情 報 保 護 學 會 誌
第 12 券 第 1 號, 2002. 2

DRM 기술

이 창 열*

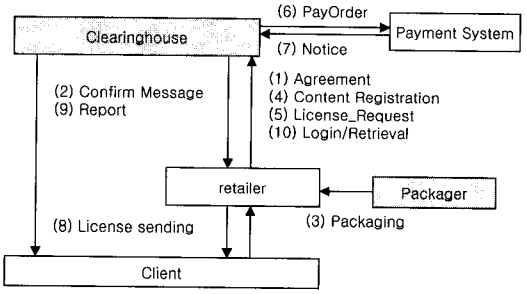
Ⅰ. 서 론

DRM(Digital Rights Management; 디지털 권리 관리) 기술은 디지털 컨텐츠 유통 과정에서 발생하는 에이전트 사이 권리와 신뢰성, 컨텐츠의 안전성 및 재 활용성, 유통의 투명성을 보장하는 종합적인 구조로 정의할 수 있다. 그러므로 DRM은 암호화기술, 워터마킹 기술, 변조방지 기술을 포함하고 컨텐츠의 가치 사슬을 지원하고, 그리고 저작권자, 유통업자, 소비자 사이에 신뢰를 제공하지만, 근본적으로 요소기술이 아니기 때문에, 특정 시스템이 DRM 체계를 갖추었는지 구별하기가 쉽지 않다.

디지털 컨텐츠 상거래 시스템이 DRM 체계를 갖추었는지는 다음과 같은 관점에서 판명할 수 있다.

- 해당 상거래 시스템이 저작권자와 유통업자 사이에 서로 신뢰할 수 있게 구조적인 체계가 지원되는가?
- 유통업자와 소비자 사이에 컨텐츠의 안전한 전송과 사용이 보장되는가?
- Superdistribution이 지원되는가? Superdistribution이란 컨텐츠를 타인에게 제공(복사 및 대여)하였을 때, 타인이 합법적으로 해당 컨텐츠를 사용할 수 있게 하는 구조이다.

위와 같은 구조를 지원하는 전형적인 형태는 그림 1과 같다.



〔그림 1〕 전형적인 DRM 기반 상거래 체계

그림 1에서 사용되는 용어는 다음과 같다

- Clearinghouse. 클리어링하우스. 거래의 투명성을 보장하는 기능을 하는 것으로 retailer가 라이선스 발급을 요청하면, 해당 라이선스를 발급하여 소비자에게 제공한다.
- Packager. 패키저.
- Retailer. 유통업자.

그림 1을 기반으로 유통 과정을 설명하면 다음과 같다 :

- (1) 클리어링하우스와 유통업자간에 라이선스 서비스 계약을 한다.
- (2) 클리어링하우스는 계약의 결과로 패키저를 포함한 툴을 제공한다.
- (3) 유통업자는 DRM 서비스를 하기 위하여 패키저를 이용하여 컨텐츠를 암호화한다.
- (4) 패키징 결과 정보를 클리어링하우스에 등록한다.

* 동의대학교 컴퓨터공학과 교수(lcy@dongeui.ac.kr)

- (5) 유통업자는 컨텐츠를 소비자에게 판매하고, 소비자가 특정 컨텐츠를 구매시 해당 컨텐츠를 위한 라이선스 발급을 클리어링하우스에 요청한다.
- (6)-(7) 해당 컨텐츠의 지불 처리를 한다.
- (8) 지불 처리가 완료되면 소비자에게 클리어링하우스는 라이선스를 제공한다.
- (9) 주기적으로 발급한 라이선스에 대한 정보를 유통업자에게 제공한다.
- (10) 필요시 유통업자는 거래 정보의 자세한 것을 클리어링하우스에 들어와서 볼 수 있다.

위와 같은 DRM 서비스에서 클리어링하우스와 유통업자의 분리는 저작권자와 유통업자간에 신뢰성을 제공한다. 즉 유통업자의 판매 내역을 클리어링하우스가 가지고 있음으로 거래 내역을 속일 수 없는 것이다.

이러한 DRM 기술을 제공하는 대표적인 제품을 살펴보자.

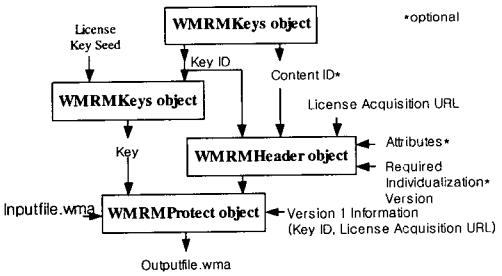
2. DRM 제품

2.1. MS-DRM

Microsoft의 WMT(Windows Media Technology)는 비디오/오디오에 대한 DRM API를 제공한다. 현재 전 세계에 약 4억 개의 Microsoft Media Player가 다운로드 되었으며 *de facto* 표준으로 확고한 자리를 잡아가고 있다[13][20].

2.1.1. 패키징

그림 2는 PWMF(Packaged Windows Media Files)를 만드는 정보의 흐름을 보여주고 있다.



