

사용자 및 디바이스 기반의 도메인 관리

변영배 추헌곤 최범석 남제호

한국전자통신연구원(ETRI) 방통융합콘텐츠보호연구팀

*byun@etri.re.kr

Domain Management based on User and/or Device

YoungBae Byun, HuonGon. Choo, BumSuk Choi, JeHo Nam

ETRI, Broadcasting Media Research Group

요약

본 논문에서는 사용자 및 디바이스 기반의 도메인을 구현하고, 그 관리 방법에 대해서 논의하였다. 도메인 구성에 사용자와 디바이스를 동시에 포함시킨 것과 각 사용자가 사용할 수 있는 디바이스들을 정의할 수 있고, 반대로 디바이스를 사용할 수 있는 사용자를 한정 정의할 수 있다는 것이 특징이다. 본 논문에서 제안하는 사용자 및 디바이스 기반의 도메인을 적용하면, 사용자와 디바이스를 기반으로 서버 도메인을 구성하여 라이선스를 발급할 수 있기 때문에 폭 넓은 라이선스 정책을 수립할 수 있다.

1. 서론

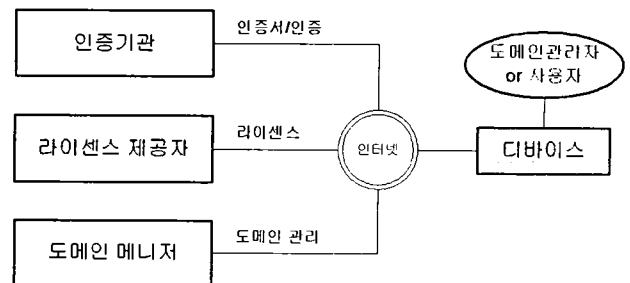
디지털 방송환경의 도입으로 다양한 형태의 서비스가 가능해짐과 동시에 부가적인 요구사항들이 발생하게 되었다. 디지털화는 콘텐츠 제작, 유통 및 소비 구조에 획기적인 변화를 유발시킴으로써, 고화질, 다채널, 다기능의 서비스 제공에 많은 변혁을 가져왔다. 앞으로의 디지털 방송은 콘텐츠 자체만을 일방적으로 내보내는 방식에서 발전하여 데이터 방송, 대화형 방송 환경으로 발전될 것이다. 또한 상대적으로 넓은 대역폭을 지니는 방송 환경은 인터넷을 통한 서비스에 비해 고품질, 고화질의 방송콘텐츠 제공이 가능하다. 그러나 디지털 콘텐츠는 아날로그와 비교하여 접근, 전달, 편집 및 보관이 용이하고 전파 또는 통신망 등을 통한 배포 과정에서 데이터의 열화가 없다는 장점이 있다. 하지만 이러한 장점은 디지털 콘텐츠의 '저작권의 보호'라는 새로운 문제점을 낳게 되었다[1].

디지털 방송콘텐츠의 저작권을 보호하면서 사용자의 이용에 대한 편리성을 도모하기 위해서는 콘텐츠를 패키징하고 그 패키징에 사용된 키를 라이선스에 포함시켜 사용자에게 전달하는 과정이 요구된다 [2,3]. 각 사용자가 여러 개의 디바이스를 보유하고 있기도 하고, 가정이나 학교 등과 같은 그룹의 구성원들이 함께 디지털 콘텐츠를 즐기길 원한다는 사실의 현실적인 필요성을 만족시키기 위해서 도메인이라는 개념을 도입하고, 도메인에 한정된 라이선스를 발급하거나 도메인 내의 일부 디바이스에게만 사용권한을 허가하는 라이선스를 발급하기도 하였다. 그런데, 종래 기술은 각 사용자별, 또는 디바이스별로 라이선스를 발급하는 방법에 한정되어 왔다[4].

본 논문은 사용자와 디바이스 그룹, 사용자만의 그룹, 또는 디바이스만의 그룹으로 서버도메인을 구성하여 라이선스를 발급하거나, 특정 사용자, 디바이스, 또는 특정 사용자가 특정 디바이스에서만 콘텐츠를 사용할 수 있도록 라이선스를 발급할 수 있는 사용자 및/또는 디바이스 기반의 도메인 개념을 도입하여 보다 폭 넓은 라이선스 정책을 도출할 수 있는 서비스 환경을 개발하였다.

