

다수 DRM 지원 클리어링하우스 모델

이 창 열†

요 약

현재 시장에 유통되는 대부분의 DRM 시스템은 자체적으로 클리어링하우스를 가지고 있으며, 클리어링하우스는 콘텐츠 유통 메커니즘에서 중요한 역할을 차지하고 있다. 본 연구에서는 DRM 기능에서 중요한 위치를 차지하는 클리어링하우스 기능을 통합하여, 어떤 DRM으로부터 요구가 발생하여도 지원할 수 있는 다수 DRM 지원 클리어링하우스를 모델링하였으며, 초기 형태로 대표적인 Microsoft의 WMT, Adobe의 ACS 그리고 자체 DRM인 MR_DRM을 지원하는 체계를 구축하였다.

The Clearinghouse Model Supporting Multiple DRMs

ChangYeol Lee†

ABSTRACT

The DRM system has a clearinghouse module which is in the important position in content delivery mechanism. Currently, the most of DRM systems in the market does not support compatibility functions with other DRM systems. The shopping malls must consider the multiple clearinghouses services if they have many contents using diverse DRMs. In this paper, we are modelling a clearinghouse module which can support several DRM systems. As a first step, this model supports Microsoft WMT, Adobe ACS, and our own DRM system.

키워드 : 권리관리정보(RMI), 클리어링하우스(Clearinghouse), 디지털 권리관리(DRM)

1. 서 론

1996년 WIPO(World Intellectual Property Organization) (<http://www.wipo.org/>)는 6년간의 저작권법 협상을 마무리하면서 WCT(WIPO Copyright Treaty)와 WPPT(WIPO Performance and Phonogram Treaty)를 발표[1]하였으며, 이에 따라 미국은 1998년 DMCA(Digital Millenium Copyright Act)[1, 2]를, 유럽은 2001년 European Copyright Directive[2]를 발표하였다. 이들 법의 특징은 디지털 콘텐츠를 유통하는데 있어서 콘텐츠에 권리관리정보(RMI; Rights Management Information)를 부착 후, 기술 조치(Technological Measures)를 취하는 의무사항을 언급한 것으로, 이 기술 조치를 파괴하거나, 우회하는 어떤 S/W나 H/W에 대하여 개발하거나 배포하는 업체를 처벌하는 것을 주요 골격으로 하고 있다.

우리가 현재 언급하는 DRM(Digital Rights Management)라 불리는 기술은 디지털 저작권법이라고 불리는 WCT와 WPPT에서 언급한 RMI가 첨부되고, 기술조치가 이루어진 콘텐츠를 유통시키는 기술로 일반적으로 알려져 있다.

DRM은 이러한 관점에서 기술인지 모델인지 논란의 여지가 많이 있으나, 보편적으로 DRM은 디지털 콘텐츠를 유통시키는 신뢰 체계(Trusted Framework)라고 정의할 수 있다. 그러므로, 상거래 모델에서 신뢰를 제공(대표적으로 저작권자와 유통업자 사이) 할 수 있는 구조가 이루어지고, 유통을 활성화할 수 있는 Superdistribution(재배포) 기능을 만족(소비자에게 다양한 콘텐츠 사용 모델 제공)시키면, DRM 시스템이라고 단언할 수 있다. 그러므로 기존의 요소 기술로 언급되는 PKI(Public Key Infrastructure), Watermarking, 또는 TRS(Tamper Resistance System) 등과 확연히 구별된다.

DRM과 관련된 표준화 연구는 MPEG-21[3-6], DVB-CP[7], ISMA DRM Task Force[8], IRTF-IDRM(Internet DRM)[9-12], CEN/ISSS(<http://www.cenorm.be/iss/>), AAP-DRM report[13] 등에서 연구되고 있으며, 이들 연구는 개별적이거나보다는 상호보완적으로 추진되고 있다. 시장 기술로는 대표적인 일반 목적의 DRM 제품으로 ContentGuard의 CGBO(ContentGuard Back-Office)[14]와, Intertrust의 RightsSystem[15]이 있으며, Vendor DRM(DRM 개발 업체라기보다, 기존의 자사 제품에 DRM 기능을 첨부한 시스템)의 대표적 업체로 Microsoft의 WMT(Windows

