

Post Internet을 위한 모바일 디지털 콘텐츠 관리기술

장 의 진*

오 성 훈**

◆ 목 차 ◆

1. 서 론
2. OMA DRM

3. 표준화 현황
4. 결 론

1. 서 론

현재 우리나라 이동통신 가입자 수는 전체 인구의 65% 수준인 3,000만명을 넘어섰고 모바일 비즈니스의 기본 매체인 PDA, 스마트폰 등이 새로운 운영체제, 이동통신 기술과 접목되어 향후 차세대 인터넷을 주도적으로 이끌어 나갈 것으로 예상됨에 따라 모바일 비즈니스를 위한 기본 인프라는 충분히 조성되었다고 할 수 있다.

모바일 통신 기술은 기존 CDMA 1x보다 20배 정도 빠른 통신 속도를 구현할 수 있는 CDMA 1x EV-DO와 그보다 5배정도 빠른 무선 랜이 상용화됨에 따라 이를 통한 문자 전송, 게임 다운로드 등에 머무르던 모바일 콘텐츠 서비스는 차세대 모바일 인터넷을 기반으로 보다 다양해질 것으로 전망된다.

지금까지 유선 인터넷망에 적용되어 온 DRM 기술은 모바일 콘텐츠 시장이 활성화됨에 따라 차세대 인터넷 망으로 점차 그 적용 범위를 확대해가고 있으며, 이동통신 단말기 상에서 콘텐츠의 불법적인 사용 및 복제를 방지하고 저작권을 보호하기 위한 유망 콘텐츠 보호 기술로 주목받고 있다.

DRM은 콘텐츠의 지적 재산권이 디지털 방식에 의해서 안전하게 보호·유지 되도록 하여 콘텐츠가 창작에서부터 소비에까지 이르는 모든 유통 시점에서 거래 및 분배규칙, 사용규칙이 적법하게 성취되도록 하

는 기술이다. 또한, 콘텐츠의 판매 및 배포, 소비에 이르는 새로운 방법을 제공하여 콘텐츠를 제공하는 CP(Content Provider)/SP(Service Provider)가 콘텐츠의 맛보기(preview), 사용 횟수 혹은 만료일의 제한, 콘텐츠의 구독(subscription), 콘텐츠의 다운로드 혹은 스트리밍 서비스와 같은 다양한 비즈니스 모델을 허용하기 위한 사용 규칙(Usage rules)을 적용할 수 있다.

현재 유선 통신 서비스와 비슷한 수의 모바일 콘텐츠가 제공되고 있으나 이용자 수나 콘텐츠의 질적인 측면에서는 아직 미흡한 실정이며, 이는 모바일 콘텐츠가 유선 콘텐츠에 비해 질적으로 많이 떨어지고, 적은 메모리 자원과 제한된 데이터 처리 능력 등의 한계를 가진 이동통신 단말기의 특성에 기인한 것이다.

그러나 이동통신망 기술과 이동통신 단말기의 획기적인 발전으로 모바일 서비스도 보다 다양하고 질적으로 향상된 콘텐츠를 제공할 것으로 예상되므로 통신망과 단말기의 특성을 고려한 DRM 기술의 적용은 필수적이다.

본 고에서는 Post Internet을 위한 모바일 디지털 콘텐츠 저작권 관리기술과 관련하여 모바일 DRM의 국제 표준인 OMA DRM Version 1.0 규격에서 제시하는 전체 시스템 구성과 기능, 그리고 콘텐츠 전달방식과 콘텐츠 포맷, 권리명세, 다운로드 방식 등에 대해 서술한다.

본 고의 구성은 다음과 같다. 2장에서는 OMA 규격을 준수한 모바일 DRM의 구조와 기능을 살펴보고, 3장에서는 OMA와 3GPP를 통한 표준화 진행 현황에

* (주)디지캡 기술연구소 선임연구원

** (주)디지캡 기술연구소 책임연구원

대해 설명한다. 마지막으로 4장에서는 결론을 맺도록 한다.

