제1회 정보통신표준화 우수논문집

02 우수상 / 일반부문

상호호환성 지원을 위한 모바일 DRM 표준안

A Mobile DRM Specification to Support Interoperability among Different DRM Systems

황성운, 윤기송 / 한국전자통신연구원 디지털콘텐츠연구단

Seong Oun Hwang, Ki Song Yoon / Digital Content Research Division, ETRI

상호호환성 지원을 위한 모바일 DRM 표준안

A Mobile DRM Specification to Support Interoperability among Different DRM Systems

황성운, 윤기송 / 한국전자통신연구원 디지털콘텐츠연구단
Seong Oun Hwang, Ki Song Yoon / Digital Content Research Division, ETRI

요 약

인터넷 상에서 디지털 콘텐츠에 대한 저작권 보호 및 유통을 위해 등장한 DRM 기술은 점차 디지털 홈, 모바일 단말, MP3 플레이어 등 다양한 장치 및 서비스 환경으로 그 활용 영역을 넓혀가고 있다. 그러나 모바일 단말 환경에서는 DRM간 상호호환성 부재로 인해 사용자 불편이 증가하고 있으며 이로 인해 DRM이 자칫 콘텐츠 유통의 장벽으로 작용할 수도 있다. 또한 기존 모바일 DRM 표준안은 높은 비용의 라이센싱 지불 문제를 안고 있다. 이에 대한 대응 방안으로, 본 논문에서는 상호호환성 및 라이센싱 지불 문제를 해결하는 모바일 DRM 표준안을 제안한다.

Ⅰ. 서론

1-1 DRM 정의

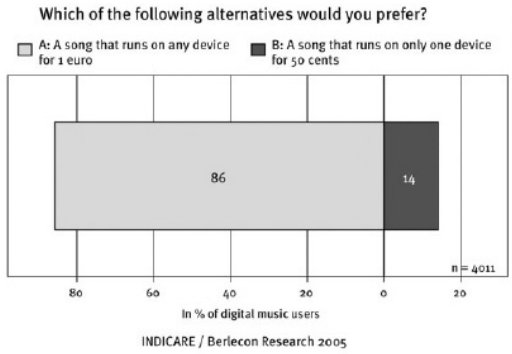
DRM (Digital Rights Management)은 인터넷의 보급과 더불어 디지털 콘텐츠가 활발히 사용되면서 나온 새로운 개념이라고 할 수 있다. 디지털 콘텐츠는 아날로그 콘텐츠와 달리 쉽고, 빠르게 복사할 수 있으며 복제품은 원본에 비해 질적인 저하가 없고 확산 속도가 빠른 속성을 가지고 있기 때문에 콘텐츠의 불법 복제 및 비정상적인 유통 문제에 취약하다. DRM은 이러한 디지털 콘텐츠에 대한 불법 복제 및 불법 유통을 방지 또는 억제함으로써 디지털 콘텐츠에 연관된 콘텐츠 제작자 또는 저작권자의 권리를 보호하기 위해 등장한 기술이라고 할 수 있다. 즉, DRM 기술은 인터넷을 비롯한 무선 통신망, 디지털 TV 등을 이용한 콘텐츠의 전달 및 소비, 유통에 필요한 기술적 장치, 즉 불법 복사 및 유통 방지를 통한 저작권의 보호 및 관리 문제, 올바른 유통 체계 확립 문제 등을 효과적으로 해결할 수 있는 기술이다. DRM 기술은 현재 인터넷에 연결된 PC 상에서 문서 또는 동영상 어플리케이션에 보편적으로 적용되고 있으며 디지털 홈 디바이스 및 모바일 단말 환경으로 그 영역을 점차 확장하고 있다.

1-2 본 연구의 필요성

1-2-1 모바일 DRM 상호호환의 필요성

과거와 달리 DRM 기술 및 시장이 성숙함에 따라 상호호환성의 중요성이 날로 증가하고 있다. 여기서 DRM 상호호환성은 보호된 콘텐츠를 지원되는 DRM 또는 기타 보호 기술에 관계없이 다수의 디바이스에서 사용할 수 있음을 의미한다. 초창기 PC 도메인에서 출발했던 DRM은 현재 디지털 홈, 휴대폰, MP3 플레이어 등 다양한 장치 및 서비스 환경으로 그 활용 영역을 넓혀가고 있다. 그러나 문제는 기존의 DRM 포맷들이 업체 마다 다르며 DRM 표준화 단체들의 표준안들도 상호호환성에 대한 문제점을 제대로 해결하지 못하고 있다는 점이다. 그 결과 일반 사용자가 구매한 콘텐츠가 특정 디바이스에서만 실행되고 기타 디바이스에서는 동작하지 않는 불편함이 발생하고 있다. 현실적으로 DRM은 상호호환성을 제공하지 않음으로써 콘텐츠 유통 비즈니스의 촉진제가 아닌 장벽으로 전락할 가능성도 존재한다.

(그림 2-1)은 Indicare에서 2005년 5월 유럽 7개국 4852명의 인터넷 사용자들을 대상으로 설문 조사한 결과를 나타낸 것이다. 콘텐츠 공유 및 상호호환성이 콘텐츠 서비스 시장 측면에서 얼마나 중요한지를 단적으로 보여주는 시장 조사 자료이다. 즉, 디지털 음악 소비자들 중 86%는 상호호환성을 지원하는 1 유로 (EURO) 콘텐츠를 사겠다고 답변했고, 14%만이 동일한 콘텐츠이나 상호호환성이 지원되지 않는 50 센트 (CENT) 가격의 콘텐츠를 사겠다고 답변했다 [1]. 즉 대다수의 사용자가 가격이 높더라도 상호호환성이 지원되는 콘텐츠를 선호한다는 것이다.



(그림 2-1) DRM 상호호환성에 대한 선호도 조사

위 사례 외에도 상호호환성 미비로 인해 프랑스에서는 소비자 단체들이 애플과 소니를 상대로 소송 [26]을 진행 중 이며, 우리 나라 에서도 유사한 분쟁이 예상된다.

PC상에서는 여러 업체의 DRM 처리 모듈 (DRM 클라이언트 모듈이라고도 함)을 설치함으로써 DRM 상호호환성 문제를 완화할 수 있다. 그러나 모바일 단말 환경에서는 여러 개의 DRM 처리 모듈을 설치 및 운영하기에는 컴퓨팅 자원이 제약되어 있기 때문에 상호호환성 문제를 근본적으로 해결하는 것이 어려우면서도 시급한 실정이다.

1-2-2 로열티 프리 표준안의 필요성

DRM 표준화의 또 다른 이슈는 라이센스 로열티 지불 비용 문제이다. 2005년 1월 초기 특허

보유자인 Contentguard, Intertrust, Matsushita Electric Industrial, Koninklijke Philips Electronics, Sony와 MPEG LA [2]는 OMA DRM [3] 1.0 규격 사용 (OMA DRM 1.0과 2.0을 모두 지원하는 시스템도 포함)에 대한 "The term of a joint patent portfolio license"에 대한 잠정적인 협약에 도달하였고, OMA DRM v1.0의 경우 단말기에 DRM 클라이언트를 실제로 탑재한 업체는 DRM 단말기당 US $1.00, 사용자가 지불하는 모든 트랜잭션에 대한 1% (혹은 1 Cent)를 서비스 제공자가 특허 로열티로 제공해야 한다고 주장했다. 이에 대해 GSMA (GSM Association) (OMA DRM은 주로 GSM 계열의 폰 제조사 및 이동통신 서비스 사업자가 주축이 되어 구성되어 있으므로 GSMA는 OMA 회원사들의 이익을 대변하는 입장에 있다고 보여진다)는 강경한 반대 입장을 천명하였고 이에 대응하여 MPEG LA는 기존 로열티 비용을 단말의 경우 $1.00에서 $0.65로, 모든 트랜잭션당 1%에서 매년 처음 서비스를 사용한 사용자당 $0.25로 변경된 (완화된) 안을 제출하였다. GSMA의 강경한 대응에 MPEG LA와 Licensor 들이 대응책을 마련 중에 있으며, GSMA 에서도 자체적으로 로열티 프리 (royalty-free)인 DRM을 제출해줄 것을 전세계 DRM 개발 업체에 요청한 상태인 것으로 알려지고 있다. 만일 MPEG LA 주장대로 로열티 비용이 결정된다면 유럽 쪽에 수출하는 국내 무선 단말기 제조업체 및 서비스 업체의 비용 부담으로 인해 천문학적인 로열티 유출이 우려된다. 따라서 상호호환성을 지원하는 DRM 기술 규격은 반드시 로열티 프리가 바람직하며, 이를 위해서는 국내에서도 국제 표준안과 경쟁할 수 있는 표준안 제정이 시기적으로 적절하다고 보여 진다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 통해 기존의 표준안 및 기술 분석 결과를 제시한다. 이를 통해 각 기관 또는 단체의 상호호환성에 대한 접근 전략을 분석하고 특히 상호호환성에 대한 보다 더 엄밀한 정의 및 분류를 하고 있다. 3장에서는 본 연구에서 제안하는 상호호환성을 지원하는 모바일 DRM 표준안을 자세히 설명한다. 표준안의 목표 및 범위, 요구 사항, 아키텍쳐 및 그를 지지하는 여러 가지 기술 규격들을 자세히 설명하며 주요 이슈들을 논의한다. 4장에서는 상호호환성 분류 기준을 정의하며 이 기준을 바탕으로 본 논문에서 제안된 표준안과 기존의 국제 표준안 및 기술들과의 비교 분석 결과를 제시한다. 5장에서는 본 연구가 기여하는 점을 요약하고 향후 연구 방향에 대해서 논의하며 결론을 맺는다.

Ⅱ. 관련 연구

다음은 지금까지 진행된 DRM 표준화 활동 및 주요 DRM 업체들의 기술 개발 현황을 간략히 살펴보고, 상호호환성 관련 이슈에 대해서 논의하고자 한다.

2-1 DRM 표준화 현황

2000년을 전후로 MPEG-21 [4] 이외에도

SDMI [5], OeBF [6], DVD Forum [7], iDRM [8], DOI [9], OPIMA [10], CIDF [11]와 같은 다양한 표준화 기구들이 등장하였다. 이를 뒤이어 W3C [12], ISMA [13], TV-Anytime [14], OMA, DLNA [15], DMP와 같은 기구들이 설립되었다. 이 중에서 MPEG, OMA, DMP [19], ISMA가 오늘날까지 활동을 계속해 오고 있다.

