단말적응형 방송콘텐츠 보호관리를 위한 라이센스 관리 방법

추현곤 *고병수 남제호

한국전자통신연구원 방통융합콘텐츠보호연구팀

*(주)디지캡

hyongonchoo@etri.re.kr, bskoh@digicaps.com, namjeho@etri.re.kr

License Management for Device-adaptable Proctection and Management of Broadcasting Contents

Hyon-Gon Choo *Byongsu, Ko Jeho Nam

ETRI, Broadcasting Media Research Group

*Digicaps Inc.

요약

디지털 방송기술의 발달과 더불어 컴퓨터 및 단말 기술의 발전은 방송콘텐츠에 대한 활용 범위를 증대시키고 있다. 본 논문에서는 다양한 단말기기에서의 안전한 방송콘텐츠의 이용 및 보호관리를 위한 라이센스 정책 및 관리방법을 제시한다. 제안하는 방법은 수신단말과 단말에 접근이 가능한 사용자 및 디바이스를 하나의 도메인으로 묶고, 각각의 도메인에서의 사용자 및 디바이스 정보를 이용한 다양한 비즈니스 모델에 활용 가능한 라이센스 발급 정책 및 접근 방법을 제시하며, 도메인과 사용 정보에 대한 라이센스를 위한 키 관리 방법을 정의한다.

1. 서론

디지털 방송 기술의 발달과 더불어 컴퓨터 및 단말 기술의 발전은 방송콘텐츠에 대한 활용 범위를 증대시키고 있다. 현재 대부분의 방송콘텐츠는 지상파, 위성 및 케이블, DMB 등의 여러 방송망을 통하여 셋탑, 핸드폰과 같은 다양한 단말에서 시청이 가능하며, 각 방송사의 인터넷 서비스를 통해 PC 등을 통해 스트리밍 서비스를 받을 수 있다. 이와 더불어 일반 사용자들이 손쉽게 방송콘텐츠를 재가공, 생산, 유통시킬 수 있게 되어, 이에 따른 방송콘텐츠에 대한 기술적인 보호관리 기술 역시 대두되고 있는 상황이다. 이러한 방송콘텐츠의 보호관리와 관련하여, 디지털 콘텐츠의 저작권 보호, 관리, 유통을 위한 기술 체계인 DRM(Digital Rights Management) 및 IPMP(Intellectual Property Management and Protection) 기술의 연구 및 관련 표준화가 전세계적으로 진행 중에 있다 [1][5].

DRM 및 IPMP 보호관리를 위한 시스템에 있어서, 사용자가 자신이 보유 또는 구매한 콘텐츠의 사용 권한에 대한 표현을 담고 있는 것이 라이센스이다. 라이센스를 통해 사용자는 본인이 구매한 정보를 확인하고, 원하는 콘텐츠를 사용하기 위한 키와 같은 보안 및 인증에 필요한 도구 및 정보를 얻을 수 있다 [1][2]

대부분의 DRM 기술에서 사용되는 라이센스에서는, 수요자가 구입한 콘텐츠와 라이센스의 내용에 따라 하나의 기기 또는 특정 사용자에 대해 재생만을 지원한다. 홈네트워크와 같은 환경에서도 네트워크에서 지원하는 라이센스를 통해 등록된 모든 기기에서 사용을 지원하도록 함에 따라, 라이센스에 대한 제한 및 관리에 어려움을 보이게 된다. 따라서 여러 단말로 구성된 네트워크 및 도메인과 같은 환경에서의 동시 지원 및 특정 환경에서의 제한 등의 다양한 정책에 활용함에 있어서 제약을 가진다.

본 논문에서는 다양한 단말기기에서의 방송콘텐츠의 안전한 이용 및 보호관리를 위한 라이센스 정책 및 관리방법을 제시한다. 제안하는 방법은 수신단말과 단말에 접근이 가능한 사용자 및 디바이스를 하나의 도메인으로 묶고, 각각의 도메인에서의 사용자 및 디바이스 정보를 이용한 다양한 비즈니스 모델에 활용이 가능한 라이센스 발급 정책 및 접근 방법을 제시하며, 도메인과 사용 정보에 대한 라이센스를 위한 키 관리 방법을 정의한다. 구현 및 실험을 통해 제안하는 방법의 효율성을 확인할 수 있다.