2. 시스템 구성도

사용자 및 디바이스 기반의 도메인 관리와 도메인 및 서버도메인에 입각한 라이선스 발급에 필요한 전체 시스템 구성도는 그림 1과 같다. 인증기관은 도메인의 요소인 사용자와 디바이스의 인증서를 발급하는 기관이고, 라이선스 제공자(License Provider)는 디지털 콘텐츠를 유통하는 서비스 제공자(Service Provider)의 내부 프로세스으로써, 콘텐츠의 사용에 필요한 라이선스를 발급하는 역할을 담당하고, 도메인 매니저는 사용자 및 디바이스를 도메인에 포함시키거나 제거하는 작업과 라이선스 제공자가 라이선스 제작에 필요한 도메인 키, 사용자 키 및 디바이스 키를 전달하는 기능을 담당한다.



[그림 1] 시스템 구성도

3. 사용자 및 디바이스 기반의 도메인

가. 도메인 구성 요소

사용자 및 디바이스 기반의 도메인 구성 요소로는 사용자와 디바이스가 있다. 특히 사용자 중에서 하나의 도메인을 생성하거나 사용자 및 디바이스를 도메인에 포함시키거나 삭제하는 등의 도메인을 관리하기 위한 모든 작업을 총괄로 수행하는 사용자를 도메인 관리자라 한다. 하나의 도메인에는 반드시 한 명 이상의 도메인 관리자를 포함해야

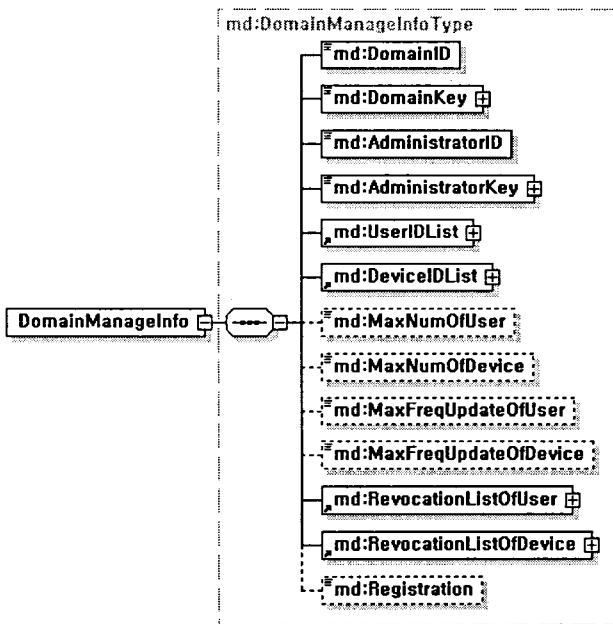
하고, 한 사용자가 여러 도메인의 관리자가 될 수 있으며, 도메인 관리자에겐 도메인 사용자 및 디바이스에서 이용한 콘텐츠의 사용에 관한 모든 결재 의무를 부여한다.

도메인 사용자는 한 도메인에 포함되어 그 도메인에 포함된 디바이스 중에서 자신에게 허용된 디바이스를 사용하여 콘텐츠를 소비할 수 있도록 허용된 사용자를 의미한다.

도메인 디바이스는 도메인에 포함된 디바이스로서, 각 디바이스에는 도메인 사용자 중에서 한 명 이상의 사용자에게 할당되어야 한다. 만약, 할당된 사용자가 없을 경우에는 해당 디바이스의 사용 권한은 일시 정지 상태가 된 것으로 간주될 수 있다.

나. 도메인 리소스

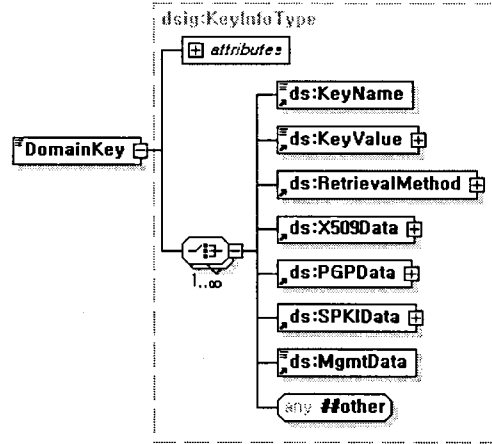
하나의 도메인이 생성되면 도메인 매니저는 그림 2와 같은 도메인 관리 정보(DMI:Domain Manage Infomation)이라는 정보를 생성하여 관리하게 된다.