• MPEG-2/4/21

IPMP (Intellectual Property Management and Protection)는 MPEG-2/4/21 구성요소 중 여러 종류의 네트웍이나 단말기에서 모든 사용자가 사용하는 디지털 품목(Digital Items: 일반적으로 MPEG에서 디지털 컨텐츠에 대한 정의)의 저작권이나 사용권리를 표현하고 서로 다른 환경 아래에서 지속적으로 안전하게 보호받는 멀티미디어 DRM 프레임웍을 제공한다. MPEG-4 IPMP Extensions [16]과 MPEG-2 IPMP Extensions [17]은 이미 국제 표준이 되었다. MPEG-21은 IPMP를 포함하여 멀티미디어 프레임워크를 모두 7가지 요소 - Digital Item Declaration, Digital Item Identification & Description, Contents Representation, Digital Item Management and Usage, Intellectual Property Management and Protection, Terminal and Network, Event Reporting - 로 분류하고, 각 요소별로 표준화 작업이 끝났거나 진행 중이다. MPEG-n IPMP 프레임워크는 하나 이상의 IPMP 시스템 (IPMP Tool) 들 사이에 인터페이스를 도입함으로써 멀티미디어 콘텐츠의 보호 및 관리를 제공하는 개념이다. 즉 MPEG-n IPMP는 IPMP 시스템 자체를 표준화하는 것이 아니라 IPMP 인터페이스를 표준화함으로써 표준안으로 규정하기에는 벅찬 내용인 IPMP 시스템과 표준안에 포함되어진 요소들 간의 융통성 있는 응용을 가능하게 한다. 단말(Terminal)이 콘텐츠의 IPMP 툴 리스트에 접근해서 콘텐츠를 사용하기 위해 요구 되어지는 IPMP Tool을 결정한다. 결정되어진 IPMP 툴이 단말 내에서 이용되어질 수 있다면 바로 IPMP 툴에 접근하겠지만 그렇지 않은 경우라면 콘텐츠를 사용해야 할 단말에서 빠져있는 IPMP Tool들을 가져와야 한다. 단말은 IPMP 툴 인스턴스를 실행하고 그 실행된 IPMP 툴은 콘텐츠로부터 초기화에 필요한 IPMP 정보를 가져온다. 메지시 라우터가 IPMP 정보를 IPMP 툴에 라우팅하고 단말은 IPMP 툴의 결과에 따라 콘텐츠를 사용한다. MPEG-n IPMP는 콘텐츠의 복호화 처리에 필요한 툴을 필요할 때 찾아서 설치함으로써 상호호환성 문제를 해결하려 하고 있다.

• OMA

OMA (Open Mobile Alliance)는 모바일 환경에서 상호호환성 있는 모바일 서비스를 제공하기 위하여 조직된 기구이다. 이 기구는 2002년 9월에 OMA는 DRM specification v1.0을 출시하였다. OMA DRM v1.0은 콘텐츠 적용 방식(Forward Lock, Combined Delivery, Separate

Delivery), DRM 메시지 및 보호된 콘텐츠에 대한 포맷 (DCF), ODRL [18] 기반 REL 1.0, 콘텐츠와 권한 객체를 전달하기 위한 프로토콜(다운로드 아키텍쳐, ROAP)를 명시하였다. 즉 OMA DRM 1.0은 콘텐츠 패키징 및 사용 권한 표현에만 집중했고 콘텐츠 보호를 위한 강한 보안 메커니즘을 포함하지 않았다 (이때의 보호 대상은 다운로드 가능한 ringtone, wallpaper, screensaver 등 저가의 콘텐츠가 주류를 이룸). 이에 비해 2004년 2월에 출시된 OMA DRM 2.0에서는 MP3 오디오 파일 또는 비디오 클립과 같은 고액의 디지털 콘텐츠를 보호하기 위해 PKI (Public Key Infrastructure) 기반의 높은 레벨의 보안 메커니즘을 채용하였고 부수적으로 몇 가지 특징을 추가하였다.

주요 특징으로는 스트리밍 콘텐츠에 대한 보호 포맷인 PDCF를 추가하였고, 도메인 개념을 도입함으로써 여러 사용자/디바이스들간에 콘텐츠 공유를 지원하고, SD 카드 및 모바일 음악 플레이어와 같은 unconnected device를 지원하도록 설계되었다. OMA DRM은 OMA 이외의 다른 DRM 규격으로의 콘텐츠 및 사용 권한의 Export를 언급하고 있으나 Export 과정에서 발생하는 구체적인 보안 이슈를 적절히 언급하지 못하고 있으며, 대부분을 표준 범위 밖의 문제로 명시함으로써 상호호환성 부분을 명쾌하게 언급하지 못하고 있다.

• DMP

DMP (Digital Media Project)는 2003년 10월에 출범한 국제 단체로 DRM과 기기의 상호호환성 확보를 주된 목적으로 하고 있다.

DMP에서는 가치 사슬 (value chain) 상의 모든 행위자 (actor)들-모두 사용자 (user)라 부름-간에 비즈니스를 하기 위해서 어떤 기능(function)들을 수행하게 되는데 그 기능들은 디지털 미디어를 다루는 기술들을 대표하는 툴(tool)들에 의해 구현된다. 그런데 이 툴들을 포함하여 기술은 급속히 변하므로 오늘 쓰인 어떤 기능이 앞으로도 오랫동안 변함없이 존재하리라고 보장할 수 없다. 이 때문에 DMP에서는 인지된 기능들을 작으면서도 변화하지 않고 안정적으로 보이는 원시 기능 (primitive function)들로 분해한 다음 이 원시 기능들을 표준화 한다. 원시 기능은 간단한 행위를 기술하며 예로는 “Identify data”, “Authenticate user”, “Access content” 등이 있다.

원시 기능들에 바탕을 둔 표준화된 DRM 툴들의 집합을 IDP (Interoperable DRM Platform) 툴킷 이라고 한다. DMP에서 바라보는 상호호환성은, 가치 사슬에 있는 사용자들이 표준화된 툴(공개된 스펙을 가지고 있으나 독립적으로 구현된)들을 사용하여 기능들을 수행할 수 있는 능력을 의미한다. 따라서 IDP는 다양한 가치 사슬들이 표준 기술을 사용하고 상호호환되는 툴들로부터 만들어지기 때문에 compatible하다고 주장한다. 2005년 4월 PAV (Portal Audio & Video Devices)를 위한 IDP-I 스펙을 출시하였으며 현재는 SAV (Stationary Audio & Video Devices)를 위한 IDP-II 스펙을 만들고 있다.

• Coral

Coral [20]이라는 콘소시엄 프로젝트에서는 DRM Interoperabililty 문제를 DRM-중립적인 프레임워크를 통해 서로 다른 DRM간 상호호환성을 제공하는 방법에 접근하고 있다. 이 프로젝트에는 디바이스 제조업체, 헐리우드 영화 배급사, DRM 업체 등이 참여하고 있으며 올 연말에 최종 스펙이 출시될 것으로 알려지고 있다. Coral이 취하는 전략은 DRM-중립적인 상호호환성을 위한 프레임워크를 표준화하는 것으로, 중간의 네트웍/디바이스 레벨에서 권한 중재 및 콘텐츠 변환 (translation)을 함으로써 궁극적으로 서비스 레벨의 상호호환성을 제공하는 것이다.

2-2 주요 DRM 기술 현황

• Microsoft

Microsoft [21]는 DRM 자체의 시장 보다는 자사의 윈도우 OS 시장의 성장을 촉진하는 도구로써 DRM에 접근해 오고 있다. 즉 DRM 제품을 전문적으로 팔지 않고 윈도우 오피스, 윈도우 미디어 플레이어에 번들로 포함시키고 있다. 윈도우 제품은 사용자 친밀성이 높기 때문에 Microsoft의 DRM은 급격히 보급되어 사실상 업계 표준으로 자리 잡았다고 볼 수도 있다.

Microsoft는 WMRM 9 버전까지 자사의 미디어 포맷인 WMF 및 MS 오피스 문서 만을 지원했으나 최근에는 WMRM 10을 통해 PC 뿐만 아니라 Portable Device (예: 휴대형 음악 플레이어, 모바일 폰) 및 IP 네트웍에 연결된 Networked Device (예: 셋톱박스, DVD 플레이어)로 그 영역을 확장하고 있다. MS는 자사 어플리케이션에, 소스 코드 또는 SDK 형태로 제공되는 DRM 컴포넌트, 디바이스간 통신을 위한 MMTP (Microsoft Media Transfer Protocol) 등을 사용함으로써 소스 코드 레벨에서의 상호호환성을 추구한다고 보여진다.

• Realnetworks

RealNetworks [22]는 2003년 오디오와 비디오를 위한 크로스 포맷 능력을 가진 Helix DRM을 발표하였다. 지원 포맷으로는 자사의 포맷 및 MP3, AAC, MPEG-4, H.263 및 기타 다른 미디어 포맷도 지원한다고 한다. 상호호환성 측면에서 Helix DRM이 다른 DRM 포맷을 지원하는 것은 리버스 엔지니어링을 통한 방법이라고 알려져 있다. 즉 다른 회사의 DRM 포맷을 분석하여 이를 처리할 수 있는 모듈을 개발하여 자사의 미디어 플레이어인 RealOne 플레이어에 탑재한 것이다.

그러나 리버스 엔지니어링은 자칫 하면 상대편 회사로부터 지적재산권 관련하여 법률적인 소송에 휘말릴 수 있으며, 상대편 회사에서 리버스 엔지니어링을 무력화 시키기 위해서 버전 업그레이드를 하는 경우에는 DRM 기능을 일관되게 지원하지 못한다는 측면에서 결코 바람직하지 않다고 보여진다. 리버스 엔지니어링과 DRM간의 이슈는 Bechtold의 논문[30]을 참조하기 바란다.

2-3 DRM 상호호환성에 대한 분석

본 논문에서는 다음과 같은 두 가지 범주의 상호호환성을 인용 [23] 하고 이에 대한 기술적 분석을 제시하고자 한다.

상호호환성에는 크게 동일한 규격을 따르는 DRM들 간의 상호호환성 (Intra-DRM Interoperabililty) 및 서로 다른 규격을 따르는 DRM들 간의 상호호환성 (Inter-DRM Interoperabililty) 으로 분류할 수 있다.

