End-to-end 콘텐츠 보호를 위한 DRM 시스템 설계 및 구현

정 연 정[†] · 윤 기 송[††]

요 약

현재의 저작권 보호 기술 개발은 디지털 콘텐츠의 최종 소비자인 구매자단을 대상으로 해서 주로 이루어지고 있다. 그러나, 불법복제는 최종 소비자인 구매자뿐만 아니라 디지털 콘텐츠의 유통 가치사슬 중간 단계인 공급자와 배포자단에서도 항상 발생할 수 있다. 이에 본 논문에서는 창작자가 콘텐츠를 배포한 시점부터 구매자가 소비하는 시점까지 모든 유통 가치사슬에서 콘텐츠의 저작권 보호를 지원하는 End-to-end 디지털 저작권 보호 시스템을 설계하고 구현한다. 제안하는 시스템은 창작자, 공급자, 배포자 단에서도 구매자 단에서와 같이 콘텐츠 저작권을 안전하게 관리하고 콘텐츠의 불법 사용을 방지할 수 있는 기술적 장치를 제공함으로써 각 유통주체의 저작권을 보호하고 소유권 침해를 방지할 수 있는 환경을 제공한다.

키워드 : 콘텐츠, 저작권 보호, DRM

Design & Implementation of DRM System for End-to-end Content Protection

Yeonjeong Jeong[†] · Kisong Yoon[††]

ABSTRACT

Current technologies on digital rights management (DRM) have focused on security and encryption as a means of solving the issue of unauthorized copying, that is, locking the content and limiting its distribution to only purchasers. But, illegal content copy should be protected not only from purchasers but also from other principals such as media distributors and content providers. In this paper, we designed and implemented end-to-end digital rights management system that can cover a content protection on the overall value-chains of content distribution. Proposed system provides content protection and secure management of digital rights in creator, provider, and distributor like in purchaser. Accordingly it can provide an environment protecting each principal's digital rights and prohibiting illegal usage of content.

Key Words : Content, Digital Rights Management, DRM

1. 서 론

최근 디지털 기술의 발전으로 인해 고품질의 디지털 콘텐츠를 제작할 수 있게 되었고 인터넷과 통신 기술의 발전으로 인해 이를 손쉽게 이용할 수 있게 되었다. 그러나, 디지털 콘텐츠는 원본과 동일한 품질을 가지는 무한대의 복제가 가능할 뿐만 아니라 인터넷을 통해 전세계 어디라도 전파되기 때문에 불법복제가 빈번히 발생하고 있다. 불법복제는 디지털 콘텐츠의 저작권자나 서비스 제공자들로 하여금 디지털 콘텐츠의 저작이나 서비스 제공을 꺼리게 만들고 있다. 이러한 디지털 콘텐츠의 불법복제에 따른 문제를 해결해 줄 수 있는 것이 바로 디지털 콘텐츠에 대한 저작권 보호이다[4, 5, 6, 8, 13, 14].

현재의 저작권 보호 기술 개발은 디지털 콘텐츠의 최종 소비자인 구매자단을 대상으로 해서 주로 이루어지고 있다. 구매자단에 대해 저작권 보호 기술이 시급히 이루어지고 있는 이유는 디지털 콘텐츠가 다수의 구매자를 상대로 하여 배포되기 때문에 불법복제에 대한 시도가 높게 발생하고 있으며, 구매자가 전문적 지식 없이 간단한 캡쳐 소프트웨어와 같은 해킹 툴을 이용하여 쉽게 불법복제가 가능하며, 불법복제를 하여도 누가 불법 복제하여 배포하였는지를 알아내기가 쉽지 않기 때문이다[7, 10, 11].

한편, 디지털 콘텐츠가 최종 소비자인 구매자에게 전달되

† 정 회 원 : 한국전자통신연구원 선임연구원
†† 정 회 원 : 한국전자통신연구원 책임연구원
논문접수 : 2005년 8월 10일, 심사완료 : 2006년 1월 4일

기 이전의 유통 가치사슬을 살펴보면 디지털 콘텐츠를 생성하는 창작자(Creator)자, 디지털 콘텐츠를 상품화하는 공급자, 디지털 콘텐츠를 판매하는 배포자(Distributor)라는 유통주체가 존재함을 알 수 있다. 이들 유통주체는 창작자 측면에서는 공급자와 배포자가 자신의 디지털 콘텐츠를 불법 복제하여 사용할 가능성이 있는 유통주체이고, 공급자 측면에서 배포자가 자신의 디지털 콘텐츠를 불법 복제하여 사용할 가능성이 있는 유통주체이다. 일례로 영화가 상영되기 이전에 최종 소비자인 구매자가 아니라 중간 단계의 유통주체를 대상으로 하여 평가판으로 배포된 DVD가 불법복제되어 배포되거나 시사회에서 녹화되어 불법 배포되기도 하였다. 이처럼 불법복제는 디지털 콘텐츠의 유통 가치사슬 어디서나 발생할 수 있기 때문에 최종 소비자인 구매자뿐만 아니라 중간 단계의 유통주체인 공급자와 배포자단에서도 디지털 콘텐츠 저작권 보호가 필요하다[1, 2, 3].

따라서, 유통 가치사슬의 각 단계마다 불법복제를 방지하기 위해서는 중간과정에서도 원본 콘텐츠의 누출 없도록 보호할 수 있는 DRM 기술이 필요하다. 이에 본 논문에서는 창작자가 콘텐츠를 배포한 시점부터 구매자까지의 유통 가치사슬에서 콘텐츠에 대한 저작권 보호를 해결할 수 있는 End-to-end 저작권 보호 시스템(E2E DRM 시스템)을 설계하고 구현하였다.