2. OMA DRM

OMA DRM은 OMA에서 명세한 모바일 DRM 시스템에 대한 규격으로써 다음과 같은 특징을 갖는다.

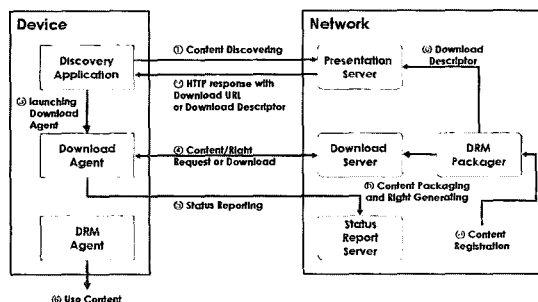
- 콘텐츠 제공자는 DRM Content 사용에 대한 Rule을 정의할 수 있다. 즉, DRM 도입 이전에는 단일 가격 정책으로 콘텐츠를 판매할 수밖에 없었지만, OMA DRM은 동일한 콘텐츠에 다양한 사용 권리 조건을 명시함으로써 다수의 가격 정책으로 콘텐츠를 판매할 수 있다.
- OMA DRM은 더 이상 콘텐츠에 가치를 두지 않고 콘텐츠의 사용 권리인 Rights에 가치를 둔다.
- 콘텐츠 자체에 대한 판매가 아닌 Rights를 판매하는 것이 가능하다.

다음은 앞서 서술한 특징을 갖는 OMA DRM System의 전체 구성과 콘텐츠 전달 방식, 권리 명세 등에 대하여 서술한다.

2.1 OMA DRM System

OMA DRM System은 그림 1과 같이 Discovery Application, Download Agent, DRM Agent로 구성되는 Device-side와 Presentation Server, Download Server, DRM Packager, 그리고 Status Report Server로 구성되는 Network-side로 구분된다.

- **Presentation Server**
콘텐츠의 Browsing을 돕는 웹 서버이다. 디바이스는 Presentation Server를 통해 HTML/WML page를 Browsing할 수 있으며 콘텐츠의 다운로드를 위하여 Download Server로 Redirection 한다.
- **Download Server**
사용자가 선택한 콘텐츠(원본 콘텐츠 또는 DRM Content)에 대한 다운로드 서비스를 제공한다. 사용자의 디바이스에 콘텐츠 그리고/또는 권리 개체의



(그림 1) OMA Download System Architecture

다운로드 처리를 담당한다.

- **Status Report Server**
디바이스 상에서 콘텐츠의 정상적인 다운로드, 설치 및 사용 정보에 대한 보고를 수집한다.
- **DRM Packager**
콘텐츠의 암호화 수행 후 암호화 된 원본 콘텐츠를 헤더와 함께 DRM Content의 형태로 구성된다. DRM Content에 포함되는 헤더 정보에는 원본 콘텐츠의 형식, 콘텐츠 식별자, 암호화 정보, Rights 발급 서비스 정보 등이 포함되어 있다.
- **Discovery Application**
디바이스 상에서 콘텐츠 형식에 적합한 웹 브라우저 혹은 어플리케이션을 사용하여 콘텐츠를 검색하기 위한 User Agent이다.
- **Download Agent**
Download Descriptor에 의해 설명되는 콘텐츠의 다운로드 기능을 담당한다. Download Descriptor는 콘텐츠의 다운로드를 위한 콘텐츠 메타데이터(type, objectURI, Right-Issuer URL 등)와 Download Agent에 대한 지시 사항을 정의한다.
- **DRM Agent**
콘텐츠의 다운로드, 권리 개체에 따른 콘텐츠의 사용 제어, 권리 개체의 관리 등을 처리한다.

OMA Download System은 그림 1에서와 같이 콘텐츠의 다운로드를 위해 다음과 같은 과정을 수행한다.