† 종신회원 : 동의대학교 교수, DRM/URI Forum 분과위원장
논문접수 : 2002년 1월 18일, 심사완료 : 2002년 4월 10일

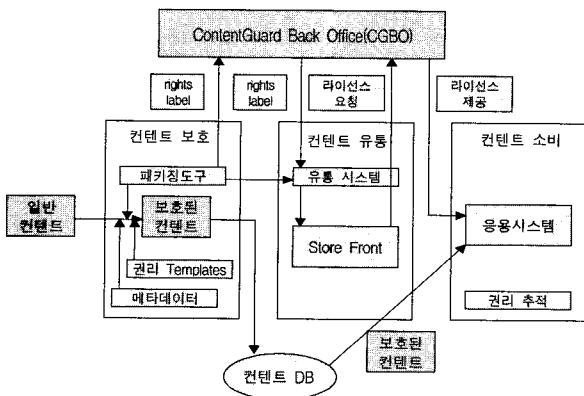
모든 DRM 시스템은 위와 같은 특징을 가지고 있으나, 시장에서 소비자가 선택하는 DRM 제품에 대한 평가는 다음과 같은 기준에 의하여 발생한다[15] :

- 기능적 제어 : 서비스 구조에 적절한 DRM 시스템인가?
- 시장에서 강점 : 표준 암호 체계를 사용하는지?, TRS 기능 제공은?, 갱신이 쉽게 가능한가?
- 융통성 : 다양한 미디어, 다양한 형식, 플랫폼을 지원 하는가?
- 호환성 : 기존의 다양한 시스템과 통합되어 서비스되기 위한 표준 기능 지원하는가?
- 사용자에 대한 충격 : 소비자가 특별한 조치 없이 쉽게 사용 가능한가?
- 기술적 신뢰성 : 제품 기술에 대한 신뢰성.
- 사업적 기준 : DRM 판매업체의 신뢰성(키 관리), 가격, 수익성, 제품의 생존성을 고려.

본 논문에서는 *de facto* 표준과 진행 중인 *de jure* 표준이 만족할 수 있는 모델을 제공하는 것으로, 다양한 DRM을 지원할 수 있는 클리어링하우스 시스템에 대하여 연구를 진행하였다.

2.2 쇼핑몰 운영

여기서는 ContentGuard의 CGBO를 기반으로 콘텐츠를 제작하여 유통하는 구조를 살펴보자. (그림 2)는 ContentGuard의 DRM 기반 서비스 시스템이다. 여기서 CGBO는 클리어링하우스이며, 패키징 도구를 사용한 결과인 *rights-label*은 클리어링하우스에 저장되고, 유통시스템에서 해당 콘텐츠를 서비스하기 위하여 CGBO로부터 *rights-label*을 제공받아서 사용한다. 이와 같은 모델은 단일 DRM 체계에서 적절하나, 쇼핑몰이 다양한 DRM으로 패키징된 콘텐츠를 사용할 경우, 복잡한 상황이 발생할 수 있다.



(그림 2) ContentGuard의 DRM 서비스

예를 들어, 쇼핑몰이 오디오/비디오 콘텐츠는 *de facto* 표준으로 제시되는 MS_WMT로 패키징된 콘텐츠를, 전자책

은 ContentGuard의 콘텐츠를 판매한다면 다음과 같은 상황이 일어날 수 있다 :

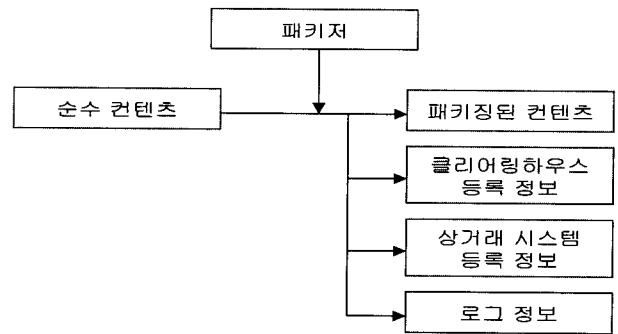
- 쇼핑몰은 2개의 별도의 클리어링하우스에 라이선스를 요청하며,
- 각각의 클리어링하우스는 주기적으로 쇼핑몰에 거래 내역 정보를 제공하고,
- 쇼핑몰은 클리어링하우스에서 제공한 각각의 거래 내역을 통합하여 처리한다(쇼핑몰에서 거래 내역 종합하는 번거로움이 강요됨).

