

디지털 콘텐츠 유통 관리 기술

이 창 열*

◆ 목 차 ◆

1. 서 론
2. DRM 기술

3. DRM 기술 동향
4. 결 론

1. 서 론

DRM(Digital Rights Management)은 디지털 콘텐츠에 대한 유통 프레임워크로 기존에 콘텐츠 상거래 프레임워크가 제공하지 못하는 거래의 신뢰성과 유통성을 제공하고 있다.

여기서 기존의 거래란 단순한 PKI (Public Key Infrastructure)를 암호화 방식을 사용한 상거래 방식을 지칭하는 것이다.

PKI 기술이 콘텐츠 유통에 안전성에 목표를 두었다면, DRM은 콘텐츠 거래에서 발생하는 모든 에이전트, 즉 소비자, 상거래업자, 저작권자를 고려한 새로운 메카니즘의 유통 비즈니스 모델일 수 있다.

즉 소비자에게는 다양한 사용 규칙(Usage Rule)을, 상거래업자에게는 다양한 비즈니스 모델(Super-distribution)을 포함하는 다양한 모델을, 저작권자에게는 투명한 거래(Transparent Transactions)를 제공하는 것을 DRM의 목표로 한다.

그러므로, 이러한 DRM의 목표는 특정 시스템이 DRM인지 아닌지를 판가름하는 중요한 잣대로 활용할 수 있다. 구조적으로 보면 재유통 (Superdistribution)과 투명한 거래 2가지 요소가 DRM의 필수조건에 해당된다.

PKI에서 언급하는 복사방지와 안전성은 DRM이 갖추어야 할 기본 요건이지 충분요건이 아닌 것이

다.

2. DRM 기술

2.1 라이선스 구조

DRM 환경 하에서 콘텐츠는 기존 환경과 달리 해당 콘텐츠에 대한 라이선스가 있어야 작동한다. 쇼핑몰에서 콘텐츠의 구입은 해당 콘텐츠의 무한정 사용을 허가하지만, DRM 환경 하에서 콘텐츠는 무료이며 사용 규칙을 구매하는 것으로 전개된다. 사용 규칙이란 해당 콘텐츠를 보는 조건, 예를 들어 “1일 무제한 보기”, “5번 보기” 등과 같은 것이다. 이러한 사용 규칙에 대한 정보는 라이선스 파일에 저장되어 있다.

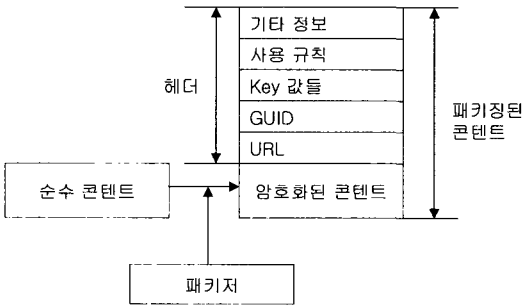
암호화에 있어서도 기존의 상거래 방식은 사용자별로 키가 할당되고 사용자의 공개키로 콘텐츠를 암호화하고, 해당 사용자의 개인키로 암호화를 푸는 형식으로 상거래가 발생하였다. 그러나 DRM 환경 하에서는 콘텐츠별로 키가 할당되고, 해당 콘텐츠에 할당된 공개키로 암호화하고, 개인키를 파는 형식을 취하고 있다. 그러므로 구매는 해당 콘텐츠의 개인키를 구매하는 것이며, 누구나 콘텐츠의 개인키를 구매할 수 있는 것이다.

위의 2가지 설명을 복합하면, 콘텐츠의 구매는 사용 규칙과 개인키를 사는 것이며 이들 정보는 라이선스 속에 함께 존재하는 것이다.

* 동의대학교 컴퓨터공학과 조교수

2.2 상거래 업자의 비즈니스 모델

DRM에서 가장 대표적인 비즈니스 모델이 재유통이다. 개념적으로 재유통은 특정 콘텐츠를 다른 사람에게 배포하여도 통제가 가능하게 하는 기술을 말한다. 다시 말하면 재유통 기능은 기존 상거래 시스템에서 언급하는 복제방지 기술과 대립되는 용어로 복사를 권장하는 비즈니스 모델이다.



(그림 1) DRM 기능 콘텐츠 제작

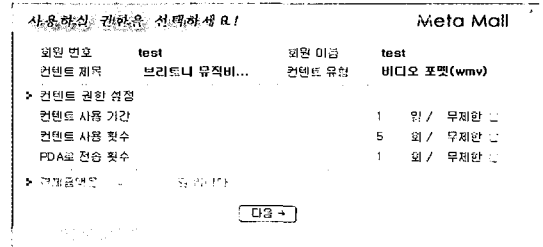
복사 권장 기술은 DRM의 구조에서 추출할 수 있다. 그림 1은 일반 콘텐츠(화면에서는 순수 콘텐츠를)를 DRM에서 제공하는 콘텐츠(화면에서는 패키징된 콘텐츠)로 제작하는 과정을 나타내고 있다.

