상이한 DRM간 연동을 통한 DRM 상호 호환성 지원 방안

정 연 정[†] · 윤 기 송[††] · 강 호 갑[†††]

요 약

오늘날 상용화된 DRM(Digital Rights Management) 제품들은 많이 있으나 DRM간 상호 호환성이 없는 상태이다. DRM간 호환성 결여로 인하여 사용자의 불편은 증대되고 디지털 콘텐츠의 유통은 제한된 범위로 제약을 받고 있다. 이러한 문제점을 해결하기 위하여 DRM의 호환성 지원을 위해 DRM 표준화에 대한 요구가 증대되고 있으나 지배적 위치의 DRM 표준이 마련되지 않아 호환성 문제를 해결하지 못하고 있는 상태이다. 이에 본 논문은 MP3 파일의 저작권보호를 위해 사용되는 상이한 DRM 시스템간 상호 호환을 위한 보완재적 DRM 기술로써 DRM 콘텐츠의 반출(EXport) 및 반입(IMport)을 통한 연동 방안(EXIM)을 제안한다. 제안하는 EXIM 방안은 상호 연동이 필요한 두 DRM 시스템이 자신의 구조를 공개하거나 변경하지 않고도 개방형 기술규격을 통해 DRM 콘텐츠를 상호 호환될 수 있도록 한다.

키워드 : 콘텐츠, 저작권 보호, DRM

DRM interoperable scheme by connection between heterogeneous DRM systems

Yeonjeong Jeong[†] · Kisong Yoon[††] · Hogab Kang[†††]

ABSTRACT

Currently we have many DRM(Digital Rights Management) products but they do not provide interoperability between them. It causes user's inconvenience to use a DRM content and places restrictions to digital content distribution. DRM standardization to solve these sorts of problem has been discussed but dominant standardization which can provide DRM interoperability has not been made. In this paper, we propose DRM interoperable scheme by connection between heterogeneous DRM systems (EXIM) which uses export and import functions. Proposed EXIM can make a DRM content exchangeable between heterogeneous DRM systems with an open type of technology specification although they don't have to open their DRM structure.

Key Words : Content, Digital Rights Management, DRM

1. 서 론

디지털 콘텐츠는 누구나 쉽게 원본과 동일한 복제본을 만들어 인터넷을 통해 배포 할 수 있다는 특성 때문에, 대부분의 콘텐츠 제공자들은 DRM과 같은 불법복제 및 사용 방지 기술을 통해 자신들의 콘텐츠를 보호 하고자 한다[3], [4], [5], [6], [11].

DRM 기술은 디지털 콘텐츠에 대한 불법적인 사용을 효과적으로 차단할 수 있는 기술이지만 아직까지 지배력 있는 표준화된 모습을 갖추지 못하고 있기 때문에, 현재 시장에서는 여러 개의 DRM 솔루션들이 공존하고 있는 상태이다. 이러한 이유에서 많은 디지털 콘텐츠들은 통일화 되지 않은 여러 DRM솔루션을 통해 보호를 받고 있으며, 이는 사용자들이 서로 다른 콘텐츠 제공자들로부터 제공되는 디지털 콘텐츠를 한 기기에서 사용 하고자 할 경우, 사용을 할 수 없는 상황이 되거나 또는 사용기기에 복수개의 DRM 클라이언트를 설치해야 하는 번거로움이 발생하게 된다. 즉, 한 기기 안의 복수 DRM 클라이언트에 대한 설치는 콘텐츠 제공자의 수가 많으면 많을수록 설치되는 클라이언트의 수도 문제지만 복수개의 DRM 시스템이 동시에 구동되는 데에 따른 DRM 시스템간의 충돌 또한 무시할 수 없다. 더욱이 사용기기가 PC가 아닌 MP3 Player나 PDA같은 이동기기 일 경우는 기기의 특성상 리소스의 부족을 고려해야 하기 때문에, 복수 DRM 클라이언트 설치 방법은 올바른 해결 방법이 될 수 없다.

