DRM 기술 동향

Trends of DRM Technology

융합 시대를 주도할 디지털콘텐츠 기술 특집

박지현 (J.H. Park) DRM연구팀 선임연구원
정연정 (Y.J. Jeong) DRM연구팀 선임연구원
윤기송 (K.S. Yoon) DRM연구팀 책임연구원

목 차

* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S-017-01, 사용자 중심의 콘텐츠 보호·유통 기술]

최근 들어 새로운 형태의 디지털 콘텐츠 관련 시장과 기술 분야가 등장하고 컨버전스나 통방 융합과 같은 흐름에 따라 기존의 산업에 많은 변화가 가해지고 있는데, 이는 기존의 산업에 대한 국외 선도 업체들의 영향력이 약화되고 있음을 의미하고, 새로운 산업 형태에 대해 기술과 표준에 대한 주도권을 확보하기 위한 경쟁이 심화됨을 의미한다. DRM 기술 관련 분야에서도 이러한 현상이 나타나고 있는데, 향후 가장 큰 시장으로 예상되는 디지털 홈 관련 DRM 기술 분야에서 이미 여러 업체 및 표준화 단체를 중심으로 주도권 경쟁을 하고 있다. 본 고에서는 디지털 홈 환경에서의 콘텐츠 보호를 위한 DRM 요소 기술에 대하여 살펴보고, 각 요소 기술 분야에서 강점을 보이는 주요 DRM 기술들에 대하여 설명한다.

Ⅰ. 서론

인터넷의 대중화, 가전제품의 지능화 및 네트워크화, 무선 네트워크의 활성화, 그리고 모바일 기기의 활용 증대와 함께 다양한 서비스와 디지털 콘텐츠의 융합에 따른 디지털 콘텐츠 서비스 기술이 하루가 다르게 발전하고 있다. 특히, 디지털 홈 엔터테인먼트는 세계 IT 및 가전 업계의 화두로 떠오르고 있으며, 이와 더불어 새로운 콘텐츠 소비 환경에서의 콘텐츠에 대한 저작권 문제 또한 관심이 높아지고 있다. 한편, 통방 융합에 따라 기존의 방송서비스는 인터넷을 통한 콘텐츠 서비스로 영역을 넓히고 있으며, 방송된 콘텐츠를 저장한 후 다른 기기로 이동하여 사용할 수 있게 하는 서비스가 시도되고 있다. 이를 지원하기 위하여 방송 프로그램이 송출되는 시점에서만의 콘텐츠 보호만을 목적으로 하던 CAS 기술이 저장 이후 다양한 기기에서의 콘텐츠 사용을 지원하기 위한 영역으로 기술 범위를 넓히려는 시도가 이루어지고 있다.

이와 같은 컨버전스 환경에서 디지털 콘텐츠 산업을 보다 활성화하기 위해서는 다양한 콘텐츠 서비스 모델과 사용자 환경을 지원할 수 있는 DRM 기술과 함께 각 DRM 기술간의 상호호환성을 확보할 수 있는 방안이 마련되어야 한다.

DRM은 디지털 콘텐츠에 대한 불법적인 사용을 효과적으로 차단할 수 있는 기술이지만 아직까지 표준화된 모습을 갖추지 못하고 있기 때문에, 현재 시장에서는 여러 개의 DRM 솔루션들이 공존하고 있는 상태이다. 이러한 이유에서 많은 디지털 콘텐츠들은 통일화되지 않은 여러 DRM 솔루션을 통해 보호를 받고 있다. 각 사용자 기기에 탑재된 DRM은 이를 지원하는 콘텐츠 제공자들의 콘텐츠만을 이용할 수 있도록 제한하기 때문에 사용자에게서 선택의 기회를 박탈하고 있다. 이를 해결하기 위해 콘텐츠 제공자가 각각의 DRM 별로 콘텐츠를 따로 준비하여 제공한다든가, 기기 제조업체가 복수 개의 DRM 클라이언트를 탑재하는 등의 번거로움이 발생하게 된다. 이는 관리 및 비용 등의 문제뿐만 아니라 각 DRM 간의 충돌로 인한 시스템 불안정을 초래할 수 있는 문제점을 지닌다.

이 때문에 최근 DRM 기술은 특정 서비스를 지원하기 위한 기술 개발보다는 다양한 서비스 환경에서 DRM 사이의 상호호환성 지원을 위한 기술 개발이 활발히 이루어지고 있다. 특히, 상이한 망구조의 통합과 서비스/디바이스/콘텐츠의 융합과 같은 디지털 컨버전스 현상이 가속화되고 있는 디지털 홈 환경에서 DRM 기술이 콘텐츠 서비스의 장벽으로 작용할 것으로 예상되는바, 이를 해결하기 위한 표준 및 기술 개발이 진행되고 있다.

본 고에서는 디지털 홈 환경에서의 콘텐츠 보호를 위한 DRM 요소 기술에 대하여 설명하고, 이를 지원하기 위한 주요 DRM 기술들에 대하여 설명한다.

● 용 어 해 설 ●

DRM(Digital Rights Management): 디지털 콘텐츠의 불법유통과 복제를 방지하고, 적법한 사용자만이 주어진 권한 내에서 콘텐츠를 사용케 하여 디지털 콘텐츠 저작권을 관리하는 기술

Ⅱ. 디지털 홈 DRM 요소 기술

콘텐츠 보호 기술은 그 사용목적에 따라 복제방지 기술, CAS, DRM으로 구분된다.

복제방지 기술은 기기간 전송 또는 기록장치로 저장시 콘텐츠의 불법복제 방지를 위한 기술이다. 이 기술은 기기들간 콘텐츠 복사나 이동 시의 콘텐츠 보호는 가능하지만 콘텐츠에 대한 다양한 권한제어가 불가능하다.

CAS 기술은 디지털방송 콘텐츠의 보호를 위한 기술로, 방송망을 통하여 전송되는 콘텐츠에 대하여 허가된 사용자에게만 수신 권한을 부여하는 기술이다. 방송되는 콘텐츠의 수신 권한 제어만을 목적으로 하므로 이를 저장한 이후의 보호 수단 및 다양한 권한 제어를 제공하지 못하였으나, 최근 방송 서비스를 인터넷으로 옮기려는 시도와 함께 저장 이후의

지속적인 콘텐츠 보호를 지원할 수 있도록 기술을 확장하고 있다.

DRM 기술은 콘텐츠의 생성에서 소멸에 이르는 전과정에 걸쳐 콘텐츠의 저작권을 지속적으로 보호하기 위한 기술이다. 기존의 DRM 기술은 주로 저장되는 콘텐츠를 대상으로 하고 있으며, 암호화 기술, 인증 기술, 키관리 기술, 패키징 기술, 권리표현 기술, 사용통제 기술, 탬퍼링 방지 기술 등을 이용하여 콘텐츠를 지속적으로 보호한다.

각각의 영역에서 콘텐츠를 보호해 왔던 이 같은 기술들이 디지털 홈에서는 점차 타 기술의 기능을 포함하는 형태로 확장하고 있으며, 이들간의 상호호환성을 지원하는 기능을 추가하며 발전해 나가고 있다.

DRM 기술의 관점에서 보면 디지털 홈 환경에서 서비스되는 콘텐츠를 보호하기 위한 DRM 기술은 기존의 DRM 기술의 기반 위에 스트리밍 콘텐츠 보호, DRM 상호연동, 도메인 권한 관리 등의 기술이 추가로 지원되어야 한다.

스트리밍 콘텐츠 보호 기술은 네트워크로 연결된 기기를 이용하여 콘텐츠를 서비스하는 환경에서 콘텐츠를 보호하기 위한 DRM 기술로, 일대일 서비스인 VOD 콘텐츠용 DRM 기술과 동시에 여러 사용자에게 서비스되는 멀티캐스트 콘텐츠용 DRM 기술로 구분할 수 있다. 현재 ISMA, OMA, DVB 등에서 표준화가 완료되었거나 진행되고 있는데, CAS와 DRM 기술이 상호 보완적 또는 상호 경쟁적 관계를 형성하며 기술 개발이 진행되고 있다.