[그림 2] 도메인 매니저의 정보

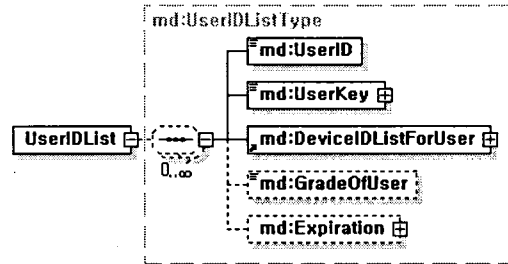
DMI에 포함된 각 항목은 다음과 같다.

- ① DomainID : 각 도메인에 중복되지 않게 할당되는 ID로써 새로운 도메인의 등록과 함께 부여되며, 도메인 등록이 취소(해지)될 때까지 관리된다.
- ② DomainKey : 도메인의 키는 그림 3에 도시한 바와 같은 구조로 정의된 것으로써, 도메인 등록과 함께 도메인 매니저가 생성한다. 이 키는 관리를 위하여 필요한 경우 갱신 가능하다. 도메인 키는 도메인 인증서로 대처할 수도 있고, 단순히 도메인의 비대칭 키쌍을 저장하여 관리하여도 된다.
- ③ AdministratorID : 모든 도메인에는 한 명 이상의 도메인 관리자를 등록해야 하고, 이 도메인 관리자에게 중복되지 않게 할당된 ID로서 새로운 도메인 등록과 함께 부여되며, 향후 도메인 관리시 사용자 확인에 사용하는 ID이다.
- ④ AdministratorKey : 도메인 관리자가 도메인 등록 시에 입력한 키로서, 도메인 관리시 관리자 확인에 사용할 암호이다.

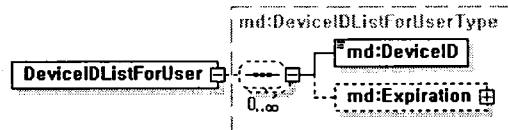


[그림 3] 도메인 키

- ⑤ UserIDList : 사용자 ID 목록은 그림 4에 도시한 바와 같이 도메인에 포함된 사용자들의 ID 목록이다. 이 목록에 포함된 DeviceIDListForUser는 그림 5에 도시한 바와 같이 해당 사용자가 사용할 수 있도록 허락된 도메인 디바이스의 ID 목록을 의미한다.

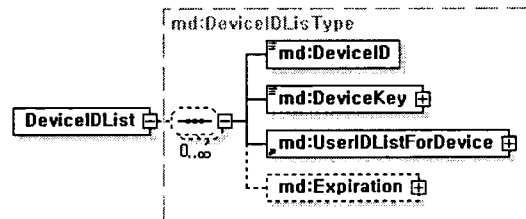


[그림 4] 사용자 ID 목록



[그림 5] 사용이 허락된 디바이스 목록

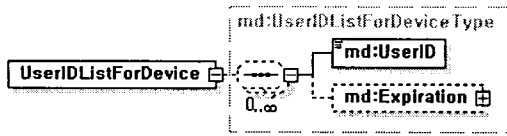
- ⑥ DeviceIDList : 디바이스 ID 목록은 그림 6에 도시한 바와 같이 도메인에 포함된 디바이스들의 ID 목록이다. 이 목록에 포함된 UserIDListForDevice는 그림 7에 도시한 바와 같이 해당 디바이스를 사용할 수 있도록 허락된 도메인 사용자의 ID 목록을 의미한다.



[그림 6] 디바이스 ID 목록

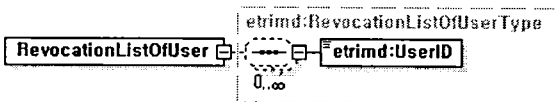
- ⑦ MaxNumOfUser : 이 항목은 하나의 도메인에 포함시킬 수 있는 최대 사용자의 수이다. 이것은 사용자와 콘텐츠 서비스 제공

자간의 계약에 의해서 한정될 수도 있다.