〔그림 2〕 WMF 패키지화 과정 흐름 정보

WMF는 다음 절차를 사용하여 패키징한다 :

(1) WMRMKeys 객체를 사용하여 key ID와 content ID 발생
(2) key ID와 LKS(License Key Seed)를 가진 WMRMKeys 객체를 사용하여 Key 생성
(3) key, key ID, content ID, LAU(License Acquisition URL)를 가지고 WMRMHeader 객체를 사용하여 content header를 생성한다. 여기서 속성(Attributes)를 추가하고, 선택적으로 Required Individualization version number를 선택하는 것을 권장한다.
(4) 입력 파일, key, content header를 가지고 WMRMProtect 객체를 사용하여 PWMF를 만든다. 이때 version 1 Key ID와 LAU를 추가한다.

다음 리스트는 패키징을 위하여 나타내거나 발생되는 정보를 나타낸다 :

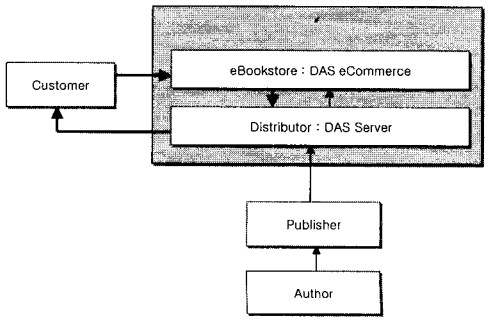
- LKS : WMF를 위한 키를 발생하는데 사용하는 값. WMRMKeys 객체의 GenerateSeed 메소드를 사용하여 라이선스 키 씨앗을 발생시키거나, WMRM 버전 1에서, 같은 값을 계속 사용할 수 있다.
- key : WMRMKeys 객체로 만들어지는 값. WMF 암호화에 사용
- key ID : WMRMKeys 객체로 만들어지거나 당신이 표기할 수 있다. 이 값은 키를 재생하기 위하여 라이선스 키 씨앗과 함께 사용된다.
- LAU : 라이선스 습득을 위한 URL 첫 페이지 지적
- input file name : WMF 이름
- output path and file name : 최종 패키지화된 파일의 패스와 이름으로 입력 파일과 같지 않다.
- content ID : 각 PWMF의 유일한 값. WMRMKeys 객체에 의해 발생되며, 사용하는 것을 권장한다.
- attributes : WMF의 content header에 포함시킬 추가 정보 쌍. 사용하는 것을 권장한다.
- Required individualization version : WMF 파일 작동에 필요한 최소 개인(보안 향상) 버전으로 선택 사항이다.
- version 1 LAU : 버전 1만 지원하는 플레이어용 URL.

- http://www.microsoft.com/isapi/redir.dll?prd=wmdrm& pver=2&os=win&sbp=newclient : 소비자가 WMRM 7을 지원하는 플레이어를 얻을 수 있는 웹 페이지를 표시한다.
- version 1 key ID : 만약 버전 1 라이선스를 포함할 때 값; 이 같은 버전 7 key ID와 같을 것이다.

2.1.2. 권리

- **AllowPlayOnPC** : 이 권리는 소비자가 한 컴퓨터에서 WMF를 작동하는 것을 허가한다. 디폴트로 이 권리가 설정된다.
- **Playcount** : 이 권리는 소비자가 WMF를 작동 횟수를 나타내는 것으로, 디폴트로 이 권리는 설정되지 않고 무한정 작동이 허가된다.
- **AllowBurnToCD** : 이 권리는 소비자가 하나의 WMF를 RedBook Audio 형식으로 CD로 복사되는 것을 허가한다. 예를 들어, 소비자는 음악을 CD로 복사할 수 있어 카 스테레오로 들을 수 있다. 그렇지만, 한번 WMF가 CD로 복사되면, WMF는 더 이상 보호되지 않는다. 디폴트로 이 권리가 설정된다.
- **BurnToCDCount** : 이 권리는 소비자가 WMF를 CD로 복사하는 횟수를 나타내는 것으로, 디폴트로, 이 권리는 설정되지 않고 무한정 복사가 허가된다.
- **AllowBackupRestore** : 이 권리는 소비자가 라이선스를 백업하고 복구하는 것을 허가한다. 소비자는 같은 컴퓨터(새 컴퓨터 구매)나 다른 컴퓨터들(작업 컴퓨터와 집 컴퓨터)로 라이선스를 복구할 수 있다.
- **BeginDate** : 이 권리는 라이선스가 유효하기 시작한 날짜를 나타낸다. 이 날짜 전에는 WMF가 작동되지 않고, 디폴트로 이 라이선스는 즉시 유효하다.
- **ExpirationDate** : 더 이상 라이선스가 유효하지 않는 날짜를 나타내는 것으로 디폴트로 이 권리는 설정되어있지 않고 결코 라이선스가 사라지지 않는다.
- **DeleteOnClockRollback** : 이 권리는 고객의 컴퓨터 시계가 earlier time으로 설정되면 라이선스를 삭제한다. 예를 들어, 라이선스가 만기일을 표시하면 이 권리를 사용할 수 있다. 디폴트로 이 권리는 설정되지 않는다.
- **DisableOnClockRollback** : 만약 고객의 컴퓨터 시계가 rolled back되면, 이 권리는 라이선스를 사용할 수 없다. 라이선스는 시계가 교정되면 다시 가능하게 되며, 디폴트로 이 권리는 설정되지 않는다.
- **AllowTransferToNonSDMI** : 이 권리는 고객이 WMF를 SDMI-비 호환 휴대 장치와 미디어로 전송을 허가하는 것으로 디폴트로 이 권리가 설정되어 있다.
- **AllowTransfertoSDMI** : 이 권리는 고객이 WMF를 SDMI-호환 휴대 장치와 미디어로 전송을 허가하는 것으로 디폴트로 이 권리가 설정되어 있다. 이 권리를 사용할 때, SDMI 사양을 따라야한다.
- **TransferCount** : 이 권리는 고객이 WMF를 SDMI-호환 휴대 장치와 미디어로 전송하는 횟수를 나타내는 것으로, 디폴트로, 이 권리는 설정되어있지 않고 무제한 전송이 허가된다.
- **PMRights** : 이 권리는 휴대용 라이선스에 주는 권리를 나타낸다. 디폴트로 이 권리는 휴대용 장치에서 파일을 작동하는 것과 전송하는 것을 나타내는 것으로 19로 설정되어있다.
- **PMExpirationDate** : 휴대용 라이선스 만기일을 표시한다. 한번 휴대용 라이선스가 소멸하면, 파일은 컴퓨터나 휴대용 장치에서 전송될 수 없다. 휴대용 라이선스가 휴대용 장치에서 만기되면, 파일은 더 이상 작동되지 않는다. 디폴트로, 이 권리는 설정되지 않으며, 휴대용 라이선스는 결코 소멸되지 않는다.

