모바일 DRM 기술 분석 및 시장 동향

숭실대학교 신용태 · 장의진
디지캡 기술연구소 정인성

1. 서 론

기존 인터넷 및 인트라넷 기반의 e-Business 플랫폼이 모바일과 연계한 유무선 통합 플랫폼으로 확대되면서 무선 콘텐츠의 유통, 소비에 대한 다양한 비즈니스 모델을 수립할 수 있게 되었다. 이로 인하여 기존의 모바일 기기에서 사용하던 콘텐츠 보호 방식은 한계를 나타내고 있다. 예를 들어, 모바일 기기에서 유통, 소비되는 콘텐츠의 중심은 기존 벨소리, 이미지, 저용량 게임등과 같은 Light Media 콘텐츠에서 음악, 영화, 게임, 방송 등의 Rich Media & High-Value 콘텐츠로 이동하고 있다. 무선 망 개방, 와이브로, 홈 네트워크 등의 네트워크 인프라를 통한 모바일 기기의 콘텐츠 획득 및 배포 채널은 다양해지고 적용 범위는 점차 확대되고 있다. 유비쿼터스 시대의 도래로 하나의 모바일 기기에 여러 기능의 융복합, 다양한 콘텐츠 미디어 처리 등이 가능하게 되었다. 이러한 추세가 점차 일반화될 것으로 예측되며 이에 따라 모바일 DRM의 적용에 따른 수익률도 매년 큰 폭으로 증가할 것이다.

모바일 DRM 기술은 OMA(Open Mobile Alliance)[1]와 3GPP(3rd Generation Partnership Project)에 의해 국제 표준이 선도되고 있으며, MS, Sony 등에서도 자체 DRM을 통해 빠르게 시장을 잠식하고 있다. 특히, OMA DRM의 표준 규격을 준수한 모바일 DRM 솔루션들이 여러 업체들에 의해 개발되고 있다. 본 고에서는 모바일 DRM의 개념과 국내외 모바일 DRM의 시장 동향을 살펴보고, OMA에서 정의한 OMA DRM의 특징 및 시스템 구조 등을 살펴본다. 더불어, 모바일 DRM의 당면 과제와 이에 대한 해결 방안 등에 대해서 조망해 본다.

2. 모바일 DRM의 이해

2.1 모바일 DRM이란?

모바일 DRM 시스템은 콘텐츠 제공자, 콘텐츠 서비스업자, 이동통신 사업자와 최종 사용자 등으로 구성되는 무선 디지털 콘텐츠 유통 시장에서 콘텐츠 및 지적 재산권을 보호하고 사용자에게 새로운 구매 서비스를 제공한다. 즉, 원본 디지털 콘텐츠를 암호화하여 권한이 없는 접근에 대해 콘텐츠를 보호하고 유통에 필요한 메타데이터를 도입하여 다양한 콘텐츠 유통 서비스를 가능하게 한다. 또한, 디지털 콘텐츠와 콘텐츠의 사용 권리를 분리하는 개념을 통해 콘텐츠의 사용 권리를 정당하게 구매한 최종 사용자 만이 콘텐츠를 사용할 수 있도록 한다. 이는 콘텐츠 사용 시 판매자가 지정한 규칙에 의해 이용이 가능하다. 디지털 콘텐츠를 최종 사용자에게 전달하기 이전에 콘텐츠 관련 거래에 대한 다수의 권리 보유자가 존재할 수 있다. 모바일 DRM 시스템은 이들 간의 신뢰성 있는 온라인 거래가 가능하도록 지원한다.

2.2 주요 기능

모바일 DRM 시스템은 그림 1에서 보는 바와 같이 DRM Server와 모바일 기기에 탑재되는 DRM Client로 구분된다. DRM Server는 Content Packager와 Rights Issuer, DRM Client는 DRM Agent를 포함한다. DRM Server는 DRM Client와의 통신을 통해 Rights Issuer 등록 및 재등록, Domain 가입과 탈퇴 그리고 1)사용 권리 정보 획득 처리 등의 다양한 서비스를 위한 요구를 처리하며, DRM Content 제공 기능을 담당한다. DRM Client는 모바일 기기에 내장되어 인터넷 혹은 CDMA 망을 통해 보호된 콘텐츠와 사용 권리 정보를 요청한다. PC, Handset, PDA 등의 유, 무선 통신이 가능한 기기 중에서 성능이 뛰어난 PC에 탑재된 DRM Client는 모든 단말의 허브 역할을 하기도 한다. DRM에서 다루는 콘텐츠가 대용량화 추세에 있으므로 대부분의 사용자는 PC를 통해서 암호화된 콘텐츠를 획득한 후, 이를 여러 종류의 모바일 기기로 전달하여 소비하는 시나리오가 가능할 수 있다. 아마도 무선 인터넷의 통신비용이 현재의 인터넷 수준에 버금갈 때까지는

1) 권리 정보는 OMA DRM V2.0의 Rights Object, MS WMRM의 License와 같은 형태를 갖는다.

이와 같은 서비스가 보편화될 것으로 예측된다. 즉, PC는 타 단말에 비하여 높은 대역폭의 네트워크에 연결되어 있고, 대용량의 저장 공간을 가지고 있으며, 처리 성능도 우수하다는 특성을 갖기 때문이다. 모바일 DRM 시스템의 구성요소 별 기능은 다음과 같다.