본 논문에서 제안 하는 방안은 이러한 문제점을 해결하여 상이한 DRM간의 호환성을 제공하고자 한다. 제안하는 방안은 다양한 DRM으로 보호되어 있는 디지털 콘텐츠를 서로

† 정 회 원 : 한국전자통신연구원 선임연구원
†† 정 회 원 : 한국전자통신연구원 책임연구원
††† 정 회 원 : 디알엠인사이드 연구소장
논문접수 : 2006년 2월 2일, 심사완료 : 2006년 3월 8일

상대방의 DRM 포맷으로 쉽고 안전하게 변환 할 수 있는 중재자 역할을 수행함으로써 한 개의 DRM 클라이언트만을 가지고 있는 기기에서도 여러 종류의 DRM 콘텐츠를 사용할 수 있도록 한다. 각 DRM 솔루션들은 제안하는 방안을 사용하더라도 자신의 DRM 구조를 공개하지 않고 타 DRM 포맷으로 변경할 수 있을 뿐만 아니라 한번 생성해 놓은 DRM 상호 연동 모듈들은 모든 DRM에 대해서 재 구현 없이 상대방에 대한 인증 작업만으로 해당 모듈에 대한 재사용이 가능하여 N-to-N 관계의 복잡한 DRM들이 상호 호환성을 유지 할 수 있다.

2. DRM 상호 호환성 지원 방안

DRM 콘텐츠 포맷, 서비스, 디바이스에 대한 상호 호환 지원은 사용자에게 디지털 콘텐츠의 편리한 사용을 제공할 수 있으며 창조자, 공급자, 배포자와 같은 다른 유통 주체에게 콘텐츠 보호를 위한 경쟁력 있는 시스템을 제공할 수 있다.

현재 DRM의 상호 호환 지원을 위한 다양한 표준이 존재하거나 진행 과정에 있다. 이러한 표준은 지배적인 위치로 자리 매김을 하지 못하는 상황이며, 표준의 부재 속에 특정 유통 방식에 맞는 기술 분화가 이루어지고 있는 상태이다[2], [5], [8], [11].

그러나 콘텐츠 유통 도메인 내에서 또는 도메인 간 상호 호환을 위한 표준적 측면은 사용자의 요구사항 증가와 새로운 비즈니스 모델의 출현으로 그 필요성이 증대되고 있으며, 이는 사용자뿐만 아니라 콘텐츠 유통에 참여하고 있는 모든 유통 주체를 위해 바람직하다. 이를 위한DRM의 상호 호환을 지원하는 방안으로 아래와 같은 세 가지를 고려할 수 있다[7], [8], [9], [10].

- 기술 규격 통일 방안

DRM 기술 규격을 표준화하고 준수하여 상호 호환하는 방안

- 복수의 DRM 툴 설치 구조 방안

End-user 디바이스 단에서 모든 DRM 툴을 다운로드 함으로써 모든 DRM의 DRM 콘텐츠를 처리할 수 있는 구조를 가지는 방안

- 상호 연동 방안

상이한 DRM간 상호 연동을 통하여 상호 호환하는 방안

기술 규격 통일 방안은 하나의 DRM 기술 사양을 표준으로 정하고 모든 DRM 제품이 이를 따르는 방안이다. 이러한 방안은 다양한 유통 주체가 애플리케이션, 디바이스, 서비스 등을 위해 효과적으로 DRM 시스템을 구성할 수 있고 호환성을 보장받을 수 있다. 그러나 이러한 표준화를 바탕으로 한 호환성 지원은 산업적 요구를 바탕으로 장기적으로 진행되어야 하고, DRM 특성상 보안과 관련하여 기술의 공개에 따른 취약성 발생과 다양한 보안 메커니즘 적용에 제한성이 따른다. 또한 현재 각 DRM이 콘텐츠 보호를 위해 자신의 고유한 형식을 가지는 DRM 콘텐츠를 만들어 서비스하고 있는 상황에서 이를 다른 형식의 새로운 DRM 콘텐츠로 변환하기에는 기술적으로 정책적으로 어려움이 따른다.

복수의 DRM 툴 설치 구조 방안은 특정 DRM 콘텐츠를 처리하도록 사용자 디바이스에 DRM 모듈을 실시간으로 다운로드하고 설치하는 방안이다. 이 방안은 작은 컴퓨팅 능력을 가진 PDA나 MP3 플레이어의 경우 복수개의 DRM 시스템이 동시에 구동되는 데에 따른 리소스의 부족을 고려해야 하고 DRM 시스템간의 충돌 또한 무시할 수 없다.

