http://dx.doi.org/10.7236/JIIBC.2013.13.1.205
JIIBC 2013-1-28

EPUB 기반 전자책 DRM의 상호호환성을 지원하는 라이선스 발급 방법에 관한 연구

A Study of License acquisition Method Supporting Mutual Compatibility of EPUB-based eBook DRM

김태현*, 강호갑**, 김윤호***, 조성환****

Tae-Hyun Kim, Ho-Gap Kang, Yoon-Ho Kim, Seong-Hwan Cho

요 약 한국저작권위원회의 CT R&D 과제로 진행되고 있는 EPUB DRM 호환성 기술 연구((과제명 : 국제표준의 EPUB 기반 전자책 DRM 표준 레퍼런스 소프트웨어 기술 개발)는 2011년 전자책 시장의 사실상표준으로 자리매김을 하고 있는 EPUB 표준을 기반으로 암호화 및 전자서명 프로파일 표준안과 인증서 프로파일 표준안, 그리고 권리정보 용어에 대한 표준안을 개발하였다. 이들 4개의 표준안들은 각각 '전자책 DRM 암호화 명세서', '전자책 DRM 전자서명 명세서', '전자책 DRM 인증서 명세서', '전자책 DRM 권리용어 정의' 라는 제목으로 전자출판물표준화포럼(ODPF)과 한국정보통신기술협회(TTA)를 통해 2012년 국내 산업표준으로 제정이 완료되었다. 그러나 전자책 DRM 표준 제정에도 불구하고 라이선스 발급 또는 교환에 대한 호환성을 보장하는 표준 기술의 부재로 서로 다른 전자책 유통사들에 의해서 유통된 전자책의 이용은 불가능한 상태이다. 본 논문에서는 상기 4개의 전자책 DRM 표준을 기반으로 전자책 DRM의 상호호환성을 지원하는 라이선스 발급 방법에 대하여 기술적인 접근 방법을 살펴보고, 산업적으로 허용되는 범위에서의 기술적 모델을 제시하도록 한다.

Abstract The study of the compatibility of EPUB DRM, granted by the Korea Copyright Commission, as a CT R & D project (Project Title: Development of standard reference software technology for the International Standard EPUB-based eBook DRM) developed standards such as profile standards for encryption, digital signature and authentication certificates and standards for technical terms of rights information. In 2012, these four standards have been established as the Korean Industrial Standards under the names of 'Encryption specification for EPUB DRM,' 'the Digital signature specification for EPUB DRM,' 'the Certificate specification for EPUB DRM,' and 'Definitions of Right Terms for EPUB DRM' through the ODPF(Open Digital Standardization Forum) and the TTA(Telecommunications Technology Association). In spite of the establishment of the eBook DRM standards, however, the absence of the standard technology which supports the compatibility for issues and changes of licenses makes it unable to use eBooks served by different eBook distributors. This study tries to investigate technological approaches to methods of license issues supporting eBook DRM compatibility on the basis of the above-mentioned four EPUB DRM standards and to provide an industrially accepted technological model.

Key Words : EPUB, 저작권 보호기술, DRM, 라이선스 발급, 상호호환성

*정회원, 디알엠인사이드
**정회원, 디알엠인사이드
***정회원, 상명대학교
****정회원, 금강대학교
접수일자 2013년 1월 9일, 수정완료 2013년 2월 6일
게재확정일자 2013년 2월 8일

Received: 9 January 2013 / Revised: 6 February 2013 / Accepted: 8 February 2013
*Corresponding Author: thkim@drminside.com
CTO, DRM inside, Korea