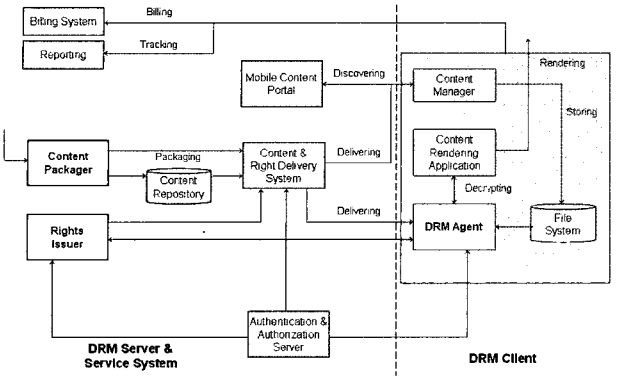

그림 2 모바일 DRM 시스템의 구성

- Content Packager
  - 원본 콘텐츠를 DRM 포맷으로 패키징하는 기능
  - 패키징 정보를 DRM Server로 전송 및 등록하는 기능
  - 네트워크 운영자를 위한 서비스 정책의 수신 기능
- Rights Issuer
  - 콘텐츠의 구입 내역과 Usage Rule을 명시하는 권리 정보의 발급 기능
  - 기기 등록과 관리 기능
  - 권리 정보 발급과 관리 기능
  - 도메인 관리 기능
- DRM Agent
  - DRM Agent를 위한 전체 절차의 제어 및 관리 기능
  - DRM 서비스를 위한 초기 환경 설정 기능
  - DRM Agent 정보 제공 기능
  - DRM Agent 관리 기능
  - 플랫폼에 종속된 기능 제어

2.3 CAS와 DRM의 차이

CAS(Conditional Access System)와 DRM은 기본적으로 디지털 콘텐츠의 기밀성 보호와 콘텐츠의 사용 제어라는 목적을 추구하는 측면에서는 유사한 기술이다. 그러나 Persistent Protection이라는 기술적인 측면에서는 차이가 있다. CAS는 디지털 방송 콘텐츠의 기밀성을 보호하고 시청 자격을 가진 가입자(Parental Rating, Blockout Limits, 구매 여부 등)만이 구입한 프로그램/채널을 제어 방식(Expire Date, One-Time 등)에 의해 시청할 수 있도록 한다. DRM은 디지털 콘텐츠의 기밀성을 보호하고 콘텐츠 제공업체나 서비스 제공업체가 정의한 사용 방안을 기술한 권리를 구매함으로써 콘텐츠의 사용을 제어한다. 보호 대상의 관점에서는 CAS는 프로그램(콘텐츠)과 채널을 보호하지만 DRM은 콘텐츠만을 대상으로 한다. CAS와 DRM의 주요 기능 및 차이점은 표 1과 같다.

표 1 CAS와 DRM의 비교

	CAS	DRM
주요기능	▪ 콘텐츠의 기밀성 제공 ▪ 콘텐츠의 사용 제어 기능 ▪ 사용 권한 정보(EMM[2]) 생성·전달 기능 ▪ 가입자 및 서비스 관리 기능 ▪ 스마트카드 발급 기능	▪ 콘텐츠의 기밀성 제공 ▪ 콘텐츠의 사용 제어 기능 ▪ 사용 권한 정보 생성·전달 기능 ▪ Consumer 및 Right Offer 관리 기능 ▪ DRM Certificate 발급 기능 ▪ 저장된 콘텐츠 보호 및 재배포 지원 ▪ Right 선물, 양도 등의 Right 전송 기능 지원
차이점	▪ 콘텐츠의 스크램블링은 콘텐츠 송출 시 Real-time 방식으로 이루어짐 ▪ 저장되는 콘텐츠에 대한 기밀성 보호 기능을 제공하지 않음 ▪ 한 채널 및 프로그램 내에서도 콘텐츠의 암호화 키는 지속적으로 갱신 가능 ▪ 암호화된 콘텐츠의 암호화 키는 Scrambled Content와 함께 ECM[3]의 형태로 송출 및 전송	▪ 콘텐츠 암호화는 Pre-Packaging 및 Real-Time 방식으로 처리 ▪ Persistent Protection 개념을 제공하여 서비스 채널에 대한 보호 및 저장된 콘텐츠에 대한 기밀성 제공 ▪ 하나의 콘텐츠 암호화를 위해 사용되는 암호화 키는 오직 한 개 ▪ 콘텐츠 암호화 키는 사용 권한 정보에 포함되어 전달

2.4 인터넷 DRM과 모바일 DRM의 차이

유선과 무선 네트워크를 통합하는 유비쿼터스 시대의 도래로 어느 곳에서나 무선 인터넷이 가능해지고 유선과 무선의 경계가 사라지면서 콘텐츠 서비스도 새로운 전환하기를 맞고 있다. 무선 망 개방과 WiBro와 같은 무선랜 인프라로 모바일 콘텐츠 배포 채널이 다양해지고 있으며, 모바일 컨버전스를 통해 여러 IT 제품의 기능이 사용자가 친숙한 하나의 모바일 디바이스에 융·복합되는 추세가 일반화 되고 있다. DMB 폰, 게임 폰, 스마트폰, PMP(Portable Media Player)와 PDA가 그 좋은 예가 될 수 있다. 즉, 기본 유선 인터넷 망에 적용되

2) Entitlement Control Message 즉, 프로그램자격제어메시지로 CW(Control Word)와 채널별 수신 자격 전송 기능을 담당한다.
3) Entitlement Management Message 즉, 시청자격관리메시지로 ECM의 스크램블 키와 가입자별 시청 자격 전송 기능을 담당한다.