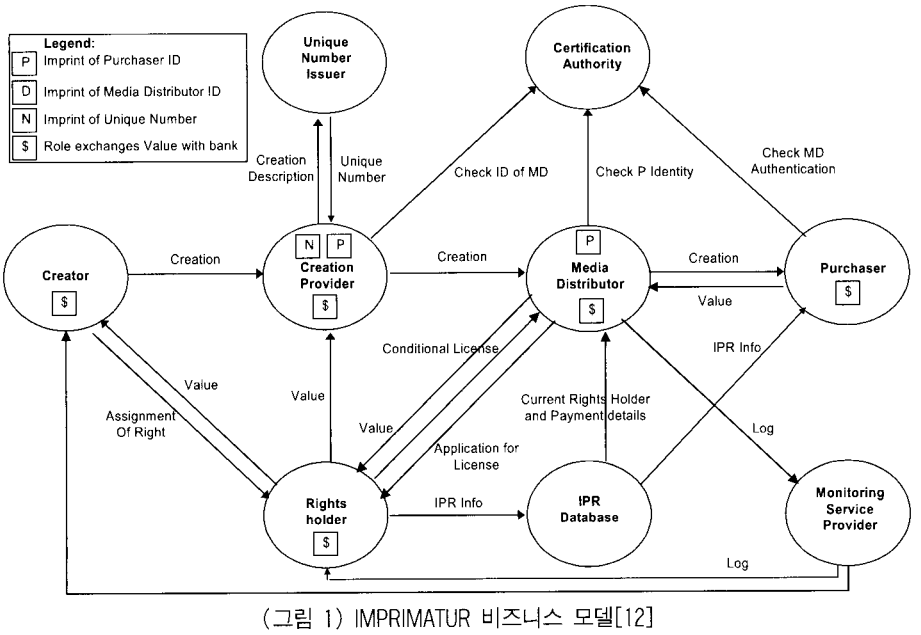
본 논문은 제 2장에서 디지털 콘텐츠 유통에 대해서 알아보고, 제 3장에서 제안하는 저작권 보호 시스템을 살펴보고, 제 4장에서 구현 시스템과 타 시스템을 비교하고, 제 5장에서 결론을 맺는다.

2. IMPRIMATUR 비즈니스 모델

IMPRIMATUR 비즈니스 모델은 콘텐츠 배포 모델로서 MPEG-21에서 표준으로 채택한 전자상거래 모델이다. 이 모델은 디지털 콘텐츠가 창작자(Creator)에서부터 생성되어 최종 소비자인 구매자(Purchaser)에서 소비되기까지 일련의 유통 과정에 참여하는 각 주체들의 역할 및 요구사항들을 정의하고 이들간의 상호관계 및 트랜잭션들을 명시하고 있다. (그림 1)은 IMPRIMATUR비즈니스 모델을 나타내며 유통주체를 각각의 역할(Role)별로 창작자, 공급자, 배포자, 저작권자, 구매자, 인증기관 등으로 구분하고 이들 간의 콘텐츠의 전달 및 콘텐츠의 저작권 정보 흐름에 대해 표현하고 있다(<표 1> 참조)[9, 12, 15].

〈표 1〉 IMPRIMATUR 비즈니스 모델의 유통주체

모델에 참여하는 유통주체	기 능
창작자(Creator)	디지털 콘텐츠를 창작
창작물 공급자(Creation Provider)	디지털 콘텐츠를 상업적 이용이 가능하게 함
미디어 배포자(Media Distributor)	디지털 콘텐츠를 분배
저작권자(Rights Holder)	지적재산권의 소유자
구매자(Purchaser)	디지털 콘텐츠를 구입하는 사람
식별번호 발행자 (Unique Number Issuer)	디지털 콘텐츠에 고유번호를 제공
지적 재산권 데이터베이스 (IPR Database)	지적재산권의 소유권에 관한 현재 정보를 유지
모니터링 서비스 제공자 (Monitoring Service Provider)	디지털 콘텐츠의 합법적 불법적 사용여부 확인
인증기관(Certificate Authority)	미디어 배포자와 구매자 인증
은행(Bank)	지불과 관련된 편의 제공



(그림 1) IMPRIMATUR 비즈니스 모델[12]

IMPRIMATUR 비즈니스 모델을 기반으로 해서 저작권 보호 측면에서 디지털 콘텐츠가 최종 소비자인 구매자에게 전달되기 이전의 유통 가치사슬을 살펴보면 디지털 콘텐츠를 생성하는 창조자(Creator)자로부터 디지털 콘텐츠를 전달받는 공급자(Provider)와 디지털 콘텐츠를 상품화하는 공급자로부터 디지털 콘텐츠를 전달받는 배포자(Distributor)라는 중간 단계의 유통주체가 존재함을 알 수 있다. 이들 중간단계의 유통주체는 창조자 측면에서는 공급자와 배포자가 자신의 디지털 콘텐츠를 불법복제하여 사용할 가능성이 있는 유통주체이고, 공급자 측면에서 배포자가 자신의 디지털 콘텐츠를 불법복제하여 사용할 가능성이 있는 유통주체이다. 일례로 영화가 상영되기 이전에 최종 소비자인 구매자가 아니라 중간 단계의 유통주체를 대상으로 하여 평가판으로 배포된 DVD가 불법복제되어 배포되거나 시사회에서 녹화되어 불법 배포되기도 하였다. 이처럼 불법복제는 디지털 콘텐츠의 유통 가치사슬상에서 항상 발생할 수 있기 때문에 최종 소비자인 구매자뿐만 아니라 중간 단계의 유통주체인 공급자와 배포자단에서도 디지털 콘텐츠 저작권 보호가 필요하다.

현재의 일반적인 창작자, 공급자, 배포자 사이의 콘텐츠 유통을 살펴보면 유통주체간 동의 하에 이루어지는 오프라인 계약 형태로 이루어지고 있다. 계약을 기반으로 한 콘텐츠 유통은 법률적 장치에 의해 보호받게 되는데, 이러한 방법은 유통주체의 신뢰에 기반으로 하여 지켜질 수 밖에 없기 때문에 계약에 대한 위반 사항을 발견하거나 콘텐츠의 불법 유통을 감지하는 것이 어렵다. 따라서, 창작자, 공급자, 배포자 단에서도 구매자단에서와 같이 콘텐츠 저작권을 관리하고 콘텐츠의 불법 사용을 방지할 수 있는 기술적 장치가 필요하다.

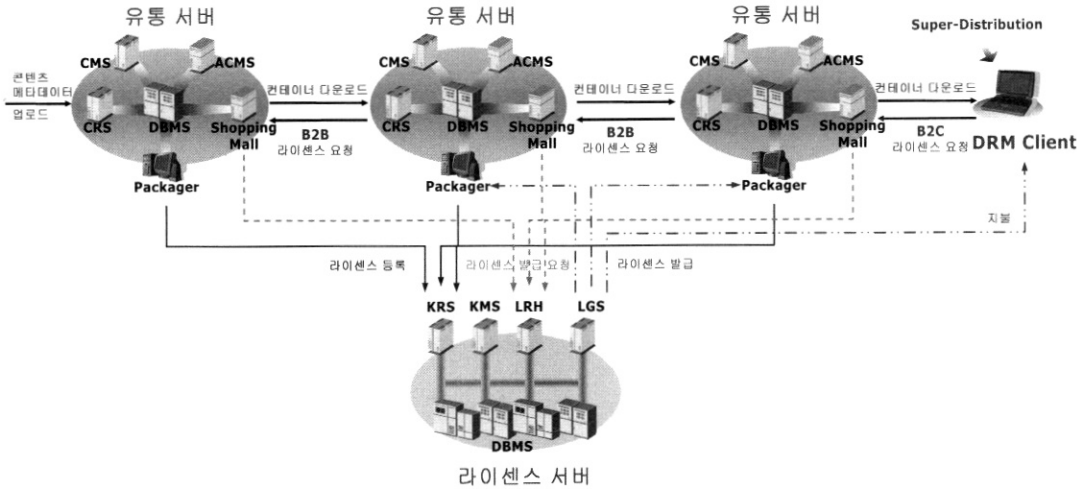
이에 본 논문에서는 창조자가 콘텐츠를 배포한 시점부터 구매자까지의 유통 가치사슬에서 콘텐츠에 대한 보호와 사용권한을 제어할 수 있는 E2E DRM 시스템을 제안한다.