본 상황은 특정 DRM 시스템의 문제이기보다는 특정 DRM 시스템이 모든 유형의 미디어 시장을 장악하지 못하는 시장 경쟁의 문제에서 발생하는 것이다. 이와 같이, 시장에는 분야별, 미디어별, 응용별로 우세한(또는 선호하는) 다양한 DRM 제품이 존재하는 환경을 고려하여 본 연구가 진행되었다.

본 연구에서 DRM 체계는 기존 제품을, 클리어링하우스 서비스는 여기서 모델링한 단일 클리어링하우스를 사용할 수 있게 본 모듈을 일반화하고, 구조화하고, 그리고 계층화하였다.

3. 다수 DRM 지원 클리어링하우스 설계

3.1 패키지 설계



(그림 3) 패키징 과정

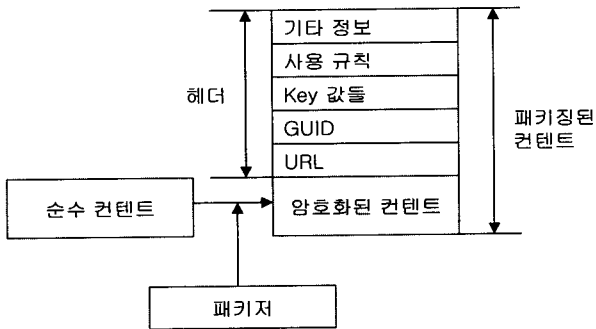
패키저는 순수 콘텐츠에 DRM이 가능한 구조를 취하는 도구로, 클리어링하우스가 계약된 상거래업체에게 배포하는 일종의 DRM 제작 도구이다. 패키저를 사용하여 패키징이 수행된 결과물은 (그림 3)과 같이 4가지 유형으로 분류될 수 있다. 본 결과물은 실제 상용 시스템에 따라서 다를 수 있다. 예를 들어 ContentGuard의 결과물[14]에는 (그림 3)의 '상거래 시스템 등록정보'가 없다. 이 정보는 (그림 2)의 메타데이터에 해당되는 것으로, (그림 2)에서는 기존에 별도로 존재한다는 가정 하에서 수행된 것이다.

이러한 패키징의 결과물에서 다양한 DRM을 지원하기 위하여 가장 중요한 모듈은 각 DRM의 특성을 가진 '클리어링하우스 등록정보'가 가장 중요하다. 이 정보를 (그림 2)에서처럼 ContentGuard에서는 *rights-label*로 기술하고, In-

tertrust에서는 *RightsPack*으로 불리워진다. 이 ‘클리어링하우스 등록정보’는 패키징된 결과 정보를 클리어링하우스에 등록하기 위하여 만들어진 메타데이터 정보라고 할 수 있다.

(그림 3)의 각 모듈을 설명하면 다음과 같다 :

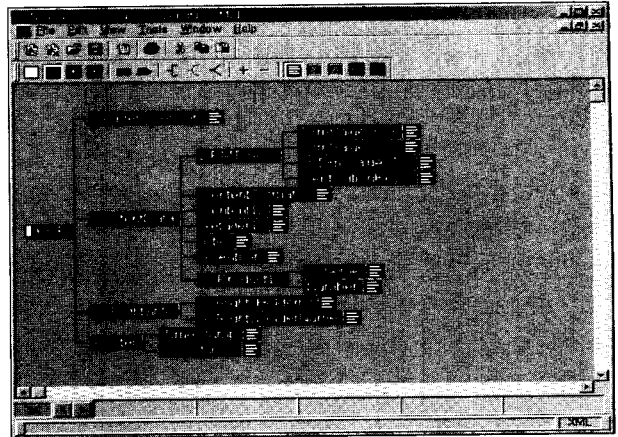
- **패키징된 콘텐츠** : 각 DRM 제품의 메카니즘에 적절한 헤더 정보를 기존에 콘텐츠에 부착한 형태로 (그림 4)처럼 구성된다.