DRM 상호 연동은 상이한 DRM 기술들 간의 상호호환성을 보장하는 기술로서 DMP 및 MPEG-21에서 표준화가 진행되고 있다. 국내에서는 한국전자통신연구원(ETRI)에서 DRM 연동 기술인 EXIM 기술을 개발하였으며, 이를 기반으로 하여 MP3 DRM 상호연동 기술이 표준화되었고, 동영상 DRM 상호연동 기술 표준화가 진행되고 있다.

도메인 권한 관리는 사적 복제를 보장을 통한 콘텐츠의 이용 편리성 보장(fair use)을 지원하기 위해, 사용자가 사용하는 기기들(도메인) 간의 자유로운 콘텐츠 이용 및 배포를 허락하는 기술로서 MPEG-21, OMA, DMP, DVB 등에서 표준화가 진행되고 있다.

Ⅲ. 스트리밍 콘텐츠용 DRM 기술

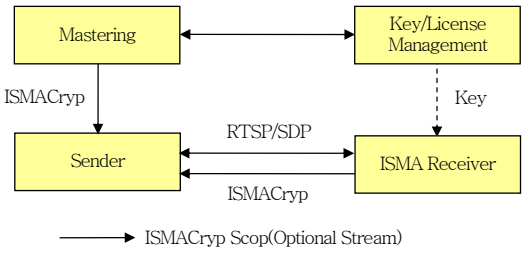
1. ISMACryp

ISMA는 2000년 애플, 시스코, IBM, 소니 등에 의해 설립된 단체로 인터넷기반 콘텐츠 스트리밍 기술에 대한 표준을 제정한다. ISMA 버전 1.0에서는 MPEG-4 part2 비디오 콘텐츠에 대한 스트리밍 방안을 표준화하였고, 버전 2.0에서는 H.264 비디오에 대한 스트리밍 방안을 표준화하였다[1].

ISMACryp은 ISMA 표준을 기반으로 스트리밍되는 콘텐츠에 대한 보호 방안을 기술하고 있는 ISMA 암호화 및 인증(ISMA encryption and authentication) 규격의 별칭이다[2]. ISMA는 ISMACryp 버전 1.1을 2005년 12월에 발표하였고, 현재 2.0에 대한 검토가 진행중이다. ISMACryp은 OMA BCAST의 스트리밍 데이터 보호 방법의 하나로 채택되어 모바일 기기 대상의 콘텐츠 서비스에서 확산이 예상된다[3],[4].

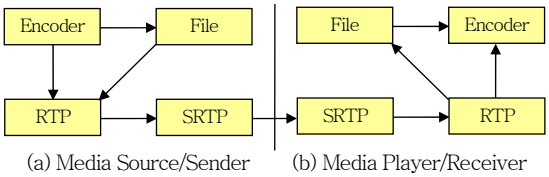
ISMACryp에서 제시하는 DRM 구조는 (그림 1)과 같다. 그림에 나타난 요소 중 키/라이선스 관리(key license management)는 ISMACryp의 규격에 포함되지 않는다.

마스터링(mastering)은 서비스될 콘텐츠를 준비하는 작업이다. 여기서 콘텐츠는 암호화되고 사용권한이 부여된다.



<자료>: ISMA(2005)

(그림 1) ISMA DRM Architecture



(a) Media Source/Sender (b) Media Player/Receiver

<자료>: ISMA(2005)

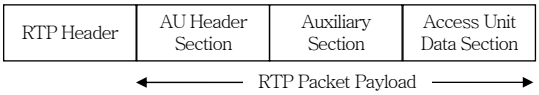
(그림 2) ISMACryp End-to-End Flows

키/라이선스 관리는 권한정보와 암호화키를 콘텐츠와 연관시키는 기능을 한다. 권한정보를 토대로 라이선스를 생성 발급한다. 또한 송신기(sender)에 콘텐츠를 암호화하는 데 사용할 암호화키를 발급하고 수신기(receiver)에게 복호화키를 발급하여 콘텐츠를 사용할 수 있도록 한다.

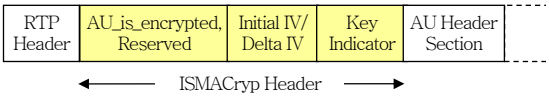
송신기는 ISMACryp 프로토콜을 이용하여 콘텐츠를 수신기에게 전송하는 기능을 한다. ISMACryp 프로토콜에 사용될 정보는 ISMA 1.0과 2.0에 정의된 RTSP/SDP 정보에 ISMACryp 정보를 추가하여 전송하거나, 수신기가 다른 기기로부터 정보를 받게 할 수 있다.

수신기는 보호된 콘텐츠를 복호화하고 인증하여 필요에 따라 제어정보를 복호화하고 인증한다. 수신기는 암호화된 ISMACryp 스트림을 처리할 수 있고, 인증 메시지와 기타 제어정보를 처리한다. 인증된 수신기임을 증명하기 위하여 키/라이선스 관리 서버와 통신하여 인증절차를 수행하는데, 세부 절차는 사용하는 키/라이선스 관리 방법에 따라 달라질 수 있다. 이러한 과정은 라이선스에 의해 제어되는데, 라이선스는 교환되어야 할 인증정보를 결정하며, 콘텐츠에 대한 사용권한 정보를 제공한다.

(그림 2)는 ISMACryp의 송신측과 수신측의 구성환경을 보여준다. 송신기에 의해 전송되는 콘텐츠는 미리 만들어진 보호된 파일일 수도 있고 인코딩 프로그램에 의해 실시간으로 생성되는 것일 수도 있다. 어느 경우에든 암호화는 전송이전에 수행된다. 수신기가 수신한 스트림은 개인용 녹화기(PVR)와 같은 장치를 통하여 파일로 저장될 수도 있고, 바로 디코딩되어 사용자에게 보여질 수도 있다. 송신기에서의 ISMACryp 변환은 인코더 바로 뒤에서 수행되고, 수신기에서의 ISMACryp 해석은 디코더 바로



(그림 3) mpeg4를 전송하는 RTP 패킷 구조



(그림 4) ISMACryp 헤더

앞에서 수행된다. 메시지 인증은 SRTP 송신측과 수신측 사이에서 수행된다.

ISMACryp 패킷은 RTP를 이용하여 전송되는데, (그림 3)과 같이 RFC3610에서 정의한 mpeg4-generic 유료부하 포맷을 기반으로 하고 있다. ISMACryp은 각 AU 헤더의 시작부분에 (그림 4)와 같은 암호화에 관련된 메타데이터를 추가한다.

ISMACryp 헤더에서 AU_is_encrypted는 선택적 암호화가 적용되었을 때 나타나는 필드로 해당 패킷의 암호화 여부를 표시한다. 이 값이 1이면 암호화된 패킷이고, 0이면 암호화되지 않은 패킷이다. initial_IV와 delta_IV는 암호화시 사용한 초기벡터(initial vector) 값을 가진다. key_indicator는 각 AU를 다른 키를 사용하여 암호화하였을 경우 해당 키를 알려주기 위한 필드이다. 기본 암호화 알고리듬으로 AEC-CTR을 채택하고 있으나, 이외의 암호화 방법 사용이 가능하다.

2. MPEG-2 TS 기반 스트리밍 DRM

MPEG-2 TS 콘텐츠를 기반으로 하는 스트리밍 환경을 지원하는 DRM은 서비스 타입에 따라 VOD 지원 DRM과 멀티캐스트 지원 DRM으로 구분할 수 있다. <표 1>은 이들간의 차이를 요약한 것이다.