• Intra-DRM Interoperabililty

현재까지 진행되고 있는 표준화 기구들에서 진행된 스펙들에서 추구하는 상호호환성이 이 범주에 속한다.

현재 OMA DRM 스펙을 구현한 두 구현물 간에도 상호호환이 되지 않는 실정이라고 한다. 결론적으로 서로 다른 두 DRM 회사가 동일한 국제 표준안을 따른다고 하더라도 둘 간의 상호호환성을 지원하는 것은 쉽지 않다고 판단된다.

• Inter-DRM Interoperabililty

설사 동일한 표준 규격 내에서의 서로 다른 구현물이 상호호환성을 지원한다고 하더라도 최종 사용자들이 원하는 수준의 상호호환성을 지원하기 위해서는 서로 다른 표준 규격 간에 DRM 상호호환성 (Inter-DRM Interoperabililty)을 제공해야 한다.

그러나 서로 다른 DRM 간 상호호환성은 다음과 같은 DRM 기술 본래의 특성에 기인하는 여러 가지 기술적 이슈 때문에 해결하기가 어렵다 : 무엇보다도 각 DRM 규격이 바탕으로 삼고 있는 신뢰 모델 (Trust Model)이 다르기 때문이다. 또한 신뢰 모델이 달라지면 당장에 사용 권한 표현 및 발급 체계 부분에서 달라지게 된다. 마지막으로 서로 다른 식별 체계 (콘텐츠 식별 체계, 디바이스 식별 체계), 서로 다른 콘텐츠 포맷 때문에 상호호환이 기술적으로 어렵다.

이에 대한 보다 더 자세한 설명은 [23]을 참조하기 바란다. 뒤에 설명될 Coral과 본 논문이 추구하는 상호호환성은 이 범주에 속한다.

Ⅲ. 상호호환성 지원을 위한 모바일 DRM 표준안의 제안

다음은 본 논문에서 제안하는 모바일 DRM 표준안의 구성 내용을 자세히 소개한다. 본 표준안은 크게 목표 및 범위, 요구사항 분석, DRM 아키텍쳐, Use Cases, Profile TS (Technical Specification), REL TS, Application Service API TS, Protocol TS로 이루어진다.

각 파트의 문서는 방대하며 본문에 다 싣는 것은 부적절하다고 판단된다. 여기서는 본 표준안을 이해하는데 도움이 되는 수준에서 각 파트별 개요, 특징, 주요 이슈 및 이에 대한 본 논문의 접근 방법 위주로 기술한다.

3-1 표준안 목표 및 범위

3-1-1 표준안 목표

본 표준안은 모바일 환경에서 콘텐츠의 유통

및 소비 과정에서 상호 신뢰 구조를 제공함으로써 불법 복제 및 권리 침해를 방지하고 더 나아가 다양한 콘텐츠 유통 모델이 활성화되는 것을 지원하는 것을 목적으로 한다.

상기 목적을 달성하기 위하여 본 표준안은, 무선 환경에서 다음과 같은 주요 특징을 갖는 DRM 규격을 제공하는 것을 목표로 설정하였다.

첫째, 본 표준안은 DRM 시스템들 간의 상호호환성을 위한 기술적 기반 구조를 제공하는 것을 특징으로 한다. 그 구조는 기존 시스템에 적용시 변경 및 관련 비용을 최소화해야 한다. 둘째, 본 표준안은 로열티 프리라는 특징을 갖는다. 이를 위해 본 표준안에서 제안하는 모든 기술 및 개념은 특정 회사의 특허 및 지적재산권에 종속되지 않아야 한다.

또한 본 표준안은 공개된 표준안이므로 누구나 자유롭게 구현할 수 있어야 한다.

3-1-2 표준안 범위

본 표준에서는 지원 대상 콘텐츠로 다운로드 형태 또는 저장 매체를 통해 전달되는 콘텐츠로 제한하며 (스트리밍 콘텐츠는 차후 버전에서 고려) 단말 플랫폼은 일반적인 모바일 단말 플랫폼을 지원한다.

일반적으로 공개된 플랫폼 (MS .Net 계열, 심비안, 리눅스) 뿐만 아니라 WIPI [24]와 같은 폐쇄형 모바일 플랫폼 등 모든 플랫폼에 적용 가능해야 한다. 본 표준화 범위는 장단기 로드맵에 따라 지속적으로 확장 및 발전될 것이다.

3-2 요구 사항 분석

DRM 표준안 도출에 앞서 실제 시장에서 필요로 하는 기술 및 표준안이 무엇이며 거기에는 어떤 문제가 있는지를 검토하였다. 아래는 도출된 주요 요구 사항을 크게 산업계 요구 사항, 기술적 요구 사항 및 상호호환성 요구 사항으로 분류하였다.

3-2-1 산업계 요구 사항

- 단말 제조사 경쟁력 강화, 국내 콘텐츠 산업 보호, 해외에서의 DRM 기술 경쟁력 강화를 위해 본 표준에서는 로열티-프리 또는 줄일 수 있는 방안을 제시해야 한다.
- 기존 표준안과 차별성이 없는 또 다른 DRM 표준안이 되어서는 안 된다. 현실적으로 기존 시스템을 다 지원하는 것은 어렵지만 모델링 과정에서 고려해야 한다.
- 우리나라의 실질적인 모바일 플랫폼인 WIPI 환경에 포팅이 쉽고 변경을 최소화해야 한다.

3-2-2 기술적 요구 사항

- 기존 DRM의 보호 레벨을 그대로 유지하면서 상호호환성에 대한 구조를 제공해야 한다.
- Secure Environment를 통해 지속적으로 신뢰성 및 위험 요소를 관리할 수 있어야 한다.
- 다양한 권리 방법의 표현 및 비즈니스 모델 적용이 가능해야 한다.
- 표준안은 장단기 로드맵을 제시함으로써 새로운 기술의 발전을 수용하기 위한 확장

성 있는 구조를 갖추어야 한다.
- 사용 규칙은 단순 명료해야 하며 복잡하지 않아야 한다.
- 본 표준안의 빠른 이동통신 환경에의 적용을 위해서 쉽고 이해하기 쉬운 형태의 API를 제공해야 한다.

3-2-3 상호호환성 요구 사항
- 최종 사용자는 사용권한이 허락하는 범위 내에서 구매한 콘텐츠를 여러 단말에서 쉽게 공유하여 사용할 수 있어야 한다.
- 상호호환성을 위해 사용자가 해야 하는 일은 없거나 최소화 되어야 한다.
- 단말기 제조사는 구 포맷의 콘텐츠가 새로운 단말들에서 사용될 수 있기를 바란다.
- DRM 업체는 기존 DRM 구조에 큰 영향을 미치지 않는 범위에서의 상호호환성을 요구하며, 호환 과정에서 신뢰성 및 안전성을 보장 받기를 원한다.
- 이동통신업체는 시간이 지날수록 다양한 DRM 기술들을 적용함에 따라 관리의 복잡도가 증가하는데, 이를 감소하는 방향으로 상호호환성이 제공되어야 한다.
- 콘텐츠 서비스 업체는 동일한 콘텐츠에 이동통신업체마다 달리 보호 기술을 적용함으로써 발생하는 비용을 줄일 수 있어야 한다.

3-3 DRM 아키텍쳐

다음은 본 표준안의 개념 및 구조를 아키텍쳐를 통해 설명한다. 아키텍쳐는 상호호환성 요구 사항을 필수적으로 만족시켜야 하며, 기타 상기 요구 사항들을 모두 고려하여 설계되었다.

3-3-1 아키텍쳐 개념

상호호환성을 제공하기 위해 본 논문의 DRM 아키텍쳐는 두 가지 개념을 바탕으로 한다. 그 중 하나가 도메인이며 다른 하나는 프로파일이다.

정의 1 도메인 (domain) 이란 콘텐츠를 소비하는 주체 (player)–디바이스, 사용자, 그룹 등 어떤 단위도 될 수 있음–들을 그룹핑 (grouping) 하는 논리적인 개념으로써 동일한 콘텐츠에 대하여 동일한 사용권한을 부여하는 단위를 일컫는다.

따라서 동일한 도메인에 소속된 개체 (entity)들을 하나의 콘텐츠 소비 주체로 보고 사용권한을 발급함으로써 동일한 도메인에 속하는 엔터티들은 비록 각각이 다른 디바이스 환경에 놓여 있을지라도 사용권한이 허용하는 범위 내에서 자유롭게 상호호환이 가능해진다. 그러나 도메인 내의 모든 엔터티들이 동일한 사용권한을 가지고 있을 지라도 보호된 콘텐츠 포맷 (DCF)이 회사별로 각기 다름에 유의해야 한다 (주의: 본 논문에서는 기존 회사의 DRM 모듈에 의해 이미 보호된 콘텐츠 포맷을 변경하지 않고 그대로 이용한다). 즉 각 회사별로 보호된 콘텐츠 포맷을 해석할 수 있어야 궁극적으로 상호호환성을 이룩할 수 있다. 각 회사별로 다른 보호된 콘텐츠 포맷을 기술하고 해석하기 위해 나온 개념이 프로파일 (profile) 이다. 다른 사용권한 (ROs)

을 가지고 보호된 콘텐츠 (DCF)를 해석하고 DRM을 처리하는 DRM 엔진 (구조)이 다르다면 상호호환성은 기술적으로 이룩할 수 없다. 이 부분을 해결하기 위해서 본 논문에서는 프로파일 이라는 개념을 도입하였다.