3. 제안하는 E2E DRM 시스템

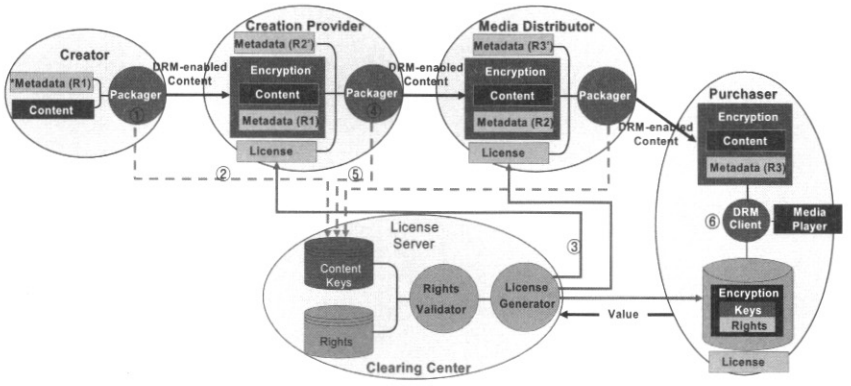
E2E DRM 시스템의 구성 요소는 패키저, 유통 서버, 라이센스 서버, DRM 클라이언트이다(그림 4 참조). 창작자, 공급자, 배포자 각각은 패키저와 유통 서버를 가지고, 클리어링하우스는 라이센스 서버를 가지며, 구매자는 DRM 클라이언트를 가진다(그림 2 참조).

E2E DRM 시스템 구조에서 DRM을 수행하는 프로세스는 콘텐츠 유통을 위해 최초로 원본 콘텐츠를 DRM 콘텐츠로 패키징하는 창작자(Creator)측 프로세스와 DRM 콘텐츠를 재패키징하여 유통시키는 공급자(Provider)와 배포자(Distributor)측 프로세스, 그리고 DRM 클라이언트에서 DRM-enabled콘텐츠를 재생하는 구매자(Purchaser)측 프로세스로 구분된다. E2E DRM 시스템은 공급자와 배포자 측 프로세스에서 라이센스를 기반으로 하여 DRM 콘텐츠에 대한 재패키징을 수행함으로써 유통주체간 콘텐츠 유통이 가능하도록 한다.

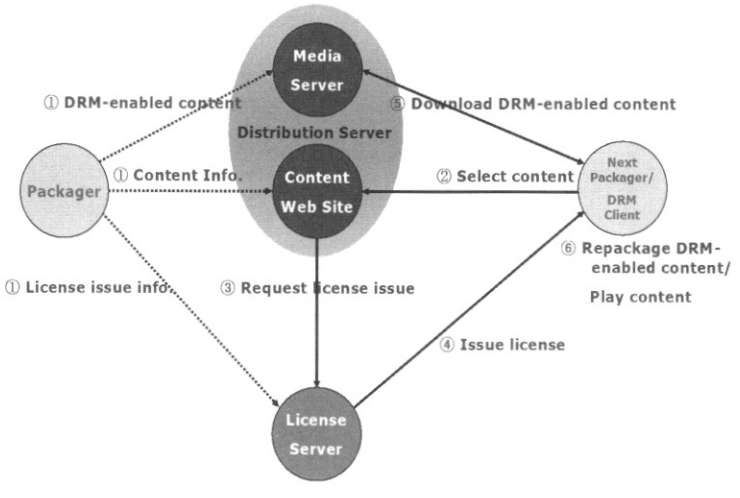
①창작자는 자신의 패키저를 이용하여 원본 콘텐츠를 DRM 콘텐츠로 패키징한 후 ②DRM 콘텐츠를 유통 서버에 등록하고, 라이센스 발급 정보를 라이센스 서버에 등록한다. ③공급자는 창작자의 DRM 콘텐츠를 창작자의 유통 서버로부터 다운받고 이를 사용하기 위한 라이센스를 라이센스 서버로부터 발급받는다. ④공급자는 자신의 패키저를 이용하여 창작자의 DRM 콘텐츠를 발급받은 라이센스에서 명시하는 사용권한 범위 내에서 재패키징한 후 ⑤재패키징된 DRM 콘텐츠는 자신의 유통 서버에 등록하고, 재패키징된 DRM 콘텐츠에 대한 라이센스 발급 정보는 라이센스 서버에 등록한다. 배포자 역시 공급자의 DRM 콘텐츠에 대해 재패키징 과정을 수행하고 자신의 DRM 콘텐츠를 구매자에게 제공한다. ⑥마지막으로 구매자는 DRM 클라이언트를 통하여 배포자의 DRM 콘텐츠를 라이센스 범위 내에서 사용하게 된다(그림 3 참조).