MPEG-2 TS 기반 스트리밍은 전송 포맷인 MPEG-2 TS에 대한 표준만 있을 뿐, 스트리밍 서버와 클라이언트 사이에 주고 받는 제어정보에 대한 표준은 없기 때문에 각 제품마다 독자적인 방법으로 구현하고 있다. 이 때문에 특정 스트리밍 서버에 종속되지 않도록 DRM 기술이 개발되어야 하는데, 주

〈표 1〉 스트리밍 DRM 비교

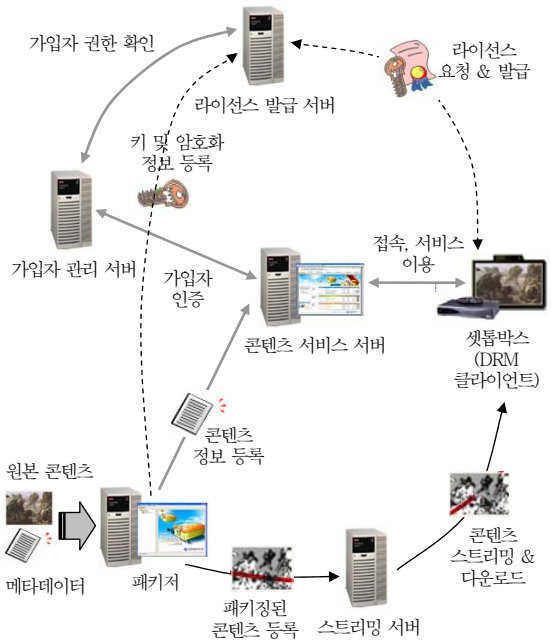
	VOD 지원 DRM	멀티캐스트 지원 DRM
정의	스트리밍 서버에서 하나의 스트림을 IP 망을 통해서 한 명의 사용자에게 전송	스트리밍 서버에서 하나의 스트림을 IP 망을 통해서 동시에 여러 사용자에게 전송
암호화	- Pre-encryption - 파일별로 암호화	- 실시간 live encryption - 채널별로 암호화
키 전달	키를 라이선스에 넣어 단말에 전달	- 스트림에 키를 직접 삽입 - 키를 라이선스에 넣어 단말에 전달
키 갱신	재패키징이 필요하므로 어려움	주기적인 업데이트 가능
응용	소규모 사용자 환경	대규모 사용자 환경

로 MPEG-2 TS 파일 포맷을 유지하면서 DRM을 적용하는 방법을 사용한다.

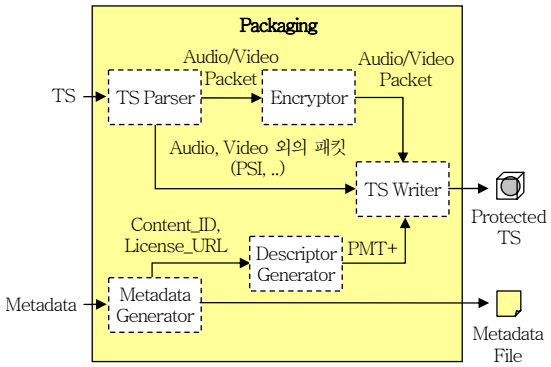
가. VOD 콘텐츠용 DRM

VOD 서비스를 위한 DRM 시스템은 (그림 5)와 같이 가입자 관리 서버, 스트리밍 서버, 패키저, 라이선스 발급 서버, 콘텐츠 서비스 서버, 클라이언트로 구성된다.

콘텐츠에 대한 보호는 패키저와 라이선스 발급 서버에 의해서 수행된다. 패키저는 콘텐츠를 암호화하고, 콘텐츠 관리 및 라이선스 발급에 필요한 정보



(그림 5) VOD 서비스를 위한 DRM 시스템



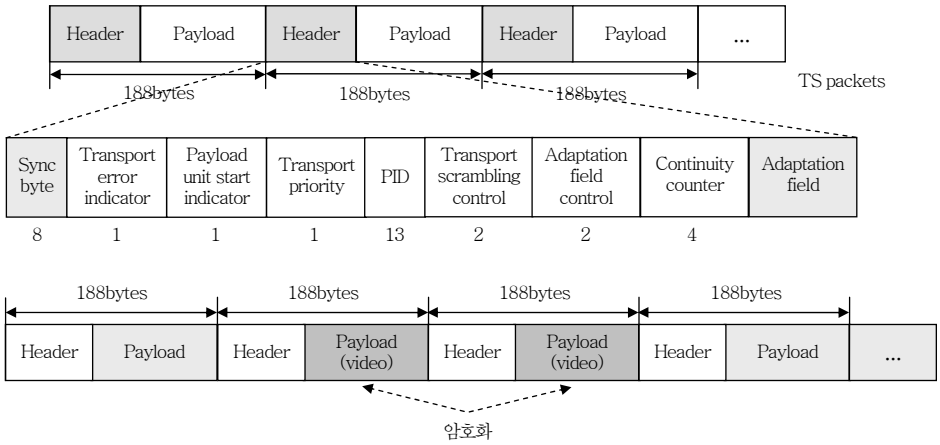
(그림 6) VOD 콘텐츠를 위한 DRM 패키저

를 입력하여 메타데이터를 생성한다. 또한, 패키징 결과물인 암호화된 콘텐츠 및 메타데이터를 VOD 서비스 서버에 전송하는 역할을 한다. (그림 6)은 VOD 콘텐츠를 위한 DRM 패키저의 구조를 보여준다.

서버측에서는 패키징 과정을 통해 콘텐츠를 암호화하고 메타데이터를 콘텐츠에 삽입하여 보호된 형태로 스트리밍이 가능하게 하고, 수신측에서는 언패키징 과정을 통해 암호화된 콘텐츠를 해석하고 재생하게 된다. 이때 사용되는 패키징 메커니즘은 다음의 요구사항을 만족해야 한다.

- 패키징 후에도 동영상 포맷을 유지해야 한다.
- 암호화된 콘텐츠를 스트리밍 서버가 스트리밍 할 수 있어야 한다.
- 복호화로 인한 지연이 발생하지 않도록 한다.

이와 같은 요구사항을 만족하기 위하여 (그림 7)과 같이 MPEG-2 TS의 유료부하 중 스트리밍 서버에 의해 참조되지 않는 부분만을 선택하여 암호화하는 방법을 사용한다.



(그림 7) MPEG-2 TS 암호화

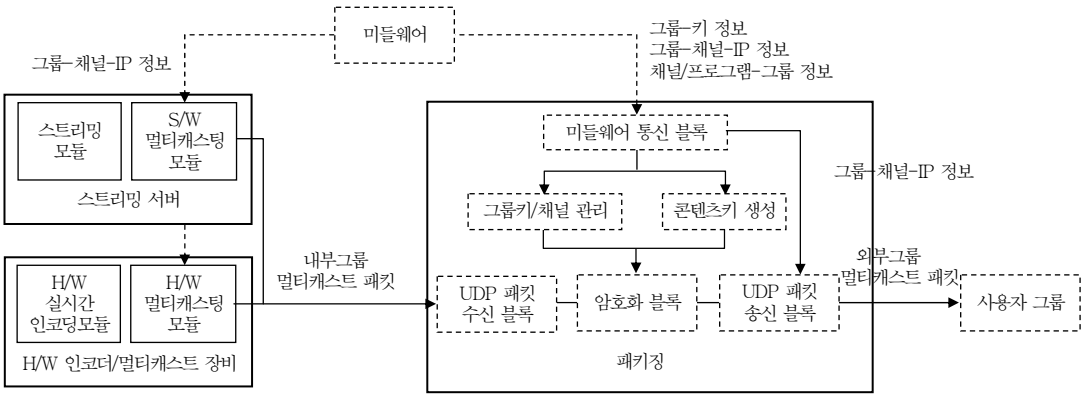
나. 멀티캐스트 콘텐츠용 DRM

멀티캐스트 서비스를 위한 DRM 시스템은 가입자 관리 서버, 스트리밍 서버, DRM 멀티캐스터, 키관리 서버, 콘텐츠 서비스 서버, 클라이언트로 구성된다. 콘텐츠에 대한 보호는 DRM 멀티캐스터와 키관리 서버에 의해 수행된다. DRM 멀티캐스터는 스트리밍 서버로부터 송출된 멀티캐스트 콘텐츠를 각 채널별로 실시간으로 암호화하여 다시 멀티캐스트로 재전송한다. 클라이언트는 스트리밍 서버로부터 송출된 비암호화 방송 콘텐츠가 아니라 DRM 멀티캐스터에서 송출된 암호화된 방송 콘텐츠를 수신한다. DRM 멀티캐스터는 콘텐츠를 암호화할 때 이용하는 키 정보를 키관리 서버로부터 받는다.