I. 서 론

전자책은 출판물의 보관에 필요한 공간적인 제약이 없고, 네트워크를 통해 유통이 간편하며, 도서 열람 시 다양한 부가정보를 함께 사용할 수 있다는 장점이 있기 때문에 음악 및 동영상에 이어 차세대 콘텐츠 산업계를 주도할 핵심 콘텐츠로 주목받고 있다. 이런 전자책의 산업적인 가능성을 반영하여 2007년 9월 IDPF (International Digital Publishing Forum)에서는 전자책 기술규격으로 EPUB(Electronic Publication)이라는 표준을 발표하였고, 2011년 10월에는 EPUB 3.0을 발표하여 PDF형태가 주류를 이루고 있는 전자책에 새로운 기술표준을 제시하고 있다[1]. IDPF의 기술 표준화에 힘입어 2009년 이후부터 스마트 패드기기를 포함한 다양한 모바일 기기들이 EPUB 포맷을 지원하는 전자책 열람 소프트웨어를 탑재하여 출시하고 있고, 국내외 전자책 서비스 제공자들도 대부분 EPUB을 필수 지원 포맷으로 제공하고 있는 추세에 있어 이제 EPUB은 산업적인 표준으로 자리매김하고 있다.

그러나 전자책은 디지털콘텐츠의 특성상 기술적 보호조치가 없는 상태에서 콘텐츠가 유통될 경우, 상품화 과정에서 관계자들에 의한 부주의나 또는 일부 소비자들의 불법복제를 통해 인터넷을 매개체로 무차별 재배포 될 수 있기 때문에 저작권자들은 서비스 사업자들이 DRM과 같은 강력한 기술적 보호조치가 전자책의 불법복제를 방지하기 위한 수단으로 사용되기를 요구하고 있다.

그러나 전자책을 포함해서 디지털콘텐츠 전반에 걸쳐 사용되고 있는 기술적 보호조치들은 관련 표준이 마련되기 전에 이미 상용 DRM 기술이 개발되어 있었고, 대부분의 전자책 서비스 사업자들은 저작권 보호의 필요에 따라 기존 상용 DRM 기술을 사용할 수밖에 없었다. 결과적으로 EPUB 표준이 확산되기 이전에 이미 전자책 서비스 업체들은 업체별로 통일되지 않은 DRM 기술을 사용할 수밖에 없었다. 이러한 와중에 IDPF의 EPUB 표준이 발표되고 EPUB에서 권장하는 보호기술이 공표 되었지만 서비스 사업자들은 지금껏 문제없이 사용해온 기존 솔루션을 제거하고 IDPF 방식을 즉시 수용하기란 쉽지 않은 상황이다. 또한 EPUB 표준을 채용했다 하더라도 EPUB 표준 보호 기술 명세서에서 권장하고 있는 W3C XML Encryption[2]과 Signature[3]의 적용 방법이 다양하고, DRM 솔루션 제공업체들의 표준 이해 방식에 차이가 있어 구현된 방식들이 상호 연동될 수 있을 정도의 호환성을 지원하지 못했다. 또한 EPUB 표준안 항목에서 제외된 권리정보 부분에 대해서는 DRM 솔루션 업체 별로 다른 구현 방식을 사용하고 있기 때문에 표준과는 더욱 멀어지게 되었다. 이는 EPUB 표준이 적용된 전자책임에도 불구하고 소비자들은 두 곳 이상의 서비스 업체로부터 전자책을 구매하였을 경우에 복수개의 전자책 열람 소프트웨어를 사용해야하는 불편을 감수해야 하는 결과를 초래할 수밖에 없었다[4].

이러한 문제점을 해결하기 위해 EPUB DRM 호환성 기술 연구는 사실상 산업표준이 되고 있는 EPUB 표준 포맷을 기반으로 W3C XML Encryption과 XML Signature 대한 프로파일 표준안을 마련하여 기존 DRM 솔루션업체들의 표준 구현 부담을 줄일 수 있도록 하였고, ITU-T X.509[5]를 기반으로 전자책 DRM의 인증서 프로파일 표준안을 작성하여 IDPF EPUB에는 언급이 없었던 인증서의 기술규격을 개발하였다. 또한 특허문제로 IDPF에서조차 표준을 정하기 어려워하고 있는 권리관리 정보 표준에 대해서도 다양한 종류의 권리표현언어가 사용되더라도 전자책에서 사용될 때 공통된 표준 의미가 사용되도록 하기 위해 권리관리정보 용어에 대한 표준안을 마련하였다. 이들 4개의 표준안들은 전자출판물표준화포럼(ODPF)[6]과 한국정보통신기술협회(TTA)[7]의 표준화 작업을 거쳐 각각 '전자책 DRM 암호화 명세서'[10][13], '전자책 DRM 전자서명 명세서'[11][14], '전자책 DRM 인증서 명세서'[12][15], '전자책 DRM 권리용어 정의'[9][16] 라는 제목으로 2012년 국내 표준으로 제정되었다.