(그림 4) 패키징된 콘텐츠의 상세 구조

콘텐츠에 부착되는 헤더 정보는 DRM에 따라 다르다. 그러나 보통 GUID(Global Unique ID), URL(사용 규칙 만료 시 또는 라이선스 없을 시 플레이어가 자동으로 띄워주는 웹사이트), ‘Key 값들’(콘텐츠 암호화와 관련된 키 값, 비즈니스 모델에 따른 키 값 등), 사용 규칙(저작권자가 본 콘텐츠에 대하여 미리 요구하는 사용 규칙, 등을 가지며, 본 헤더 정보 변경 방지를 위하여 기술 조치(전자 서명 등)를 한다.

- **클리어링하우스 등록정보** : 콘텐츠를 관리하며, 라이선스를 발급 시 필요한 정보로 구성되었으며, 클리어링하우스에 등록한다. 다수의 DRM을 지원하기 위하여, (그림 5)처럼 각 DRM 제품이 가지는 정보의 합집합 형태로 디자인하였다. (그림 5)는 XML-DTD 편집기인 *Near&Far*를 사용하여 해당 구조를 표시한 것으로, 여기서 중요한 항목만 설명하면 다음과 같다 :
 - **DRMType** : 속성 값으로 지원하는 DRM 이름을 기록한다. 현재 모델이 지원하는 구조는 MS_WMT, ACS, 그리고 MR_DRM(자체 DRM) 3개이다.
 - **DRMValue_C, DRMValue_S, DrmValue_T** : 다양한 DRM에서 사용하는 비즈니스 모델, 콘텐츠 암호화 등과 관련된 키 정보로 실제 사용되는 값, 형태, 방법은 DRM에 따라 다르다.
 - **VerificationKey** : 콘텐츠에 부착하는 (헤더)정보의 변조를 확인할 수 있게 전자서명된 결과를 확인하는 키
 - **ContentData** : 패키징되는 콘텐츠 정보
 - **RightsInfo** : 본 콘텐츠의 저작권자 관련 정보
 - **Signature** : 본 ‘클리어링하우스 등록정보’ 파일에 대한 전자서명.



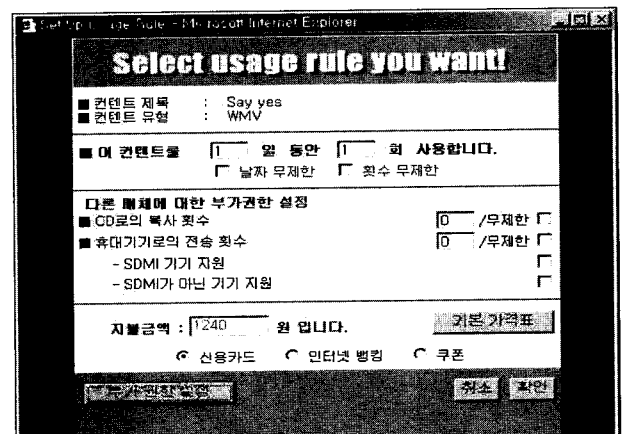
(그림 5) 클리어링하우스 등록 정보 구조

- **상거래 시스템 등록정보** : 본 콘텐츠를 쇼핑몰에서 판매하기 위하여, 상거래 시스템이 필요한 최소 메타데이터 정보로 구성되고, 보통 선택적 사양으로 쓰인다.
- **로그 정보** : 패키징 과정과 결과에 대한 정보 파일.

3.2 라이선스 요청 구조 설계

플레이어가 콘텐츠에 대한 라이선스가 없거나 있어도 사용 권한이 만료된 경우 (그림 4)의 콘텐츠 헤더에 부착된 ‘URL’로 자동 연계시킨다. ‘URL’로 자동 연계는 (그림 1)에서 (5) 동작 바로 이전에 발생하는 것이다. (그림 6)은 해당 URL로 자동 연계된 사이트에 대한 사례로, 소비자는 해당 콘텐츠의 사용 권한을 구입하기 위하여 본 화면을 채워야 한다.