키관리 서버는 DRM 멀티캐스터에서 방송 콘텐츠를 암호화할 때 이용하는 키를 생성, 관리한다. 키관리는 멀티캐스트 서비스를 위한 DRM 시스템의 핵심적인 요소이다. 키관리 메커니즘의 궁극적인 목적은 멀티캐스트 그룹의 구성원들이 공유할 수 있는 키를 제공, 관리함으로써 그룹 구성원들이 동시에 동일한 데이터를 안전하게 수신하도록 하는 것이다. 키관리 메커니즘은 크게 멀티캐스트 그룹을 동일한 그룹키로 초기화하는 부분(initialize)과 멀티캐스트 그룹의 그룹키를 변경(rekey)하는 것으로 나눌 수 있다.

일반적으로 멀티캐스트 DRM에서는 사용되는 암호화키는 그룹키, 채널키, 미디어의 계층적인 구조를 가지며, 각각의 기능은 다음과 같다.

- 미디어키(Media Encryption Key): 채널로 전



(그림 8) 멀티캐스트 콘텐츠를 위한 DRM 패키저

송되는 미디어 스트림을 암호화하는 데 사용된다. 채널 속의 각각의 프로그램별로 서로 다른 미디어키로 암호화를 적용하여 프로그램 단위의 접근 제어를 제공하는 데 사용될 수 있다. 주기적으로 변경되며, 채널키로 암호화되어 멀티캐스트 스트리밍 채널에 삽입되어 전달된다.

- 채널키(Channel Key): 각각의 방송 채널에 주어진 키로 미디어키를 암호화하는 데 사용되며, 주기적으로 변경된다. 채널키는 그룹키로 암호화되어 멀티캐스트 스트리밍 채널을 통해 전달된다.
- 그룹키(Group Key): 하나의 그룹은 여러 개의 채널로 구성되며, 각각의 그룹에 대해 주어진 키를 말한다. 따라서 그룹키는 해당 그룹에 포함되어 있는 채널들의 집합에 대한 접근 권한이 된다.

(그림 8)은 이들 키를 사용하여 멀티캐스트 콘텐츠를 보호하는 패키저 구조를 나타낸다.

Ⅳ. 도메인 권한 관리 기술

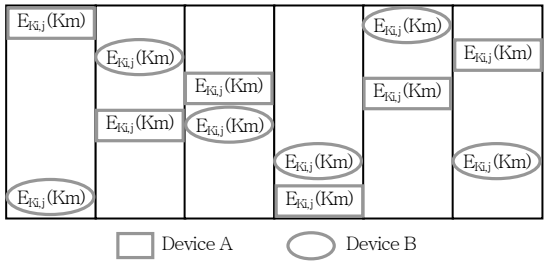
도메인은 디지털콘텐츠 소비의 기본 단위인 사용자 또는 단말기로 구성된 집합적인 개념으로서, 기존의 DRM이 개별 사용자별로 혹은 개별 단말기별로 인증하고 권한을 부여했던 것에 반해, 특정 사용자가 소유한 다수의 단말기 또는 한 가정의 구성원과 그들의 단말기와 같은 좀 더 상위 단계의 개념에 대해 인증과 권한 부여를 수행하기 위한 DRM에서의 권한 관리 단위이다. 도메인 권한 관리 기술은 도메인을 구성하는 디바이스간의 상호 인증처리 기술과 도메인 내의 콘텐츠 권리정보 관리 기술을 포함하며 xCP[5]와 DVB-CPCM[6] 등에서 이를 지원하고 있다.

1. xCP

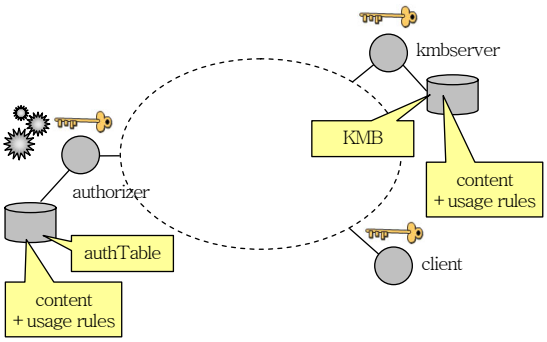
xCP는 IBM이 디지털 홈 네트워크 안에서의 콘텐츠 보호를 위해 2003년 발표한 DRM 기술로, 디지털 홈 환경에서 사용되는 기기들을 도메인 개념으로 관리하여 이들간의 콘텐츠 공유를 가능케 하는 기술이다. xCP 클러스터 프로토콜(xCP cluster protocol)이라고도 불리는 이 기술은 특정 저장장치나 전송 인터페이스 및 프로토콜에 무관하게 네트워크 기능을 가진 저장장치 또는 재생장치로 콘텐츠를 전달함에 있어 효과적인 복제방지를 할 수 있는 방법을 제시하고 있다. 이 기술은 디지털 홈을 하나의 보호된 도메인으로 간주하여 홈 네트워크에 연결된 기기들간의 콘텐츠 이동 및 복사는 아무 제약없이 가능하게 하는 반면, 홈 네트워크를 벗어나는 콘텐츠는 반드시 보호된 형태로 만들어지도록 강제한다.

xCP는 브로드캐스트 암호(broadcast encryption)에 기반하고 있으며 휴대용 저장 매체에서의 콘텐츠 보호를 위한 기술인 CPRM[7]에서 사용하는 MKB와 유사한 키집합인 KMB를 사용하여 콘텐츠를 보호한다[8]. KMB는 암호화키로 사용될 수 있는 많은 수의 난수들의 행렬로, 디지털 홈 구성시 외부 키발급 서버에 의하여 디지털 홈내 키관리 서버에 발급된다. 이 행렬의 각 열은 하나의 공통된 키를 각 기기들에 부여된 비밀키를 이용하여 암호화한 값을 가지며, 각 기기들은 각 열마다 하나의 값을 열어볼 수 있다. (그림 9)는 KMB의 일례를 나타낸다. 그림에서 사각형과 타원으로 표시된 값들은 각각 단말기 A와 단말기 B에 할당된 키를 표시한다. 만약 어떤 단말기가 콘텐츠 유출을 위한 비정상적인 동작을 한다면 이 단말기가 사용하는 키들을 무효화시킴으로써 콘텐츠를 보호할 수 있다.

각 도메인에는 키관리 서버(KMB server)가 존재하여 KMB를 관리하고 이를 갱신하는 기능을 한다. 키관리 서버는 신뢰할 수 있는 외부 서버와 연결



(그림 9) Key Management Block



(그림 10) xCP 클러스터 모델

하여 갱신되는 미디어키 정보를 받아 온다. 각 기기들은 도메인에 참여할 때 키관리 서버로부터 KMB를 받아 오고 이를 이용하여 도메인 내에서 사용되는 공유키를 계산한다. 인증서버(authorizer)는 기기들이 클러스터에 참여시 외부의 인증서버를 대신하여 이를 인증하는 기능을 한다. (그림 10)은 이들 서버를 포함한 xCP 클러스터 모델을 보여준다.