상호 연동 방안은 각기 다른 DRM 시스템 간 DRM 콘텐츠를 변환하거나 연결할 수 있는 모듈을 이용하여 상호 호환을 지원하는 방안이다. 이 방안은 각 DRM은 고유의 솔루션을 지원할 수 있고 사용자에게는 호환성을 지원할 수 있다. 상이한 DRM은 각각 고유 형식의 DRM 콘텐츠를 사용하고 있는 것으로 가정되며, 상이한 DRM간 상호 연동은 DRM의 주요 데이터인 메타데이터, 사용권한, 리소스에 대해 연동이 될 수 있도록 고려되어야 한다. 즉, DRM의 주요 데이터에 대한 연결 요소로 작용하기 위해서 메타데이터, 사용권한, 리소스에 대한 암호화 방법 각각에 대해 중립적 메타데이터, 사용권한 표현 언어, 리소스 암호화 방법이 요구된다. 이들 데이터의 변환을 통해 상호 연동 방안은 상이한 DRM 시스템간의 DRM 콘텐츠의 안전한 전송을 위한 연결요소로 작용하여 서로 다른 형식의 DRM 콘텐츠가 상호 연동되도록 할 수 있다.

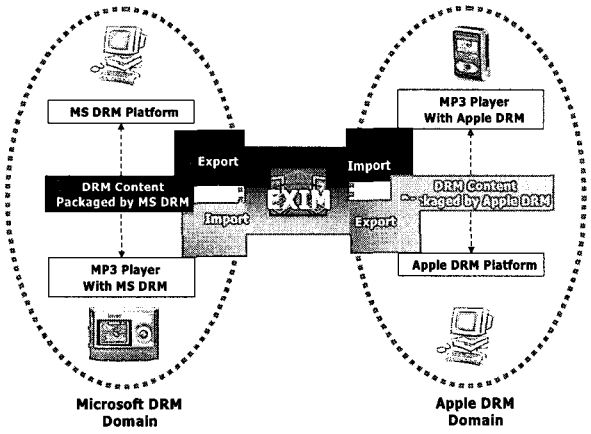
3. DRM 상호 호환성 지원을 위한 상이한 DRM 간 연동 방안 (EXIM)

본 논문은 상이한 DRM간 DRM 콘텐츠의 반출(Export) 및 반입(Import)을 통한 연동 방안(EXIM, EXport/IMport)을 제안한다. 제안하는 방안은 서로 다른 형식의 DRM 콘텐츠를 상호 반출/반입(Export/Import)하기 위해서 공개된 중립적인 DRM 콘텐츠인 EXIM 콘텐츠 형식을 설정하고 EXIM 콘텐츠를 매개로 하여 상이한 DRM사이에서 DRM 콘텐츠의 연동이 이루어지도록 한다(그림 1 참조).

자신의 DRM 콘텐츠를 반출하려는, 즉 콘텐츠와 사용권한을 가지고 있는 DRM을 소스 DRM이라고 하고, 소스 DRM 으로부터 콘텐츠와 사용권한을 받아 사용하려고 하는 DRM을 타겟 DRM이라고 하면 소스 DRM과 타겟 DRM 간 연동은 다음과 같다. 소스 DRM은 탑재된 EXIM 모듈을 통해 자신의 DRM 콘텐츠를 EXIM 콘텐츠로 변환한 후 타겟 DRM으로 이를 반출한다. EXIM 콘텐츠는 타겟 DRM 에 탑재된 EXIM 모듈을 통해 반입되고 최종적으로 타겟 DRM은 EXIM 콘텐츠를 자신의 DRM 콘텐츠로 변환하여 사용하게 된다. 중립 포맷으로 사용되는 EXIM 콘텐츠는 전달받은 타겟 DRM에서 타겟 DRM 콘텐츠로 변환 과정에서만 이용된다.

각 DRM은 자신의 DRM 콘텐츠와 공개된 중립 포맷의 EXIM 콘텐츠간 상호 변환(Adaptation)하는 모듈을 추가적

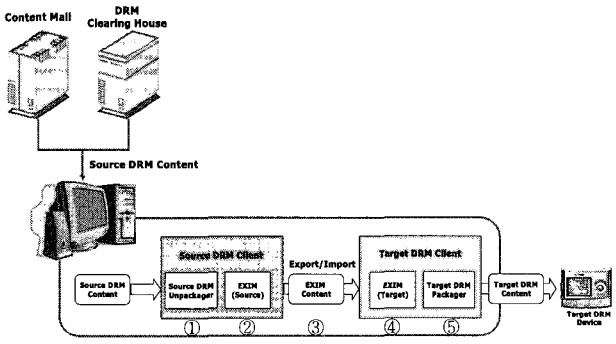
으로 탑재하고, 소스 DRM과 타겟 DRM에서 콘텐츠의 Export/Import를 위해 공개된 API를 지원함으로써 DRM 콘텐츠 연동을 통해 상이한 DRM간 콘텐츠 상호 호환을 실현할 수 있다.