이와 같이 DRM으로 제작하는 도구를 일반적으로 패키지라 부르며, 제작 과정을 ‘패키징한다’고 한다.

패키징은 PKI를 사용한 (1)순수 콘텐츠의 암호화, (2)콘텐츠 앞 부분(헤더)에 특수 정보 삽입, 그리고 (3)특수 정보에 대한 전자 서명 과정으로 분리된다.

본 패키징 과정에서 중요한 사항은 헤더에 기술된 GUID와 URL인 것이다. GUID는 Global Uniqueness ID로 콘텐츠에 대한 ID이며, URL은 본 콘텐츠의 사용을 허가하는 사이트에 대한 정보인 것이다.

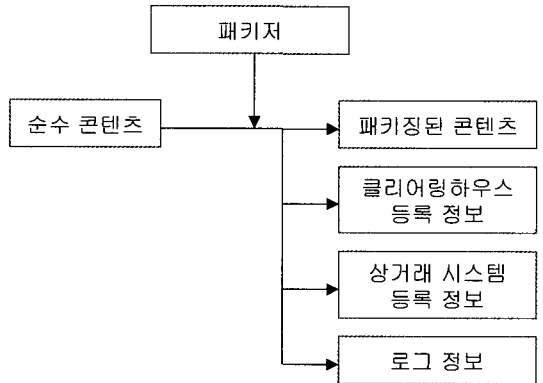
다시 말하면, ‘패키징된 콘텐츠’가 누구에게 가 있던지, 해당 콘텐츠의 사용 허가를 받을 수 있는 웹 사이트 정보가 콘텐츠에 저장되어 있기 때문에 본 콘텐츠를 복사하여도 해당 콘텐츠를 통제할 수 있는 것이다.



(그림 2) URL 샘플

그림 2는 샘플 URL을 나타내고 있다. 즉 플레이어가 해당 콘텐츠에 대한 라이선스가 없으면, 콘텐츠 앞 부분에 있는 URL 화면을 띄워주는 것이다. 그림 2는 이러한 URL에 대한 샘플로 해당 콘텐츠에 대한 사용 규칙을 설정하게 되어 있으며, 본 화면을 따라 진행하면 본 콘텐츠를 작동시킬 수 있는 라이선스를 받을 수 있는 것이다.

2.3 클리어링하우스 등록



(그림 3) 패키지 과정

그림 1은 그림 3에서 패키징의 다양한 결과물 중에서 ‘패키징된 콘텐츠’만 표시한 것이다. 패키징 결과는 그림 3과 같이 여러가지 결과물을 제공한다. 이 중에서 ‘클리어링하우스 등록정보’는 추후 소비자가 본 콘텐츠를 사용하기 위하여 암호를 풀어야하는데 필요한 키 값 등을 기록한 XML 기반 파일이다. 콘텐츠를 제작하면서 추후 콘텐츠를 합법적으로 풀 수 있는 키 값 정보를 추출하여 ‘클리어링하우스 등록정보’에 저장하고 본 정보를 클리어링하우스에 등록한다

록 시스템이 구성되어있다. 상거래 과정에서 라이선스 발급과 거래 정보를 관리하는 모듈을 클리어링하우스라 부른다.

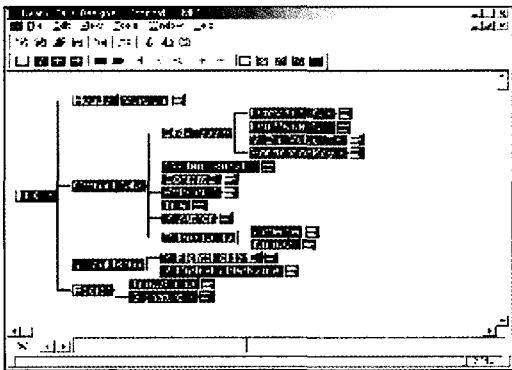
클리어링하우스 등록정보 :

콘텐츠 정보와 라이선스 발급시 필요한 정보를 포함하고 있으며 별도의 루틴을 통하여 본 내용을 클리어링하우스에 등록한다. 그림 4는 XML-DTD 편집기인 Near& Far를 사용하여 샘플 클리어링하우스 등록 정보를 표시한 것으로, 여기서 중요한 항목만 설명하면 다음과 같다.