그러나 이러한 표준화 노력에도 불구하고 사용자들이 자신들이 선호하는 하나의 도서 열람 소프트웨어를 통해 복수의 서비스 사이트로부터 도서를 구매할 수 있는 진정한 의미의 호환성이 지원되기까지는 여전히 해결되지 않은 문제가 남아있다. 이는 기술적으로 한 서비스사업자로부터 발급된 라이선스 정보(키 정보, 권리관리정보)가 타 서비스사업자가 지원하는 전자책 열람 장치에서도 유효하게 작동될 수 있어야 하는데, 서비스 사업자들을 포함하여 DRM 솔루션 사업자들이 보안적인 이유에서 자신들이 발행한 전자책 라이선스 정보를 타 DRM 솔루션에서 사용하는 것을 허락하지 않으려 하기 때문에 발생되는 문제이다. 상기에서 설명된 문제점을 해결하기 위해서는 전자책에 사용되는 라이선스를 발급하는 DRM 서버와 DRM 클라이언트간의 프로토콜에 대한 표준이

필요하지만 이 조차도 보안적인 이슈로 인해 표준화가 어려웠다.

본 논문에서는 이러한 문제점을 해결하기 위해 2011년 한국저작권위원회의 EPUB DRM 호환성 기술 연구과제로 진행된 4개의 전자책 DRM 표준을 기반으로 전자책 DRM 라이선스 발급 프로토콜에 대한 기술적인 접근 방법을 살펴보고, 산업적으로 허용되는 범위에서의 기술적 해결 모델을 제시하도록 한다.

II. 호환성을 지원하는 전자책 라이선스 발급 방법

전자책 DRM에서 사용되는 라이선스는 불법복제를 방지하기 위한 목적으로 암호화를 풀 수 있는 복호화 키와 권리관리정보를 기술해 놓은 것으로, 전자책 콘텐츠가 사용자 기기로 전달되었을 때 서비스사업자가 허용한 범위에서만 전자책의 이용을 제어하는 용도로 사용된다. 라이선스에 대한 호환성은 라이선스를 요청하는 DRM 클라이언트와 라이선스를 발급하는 DRM 서버 측면에서 고려될 수 있는데, 일반적인 경우 서버와 클라이언트간의 라이선스 프로토콜에 대한 표준이 결정될 경우 라이선스 발급에 대한 호환이 보장된다고 할 수 있다. 그러나 서비스 사업자가 보안적인 이유로, 또는 현재 사용되고 있는 기존 프로토콜에 대한 변경 부담이 있기 때문에 적용에 따른 산업적 비용이 적게 들고 프로토콜 공개에 대한 위험이 낮은 방식이 요구된다.

그림 1은 전자책 서비스 사업자가 각각 자신들의 고유한 프로토콜을 이용하여 전자책 DRM 라이선스를 발급하는 서로 다른 서비스 사업자간의 라이선스 호환을 보여주는 개념도이다. 호환 방법으로 고려될 수 있는 방식은 이기종 서버와 클라이언트 간에 발생할 수 있는 프로토콜을 표준으로 변경하는 '클라이언트-서버간 호환 방법' 과 기존 프로토콜 A와 B를 변경하지 않는 상태에서 전자책 DRM 클라이언트간 상호 라이선스 사용을 허용하는 '클라이언트간 호환 방법', 그리고 서버에서 상대방의 라이선스 발급을 대행하거나 중계하는 '서버간 호환 방법'을 고려해 볼 수 있다.

