OMA 표준화 동향
- OMA DRM

LG전자 이동통신기술연구소 **이 승 제**

OMA 표준화 동향

1. OMA DRM 탄생 배경

이동통신 산업이 급속도로 발전하고 휴대용 단말기 보급률이 계속해서 높아짐에 따라 벨소리, 바탕화면, 음악파일, 자바 응용프로그램 등 콘텐츠의 다운로드 횟수도 계속 증가하였다. 초기 휴대용 단말기들은 이들 콘텐츠를 받기만 하고 타 기기로 내보내기가 불가능했기 때문에 콘텐츠의 복사방지에는 관심이 없었다. 그러나 콘텐츠의 다운로드가 곧바로 수익으로 연결되고 휴대용 단말기가 외부장치와 통신하는 기술이 발달함에 따라 자연히 이동통신사업자들은 다운로드된 데이터를 함부로 다른 기기 또는 매체에 복사하지 못하도록 하는 기술에 관심을 기울였다. 때마침 유선 인터넷의 발달에 힘입어 이미 저작권이 있는 데이터에 대한 복사방지 기술(DRM; Digital Rights Management)이 널리 퍼지고 있었으므로 이동통신 관련 회사들은 이러한 기존 기술들을 무선상에서 사용하고자 하는 노력을 기울였으며 이러한 노력은 자연스럽게 기존에 존재하는 여러 회사의 상이한 DRM 기술들간의 표준화로 이어졌다.

2001년 WAP Forum 내에 WAG Download Group이 신설되었고 여기서 무선 단말에 사용될 DRM 기술에 대한 표준화가 진행되었다. 2002년 OMA(Open Mobile Alliance)라는 민간표준화기구가 WAP Forum, SyncML, Wireless Village 등 기존의 모바일 표준화기구들간의 연맹형태로 결성되었고, WAP Forum에서 진행되었던 DRM 표준화 작업을 물려받아 오늘날의 OMA DRM 기술로 발전하였다.

OMA DRM은 다음과 같은 목표를 가진다.

- 콘텐츠의 다운로드시 쉽고 요금 청구가 가능할 것
- 복사방지와 미리 보기 기능 제공
- 기존 이동통신 콘텐츠 사업에 가치와 유연성을 부여
- 신속한 규격개발과 구현
- 고가의 콘텐츠에 대한 충분한 보안 지원

2. OMA DRM 현황

2001년 12월에 WAP WAG Download Group이 결성된 이후 2002년 10월까지 총 5개의 DRM 규격이 승인되었다. 2002년 11월에는 OMA의 이름으로 DRM 1.0이 발표되었다.

2002년 8월에 OMA MAG Download Group이 결성되었으며 DRM 2.0에 대한 표준화 작업이 시작되었다. 약 2년간의 작업 끝에 2004년 7월에 1차 Candidate Enabler가 발표되었고, 2004년 12월에 2차 Candidate Enabler가 발표되었다. 이제 기술규격에 대한 테스트 규격을 만들고 테스트를 직접 해보는 일만 남았다. 2005년 3월 현재 기준으로 DRM 2.0은 2005년 3Q에 완료될 것으로 예상하고 있다.

한편 OMA DRM 2.0 기술을 타 OMA WG에 적용하려는 시도가 있다. 현재는 OMA BCAST와 joint meeting을 통해서 DRM 확장규격을 만들어내고 있으며 이 규격은 2.1에 포함될 예정이다.

3. 아키텍처

그림 1은 DRM의 기능적 아키텍처를 보여준다. 콘텐츠 발급자로부터 다운로드된 보호된 콘텐츠는 권리객체(Rights Object; RO)를 권리 발급자(Rights