(그림 1) 상이한 DRM간 연동 개념도

3.1 EXIM 프로세스

상이한 DRM간 연동시 상호 반출/반입을 위해 공개된 중립적인 DRM 콘텐츠(EXIM 콘텐츠) 형식을 설정하고 이를 중심으로 DRM의 주요 데이터인 메타데이터, 사용권한, 암호화된 리소스 세 가지에 대해 연동 과정을 수행한다. 이를 위한 EXIM 프로세스는 아래와 같다(그림 2 참조).



(그림 2) EXIM 프로세스

• 소스 DRM 측 프로세스

① 소스 DRM 은 자신의 DRM 콘텐츠를 언패키징하여 메타데이터, 사용권한, 원본 리소스를 추출하는 과정

② 메타데이터, 사용권한, 원본 리소스를 이용하여 중립 포맷 DRM 콘텐츠로 패키징하는 과정

③ 중립 포맷 DRM 콘텐츠를 타겟 DRM으로 Export하는 과정

• 타겟 DRM 측 프로세스

④ 소스 DRM으로부터 Import한 중립 포맷 DRM 콘텐츠를 언패키징하여 메타데이터, 사용권한, 원본 리소스를 추출하는 과정

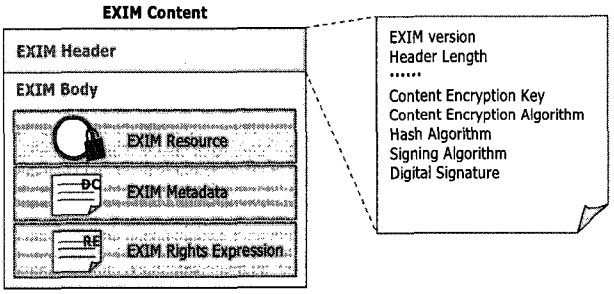
⑤ 추출된 메타데이터, 사용권한, 원본 리소스를 타겟 DRM 고유의 DRM 콘텐츠형태로 패키징 후 해당 기기에 전송하는 과정

3.2 EXIM 콘텐츠

상이한 DRM사이에서 DRM 콘텐츠의 연동이 이루어지도록 공개된 중립적인 DRM 콘텐츠 형식이 EXIM 콘텐츠이다. 각 DRM은 이를 이용하여 자신의 고유한 DRM 콘텐츠에 대한 정보를 공개하지 않고서 상호 연동을 수행할 수 있다.

EXIM 콘텐츠는 헤더(Header)와 바디(Body)로 구성되며 헤더에는 Version, Length, Hash value, Algorithms, Encrypted resource encryption key, Digital signature 등의 값을 명시한다. 바디에는 리소스 변환, 사용권한 변환, 메타데이터 변환의 처리결과가 각각의 형식에 따라 저장된다 (그림 3 참조).

해쉬 코드와 전자서명 부분을 제외한 헤더와 바디에 대해 해쉬 값이 계산되어 헤더의 해쉬 영역에 기록된다. 소스 DRM은 자신의 비밀키(Private key)를 이용하여 해쉬 코드 정보를 전자서명하고, 이를 전자서명 필드에 기록한다. 타겟 DRM은 소스 DRM의 공개키(Public key)를 이용하여 전자서명을 확인함으로써 해쉬 코드의 무결성을 체크하고, 다시 해쉬 코드를 이용하여 헤더와 바디의 무결성을 확인할 수 있다.



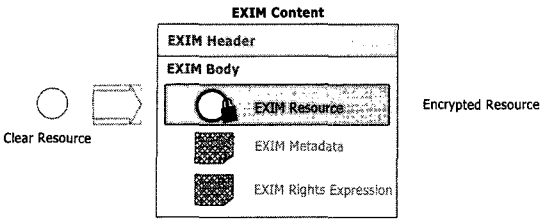
(그림 3) EXIM 콘텐츠 구조

3.2.1 리소스 변환

리소스 변환 과정은 소스DRM으로부터 받은 원본 리소스를 중립 포맷 DRM 콘텐츠의 암호화된 리소스로 만들거나 역으로 이를 복호화하여 타겟 DRM에서 원본 리소스로 만드는 과정이다.