여기서는 “Say yes”라는 제목의 비디오(WMV) 콘텐츠를 1일 1회 보는 조건으로 구입하는 것으로 가격은 1,240원이고, 신용카드로 구매한다고 기술되었다.

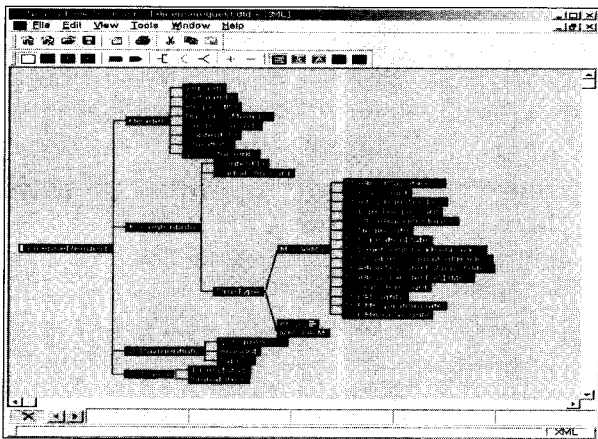


(그림 6) 자동 연계된 URL 사이트

소비자가 본 화면을 채우고 “확인” 버튼을 선택하면, 쇼핑몰은 자동으로 라이선스를 요청하게 된다. 즉 (그림 1)의 (5)를 수행하는 것이다. 여기서 클리어링하우스 설계는 다음과 같은 이유로 인하여 다양한 DRM 시스템을 지원할

수 있게 설계하였다 :

- 다양한 DRM 사용 : 특정 상거래 시스템에서 사용하는 DRM은 다양하다. 예를 들어, 비디오 콘텐츠는 MS_WMT 를, 전자책 콘텐츠는 Adobe의 DRM(ACS)이 적용된 것 일 수 있다.
- 단일 클리어링하우스 사용 : DRM별로 라이선스를 발급받는 클리어링하우스가 다르다면, 상거래 시스템은 전체 판매 내역, 라이선스 관리 등 상황을 종합적으로 판단하기가 어려우며, 중복적인 작업이 필요하다. 그러므로 DRM이 다르더라도 동일한 클리어링하우스로부터 라이선스 서비스를 받으면, 권리 정산과 지불 정산에 매우 효과적이다. 본 사항은 자연스럽게 '라이선스 요청' 구조의 일관성이 필요하다. 이러한 '라이선스 요청' 구조는 상거래 업자의 다양한 비즈니스 모델, 판매 정책 등이 반영되고, 다양한 DRM을 지원할 수 있는 구조로 만들어져야 한다.



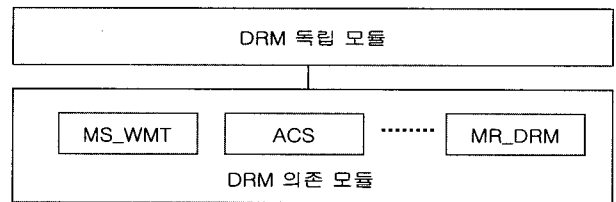
(그림 7) '라이선스 요청' 구조

(그림 7)은 (그림 6)의 정보를 바탕으로 만들어진 '라이선스 요청' XML-DTD이다. (그림 7)의 구조를 설명하면 다음과 같다 :

- 전체적 모습 : 라이선스 요청은 헤더 정보(Header), 콘텐츠 정보(+ContentInfo)(반복 구조 ; 콘텐츠를 소비자가 여러 개를 동시에 구매하고, 한 번에 라이선스 요청 지원), 지불 정보(PaymentInfo), 그리고 기타 정보(Trailer)로 나누어진다.
- 헤더 정보 : 라이선스 요청 상거래업체 ID(RetailerID), 요청 ID, 비즈니스 모델(기본적으로 Subscription, Pay-per-use, Free Delivery 등 지원), 등 기술.
- 콘텐츠 정보 : 해당 콘텐츠 가격, DrmType(현재는 MS_WMT, ACS, 그리고 MR_DRM로 3개 DRM 지원 모델)
- 지불 정보 : 통화, 전체 가격, 지불 방법 기술.
- 기타 정보 : 본 라이선스 요청 파일에 대한 전자서명 정보 기본적으로 (그림 7)에서 고려한 사항은 다음과 같다 :

- 다양한 DRM 지원 : MS_WMT, ACS, MR_DRM
- 다양한 비즈니스 모델 지원 : Subscription, Pay-per-use, Free Delivery
- 다수의 콘텐츠 구매 : 콘텐츠 정보의 반복 구조 지원.
- Trouble Shooting 정보 : 라이선스 발급이 중지될 때, 문제 해결을 위한 구조로 RequestID, RetailerID, CustomerID, ContentID, Partial_Amount 등 지원.