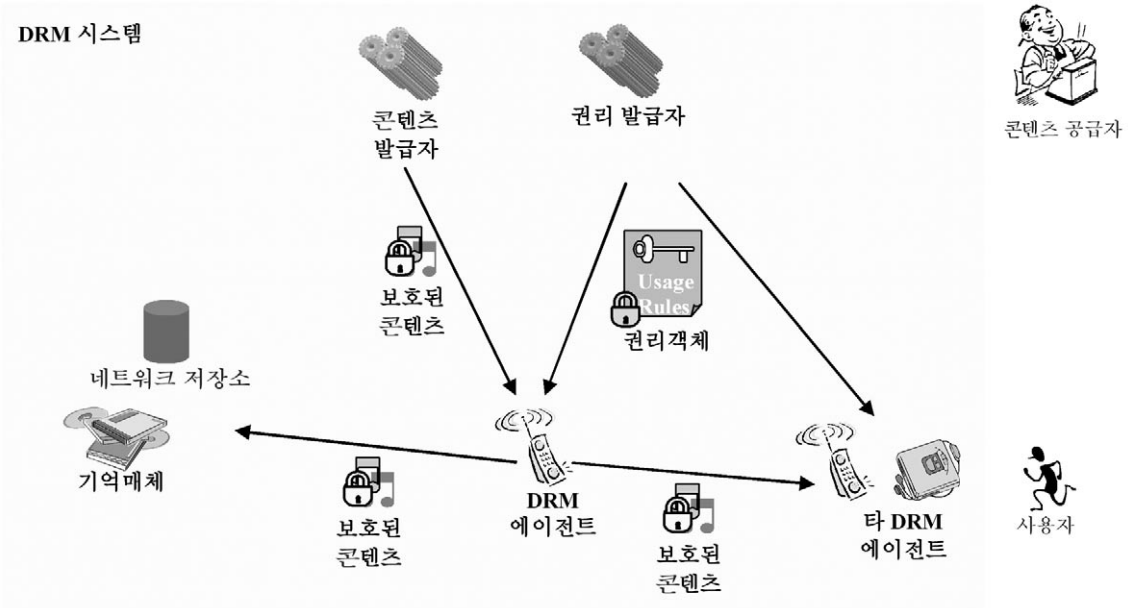

그림 1. DRM 기능적 아키텍처

Issuer; RI)로부터 다운로드 받아야만 사용할 수 있다. 이때 보호된 콘텐츠를 타 DRM 에이전트 또는 네트워크 저장소나 기억매체로 복사할 수 있지만 이를 사용하기 위해서는 권리객체를 권리발급자로부터 발급받아야만 한다.

OMA DRM 규격은 DRM 콘텐츠의 포맷과 보호방법, 권리객체의 포맷과 보호방법, 암호키 관리에 대한 보안 모델을 정의한다. 또한 OMA DRM 규격은 DRM 콘텐츠와 권리객체가 디바이스로 Pull(HTTP Pull, OMA Download), Push(WAP Push, MMS), 스트리밍을 통해 어떻게 전달되는지를 정의한다.

DRM 버전 1.0은 Forward Lock, Combined Delivery, Separated Delivery만을 다루었으나 버전 2.0은 이외에도 Domain, Backup, Super Distribution, Export, Unconnected Device Support, Basic Pull Model, Push of DRM Content, Streaming of DRM Content의 사용예들을 다룬다.

DRM이 제공하는 신뢰모델은 표준 PKI 모델에 기반한다. DRM 에이전트는 권리발급자에게 신뢰를 받을 수 있어야 하며 이를 위해 DRM 에이전트에게 유일한 키 쌍과 이에 관련된 인증서가 공급된다.

DRM은 보안을 위해 DRM 콘텐츠를 전달할 때 다음과 같은 절차를 밟는다.

- 콘텐츠 패키징: 콘텐츠를 콘텐츠 암호화 키(CEK)로 암호화 하여 DCF라는 포맷 안에 담는다.
- DRM 에이전트 인증: 모든 DRM 에이전트는 유일한 개인키/공개키 쌍과 인증서를 갖는다. 권리발급자는 이를 통하여 DRM 에이전트를 인증할 수 있다.
- 권리객체 생성: 권리객체는 허가권과 콘텐츠의 사용조건을 명시한 XML 문서이다.
- 권리객체 보호: 권리발급자는 콘텐츠 암호화 키(CEK) 등 민감한 부분을 암호화 함으로써 특정 DRM 에이전트만 열 수 있도록 한다. 그리고 나서 권리객체에 서명한다.
- 콘텐츠와 권리객체 전달: 콘텐츠와 권리객체는 DRM 에이전트로 전달된다. 이 때 이들은 이미 암호화 되어 있으므로 아무 전달방법으로나 전달되어도 좋다. 권리객체는 DCF(DRM Content Format)에 실려 보내질 수도 있고 MIME Multipart를 써서 콘텐츠와는 별개로 보내질 수도 있다.

4. 상세 기술

– ROAP

ROAP(Rights Object Acquisition Protocol)은 권리발급자(Rights Issuer, RI)와 디바이스 내의 DRM 에이전트 사이에서 주고받는 DRM 보안 프로토콜의 이름이다. ROAP은 다음의 프로토콜들을 포함한다.

