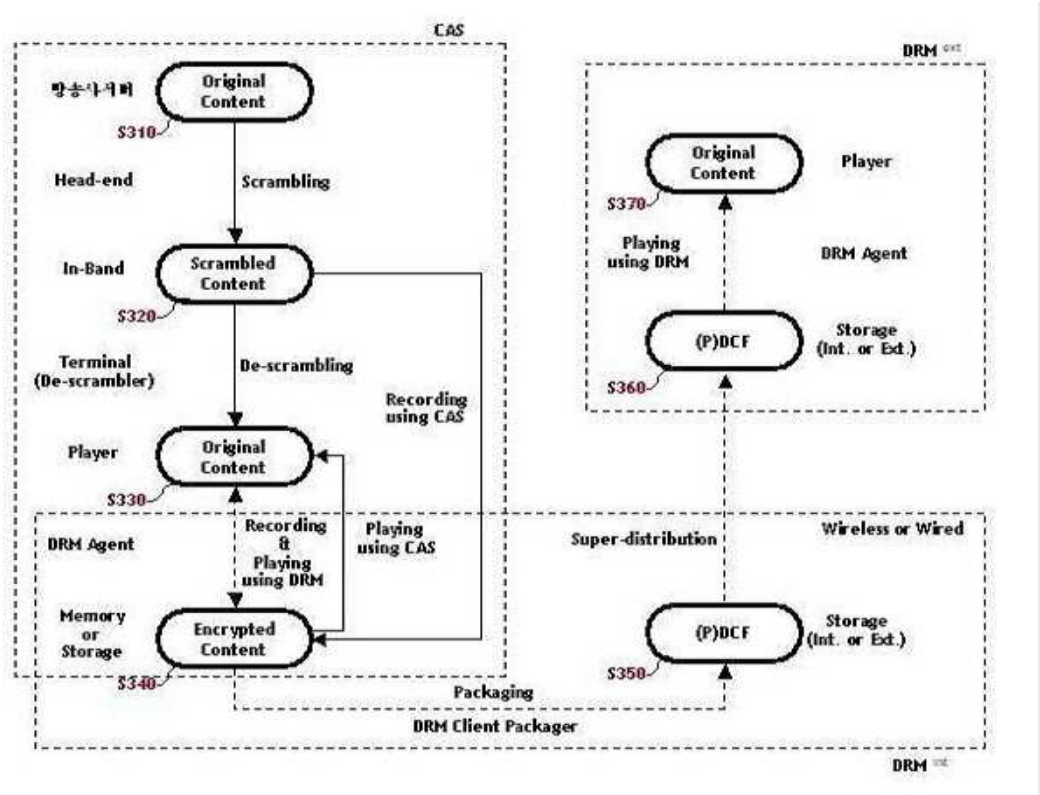
도면1


100
200
방송 Contents Broad-casting
방송 Contents Uni-casting(유 권/무권 택)
Super-distribution
(유 권/무권을 도람한 가입자 택)
Content 구매 요청
Content & Rights 다운로드
Right 구매 요청
Right 받급 및 다운로드
External Memory
Mobile Terminal
PC
300