2.2. Microsoft Reader



〔그림 3〕 DAS 기반 DRM 흐름도

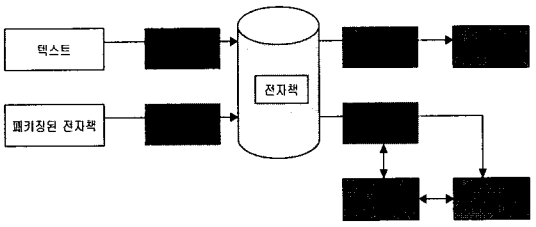
Microsoft의 전자책인 리더는 인쇄된 페이지에서

보는 것 같은 폰트를 만들어 제공하는 ClearType 기술을 제공하고 있다. 부가적으로, 글자 모양의 질, 마진 처리, 적절한 띄우기, 모서리, 북마킹 도구, 하이라이트, 주석달기 등의 기능을 제공한다. http://www.microsoft.com/reader.에서 다운로드 가능하며, Encarta Pocket Dictionary를 설치한 뒤, 특정 단어를 클릭하면, 해당 단어에 대한 정의가 나타난다. 그림 3은 Microsoft 전자책에 라이선스를 제공하는 클리어링하우스 시스템인 Digital Asset Server(DAS)의 서비스 과정을 보여주고 있다. DAS Server는 보통 클리어링하우스 기능을 가지고 있으며, 전자책 컨텐츠를 많이 소유하고 있는 출판사들이 주로 운영하고 있다.

2.3. Adobe ACS

PDF 기반 DRM 시스템은 여러 플랫폼에서 작동되나, 다른 크기 스크린에서 문서를 적당한 크기로 조절하지 못하고 있다(즉 책 크기는 같고, 스크린만 적기 때문에 스크롤을 사용하여 조정). 원 문서의 폰트, 이미지, 레이 아웃이 유지되기 때문에 가독력이 뛰어나다. Adobe Content Server(ACS)는 PDF 기반 전자책 서비스 서버로, 전자책을 준비하고, 제작하여 판매할 수 있게 하는 것으로 다음 기능을 제공한다.

- 전자책 암호화를 위한 패키징 서비스. 소비자의 권리 기술
- 유통업체에게 공급하는 유통 서비스
- 패키징된 컨텐츠를 얻어서 판매 가능하게 하는 서비스
- 전자책 주문 받고, ACS DB로부터 다른 ACS나 소비자로 제공하는 서비스

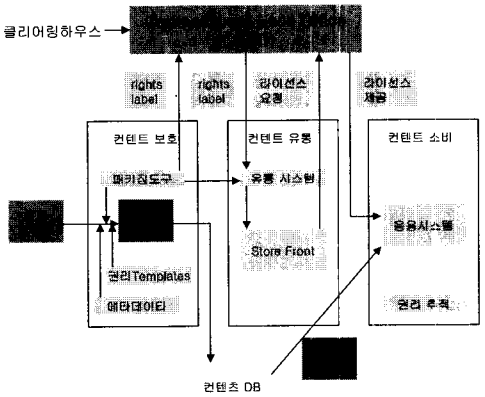


〔그림 4〕 ACS 서비스 모듈

ACS의 서비스 흐름은 그림 4와 같다. 전자책을 컨텐츠 서버를 통하여 제어하고, 온라인 서점을 통하여 소비자가 구매할 수 있는 체계를 제공한다. 내부적으로는 PDF Merchant DRM과 EBX (Electronic Book eXchange) DRM을 선택 지원할 수 있게 구성되어 있다.