- ① Content Registration/ ② Content Packaging and Right Generating/ ③ Download Descriptor
CP/SP는 콘텐츠에 대한 과금 정책을 설정하고 콘텐츠

를 등록하기 위해 DRM Packager를 이용한다. DRM Packager는 CP/SP가 서비스하려는 콘텐츠를 패키징 하고 Rights를 생성하며, 패키징된 DRM Content를 최종적으로 서비스하기 위해 Presentation Server와 Download Server에 해당 콘텐츠에 대한 정보 및 Download Descriptor를 등록한다.

① Content Discovering

사용자는 Discovery Application을 사용하여 구매하려는 콘텐츠를 검색한다.

② HTTP Response with Download URL or Download Descriptor

HTTP 프로토콜을 사용하여 Presentation Server로부터 콘텐츠를 다운로드 할 수 있는 URL 이나 Download Descriptor를 가져온다.

③ Launching Download Agent

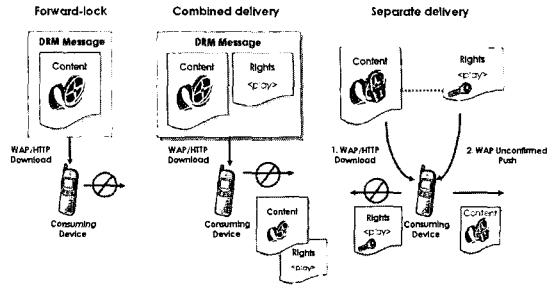
Download Agent가 실행된다. Download Descriptor가 처리 규칙에 따라 실행되어야 하며 Download Descriptor에 오류가 있을 경우 오류 메시지가 사용자에게 나타나야 한다. Download Agent에 InstallNotifyURI가 정의되어 있을 경우 Status Report Server에 오류 보고를 수행해야 한다. Download Descriptor의 버전이 디바이스에 의해 지원되지 않는 버전일 경우 상태보고 후 콘텐츠 다운로드 과정을 중단한다.

④ Content/Right Request or Download

Download Agent는 HTTP(또는 HTTPS)를 사용하여 Download Server에 콘텐츠와 Rights의 다운로드를 요청한다. 콘텐츠의 다운로드를 Download Descriptor에 명시된 objectURI를 통해 수행된다. 콘텐츠가 존재하지 않을 경우, 콘텐츠의 다운로드 중에 네트워크 연결이 끊어진 경우, 그리고 사용자가 콘텐츠의 다운로드를 중지한 경우에는 DRM Agent가 Status Report Server에 오류 메시지를 전송하게 된다.

⑤ Status Reporting

Status Report는 콘텐츠가 올바르게 수신되고 설치되었음을 Download Server에 알리기 위한 목적으로 사용된다. Download Agent는 콘텐츠와 Rights의 정상적인 다운로드와 설치에 대한 성공/실패 여부, 그리고 사용 정보 관련 메시지를 Status Report Server에 전송한다.



(그림 2) OMA DRM의 세 가지 콘텐츠 전달방식

⑥ Use Content

DRM Agent는 다운로드 된 콘텐츠를 Rights의 명시된 내용에 따라 사용자가 사용할 수 있도록 한다.

2.2 OMA DRM Delivery Method

OMA DRM은 그림 2와 같이 세 가지의 콘텐츠 전달 방식(Contents Delivery Method)을 정의한다.

가. Forward-lock

Forward-lock은 디바이스에 전달된 콘텐츠가 다른 디바이스로 전송되지 않도록 하는 방식이다. Right가 존재하지 않으며 사용자는 기본 사용 방침에 따라 콘텐츠를 이용한다.