어 온 DRM 기술은 무선 인터넷 망으로 그 범위가 급속하게 확대되어 가고 있으며, DRM 적용을 위한 구성요소의 특징에서도 그 차이를 보인다. 표 2는 인터넷 DRM과 모바일 DRM의 비교를 나타낸다.

표 2 인터넷 DRM과 모바일 DRM의 비교

	인터넷 DRM	모바일 DRM
콘텐츠타입	• 영화, 음악, 기밀문서, 기업 문서와 같은 Rich Media & High-Value 콘텐츠가 주류	• Light Media 콘텐츠가 주류이나 최근 영화, 음악, 방송, 게임과 같은 Rich Media 콘텐츠가 점차 대두
서비스제공업체	• Value Chain에서 상대적으로 적은 역할 담당	• 인터넷 SP에 비해 보다 다양하고 안정적인 서비스 제공 • Value Chain에서 보다 큰 역할 담당
기기	• 파일 포맷 및 렌더링 어플리케이션에 종속적인 DRM 시스템이 주류 • 충분한 컴퓨팅 자원 (예. 대역폭, 메모리, 저장 공간) • 필요한 S/W의 자유로운 업그레이드 및 패치 가능 • 주류 OS 존재	• 파일 포맷 및 렌더링 어플리케이션에 독립적인 DRM 시스템 (Proprietary DRM with OMA DRM) • 부족한 컴퓨팅 자원 • OS의 영향으로 S/W의 업그레이드 및 패치에 있어서의 제약 • OS 및 Platform 종속적 성향
사용자	• 대다수의 PC 사용자는 콘텐츠가 공짜라는 의식이 강함 • DRM 적용에 따른 거부감이 강함	• 벨소리 등을 중심으로 콘텐츠 유료화에 대한 거부감이 적음. 2001년 기준 벨소리, 이미지의 판매액이 PC용 유료 콘텐츠 판매액의 2배가 넘음
표준화	• MS WMRM과 같은 Proprietary DRM을 기반으로 De facto Standard가 주류	• OMA DRM과 같은 De jure Standard가 주류이나 Proprietary DRM의 영향력이 점차 높아짐 (MS WMRM, Apple Fairplay, etc)

3. 모바일 DRM 산업 동향

3.1 시장 동향

모바일 DRM의 시장 규모는 모바일 기기의 시장과 비교 했을 때 아직 진입기에 있다고 볼 수 있다. 사용자의 요구와 서비스를 만족하는 다양한 종류의 모바일 기기가 보급되고 유통 가능한 콘텐츠의 종류도 지금보다 대폭 늘어남과 동시에 모바일 기기 중심의 유통 채널도 넓어지는 시점에서 모바일 DRM의 시장 규모 역시 확대될 것으로 예상되며, 이미 그와 같은 현상이 여러 곳에서 발견되고 있다.

Digital Tech Consulting[6]에서 발표한 2005년 모바일 DRM 자료에 따르면, 전체 콘텐츠 보호 기술 시장이 2004년 약 7억불에서 2009년에는 그 3배에 해당하는 약 20억불에 다다를 것으로 예상했다. 이 중에서 모바일 DRM 시장은 2004년 약 2억불 규모에서 2009년경에는 약 5억불 규모로 증가할 것이라고 내다 봤다. 이를 뒷받침하는 가장 큰 이유로 핸드폰과 같은 모바일 기기의 모바일 DRM 채택이 보편화될 것이라는 점을 들 수 있다. 이미 여러 모바일 DRM 전문 업체들은 모바일 DRM 솔루션을 개발하여 이동통신사, 단말제조사, 플랫폼 제공업체와 함께 모바일 DRM의 탑재에 박차를 가하고 있다.

특히, DRM을 탑재한 모바일 기기는 2004년 전체 모바일 기기의 약 10%에서 2009년에는 약 40%까지 증가할 것이며, 모바일 DRM의 판매 수는 약 2천만 개에서 3억 개로 크게 증가할 것으로 예측하고 있다. 모바일 DRM의 판매수가 급격히 늘어나는 이유는 최근 진행되고 있는 모바일 환경에서의 다양한 서비스와 연관된다고 볼 수 있다.