소스 DRM의 DRM 콘텐츠는 리소스 보호를 위해 자신의 암호화 방식으로 원본 콘텐츠를 암호화하고 있다. 이 암호화된 리소스가 타겟 DRM에서 이용되기 위해서는 타겟 DRM 고유의 암호화 방식으로 변환되는 것이 필요하다.

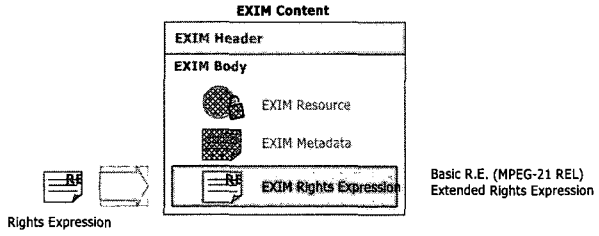
소스 DRM은 자신의 고유 DRM 콘텐츠로부터 원본 리소스를 추출하고 소스측 EXIM 모듈은 EXIM에서 지원하고 있는 암호화 방식에 따른 임의의 암호화 키를 생성하고, 이를 이용하여 원본 리소스를 암호화 한다. 암호화된 리소스는 EXIM 콘텐츠를 구성하는 요소로 삽입되고, 리소스 암호화에 사용된 키는 타겟 DRM과의 키 공유 방법에 따라 EXIM 콘텐츠의 구성 요소로 안전하게 전달되게 된다(그림 4 참조).



(그림 4) 리소스 변환

3.2.2 사용권한 변환

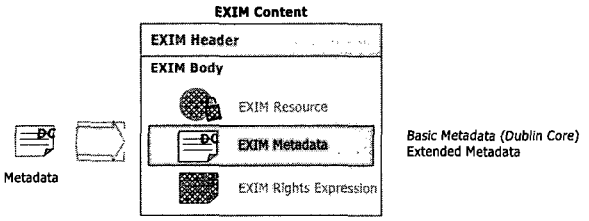
사용권한 변환 과정은 소스 DRM과 타겟 DRM에 종속적이지 않은 중립적인 사용권한 표현으로 변환하는 과정이다. 소스 DRM과 타겟 DRM은 중립적인 사용권한 표현의 범위 내에서 사용권한을 상호 연동할 수 있게 된다. 중립적인 사용권한 표현으로 MPEG-21 REL이나 ODRL을 이용할 수 있다(그림 5 참조).



(그림 5) 사용권한 변환

3.2.3 메타데이터 변환

메타데이터 변환 과정은 각 DRM 고유의 메타데이터를 중립적인 메타데이터로 변환하는 과정이다. 중립적인 메타데이터로 Dublin Core를 기본으로 하며 Dublin Core에서 정의되지 않은 메타데이터는 Dublin Core가 기술된 XML 문서에 확장 영역을 만들고, 그 안에 삽입하도록 한다. 확장 영역에 삽입된 메타데이터는 이를 인지하는 DRM 시스템에서만 이용할 수 있다. 중립적인 메타데이터로 변환되는 내용은 소스 DRM 및 타겟 DRM 의 정책 또는 메타데이터의 종류에 따라 가감될 수 있다(그림 6 참조).



(그림 6) 메타데이터 변환

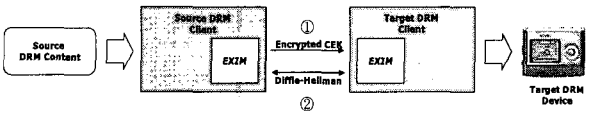
3.3 콘텐츠 암호화 키 교환

소스/타겟 EXIM 모듈은 상대방에게 전달하는 메시지(또는, 데이터)를 암호화하여 메시지의 유출이나 공격 시도에 대해 안전하게 보호할 수 있도록 한다. 이를 수행하기 위한 선행 과정으로 암호화에 필요한 암호화 키를 서로 공유해야 하는데, 키 교환 채널의 안전성에 관한 문제로 인해 직접적인 키 교환 방식은 바람직하지 못하며 아래와 같은 두 가지 방식을 고려할 수 있다(그림 7 참조).

① DRM모듈마다 인증서를 발급하여 비대칭 키를 이용하여 암호화 키를 전달하는 방식

② Diffie-Hellman 알고리즘과 같이 키를 교환하지 않더라도 양측에서 동일한 키를 생성하는 방식

위 알고리듬은 소스 DRM과 타겟 DRM간에 협의를 할 수 있으며 협의된 알고리듬은 EXIM 콘텐츠 내에 명시한다.