나. Combined delivery

Combined delivery는 Rights object와 원본 콘텐츠가 함께 DRM Message의 형태로 패키징 된다. Rights object는 사용권한에 대해 정의하며 CP/SP는 play, display, print, execute 의 권한을 설정할 수 있다. Rights에 명시할 수 있는 Usage Rule의 Syntax 및 Semantic은 2.4절에서 설명한다. 다운로드 된 콘텐츠 및 Rights object는 다른 디바이스에 전달될 수 없으며, 최종 사용자는 DRM Content의 저장, 설치, 삭제 등을 할 수 있어야 한다.

다. Separate delivery

Separate delivery에서는 콘텐츠와 Rights object가 서로 다른 채널을 통해 디바이스에 전달된다. Rights는 Push 서비스를 통해 단말기에 전달된다. 콘텐츠는 AES 알고리즘을 이용하여 암호화되며 CEK(Content Encryption

Key) 없이는 복호화 될 수 없다.

콘텐츠는 DCF(DRM Content Format)의 형태로 암호화되며 CEK(Content Encryption Key) 없이는 복호화 될 수 없다. CEK는 Rights에 포함되어 사용자에게 전달된다.

암호화된 콘텐츠는 다른 디바이스로 전달될 수 있지만 Rights의 전달은 불가능하며 콘텐츠를 전달받은 다른 디바이스의 사용자는 새로운 Rights를 발급받아야 한다. Separate delivery 방식은 콘텐츠를 구입한 사용자가 해당 콘텐츠를 제삼자에게 자유롭게 배포할 수 있게 함으로써 다양한 콘텐츠 유통 채널을 제공하며 제삼자가 해당 콘텐츠를 합법적으로 사용할 수 있게 하는 Superdistribution을 가능하게 한다.

PC 기반의 DRM 기술과는 달리 모바일 디바이스 플랫폼의 폐쇄된(closed) 환경으로 인하여 Forward-lock 과 Combined delivery 방식만으로도 콘텐츠의 외부 유출로 인한 불법복제를 방지할 수 있었으나, 디바이스의 성능 향상과 디바이스 간 통신이 가능해짐에 따라 Separate delivery를 통한 콘텐츠 자체의 기밀성에 대한 요구가 점차 증가하고 있다.

라. Superdistribution

Superdistribution은 콘텐츠 사용자가 자신이 구입한 콘텐츠를 E-mail, CD-ROM, 디스켓 등을 통해 다른 사람에게 반복적으로 배포할 수 있게 하여 콘텐츠의 급속한 확산을 가능하게 하는 기술이다. Superdistribution은 DCF형태의 콘텐츠에 대한 배포를 허용하며 super-distributed 된 콘텐츠의 사용을 위해 Rights를 발급받을 수 있게 해준다. 디바이스는 DCF의 Rights-Issuer 필드에 정의된 URL을 통해 Rights 발급 요청을 하게 된다.

기존 Secure distribution 기술은 사용자에게 종속적인 키를 이용하여 콘텐츠를 암호화함으로써 콘텐츠의 이동을 크게 제한한 반면 Superdistribution은 콘텐츠의 이동 및 복사는 자유롭게 허락하되 사용 시점에서 사용권한을 획득해야만 콘텐츠의 이용이 가능한 기술적 매커니즘을 통해 디지털 콘텐츠의 안전한 유통을 유도한다.

2.3 콘텐츠 패키징

OMA DRM 시스템은 원본 콘텐츠의 기밀성 보호를 위해 대칭 암호화 알고리즘(Symmetric Encryption

Algorithm)을 이용하여 콘텐츠를 암호화(또는 패키징)한다. OMA DRM 규격에서는 이를 위해 DCF(DRM Content Format) 규격을 명세하였으며 콘텐츠의 유통을 위한 메타데이터 구성 및 파일 구조를 명시하고 있다. DRM Content를 표현하기 위한 DCF는 OMA DRM Content Format Version 1.0을 지원하며 Version 2.0 규격에 대한 Draft가 현재 진행 중에 있다.