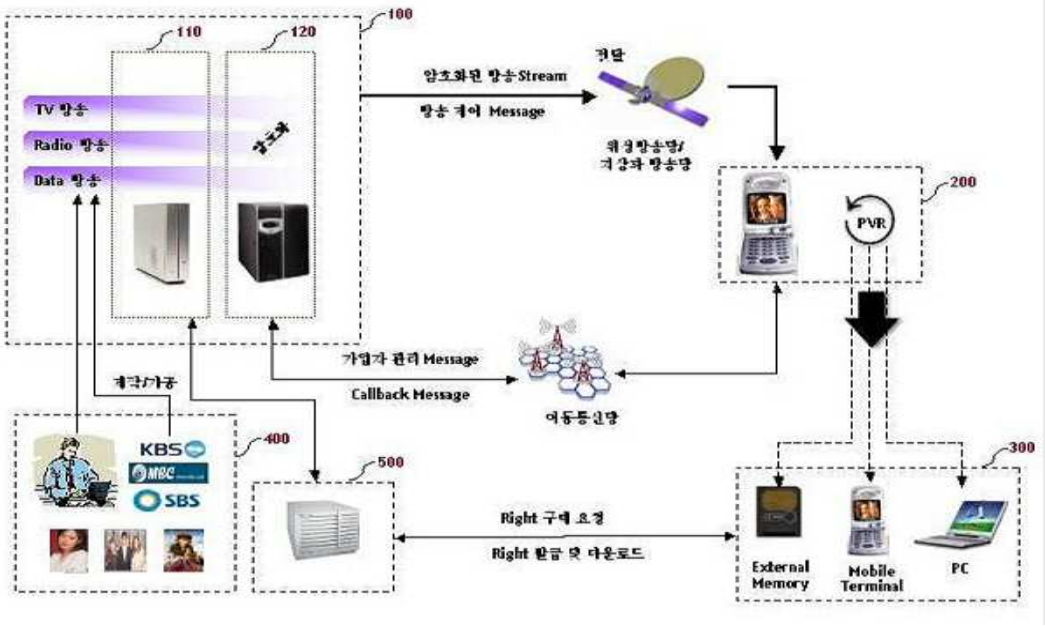
도면2


200
250
DCP
270
DRM Agent
280
Memory
260
Smart-Card

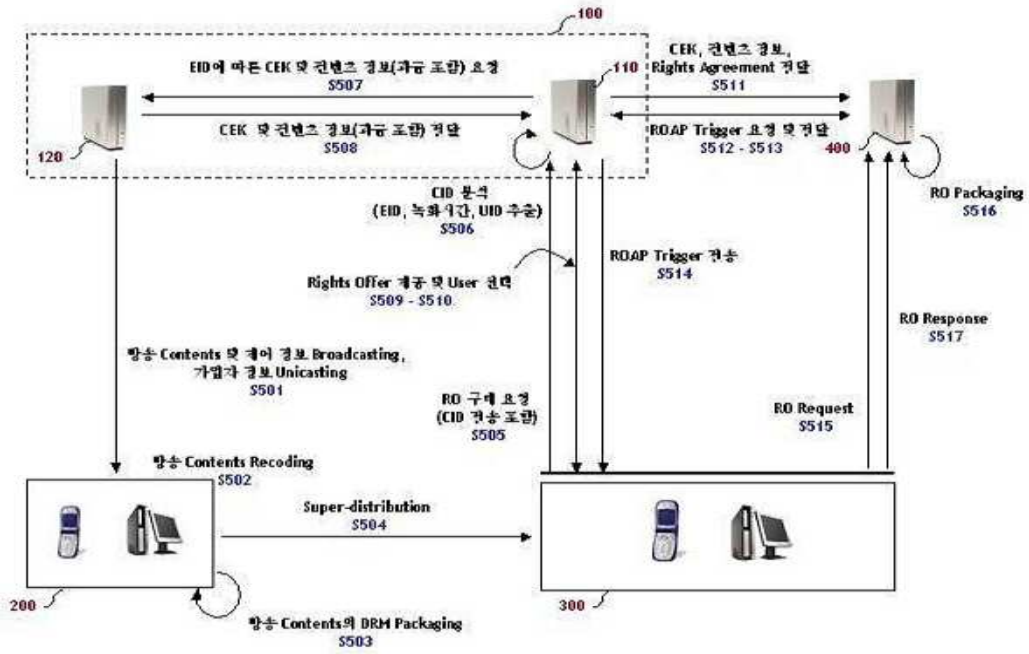
도면3


CAS
DRM
Original Content
S310
Head-end
Scrambling
In-Band
Scrambled Content
S320
Terminal (De-scrambler)
De-scrambling
Recording using CAS
Player
Original Content
S330
DRM Agent
Recording & Playing using DRM
Playing using CAS
Memory or Storage
Encrypted Content
S340
Packaging
DRM Client Packager
Original Content
Player
S370
Playing using DRM
DRM Agent
(P)DCF
Storage (Int. or Ext.)
S360
Super-distribution
Wireless or Wired
(P)DCF
Storage (Int. or Ext.)
S350

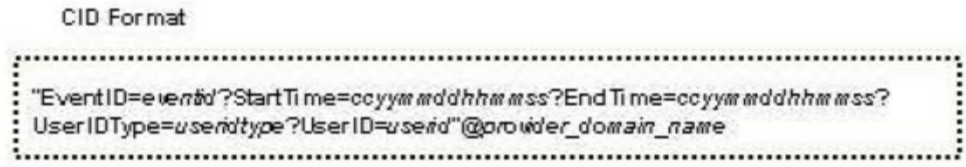
도면4


100
110
120
TV 방송
Radio 방송
Data 방송
암호화된 방송Stream
방송 제어 Message
위성방송망/
지상파 방송망
200
PVR
가입자 관리 Message
Callback Message
이동통신망
400
500
KBS
MBC
SBS
Right 구매 요청
Right 받음 및 다운로드
300
External Memory
Mobile Terminal
PC