(그림 7) 콘텐츠 암호화 키 교환

3.3.1 인증서 기반 키 교환 방식

소스 DRM과 타겟 DRM간의 안전한 콘텐츠 전송을 위하여 PKI방식을 이용한다. 즉, 소스 DRM과 타겟 DRM은 PKI기반 키쌍을 이용하여 콘텐츠 암호화키 전송 및 무결성 보장을 지원한다. 콘텐츠 암호화키 전송을 위해 소스 DRM은 자체적으로 생성한 콘텐츠 암호화 키를 타켓 DRM의 공개키로 암호화 한다. 그리고, 무결성 보장을 위해 소스 DRM은 자신의 비밀키(Private key)를 이용하여 해쉬 코드 정보를 전자서명하고, 이를 전자서명 필드에 기록한다. 이를 위해 필요한 기본 알고리듬은 아래와 같다

- 키 전송 및 무결성 보장: 비대칭 암호화 알고리듬 (RSA)
- Resource의 암호화 알고리듬: 대칭 암호화 알고리듬 (AES-128)
- Hash 알고리듬: SHA-1

3.3.2 Diffie-Hellman 기반 키 교환 방식

Diffie-Hellman 키 교환 방식을 이용하여 공개키 키 암호화 프로토콜로 양측에서 보안성을 보장받을 수 없는 일반 통신채널을 통해 공동의 보안을 설정할 수 있게 한다. Diffie-Hellman방식으로 콘텐츠 암호화 키를 생성하여 콘텐츠 암호화 키(CEK)를 공유함으로써 콘텐츠를 안전하게 전송한다. 또한, 무결성 보장을 위해 해쉬 값의 산출 방식은 EXIM 헤더와 EXIM 바디를 기반으로 산출하는 점은 인증서 기반 방식과 동일하나 해쉬 값을 CEK로 암호화하여 전송하고 해쉬 값의 복호화를 통하여 자체적으로 산출한 해쉬 값과 비교하여 무결성을 검증한다. 이를 위해 필요한 기본 알고리듬은 아래와 같다

- 키 전송 및 무결성 보장: Diffie-Hellman
- Resource의 암호화 알고리듬: 대칭 암호화 알고리듬 (AES-128)
- Hash 알고리듬: SHA-1

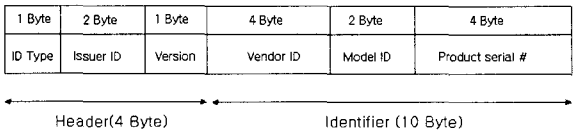
3.4 디바이스 식별자(Device Identification)

모든 디바이스는 유일하게 식별될 수 있는 식별자를 가져

야 하며, 이는 디바이스 인증서를 디바이스 내에 탑재하는 방식을 이용할 수도 있고, 디바이스가 가지고 있는 Vendor ID, Product ID, Serial Number 등을 이용하여 서버에서 식별자를 생성 후 발급하는 방식을 이용할 수도 있다.

3.4.1 디바이스 정보 기반 디바이스 식별자

디바이스 정보 기반 디바이스 식별은 Vendor ID, Model ID, Product Serial Number와 같은 정보를 이용하여 디바이스에 대한 식별자를 생성하는 방법이다. 디바이스에 관련된 정보를 이용하여 특정 디바이스에 대한 유일한 식별자를 생성하고 관리하는 역할을 디바이스 식별자 서버가 수행하게 된다. 디바이스 식별자는 헤더 부분과 식별자 부분으로 나누어 구성되며 아래 그림과 같이 구성된다(그림 8 참조).

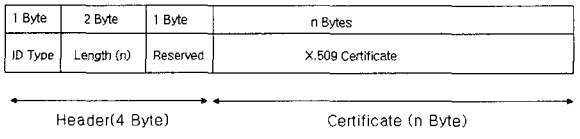


(그림 8) 디바이스 정보 기반 디바이스 식별자 포맷

- ID Type(1 byte): 디바이스 식별자 종류(0x00~0xFF)
- Issuer ID (2 bytes): 디바이스 식별 서버 ID (0x0000~0xFFFF)
- Version (1 byte): 식별자 포맷 버전 (0x00~0xFF)
- Vendor ID (4 bytes): 디바이스 제조사 ID (0x00000000~0xFFFFFFFF)
- Model ID (2 bytes): 제품 모델 ID (0x0000~0xFFFF)
- Product Serial # (4 bytes): 제품 시리얼 번호 (0x00000000~0xFFFFFFFF)

3.4.2 디바이스 인증서 기반 디바이스 식별자

디바이스 인증서 기반 디바이스 식별은 디바이스 식별 서버에서 X.509 인증서를 생성하고 이 인증서를 디바이스에 저장하는 방식이다. X.509 인증서는 디바이스 식별자를 전달하기 위한 수단으로 이용되며 인증서의 DN(Distinguished Name)을 디바이스 식별자로 사용한다. 디바이스 식별자는 헤더 부분과 식별자 부분으로 나뉘어 구성되며 식별자 부분에 인증서가 이용된다(그림 9 참조).