2. 단말적응형 방송콘텐츠 보호관리를 위한 라이센스 관리

본 장에서는 여러 이종단말 환경으로 구성된 도메인 상에서의 방송콘텐츠 보호관리를 위한 라이센스 관리 및 키 관리 방법에 대해서 다룬다. 먼저 방송콘텐츠를 중심으로 이종단말 환경으로 구성된 도메인인 홈도메인에 대해서 설명한 후, 홈도메인에서의 라이센스에 대해서 기술한다.

가. 홈도메인

홈도메인(Home Domain)이란 하나의 셋탑과 그 셋탑에 속한 사용자 및 디바이스의 그룹으로써, 툴 및 방송콘텐츠를 공유할 수 있는 집단을 의미한다. 방송콘텐츠에 있어서 홈도메인의 구별은 방송수신단말인 셋탑(또는 수신장치 보유 단말)을 기준으로 한다. 즉, 하나의 수신단말을 기준으로 하나의 홈도메인을 구성하고, 각 도메인에는 여러

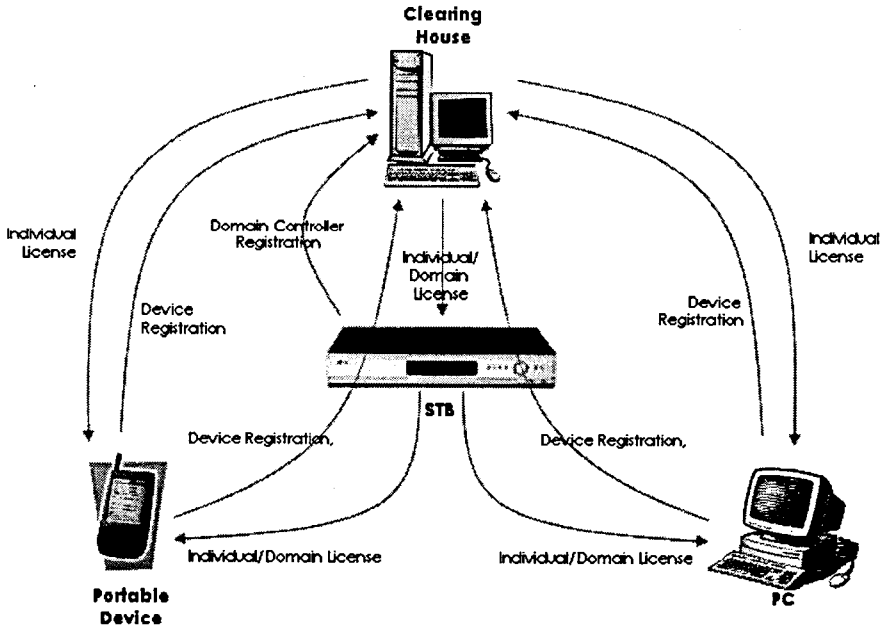

그림 1 . 홈도메인의 구성

사용자 및 디바이스를 포함한다. 그림1은 하나의 셋탑(STB)를 기준으로한 휴대단말 및 PC로 구성된 홈도메인의 예를 보여준다.

나. 홈도메인에서의 라이센스

홈도메인에서의 라이센스 발급과 관리는 그림 1에서 보는 바와 같이 홈도메인의 수신단말이 등록된 클리어링 하우스 또는 유통서버를 통해 이뤄진다. 홈도메인 내에서 사용되는 모든 방송콘텐츠는 도메인에 등록된 디바이스 및 사용자에 대해서만 사용이 가능하며, 이에 대한 정보는 클리어링 하우스를 통하여 관리된다. 홈도메인에서의 방송콘텐츠의 사용을 위해, 라이센스에서는 사용하고자 하는 콘텐츠 정보 및 콘텐츠에 대한 유통 정보 및 사용자, 디바이스 및 도메인 정보, 그리고 콘텐츠를 사용하기 위한 복호화 키를 포함한다.

다. 라이센스 형식에 따른 사용 정책

종래의 DRM 기술에서 사용되는 라이센스에서는, 수요자가 구입한 콘텐츠와 해당 콘텐츠를 위한 라이센스의 내용에 따라 하나의 기기 또는 특정사용자에 대해서만 재생이 가능하였다.

라이센스는 콘텐츠의 사용을 기간, 횟수 등을 한정하여 라이센스를 발급할 수 있는데, 클리어링 하우스에 저장된 홈도메인과 사용자 디바이스의 정보를 이용하여 다양한 비즈니스 모델을 구현할 수 있다. 다양한 사용자와 디바이스의 관리의 측면에서 다음과 같은 사용 규칙을 라이센스에 적용할 수 있다.