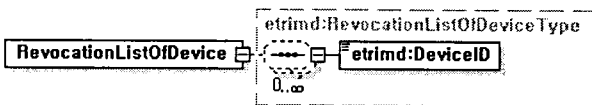


[그림 7] 사용이 허가된 사용자 목록

- ⑧ MaxNumOfDevice : 이 항목은 하나의 도메인에 포함시킬 수 있는 최대 디바이스의 수이다. 이것은 사용자와 콘텐츠 서비스 제공자간의 계약에 의해서 한정될 수도 있다.
- ⑨ MaxFreqUpdateOfUser : 너무 빈번하게 도메인 사용자를 포함시키거나 제거하는 변경을 가할 경우 도메인 매니저에 부하가 발생할 수도 있으므로 도메인 사용자 갱신 빈도수를 제한할 때 사용한다. 이 항목도 사용자와 콘텐츠 서비스 제공자간의 계약에 의해서 변경될 수 있다.
- ⑩ MaxFreqUpdateOfDevice : 너무 빈번하게 도메인 디바이스를 포함시키거나 제거하는 변경을 가할 경우 도메인 매니저에 부하가 발생할 수도 있으므로 도메인 디바이스 갱신 빈도수를 제한할 때 사용한다. 이 항목도 사용자와 콘텐츠 서비스 제공자간의 계약에 의해서 변경될 수 있다.
- ⑪ RevocationListOfUser : 도메인에 포함시킨 사용자를 도메인으로부터 제거하였을 경우 그림 8에 도시한 바와 같이 사용자 ID를 이 목록에 추가하여 관리하게 된다.
- ⑫ RevocationListOfDevice : 도메인에 포함시킨 디바이스를 도메인으로부터 제거하였을 경우 그림 9에 도시한 바와 같이 디바이스 ID를 이 목록에 추가하여 관리하게 된다.
- ⑬ Registration : 새로이 도메인을 생성하여 등록한 일시를 저장한다.



[그림 8] 도메인에서 삭제된 사용자 목록



[그림 9] 도메인에서 삭제된 디바이스 목록

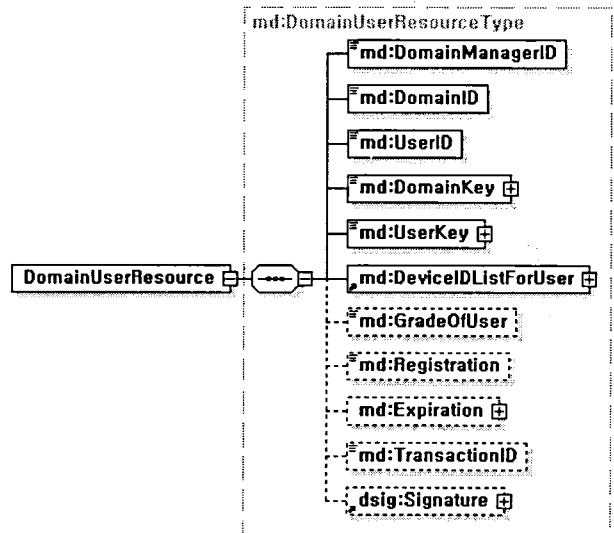
DMI는 도메인 관리자가 서비스 제공자와의 계약에 의해서 도메인을 새롭게 등록할 때 생성되고, 계약을 파기함으로써 제거된다. 한 명의 사용자가 복수의 서비스 제공자와의 계약에 의해서 여러 개의 도메인을 생성할 수 있고, 각각의 도메인을 관리하기 위해서는 각각의 DMI에 등록되어 있는 도메인 관리자 ID와 패스워드를 사용한다. 도메인 관리자가 콘텐츠를 사용하기 위해서는 한 명의 도메인 사용자 등록해야만 하고, 도메인 관리자도 도메인 사용자 리소스를 가지게 된다.

다. 도메인 사용자 리소스

사용자를 도메인에 포함시키기 위해서는 도메인 관리자가 도메인 매니저에게 사용자를 도메인에 포함시켜야 가능하다. 이 때 도메인 매니저는 그림 10에 도시한 바와 같은 도메인 사용자의 리소스를 생성하

여 도메인 관리자에게 전달하게 되고, 도메인 관리자는 도메인 사용자에게 전달해야 한다.

도메인 사용자 리소스에는 그림 10에 도시한 바와 같이 11개 항목으로 구성되는데, 특히 DeviceIDListForUser란 해당 도메인 사용자가 사용할 수 있게 허락된 도메인 디바이스의 목록으로서, 그림 5에서 설명한 것과 같이 허락된 도메인 디바이스의 DeviceID를 포함하고 있다. 이 디바이스의 목록은 새롭게 도메인 사용자를 등록할 때 지정하여도 되고, 나중에 별도로 지정하여도 된다. 만약, 도메인 사용자가 사용할 수 있는 도메인 디바이스를 할당하고 싶지 않을 경우에는 GradeOfUser를 이용하여 행하여도 된다.