DCF는 콘텐츠 데이터, 원본 콘텐츠의 MIME Type, 콘텐츠 식별자, 암호화 방법, 사용 권리를 구입하기 위한 URI 정보 등을 나타내는 DRM Content Metadata를 정의하며, MIME Type은 "application/vnd.oma.drm.content"이다.

2.3.1 DRM Content Format Version 1.0

DRM Content Format Version 1.0은 그림 3과 같이 구성된다.

헤더는 DRM Content와 원본 콘텐츠에 대한 추가적인 메타데이터를 정의하며 해당 항목에는 다음과 같은 헤더 정보가 포함될 수 있다.

- Encryption-Method header

원본 콘텐츠의 암호화 방법을 정의한다. 즉, 암호화 알고리즘과 Padding Scheme을 지정한다. OMA DCF 규격에 따라 암호화 알고리즘은 NIST에 의해 정의된 AES symmetric encryption algorithm(128-bits key, 128-bits block size, CBC(Cipher Block Chaining) mode, RFC2630 "Cryptographic Message Syntax" padding scheme)을 기본적으로 지원한다.

- Rights-Issuer header

DRM Content를 사용하기 위해 필요한 Rights를 획득

Version	버전 번호
ContentTypeLen	ContentType 필드의 길이
ContentURLen	ContentURL 필드의 길이
ContentType	원본 데이터의 MIME media type
ContentURI	Content object의 유일한 식별자
HeadersLen	Headers 필드의 길이
DataLen	Data 필드의 길이
Headers	Content object에 대한 추가적인 메타데이터(정의된 헤더)
Data	암호화된 데이터

(그림 3) DRM Content Format v1.0

특할 수 있는 Rights-Issuer URL을 정의한다.

- Content-Name header
DRM Content의 이름을 명시하며 DRM Content가 디바이스에 저장될 때의 파일 이름으로 사용할 수 있다.
- Content-Description header
DRM Content 및 원본 콘텐츠에 대한 일반적인 정보를 기술한다.
- Content-Vendor header
콘텐츠를 제공하는 Content Provider에 대한 정보를 기술한다.
- Icon-URI header
디바이스에서 DRM Content를 지칭하는 아이콘에 대한 URI를 기술한다.

2.3.2 DRM Content Format Version 2.0

OMA DRM Content Format Version 2.0은 Discrete Media(벨소리, 어플리케이션, 이미지 등)와 Continuous (Packetized) Media(오디오나 비디오)로 구분되는 두 가지 콘텐츠 포맷에 대한 프로파일을 정의한다는 점에서 Version 1.0 과 차이가 있다.

프로파일은 Discrete Media의 패키징 및 보호를 위한 DCF와 Continuous Media의 보호를 위한 PDCF(Packetized DRM Content Format)에 대해 명시한다. Continuous Media는 PDCF로 보호되며 스트리밍 서버는 PDCF 형태의 콘텐츠를 인식하는 디바이스에게 헤더와 패킷이 분리된 형태로 전송할 수 있도록 해야 한다.

2.4 권리 명세 언어

OMA DRM은 REL(Rights Expression Language)을 사용하여 DRM Content에 대한 사용 규칙을 정의한다. DRM Content의 사용은 Rights Offer와 Right Agreement를 통해 수행된다.

2.4.1 Right Offer

콘텐츠에 대한 지적 재산권을 보유한 자(Right Holder)들이 허용할 사용 및 분배 규칙 등의 특정한 권리를 명세하여 제공한 것을 의미한다. Right Offer를 명세하기 위해 국제 규격인 ODRL(Open Digital Rights Language)

표준을 이용한다.

CP/SP는 등록하는 콘텐츠에 대해 허용할 사용 및 분배 규칙 등을 Right Offer에 명세하며 다음과 같이 구성된다.