먼저 방송콘텐츠에 대한 가장 간단한 사용에 대한 정책은 사용자 및 디바이스에 대한 제약이다. 표1에서 보는 바와 같이 도메인에 등록된 특정 사용자 또는 디바이스에 대해서 규정할 수 있다. 각각의 사용자 ID 및 Device ID는 복수개로 정의될 수 있으며, 정의되지 않을 경우, 모든 경우에 대해서 permission이 주어진 경우이다.

Item	Value	Description
User	NULL	제한된 사용자만 이용가능
	User ID	도메인 내의 모든 사용자에게 허용
Device	NULL	제한된 장치에만 이용 가능
	Device ID	도메인 내의 모든 장치 이용 가능

표 1. 라이센스에 따른 방송콘텐츠 사용 정책 1- simple cases

라이센스 정책은 사용자와 디바이스 개념의 조합에 따라 표2와 같이 확장되어 사용될 수 있다.

Value		Description
User	Device	
NULL	NULL	도메인 내의 모든 사용자가 도메인 내의 모든 장치를 이용 가능
NULL	Device ID	도메인 내의 모든 사용자가 한정된 장치만을 이용 가능
User ID	NULL	제한된 사용자에 대해 모든 장치를 이용 가능
User ID	Device ID	제한된 사용자에 대해 제한된 장치를 허용

표 2. 라이센스에 따른 방송콘텐츠 사용 정책 2- composite cases

라. 홈도메인에서의 라이센스 관리

1) 라이센스의 발급

홈도메인에서의 라이센스 발급은 수신단말이 등록된 라이센스 관리 서버를 통해 이뤄진다. 먼저 도메인에 등록된 수신단말 등을 통해 해당하는 방송콘텐츠의 콘텐츠 정보와 사용자 및 디바이스 정보를 제공한

다. 이를 바탕으로 방송콘텐츠의 서비스 제공자가 등록한 콘텐츠에 관한 유통정보를 바탕으로 사용자 및 디바이스 정보를 포함하여 라이센스를 생성하여 발급한 후, 사용 디바이스에 전송한다. 본 논문에서는 라이센스 발급에 필요한 사용자 및 디바이스에 관련된 인증 문제는 다루지 않는다.

2) 콘텐츠 이동에 따른 라이센스 정보의 관리

서로 다른 이종의 단말을 위한 방송콘텐츠의 이동은 라이센스 내에 표현된 콘텐츠의 사용정보(grant)에서 허용되는 범위에 제한된다. 수신단말에 저장 녹화된 방송콘텐츠에 대하여, 라이센스에 콘텐츠이동에 관한 권한이 보장되어 있을 경우, 라이센스 정보로부터 가능한 변환에 대한 범위를 검색한다. 이 변환에 관한 정보 등은 MPEG-21 REL 및 TV-Anytime RMPI에서 정의한 변환 정보를 활용할 수 있다 [3][4]. 그림 2는 TV-Anytime RMPI의 ExtendRights에 대한 스키마를 보여준다 [4]. TV-Anytime RMPI의 ExtendRights에서는 각각의 변환되는 권한과 이에 따른 보안레벨 및 부가 속성 등에 대해 정의할 수 있다.

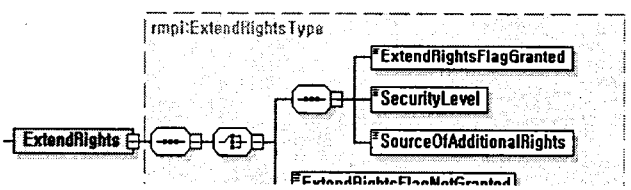

그림 2. TV-Anytime RMPI의 ExtendRights [4]

마. 라이센스를 위한 키 관리

방송콘텐츠의 유통관리에 있어서 라이센스의 가장 중요한 사용 목적 중 하나는 방송콘텐츠를 위한 보호 키(Key)의 관리에 있다. 본 논문에서는 홈도메인에 등록된 여러 사용자 및 단말에서의 선별적인 복호화 키의 사용을 위한 키 관리 방법을 제시한다.