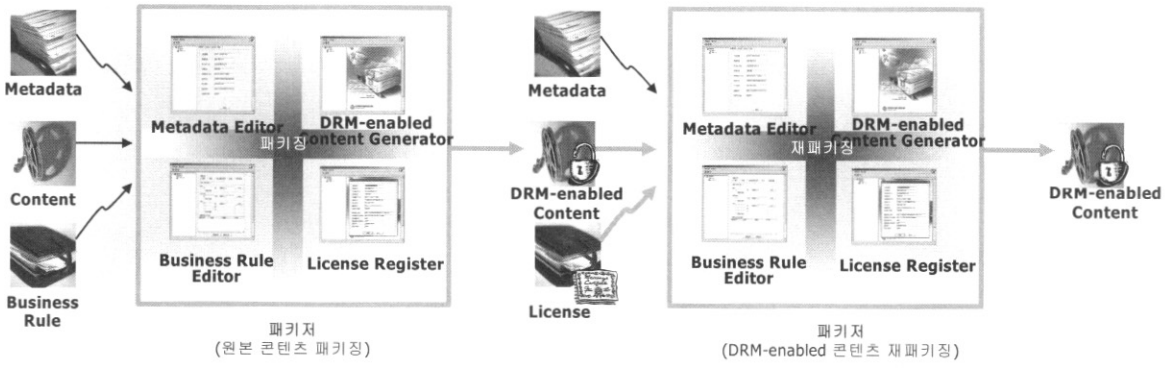
(그림 2) E2E DRM 시스템 구성도



(그림 3) E2E DRM시스템의 프로세스 흐름도



(그림 4) E2E DRM 시스템의 서비스 흐름도



(그림 5) 패키징/재패키징 흐름도

각 프로세스에서 수행되는 서비스 흐름을 (그림 4)에서 살펴보면 먼저, ①서비스 제공자는 패키저를 이용하여 DRM 콘텐츠와 콘텐츠에 대한 정보를 생성하여 유통 서버에, 라이센스 발급 정보를 생성하여 라이센스 서버에 등록한다. 콘텐츠 정보는 콘텐츠에 대한 메타데이터와 사용권한 정보를 포함하고, 라이센스 발급 정보는 라이센스를 발급하는데 필요한 암호화 키(CEK : Content Encryption Key)와 암호화 정보를 포함한다. ②서비스 소비자는 유통 서버에 접속하여 자신이 원하는 콘텐츠를 검색/조회하여 선택하고, 선택한 콘텐츠 이에 대한 사용권한을 서비스 제공자에게 요청한다. 사용권한은 콘텐츠는 종류에 따라 다양한 권한과 조건들이 제시되며, 소비자는 제시된 사용권한과 조건을 선택한다. ③유통 서버는 소비자가 선택한 사용권한과 조건을 라이센스 서버에 라이센스 발급 요청을 한다. ④라이센스 서버는 요청된 사용권한과 조건에 맞게 라이센스를 생성하여 소비자에게 발급한다. ⑤⑥소비자는 발급된 라이센스 범위 내에서 콘텐츠를 이용할 수 있게 된다.

3.1 패키저

콘텐츠 패키징(Content Packaging)은 콘텐츠, 메타데이터, 비즈니스 룰 등 콘텐츠 보호와 유통에 관련되는 정보들로써 DRM 콘텐츠를 구성하는 작업이며 패키저(Packager)를 통하여 수행된다. 콘텐츠는 오디오/비디오/문서 등과 같은 미디어이며, 메타데이터는 콘텐츠에 대한 DC(Dublin Core) 메타데이터와 유통주체에 대한 메타데이터를 포함한다. 비즈니스 룰은 사용권한과 사용권한에 대한 결제 정보를 포함한다.

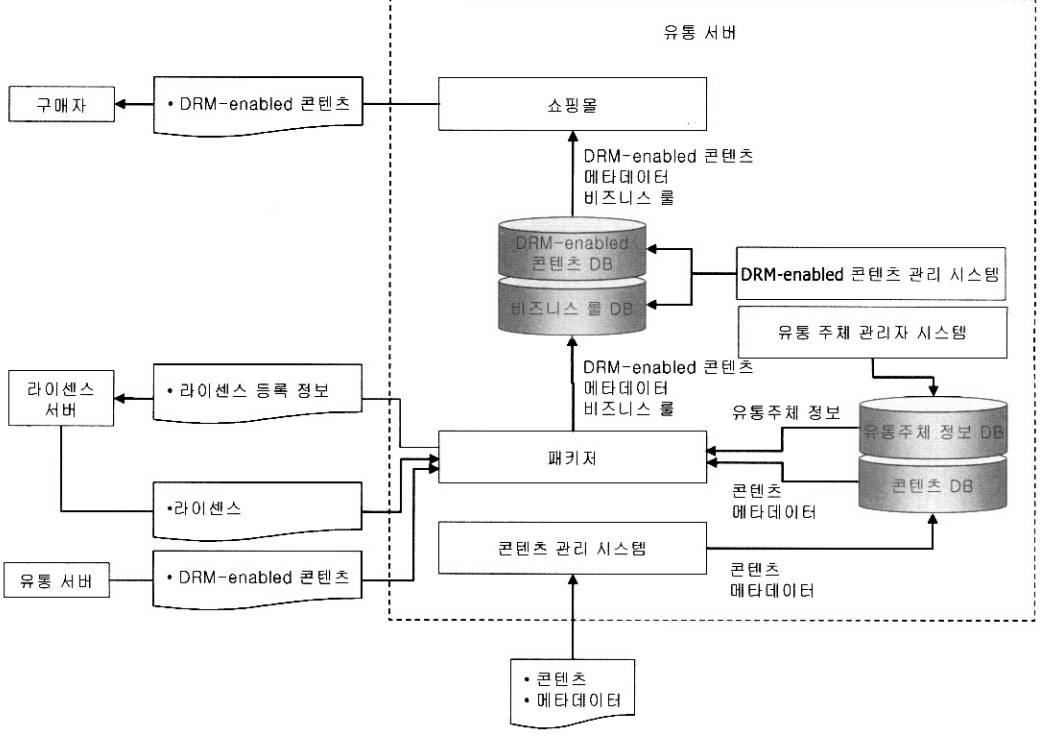
패키징 작업은 원본 콘텐츠를 대상으로 하여 패키징을 수행하는 원본 콘텐츠 패키징과 이미 패키징된 DRM 콘텐츠를 재패키징하는 DRM 콘텐츠 패키징으로 나뉜다. (그림 5)에서 콘텐츠 패키징 과정과 재패키징 과정을 볼 수 있다.