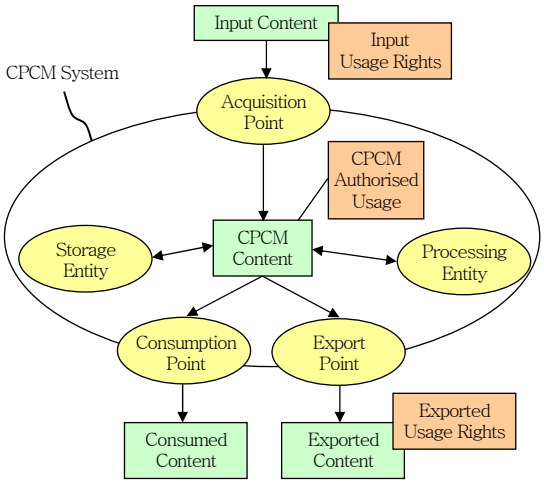
하나의 클러스터에 속한 기기들은 KMB와 클러스터 ID를 공유하게 되며, 도메인 내의 콘텐츠는 암호학적으로 해당 도메인 내의 기기들만 복호화 할 수 있도록 암호화된다. xCP는 인증된 기기들만이 도메인에 참여할 수 있도록 하며, 특정 기기에 대한 인증을 철회할 수 있는 방안을 제공한다.

xCP는 내부적으로 두 가지 종류의 암호화키인 타이틀키(title key)와 바인딩키(binding key)를 사용한다. 타이틀키는 콘텐츠나 콘텐츠 스트림을 암호화하는 데 사용된다. 바인딩키는 각 타이틀키를 암호화하는 마스터키(master key)로서 각 홈 네트워크마다 다르며 홈 네트워크에 새로운 기기가 추가되거나 KMB가 바뀌면 갱신된다.

일반적으로 사용자가 새로운 기기를 자신의 디지털 홈에 설치할 때 사용자에 의한 설정과정에서 오는 불편함과 더불어 어떠한 정보를 설정과정 중에 입력해야 하는지 등에 대한 어려움이 발생할 수 있다. xCP는 기기 등록을 위한 절차 및 기기 인증, 키 발급, 도메인 참가 등의 작업이 사용자의 손을 거치지 않고 자동적으로 수행될 수 있도록 구성되어 있다.

2. DVB-CPCM

DVB-CPCM은 DVB 표준을 따르는 디지털 방송 콘텐츠가 CAS에 의해 보호되는 사용 범위를 넘어서 디지털 홈 환경이나 개인용 녹화기 등에 저장될 때 지속적인 콘텐츠 보호를 위한 표준 사양이다. 이 기술은 (그림 11)과 같이 디지털 홈 환경에서의 콘텐츠 유통에 대해 AP, SE, PE, CP, EP와 같이 2개의 개체(entity)와 3개의 외부와의 접점(point)으로 구성된 참조모델을 제시하고, 이에 따른 각 구성요소들 간의 역할과 기능을 정의하고 있다.



<자료>: DVB(2005)

(그림 11) CPCM의 구성 개체

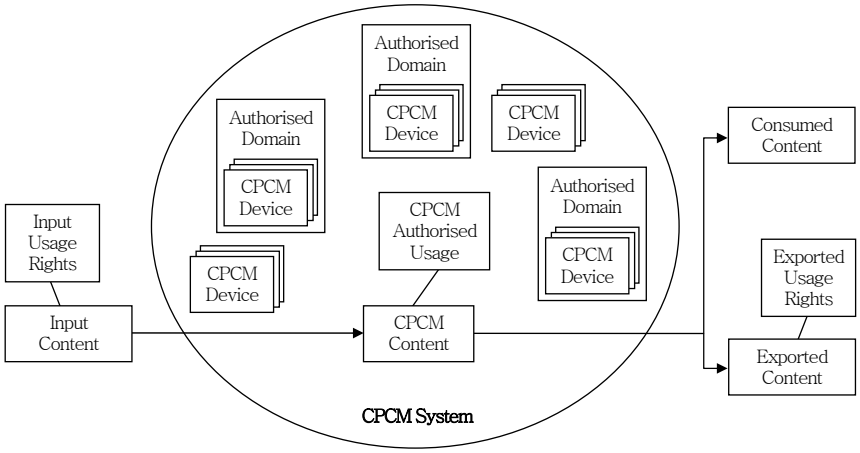
DVB-CPCM에서는 도메인(authorised domain)의 개념을 통하여 도메인 권한 관리 기술을 제공하고 있다. 도메인은 DVB-CPCM을 지원하는 기기들 중 하나의 디지털 홈에 속하여 사용되는 기기들의 집합으로 콘텐츠의 정당한 이용을 위한 신뢰성 있는 환경을 나타낸다. 이에 속한 기기들간 콘텐츠의 자유로운 이동 및 사용을 보장하며, 이를 벗어난 콘텐츠의 사용을 제한한다. (그림 12)는 도메인 개념을 지원하는 CPCM의 개념적인 구조를 보인다.

하나의 CPCM 기기는 한 번에 하나의 도메인에만 속할 수 있고 마찬가지로 하나의 콘텐츠는 하나의 도메인 내에서만 사용될 수 있다.

도메인 관리(authorised domain management)

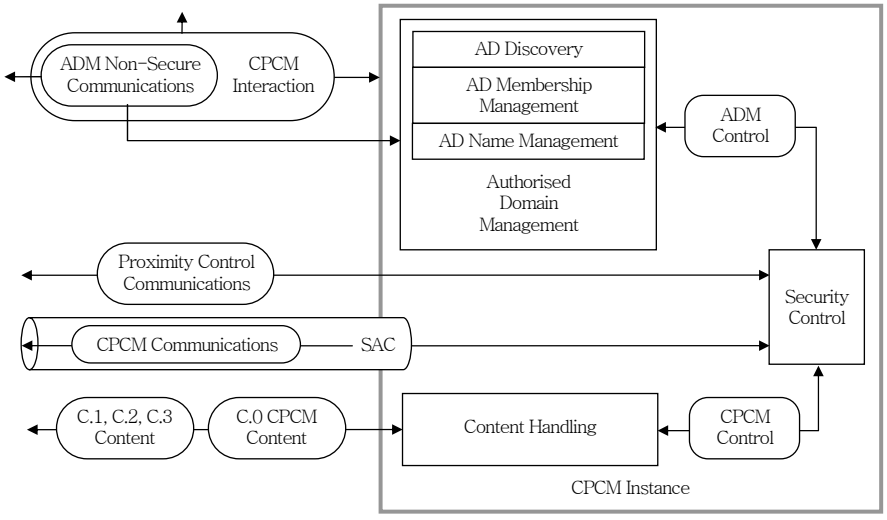
는 기기들이 동적으로 도메인에 참가하거나 탈퇴할 때 지켜져야 할 규칙들을 정의하고 있으며, (그림 13)과 같이 도메인 탐색(AD discovery), 도메인 구성원 관리(AD membership management), 도메인 이름 관리(AD name management)의 기능을 수행한다. 도메인 탐색은 CPCM 기기로 하여금 자신이 참가할 수 있는 도메인을 검색하거나, 하나의 디지털 홈 내에 다수의 도메인이 존재할 경우 기기가 속한 도메인을 다른 도메인에게 알려주기 위한 기능을 제공한다. 도메인 구성원 관리는 단말기가 도메인에 참가하는 과정 또는 탈퇴하는 과정을 처리하거나 새로운 도메인을 생성하는 기능을 제공한다. 도메인 이름 관리는 사람이 인식할 수 있도록 각 도메인에 도메인 이름을 부여하고 관리하는 기능을 제공한다.

DVB-CPCM에서의 권한 정보는 USI를 이용하여 표현할 수 있는데, USI는 도메인 내 또는 특정 지역 내에서 콘텐츠에 대한 복사, 사용, 이동에 관한 권한을 표현할 수 있으며, 다른 콘텐츠 보호 시스템으로 콘텐츠를 내보내기 위한 권한의 표현도 정의하고 있다.