2.4. ContentGuard DRM

ContentGuard는 DRM 전문업체로 2000년에 Microsoft로부터 투자받고, Xerox로부터 분사된 회사이다. Xerox에서 개발한 권리 기술 언어인 DPRL을 바탕으로 XrML(eXtensible rights Markup Language)[6]을 개발하였으며, XrML 2.0은 MPEG-21의 REL로 채택된 상태이다. ContentGuard의 DRM은 이러한 XrML 기반으로 만들어졌으며, 그림 5는 ContentGuard의 클리어링하우스인 CGBO (ContentGuard Back-Office)를 기반으로 만들어진 DRM 시스템에 대한 흐름도이다[5].



〔그림 5〕 CGBO기반 컨텐츠 유통 시스템

여기서 CGBO는 CGBO의 컨텐츠 등록 정보인 rights-label을 등록받고, 필요한 유통 회사에 rights-label을 제공하여 판매할 수 있는 형태로 서비스가 구성된다. ContentGuard 시스템의 특징은 다음과 같다 :

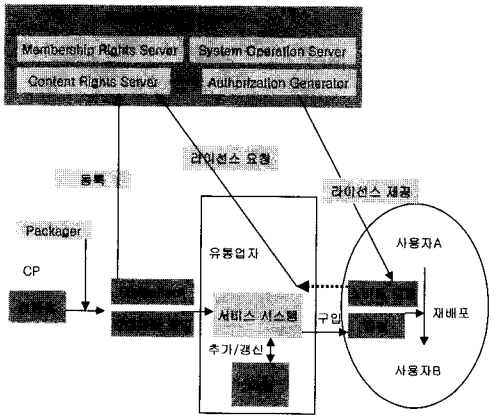
- RightsEdge 플랫폼, DRM 서비스, CGBO SDK 그리고 XrML을 제공한다. RightsEdge 플랫폼은 다음 정보를 포함한다 :
  - 서버는 권리, 라이선스, 회계, 거래 로얄티 정보 관리
  - 암호화된 키 관리를 위한 Activation Server
- 회사의 초기 초점은 법률, 정부, 건강, 재정,

제조업체의 문서 출판에 중점을 두었으며, 고객으로 IndyPublish, Libronauta, Time Warner's iPublish, iBooks, Pearson Education Canada, McGraw-Hill, 그리고 National Music Publisher가 있다.

- Adobe Acrobat Reader를 라이선스하였으며, XrML을 기반으로 MPEG, OeBF, EBX, W3C 등에 표준화 노력을 제공하고 있으며, 전 세계 1,800명의 기관과 사용자가 XrML 라이선스를 발급 받았다.

2.5. Intertrust DRM

Intertrust는 1990년도 설립된 일반 목적의 DRM 플랫폼을 제공하는 회사로 DRM 전문 회사이다. 61개 파트너 회사와 넓은 시스템 플랫폼을 가지고 있으며, DRM의 가장 선발 업체로써 많은 파트너 회사를 가지고 있다[13].



〔그림 6〕 Intertrust DRM 기반 컨텐츠 유통 시스템

그림 6은 Intertrust의 Rights|System에 대한 것으로 컨텐츠를 제작하는 패키저, 서버, 클라이언트 모듈, 그리고 Toolkit으로 전체 구성이 이루어졌다[14].

기능은 다음과 같다.

- 패키저 : 패키저는 순수 컨텐츠를 암호화된 컨텐츠와 RightsPack으로 만드는 도구이다. RightsPack은 컨텐츠에 대한 메타데이타로, Rights|System Server에 등록한다.
- 소비자 모듈 : 컨텐츠에 대한 라이선스를 요청하며, 제공받은 라이선스에 따라 작동시킨다.
- 서버 : 소비자가 요청한 사용 규칙 정보 등이 RightsPack에 추가되어, 컨텐츠 서버를 거쳐 Authorization Generator로 라이선스가 발급된다.
- 툴킷 : 다양한 소비자 모듈을 개발하기 위한 SDK가 제공된다.

3. 표준화 기술

표준 기술은 전 세계 민간 단체나 국제 표준화 기구에서 추진하는 표준화 작업 기술을 의미하는 것이며, DRM와 관련된 주요 표준화 작업으로 MPEG-21, DVB-CP, ISMA DRM Task Force, CEN/ISSS의 DG Infosoc, AAP의 DRM 스펙[4][8][9], CPTWG, IRTF-IDRM 등을 들 수 있다.

3.1. MPEG-21

MPEG-21은 2000년 초 MPEG에서 멀티미디어 컨텐츠 유통 프레임워크 개발을 위하여 추진하는 표준화 그룹으로, 일반적으로 언급하는 DRM이라는 용어가 나타내는 그림보다 훨씬 큰 형태의 프레임워크를 추진 중에 있다[2][11][16].

3.1.1. 소개

멀티미디어 컨텐츠의 유통과 소비를 위한 인프라 구축을 위한 많은 요소가 존재하지만, 어떻게 이러한 원소들이 각각 관련되어 커다란 모습으로 나타나는지에 대하여 기술한 것이 현재까지 없었기 때문에 MPEG-21에서는 이러한 요소들을 적절하게 융합하여, 유통이 가능한 커다란 프레임을 만드는 것이다.