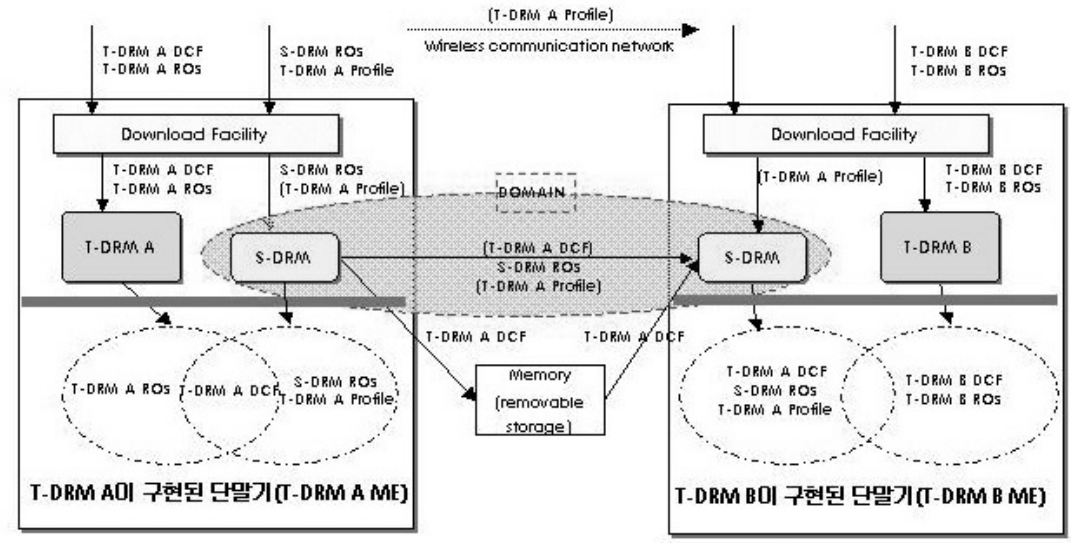
정의 2 프로파일 (profile) 이란 각 DRM 시스템의 구조를 대표하는 정보 구조체 라고 정의할 수 있다. 즉 프로파일은 보호된 콘텐츠 구조, 사용권한 정보 구조 및 데이터를 제공함으로써 DRM 프로세스를 가능하게 하는 최소한의 필수적인 정보 구조체이다.

3-3-2 아키텍쳐 구성

(그림 3-1)는 본 논문에서 제시하는 DRM 아키텍쳐를 개념적으로 나타낸 것이다. <표 3-1>은 본 논문에서 사용된 용어 들을 설명한 것이다.

먼저 (그림 3-1)에서는 두 개의 모바일 단말기에 서로 다른 두 DRM 회사의 모듈 T-DRM A, T-DRM B가 설치되어 있으며 둘 간에는 상호호환성을 제공하지 않는다고 가정한다. 또한 각 단말기는 고유한 식별체계를 이미 가지고 있으며 두 단말기는 동일한 특정 도메인에 소속되어 있다고 가정한다. 본 논문에서 제시하는 S-DRM이 설치되어 있지 않다면 두 단말기 간에는 DRM이 적용된 콘텐츠에 대해서는 상호호환성이 제공되지 않는다.

예를 들어 T-DRM A 회사의 포맷으로 보호된 콘텐츠 (T-DRM A DCF)는 T-DRM A가 구현된 단말기에서는 사용권한 (T-DRM ROs)이 허용하는 범위 안에서 소비될 수 있으나, T-DRM B가 구현된 단말기에서는 적용된 DRM 포맷을 이해할 수 없기 때문에 처리가 불가능하여 결과적으로 상호호환성을 제공하지 못한다. 반대의 경우도 마찬가지이다.



(그림 3-1) 아키텍쳐 개념도

<표 3-1> 용어 설명

용어	설명
S-DRM	본 논문에서 제안하는 표준 DRM 시스템
T-DRM	기존에 존재하는 Traditional DRM 시스템
S-DRM ME	S-DRM이 설치된 단말기
T-DRM ME	T-DRM이 설치된 단말기
T-DRM DCF	T-DRM이 이미 정의한 보호 콘텐츠 포맷
T-DRM REL	T-DRM에서 이미 정의한 REL (Rights Expression Language)
S-DRM REL	S-DRM에서 정의한 REL
T-DRM RO	T-DRM REL의 Instance
S-DRM RO	S-DRM REL의 Instance

본 논문의 상호호환성을 지원받기 위해서는 두 단말기에 표준 DRM 모듈 (S-DRM)이 설치되어 있고, 단말기의 서버 측(즉, 기존의 DRM 서비스 제공자)에도 S-DRM에서 처리하는데 필요한 정보, 즉 S-DRM ROs 및 프로파일을 생성하는데 필요한 모듈이 설치되어 있어야 한다. 사용자가 T-DRM A 단말기 상에서 사용하던 특정 콘텐츠, 즉 T-DRM A DCF를 B 단말기 상에서도 사용하려면 다음과 같다. 먼저 사용자는 S-DRM 모듈을 통해 T-DRM A 서버측 으로부터 S-DRM ROs 및 T-DRM A Profile를 다운로드 받아 설치한다. S-DRM 모듈은 다운로드 받은 파일 중에서 S-DRM 및 T-DRM A Profile을 B 단말기의 S-DRM 모듈에게로 전송 프로토콜 (뒤에 자세히 설명됨)을 이용하여 전송한다. 이때 T-DRM A DCF는 이 전송 프로토콜을 통해 단말기 간에 전송될 수도 있고, 메모리 카드에 담겨서 전송될 수도 있다. T-DRM A Profile은 동일한 전송 프로토콜을 통해 단말기 간에 전송될 수도 있고 서버 측 전송 채널을 통해 전송될 수도 있다.

B 단말기 상의 S-DRM 모듈은 전송되어온 콘텐츠 관련 정보, 즉 프로파일, 사용권한 정보를 이용하여 콘텐츠를 소비하게 된다. 즉, B 단말기상의 S-DRM 모듈은 먼저 T-DRM A Profile에 접근함으로써 T-DRM A DCF와 S-DRM ROs을 어떻게 접근하고 해석하여 DRM 처리를 할 것인지에 관한 정보를 획득하게 된다. 그리고 T-DRM A DCF를 복호화 하는데 필요한 정보는 S-DRM ROs로부터 얻게 된다.

3-3-3 요구되는 신뢰 기관들 (Trusted Authorities)

본 논문에서는 상기 아키텍쳐가 동작하기 위해 필요한 신뢰 기관 및 그들의 역할을 도출하였다. 이것은 논리적인 의미에서 바라본 것이며 실제 현실에서는 한 기관에서 모두 수행할 수도 있다. 이들 기관들의 구조 및 상호 인터페이스는 보다 더 상세히 할 필요가 있으나 본 표준안의 범위 밖이다.

기본적으로 다음과 같은 5개의 신뢰 기관이 필요하다: (1) 도메인 식별체계 (Domain ID) 발급 기관, (2) S-DRM 모듈 제공자, (3) S-DRM 프로파일 제공자, (4) S-DRM 사용권한 제공자, (5) DRM System 식별체계 발급 기관. Interoperable-DRM 서비스를 제공하기 위해서는 각 도메인에 속한 상기 5개 기관 사이의 통신 또는 상호 접촉이 필요하다. 상기 Domain ID 관리 체계는 본 표준안에서 따로 정하지 않고 본 표준이 적용되는 산업계에서 자율적으로 결

정하는 것으로 한다. 본 표준안에서 발생되는 모든 credential 정보는 X.509 v.3 인증서 [25] 형태로 표현된다.

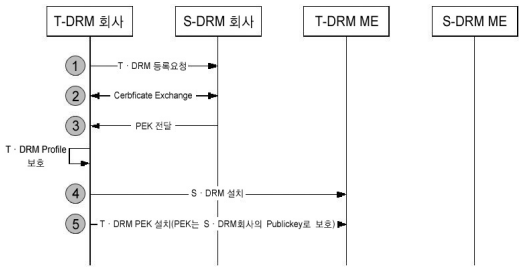
3-4 Use Cases

다음으로 상기 S-DRM의 아키텍처로부터 S-DRM의 몇 가지 기본적인 Use Cases를 도출 하였다. 본 Use Cases는 크게 S-DRM 모듈 설치, S-DRM RO 전송, T-DRM Profile 전송 방법으로 구성된다. 본 Use Cases 중 전송 부분은 3.6절 Protocol TS 파트에서 프로토콜 레벨에서 자세히 기술하고 있으며 여기서는 개괄적인 정보만을 제공함으로써 아키텍쳐에 대한 이해를 돕는다.

3-4-1 Use Case 1 : S-DRM 모듈 설치 (그림 3-2)

프로파일은 보호된 콘텐츠 포맷을 만드는 기존의 DRM 회사들이 생성하게 되며, 프로파일 정보는 기밀성이 요구되므로 안전하게 관리되어야 한다. 프로파일 보호를 위해 사용하는 키가 PEK (Profile Encryption Key) 이다. T-DRM 회사가 자신의 정보를 S-DRM 회사에 등록하고 PEK를 전달받아 S-DRM 모듈과 함께 설치하는 과정은 다음과 같다.

(1) T-DRM 회사가 S-DRM 회사에게 등록 요청함
(2) T-DRM 회사와 S-DRM 회사가 Certificate 을 교환함
(3) S-DRM 회사가 T-DRM 회사에게 PEK 전달함. T-DRM 회사는 T-DRM Profile 을 PEK를 이용하여 보호함
(4) T-DRM ME는 T-DRM 회사로부터 S-DRM 을 다운로드하고 설치함
(5) T-DRM ME는 T-DRM 회사로부터 PEK를 전송받음



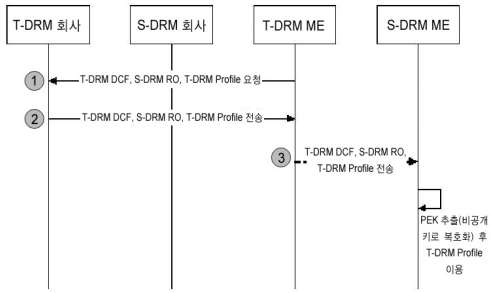
(그림 3-2) S-DRM 모듈 설치

3-4-2 Use Case 2 : S-DRM RO와 T-DRM Profile을 함께 전송 (그림 3-3)

동일한 도메인에 속하는 두 단말 간에 S-DRM RO, T-DRM Profile을 전송하는 절차는 다음과 같다.

(1) T-DRM ME는 T-DRM 회사에게 Group 1 (여기서 도메인 이름을 Group 1 이라 가정하자)에 대한 T-DRM DCF, S-DRM RO, T-DRM Profile을 요청함
(2) T-DRM 회사는 T-DRM ME에게 Group 1에 대한 T-DRM DCF, S-DRM RO, T-DRM Profile을 전송함
(3) Group 1에 속한 S-DRM ME는 T-DRM ME에게서 T-DRM DCF, S-DRM RO, T-DRM Profile을 전송받고, PEK를 이

용하여 T-DRM Profile을 추출함. S-DRM ME에서 T-DRM DCF, S-DRM RO, T-DRM Profile을 통하여 콘텐츠를 이용함



(그림 3-3) S-DRM RO와 T-DRM Profile을 함께 전송

3-4-3 Use Case 3 : S-DRM RO와 T-DRM Profile을 별도 전송

Use Case 2와 동일하나 T-DRM Profile를 T-DRM ME에게서 받지 않고 바로 T-DRM 서버로부터 받는 점이 다르다. 본 표준에서 T-DRM Profile은 보안상 주의를 요하므로 T-DRM Profile 전송 방법은 T-DRM 회사에서 결정하도록 한다.