3.3 클리어링하우스 모듈 설계

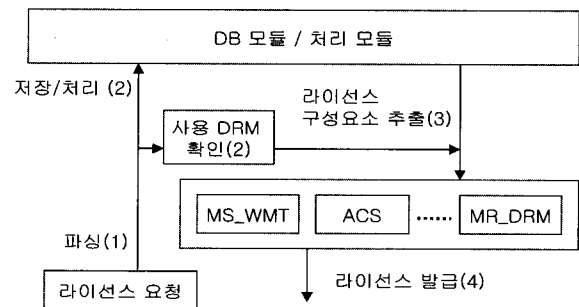


(그림 8) 다수 DRM 지원 클리어링하우스 구조

클리어링하우스는 다수의 DRM을 지원하기 위하여 계층적 구조를 가져야 한다. (그림 8)은 클리어링하우스 설계 구조로, 클리어링하우스 모듈을 DRM 독립 모듈과 의존 모듈로 분리하여 설계하였다.

현재 지원하는 구조로, MS_WMT는 Windows 2000에서만 작동하며, ACS는 다양한 플랫폼에서, 그리고 MR_DRM은 Linux 환경에서 작동하는 시스템으로 구성되었다. DRM 독립 모듈은 대부분 DB 모듈이거나 Back-End 처리기로 구성되어 있으며, DRM 의존 모듈은 라이선스 발급과 관련된 것으로 제품이 요구하는 플랫폼에 따라 다르게 구성된다.

이러한 계층적 환경 하에서 '라이선스 요청'을 받은 후 클리어링하우스에서 처리되는 과정을 (그림 9)에 기술하였으며, 자세한 과정은 다음과 같다 :



(그림 9) 클리어링하우스의 라이선스 발급 과정

- (1) 라이선스 요청은 DRM 독립적인 XML 형태로 구성되었으며(그림 7), 본 내용을 파싱.
- (2) 파싱 결과, 사용하는 DRM을 확인하고 필요한 정보를 저장하며, 라이선스 요청 처리 진행.
- (3) 라이선스 발급을 위하여, 관련 요소를 추출한 뒤, DRM 의존 모듈의 해당 DRM의 API를 사용하여

라이선스 발급 처리.

- (4) 발급된 라이선스를 소비자에게 제공. 이때 라이선스에는 사용권한 정보, 콘텐츠 해독용 키 정보 등이 들어있다.

여기서는 라이선스 요청부터 발급 때까지 과정과 계층적 구조의 클리어링하우스 모듈을 살펴보았으며, 이러한 구조는 다양한 DRM을 지원할 수 있게 하기 위하여 설계된 것이다.

4. 결 론

현재 DRM 시장은 특정 DRM 시스템이 모든 미디어, 분야, 응용에서 우수하지 않고, 특정한 미디어, 분야, 응용에서만 우월한(선호하는) 형태의 DRM이 제시되고 있다[13, 18](예를 들어, 비디오/오디오에서는 MS_WMT가, 전자책에서는 Adobe의 ACS가). 이러한 환경에서 쇼핑물은 다양한 DRM 제품을 보유하게 되고, 그러므로 라이선스 발급 서비스도 여러 군데서 받아야하는 상황이 나타나고 있다.

본 연구에서는 DRM 제품은 다르더라도, 라이선스 발급을 담당하는 클리어링하우스는 동일한 서비스가 가능한 클리어링하우스를 모델링하였다.