3.2 유통 서버

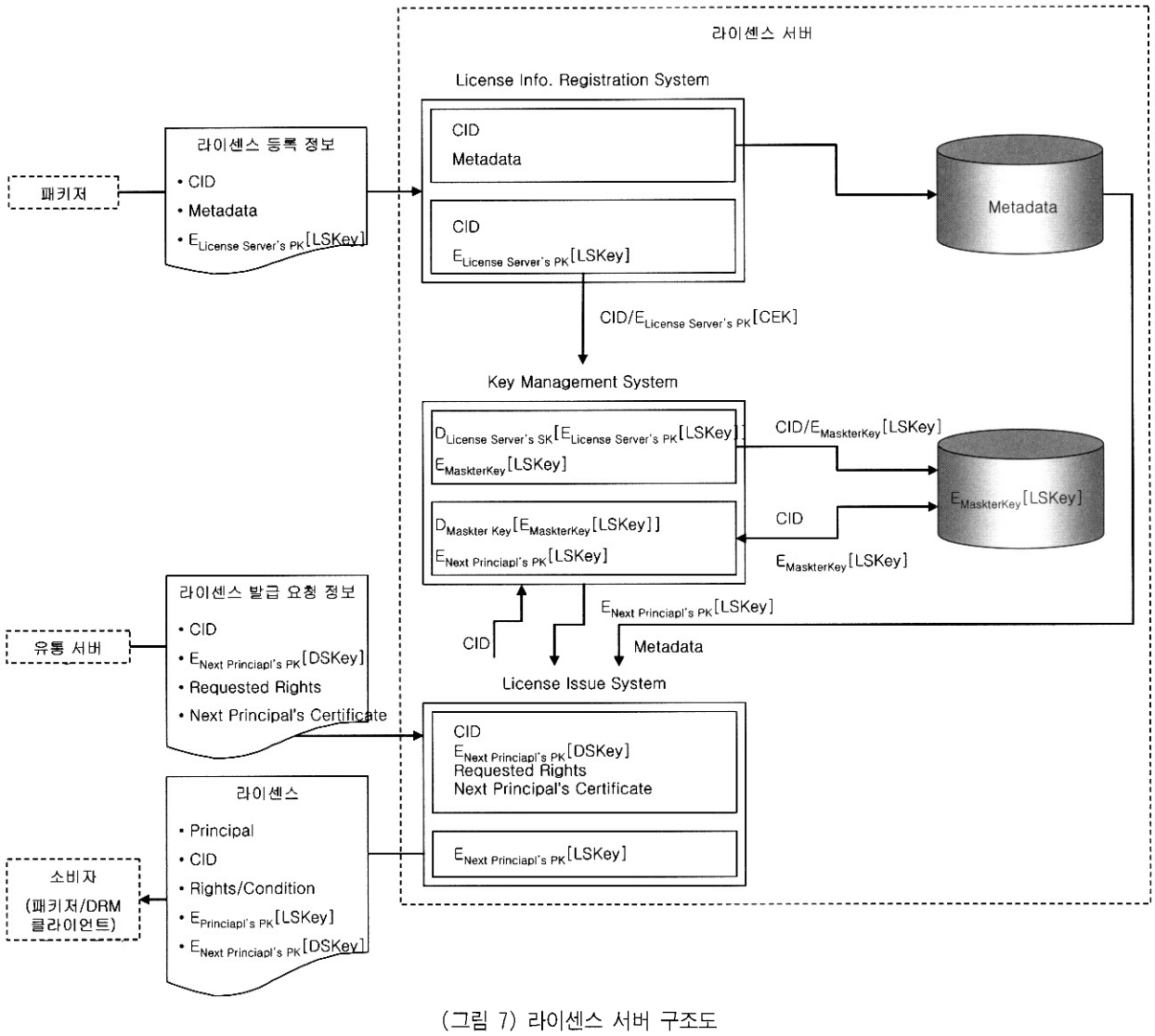
유통 서버는 유통주체 관리, 콘텐츠 관리, DRM 콘텐츠 관리, DRM 콘텐츠 사용규칙 관리, 쇼핑몰로 구성된다. 유통 서버는 콘텐츠를 유통하기 위해 콘텐츠, 콘텐츠에 관한 메타데이터, DRM 콘텐츠, DRM 콘텐츠에 관한 메타데이터, 유통주체 정보, DRM 콘텐츠에 관한 비즈니스 룰 정보를 관리한다. 유통 서버의 작업은 유통주체로부터 콘텐츠를 등록받는 단계에서부터 이를 유통시키기 전까지의 유통 준비 과정과 다음 유통주체로부터 콘텐츠 구매요청을 받고 이에 대해 라이센스 서버에 라이센스 발급을 요청하는 유통 처리 과정으로 나누어진다. (그림 6)은 유통 서버의 구성을 나타낸다.

3.3 라이센스 서버

라이센스 서버는 패키저로부터 라이센스 정보 등록 서버, 키 관리 서버, 라이센스 발급 서버로 구성된다(그림 7 참조). 라이센스 정보 등록은 패키저가 콘텐츠 암호화 키(CEK)를 보호하는데 사용한 암호화 키(LSKey)와 라이센스 발급에 필요한 정보를 라이센스 서버에 등록하는 단계이다. 암호화 키는 패키저에서 라이센스 서버로 전달시 라이센스 서버의 공개키로 암호화되어 안전하게 전달된다. 키 관리는 등록받은 암호화 키(LSKey)를 라이센스 서버의 비밀키로 복호화하고 이를 매스터 키로 암호화 한 후 데이터 베이스에 저장하여 관리한다. 라이센스 발급 서버로부터 암호화 키(LSKey)에 대한 요청이 들어오면 데이터베이스에서 액세스한 후 매스터 키로 복호화하고 이를 다음 유통주체의 공개키로 암호화한 후 제공한다. 라이센스 발급 은 다음과 같다. 유통 서버가 다음 유통주체로부터 콘텐츠에 대한 사용을 요청 받고 자신이 보관하고 있는 암호화 키(DSKey)를 소비자(다음 유통주체 또는 DRM 클라이언트)의 공개키로 암호화하고 소비자가 요청한 사용권한 정보를 라이센스 서버에 보낸다. 라이센스 서버는 요청된 사용권한이 허가된 범위 내에 있는지 검사하고 자신이 보관하고 있는 암호화 키(LSKey)를 소비자의 공개키로 암호화하고 소비자에게 라이센스를 발행한다. DRM 클라이언트는 유통 서버가 제공하는 암호화 키(DSKey)와 라이센스 서버가 제공하는 암호화 키(LSKey)를 이용하여 콘텐츠 암호화 키(CEK)를 생성함으로써 콘텐츠 복호화를 수행할 수 있다.