3-4-4 Use Case 4 : PAN (Personal Area Network) 환경에서 S-DRM RO 전송 (그림 3-4)

이전 Use Case 2와 동일하나, S-DRM ME가 T-DRM DCF를 유선 또는 메모리로 전송 받는 점이 다르다.

T-DRM DCF의 전송 방식은 제한되지 않으나 S-DRM RO 전송은 PAN 환경에서 T-DRM ME와 S-DRM ME 사이로 제한된다.

3-4-5 Use Case 5 : 무선 네트워을 이용한 RO 전송

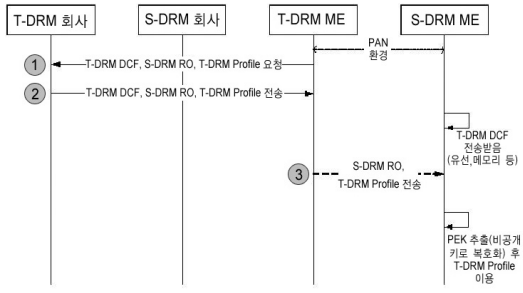
다음과 같이 두 가지로 다시 분류할 수 있다.

3-4-5-1 S-DRM RO와 T-DRM Profile를 함께 전송 (그림 3-5)

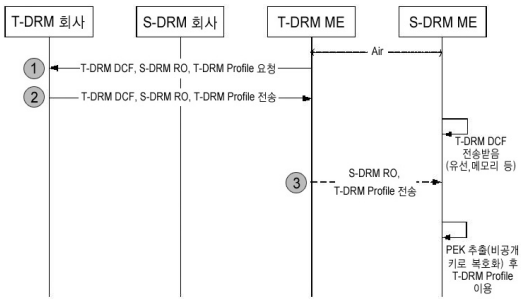
(1) T-DRM ME는 T-DRM 회사에게 Group 1에 대한 T-DRM DCF, S-DRM RO, T-DRM Profile을 요청함

(2) T-DRM 회사는 T-DRM ME에게 Group 1에 대한 T-DRM DCF, S-DRM RO, T-DRM Profile을 전송함

(3) S-DRM ME는 T-DRM DCF를 유선 혹은 메모리로 전송받음. 그 뒤 S-DRM ME는 T-DRM ME에게서 S-DRM RO, T-DRM Profile 전송받고, PEK를 이용하여 T-DRM Profile을 추출함. S-DRM ME에서 T-DRM DCF, S-DRM RO, T-DRM Profile을 통하여 콘텐츠를 이용함



(그림 3-4) PAN 환경에서 S-DRM RO 전송



(그림 3-5) S-DRM RO와 T-DRM Profile를 함께 전송

3-4-5-2 S-DRM RO와 T-DRM Profile를 별도 전송

위의 Use case 3.4.5.1과 거의 같으나, T-DRM Profile이 맨 마지막 스텝 다음에 요청되고 받아지는 부분이 다르다.

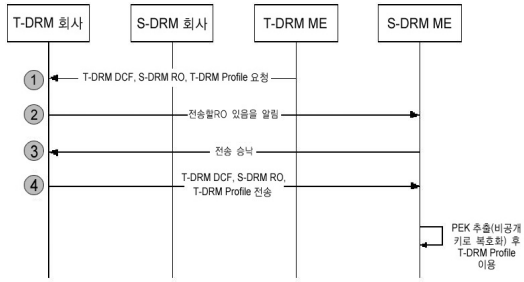
3-4-6 Use Case 6 : T-DRM 회사 서버에서 S-DRM RO 전송 (그림 3-6)

(1) T-DRM ME는 T-DRM 회사에게 Group 1에 대한 T-DRM DCF, S-DRM RO, T-DRM Profile을 S-DRM ME에게 전송하도록 요청함

(2) T-DRM 회사는 S-DRM ME에게 전송할 RO 또는 Profile이 있음을 알림

(3) S-DRM ME는 T-DRM 회사에게 전송을 승낙함

(4) S-DRM ME는 T-DRM DCF를 유선 혹은 메모리로 전송받음. 그 뒤 S-DRM ME는 T-DRM 회사 서버로부터 S-DRM RO, T-DRM Profile을 전송받고, PEK를 이용하여 T-DRM Profile을 추출함. S-DRM ME에서 T-DRM DCF, S-DRM RO, T-DRM Profile을 통하여 콘텐츠를 이용함



(그림 3-6) T-DRM 회사 서버에서 S-DRM RO 전송

3-5 Profile TS (Technical Specification)

다음은 본 표준안이 바탕하고 있는 주요 개념 중 하나인 프로파일의 구조 및 스키마를 설명한다.

3-5-1 프로파일 구조

본 규격에서 정의하는 DRM Profile은 기존 DRM 시스템이 보호하는 DRM Content (즉 보호된 콘텐츠)를 S-DRM 기술이 이용할 수 있도록 데이터와 이를 추출할 수 있는 방법을 명세한다.

DRM Profile은 XML Schema를 이용하여 명세된다. DRM Profile은 S-DRM이 기존 DRM 시스템의 DRM Content를 이용하기 위해 필요한 최소한의 정보를 우선적으로 포함하고 있다. 기본적인 DRM 처리를 위해 필요한 부분, 즉 주로 데이터를 해석하고 복호화해서 어플리케이

션에 넘겨주는데 필요한 정보를 관리한다. 기존 DRM 시스템에서 명세한 데이터 중에서 S-DRM의 운영을 위해 불필요한 데이터들이 존재할 수 있는데 이러한 데이터와 이의 추출 방법은 본 DRM Profile에 명세하지 않는다. S-DRM의 다양한 기능들이 버전 증가와 함께 추가되면서 필요한 기존 DRM Content의 데이터 및 추출 방법을 추가할 예정이다.

3-5-2 프로파일 스키마 (그림 3-7)

DRM Profile Schema는 크게 'Profile 자체에 대한 정보'와 '대상으로 하는 DRM Content에 대한 정보'로 구분된다.

(1) Profile Context: 본 구조에서는 크게 Profile, Context 구조로 구분된다.

- Profile Structure – Profile을 위한 기초 요소로써 Profile의 Root Element가 된다. Profile 자체에 대한 메타데이터와 Profile의 대상이 되는 DRM Content에 대한 메타데이터, 보호된 콘텐츠의 추출 정보가 기술되어 있다.
- Context Structure – 본 Profile 자체에 대한 정보와 본 Profile이 대상으로 하는 DRM 시스템의 식별 정보 및 버전 정보를 포함한다. 본 정보는 DRM Content에서 추출하는 정보를 나타내는 것이 아니라 Profile 자체에서 명세한 정보로써 S-DRM이 특정 DRM Content를 이용할 때 해당하는 DRM 시스템의 Profile을 검색하기 위한 정보로 사용할 수 있다.

(2) DRM Content: 본 구조는 크게 DRM Metadata, Protected Content 구조 및 프로파일의 효율적인 표현을 위한 Inventory 구조로 구분된다.

- DRM Metadata Structure – DRM Content의 메타데이터 정보를 추출하는 방법을 명시한다. 본 Profile에서 추출할 수 있는 DRM Content 메타데이터는 다음과 같다: DRM System ID, DRM System Version, Content ID, DRM Content의 MIME Type, DRM Content의 파일 확장자, 원본 콘텐츠의 MIME Type, 암호화 방법, Right Issuer URL 정보. 기존의 DRM 시스템의 DRM Content 정보 중에서 상기하지 않은 DRM Metadata로는 콘텐츠 저작자 정보, 콘텐츠 설명, 저작권 정보, 콘텐츠 이름 등이 존재한다. 이러한 정보들은 S-DRM이 DRM Content를 이용하는데 직접적으로 이용하는 정보가 아니므로 본 버전의 Profile 명세에서는 포함하지 않는다.
- Protected Content Structure – Protected Content Structure는 DRM System이 보호하는 콘텐츠를 추출할 수 있는 정보를 제공한다.
- Inventory Structure – DRM Content 자체를 표현하기 위한 구조는 아니고 Profile을 효율적으로 표현하기 위한 도구로 이용된다. DRM Content에 대한 정보를 표현하기 위해 offset 과 같은 위치 정보가 중복되어 사용될 수 있는데 공통적으로 이용될 수

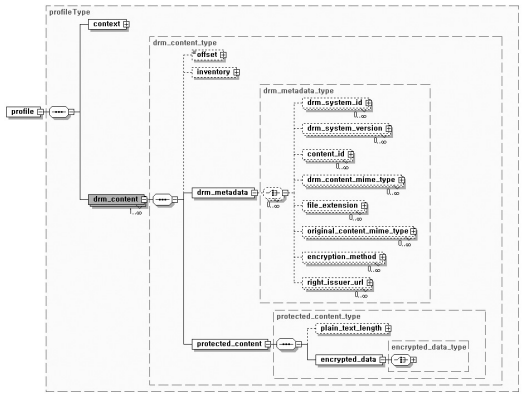
있는 정보들을 Inventory Structure를 통해 기술하고 이를 Profile 내에서 참조하여 사용할 수 있도록 함으로써 Profile의 중복성을 줄이고 간결한 표현을 가능하도록 한다.

3-5-3 프로파일 주요 이슈

프로파일은 특정 DRM 시스템뿐만 아니라 일반적인 DRM 시스템을 모두 표현할 수 있어야 한다. 표현의 일반성 (universality)을 위해서 본 논문에서는 MPEG LA에서 작성한 DRM Reference Model – DRM 시스템에서 공통으로 사용되는 구성 요소를 기술한 것 – 을 참조하였다. 그러나 아무리 DRM 기본 기능이라 하더라도 프로파일로 표현하기 어려운 경우가 있을 수 있다.

따라서 대부분의 기능은 프로파일을 통해 처리하도록 하고 극히 예외적인 경우 (예를 들어, 특정 데이터를 추출하거나 계산, 처리하는 방식이 매우 복잡하여 프로파일로 표기하는 것이 비효율적인 경우 ; 특정 DRM 시스템이 회사 정책상 프로파일에서 처리할 수 있도록 기술할 수 없어 별도로 처리를 요하는 경우 등)로 제한하여 플러그인을 통해 처리할 수 있도록 프로파일을 설계하였다.