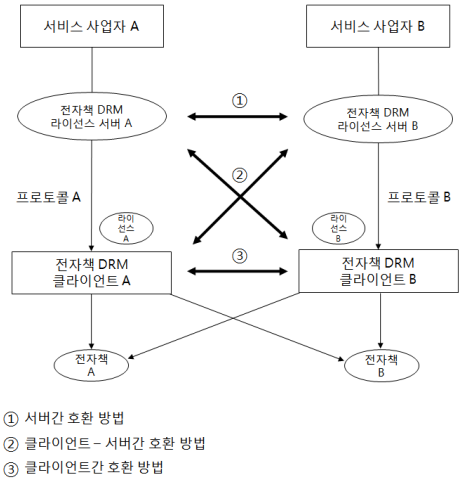

그림 1. 전자책 DRM 라이선스 발급 호환성 개념도
Fig. 1. Concept of interoperable license issuing methods for eBook DRM

1. 서버간 호환 방법

전자책 DRM 라이선스 발급 방식에서 서버간 호환 방법은 그림 1을 기준으로 서비스사업자 A가 제공하는 전자책 A와 서비스사업자 B가 제공하는 전자책 B에 대한 라이선스를 모두 가지고 있는 소비자가, 전자책 DRM 클라이언트 A를 통해 서비스사업자 B의 전자책을 열람하고자 하면 전자책 DRM 클라이언트 A는 라이선스 서버 A로 접속하여 라이선스 서버 B의 역할을 중계 또는 대행하여 라이선스 B를 발급해 주는 방식을 의미한다. 이 방식의 공통점은 다수의 전자책 서비스 사업자들 간의 연동이 발생하더라도 클라이언트와 서버간에 통신이 단일화되어 클라이언트 측 개발이 용이하다는 장점을 가지고 있다. 그러나 서비스에 대한 사용자 정보 및 판매정보가 중계 또는 대행 서비스 사업자에게 노출 될 수 있고, 타사 콘텐츠로 인해 자사 서버에 대한 부담이 걸릴 수 있는 단점이 있다.

라이선스 발급에 있어서 중계, 대행 및 위탁 방식은 라이선스를 발급하는 주체를 기준으로 구분되며, 이에 대한 내용은 다음과 같다.

가. 라이선스 발급 중계 방식

라이선스 발급 중계 방식은 전자책 DRM 클라이언트로부터 라이선스 발급을 요청받은 서버가 해당 콘텐츠에 대해서 라이선스를 발급해 줄 수 있는 서버로 라이선스 발급에 대한 재요청을 하고 이에 대한 결과를 요청한 클

라이언트에게 재전송하는 방식을 의미한다.

이 방식은 기존의 전자책 라이선스 서버와 DRM 클라이언트간의 프로토콜에 대한 변경은 필요하지 않지만 연동을 하는 전자책 라이선스 서버간에 별도의 라이선스 발급 중계 프로토콜이 필요하다. 그러나 라이선스 발급 중계 프로토콜은 다른 종류의 DRM 클라이언트와 통신이 필요 없기 때문에 보안적인 면에서 클라이언트-서버 연동 방식에 비해 프로토콜에 대한 기밀성을 유지할 수 있는 장점을 가지고 있다.

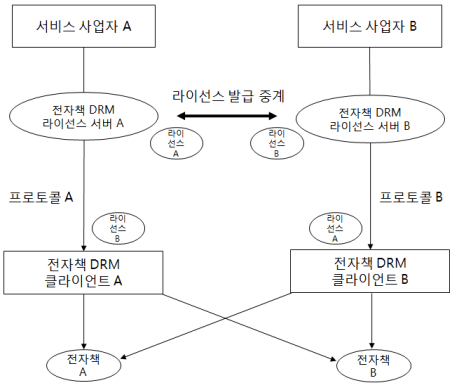

그림 2. 라이선스 발급 중계 방식
Fig. 2. License issuing server method by relay

나. 라이선스 발급 대행 방식

라이선스 발급 대행 방식은 전자책 DRM 클라이언트로부터 라이선스 발급을 요청받은 라이선스 서버가 해당 콘텐츠에 대해서 라이선스를 발급해 줄 수 있는 모듈을 통해 해당 라이선스를 발급하고 이에 대한 결과를 요청한 클라이언트에게 재전송하는 방식을 의미한다.