(그림 6) 유통 서버 구조도



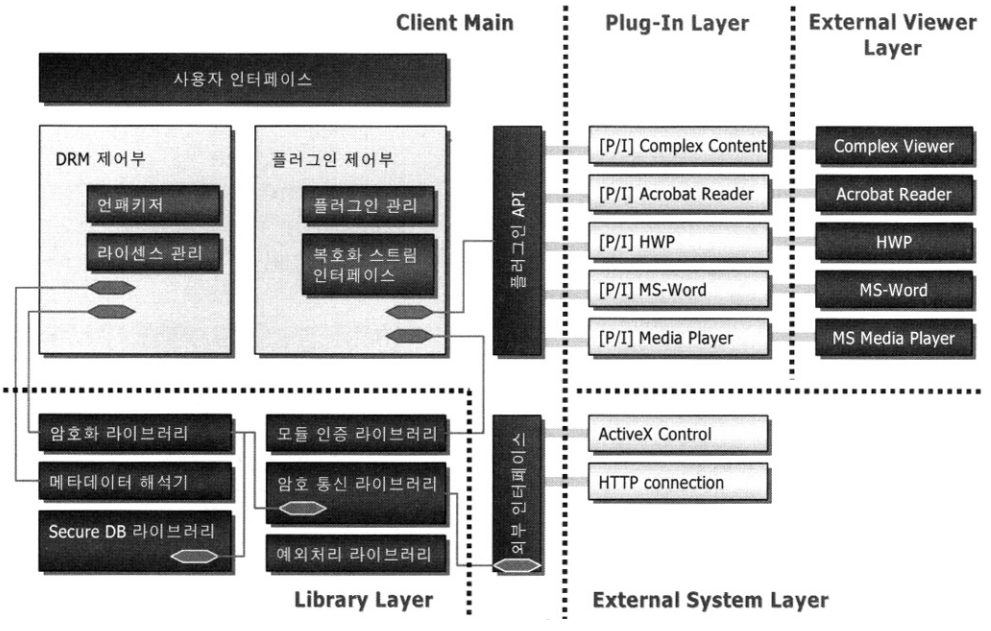
(그림 7) 라이센스 서버 구조도

3.4 DRM 클라이언트

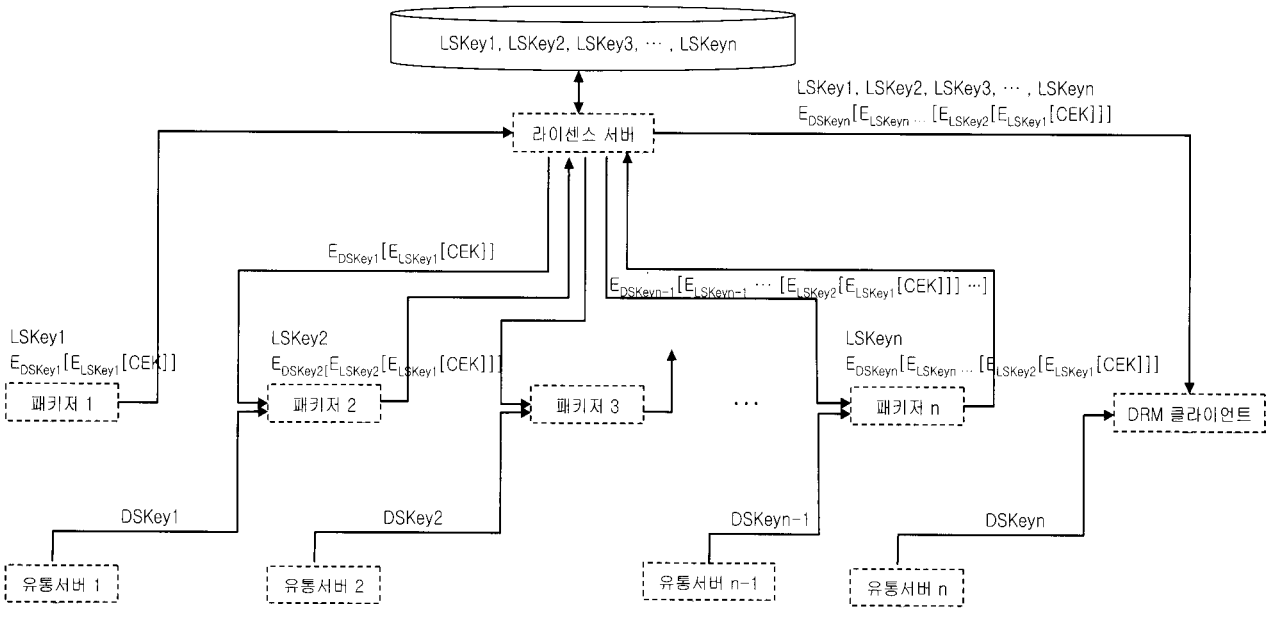
DRM 클라이언트는 DRM 제어부, 시큐어 데이터 영역 드라이버, 필터 드라이버, 플러그인 계층으로 구성된다. DRM 제어부는 클라이언트 프로그램의 가장 중심이 되는 모듈로 라이센스 서버와 통신하여 라이센스를 전송받고, 이를 시큐어 데이터 영역에 저장한다. 콘텐츠에 대한 이용 요청이 발생했을 경우 시큐어 데이터 영역 드라이버를 통하여 라이센스를 확인하고 뷰어를 실행한다. 또한, 뷰어가 실행될 때 이를 시큐어 데이터 영역내의 접근 허용 목록에 추가한다. 실행된 뷰어가 암호화된 콘텐츠에 접근할 경우에 필터 드라이버는 해당 뷰어가 콘텐츠에 접근할 수 있는 권한이 있는지의 여부를 확인한 후 복호화 하여 넘겨주게 되고 뷰어는 복호화된 콘텐츠를 재생하게 된다(그림 8 참조).

DRM 클라이언트는 일반 사용자뿐만 아니라 악의적인 사용자에게도 노출된 환경에서 동작하기 때문에 다양한 공격에 대한 강인성을 제공하기 위해 시큐어 데이터 영역 드라이버와 필터 드라이버를 이용하였다. 시큐어 데이터 영역 드라이버를 통하여 라이센스 형태로 발급받은 복호화 키를 사용자의 PC에 안전하게 보관하는데, 실제로 이를 가장 안전하게 구현하기 위해서는 스마트 카드와 같은 안전한 물리적인 저장 장치를 사용해야 하나, 아직 스마트 카드가 널리 이용되지 않는 현실적인 어려움으로 인해 하드디스크 내에 저장하되 악의적인 사용자의 공격으로부터 복호화 키를 보호할 수 있는 방법을 이용하였다. 이를 위해 커널 레벨의 드라이버를 이용해 가상 드라이브와 같은 데이터 영역을 만들고, 이 안에 복호화 키를 비롯한 중요 정보들을 암호화하여 저장하는 방법을 이용하였다. 암호화는 사용자 PC에 종속된 하드웨어 정보와 DRM 클라이언트의 설치시 생성된 난수를 조합하여 이용한다.

필터 드라이버는 커널 레벨의 드라이버로, 어떤 프로세스가 암호화된 콘텐츠에 접근할 경우에 해당 프로세스가 콘텐츠에 접근할 수 있는 권한이 있는지의 여부를 확인한 후 복호화 하여 넘겨주는 역할을 한다. 접근하는 프로세스는 콘텐츠가 암호화 되어 있는지의 여부를 알지 못하고 일반적인 파일 입출력 함수를 이용하며, 필터 드라이버는 이를 가로채어 동작한다. 필터 드라이버가 복호화를 수행할 때 필요



(그림 8) DRM 클라이언트 구조도



(그림 9) 키 관리 구조도

한 키는 시큐어 데이터 영역에 저장되어 있고, 매번 입출력이 발생할 때마다 해당 프로세스의 접근 허용 여부를 시큐어 데이터 영역의 접근 허용 목록에서 확인한 후에 복호화를 수행한다.