즉, 프로파일 처리 모듈이 처리할 수 없는 특정 DRM 시스템의 특정 기능에 대해서, 프로파일 처리 모듈이 특정 DRM 시스템이 제공하는 기능을 통해 (또는 호출하여) 이 기능을 처리할 수 있도록 인터페이스 정보를 표현하는 방법을 XML-RPC [31] 방식을 통해 제공한다.



(그림 3-7) 프로파일 스키마

또한 프로파일은 상호호환성을 지원할 기존 DRM이 추가될 때마다 확장되어야 한다. 프로파일이 XML로 표현되기 때문에 확장을 표현하는 것은 어렵지 않으나 문제는 기존 체계 내에서 확장이 체계적으로 이루어질 수 있느냐이다. 따라서 본 프로파일은 업계의 의견 수렴 과정에서 보다 더 자세히 검토되어야 할 부분이다.

3-6 REL TS

본 규격에서 정의하는 REL은 기존 DRM 시스템이 보호하는 DRM Content에 대한 접근 및 사용 제어 정보가 기술되어 있다. DRM Content는 명세된 Right에 따라 사용된다.

3-6-1 REL 구조

DRM REL은 ODRL V1.1을 참조하여 정의 한다. Right는 DRM Content 접근에 대해 어떠한 환경 조건에서 허용할 것인지를 정의한

Permission과 Constraint 정보이다. 기능에 따른 Right Elements를 <표 3-2>과 같은 Model 단위로 그룹화 하였다. Permission Model을 Constraint Model과 함께 이용함으로써 DRM Content의 접근 및 사용을 세세하게 제어할 수 있다. Inheritance model은 Right Instance 간에 부모(parent)/자식(child) 관계를 명시할 수 있도록 하여 Right가 주기적으로 갱신되어야 하는 Subscription 서비스 시나리오에서 효율적으로 이용할 수 있도록 한다.

〈표 3-2〉 REL 구성 모델 설명

모델명	설명
Foundation	Right 자체에 대한 메타 정보와 Right의 Agreement 내용 기술
Context	이 Model을 포함하는 상위 Model에 의존한 메타 정보 표현
Agreement	DRM Content에 대한 정보, Permission Model 정보를 포함
Permission	DRM Content에 대한 접근 및 사용 허용 정보 표현
Constraint	DRM Content의 접근 및 사용 제어를 위한 상세한 제한 조건을 표현
Inheritance	Right Instance 간에 부모(parent)/자식(child) 관계를 명시
Security	DRM Content와 Right Instance 간의 연관 무결성 보호를 제공하고 Permissions/Constraints 정보에 대한 무결성 보호, 암호화 키의 기밀성을 제공

3-6-2 주요 이슈

현재 실세계에서는 OMA DRM과 MS DRM 간의 상호호환성을 강하게 요구하고 있다. 또한 국내 대부분의 모바일 DRM도 이들을 수용하거나 수정해서 사용할 것으로 보인다. 이 현상을 반영하기 위해 본 표준안에서는 OMA DRM이 바탕하고 있는 ODRL를 출발점으로 했으며 여기에 MS에서 필요로 하는 부분을 추가하는 형태로 REL을 개발하였다. 본 논문에서 ODRL를 기본적으로 참조한 이유는, ODRL의 경우 라이센싱 비용이 무료인 완전히 공개된 스펙이며, OMA DRM을 비롯하여 일반적으로 무선 환경에서 많이 사용되며, 비교적 간단하면서도 대부분의 내용을 포함하는 형태의 REL이기 때문이다. 이 부분도 업계의 의견 수렴 과정에서 보다 더 자세히 검토되어야 할 부분으로 판단된다.

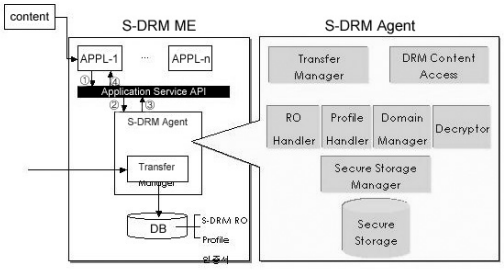
3-7 Application Service API TS

본 파트에서는 S-DRM에서 어플리케이션에 공개해야 할 API를 정의한다. API를 정의하는데 있어서 요구 사항은 다음과 같다: 첫째, 어플리케이션 개발업체는 DRM을 모른다고 하더라도 손쉽게 본 표준안에서 제공한 API를 이용하여 DRM 서비스를 이용할 수 있도록 해야 한다. 둘째, S-DRM을 다양한 사업 모델에 적용하기 위해서 S-DRM에서 제공하는 API는 확장성을 가질 필요가 있다. 이를 위해서는 어플리케이션 측면에서 꼭 필요가 있는 함수를 정의하는 것이 바람직하다. S-DRM 내부에서만 사용되는, 즉 어플리케이션으로 공개될 필요가 없는 API에 대해서는 본 표준안에서는 정의하지 아니하고 S-DRM업체가 자율적으로 정의해서 구현하도록 한다. S-DRM Agent는 모바일 단말기 상에서 보호된 콘텐츠에 관련하여 사용 권한을 허가하거나 접근을 통제하는 역할을 한다. 본 논문에

서는 먼저 (그림 3-8)와 같이 S-DRM Agent 내부의 주요 모듈을 찾고 어플리케이션 입장에서 요구하는 정보가 무엇이고 이를 위해서 S-DRM Agent와 통신해야 할 정보가 무엇인지를 찾아낸 다음 이를 API 형태로 기술하였다. 이와 관련 <표 3-3>를 참조하기 바란다.

<표 3-3> S-DRM Agent 내부 모듈 및 API

모듈명	기능	정의된 API
Transfer manager	S-DRM RO, profile의 수신 및 저장 관리	-requestTransfer()
DRM Content Access	콘텐츠를 접근하는 함수 제공	-drmFileOpen(), -drmFileClose(), -drmFileRead(), -drmFileSeek()
RO Handler	S-DRM RO의 요청 및 저장, 해석, 키관리	-IsExistingRO(), -requestRO(), -queryRO(), -manageRO()
Profile Handler	profile의 해석	-없음
Domain Manager	도메인 정보 관리(domain id, domain key 등등)	-registerDomain(), -joinDomain(), -leaveDomain(), -queryDomainInfo()
Secure Storage Manager	RO Handler, Profile Handler, Domain Manager, Decryptor의 직접적인 DB접근을 통제	-없음
Secure Storage	보안이 요구되는 키, S-DRM RO, 인증서, profile 등을 저장	-없음
Decryptor	S-DRM RO와 profile을 이용하여 암호화된 콘텐츠의 복호화	-없음



(그림 3-8) S-DRM Agent 내부 구조

3-8 Protocol TS

다음은 아키텍쳐에서 표현된 동작 (operation)을 지원하기 위한 프로토콜을 기술한다. Protocol TS는 크게 S-DRM 단말기 등록 프로토콜, S-DRM 사용권한 획득 프로토콜 및 S-DRM RO, T-DRM Profile 전송 프로토콜을 포함한다.

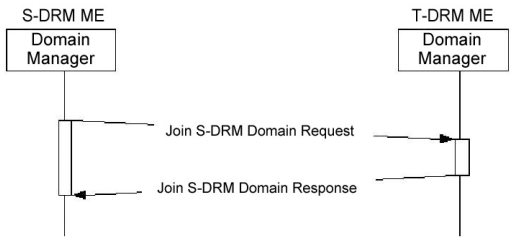
3-8-1 S-DRM 단말기 등록 프로토콜

S-DRM RO를 발행하기 위하여 T-DRM Rights Issuer에 S-DRM ME의 등록하는 방법을 기술한다. 등록 프로토콜은 RI와 S-DRM ME 간의 보안 관련 정보를 교환한다. 이 프로토콜은 처음 접속시 실행되며, 보안 사항의 업데이트가 필요할 시 추가적으로 실행될 수 있다. 이 프로토콜의 파라미터로 프로토콜 버전, T-DRM ME ID, S-DRM ME IDs가 포함한다. 등록 프로토콜이 실행된 후 S-DRM ME에 RI

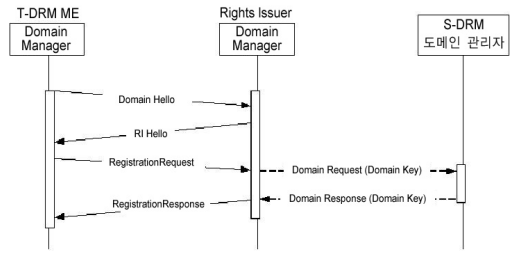
Context가 설정된다. RI (Rights Issuer) Context은 프로토콜 버전, 인증서 등의 RI 보안 정보를 포함한다. S-DRM ME 등록 프로토콜은 다른 프로토콜의 실행 전에 반드시 실행되도록 한다. S-DRM ME는 이미 T-DRM 서버에 등록된 T-DRM ME의 S-DRM 내의 Domain Manager를 통해 등록된다. 이러한 S-DRM ME를 등록하는 방법은 다음과 같이 두 가지로 나눌 수 있다.

- 다수의 S-DRM MEs가 T-DRM ME를 통해 일괄적으로 등록된다.
- 단일 S-DRM ME가 T-DRM ME를 통해 개별적으로 등록된다.

본 규격서에서는 S-DRM MEs의 일괄등록을 기술하도록 한다 (그림 3-9, 그림 3-10).



(그림 3-9) T-DRM ME의 Domain Manager에 S-DRM ME의 등록 (1단계)



(그림 3-10) T-DRM ME Domain Manager에서 S-DRM 도메인 관리자에 S-DRM MEs의 일괄등록 (2 단계)

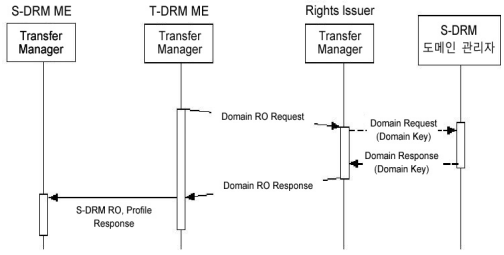
T-DRM ME의 Domain Manager는 같은 Domain에 속하는 S-DRM ME의 정보를 관리하는 기능을 갖고 있어야 한다.

T-DRM ME Domain Manager는 상기 그림과 같은 S-DRM ME 등록 절차를 이용하여 S-DRM ME를 일괄 등록하기 위한 S-DRM ME의 정보를 수집한다.