3.2 기술 동향

일반적으로 DRM은 Enterprise DRM과 Content DRM으로 구분할 수 있다. 현재 모바일 DRM은 모바일 기기에서 유통, 소비되는 콘텐츠 중심의 Content DRM이 크게 활성화되고 있다. 모바일 기기에서 유통, 소비되는 콘텐츠의 종류는 벨소리, 이미지뿐만 아니라, 음악, 영화, 게임, 방송 등으로 확산되고 있는 주체이다. 기존의 벨소리, 이미지 등과 같은 Light Media 콘텐츠는 콘텐츠 및 저작권 보호 이슈가 상대적으로 적었기 때문에 모바일 기기의 플랫폼이나 정책적인 수준에서 콘텐츠의 불법 복사를 막는 수준의 DRM 기술들이 주류를 이루었다. 즉, 높은 보안성을 만족하는 구조, 다양한 사용 제어가 가능한 DRM 적용에 대한 필요성이 적었으며, 오히려 그러한 DRM의 적용은 막 시작된 모바일 콘텐츠 유통 시장의 활성화에 걸림돌이 될 뿐이었다. 콘텐츠를 암호화하여 다른 사용자들이 사용할 수 없도록 보호하거나 콘텐츠에 일반 사용자가 불법적으로 접근할 수 없도록 단말제조사가 지정한 임의의 공간에 저장하여 접근을 제어하는 수준의 기술로도 충분하였다. 모바일 기기의 낮은 처리 속도, 작은 메모리, 플랫폼 기능상의 제약도 큰 영향을 주었다.

하지만, 최근 보편화되고 있는 음악, 영화, 게임과 같은 고품질, 고비용, 고용량의 콘텐츠는 기존의 방식으로는 콘텐츠 저작권 보호에 한계가 있다. 단순한 콘텐츠 보호뿐만 아니라, 사용자의 요구(Needs)에 맞는 비즈

니스 모델의 필요성, 콘텐츠 사용 제어의 다양화, 모바일 기기에서 콘텐츠 유통 채널의 다변화, 콘텐츠 유통에 대한 사후 관리, 모바일 기기의 Open OS 탑재의 증가로 인한 사용자 접근의 용이성, 높은 사양을 가진 모바일 기기의 등장 등은 다양하고 복잡한 모바일 DRM 기술을 요구한다. 또한, Rich Media 콘텐츠 기반의 서비스는 단일 형태의 DRM으로 각 서비스의 모든 요구 사항을 수용하기도 어렵다. 예를 들어, 게임과 같은 실행 가능한 형태의 콘텐츠와 음악, 영화와 같은 실행 불가능한 형태의 콘텐츠에 대한 DRM 요구 사항이 동일할 수는 없다. 또한, 채널 보호 중심의 방송 서비스와 콘텐츠 보호 중심의 음악 서비스를 동일한 모바일 DRM으로 적용하기에는 무리가 있다.

최근 모바일 DRM은 기존 PC 중심의 인터넷 DRM에서 채택했던 인증서 중심의 사용자 및 장치 인증, 재배포 가능한 구조, 워터마킹 적용과 같은 사후 추적 기술의 적용, 높은 수준의 암호화, 복잡한 키 관리 구조, Tamper-Resistance 기술 적용, 온라인 자동 패치 및 업그레이드 기술, 개인 정보 보호 기술 등의 활용이 보편화되고 있는 추세에 있다. 더불어, 모바일 기기가 점차 다양한 미디어를 한꺼번에 처리할 수 있는 융·복합화 추세가 가속화 될 경우, 여러 콘텐츠 제공자가 제공하는 다양한 형태의 미디어를 하나의 모바일 DRM 프레임워크 안에서 최소한의 확장을 통해 DRM 아키텍처를 구성하는 것이 무엇보다 중요시 되고 있다.

3.3 표준화 동향

모바일 DRM의 표준화는 국제 무선 인터넷 표준화 기구인 OMA가 주도하는 OMA DRM이 선도적인 위치를 차지하고 있다. OMA는 2002년 6월 발족된 표준화 기구로써 무선 인터넷 환경에서 단말간의 상호운영성 확보를 목적으로 IETF, 3GPP, 3GPP2, W3C, ITU-T 등과 협력하여 활발하게 표준화 작업을 진행 중에 있다. OMA DRM은 3GPP에서 DRM을 위한 시스템의 기능 및 요구사항을 정리하여 작업을 수행한 후, OMA와 3GPP간의 합의에 따라 DRM 규격 제정을 OMA에 이관하였고 현재에도 OMA에서 표준화를 추진 중에 있다.

OMA DRM V1.0은 2004년 6월 25일경에 정식 승인 규격(Approved Enabler)이 발표되었다. OMA DRM V1.0에는 DRM을 패키징하기 위한 DRM 콘텐츠 포맷, 권리 및 사용 제어를 위한 권리 명세, 서버로부터 단말까지 정보 전달을 위한 다운로드 아키텍처와 전체 DRM 아키텍처를 명시한 DRM 규격으로 구성되어 있다. OMA DRM V1.0의 가장 큰 특징은 시장의 빠른 시장 진입과 선점을 위해 단말에서 필요한 최소한의 요구 사항과 네트워크 자원 소모의 최소화에 부합하는 것을 목표로 했다는 점이다. 이로 인해 키 관리 및 키 전달에 관한 보안성이 상당히 취약했으며, 단말 위주로 기술되어 모호한 부분이 많은 DRM 구조를 갖게 되었다.