<자료>: DVB(2005)

(그림 12) CPCM 시스템의 개념 구조



<자료>: DVB(2005)

(그림 13) CPCM 도메인 관리

V. DRM 상호연동 기술

현재 DRM 기술 분야에서 가장 핵심적으로 제기되는 문제 중 하나가 상이한 DRM 기술들간의 상호호환성을 어떻게 보장할 것인가의 문제점이다. 이와 같은 문제점을 해결하기 위하여 MPEG-21, OMA, Coral, DMP 등 DRM 표준화 단체들이 생겨났다. 이러한 DRM 표준화 단체들 외에도 디지털 방송 콘텐츠의 보호를 위해 ATSC, CableLabs, DVB 등에서 CAS 규격과 셋톱박스의 복제 방지를 위한 기술규격을 마련하였으며, DRM과의 상호연동을 위한 규격까지 확장하고 있다. 국내에서는 한국전자통신연구원에서 DRM 연동기술인 EXIM을 개발하였고 한국정보통신기술협회(TTA)를 통하여 국내 MP3 DRM 연동 기술로 표준화되었고 현재 동영상 DRM 연동을 위한 표준화를 진행중이다.

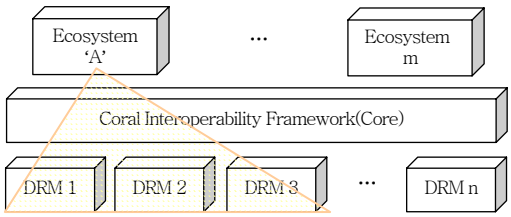
1. Coral

Coral은 서비스업체, 기기, 콘텐츠 포맷, DRM에 상관없이 디지털 음악이나 영화 등을 소비자들이 즐길 수 있도록 하기 위한 표준화를 진행하는 단체로, 2005년 4월에 기술규격에 대한 버전 1.0을 시작으로 2006년 6월 버전 3.0을 발표하였다[9],[10].

DRM 상호호환에 관한 기반 시스템 요소들을 정의하고, 이 기반 위에 실세계에서 발생할 수 있는 각 비즈니스 모델을 에코시스템(ecosystem)[11]으로 정의하여 현실적인 적용방안을 제시하고 있다. 각 에코시스템은 사용 모델, 정책, 기 정의된 역할(role) 중 해당 에코시스템 구현에 필요한 역할과 추가적으로 필요한 역할, 확장기능, 필요한 타 기술 등에 대해서 정의한다.

(그림 14)는 에코시스템의 예를 보여주고 있는데, 다수의 DRM과 다수의 에코시스템이 존재할 수 있으며, 이 중 에코시스템 A는 Coral 프레임워크를 사용하여 DRM 1, DRM 2, DRM 3 사이의 상호호환성을 제공한다.

<표 2>는 Coral에서 정의하고 있는 29개의 역할



(그림 14) Coral의 Ecosystem

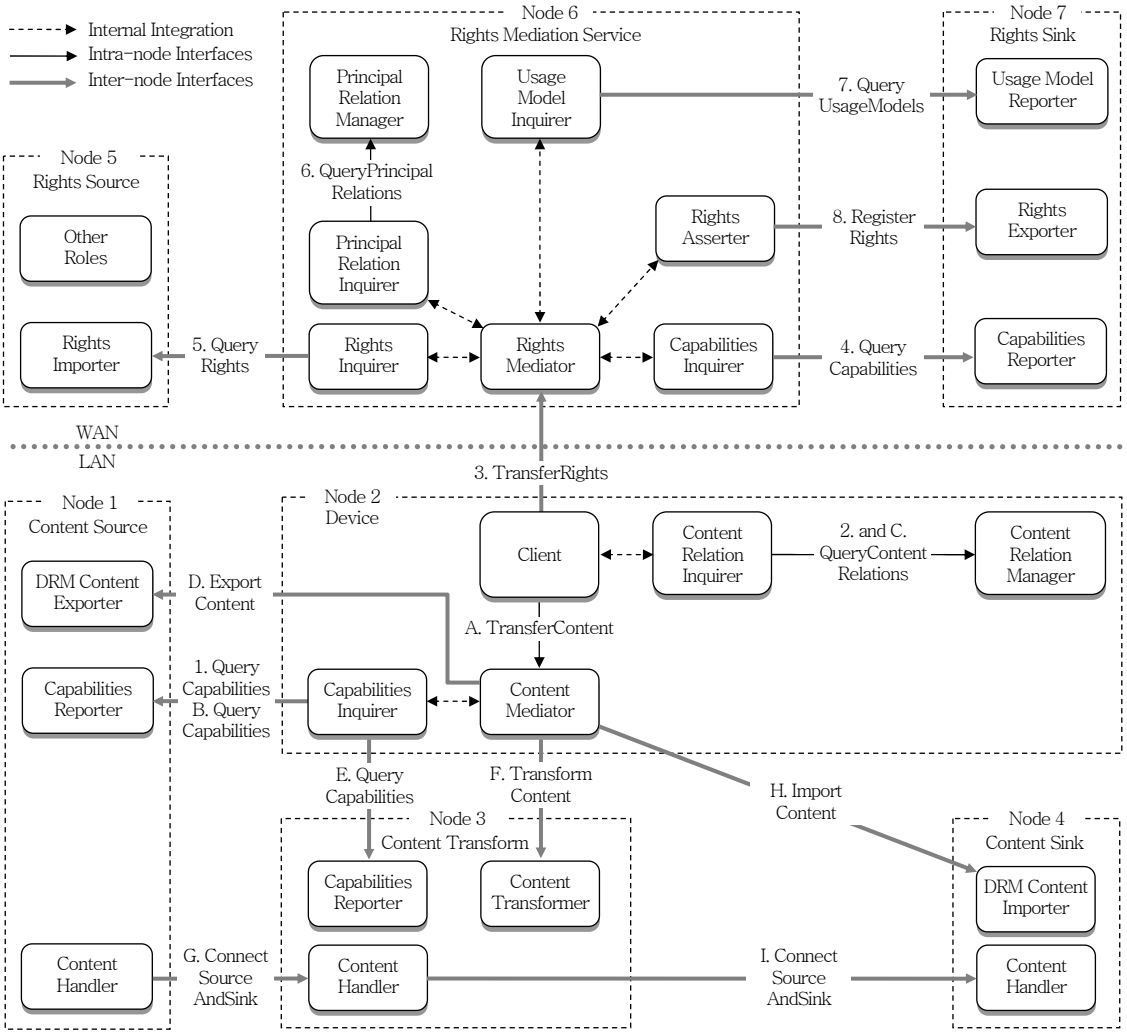
〈표 2〉 Coral 프레임워크에서의 주요 역할모델

역할	기능
DRM License Issuer	Rights token으로부터 라이선스를 생성
Capabilities Reporter	기기, DRM 시스템, 콘텐츠 시스템 등에 관한 정보를 알려줌
Rights Importer	권한 정보를 rights token을 이용하여 다른 개체에 알려줌
Rights Exporter	Rights mediator에서 생성된 rights token을 받아서 저장함
Rights Mediator	권한 변환에 필요한 정보를 수집하고, 권한 변환을 승인할 것인지를 판단
DRM Content Exporter	미리 정해진 방법에 의하여 DRM 콘텐츠를 신뢰할 수 있는 개체로 내보냄
DRM Content Importer	미리 정해진 방법에 의하여 반입된 콘텐츠를 자신의 DRM 콘텐츠로 패키징
Content Mediator	한 DRM 콘텐츠를 다른 DRM 콘텐츠로 변환
Client	사용자로부터 입력을 받아 rights mediator와 content mediator에 DRM 변환을 요청

모델 중 핵심적인 몇 가지 역할의 기능을 설명한다.