3.1.2. MPEG-21 프레임워크

현재 멀티미디어 기술은 정보와 서비스를 유통 체인을 통하여 다양한 플레이어에 제공하고 있다. 임의의 장소에서 임의의 시간에 정보와 서비스에 대한 접근은 곳곳에 존재하는 터미널과 네트워크를 통하여 제공될 수 있지만 원하는 내용, 형식, 규칙, 절차, 비즈니스 모델을 가지고, 여러 사회에서 사용될 수 있는 완전한 제품이 없기 때문에, 멀티미디어 프레임워크의 개발은 이러한 분야 사이에 공동 작업과 모델, 규칙, 절차, 원하는 내용과 형식의 통합화와 효과적 구현을 지원하는 것이다[17].

멀티미디어 컨텐츠 유통 체인은 컨텐츠의 제작, 생산, 유통과 소비를 강조하고 있으며, 이를 지원하

기 위하여 컨텐츠가 식별되어야 하고, 기술되어야 하며, 관리되고 그리고 보호되어야 한다. 컨텐츠의 전송과 유통은 사건이 발생하고 보고가 필요한 범위에서 다양한 터미널과 네트워크상에서 발생될 것이며, 신뢰성있는 유통과 개인 자료 관리 및 사생활을 고려하고 그리고 재정적 거래를 관리하여야 한다.

MPEG-21은 멀티미디어 유통망을 지원하는데 필요한 주요 요소를 정의하는 것으로, MPEG-21에서 정의되는 7개 주요 원소는 다음과 같다:

- Digital Item Declaration(DID) (디지털 항목을 선언하기 위한 추상적 스킴)
- Digital Item Identification and Description (DII&D) (엔티티를 식별하고 기술하는 구조)
- Content Handling and Usage(컨텐츠 유통과 소비에 대한 컨텐츠의 제작, 조작, 검색, 접근, 저장, 유통, 그리고 (재)사용이 가능하게 하는 인터페이스와 프로토콜)
- Intellectual Property Management and Protection(IPMP) (컨텐츠를 신뢰성있게 관리하고 보호하는 수단)
- Terminals and Networks(네트워크와 터미널를 통하여 컨텐츠에 투명하고, 상호 운용성있게 접근하는 능력)
- Content Representation(멀티미디어 자원이 표현되는 방법)
- Event Reporting(사용자가 모든 보고 가능한 사건의 실현을 정확하게 이해할 수 있는 도구나 인터페이스)

3.1.3. MPEG-21 작업 계획

MPEG-21의 부분별로 진행 계획은 표 1과 같다. 이미 많은 작업이 진행 상태이며, 2001년 12월 현재 RDD-REL에 대한 제안과 선택이 완료된 상태이다.

DID와 DIID로는 CID와 DOI[18][19]가 채택되었으며, RDD로는 〈INDECS〉2[1][3][9]가, REL으로는 XrML이 선택되어 진행 중인 상태이다.

3.2. IRTF-IDRM

3.2.1. 개요

IDRM은 2001년 3월 IETF-50차 Minneapolis 회의에서 처음 연구 그룹이 형성되었으며, 다음과 같은 목표를 가지고 연구를 진행하고 있다[15][22].

- 인터넷 구조에서 DRM의 영향에 대한 연구
- DRM을 지원하기 위한 인터넷 인프라 구축
- IDRM 참고 프레임 개발
- 유용한 컴포넌트 기술을 식별 및 통합
- IETF WG에 DRM 요구 사항을 지원하게 제안
- 개발 체계

  IETF 내부 노력 : CNRP, RESCAP, LDAP, TRADE, AAP, POLICY, IPSEC, IPSP, IPSRA, KINK, MSEC, PKIX, SACRED, STIME, TLS, AVT, IPStorage

  IETF 외부 노력 : MPEG-4/-7/-21, Oasis XACML & SAML, W3C XML, XMLsig, XKMS, DOI/Handle

3.2.2. 제안서 1 : Handle System

핸들 시스템은 인터넷에서 안전한 이름 변환과 관리를 허가하는 일반 목적의 전역적 이름 서비스 시스템이다. 핸들 시스템은 디지털 객체를 위한 유일한 이름인 핸들을 관리하는 것으로, 본 제안서에서

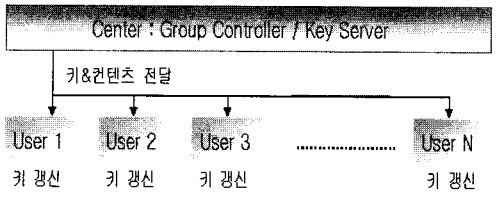
〔표 1〕 MPEG-21 작업 계획표

부분	제 목	CfP	WD	CD
1	비전, 기술, 전략			01/01
2	Digital Item Declaration		01/01	01/07
3	Digital Item Identification and Description	01/01	01/03	02/03
4	Intellectual Property Management and Protection			01/07
5	Rights Expression Language(REL)	01/07	01/12	02/07
6	Rights Data Dictionary(RDD)	01/07	01/12	02/07
7	Digital Item Usage Environment Description	01/10	02/03	02/07

는 핸들 시스템의 이름 공간, 서비스 구조, 그리고 DNS, LDAP/X.5000, URN 사이 관계를 기술하였다[21].