이 방식은 기존의 전자책 DRM 라이선스와 클라이언트간의 프로토콜 변경이 필요하지 않고, 전자책 라이선스 서버간에 별도의 라이선스 중계 프로토콜도 필요하지 않다는 장점이 있다. 그러나 전자책 라이선스 서버별로 타 서버에서 사용될 수 있는 라이선스 발급 모듈을 제공해야 하는 부담이 있다. 또한 한 서비스사업자가 복수의 서비스 사업자와 연동을 해야 할 경우 연동해야 하는 발급모듈이 증가하여 이에 대한 관리 부담이 늘어나는 문제점이 있다. 그리고 타 사업자가 가지고 있는 사용자 인증정보, 라이선스 발급 정책 정보에 대한 처리 및 관리, 그리고 키 관리 등을 위해 라이선스 발급 모듈이 본래의 DRM 라이선스 발급 서버와 연동이 되어야하는 한계점을 가지고 있다.

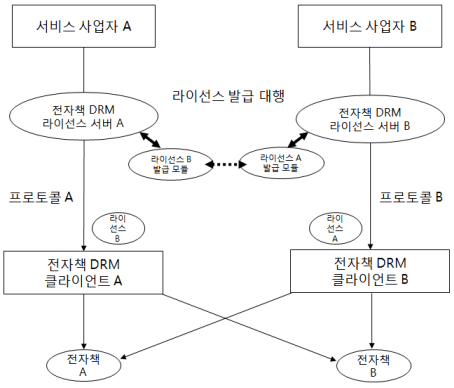

그림 3 라이선스 발급 대행 방식
Fig. 3. License issuing server method by proxy

다. 라이선스 발급 위탁 방식

라이선스 발급 위탁 방식은 전자책 DRM 클라이언트로부터 라이선스 발급을 요청받은 서버가 자신이 발행해 줄 수 없는 라이선스 발급을 라이선스 발급 위탁서버에 요청하여 해당 라이선스를 발급받고 이에 대한 결과를 요청한 클라이언트에게 재전송하는 방식을 의미한다.

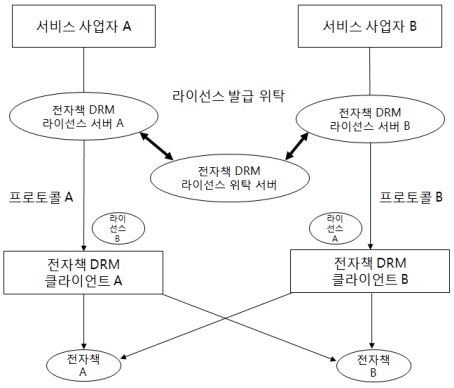

그림 4. 라이선스 발급 위탁 방식
Fig. 4. License issuing server method by trust

이 방식은 호환을 원하는 전자책 라이선스 서버들이 하나의 창구를 통해 타 전자책 DRM 라이선스를 발급 받을 수 있는 장점을 가지고 있기는 하지만 라이선스 발급을 위탁처리해 주는 대행기관이 존재해야 한다는 부담이 있다.

2. 클라이언트간 호환 방식

전자책 DRM 라이선스 발급 방식에서 DRM 클라이언트간 호환되는 방식은 그림 1을 기준으로, 서비스 사업자 A가 제공하는 전자책 A와 서비스 사업자 B가 제공하는 전자책 B에 대한 라이선스를 모두 가지고 있는 소비자인 경우에 전자책 DRM 클라이언트 A를 통해 서비스사업자 B의 전자책을 열람하고자 하면 전자책 DRM 클라이언트 A는 동일 기기에 설치되어 있는 전자책 DRM 클라이언트 B와 통신하여 DRM 클라이언트 B로 하여금 전자책 DRM 라이선스 서버 B로 접속하여 라이선스를 발급받고, 이를 전자책 DRM 클라이언트 A에 전달해 주거나 DRM 클라이언트 A에서 사용할 수 있도록 변환해 주는 방식을 의미한다. 클라이언트간 연동 방식의 공통적인 특징은 라이선스 서버간 연계가 필요 없고, 서버간 연동에서 우려되었던 타 서비스 사업자에 의해 발생하는 처리 부하로 인한 시스템 부담을 줄일 수 있으며, 사용자 인증 및 상호 인증이 서버간 연동 방식 보다 용이하다는 장점이 있다. 반면에 DRM 클라이언트에서 라이선스 전달에 대한 작업이 이루어지기 때문에 클라이언트 간 인터페이스에 대한 표준이 공개될 경우 보안의 위험성이 높다는 단점이 존재한다.