- 등록을 위한 4단계 프로토콜
- 권리객체를 요청-응답 형태로 받는 2단계 프로토콜
- 권리객체를 일방적으로 받기만 하는 1단계 프로토콜
- 도메인에 가입하고 해지하기 위한 2단계 프로토콜

– ROAP Trigger

1단계 프로토콜을 제외한 나머지 프로토콜들은 ROAP Trigger를 사용하여 시작될 수 있다.

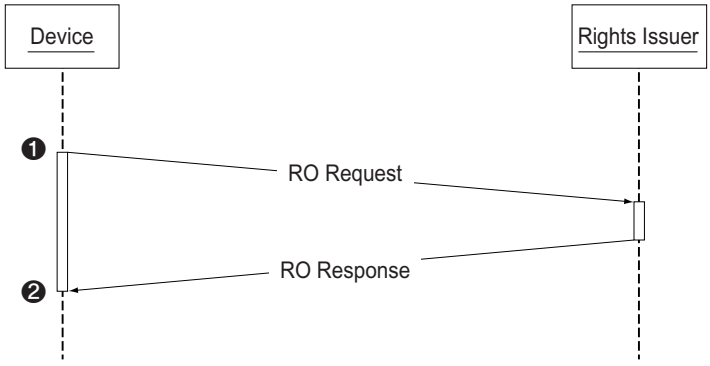

그림 2. ROAP의 예 – 권리객체를 요청 · 응답 형태로 받는 2단계 프로토콜

ROAP Trigger는 등록요청, 권리객체 요청, 도메인 가입, 도메인 해지의 ROAP 메시지를 보내도록 한다.

– 도메인

도메인은 권리발급자에 의해 발급된 도메인 키를 공유하는 디바이스의 그룹이다. 이들 도메인에 속한 디바이스들은 도메인 권리객체에 의해 관리되는 콘텐츠들을 사용할 수 있다.

도메인은 유일한 도메인 식별자에 연관되어 있으며 도메인이 업그레이드 되면 도메인 생성 카운터의 값이 증가하게 된다. 도메인 업그레이드의 결과로 여러 도메인 키가 생길 수도 있다. 디바이스는 하나 이상의 권리발급자에 의해 관리되는 여러 도메인에 가입하거나 해지할 수 있다.

– Transport

OMA DRM은 권리객체 또는 콘텐츠를 전달하기 위해 다음의 Transport 기술을 사용한다.

- HTTP: 네트워크에 연결된 디바이스는 HTTP 위에서 ROAP을 전송할 수 있어야 한다.
- OMA Download OTA: 권리발급자는 콘텐츠와 권리객체를 전송할 때 DLOTA(Download OTA)를 쓸 수 있다. DLOTA는 단말의 능력 협상 기능이나 설치여부 통지기능을 사용할 수 있게 한다.
- WAP Push: 권리객체나 콘텐츠를 WAP Push를 사용하여 전달할 수 있다.
- MMS: 콘텐츠를 전달할 때 사용할 수 있다.
- OBEX : 네트워크에 연결된 디바이스가 네트워크에 연결되지 않은 디바이스를 지원하기 위해 OBEX가 사용된다.

– REL

DRM 콘텐츠를 특정 디바이스에서 사용할 수 권리는 REL(Rights Expression Language)로 표현된다. REL은 ODRL(Open Digital Rights Language) 버전 1.1의 부분집합(또는 모바일 프로파일)이며 ODRL에서는 제공하지 않는 추가적인 허가권과 조건을 정의한 데이터 사전(Data Dictionary, DD)이 포함된다.

REL은 다음의 모델로 구성되어 있다.

- 기초 모델(Foundation Model): rights 엘리먼트
- 협약 모델(Agreement Model): agreement, asset 엘리먼트
- 컨텍스트 모델(Context Model): context, version, uid 엘리먼트
- 허가 모델(Permission Model): permission, play, display, execute, print, export 엘리먼트
- 조건 모델(Constraint Model): constraint, count, timed-count, datetime, start, end, interval, accumulated, individual, system 엘리먼트
- 상속 모델(Inheritance Model): inherit 엘리먼트
- 보안 모델(Security Model): [XMLENC]와 [XMLDSIG] 기술 사용

- DCF

OMA DRM에서는 미디어 객체가 DCF(DRM Content Format)라는 형태로 암호화되고 패키징 된다. DCF는 암호화된 미디어 객체 이외에도 다음과 같은 메타 데이터들을 담는다.