OMA DLDRM 워킹 그룹은 위와 같은 문제점을 직시하고 곧바로 OMA DRM V2.0 규격 정의를 진행하였다. 이를 통해 2004년 12월 7일 OMA DRM V2.0 Candidate Enabler 규격을 발표하였다. 본 규격은 기존의 V1.0에서 문제시 되었던 보안성 강화를 위해 PKI 구조에 기반하여 키 관리, 단말 및 사용자 인증, 권리 개체 획득 프로토콜을 정의하였으며, 다양한 비즈니스 모델의 구현이 가능하도록 다운로드뿐만 아니라 스트리밍을 위한 DRM 콘텐츠 포맷도 정의하였다. 현재에는 Candidate Enabler의 수정을 위해 제출되는 CR (Change Request)을 토대로 일부 내용을 수정하는 작업을 계속 진행 중에 있다.

국내에서는 아직까지 공개된 모바일 DRM의 표준화 내용은 없으나, 단말제조사, 이동통신사, DRM 솔루션 업체 등을 중심으로 OMA DRM의 표준화에 빠르게 대처하고 있으며, 조만간 국내 무선 인터넷 표준 플랫폼인 WIPI에 기반한 모바일 DRM 표준화 등이 가시화 될 것으로 예상되고 있다.

4. OMA DRM

4.1 주요 특징

OMA DRM에서 콘텐츠 제공자는 DRM 콘텐츠 사용에 대한 규칙을 정의할 수 있다. 즉, OMA DRM 도입 이전에는 단일 가격 정책으로 콘텐츠를 판매할 수밖에 없었지만 도입 이후에는 동일한 콘텐츠에 다양한 사용 권리 조건을 명시함으로써 다수의 가격 정책으로 콘텐츠를 판매할 수 있다. 또한 더 이상 콘텐츠에 가치를 두지 않고 콘텐츠의 사용 권리에 가치를 두며 콘텐츠 자체에 대한 판매가 아닌 사용 권리를 판매하는 것이 가능하다.

OMA DRM V1.0 규격은 DRM 규격, DRM 콘텐츠 포맷, 권리 명세, 다운로드 아키텍처에 관한 표준을 명시하며, OMA DRM V2.0 규격은 DRM 아키텍처, DRM 요구사항 정의, DRM 규격, DRM 콘텐츠 포맷, 권리 명세에 관한 표준을 명시하고 있다. OMA DRM V2.0 규격 중 OMA DRM Requirements V2.0은 OMA 내에서 지속적인 DRM 규격의 Release를 위한 비즈니스 요구사항을 정의하며, DRM Architecture V2.0은 DRM 환경에서의 Actor, 기능적인 아키텍처, Trust/Security Model과 몇 가지 Use Case를 포함한다. DRM Specification V2.0은 모바일 환경에서

DRM을 구현하기 위해 필요한 ROAP[4](Rights Object Acquisition Protocol), Domain, 키 관리와 같은 프로토콜, 메시지 포맷 및 매커니즘을 정의하며, DRM Content Format V2.0은 DRM Protected Media와 관련된 메타데이터를 위한 DRM Content Format을 정의한다.

OMA DRM V1.0은 Light media 콘텐츠를 대상으로 하여 빠른 시장 진입이 가능하였으며, Wireless와 모바일에서의 네트워크, 디바이스 등의 여러 제약사항을 고려하여 부담을 최소화 하였다. 또한, Wireless와 모바일의 종속적인 기술을 활용하여 기존 환경에서의 변화를 최소화 하였다. OMA DRM V2.0은 Rich media 콘텐츠를 대상으로 하였으며, OMA DRM V1.0이 가지는 보안 측면에서의 취약점을 고려하여 PKI를 기반으로 한 Trust mechanism을 적용하였다. 따라서 키 관리와 ROAP 기반의 디바이스 등록, RO[5](Rights Object) 획득, Domain 가입 기능을 가능하게 한다. OMA DRM V2.0의 특징 및 기능은 다음과 같다.

- Discrete media(벨소리, 어플리케이션, 이미지 등)와 Continuous(Packetized) media (오디오와 비디오)의 보호
- Silent와 In-advanced 방식의 Rights 다운로드
- 콘텐츠 암호화를 위한 CEK(Content Encryption Key)의 기밀성 보장 및 Content와 Rights의 무결성 보장
- ROAP와의 통신을 통한 Rights 획득 및 처리
- DRM Agent에 RO를 바인딩 함으로써 Domain내에서 DRM Content를 공유할 수 있는 Device Domain 기능
- Contents와 Rights의 백업
- DRM Server 혹은 SIM(Subscriber Identity Module)/로컬 디바이스로부터 Content와 Right의 복구
- Consumer에 의한 콘텐츠 생성 및 보호 그리고 Consumer가 지정하는 특정인들과의 공유 가능
- 타 DRM 시스템/Secure External Memory로의 Content/Rights Export 가능
- 하나의 Rights로 다수개의 콘텐츠 사용 가능
- Rights를 상속할 수 있는 Rights Inheritance 기능으로 하나의 Parent RO가 있을 경우 그에 속한 Constraint나 Permission 등을 Child RO가 상속 가능

4) 디바이스가 Rights Issuer로부터 RO의 요청 및 획득을 가능하게 해주는 프로토콜이다.