Coral 프레임워크를 통한 DRM 상호 연동은 접속 모델(online model), 비접속 모델(offline model), 혼합 모델(hybrid model)로 구분될 수 있다. 접속 모델의 경우 권한의 중개가 네트워크로 연결되어 있는 외부 권한 중개서버에 의해 수행되고, 반입 DRM에서 사용할 수 있는 콘텐츠가 검색된 후 네트워크를 통해 전송된다. 비접속 모델의 경우 권한의 중개, 콘텐츠 전송이 로컬 환경 내에서만 이루어지고 DRM 재패키징 또한 로컬환경에서 수행된다. 혼합 모델의 경우 권한의 중개와 콘텐츠의 변환이 네트워크와 로컬환경에서 각각 수행되는 경우이다.

(그림 15)는 권한의 중개는 네트워크를 통해 이루어지고 콘텐츠의 재패키징은 로컬환경에서 수행되는 혼합 모델을 통한 DRM 변환을 보여준다.



<자료>: Coral(2006)

(그림 15) 혼합 모델기반 DRM 변환

2. EXIM

EXIM 기술은 다양한 DRM 솔루션으로 보호되어 있는 디지털 콘텐츠들이 서로 상대방의 DRM 포맷으로 쉽고 안전하게 변환이 될 수 있는 변환 중재자 역할을 함으로써, 한 개의 DRM 클라이언트만을 가지고 있는 기기에서도 EXIM 기능을 통해 여러 종류의 DRM 콘텐츠를 사용할 수 있도록 해주는 DRM 상호연동 지원 기술이다. EXIM 기술은 상이한 기술규격을 가지는 DRM 시스템들을 통해 디지털 콘텐츠의 지속적 보호 및 권리제어가 유지될 수 있도록 상이한 DRM 제품에 독립적인 디지털 콘텐츠 전송 포맷, 라이선스, 메타데이터로 변환을 적용하는 개념적 모델을 바탕으로 하고 있다. EXIM은 DRM 시스템 간 디지털콘텐츠의 상호연동을 위한 기술규격을 제시할 뿐 아니라 공개적인 기술규격을 목표로 하고 있기 때문에 매우 간단하면서도 호환성을 보장하는 구조를 제공하고 있다.

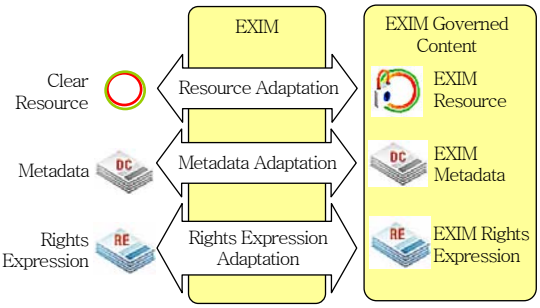
EXIM은 각 DRM 솔루션들이 자신의 DRM 구조를 공개하지 않고서도 효율적으로 타 DRM 포맷으로 변경할 수 있을 뿐만 아니라, 한번 생성해 놓은 반출(export) 모듈, 혹은 반입(import) 모듈들은 모

든 DRM 솔루션에 대해서 재구현 없이 상대방에 대한 인증 작업만으로 해당 모듈에 대한 재사용이 가능하여 N-to-N 관계의 복잡한 DRM 솔루션 업체들이 상호호환성을 유지하기 위해 매우 효율적으로 사용될 수 있는 기술이다.

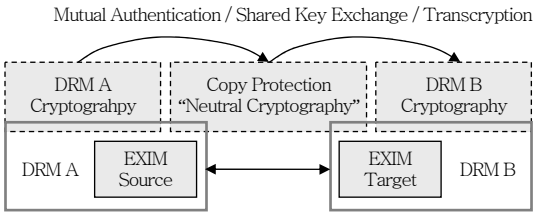
가. EXIM 변환(EXIM adaptation)

상이한 DRM 시스템간 콘텐츠의 호환성을 보장하기 위해선 상이한 콘텐츠 패키징 포맷, 라이선스 구조, 그리고 메타데이터에 대한 변환 작업이 필요하다. EXIM은 이를 위해 (그림 16)에서 보이는 바와 같이 콘텐츠 포맷, 라이선스, 메타데이터에 대해 중립적인 기술규격을 제시하고, 이를 통해 상이한 DRM 시스템이 콘텐츠를 호환할 수 있도록 할 뿐만 아니라 지속적인 보호를 가능케 하는 방식을 제시한다. 이를 통해 콘텐츠는 상이한 DRM 시스템을 통해서 호환성을 갖고 유통될 수 있게 된다.

DRM간 상호호환성을 보장하는 측면도 매우 중요하지만 상호연동을 위해 DRM의 보안성이 훼손되는 것은 매우 심각한 결과를 초래할 수 있기 때문에 상호간 보안의 신뢰성을 만족하면서 디지털 콘텐츠의 호환성을 보장하는 방식이 필요하다. 일반적으로 상이한 DRM 시스템이 상호호환성을 갖기 위해선 자신 또는 상대방의 DRM 기술규격을 공개하지 않으면 안되는데, 각 DRM 시스템에서 사용하고 있는 암호화 기술이나 콘텐츠 암호화키 관리 방식 등과 같은 DRM 기술의 세부 내용은 DRM의 핵심기술로 만약 이들의 세부사항이 공개될 경우 DRM 제품의



(그림 16) EXIM 변환 개념적 모델



(그림 17) EXIM 보안 모델

보안성이 취약해질 수 있는 위험성이 있기 때문에 DRM 공급자들은 이 부분이 외부로 공개되는 것을 몹시 꺼리고 있다.

EXIM은 (그림 17)에서 보는 바와 같이 각 DRM 시스템들의 세부 DRM 기술에 대한 공개없이 DRM 쌍방간 독립적인 중립적 암호화 채널을 형성함으로써 각 DRM 시스템들이 독자적인 기술규격을 유지하면서 호환이 될 수 있는 기술기반을 제공하고 있다.

나. 키 교환(Key Exchange)

DRM의 보안성을 유지하기 위한 핵심요소는 콘텐츠를 복호화 할 수 있는 암호키의 안전한 전달 및 관리라고 할 수 있다. EXIM은 반출 DRM과 반입 DRM 간 공유키를 공유하기 위해 1) 반출 모듈에서 암호키를 생성하고 이를 반입 모듈의 공개키를 이용하여 암호화 전송하는 방식과, 2) Diffie-Hellman 키합의방식을 이용하여 안전하고 보안성이 높은 공유키를 생성하는 방식을 제시하고 있다.

다. 소프트웨어 인증(Software Authentication)

EXIM은 공개된 기술규격을 이용하여 상이한 DRM 시스템간 연동이 가능할 수 있도록 함을 목적으로 하고 있다. 공개된 기술규격을 기반으로 하고 있기 때문에 악의적인 목적을 갖고 반입 모듈을 개발 또는 변형하고자 하는 시도가 있을 경우, 심각한 보안 위협에 노출될 수 있는데. 이를 해결하기 위해 반출 DRM과 반입 DRM은 상호 연동을 위해 상호 협의된 인증절차를 거쳐 신뢰성이 보장된 모듈임을 확인 받을 수 있는 절차가 필요하다. EXIM은 상호 신뢰성 있는 인증기반을 마련하기 위해 소프트웨어

인증서를 상호 확인할 수 있도록 기술 규격을 제공한다. 소프트웨어 인증서는 EXIM 인증기관과 같은 공인된 인증기관을 통해 발급된 것일 수도 있으며, 연동이 필요한 DRM간 상호 협의에 의해 사설 인증서를 이용할 수도 있다.

라. 기기 인증(Device Authentication)

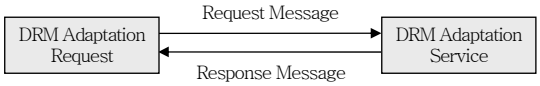
DRM으로 패키징된 콘텐츠는 콘텐츠 유통사의 비즈니스 정책에 따라 특정한 조건을 만족하는 기기(예: 제조사, 제품 모델, 일련번호 등)에서만 이용이 통제되도록 제한될 수 있어야 한다. 이를 위해 연동이 요구되는 기기 간에는 대상 기기에 대한 기기 정보를 교환할 수 있는 기술규격이 필요하다. EXIM은 대상 기기에 대한 기기 정보를 교환할 수 있도록 기기 인증에 관한 기술규격을 제시한다.