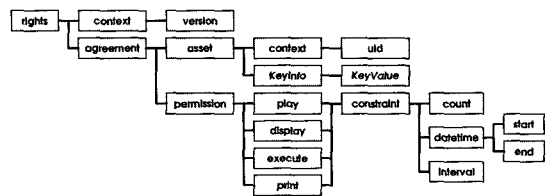
- Asset : 콘텐츠(content or asset)에 대한 정보
- Rights Holders : Right Offer를 만드는 당사자(party)들에 대한 정보
- Permission : 콘텐츠에 대해 허용하려는 사용 규칙에 대한 정보
- Context : 날짜, 시간, 위치, 식별자 등의 Right Offer에 대한 자세한 정보

2.4.2 Right Agreement

콘텐츠에 대한 특정한 권리에 대하여 당사자들 간에 이루어진 동의를 의미하며 그 구성은 다음과 같다.

- Asset: 콘텐츠(content or asset)에 대한 정보
- Party: Right에 대해 동의한 당사자(party)들에 대한 정보
- Permission: 동의한 콘텐츠 사용 규칙에 대한 정보
- Context: 날짜, 시간, 위치, 식별자 등의 Right Offer에 대한 자세한 정보

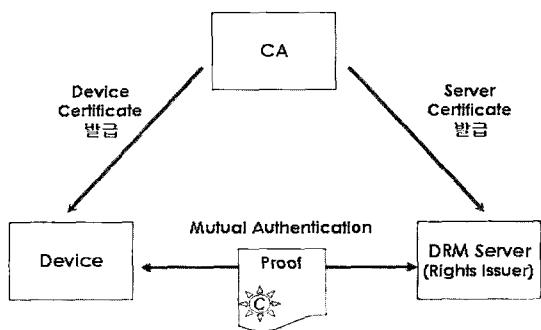
OMA DRM REL Version 1.0의 Entity Hierarchy는 그림 4와 같다.



(그림 4) OMA DRM REL

2.5 Trust and Security Model

현재 모바일 DRM의 표준인 OMA DRM 1.0은 보안 측면에서 취약성을 가진다. 즉, Rights object와 CEK는 보호되지 않으며 Rights의 발급 전에 디바이스의 인증



〈그림 5〉 PKI 기반의 DRM Trust Model

이 이루어지지 않으므로 디바이스와 Rights Issuer의 상호 인증(Mutual Authentication)이 이루어지지 않는다.

차후 OMA DRM Version 2.0에서는 그림 5와 같이 공개키 암호화와 인증서 발급, 디지털 서명과 신뢰된 CA(Certificate Authority) 등으로 구성된 PKI(Public Key Infrastructure) 기반의 Trust Relationship이 이루어질 것으로 예상된다.

PKI기반의 DRM Trust Model에서 디바이스는 Rights와 CEK의 발급 전에 Rights Issuer에게 자신을 증명하기 위한 인증서를 CA로부터 발급받는다. Rights Issuer 또한 CA로부터 인증서를 발급받게 되며 디바이스와 Rights Issuer는 인증서 교환을 통하여 상호 인증을 수행하게 된다.

PKI에서는 각 디바이스가 인증서와 개인키의 저장이 가능하고 저장된 정보에 대한 불법적인 접근을 허용하지 않는 스마트카드 형태의 스토리지(tamper-resistant storage)를 필요로 하며, 장비 제조업체(디바이스)와 DRM Server(Rights Issuer)의 상호 인증이 선행되어야 한다. PKI 기반 DRM 시스템에서의 콘텐츠 전달은 Separate delivery 방식과 유사하지만 Rights가 발급되기 전에 인증된 디바이스인지의 여부를 체크한다는 점에 있어서 다르다. 또한, 모든 Right는 디바이스의 공개키로 암호화됨으로써 보호된다.