[그림 10] 도메인 사용자 리소스

라. 도메인 디바이스 리소스

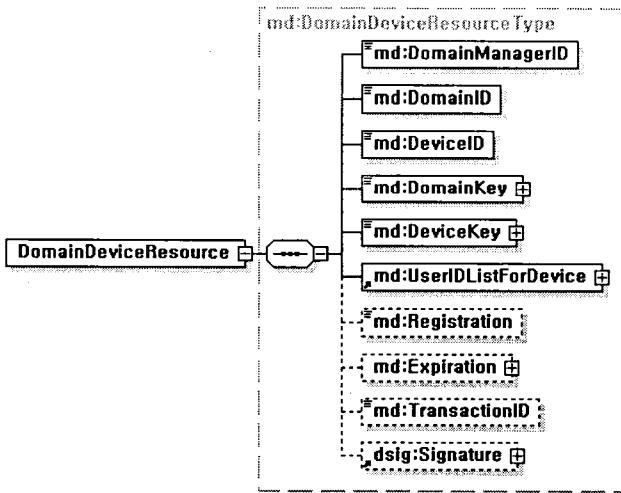
네트워크가 지원되는 디바이스를 도메인에 포함시키기 위해서는 도메인 관리자가 해당 디바이스를 이용하여 도메인 매니저에게 도메인에 포함시키면, 도메인 매니저는 그림 11에 도시한 바와 같은 도메인 디바이스 리소스를 생성하여 해당 디바이스에게 전달하게 된다. 만약, 네트워크가 지원되지 않는 디바이스를 도메인에 포함시키기 위해서는 도메인 관리자가 도메인 매니저가 제공하는 디바이스 정보 추출 유틸리티를 이용하여 해당 디바이스의 정보를 추출하여 디바이스의 등록을 행한다. 그리고 도메인 매니저가 발행한 도메인 디바이스 리소스를 도메인 관리자가 해당 디바이스에 입력해야 한다.

도메인 디바이스 리소스에는 그림 11에 도시한 바와 같이 10개 항목으로 구성되는데, UserIDListForDevice란 해당 도메인 디바이스를 사용할 수 있도록 허가한 사용자의 목록으로써, 그림 7에서 설명한 것과 같이 허락된 도메인 사용자의 UserID 등을 포함하고 있다. 이 사용자의 목록은 새롭게 도메인 디바이스를 등록할 때에 지정하여도 되고, 나중에 별도로 지정하여도 된다.

DeviceKey는 도메인 매니저가 제공한 디바이스 정보 추출 유틸리티에 의하여 추출된 특정 정보를 이용하여 암호화되어 보관될 수도 있다. 즉, 도메인 디바이스 리소스를 역세스하려면 이 특정 정보를 이용해야하기 때문에 해당 디바이스 내에서만 유효하게 된다.

그림 10에 설명한 것과 같이 사용자의 등급(GradeOfUser)을 정의하여 사용할 경우는 디바이스의 등급도 정의할 수 있다. 해당 디바이스를 사용할 수 있는 사용자들이 해당 디바이스를 사용할 때, 그 사용자

의 등급에 따라 디바이스의 등급을 정의할 수 있다.

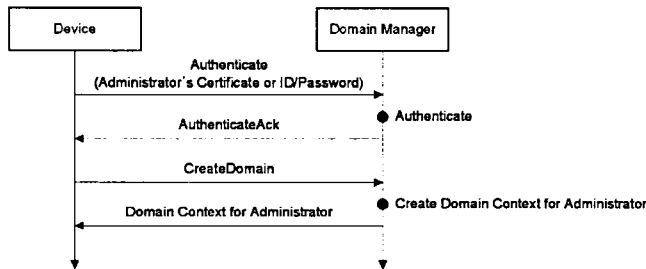


[그림 11] 도메인 디바이스의 리소스

4. 도메인 관리

가. 도메인 등록

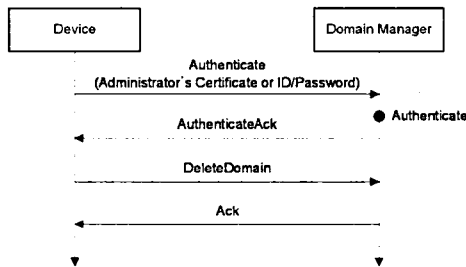
도메인을 생성하기 위해서는 그림 12에 도시한 것과 같이 도메인 관리자가 도메인 매니저에게 요구한다. 도메인 매니저는 도메인을 생성한 후에 도메인 관리자의 도메인 사용자 리소스를 생성하여 전달한다. 즉, 도메인 관리자의 도메인 사용자 리소스는 도메인 등록과 함께 생성되어 부여받는다.