클라이언트간 연동은 클라이언트가 라이선스 정보를 변경할 수 있는지 여부에 따라 중계 및 수정방식으로 구분되는데, 이에 대한 내용은 다음과 같다.

가. 라이선스 중계 방식

클라이언트간 호환 방법에서 라이선스 중계 방식은 전자책 DRM 클라이언트가 타사의 DRM 기술이 적용된 전자책을 열람하고자 할 때, 동일한 기기에 설치된 타사의 DRM 클라이언트에게 라이선스 중계를 요청하고, 요청을 받은 타사의 DRM 클라이언트는 자사의 전자책 DRM 라이선스 서버에 접속하여 라이선스를 받고, 이를 요청한 DRM 클라이언트에 전달해 주는 방식을 의미한다. 이때 라이선스 요청을 받는 전자책 DRM 클라이언트는 요청을 하는 전자책 DRM 클라이언트로부터의 인증 정보를 그대로 자신의 서버에 전달하고, 서버로부터 생성된 라이선스를 가공 없이 요청한 전자책 DRM 클라이언트에 넘겨준다.

이 방식은 기존의 전자책 DRM 라이선스 발급 서버와 DRM 클라이언트간의 프로토콜에 대한 변경이 필요하지 않지만 상호 연동을 하는 전자책 DRM 클라이언트간에 별도의 라이선스 중계 프로토콜이 필요하다. 또한 라이선스 중계를 요청하는 모듈과 중계하는 모듈이 모두 클라이언트에 존재하는 관계로 보안적인 면에서 프로토콜을 공개하기 어려운 문제점이 있다.

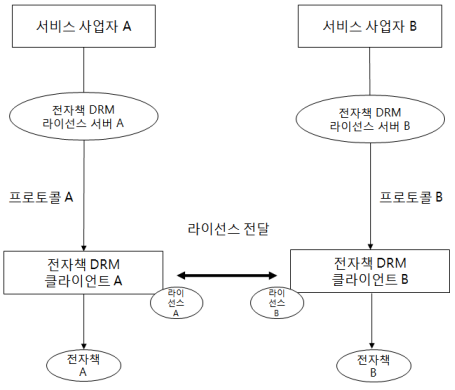

그림 5. 라이선스 중계 방식
Fig. 5. License issuing client by relay

나. 라이선스 수정 방식

클라이언트간 호환 방법에서 라이선스 수정 방식은 전자책 클라이언트가 타사의 DRM 기술이 적용된 전자책을 열람하고자 할 때, 타사의 DRM 클라이언트가 자신이 보유하고 있는 라이선스를 이용하여 필요한 정보를 추출한 후 요청한 DRM 클라이언트에서 사용할 수 있는 라이선스 규격으로 수정하여 전달하는 방식이다.

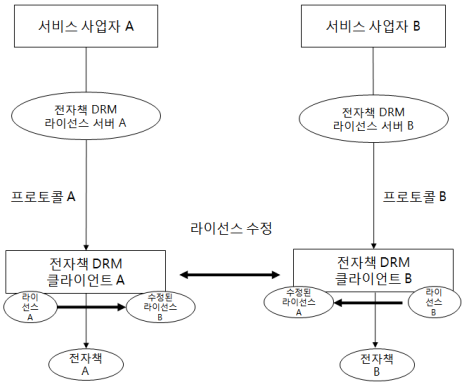

그림 6. 라이선스 수정 방식
Fig. 6. License issuing client by adaptation

이 방식은 라이선스가 존재하는 경우, 라이선스를 해석할 수 있는 클라이언트가 이에 대한 정보를 가공하여

요청한 클라이언트로 넘겨주기 때문에 라이선스 서버와의 통신 부담을 줄일 수 있는 장점이 있는 반면 라이선스에 대한 가공이 클라이언트에서 이루어진다는 보안적인 단점이 있다.