먼저 라이센스 내에 콘텐츠의 복호화 키 또는 복호화를 위한 정보는 도메인에 등록된 사용자(User)와 디바이스의 공개키로 암호화 한다. 이를 위해 클리어링 하우스에서는 1차로 사용자 및 디바이스 의 공개키로 암호화 한 후, 그 정보 및 순서를 xml과 같은 별도의 파일형식으로 저장한다. 2차로 홈도메인의 공개키로 암호화된 라이센스와 순서정보를 암호화하여 전송한다. 만약 도메인에 등록된 모든 사용자 및 디바이스를 통해 사용을 원할 경우, 1단계는 생략한다. 복호화 과정을 위한 순서 정보 생성에는 제한이 없다.

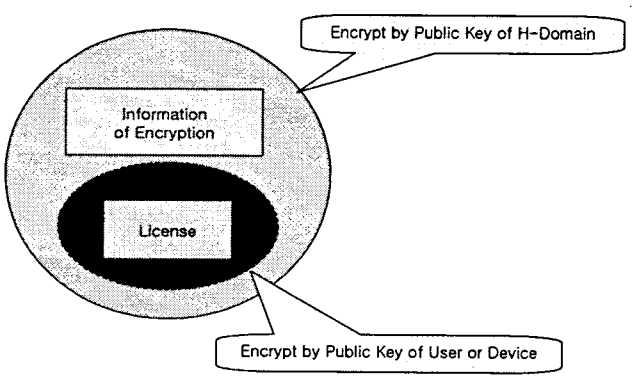

그림 3. 라이센스에서의 키 관리 방법

그림 3은 홈도메인의 라이센스를 이용한 복호화 키 관리에 대한 개괄적인 설명을 나타낸다.

도메인의 키를 이용하여 콘텐츠에 대한 키를 암호화함으로서, 주어진 도메인에서의 사용을 보장하며, 또한 내부에 특정 사용자 및 디바이스에 대한 키를 이용하여, 원하는 정보를 원하는 대상에서만 사용가능하도록 할 수 있다.

3. 구현 및 실험

본 논문에서 제안하는 다양한 라이센스 관리 방법을 위해, 클리어링 하우스에 해당하는 유통서버 및 방송수신단말, 그리고 PC 및 휴대단말을 이용하여 도메인을 구성하였다.

그림 4 는 라이센스의 발급을 위한 라이센스 등록에 대한 예를 보여준다. 콘텐츠의 사용을 위한 금액 및 권한 정보, 라이센스 발급을 위한 서버 주소 등을 설정이 가능하다.

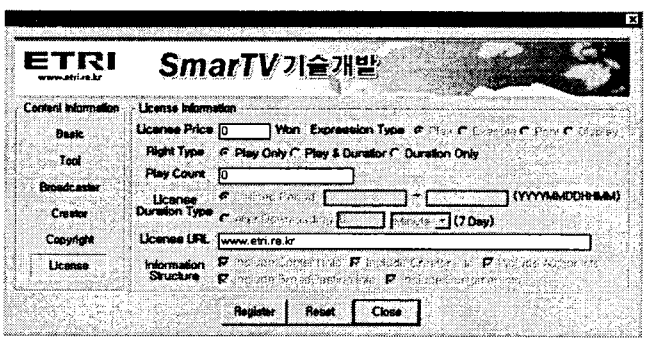

그림 4. 라이센스 등록

그림 5 는 라이센스 등록과정을 통해 생성된 라이센스에 대한 예를 보여준다. 본 논문의 실험에서 라이센스의 포맷(Format)은 MPEG21 REL 규격을 기반으로 하였다 [3]. 그림 5의 라이센스에서는 도메인에서 사용하는 장치에 대한 규격 및 콘텐츠 ID 및, 라이센스 갱신 및 유효기간 등에 대한 정보를 포함하고 있다. 그림 5의 라이센스를 통해 라이센스에서 정의된 도메인의 여러 단말에 대해서 방송콘텐츠의 안전한 재생이 가능하다.