5) Rights Document(XML)의 인스턴스를 지칭하며, DRM 콘텐츠의 권리 및 소비 규칙을 명시한다.

4.2 시스템 구조

그림 2는 OMA DRM 시스템의 기능적인 아키텍처를 나타내며, DRM Agent, Content Issuer, Rights Issuer, User와 Off-device Storage로 구성된다.

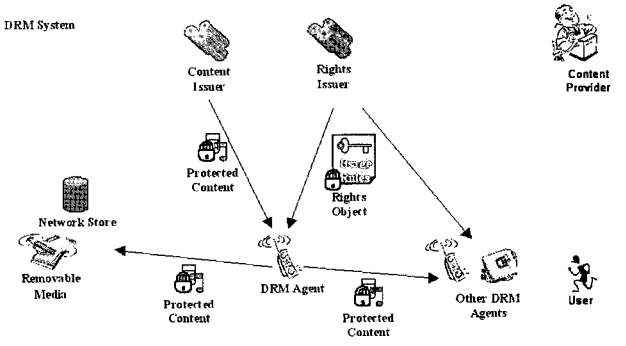

그림 3 기능적인 아키텍처

DRM Agent는 DRM Content와 관련된 Permission과 Constraint를 시행하며, DRM Content에 대한 접근을 제어한다. Content Issuer는 DRM Content를 전달하는 개체로서 OMA DRM은 DRM Agent에 전달되는 DRM Content의 포맷과 DRM Content가 서로 다른 전송 매커니즘을 사용하여 Con- tent Issuer에서 DRM Agent로 전달되는 방식을 정의한다. 또한, DRM Content의 패키징을 수행할 수 있으며, 다른 소스로부터 Pre-packaging된 콘텐츠를 받을 수 있다. Rights Issuer는 DRM Content에 Permis- sion과 Constraint를 부여하고 RO를 생성한다. RO는 DRM Content가 어떻게 사용되는지를 결정한다. User는 DRM Content의 사용자로서, 사용자는 DRM Agent를 통해서 DRM Content에 접근할 수 있다. DRM Content는 본질적으로 안전하며 네트워크 저장소나 PC 등과 같은 사용자의 off-device에 저장될 수 있고 백업 목적으로 사용될 수 있다. Stateless Per- mission을 포함하는 RO는 Off-device에 저장될 수 있다.

4.3 Use Case

OMA DRM V2.0은 융통성 있게 설계되었으며 다양한 비즈니스와 사용 모델을 지원한다. 이 절에서는 여러 가지 기술적인 Use Case를 서술하며 각각의 Use Case는 다음과 같이 요약될 수 있다.

- **Basic Pull Model**

OMA OTA Download 매커니즘을 적용한 모델로서 클라이언트는 브라우저를 띄우고 Content Issuer의 포탈에 접속하여 콘텐츠 다운로드를 위해 원하는 콘텐츠를 선택한다. DRM Content가 다운로드 되면 클라이언트는 Rights Issuer의 포탈에 접속하고 ROAP를 통해

Rights를 획득 할 수 있다.

• DRM Content의 Push

Content Push와 Push-initiated Pull로 구분된다. Content Push에서 Content Issuer는 User와 특정 Agent를 사전에 알고 있어야 하며, Push-initiated Pull은 Content의 위치 정보를 갖는 링크를 전송할 수 있다.

• DRM Content의 Streaming

Content는 패킷화 되어 스트림으로 전달될 수 있으며, CEK를 포함한 RO를 통해서만 암호화된 스트림에 접근할 수 있다.

• Domain

DRM Agent 집단에 RO를 바인딩 할 수 있으며 Domain내에서는 DRM Content가 공유될 수 있다.

• Backup

DRM Content와 Stateless RO는 백업을 위해 타 장치에 저장할 수 있다. 단, Stateful RO는 백업할 수 없다.

• Super Distribution

DRM Content는 다른 DRM Agent나 장치로 Copy 혹은 Move 될 수 있다.

• Export

DRM Content는 Rights Issuer가 정한 타 DRM 시스템이나 장치로 Export가 가능하다.

• Unconnected Device Support

네트워크에 연결할 수 없는 디바이스도 동일한 Domain의 다른 디바이스를 통하여 DRM Content와 RO를 다운로드 한다. DRM Agent는 Domain RO를 DCF[6](DRM Content Format)에 포함하여 전송할 수 있다.