- DRMTYPE의 속성 : DRM 이름을 기록한다.
- 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.

상거래 시스템 등록정보 :

본 콘텐츠를 쇼핑몰에서 판매하기 위하여, 상거래 시스템이 필요한 최소 메타데이터 정보로 구성되고, 보



(그림 4) 클리어링하우스 등록 정보 구조

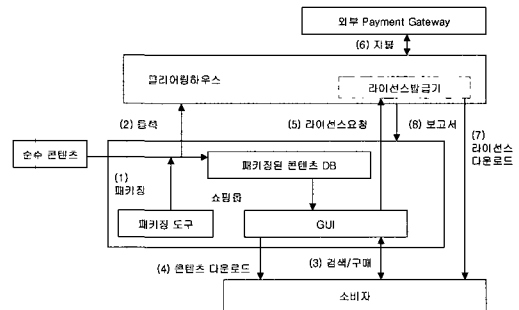
통 선택적 사양으로 쓰인다.

로그 정보 :

패키징 과정과 결과에 대한 정보 파일.

2.4 거래의 투명성

지금까지 메카니즘은 거래의 투명성을 제공하는 기능이 설명되지 않았다. 거래의 투명성은 DRM의 거래 구조에서 찾아볼 수 있다.



(그림 5) DRM 기반 쇼핑몰 구조

기 언급한 바와 같이 콘텐츠는 라이선스가 있어야만 작동이 될 수 있으며, 이러한 라이선스를 발급하는 모듈을 쇼핑몰 모듈과 분리함으로써 구조적인 투명성을 제공하는 것이다. 라이선스를 발급하는 모듈을 그림 5에서와 같이 클리어링하우스라 부른다. 클리어링하우스와 쇼핑몰이 분리되는 것은 판매와 거래 내역 정보를 분리하는 것이고, 전통적인 상거래에서 신용카드 사용 또는 금전등록기와 같이 판매와 거래를 분리하는 구조를 제공함으로써 상거래의 투명성을 제공하게끔 DRM 구조가 설계된 것이다.

그림 5의 구조를 설명하면 다음과 같다 :

- (1) 패키징도구를 사용하여 '순수콘텐츠'를 '패키징된 콘텐츠'로 제작. 패키징이라는 의미는 보통 '순수콘텐츠'에 '헤더 정보'를 부착하여 기술조치(전자서명, 암호화 등)를 취하는 과정

- (2) 패키징에 관련된 정보를 클리어링하우스에 등록. 클리어링하우스는 라이선스를 제공하고, 거래에 관련된 권리 정보에 대한 정산 기능을 제공하는 시스템으로 보통 지불(Financial) 정산과 권리(Rights) 정산을 통합하여 언급하거나 또는 권리 정산만을 의미함.
- (3) 쇼핑몰에서 소비자에게 콘텐츠에 대한 검색, 선택 등 기능 제공.
- (4) 소비자가 선택한 콘텐츠의 다운로드(또는 스트리밍). 보통, 콘텐츠 다운로드 자체는 무료임.
- (5) 라이선스 요청. DRM 체계에서는 콘텐츠 사용을 위하여, 콘텐츠와 라이선스가 있어야 하며, 보통, 콘텐츠는 무료로, 사용권한은 유료로 제공함. 라이선스 속에는 사용권한 정보가 포함되어 있음. (4)에서 제공받은 콘텐츠를 사용하기 위하여 해당 콘텐츠를 작동시키면, 플레이어(Player)가 해당 콘텐츠의 라이선스를 확인하고, 없거나, 또는 있어도 사용 권한이 만료되었으면 (5)번을 작동시킨다. (5)의 라이선스 요청 정보에는 사용 권한, 가격 처리 등이 포함되어 있음.
- (6) 해당 콘텐츠에 대한 라이선스 요청이 지불과 관련되었을 때, 지불 처리.
- (7) 라이선스 다운로드
- (8) 주기적으로 거래내역 보고서 제공. 유통업체에게 주기적으로 전체거래 내역(권리 정산과 지불 정산) 정보를 제공함.

3. DRM 기술 동향

3.1 시장 기술

DRM 기술은 상업적으로는 Intertrust 회사와 ContentGuard 회사가 선발주자였지만, Intertrust는 시장성 악화로 타 회사에 넘어갔으며, ContentGuard 역시 시장에서 두각을 나타내지 못하고 있다.