마. 콘텐츠 전달

EXIM 헤더에 필요한 헤더 정보를 추가하고, 각각의 EXIM 바디(body) 항목들의 위치를 명시하여 분리할 수 있도록 하고, 헤더와 바디에 대하여 해시코드의 계산과 전자서명을 수행한 결과를 삽입하여 EXIM 콘텐츠의 무결성을 제공한다. EXIM 바디는 리소스(resource), 메타데이터, 사용권한으로 구성된다.

바. EXIM 응용프로그램 참조 모델

EXIM을 이용한 응용프로그램은 자신의 DRM 콘텐츠를 타 DRM 시스템으로 전달하고자 하는 반출



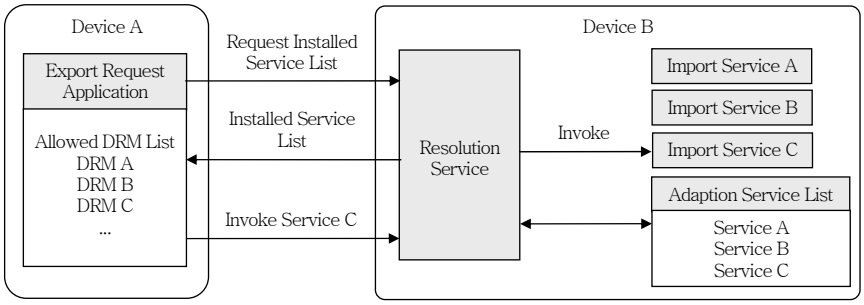
(그림 18) EXIM 응용프로그램 개념 모델

응용프로그램 형태와 타 DRM 콘텐츠를 자신의 DRM 시스템으로 가져오고자 하는 반입 응용프로그램으로 구분된다. (그림 18)과 같이 두 가지 형태의 응용프로그램은 모두 서비스를 요청하는 EXIM 요청(requestor) 모듈과 요구된 서비스를 수행하는 EXIM 서비스 모듈로 구성되는데, EXIM 서비스는 EXIM 요청에 의해 실행되어 요구되는 서비스를 마치게 되면 종료된다.

EXIM 요청과 EXIM 서비스는 네트워크를 기반으로 원격에 위치할 수 있다. 이때 EXIM 서비스는 항상 실행상태에 있으면서 요청을 처리하는 모델이 될 수도 있고, (그림 19)와 같이 요청을 받아 EXIM 서비스를 실행시켜 주는 모듈을 사용하는 모델이 있을 수 있다.

다운로드 동영상 콘텐츠를 위한 EXIM 라이브러리는 일반적으로 동영상 콘텐츠의 크기가 매우 크다는 특성을 고려하여 동영상 파일 전체를 암호화하여 전달하는 통신방법인 비제어형(uncontrolled mode)과 임의의 패킷으로 나누어 전달할 수 있는 통신방법인 제어형(controlled mode)을 모두 지원한다.

비제어형 통신은 EXIM 요청과 EXIM 서비스 사이에 전달되는 데이터의 단위가 원본 콘텐츠를 통째로 암호화한 EXIM 콘텐츠인 통신방법을 의미하며 콘텐츠의 크기가 작을 경우 유용한 방식이다. 제어형 통신은 전달하고자 하는 콘텐츠의 크기가 매우



(그림 19) 네트워크 기반의 EXIM 응용프로그램 개념 모델

클 경우 사용되는 통신방법으로 EXIM 콘텐츠를 원하는 크기로 나누어 전달하는 방식이다. 크기가 큰 동영상 EXIM 콘텐츠를 다른 기기로 전달하는 데 유용한 방식이다.

Ⅵ. 결론

지금까지의 DRM 기술은 특정 서비스 내에서의 콘텐츠 보호를 목적으로 하였지만 향후에는 다양한 서비스 환경에서 DRM 사이의 상호호환성 지원을 위한 기술이 더 요구될 것이다. DRM 상호호환성은 다양한 기기/플랫폼/콘텐츠/서비스가 혼재된 디지털 홈 환경에서 필수적으로 지원되어야 하는 기술로 인식되고 있다.

본 고에서는 디지털 홈 환경에서의 DRM에 요구되는 기술인 스트리밍 콘텐츠 보호 기술, 도메인 관리 기술, DRM 상호연동 기술에 대하여 살펴 보았고, 이들을 지원하는 대표적인 기술들에 대하여 특징을 간략히 설명하였다.

국내의 DRM 관련 기술은 세계적인 경쟁력을 보유했음에도 불구하고 기업 문서 보안 등에 치중하여, 향후 요구가 커질 것으로 예상되는 엔터테인먼트 콘텐츠 관련 DRM에서는 해외 기술에 의존하고 있는 실정이다. 특히, 향후 가장 큰 시장으로 예상되는 디지털 홈 서비스 분야에서는 이미 오래 전부터 해외의 여러 표준화 단체 및 업체에 의해서 기술 개발이 진행되었음에도 불구하고 국내의 표준화 기여 및 기술 수준은 이에 미치지 못하고 있다.

따라서 향후 국내에서 강점을 가지고 있는 DRM 상호호환 관련 기술에 대한 집중과 더불어 타 요소 기술에 대한 개발을 병행한다면 디지털 홈 DRM 기술에서도 세계적인 경쟁력을 가질 수 있을 것이다.

약 어 정 리

AES CTR	Advanced Encryption Standard Counter mode
AP	Acquisition Point
ATSC	Advanced Television Systems Committee
AU	Access Unit
CAS	Conditional Access System
CP	Consumption Point
CPCM	Copy Protection & Content Management
CPRM	Content Protection for Recordable Media
DMP	Digital Media Project
DRM	Digital Rights Management
DVB-CPCM	Digital Video Broadcasting Copy Protection & Content Management
DVB	Digital Video Broadcasting
EP	Export Point
EXIM	Export & Import
ISMA	Internet Streaming Media Alliance
ISMACryp	ISMA Encryption and Authentication
KMB	Key Management Block
MKB	Media Key Block
MPEG-2 TS	Moving Picture Experts Group-2 Transport Steam
OMA BCAST	Open Mobile Alliance Broadcasting
OMA	Open Mobile Alliance
PE	Processing Entity
PVR	Personal Video Recorder
RFC	Request for Comments
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SE	Storage Entity
SRTP	Secure Real-time Transport Protocol
USI	Usage State Information
VOD	Video on Demand
xCP	eXtensible Content Protection

참 고 문 헌

[1] ISMA, “Internet Streaming Media Alliance Implementation Specification Version 2.0,” 2005. 4.

[2] ISMA, “Internet Streaming Media Alliance Encryption and Authentication Version 1.1,” 2005. 12.

[3] OMA, “Service and Content Protection for Mobile Broadcast Services,” 2007. 5.

[4] OMA, “Mobile Broadcast Services - XML Schema for OMA DRM 2.0 Extensions for BCAST(XBS),” 2007. 5.

[5] IBM, “xCP: eXtensible Content Protection,” 2003. 7.

[6] DVB, "Digital Video Broadcasting(DVB); Content Protection & Copy Management," 2005. 11.
[7] 4C Entity, "CPRM Specification, Introduction and Common Cryptographic Elements, Revision 1.01," 2007. 5.
[8] Florian Pestoni, Jeffrey B. Lotspiech, and Stefan Nusser, "xCP: Peer-to-Per Content Protection," *IEEE Signal Proc. Magazine*, 2004. 3., pp.71-81.
[9] Coral Consortium, "Coral Consortium Core Architecture Overview Version 3.0," 2006. 6.
[10] Coral Consortium, "CCAWC Core Architecture Version 3.0," 2006. 6.
[11] Coral Consortium, "Ecosystem-A Specification," 2006. 6.