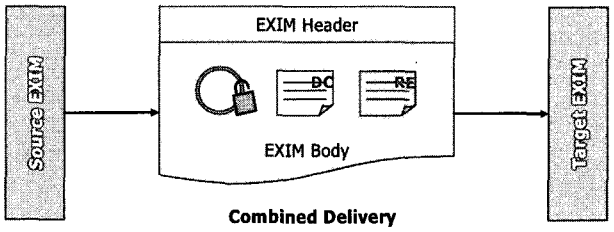
(그림 9) 디바이스 인증서 기반 디바이스 식별자 포맷

- ID Type (1 byte): 디바이스 식별자 종류 (0x00~0xFF)
- Length (2 bytes): 인증서 길이 (0x0000~0xFFFF)
- Reserved (1 byte): Not used
- X.509 Certificate (n bytes): X.509 데이터. 인증서 내의 DN을 디바이스 식별자로 사용

3.5 EXIM 콘텐츠 전달

EXIM 콘텐츠를 하나의 EXIM 헤더와 EXIM 바디로 구성하고 소스 EXIM에서 타겟 EXIM으로 전달하는 컴바인드 전달 방식(Combined delivery)을 사용한다(그림 10 참조).

EXIM 헤더에 필요한 헤더 정보를 추가하고, 각각의 EXIM 바디 항목들의 위치를 명시하여 분리할 수 있도록 하고, 컴바인드된 헤더와 바디에 대하여 해쉬 코드의 계산과 전자서명을 수행한 결과를 삽입하여 EXIM 콘텐츠의 무결성을 제공한다. EXIM 바디는 리소스, 메타데이터, 사용권한을 EXIM 리소스, EXIM 메타데이터, EXIM 사용권한으로 표현하여 EXIM 바디를 구성하도록 한다.



(그림 10) EXIM 콘텐츠 전달

3.6 DRM 연동 제어

반출/반입(Export/Import) 과정은 서로 다른 두 DRM 시스템의 경계를 넘어서 DRM 콘텐츠가 전달되는 과정이므로 정책에 따라, 또는 기술적 한계나 필요에 따라 이 과정의 수행 여부를 통제할 수 있어야 한다. 소스 DRM은 타겟 DRM의 DRM 소프트웨어와 디바이스에 대한 정보를 획득하고 이 정보를 이용하여 자신의 콘텐츠를 타겟 측에 반출할지를 결정하여 DRM간 연동을 제어 한다(그림 11 참조). 연동 제어의 대상은 다음과 같다.

① DRM 소프트웨어 (vendor, product, version)

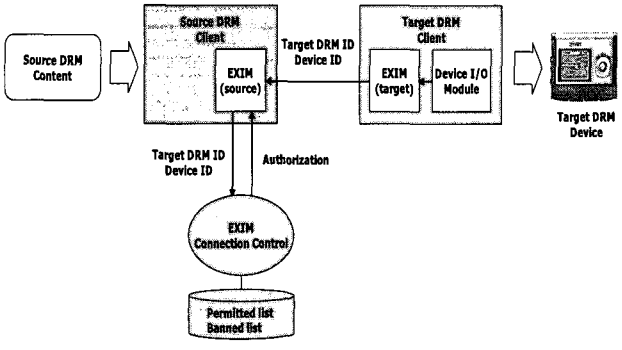
② 디바이스 (vendor, model, version)

각 연동 제어 대상에 대한 제어 방법은 다음과 같은 목록에 따라 수행할 수 있다.

① 허가 목록(Permitted list)

② 금지 목록(Banned list)

연동 제어의 대상 및 방법은 주기적으로 혹은 필요에 따라 서버로부터 업데이트 받을 수 있다.