4. 결 론

본 논문에서는 다양한 단말기기에서의 방송콘텐츠의 안전한 이용 및 보호관리를 위한 라이센스 정책 및 관리방법을 제시하였다. 제안하는 방법은 수신단말과 단말에 접근이 가능한 사용자 및 디바이스를 하나의 도메인으로 묶고, 각각의 도메인에서의 사용자 및 디바이스 정보를 이용한 다양한 비즈니스 모델에 활용이 가능한 라이센스 발급 정책 및 접근 방법을 제시하였으며, 도메인과 사용 정보에 대한 라이센스를 위한 키 관리 방법을 정의하였다. 제안하는 방법을 통해, 하나의 수신단말과 여러 이종 단말로 구성된 도메인에서의 방송콘텐츠의 권리가 보장된 이용이 가능하다. 그러나, 제한하는 방법은 하나의 도메인에서의 방송콘텐츠에 대하여 적용이 가능하나, 여러 도메인 또는 도메인 그룹에 대한 적용에는 한계를 가진다. 추후 도메인 키와 결부된 그룹키 관리에 대한 연구를 통해 이러한 문제를 해결하기 위한 방법을 연구할 예정이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<license xmlns="urn:mpeg:mpeg21:2003:01-REL-R-NS"
xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS"
xmlns:mx= "urn:mpeg:mpeg21: 2003:01-REL-MX-NS"
xmlns:dsig= "http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc= "http://www.w3.org/2001/04/xmlenc#"
xmlns:xsi= "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation ="urn:mpeg:mpeg21:2003:01-REL-MX-NS rel-mx.xsd">
<inventory>
        <licenseID>userid_category_type_0000000007</licenseID>
        <contentID>userid_category_0000000007</contentID>
        <toolID>markany support</toolID>
        <nonSecureIndirect URI="http://lis.itcontents.com/no_license.asp?cId=kbs_doc_hd_0000000007"/>
</inventory>
<otherInfo>...</otherInfo><!-- Additional Contents Infomation will be added -->
<grant>
        <mx:play/>
        <mx:diReference>
                <mx:identifier>urn:grid:a1-abcde-1234567890-f</mx:identifier><!-- STB/SAV/PAV-->
        </mx:diReference>
        <keyHolder> <!-- Domain Public Key -->
                <info>
                        <dsig:KeyValue>
                                <dsig:RSAKeyValue>
                                        <dsig:Modulus>KtdToQQyzA==</dsig:Modulus>
                                        <dsig:Exponent>AQABAA==</dsig:Exponent>
                                </dsig:RSAKeyValue>
                        </dsig:KeyValue>
                </info>
        </keyHolder>
        <dsig:KeyInfo>      <!-- Encrypted Domain Key using STB/SAV/PAV Public Key-->
                <xenc:EncryptedKey>
                        <xenc:EncryptionMethod xenc:Algorithm=
                           "http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                <xenc:CipherData>
                                <xenc:CipherValue>Base64_encoded_EncryptedDomainKey</xenc:CipherValue>
                        </xenc:CipherData>
                </xenc:EncryptedKey>
        </dsig:KeyInfo>
        <allConditions>
                <validityInterval><!-- ValidInterval: 7days -->
                        <notBefore>2005-08-01T00:00:00</notBefore>
                        <notAfter> 2005-08-08T00:00:00</notAfter>
                </validityInterval>
                <sx:exerciseLimit><!-- Exercise limit: 5times-->
                        <sx:count>5</sx:count>
                </sx:exerciseLimit>
                <sx:ValidityIntervalDurationPattern>    <!-- validation interal duration: every 3 days-->
                        <sx:duration>P3D</sx:duration>
                </sx:ValidityIntervalDurationPattern>
                <sx:ValidityFloating>        <!-- 3days from first execution-->
                                <sx:duration>P3D</sx:duration>
                </sx:ValidityFloating>
                <sx:fee>                        <!-- Flat fee: 10,000. -->
                        <sx:paymentFlat>
                                <sx:rate> 10000 </sx:rate>
                                <sx:currency> KRW </sx:currency>
                        </sx:paymentFlat>
                </sx:fee>
        </allConditions>
</grant>
</license>
```

그림 5 . 라이센스의 예

5. 참고문헌

[1] Keith Hill, "A perspective: the role of identifiers in managing and protecting intellectual property in the digital age," Proceedings of the IEEE, vol. 87, No. 7, pp.1228 - 1238, July 1999.

[2] Z. Jiang, L.Bin, Z. Li and Y. Shi-Qian, "License Management Scheme with Anonymous Trust for Digital Rights Management," ICME2005, pp.257-260, July 2005.

[3] Information technology - Multimedia framework(MPEG-21)- Part 5: Rights Expression Language, ISO/IEC 21000-5:2004(E), 2004.

[4] Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV Anytime"); Part 5: Rights Management and Protection (RMP) Sub-part 1: Information for Broadcast Applications, ETSI TS 102 822-5-1 V1.2.1, June, 2005

[5] Digital Media Project, "Interoperable DRM Platform Specification (Phase I)," dmp0440, 15 April 2005.