다수 DRM 지원 클리어링하우스를 설계하기 위하여,

- 패키지 모듈에서는 다양한 DRM 제품에 사용될 수 있는 "클리어링하우스 등록정보" 구조를 설계하였으며,
- 라이선스 요청 모듈에서는 다양한 DRM 지원(DrmType), 다양한 비즈니스 모델(BusinessModel) 지원, 여러 개의 콘텐츠 동시 구입(+ContentInfo) (여러개 동시 구입-라이선스 요청은 한번에), 여러개 라이선스를 발급하다가 중간에 문제 발생시 Trouble Shooting할 수 있는(Content-ID, Partial_Amount) 기능 등을 지원하며,
- 클리어링하우스 구조에서는 DRM 독립 모듈과 의존 모듈로 분리하였다. 독립 모듈은 거래와 관련된 DB 정보이고, 의존 모듈은 주로 OS 의존적인 API를 지원하는 형태로 구성하였다.

그러나 다양한 DRM을 지원하기 위한 구조를 일반화하기 위하여 고려한, MS_WMT, ACS, 그리고 MR_DRM(자체 DRM) 이외에 더 많은 DRM 시스템을 고려하면, 지금까지 연구된 구조가 확장, 변경될 소지가 충분히 있기 때문에 지속적인 연구가 필요하다.

참 고 문 헌

[1] 최경수, WIPO 저작권 조약과 우리의 대응, "뉴 밀레니엄에서의 저작권 환경", 세미나, 한국지적소유권학회, 1999.
 [2] Marc C. Hansen, The Legal Framework for Digital Rights Management, Digital Rights Management Seminar, Am-

sterdam 20 November, 2001.

[3] MPEG-21 Overview v3.0, N4511, December, 2001.
 [4] MPEG-21 Requirements for a Rights Data Dictionary and a Rights Expression Language, W4336, Final Vol.1.0, July, 2001.
 [5] Jan Bormans, Keith Hill, MPEG-21 Overview, ISO/IEC JTC1/ SC29/WG11/N4318, Sydney, July, 2001.
 [6] 이창열, MPEG-21 기반 방송 콘텐츠 유통 프로토타입 시스템 개발, 한국전자통신연구원, 연구결과보고서, 2000.
 [7] DVB-CP, DVB Technical Module Sub-group on Copy Protection Technologies, DVB CPT rev 1.1, 05 July, 2001.
 [8] ISMA Report, Internet Streaming Media Alliance DRM Task Force Report, IRTF-IDRM, 52 IETF meeting, October, 2001.
 [9] Sam X. Sun and Larry Lannom, Handle System Overview, <draft-irtf-idrm-handle-system-02.txt>, August, 2001.
 [10] Thomas Hardjono & Mark Baugher, IDRM Directions & Work Items, IETF-51, August, 2001.
 [11] Jeff Lotspiech, Moni Naor, Dalit Naor, Subset-Difference based Key Management for Secure Multicast, <draft-irtf-smug-subsetdifference-00.txt>, IRTF SMUG Internet Draft, July, 2001.
 [12] Mark Bauger, Internet Digital Rights Management Taxonomy, IETF-51, August, 2001.
 [13] AAP, Digital Rights Management for Ebooks : Publisher Requirements version 1.0, 2000.
 [14] ContentGuard, ContentGuard DRM Solution overview, October, 2000.
 [15] Joshua Duhl, and Susan Kevorkian, Understanding DRM Systems ; An IDC White Paper, 2001.
 [16] Microsoft, Windows Media Rights Manager 7 SDK, 2001.
 [17] Mike Clarke, Digital Rights Management for Documents, Adobe Systems, Digital Rights Management Seminar, Amsterdam 20, November, 2001.
 [18] Joshua Duhl, The DRM Landscape : Technologies, Vendors, and Markets, IDC, 2001.



이 창 열

e-mail : lcy@dongeui.ac.kr
 1985년 고려대학교 수학과 졸업(학사)
 1991년 고려대학교 전산과학과 졸업(석사)
 1997년 University Paris VII 전산과 졸업(박사)
 1987년~1994년 한국전자통신연구원 선임 연구원

1997년~2000년 한국교육학술정보원 책임연구원
 2000년~현재 동의대학교 교수
 2001년~현재 DRM/URI Forum 분과위원장
 관심분야 : DRM, 메타데이터, URI 기술