DRM 클라이언트는 플러그인 계층을 두어 사용자의 편의성을 고려한 유연한 구조를 가진다 PDF, 워드, 엑셀 파일과 같이 널리 이용되나 특정 업체의 소프트웨어에 종속된 콘텐츠를 지원하는 경우, 사용자의 편의성을 위해서는 해당 업체의 전용 소프트웨어를 이용할 수 있게 해야 한다. 하지만 포맷이 공개되지 않은 파일의 경우 타 업체에서 이를 지원하기가 쉽지 않다는 문제가 있다. 이를 위해 클라이언트 환경에서 DRM 정책을 결정하는 제어부와 뷰어 프로그램을 분리하고, 그 사이에 플러그인 계층을 두어 DRM 제어부의 결정에 따라 뷰어 프로그램을 제어하도록 한다.

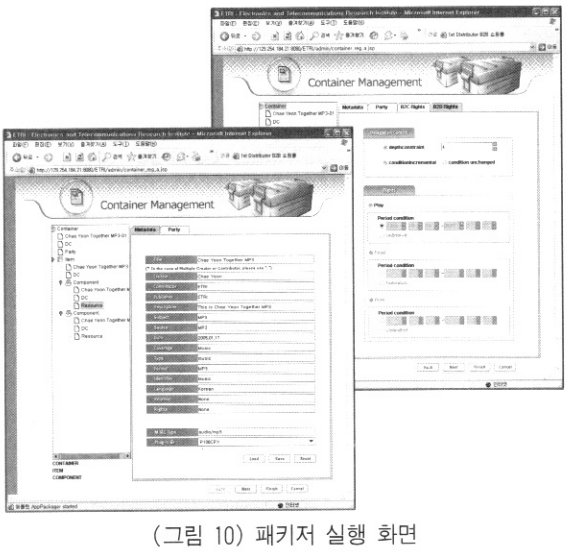
3.5 키 관리 구조

키 관리 구조는 DRM 시스템에서 콘텐츠의 안전성을 보장하는 메커니즘을 제공한다. 제안하는 키 관리는 창조자의 패키저 서버와 구매자의 DRM 클라이언트만 원본 콘텐츠를 추출할 수 있는 키 관리 체계를 제공한다. (그림 9)는 창조자의 패키저 서버로부터 구매자의 DRM 클라이언트까지의 각 유통 단계에서 발생하는 키 관리에 대한 흐름을 나타내고

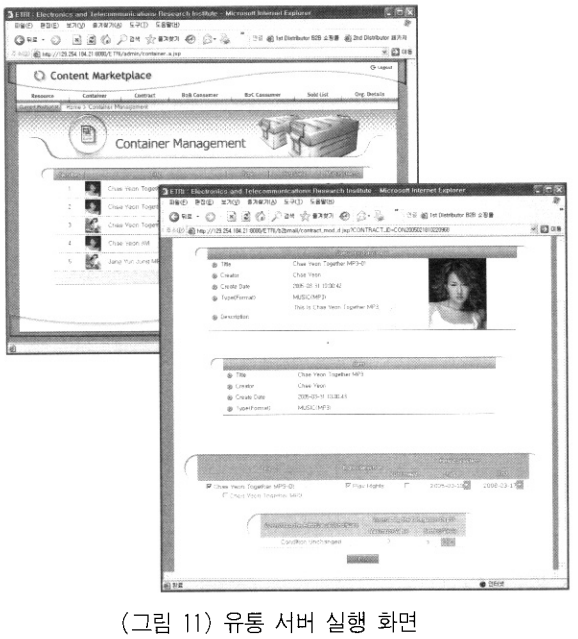
있으며, 키 전달 과정은 현재 단계의 유통주체가 DRM 콘텐츠를 생성한 후, 다음 단계의 유통주체가 현재 단계의 유통주체의 유통서버에 DRM 서비스를 요청하는 과정에서 발생한다. 창조자의 패키저 서버로부터 구매자의 DRM 클라언트까지의 키 관리를 보면 콘텐츠 암호화 키 CEK는 창조자의 패키저 서버와 구매자의 DRM 클라언트외의 다른 E2E 시스템의 구성요소에서 생성할 수 없음을 알 수 있다. 아래 (그림 9)와 같이 DRM 클라이언트 단에서만 CEK를 복호화할 수 있는 모든 키가 라이센스 서버와 유통서버로부터 제공받게 되므로 안전한 콘텐츠 전송이 보장된다.

3.6 시스템 구현

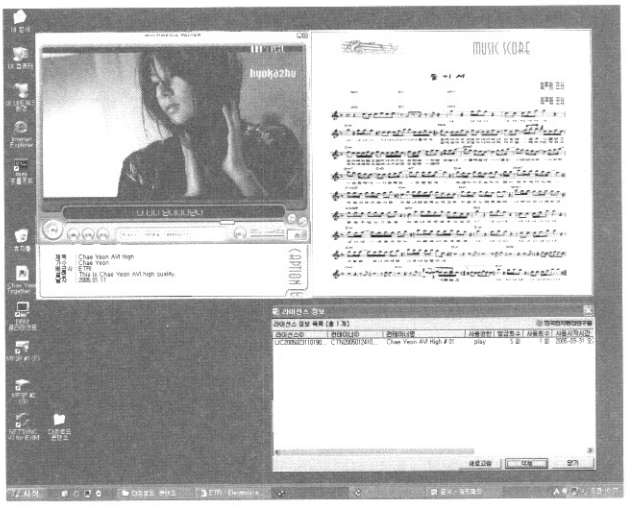
E2E DRM 시스템은 웹 브라우저를 통하여 콘텐츠/DRM 콘텐츠와 메타데이터, 유통주체 정보를 입력 받아 패키징/재패키징을 수행하여 새로운 DRM 콘텐츠로 만들 수 있으며 인터넷을 통하여 DRM 콘텐츠에 대한 라이센스를 발급받아 유통할 수 있도록 하였다. E2E DRM시스템의 유통 서버, 패키저, 라이센스 서버는 자바/JSP를 기반으로 개발되었으며, DRM 클라이언트는 Windows 운영체제를 기반으로 C/C++로 개발되었다. (그림 10)은 구현된 패키저의 실행 화면을, (그림 11)은 구현된 유통 서버의 실행 화면을, (그림 12)는 구현된 DRM 클라이언트의 실행화면을 나타낸다.