5. 모바일 DRM 당면 과제

5.1 모바일 DRM Interoperability

상호호환성은 비단 모바일 DRM만의 문제는 아니다. 상호호환성 문제는 유·무선 DRM 시장의 성장 및 콘텐츠 유통 시장의 활성화를 위해서 반드시 해결되어야 할 과제이다. 상호호환성을 해결하기 위한 다각적인 노력이 진행되고 있는 것은 사실이지만, 어떤 방법이 올바른 방법인지는 현재로서 알 수 없다. 상호 호환성을 만족하기 위한 가장 이상적인 방안은 단일 DRM 표준안을 선정하여 이에 따르는 방식이다. 모바일 DRM은 무선 인터넷 환경의 상호 호환성 확보를 위한 표준화 단체인 OMA의 OMA DRM을 바탕으로 이를 강력하게 추진하고 있다. 하지만, DRM은 One-DRM-Does-Not-Fit-All 속성을 가지고 있다. 아무리 잘 정의된 모바일 DRM 표준이라 하더라도 콘텐츠, 서비스, 플랫폼, 단말 환경을 모두 만족시키기는 쉽지 않다. 또한, 모바일 기기의 콘텐츠 유통 채널이 무선에서 유·무선 통합 환경으로 빠르게 발전하고 있는 현시점에서 단순히 무선 콘텐츠만을 위한 DRM 표준안에 따르더라도 사용자 입장에서의 상호호환성은 만족시킬 수 없다. 사용자 입장에서의 상호호환성은 사용자의 모바일 기기가 어떤 DRM을 탑재해도 자신이 구매한 콘텐츠를 재생, 소비할 수 있어야 하기 때문이다.

상호호환성 문제의 해결을 위하여 지나치게 장기적인 해결책만을 고민해서는 안된다. 이미 DRM은 콘텐츠 유통을 위한 필수 요소로 자리매김 하였으므로 단·중·장기적인 관점에서 요구에 부합하도록 해결 방안들이 모색되어야 한다. 현재 이러한 상호 호환성 문제의 해결을 위해서 Coral 컨소시움[2], DMP의 Interoperable DRM Platform[3], Opera 시스템, Realnetworks의 Harmony[4] 등 여러 업체와 단체에서 다양한 방식의 시도들이 진행 중에 있다.

5.2 모바일 DRM Persistence 제공 및 사후 관리

DRM은 Persistent Protection 기술이다. 사용자가 콘텐츠를 최종 소비하는 시점까지 콘텐츠 및 저작권 보호가 요구된다. 즉, 특정 콘텐츠에 한번 바인딩된 권리 정보는 어떠한 경우에도 변경되어서는 안된다. 이를 위해서는 해당 콘텐츠에 대한 유일한 식별자를 할당할 수 있어야 한다. 또한, 워터마킹, 핑거프린팅, Tamper Resistance 기술 등이 적절히 도입되어야 한다. 하지만, 모바일 기기에 이러한 기술들을 적용하는 것은 결코 쉽지 않은 일이다. 따라서 효율성은 높고 기술적 복잡성과 자원 소모는 낮은 모바일 DRM Persistence 모델에 대한 연구가 요구된다. 더불어 사후 처리 기술도 필수적이다. 사후 처리라 함은 콘텐츠가 배포된 후 어떻게 안전하게 유통되고 있는지를 판단할 수 있는 기술이다. 이를 위해서는 DRM 추적, 미터링 기술들이 수반되어야 한다. Persistent Protection이 깨졌을 경우를 이에 대한 증거 수집에 도움을 주기 위한 Digital Forensic 시스템과의 연동도 이루어져야 한다. 또한, 모바일 DRM Revocation, Exclusion, Renewability와 같은 패치 및 업그레이드 기술도 강화되어야 한다.

5.3 모바일 DRM Adaptability

모바일 기기를 통한 콘텐츠 유통에서 콘텐츠 소비의

6) 암호화된 콘텐츠를 위한 Secure Content Package로서 Content Description, Rights Issuer URL 등의 정보를 가진다.

질적 보장을 위한 모바일 DRM 기술의 개발은 향후 콘텐츠 유통 활성에 큰 영향을 미칠 수 있다. 모바일 DRM의 속성상 콘텐츠가 재배포되는 과정에서 각 모바일 기기에 맞는 최적의 콘텐츠 소비가 어렵게 된다. 이를 해결하기 위해서 모바일 기기나 네트워크에 따라 Content Adaptation이나 콘텐츠 타입, 콘텐츠 유통 경로에 따른 Rights Adaptation 문제를 해결해야 한다.

5.4 증가하는 모바일 DRM 성능 및 보안 요구 사항

서두에서 살펴본 바와 같이 모바일 기기에서 재생·소비되는 콘텐츠 타입이 다양해지고 고품질, 고비용, 고용량화 될수록 모바일 DRM에 대한 성능 및 보안 요구 사항은 높아질 것이다. 즉, 콘텐츠, 서비스, 플랫폼에 따른 차등화된 보안 요구 사항의 만족, 복잡한 키 관리 지원, 콘텐츠의 실시간 렌더링을 위한 실시간 복호화 기술, 단말 환경에 맞춘 XML 기술, Light-weight Stream Cipher 및 PKI 개발, 그룹 통신을 위한 암호화 알고리즘의 개발은 향후 모바일 DRM을 위해 개발되어야 할 보안 이슈들이다. 더불어, 콘텐츠 플레이어의 인증, Tamper Resistant Memory, Tamper Resistant Execution Environment, Secure Clock, Secure Storage 기술 등에 기반한 모바일 DRM 아키텍처의 개발이 요구된다.