3. 표준화 현황

3.1 3GPP

3GPP(Third Generation Partnership Project)는 1998년

12월에 설립된 수많은 표준화 기구들 사이의 공동연구 합의로 이루어졌다. 3GPP의 목적은 third generation mobile communications(3G)를 위해 광범위하게 적용할 수 있는 기술적인 규격을 제공하는 것이다. 현재 이동통신 사업자를 포함하여 500여개의 회원사가 가입되어 있다.

3GPP는 2003년 중순에 release 6에서 모바일 DRM 규격을 소개할 계획이었으나, 2002년 9월 3GPP의 모바일 DRM 표준화 작업에 대한 책임이 Open Mobile Alliance (OMA)로 전가되면서 DRM에 대한 활발한 활동은 더 이상 진전이 없게 되었다. 현재 3GPP TS 22.242 Digital Rights Management (DRM); Stage 1까지 완성되었으며, DRM 솔루션을 제공하기 위한 시스템의 기능 및 역할에 대한 요구사항이 정리된 상태이다. 요구사항 문서에서는 사용자와 사용자 디바이스, 사용권리, 보안, 프라이버시, 과금을 위한 DRM의 일반적인 조건과 요구사항을 기술하고 있다.

3.2 OMA

OMA(Open Mobile Alliance)는 Open Mobile Architecture initiative 와 WAP Forum에 의해 2002년 6월에 설립되었다. OMA는 모바일 산업을 위하여 사용자와 시장의 요구사항에 근거한 개방된 표준과 스펙에 대한 소개를 목적으로 한다. Ericsson, Microsoft, Motorola, Nokia, Openwave, Siemens, DoCoMo, Vodafone, Sonera 와 같은 국외 업체 및 삼성, SKT등과 같은 국내 업체를 포함 300여개의 회원사가 가입되어 있다.

OMA DRM Version 1.0 규격은 2002년 9월에 승인되었고 신속히 구현될 수 있는 초기 단계의 간단한 모바일 DRM 표준을 제안하는데 중점을 두었다. OMA DRM Version 1.0은 두 가지 문제점을 해결하기 위해 개발되었는데 첫째, Forward-lock 없이 디바이스 상에 있는 콘텐츠를 다른 사용자에게 불법적으로 전송하는 것을 방지하기 위한 표준화된 방법이 없다는 점이며 둘째, 모바일 디바이스 사용자가 콘텐츠를 구입하기 전에 맛보기(preview)를 위한 간편하고 효과적인 방법을 갖고 있지 못하다는 점이다. 따라서 OMA DRM Version 1.0은 Forward-lock과 맛보기 기능뿐만 아니라 좀 더 포괄적인 개념의 DRM을 제안하는데 초점을 맞

추었다. 실제로, OMA DRM은 Forward-lock, Combined delivery, 그리고 Separate delivery의 세 가지 방식을 정의한다.

OMA는 디지털 권리 표현 언어를 정의하기 위해 XML기반의 ODRL을 채택했다.

ODRL은 e-books, 음악, 오디오, 그리고 소프트웨어 형태의 디지털 콘텐츠와 함께 사용될 수 있으며 라이선스에 대한 제약사항 없이 사용 가능하다.

OMA DRM Version 1.0 규격에서는 콘텐츠 전달방식, 포맷, 권리 명세, 다운로드 방식 등에 대한 명세가 이루어졌으며 관련 규격은 다음과 같다.

- OMA Download Architecture Version 1.0
- OMA Digital Rights Management Version 1.0
- OMA DRM Content Format Version 1.0
- OMA Rights Expression Language Version 1.0

4. 결 론

최근 휴대폰, PDA, 스마트폰 등으로 대표되는 모바일 디바이스의 성능 향상과 CDMA 1x EV-DO와 무선 랜으로 대표되는 이동 통신망 기술의 급속한 발전으로 차세대 인터넷 기반 환경에 적용될 DRM 기술 개발에 대한 수요가 점차 증가하고 있다. 세계적인 무선 장비업체와 OMA를 주축으로 한 기술 표준 그룹에서도 모바일 환경에 적합한 DRM 기술 개발에 적극 나서고 있어 모바일 DRM 기술이 적용된 콘텐츠를 디바이스를 통해 접할 날이 멀지 않았다.