[그림 12] 도메인 등록 절차

나. 도메인 삭제

그림 13에 도시한 것과 같이 도메인 관리자가 도메인 매니저에게 도메인 삭제를 요구한다. 도메인이 삭제되면 해당 도메인에 포함된 모든 사용자 및 디바이스의 도메인 리소스는 무효한 정보가 된다.



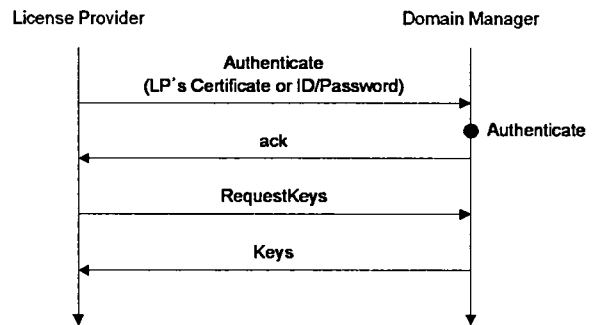
[그림 13] 도메인 삭제 절차

다. 라이선스 서버와 도메인 매니저 간의 통신 절차

라이선스 제공자가 도메인에 관계된 라이선스를 발급하기 위해서

는 도메인, 사용자, 및 디바이스의 키가 필요하다. 만약 도메인 내에 포함된 모든 사용자가 모든 디바이스에서 콘텐츠를 사용할 수 있는 라이선스를 발급할 경우는 콘텐츠 키를 해당 도메인의 공개키로 암호화하여 라이선스에 포함시켜 사용자에게 전달하면 된다. 어느 한 사용자가 그가 사용할 수 있는 모든 디바이스에서 사용할 수 있게 하기 위해서는 콘텐츠 키를 해당 사용자의 공개키로 암호화한 후에 그 암호화된 키를 다시 해당 도메인의 공개키로 암호화하여 전달하면 된다. 이와 반대로 특정 디바이스에서 그 디바이스를 사용할 수 있는 모든 사용자가 사용할 수 있게 할 경우는 해당 디바이스의 공개키로 콘텐츠 키를 암호화한 후에 도메인의 공개키로 암호화하여 전달하면 된다. 한 사용자가 그가 사용할 수 있는 특정 디바이에서만 사용하게 할 경우는 해당 디바이스의 공개키로 암호화하고, 다시 해당 사용자의 공개키로 암호화한 후에 도메인의 공개키로 암호화하여 전달하면 된다.

위에 제시한 예와 같이 도메인에 포함된 사용자와 디바이스를 이용하여 임의의 수의 사용자 또는 임의의 수의 디바이스를 그룹으로 구성한 후 서브도메인을 구성하여 라이선스를 발급할 수 있다. 이는 곧 다양한 라이선스 정책을 수립할 수 있는 방법을 제공할 수 있다는 것이다.



[그림 14] 라이선스 제공자와 도메인 매니저간의 통신 절차

5. 결론

본 논문에서는 사용자 및 디바이스 기반의 도메인 관리에 대해서 소개하였다. 제안한 도메인 개념의 특징은 도메인의 구성에 대해서 사용자와 디바이스를 포함시킨 것과 특정 사용자가 사용할 수 있는 디바이스를 정의할 수 있는 방법을 제시한 것과, 특정 디바이스에도 그 디바이스를 사용할 수 있는 방법을 제시한 것이다. 또한 라이선스 발급 시에 사용자와 디바이스를 동시에 사용하거나 일부만 사용함으로써 보다 많은 자유도를 부여할 수 있는 장점을 가진다. 본 논문에서 제안한 도메인 개념을 이용하면 폭넓고 다양한 유통 정책을 수립할 수 있다.

[참고문헌]

- [1] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding", IBM System Journ., Vol 35, Nos 3&4, 1996.
- [2] William Rosenblatt, William Trippe, Stephen Mooney: Digital Rights Management: Business and Technology, Paperback (2001)
- [3] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum, Frank L.A.J. Kamperman: A DRM security architecture for home networks, PP11 - 21, DRM'04 (2004)
- [4] DMP, Approved Document No.3 - Technical Specification, Interoperable DRM Platform (IDP-1), www.dmpf.org