그것은 자사의 플레이어를 가지지 못한 Intertrust와 다른 회사는 타 회사의 Player(여기서는 Media Player, Acrobat Reader)에 Plug-In 기능을 제공하여 DRM 기능을 제공할 수 밖에 없었고, 이러한 방식은

소비자로 하여금 DRM 사용에 부담을 제공하기 때문에 해당 회사의 DRM이 널리 사용되지 못하는 결과를 초래하였다.

그렇지만 후발주자인 Microsoft와 Adobe 회사는 이미 de facto 표준인 자사의 Player인 Media Player와 Acrobat Reader를 가지고 있었으며, 여기에 DRM 추가(Plug-In이 아니라 버전업 하면서 추가함)는 소비자로 하여금 자연스럽게 Microsoft의 DRM인 WMT(Windows Media Technologies)와 Adobe의 DRM인 ACS(Adobe Content Server)를 사용할 수 있는 환경을 제공함으로써 성공적 시장 진출을 할 수 있게 하였다.

3.2 표준화

DRM 표준화는 특정 영역에서 표준화와 일반적인 표준화로 대비된다. 일반적 표준화 기술은 MPEG-21에서 진행 중에 있는 기술로 그 규모가 매우 커서 MPEG-21을 만족시킬 수 있는 제품이 나올 수 있을까가 의심스러운 정도이다. 현재까지 진행된 과정으로 MPEG-21 DII, MPEG-21 DII-RA, RDD, REL에 대한 대부분의 진행을 마치고 계속적으로 Event Reporting 등의 항목의 표준화를 진행하고 있다.

한편 IETF의 연구 그룹인 IRTF에서 진행한 IDRM(Internet DRM)은 현재 연구가 중단된 상태이고, 방송에서 DVB-CPCM, TVAnyTime Forum에서 RMP, 전자책 EBX DRM, ISMA에서 진행 중인 ISMA DRM 등이 존재하고 있다. 이들 DRM은 대부분 MPEG-21에서 제시하는 스펙을 수용하면서 특정 전문 분야에 한정된 DRM 스펙을 제시하고 있다.

4. 결 론

DRM은 디지털 콘텐츠 유통에서 거래 당사자 사이에 신뢰를 제공하는 중요한 기술이며, 콘텐츠에 영향을 미치는 저작권자의 권리를 보호하기 위한 기술이다.

국제적으로 매우 커다란 범위의 DRM 표준화가 MPEG-21에서 진행되고 있으며, 시장에서도

Microsoft와 Acrobat 등 세계적인 업체들이 시장을 주도하고 있다. 그러나 국내의 경우 대부분이 중소기업에서 DRM 제품을 개발하고 있어서 DRM이 갖추어야 할 조건과 MPEG-21에서 채택한 XrML(eXtensible rights Markup Language)을 포함하는 다양한 표준 기술을 개발하기에는 기술적, 재정적 어려움을 가지고 있다.

DRM 자체가 콘텐츠 산업의 미래 기술로 반드시 확보하여야 하는 기술이지만, 제대로 만들기 위하여 다양한 기술, 자본, 그리고 시간이 필요한 제품이며, 장기적으로 건전한 시장 질서를 확립하기 위하여 DRM 제품은 반드시 개발하여야 하는 제품이다.

그것은 DRM이 가지는 다음 2가지 특수성을 고려하여야 하기 때문이다.

첫째, DRM은 국제 저작권 기구인 WIPO에서 제정된 WCT(WIPO Copyright Treaty) & WPPT(WIPO Performace and Phonogram Treaty)에서 언급한 저작권자 보호를 위한 기술로 법적으로 반드시 제공하여야만 한다.

두 번째로, DRM이 제공하는 클리어링하우스를 기반으로 하는 구조는 거래 내역에 대한 정보를 간직하고 있으며, 그것은 장차 상거래에서 발생하는 분쟁, 과세, 거래 통계 자료 등 다양한 용도에 사용될 수 있기 때문이다.

참 고 문 헌

- [1] DVB-CPCM : <http://www.dvb.org/>
- [2] IDRM : <http://www.idrm.org/>
- [3] ISMA : <http://www.isma.tv/>
- [4] MPEG-21 <http://www.csel.it/mpeg/>
- [5] TVAnyTime : <http://www.tv-anytime.org/>
- [6] WIPO : <http://www.wipo.org/>

◎ 저 자 소 개 ◎



이 창 열

1985년 고려대학교 수학과(이학사)
 1991년 고려대학교 전산학(이학석사)
 1997년 파리7대학원 전산학(박사)
 1987년~1994년 ETRI 선임연구원
 1997년~2000년 KERIS 책임연구원
 2000년~현재 : 동의대학교 컴퓨터공학과 조교수
 관심분야 : 콘텐츠 보안/유통, 메타데이터