- 미디어 객체 원본의 콘텐츠 타입
- 암호화된 미디어 객체를 권리와 연결시키기 위한 식별자
- 암호화 정보
- 권리발급자 정보
- 미디어 종류에 관련한 부가정보

DCF는 확장 가능하도록 설계되었기 때문에 추후 버전에서도 하위버전에 계속 호환성을 가질 것이다. 하지만 버전 1의 콘텐츠 포맷[DRMCF-v1] 규격과는 MIME 타입이 다른 관계로 호환되지 않는다.

DRM 콘텐츠 포맷에는 두 가지 프로파일이 있다. 하나는 DCF로 그림파일과 같은 Discrete 미디어를 위한 것이고 또 하나는 PDCF로 음악이나 동영상과 같은 Continuous 미디어를 위한 것이다. 이 두 프로파일은 모두 ISO Base Media File format [ISO14496-12]라는 규격을 바탕으로 하고 있다. 하지만 Discrete 미디어 프로파일은 ISO 미디어 파일규격과 완전히 호환되지는 않는다. 이러한 이유로 외부에서 볼 때 일반적으로 Discrete 미디어 프로파일은 DRM 콘텐츠 포맷처럼 보이고 Continuous 미디어 프로파일은 일반 미디어 파일처럼 보인다.

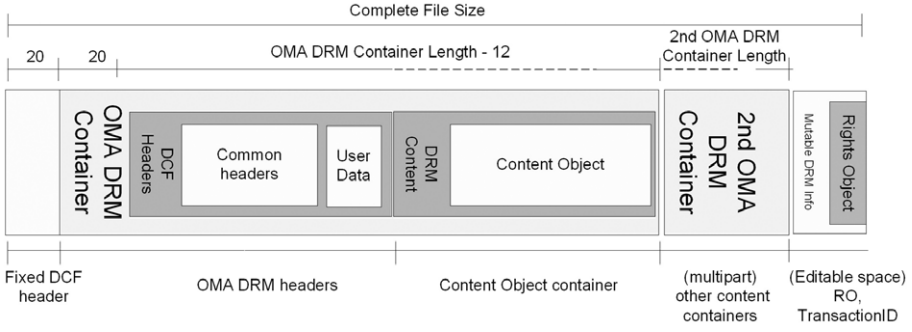

그림 3. DCF의 전체구조

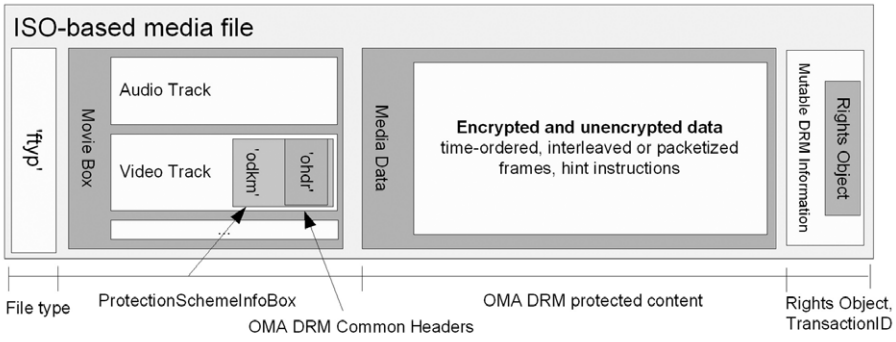

그림 4. PDCF의 전체구조

5. 결언

근래에는 전 세계적으로 음반시장과 소프트웨어 시장을 중심으로 저작권이 있는 콘텐츠의 보호에 대한 관심이 높아지고 있다. 이러한 관심은 이통통신 시장에도 지대한 영향을 미치고 있다. 이동통신 서비스 사업자들은 이제 하나둘씩 OMA DRM 1.0 기술을 도입하고 있고 OMA DRM 2.0에도 관심을 보이고 있다. 따라서 조만간 OMA DRM 기술이 적용된 단말들을 주변에서 쉽게 볼 수 있게 될 것이다.

한가지 아쉬운 점은 우리나라에서 DRM 기술에 대한 연구가 부족하다는 사실이다. 얼마 전 몇몇 DRM 관련 핵심 IPR을 보유한 업체들이 MPEG-LA를 통해 DRM 기술에 대한 사용료, 단말기 대당 1$와 서비스 사용료 1%를 받겠다고 나선 것은 특허권 확보와 관련하여 우리에게 시사하는 바가 크다. 지금이라도 DRM 응용기술에 대한 연구에 집중하면 지금보다 더 많은 IPR들을 확보하여 라이선스 비용을 줄일 수 있을 것이라 생각한다. TTA