5.5 모바일 DRM 특허 분쟁

2004년에 MPEG LA는 DRM 원천 특허 보유자들로부터 원천 특허를 취합하여 DRM 특허 포트폴리오를 구성하고 DRM Reference Model을 발표하였다. 최근에 발표된 DRM Reference Model V3.0에는 인터넷 뮤직 서비스, OMA DRM V1.0, OMA DRM V2.0에 관한 특허 적용까지 포함되어 있다. MPEG LA는 원천 특허 보유자들로부터 특허 포트폴리오를 구성하고 특허 이용자가 라이센스를 One-stop 방식의 단일 라이센스를 취득할 수 있는 서비스를 제공하는 단체이다. 이들은 최근 발표된 DRM 뿐만 아니라, MPEG-2, IEEE 1384, DVB-T, MPEG-4 Visual(Part 2), MPEG-4 System, AVC/H.264 등 다양한 기술에 대한 특허 포트폴리오를 운영 중에 있다.

MPEG LA는 발표한 DRM Reference Model에 기반하여 OMA DRM V1.0을 적용한 단말제조사에게는 단말당 0.65불, 서비스 제공업체에게는 1년마다 사용자당 0.25불의 로열티 비용을 요구하고 있다. 이에 OMA의 상위 기관인 GSMA에서는 즉각적으로 비용이 너무 비싸고 현실적으로 적용하기에 적합하지 않다는 입장을 표명하였다. 하지만, 이에 대한 뚜렷한 대응 방안이 없는 실정이다. 이는 비단 OMA DRM에 국한된 문제는 아니다. MPEG LA의 DRM Reference Model에 따르면 현재 운영되는 대부분의 유무선 DRM은 거의 벗어날 수 없는 수준의 광범위한 특허 포트폴리오를 구축해 놓은 상태이기 때문이다. 따라서 정부를 포함한 산, 학, 연이 합심하여 대응책을 마련해야 할 상황이라고 판단된다.

6. 결 론

DMB 폰, 게임 폰, 스마트 폰, PMP, PDA 등으로 대표되는 모바일 디바이스의 성능 향상과 콘텐츠 유통을 위한 기반 네트워크 망의 빠른 진보로 모바일 환경에 적용될 모바일 DRM 기술 개발에 대한 수요는 점차 증가하고 있다. 기술적인 측면에서는 모바일 네트워크의 대역폭과 모바일 디바이스의 CPU 성능 및 메모리 제한을 고려한 DRM 기술의 소형화 및 경량화 노력이 지속적으로 요구되며, 콘텐츠를 제공하는 콘텐츠 제공자나 서비스 제공자 측면에서는 콘텐츠의 불법복제와 저작권 침해로 인한 비용 손실을 사전에 방지하기 위한 모바일 DRM 기술이 필수적이다.

OMA를 통한 모바일 DRM의 표준화 작업은 현재 2.0 버전까지 진행된 상태이며 이는 V1.0에서 문제시되었던 보안성 강화를 위해 PKI 구조에 기반하여 키 관리, 단말 및 사용자 인증, ROAP 프로토콜 등을 추가로 정의하였다.

향후 모바일 DRM이 기술경쟁력과 상호운영성을 확보하기 위해서는 기술개발활동과 국제표준화 활동을 병행하여 기술개발에 필요한 정보를 습득하고, 이를 바탕으로 우리나라의 DRM 기술이 국제 표준으로 채택되도록 함으로써 세계 시장에서 우위를 확보해 나아가야 한다. 즉, 모바일 DRM 기술에 대한 IPR 보유와 외국의 기술사용에 대한 특허 분쟁 및 라이센스 비용 지불로부터 자유로워질 수 있도록 정부를 포함한 산, 학, 연이 합심하여 대응책을 모색해야 할 것이다.

참고문헌

[1] Open Mobile Alliance, http://www.openmobilelliance. org.

[2] Coral Consortium, http://www.coral-interop. org.

[3] Digital Media Project, http://www.dmpf.org.

[4] RealNetworks, http://www.realnetworks. com.

[5] IT Forum Korea 2005 초청강연 및 포럼 튜토리얼 자료집.

[6] Myra Moore, "Global Market for Digital Content Protection Technologies To Explode," Digital Digest Journal, 2005.

신 용 태

한양대학교 산업공학과(학사)
Univ. of Iowa 전산학과(석사)
Univ. of Iowa 전산학과(박사)
Michigan State Univ. 전산학과 객원교수
현재 숭실대학교 컴퓨터학과 부교수
KRNET 프로그램 위원/부위원장
개방형통신연구회(OSIA) 이사
현재 한국정보과학회 학회지편집 부위원장
관심분야 : DRM, 멀티캐스트, 실시간통신, 이동 인터넷, 전자상거래
E-mail : shin@comp.ssu.ac.kr

정 인 성

숭실대학교 소프트웨어공과(학사)
숭실대학교 대학원 컴퓨터학과(석사)
숭실대학교 대학원 컴퓨터학과(박사)
현재 (주)디지캡 기술연구소 과장
관심분야 : 콘텐츠 DRM, Mobile DRM, 인터넷 프로토콜, 인터넷 보안, 멀티캐스트
E-mail : dormouse@digicaps.com

장 의 진

숭실대학교 컴퓨터학과(학사)
숭실대학교 컴퓨터학과(석사)
현재 숭실대학교 컴퓨터학과 박사과정
현재 (주)디지캡 기술연구소 선임연구원
관심분야 : DRM, 멀티캐스트, RFID, 인터넷보안
E-mail : neon@digicaps.com