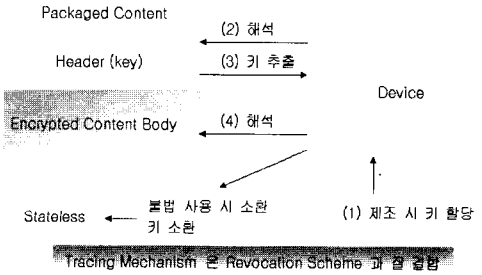
3.2.3. 제안서 2 : 키 관리

Subset-Difference 알고리즘에 기반한 멀티캐스팅 통신 세션을 위한 키 관리 메카니즘을 기술한다[12](그림 7). Subset-Difference 알고리즘은 센터(키 관리자)에서 모든 수신자에게 메시지를 보내는 방식으로, 취소 스킴(Revocation Scheme)에 따라 취소된 수신자는 받은 메시지를 해독할 수 없게 하는 것이다. 메시지는, r이 소환된 그룹 회원 수일 때, 단지 2r 키로 구성되며, 이러한 방식이 어떻게 사용될 수 있는지에 관하여 기술하였다. 주요 장점은 메시지를 받을 수 없는 개인에 대한 개별적 갱신이 필요 없는 것이며, 이것은 통신 장애나 손실률이 높은 통신 환경에서 더욱 유용하다.



〔그림 7〕 멀티캐스팅 환경에서 키 관리

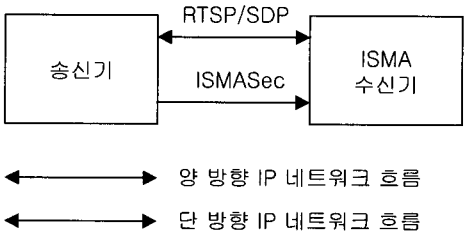
이와 같은 기능은 그림 8과 같은 DVD Player에서 사용되는 키의 사용과 취소에서 같은 형태로 적용될 수 있다. 본 방식은 Group Key Server에서 컨텐츠를 암호화하고, 해석에 필요한 정보를 Header에 부착하여 보내는 것이며, 사용자는 자신이 정당한 사용자일 경우, Header에 부착된 정보를 이용하여 컨텐츠를 풀 수 있게 처리되는 것이다.



〔그림 8〕 DVD Player에서 키 관리 기능

3.3. ISMA DRM

ISMA는 공개 표준 기반 오디오 비디오 컨텐트 스트리밍 제품을 개발하기 위한 기관으로 2001년 9월 ISMA 1.0 사양서를 발표하였다. 본 사양서는 다양한 구성요소 사이 상호 운용성을 보장받기 위하여 단계별로 사양을 제시한 것으로, 하나는 모바일 폰이나 PDA와 같은 좁은 영역의 스트리밍에 관한 것이고, 다른 것은 대역폭에 대한 네트워크 서비스에 관한 것이다. 이러한 서비스는 궁극적으로 Set Top Box나 개인용 컴퓨터에서 작동하는 것이다.



〔그림 9〕 ISMA 구조

ISMA 구조는 그림 9와 같이 구성되며 IP/UDP/RTP (Real-Time Protocol) /MPEG-4와 RTSP (Real-Time Streaming Protocol) 제어 프로토콜을 사용한다.

2001년 가을 DRM Task Force 팀을 구성하였으며, AOL/Time Warner, Bertlesmann, Disney, Electronic Freedom Foundation, Intel Content Protection Group, MPEG-4 IPMP WG, Motion Picture Association, Reutiers, SMPTE CP WG, Sony Pictures IPR Group, WMF, Yahoo에서 참여하고 있다. 구성되는 DRM의 궁극적인 모습은 전형적인 DRM의 유통 환경에서 다음과 같은 흐름을 가진다[10].

- 전형적인 흐름 : 라이선스 서버가 〈rights〉 정보와 DII&D 정보를 가지고, 유통업자는 DII&D를 소비자에게 제공하고, 이 정보로 라이선스 서버로부터 라이선스(〈rights〉와 DII&D로 구성)를 받아서 사용
- 컨텐츠 총괄 : 암호화, 메타데이타 할당, 선택적 워터마킹, 인증, 키와 권리 정의, DII&D / UID 할당

- 라이선스 서버는 키와 권리를, 유통 서버는 컨텐트와 DII&D와 UID를 할당
- 사용자가 컨텐츠 요구(DII&D)
- 라이선스 서버에게 인증 요청 : 유통업체는 파일 작동
- 사용자는 라이선스, 키, 컨텐츠 제공받음

ISMA가 지향하는 바는 공개 표준화 인터페이스와 IPMP의 파라메터 도구를 정의하여 장치 사이에 상호운용성 확보, 기술 조치 보존과 라이선스 허가를 위한 버전 통제 기능 개발하는 것이며, 비즈니스 규칙을 정의하여 작동시키는 것이다. 그러므로 MPEG-21의 권리 사양, 비즈니스 규칙을 추적하며, IETF의 키 관리 기능을 주시하고 있다.