3-8-2 S-DRM 사용권한 획득 프로토콜

S-DRM 사용권한 획득 프로토콜은 S-DRM RO와 T-DRM Profile을 발급하는 프로토콜이다. 이 프로토콜은 S-DRM ME와 RI 간의 무결성이 보장된 request, S-DRM RO 와 T-DRM Profile의 전송을 포함한다. S-DRM RO 발급 프로토콜의 실행 전에 S-DRM ME는 이미 RI Context를 보유하고 있어야 한다.

(그림 3-11)에서 Domain RO는 T-DRM ME와 도메인을 공유하는 단말들에게 제공되는 RO를 의미한다. T-DRM ME가 RO 발급을 RI에게 요청하면, RI는 S-DRM 도메인 관리자로부터 받은 도메인 키로 Domain RO를 바인딩 하여 T-DRM ME 또는 S-DRM ME에게 내려 보낸다.



(그림 3-11) S-DRM ME에 의한 S-DRM RO 전송

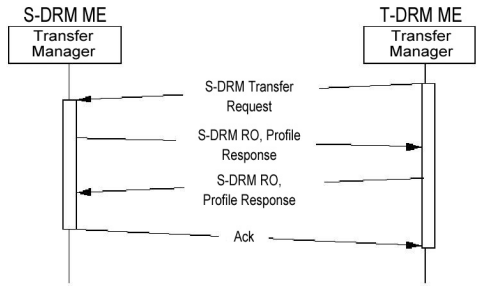
3-8-3 S-DRM RO 및 T-DRM Profile 전송 프로토콜

S-DRM RO와 T-DRM Profile을 S-DRM ME로 전달하는 절차를 기술한다. S-DRM RO 및 T-DRM Profile 전송 프로토콜의 실행 전에 S-DRM ME는 이미 RI Context를 보유하고 있어야 한다.

S-DRM ME는 S-DRM Transfer Protocol을 통해 S-DRM RO와 T-DRM Profiile을 전송받는다. 이러한 S-DRM RO와 T-DRM Profile을 전송하는 방법은 크게 단말간 전송(블루투스, IrDA, 메모리, 케이블) 및 서버 (무선 네트워크)를 통한 전송으로 나뉜다. 구체적으로 다음과 같이 네 가지로 나눌 수 있다.

- T-DRM ME와 S-DRM ME간에 S-DRM RO와 T-DRM Profile을 OBEX로 전송한다.
- T-DRM ME와 S-DRM ME간에 S-DRM RO와 T-DRM Profile을 MMS로 전송한다.
- T-DRM 서버와 S-DRM ME간에 T-DRM Profile을 HTTP로 전송한다.
- T-DRM 서버와 S-DRM ME간에 S-DRM RO와 T-DRM Profile을 SMS URL Callback으로 전송한다.

(그림 3-12)은 T-DRM ME와 S-DRM ME간에 S-DRM RO와 T-DRM Profile을 OBEX [27] 또는 MMS [28]로 전송하는 것을 나타낸다.



(그림 3-12) S-DRM RO, T-DRM Profile 전송 프로토콜

본 프로토콜의 장점은 다양한 기존의 전송 프로토콜(OBEX, MMS, HTTP [29])을 이용할 수 있도록 설계되었다는 점이다. 따라서 사용자는 단말간 전송 또는 서버를 통한 전송을 택할 수 있다.

Ⅳ. 제안된 표준안의 분석

본 절에서는 상호호환성을 중심으로 제안된 표준안에 대한 분석 및 타 표준안과의 비교 결과를 제시한다. 이를 위해 본 논문에서는 비교 기준으로 상호호환성 분류를 위한 두 가지 기준을 제시한다. 또한 각 기준 별로 본 논문에서 제시한 표준안이 갖는 특성을 분석하고 기존 DRM과 비교한다 (<표 4-1> 참조).

다음은 상호호환성 분류를 위한 첫째 기준 및 그에 따른 분석 결과 이다.

- DRM 콘텐츠의 수정 여부–상호 호환성을 제공하기 위해 DRM Format, DRM Message, DRM Right와 같은 DRM 데이터의 변경, 변환, 변형과 같은 조작이 발생하느냐에 따라 분류할 수 있다. <표 4-1>에서 알 수 있듯이 Coral, Realnetworks를 제외한 대부분의

DRM이 상호호환성 지원을 위해서는 DRM 콘텐츠의 수정이 필수적이다. 본 표준안은 DRM 콘텐츠의 수정이 불필요하다.

- 타 DRM의 허용 여부 – 다른 형태 혹은 규격의 DRM이 존재하더라도 상호 호환성이 보장되는지에 따라 분류할 수 있다. Coral, Realnetworks 및 본 표준안은 Inter-DRM Interoperability를 염두해 두고 개발되었기 때문에 타 DRM도 지원 가능하다.
- DRM 자체의 수정 여부 – 다른 형태의 타 DRM이 상호 호환성을 만족하기 위해 변경, 수정, 패치, 혹은 업데이트가 필요하느냐에 따라 분류할 수 있다. Coral, Real-networks 및 본 표준안을 제외한 다른 DRM 시스템들은 상호 호환성을 제공하기 위해서는 부분적인 수정이 필요하거나 불가능할 수도 있다.
- 사용자의 인식 및 개입 여부 – 상호 호환성을 위해 사용자가 명시적으로 개입하거나 인식하느냐에 따라 분류할 수 있다. 사용자가 DRM에 대한 인식 없이 손쉽게 콘텐츠를 소비할 수 있는 것은 일반적인 DRM 시스템의 중요한 요구 조건 중의 하나이다. 유일하게 Coral은 사용자 인식이 불필요하다고 알려져 있다. 본 표준안의 경우에는 사용자가 행하는 액션 부분의 대부분을 서버 쪽에서 대행할 수 있는 구조를 제공함으로써 상당 부분 인식이 불필요하다.
- DRM 규격의 공개 여부 – 산업계 콘소시엄을 비롯한 대부분의 표준화 단체에서 추진하는 규격들은 공개되어 있으나 기업들의 제품 규격은 비공개되어 있는 실정이다. 따라서 본 논문에서 제시한 기업들의 제품에 대한 평가는 주로 제품 사용 경험이나 내부 정보에 의존하고 공식적인 규격에 의존하지 않는 한계점을 갖고 있을 수도 있다.
- Lossless vs. Lossy 변환 – 상호 호환성으로 인해 DRM Format, DRM Message, DRM Right에 포함된 메타 정보, Right 정보 등과 같은 DRM 정보의 손실이 발생하는지에 따라 분류할 수 있다. Coral과 본 표준안은 기존의 시스템에 DRM 처리 기능을 추가하여 상호호환성을 지원하기 때문에 상호 호환성 지원과정에서 정보의 손실이 발생하지 않는다.
- 확장성 – 새로운 기능이나 요구 사항, 기존의 DRM 등을 추가할 수 있을 뿐만 아니라 기존에 제공되던 상호호환성을 보장할 수 있느냐에 따라 분류할 수 있다. 본 표준안에서는 기존 DRM을 새로 추가하기 위해서는 프로파일을 새로 생성하고, 관련 REL 부분을 본 표준안의 REL 에 추가함으로써 가능하다.
- Media, network, device 제약 – Content Media Type, network 환경, device 환경에 대한 제약이 있느냐에 따라 분류할 수 있다. 본 표준안은 현재 모바일 환경 하의 다운로드형 콘텐츠로 국한되어 있지만 본 표준안의 아키텍쳐 상에서 스트리밍 콘텐츠 및 타 디바이스로 확장하는 것은 가능하며 차후 버전에서 고려하고 있다. 또한 MPEG 등 국제 표

준 콘텐츠 포맷 뿐만 아니라 기업의 특정 포맷도 지원 가능하다. Coral의 경우 네트웍에 상당 부분 의존하지만 본 표준안은 오프라인 환경에서도 동작 가능한 것이 특징이다.

- 플레이어의 변경 여부 – 상호 호환성을 제공하기 위해 DRM 기능을 이용하는 랜더링 어플리케이션 혹은 플레이어가 변경되느냐에 따라 분류할 수 있다. 일반적으로 DRM은 기술적으로 플레이어 변경이 전혀 없을 수 없다. 본 표준안에서는 플레이어에서 본 표준안을 쉽게, 적은 비용으로 조기에 적용할 수 있도록 최소한의 어플리케이션 서비스 API 집합 (총 13개임)을 공개하는 특징을 갖고 있다.

다음은 상호호환성 분류를 위한 둘째 기준 및 분석 결과이다:

- Full-format interoperability (DMP, OMA; MS): 가장 손쉽게 상호호환성을 제공하나, 모든 멀티미디어 터미널에 적합한 단 하나의 표준을 정의한다는 것은 쉽지 않은 일이다.
- Configuration-driven interoperability (MPEG 2/4/21): 모든 터미널(어플리케이션 플레이어)이 모든 DRM 툴 들 (인증, 암복호화, 워터마크 등등)에 접근할 수 있다는 가정하에, 콘텐츠를 소비할 때 필요한 툴을 검색 및 다운로드 해서 쓰는 개념이다. 그러나 특정 플랫폼에 특정 툴들만이 적용 가능할 수 있으며, 모든 디바이스들이 (특히 모바일과 같은 소규모 디바이스) 사용자에 의해 소유된 멀티미디어를 접근하는데 요구되는 모든 툴들을 저장하고 실행하기 위한 모든 리소스들을 반드시 갖는다는 것이 불명확하다.
- Translation-driven interoperability (RealNetworks, Coral): 네트웍으로 연결된 TTP(Trusted Third Party)에 의해 서로 다른 DRM 포맷들간에 변환 (translation) 연산을 통해 상호 호환성을 제공한다.