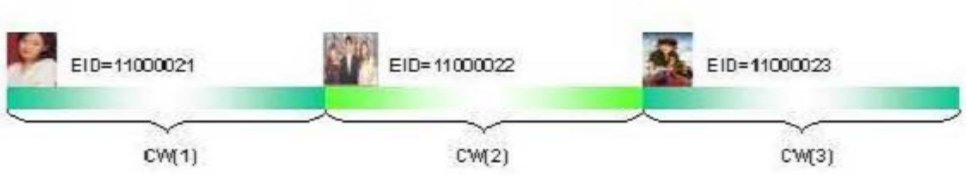
도면5



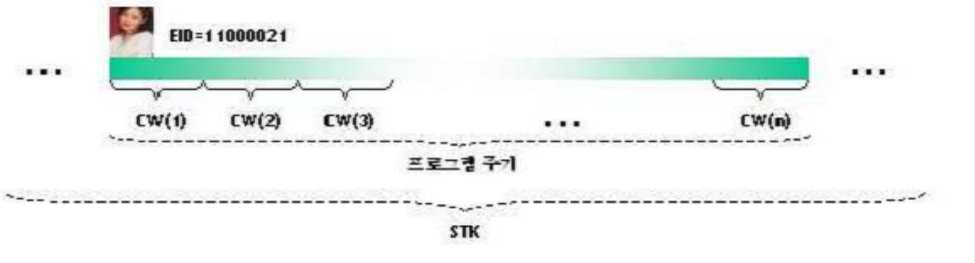
도면6



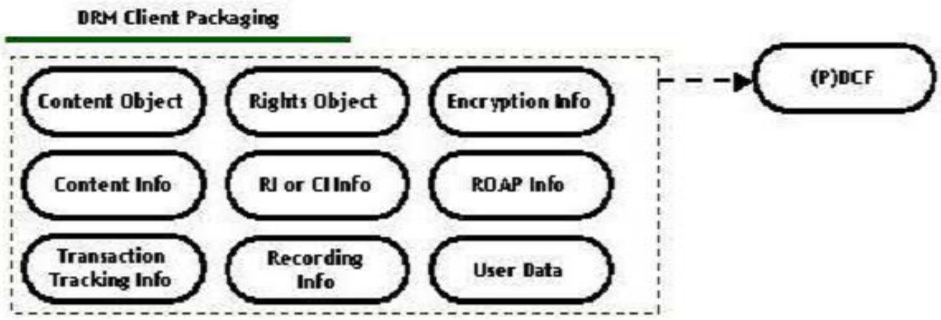
도면7



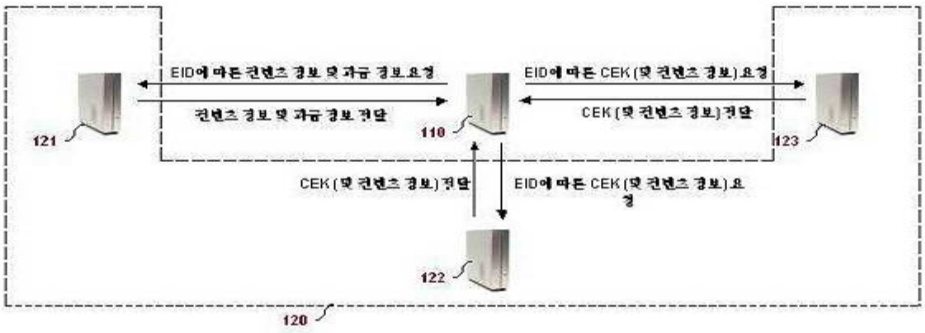
도면8



도면9


DRM Client Packaging
Content Object
Rights Object
Encryption Info
Content Info
RI or CI Info
ROAP Info
Transaction Tracking Info
Recording Info
User Data
(P)DCF

도면10


EID에 따른 컨텐츠 정보 및 과금 정보요청
컨텐츠 정보 및 과금 정보 전달
EID에 따른 CEK(및 컨텐츠 정보)요청
CEK(및 컨텐츠 정보)전달
CEK(및 컨텐츠 정보)전달
EID에 따른 CEK(및 컨텐츠 정보)요청
121
110
123
122
120