그림 9에 정의된 송신기와 수신기 사이의 ISMASec은 MPEG-4와 RTP를 인증하며, 스트리밍과 다운로드를 지원하며, IPMP를 본 구조에 합병하는 것이다.

3.4. DVB-CPCM

본 기술에 대한 공식적인 명칭은 DVB-CPCM (DVB-Content Protection and Copy Management)으로 디지털 방송과 관련하여, 홈 디지털 네트워크와 PVR(Personal Video Recorder)에서 컨텐츠의 이동과 복사와 관련된 내용을 다루는 것이다[7].

3.4.1. 배경

DVB는 아나로그에서 디지털 방송으로 이전하는 국제 표준화 정착을 위한 방송 분야, 제조분야, 운영 분야 등의 300여 개 업체의 콘소시엄으로 만들어진 기구이다. DVB-CPCM에 대한 표준화 특징은 다음과 같다.

- 공개성 : 표준이 만들어지면, ETSI(http://www.etsi.org/)를 통하여, 정상 비용으로 누구에게나 공개
- 상호운용성 : 표준화에 따른 제품은 다른 장비와 함께 작동을 보장함.
- 융통성 : 데이터 컨테이너로 MPEG-2 패킷을 사용하여, DVB는 HDTV, 다수 채널(PAL, NTSC, SECAM), 또는 DVB-MHP에 의해 제공되는 대화형 서비스 등에 전송
- 시장 주도형 : 유럽과 미국 기구에 비하여, DVB 프로젝트는 시장의 요구사항을 구축하는데 주력했다.

DVB는 광범위한 표준(http://www.dvb.org/standards/index.html)을 가진 조건부 접근(Conditional Access) 부분에서 사양서를 개발하여 왔고, DVR 기술과 계속 기술의 발전으로 DVB는 복제 방지와 관리 기술 부분에서 작업하고 있다. 현재 상업적 모듈에 의해 DVB-CP(DVB Copy Protection) 그룹을 구성하여 DVB-CP 요구 사양서와 DVB-CPCM의 상업적 요구사항에 관한 약어 테이블을 만든 상태이다. DVB TM(Technical Module)은 상업적 요구에 대한 기술적 사양서를 개발하는 것이며, DVB CPT(Copy Protection Technologies) 하부 그룹을 만들었으며, 정기적인 기술서를 보고하고 있다. DVB CPT는 본 Call For Proposals을 제시하였다.

3.4.2 약어 및 용어

- 약어

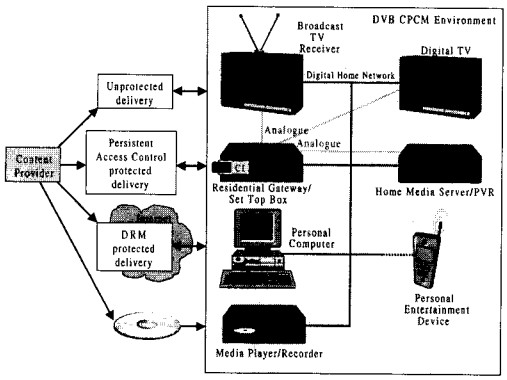
  API : Application Programming Interface
  CAS : Conditional Access System
  DRM : Digital Rights Management
  RG : Residential Gateway

- 용어

  API : DVB CPCP 시스템에 의해 어떤 특정 시스템의 플러그-인에 노출되는 소프트웨어 인터페이스
  RG : 외부, 네트워크 접근 그리고 홈 네트워크에 연결되는 장치

3.4.3. 사용 상태와 통신 구조

그림 10는 기본적인 소비자 영역의 구조를 보여주는 것으로, 본 그림을 바탕으로 DVB-CP의 요구사항이 다음과 같이 만들어진다.



〔그림 10〕 소비자 영역 구조

- 컨텐트는 CP로부터 SP(Service Provider)를 통하여 소비자에게 다양한 유통 방법(보호 없이 유통, 보호되어서(CAS나 DRM) 유통, 그리고 사전 녹화된 미디어로 유통)을 통하여 제공된다.
- 컨텐트가 DVB CPCM 환경에서는 전통적 보호 장치인, CAS를 사용하는 RG, STB(Set Top Box)에서 DVB CPCM으로 이동한다.
- BaseLine DVB CPCM은 'Copy Control Not Asserted', 'Copy Once', 'Copy No More', 그리고, 'Copy Never'라는 4개의 통제된 사용을 지원한다. 또한 CAS에 의해 보호된 컨텐트의 제어는 BaseLine DVB CPCM과 관련될 수도, 안 될 수도 있다. CPCM에 들어가기 전에 보호되지 않는 환경으로 들어갈 수도 있다. 어떻게 들어가든지, DVB CPCM은 소비자에 의해 소비되는 지점에서 사용 상태와 컨텐트 보호를 제공한다.
- 합법적인 아나로그 장치로 인하여, DVB CPCM 시스템은 소비자 영역에서 아나로그와 디지털 장치 사이 컨텐트 흐름을 보호한다. 사용 상태 정보는 아나로그 신호로 사상되어서 아나로그 보호 장치에 '승인된 시장'에 작용한다.
- 영구한 컨텐트 보호는 보호되는 컨텐트 제공자(예를 들어, 사설 CA를 사용하는 지불 TV 방송자)가 적절하게 여기는 시간까지 보호됨을 의미한다. CAS에 의해 제공되는 보호는 접근 통제, 복사 통제를 제공한다. 컨텐트의 비즈니스 모델이 제시되면, CAS는 접근과 복사 통제를 DVB CPCM에 넘길 수 있다. DRM은 자연스러운 방법으로 보호의 영구성을 제공한다.
- DVB CPCM은 두 개 이상의 DVB CPCM 사양 장치 사이에 안전하게 교환될 수 있는 컨텐트 사용 제어, 사용 상태 정보, 보호를 허가하는 표준화된 인터페이스를 제공한다.