〈 표 4-1〉 상호호환성 분류 기준

	Full Format		Configuration	Networked	Translation		Profile
	DMP	OMA	MPEG 2,4,21	Coral	Real	MS	S-DRM
DRM 콘텐츠 수정 여부	수정		수정	수정, 수정 안함	수정 안함	수정	수정 안함
타 DRM 허용 여부	허용 안함		허용 안함	허용	허용	허용 안함	허용
DRM 자체의 수정 여부	수정 필요		부분적 수정	수정 불필요	수정 불필요	수정 필요	수정 불필요
사용자 인식 여부	–	인식	부분적인식	인식 안함	–	–	인식 안함
DRM 규격의 공개 여부	공개		공개	부분적 공개	–	–	공개
Lossless 변환	–	지원 안함	부분적지원	지원	부분적지원	–	지원
확장성	–	낮음	낮음	높음	–	낮음	높음
Media 제약	있음		있음	없음	없음	–	없음
Device 제약	있음		있음	없음	없음	–	없음
Network 제약	있음		있음	다소 있음	있음	–	없음
플레이어 변경	많음		보통	낮음	낮음	–	낮음

- Networked interoperability (Coral): 네트워크에 연결된 Trusted Third Party 혹은 별도의 시스템을 통해 DRM 자체의 변환이나 사용자 인식 없이 서로 다른 DRM간의 상호 호환성을 제공한다.
- Profile-based interoperability (S-DRM): 본 논문에서 제안한 표준안은 위의 분류 중 어느 것에도 속하지 않는다고 보여 진다. 따라서 별도의 범주로 분류하는 것이 바람직하다고 본다.

본 연구에서는 DRM 상호호환성 측면에서 Coral의 접근 방법을 가장 좋은 역할 모델로 설정하고 연구를 시작하였다. 위 분류 기준을 보면 대부분을 만족시키고 있기 때문이다. 그러나 본 표준안의 분석 결과를 보면 접근 방법은 다르지만 대부분의 상호호환성 기준 측면에서 Coral과 대등하거나 우수하다는 것을 알 수 있다. Coral의 상호호환성 모델은, 중간에서 누군가가 (서버, 네트웍, 또는 단말) 변환 작업을 해주어야 하는데 그 비용이 크며, 상당 부분의 DRM 처리 과정에서 네트웍 접속이 요구된다는 점은 단점이 아닐 수 없다. 또한 Coral의 모델은 기본적으로 상호호환을 제공하고자 하는 기업들 간에 상호 협의 (bilateral agreement)가 선결되어야 가능하다는 측면에서 기술적인 해결책보다는 비즈니스적인 해결책에 가깝다고 보여 진다.

An open issue : How to guarantee a security level among interoperable DRM systems?

어떤 시스템에 상호호환성을 도입한다는 것은 보안 (security) 측면에서 새로운 위험이 될 수 있다. 외부의 DRM 처리 모듈들이 내부 시스템 안으로 들어오고, 보호된 콘텐츠 및 사용권한 정보가 외부로 노출되기 때문이다. 또한 기존의 DRM 시스템에서 요구되는 보안 레벨이 상호호환성이 지원되는 또 다른 외부 DRM 시스템 환경에서 제대로 지켜지는지가 중요한 문제이다. 그러나 지금까지 몇 가지 보안 평가에 관한 방법들 [32, 33, 34] 이 제안되었으나 각각 많은 제약점을 가지고 있으며 DRM 시스템들을 평가하기에는 부족하다. 따라서 DRM 시스템들 및 이들 간의 보호 레벨을 보장할 수 있는 새로운 평가 체계가 필요하다. 이를 위해서는 보호된 콘텐츠가 소비되는 신뢰된 실행 환경(Trusted Execution Environment; 신뢰할 수 있는 컴퓨팅 환경을 구성하는 하드웨어, 소프트웨어, 인프라스트럭쳐를 총칭함)에 대한 인증 절차 (certification process) 및 보호 대상 콘텐츠에 대한 보호 레벨을 지정할 수 있는 콘텐츠 보호 레벨 지정(Content Protection Level Assignment) 메커니즘이 도입될 필요가 있다. 이렇게 함으로써 콘텐츠는 원래 설정된 보호 레벨을 만족시키는 신뢰된 실행 환경에서만 소비되는 것을 보장해야 한다. 이 이슈는 그 자체로서 매우 광범위한 연구를 필요로 하며 본 표준화 장기 로드맵의 의제로서 지속적으로 연구되어야 한다.

Ⅴ. 결론

본 연구에서는 DRM 상호호환성 분야를 중심으로 기존의 표준안 및 기술 개발 현황을 살펴

보았다. 이를 통해 각 기관의 상호호환성에 대한 접근 전략을 분석하고 상호호환성에 대해 보다 더 엄밀한 분류를 제시했다. 본 논문에서 기여하는 부분 중 하나는, 상이한 DRM간 상호호환성을 지원할 수 있는 모바일 DRM 표준안을 제안했다는 점이다. 본 표준안은 프로파일과 도메인이라는 개념을 바탕으로 기존 접근 방법과 전혀 다른 방법으로 상호호환성을 제공한다. 본 표준안은 기본적으로 상호호환성을 제공하면서도 그에 따른 비용이 작고 로열티 프리라는 특성을 갖는다. 본 표준안이 상호호환성 요구 조건을 제대로 만족하는지를 확인하기 위하여 상호호환성 분류 기준을 새로 정의하였으며 이를 바탕으로 기존의 방법들과 비교 분석하여 그 결과를 제시하였다. 표준안의 세부 사항으로 표준안의 목표 및 범위, 요구 사항, 아키텍쳐 및 이 사항들을 지지하는 여러 가지 기술 규격들을 자세히 설명하였으며 주요 이슈들을 논의하였다.

향후에는 본 연구를 바탕으로 실제적으로 국내 표준화 및 국제 표준화를 진행할 예정이다. 이를 위해 국내에서는 본 표준안에 대한 폭넓은 업계 의견 수렴 과정이 진행되어야 한다. 이러한 국내의 활동과 병행하여 GSMA에 본 표준안을 제출하고 기타 다른 국제 표준화 기구들과 협력 모델을 구축하는 등 다각도의 국제 표준화 활동이 필요하다고 사료된다.

Ⅵ. 감사의 글

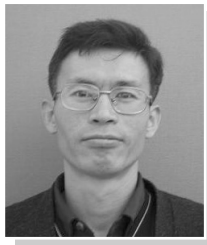
본 논문이 나오기까지 많은 토론과 제안을 해주신 모바일 DRM 표준화 회의 구성원들 -디지캡의 오성흔 박사, 정인성 박사, 유희수 연구소장, 제주대의 좌정우 교수, 제주 DCRC의 김미옥 연구원, 한국전자통신연구원의 이정수 박사에게 감사드린다.

>> 참고문헌

[1] INDICARE (The INformed DIalogue about Consumer Acceptability of DRM Solutions in Europe), "Consumer Survey on Digital Music and DRM", http://www.indicare.org, May 2005.
[2] MPEG LA (Licensing Authority), http://www.mpegla.com.
[3] OMA (Open Mobile Alliance), http://www.openmobilealliance.org.
[4] MPEG-21,http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm.
[5] SDMI (Secure Digital Music Initiative), http://www.sdmi.org.
[6] OeBF(Open eBook Forum), http://www.openebook.org.
[7] DVD Forum, http://www.dvdforum.org.
[8] iDRM (Internet DRM), http://www.idrm.org.
[9] Digital Object Identifier, http://www.doi.org.
[10] OPIMA (Open Platform Initiative for Multimedia Access), http://www.chiariglione.org/leonardo/standards/opima.
[11] CIDF (Content ID Forum), "CIDF Specification 1.0", http://www.cidf.org.
[12] W3C, http://www.w3.org.
[13] ISMA (Internet Streaming Media Alliance), "Encryption and Authentication Specification Version 1.0", http://www.isma.tv.
[14] TV Anytime, http://www.tv-anytime.org.
[15] DLNA (Digital Living Network Alliance),

http://www.dlna.org.
[16] ISO/IEC 14496-1:2001/FDAM 3:2003(E), SC 29/WG11 W5282, Information Technology Coding of audio-visual objects Part1:Systems, AMENDMENT3:Intellectual Property Management and Protection(IPMP), extensions, December 2002.
[17] ISO/IEC 13818-1:2000/FDAM 2:2003(E), SC 29/WG11 W5604, Information Technology Generic coding of moving pictures and associated audio information Part 1: Systems, AMENDMENT 2: Support of IPMP on MPEG-2 systems, April 2003.
[18] ODRL (Open Digital Rights Language), "Open Digital Rights Language v1.1", http://www.odrl.net.
[19] DMP (Digital Media Project), http://www.dmpf.org.
[20] Coral, http://www.coral-interop.org.
[21] Microsoft, http://www.microsoft.com.
[22] RealNetworks, http://www.realnetworks.com.
[23] 황성운, 윤기송, "외국 DRM 기술 지적재산권 회피를 위한 국내 DRM 기술 표준화 전략", 한국표준협회 표준화 우수 논문 공모, 2005. 10.
[24] WIPI (Wireless Internet Platform for Interoperability), http://www.wipi.or.kr.
[25] R. Housely et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), 2002.
[26] Anne-Marie Pecoraro, "Content Owner Security Requirement", Mobile DRM Conference, 2005. 7.
[27] OBEX, IrDA Object Exchange Protocol (OBEX), Version 1.3, January 2003.
[28] MMS, 3GPP TS 23.140 V 6.8.0 :"Multimedia Message Service; Stage 2", 2004. 12.
[29] HTTP, Hypertext Transfer Protocol - HTTP/1.1, RFC 2616, June 1999.
[30] Stefan Bechtold, "The Present and Future of Digital Rights Management - Musings on Emerging Legal Problems", Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer-Verlag, 2003.
[31] XML-RPC, http://www.xmlrpc.com.
[32] OCTAVE, http://www.cert.org/octave/.
[33] Common Criteria for Information Technology Security Evaluation, v1.0, January 1996.
[34] B. Schneier. "Attack Trees", Dr. Dobb's Journal, December 1999.

>> 저자 소개



황성운 (Seong Oun HWANG)
Email: sohwang@etri.re.kr
Tel: +82-42-860-4990
Fax: +82-42-860-6699

1993. 8: 서울대학교 수학과 (학사)
1998. 2: 포항공과대학교 정보통신학과 (석사)
2004. 8: 한국과학기술원 전자전산학과 (박사)
1994.1 ~ 1996.2 : LG-CNS Inc. 소프트웨어 엔지니어
1998.1 ~ 현재 : 한국전자통신연구원 선임연구원
주관심분야 : 정보보호, DRM

윤기송 (Ki Song Yoon)
Email: ksyoon@etri.re.kr
Tel: +82-42-860-4992
Fax: +82-42-860-6699

1984. 2 : 부산대학교 조선공학과 (학사)
1988. 2 : City University of New York 전산학과(석사)
1993. 2 : City University of New York 전산학과(박사)
1993. 3 ~ 현재 : 한국전자통신연구원 책임연구원
주관심분야 : 메시징, 분산처리