(그림 10) 패키저 실행 화면



(그림 11) 유통 서버 실행 화면



(그림 12) DRM 클라이언트 실행 화면

4. 제안하는 DRM 시스템과 타 DRM 시스템 비교

InterTrust DRM은 DRM 기술에 있어서 세계 최초의 DRM 시스템으로서 대부분 DRM 기술의 바탕이 되고 있으며, Microsoft DRM은 세계에서 가장 많이 적용된 DRM 기술이다. <표 2>는 제안하는 시스템과 기존의 대표적인 DRM 시스템인 InterTrust DRM 시스템과 Microsoft DRM 시스템을 비교한다.

<표 2> 구현 시스템 비교

	InterTrust	Microsoft	Proposed System
Supported Business Model	Distributor~ Purchaser	Distributor~ Purchaser	Creator~ Purchaser
*End-to end Content Protection	Not support	Not support	Support
Usage Rule	Proprietary	XrML	MPEG-21 REL
Metadata	Proprietary	Proprietary	DIDL
Viewer	InterTrust's proprietary viewer	Windows Media Player	All type of external viewers
DRM-enabled Content Capacity	Single Resource	Single Resource	Multiple Resources

5. 결 론

디지털 콘텐츠는 원본과 동일한 품질을 가지는 무한대의 복제가 가능할 뿐만 아니라 인터넷을 통해 전세계 어디라도 전파되기 때문에 불법복제가 빈번히 발생하고 있다. 이러한 불법복제는 디지털 콘텐츠의 저작권자나 서비스 제공자들로 하여금 디지털 콘텐츠의 저작이나 서비스 제공을 꺼리게 만들고 있다. 불법복제는 디지털 콘텐츠의 유통 가치사슬상에서 항상 발생할 수 있기 때문에 최종 소비자인 구매자뿐만 아니라 중간 단계의 유통주체인 공급자와 배포자단에서도 디지털 콘텐츠 저작권 보호가 필요하다. 그러나, 현재 콘텐츠에 대한 보호 및 유통은 최종 구매자로부터의 콘텐츠 보호에 중점을 두고 있어, 콘텐츠 창작자, 제공자, 분배자 등 콘텐츠 유통에 참여하는 모든 주체들에게 저작권의 보호 및 관리를 효과적으로 해결할 수 있는 수단을 제공하지 못하고 있다.

이에 본 논문에서는 창조자가 콘텐츠를 배포한 시점부터 구매자까지의 유통 가치사슬에서 콘텐츠에 대한 연속적인 저작권 보호를 해결하기 위해 일반적인 DRM 시스템의 구성요소의 역할과 기능을 확장하여 구성요소들간에 연동할 수 있는 End-to-end 디지털 저작권 관리 시스템을 설계 및 구현하였다. 제안하는 시스템은 창작자, 공급자, 배포자, 구매자 등이 참여하는 유통모델에서 콘텐츠의 전달 및 소비되는 각 유통 단계마다 DRM을 적용하기 위한 패키저, 유통서버, 라이센스 서버, DRM클라이언트 등을 설계하여 디지털 콘텐츠의 안전한 유통을 지원하는 End-to-end 디지털 저작권 관리 시스템을 구현하였다.

제안하는 DRM 시스템은 창작자, 공급자, 배포자 단에서도 구매자 단에서와 같이 콘텐츠 저작권을 안전하게 관리하고 콘텐츠의 불법 사용을 방지할 수 있는 기술적 장치를 제공함으로써 각 유통주체의 저작권을 보호할 수 있는 환경을 제공한다.

향후, DRM의 범위 내에서 콘텐츠 유통의 모든 가치사슬을 유연하게 지원하기 위해 기존의 전통적인 사용권한(Traditional Rights and Usages)에 대한 표현과 처리 방법에 대한 연구가 필요하다.

참 고 문 헌

[1] R. H. Koenen, J. Lacy, M. Mackay, S. Mitchell, "The long march to interoperable digital rights management", Proceedings of the IEEE, Volume 92, Issue 6, pp.883~897, June, 2004.

[2] B. C. Popescu, B. Crispo, A. S. Tanenbaum, "Digital rights management : Support for multi-level security policies in DRM architectures", Proceedings of the 2004 workshop on New security paradigms, pp.3~9, Sep., 2004.

[3] M. L. Smith, "Digital rights management & protecting the digital media value chain", Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia MUM '04, pp.187~191, Oct., 2004.

[4] Y. Jeong, K. Yoon, J. Ryou, "A Trusted Key Management Scheme for Digital Rights Management", ETRI Journal, Vol.27, No.1, Feb., 2004.

[5] G. Hanaoka, K. Ogawa, I. Murota, G. Ohtake, K. Majima, S. Gohshi, K. Oyamada, S. Namba, and H. Imai, "Managing Encryption and Key Publication Independentaly in Digital Rights Management Systems", IEICE TRANS. FUNDAMENTALS, Vol.E87-A, No.1, Jan., 2004.

[6] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital rights management for content distribution", Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, Vol.21, Jan., 2003.

[7] M. Fetscherin, M. Schmid, "Comparing the usage of digital rights management systems in the music, film, and print industry", Proceedings of the 5th international conference on Electronic commerce ICEC '03, pp.316~325, Sep., 2003.

[8] ISO/IEC JTC 1/SC 29/WG 11 MPEG/N5235 Draft Requirements for MPEG-21, Intellectual Property Management and Protection, 2002.

[9] ISO/IEC JTC 1/SC 29/WG 11, Information Technology - Multimedia Framework(MPEG-21) - Part 1 : Vision, Technologies and Strategy, N3939, Jan., 2001.

[10] F. Hartung and F. Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications", Communications Magazine, IEEE, Vol.38, pp.78~84, Nov., 2000.

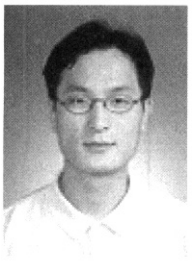
[11] G. Durfee and M. Franklin, "Distribution chain security", Proceedings of the 7th ACM conference on Computer and communications security, pp.63~70, Nov., 2000.

[12] http://www.imprimatur.net, IMPRIMATUR

[13] http://www.intertrust.com/, InterTrust

[14] http://www.microsoft.com/, Microsoft

[15] http://www.markany.com/, Markany



정 연 정

e-mail : yjjeong@etri.re.kr

1994년 부산대학교 전자계산학과(학사)

1996년 부산대학교 전자계산학과(석사)

2005년 충남대학교 컴퓨터과학과(박사)

1996년~현재 한국전자통신연구원 선임연구원

관심분야 : 정보보호, DRM

윤 기 송

e-mail : ksyoon@etri.re.kr

1994년 부산대학교 조선공학과(학사)

1988년 City University of New York 전산학과(석사)

1993년 City University of New York 전산학과(박사)

1993년~현재 한국전자통신연구원 책임연구원

관심분야 : 정보보호, 저작권 보호, 분산처리