기술적인 측면에서는 차세대 인터넷 환경과 모바일 디바이스의 CPU 성능 및 메모리 제한을 고려한 DRM 기술의 소형화 및 경량화 노력이 필요하며, 모바일 콘텐츠를 서비스하는 모바일 비즈니스 측면에서는 모바일 콘텐츠의 불법복제와 저작권 침해로 인한 비용 손실을 사전에 방지하기 위한 디지털 콘텐츠 관리 기술이 필수적이다. 그러나 DRM 기술 적용으로 인한 사용상의 불편함으로 인하여 사용자를 놓치는 위험에 직면할 수도 있으므로 모바일 비즈니스의 이익을 창

출할 수 있는 차세대 인터넷을 위한 모바일 디지털 콘텐츠 관리 기술을 제공하는 것이 관건이다.

OMA를 통한 모바일 DRM의 표준화 작업은 현재 1.0 버전까지 진행된 상태이나 보안 측면에서 취약점을 가진다. 이러한 취약점을 고려하여 OMA DRM 2.0은 PKI를 기반으로 한 Trust & Security Model이 적용될 것이며, 콘텐츠의 다운로드 서비스뿐만 아니라 스트리밍 서비스를 위한 콘텐츠 포맷의 규격 정의, 그리고 콘텐츠의 Superdistribution등이 정의될 것으로 예상된다.

향후 모바일 DRM이 기술경쟁력과 상호운용성을 확보하기 위해서는 기술개발활동과 국제표준화 활동을 병행해 기술개발에 필요한 정보를 습득하고, 이를 바탕으로 우리나라의 DRM 기술이 국제 표준으로 채택되도록 함으로써 세계 시장에서 우위를 확보해 나아가야 한다. 또한, 차세대 인터넷 환경에 DRM을 효율적으로 적용하기 위한 환경 조성 및 법제도적인 측면의 정비와 DRM 기술을 효과적으로 활용하기 위한 비즈니스 모델의 개발 및 연구가 필요하다.

참고문헌

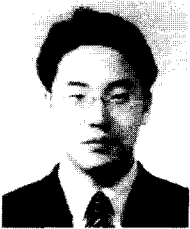
- [1] Open Mobile Alliance, <http://www.openmobilealliance.org>
- [2] Open Digital Rights Language (ODRL) 1.1, The Open Digital Rights Language Initiative <http://www.odrl.net>, 2002.
- [3] Extensible Rights Markup Language (XrML) 2.0, ContentGuard, <http://www.xrml.org>.
- [4] "Mobile Digital Rights Management White Paper," Sonera MediaLab, 2003.
- [5] "Digital Rights Management for Mobile Solutions," Siemens, 2002.
- [6] Zheng Yan, "Mobile Digital Rights Management," Nokia Research Center, Network Security 2001.
- [7] 문형돈, "세계 디지털콘텐츠 시장 현황 및 전망", 주간기술동향, 통권 1105호, IITA, 2003.
- [8] 정상원, "DRM", ITZine, ETRI, 2002.

◎ 저 자 소개 ◎



장 의 진

1999년 송실대학교 컴퓨터학과(학사)
2002년 송실대학교 컴퓨터학과(석사)
2002년~현재 : (주)디지털 기술연구소 선임연구원
관심분야 : 컴퓨터네트워크, DRM



오 성 훈

1996년 인천대학교 정보통신공학과(학사)
1998년 송실대학교 컴퓨터학과(석사)
2002년 송실대학교 컴퓨터학과(박사)
2002년~현재 : (주)디지털 기술연구소 책임연구원
관심분야 : DRM, 암호학, 실시간 시스템, 멀티미디어 시스템 등