(그림 11) DRM 상호 연동 제어

4. 결 론

오늘날 상용화된 DRM 제품들은 많이 있으나 DRM간 호환성이 없는 상태이고, DRM의 호환성 보장을 위해 DRM 표준화에 대한 요구가 증대되고 있으나 DRM 표준으로서 지배적 위치의 표준이 마련되지 않아 호환성 문제를 해결하지 못하고 있는 상태이다. 이와 같은 DRM 기술의 비호환성으로 인하여 사용자의 불편이 증대되고 디지털 콘텐츠 유통 또한 제한된 범위로 제약을 받고 있다.

이러한 문제점을 해결하기 위하여 DRM의 끊김없는 서비스 환경을 제공할 수 있는 DRM 호환성 충족이 필요하다. 이를 위한 DRM 상호 호환 기술로서 본 논문은 상이한 DRM간 DRM 콘텐츠의 반출(Export) 및 반입(Import)을 통한 연동 방안(EXIM)을 제안한다. 제안하는 방안은 공개된 중립적인 DRM 콘텐츠(EXIM 콘텐츠) 형식을 설정하고 이를 중심으로 DRM의 주요 데이터인 메타데이터, 사용권한, 리소스를 연동하여 N-to-N 관계의 복잡한 DRM들이 상호 호환성을 유지 할 수 있다.

참 고 문 헌

[1] IMPRIMATUR Business Model, Version2.1, June, 1999, Available at http://www.imprimatur.net

[2] ISO/IEC JTC 1/SC 29/WG 11 MPEG/ N3939 Information technology- Multimedia framework(MPEG-21)- Part 1: Vision, Technologies and Strategy, Jan., 2001.

[3] J. E. Cohen, "DRM and Privacy," Communications of the ACM, Vol.46, No.4, Apr., 2003.

[4] D. K. Mulligan, J. Han, and A. J. Burstein, "How DRM-Based Content Delivery Systems Disrupt Expectations of Personal Use," Proceedings of the 2003 ACM Workshop on Digital Rights Management, pp.77~88, Oct., 2003.

[5] T. S. Messerges and E. A. Dabbish, "Digital rights management in a 3G mobile phone and beyond," Proceedings of the 2003 ACM workshop on Digital rights management, pp.27~38, Oct., 2003.

[6] L. J. Camp, "First Principles of Copyright for DRM Design," Internet Computing, IEEE, Vol.7, pp.59~65, 2003.

[7] N. Rump, "Can digital rights management be standardized?," IEEE Signal Processing Magazine, Vol.21, No.2, pp.63~70, Mar., 2004.

[8] R. H. Koenen, J. Lacy, M. Mackay, and S. Mitchell, "The long march to interoperable digital rights management," Proceedings of the IEEE, Vol.92, No.6, pp.883~897, Jun., 2004.

[9] A. U. Schmidt, O. Tafreschi, and R. Wolf, "Interoperability challenges for DRM systems, In International Workshop for Technology," Economy, Social and Legal Aspects of Virtual Goods, Ilmenau, Germany, 2004.

[10] Digital Media Project(DMP) / No. DMP057, Portable Audio/Video IED Requirement, Apr., 2004.

[11] Digital Media Project(DMP) / No. DMP403, Approved Document No.3- Technical Specification: Interoperable DRM Platform, Apr., 2005.

정 연 정

e-mail : yjjeong@etri.re.kr

1994년 부산대학교 전자계산학과(학사)

1996년 부산대학교 전자계산학과(석사)

2005년 충남대학교 컴퓨터과학과(박사)

1996년~현재 한국전자통신연구원 선임연구원

관심분야 : 정보보호, DRM

윤 기 송

e-mail : ksyoon@etri.re.kr

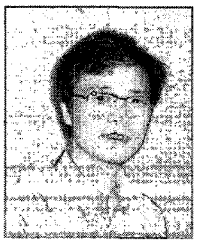
1994년 부산대학교 조선공학과(학사)

1988년 City University of New York 전산학과(석사)

1993년 City University of New York 전산학과(박사)

1993년~현재 한국전자통신연구원 책임연구원

관심분야 : 정보보호, 저작권 보호, 분산처리



강 호 갑

e-mail : hgkang@drminside.com

1985년 성균관대학교 전자공학과(학사)

1988년 성균관대학교 전자공학과(석사)

1991년~2000년 삼성SDS 책임연구원

2000년~2003년 파수닷컴 연구소장

2004년~2004년 헤라수 연구소장

2005년~현재 디알엠인사이드 연구소장

관심분야 : DRM, CBD