4. 결 론

DRM 기술은 디지털 컨텐츠의 안전한 유통과 저작권 보호, 그리고 소비자의 재 활용도를 높인 기술로 여러 기구에서 표준화가 진행 중에 있다. 그 중에서도 MPEG-21과 IRTF-IDRM이 가장 대표적인 DRM 표준화 활동이라고 할 수 있다. DRM은 WIPO에서 제시한 WCT(WIPO Copyright Treaty) & WPPT(WIPO Performances and Phonograms Treaty)[3]에 제시된 언급한 기술로써 선택적으로 갖추어야할 사항이 아니라 법적으로 반드시 사용하여야 하는 기술이다. 그러므로 DRM에 대한 깊은 이해와 적극적인 국내 대응이 필요하다.

참 고 문 헌

〔1〕 이창열, "디지털 정보에 대한 식별자 부여 및 전자상거래용 메타데이타 모델에 관한 연구", 한국교육학술정보원, RR-1999-2
〔2〕 이창열, "MPEG-21 기반 방송 컨텐츠 유통 프로토타입 시스템 개발", 한국전자통신연구원, 연구결과보고서, 2000년 12.
〔3〕 최경수, "WIPO 저작권조약과 우리의 대응", "뉴 밀레니엄에서의 저작권 환경" 세미나, 한국지적소유권학회, 1999년 9월
〔4〕 AAP, "Digital Rights Management for Ebooks : Publisher Requirements version 1.0", 2000
〔5〕 ContentGuard, "ContentGuard DRM Solution overview", October 2000
〔6〕 ContentGuard, "eXtensible rights Markup Language", November 2001
〔7〕 DVB-CP, "DVB Technical Module Sub-group on Copy Protection Technologies", DVB CPT rev 1.1, 05 July, 2001
〔8〕 Godfrey Rust and Bike, Mark, "The 〈indecs〉 metadata model", 〈indecs〉 London conference, 1999, http://www.indecs.org/

[9] Godfrey Rust and Bike Mark, "Introduction to the INDECS metadata schema", Wp1a-001-1.4, 1999, http://www.indecs.org/
[10] ISMA Report, "Internet Streaming Media Alliance DRM Task Force Report", IRTF-IDRM, 52' IETF meeting, October 2001.
[11] Jan Bormans, Keith Hill, "MPEG-21 Overview", ISO/IEC JTC1/SC29/WG11/N4318, Sydney, July 2001
[12] 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.
[13] Joshua Duhl, "The DRM Landscape : Technologies, Vendors, and Markets", IDC, 2001.
[14] Joshua Duhl, and Susan Kevorkian, "Understanding DRM Systems: An IDC White Paper", 2001.
[15] Mark Bauger, "Internet Digital Rights Management Taxonomy", IETF-51 August 6, 2001
[16] MPEG, "MPEG-21 Ovierview v3.0", N4511, December 2001, http://mpeg.telecomitalialab.com/
[17] MPEG, "MPEG-21 Requirements for a Rights Data Dictionary and a Rights Expression Language", W4336, Final v1.0, July 2001
[18] Norman Paskin, "The DOI Handbook", version 0.3 July, 2000
[19] Norman Paskin, "The Digital Object Identifier Initiative: Current Position and Review Forward", IDF, 1999
[20] Paul, John D., and Butler W., "Digital Rights Management Operating System", United State Patent 6,330,670, December 11, 2001. http://cryptome.org/ms-drm-os.htm
[21] Sam X. Sun and Larry Lannom, "Handle System Overview", <draft-irtf-idrm-handle-system-02.txt> August 2001
[22] Thomas Hardjono and Mark Baugher, "IDRM Directions & Work Items", IETF-51 August 6, 2001

〈者 著 紹 介〉

이 창 열 (Chang-Yeol Lee)
1985년 : 고려대학교 수학과(학사)
1991년 : 고려대학교 전산과학과(석사)
1997년 : University Paris VII 전산학과(박사)
1987년~1994년 : ETRI
1997년~2000년 : KERIS
2000년~현재 : 동의대학교 컴퓨터공학과
관심분야 : DRM, 메타데이타 기술, XML