3. 클라이언트 서버간 호환 방식

전자책 DRM 라이선스 발급 방식에서 클라이언트 서버간 호환되는 방식은 그림 1을 기준으로 서비스사업자 A가 제공하는 전자책 A와 서비스사업자 B가 제공하는 전자책 B에 대한 라이선스를 모두 가지고 있는 소비자가, 전자책 DRM 클라이언트 A를 통해 서비스사업자 B의 전자책을 열람하고자 하면 전자책 DRM 클라이언트 A는 표준 프로토콜로 정의된 방식에 따라 전자책 DRM 라이선스 서버 B에 접속하여 라이선스를 발급받아 사용하는 방식이다. 이 방식은 표준방식을 사용한 가장 간단한 방식이라는 장점이 있기는 하지만 라이선스에 대한 발급 프로토콜이 공개된다는 단점과 서비스 사업자들의 기존 라이선스 발급 프로토콜 방식을 변경해야 하는 부담이 존재한다.

III. 라이선스 발급 방법에 대한 장단점 및 시사점 분석

현재 논의 되고 있는 상호호환성을 지원하는 전자책 DRM 라이선스 발급 방법들의 장단점 및 시사점을 분석하면 표1, 표2와 같다.

표 1. 라이선스 발급 방법에 대한 장단점 분석결과
Table 1. Analysis result on the considering license issuing methods

방식		장점	단점
서버간 호환 방법	발급 중계	· 복수 서비스 제공자간 연동 시 용이	· 라이선스 서버간 연동 프로토콜 필요
	발급 대행	· 연동 프로토콜 필요 없음	· 연동 업체 증가시 복잡도 증가
	발급 위탁	· 연동 서비스사 수와 상관없이 확장 가능	· 별도의 위탁기관 설립 필요
	공통	· 클라이언트 측 개발 용이 · 클라이언트에 프로토콜 미공개 가능	· 자사 판매 및 인증정보에 대한 노출 · 타사 콘텐츠로 인한 서버 부담 증가
클라이언트	발급 중계	· 라이선스 수정 방식 보다는 안전	· 연동 프로토콜 필요
간 호환 방법	라이선스 수정	· 서버 부담 감소	· 클라이언트에서 라이선스 수정 (보안에 가장 취약) · 소비자 사용정보 획득 및 통제 어려움
	공통	· 현 클라이언트- 서버간 라이선스 발급 프로토콜 유지 · 서비스 사업자간 1:1 연동 시 유리	· 보안에 취약 · 연동 업체 증가시 복잡도 증가
클라이언트 서버간 호환 방법		· 단일 표준시 가장 간단하고 확실한 연동 방식 · 타사 콘텐츠로 인한 서버 부담 없음 · 자사 판매 및 인증정보에 대한 노출 없음 · 연동 업체 증가시 복잡도 증가 없음	· 단일 표준화 어려움 · 프로토콜 공개에 로 인해 보안성 훼손 가능성에 따른 거부감 · 권리정보에 대한 호환 방법 부재

표 2. 라이선스 발급 방법 분석에 따른 시사점
Table 2. Remarks of the considering license issuing methods.

방식	시사점
서버간 호환 방법	불필요한 프로토콜을 공개하지 않아도 되는 장점이 있지만 판매정보와 인증정보에 대한 노출 우려가 부담되는 모델
클라이언트간 호환 방법	현재의 각 서비스 사업자가 운영하고 있는 개별 클라이언트-서버간 라이선스 발급 프로토콜을 유지할 수 있는 장점과 클라이언트의 복잡도와 보안 위험성에 따른 단점이 양립하는 모델
클라이언트-서버간 호환 방법	권리정보 전달에 대한 문제점 상존과 기존 프로토콜 수정에 대한 부담, 그리고 프로토콜 공개에 따른 서비스 사업자들의 불안감이 문제점으로 지적되나 단일 표준으로 가장 확실할 표준 모델

표 1과 표2의 분석결과에 의하면 호환성 지원을 위한 라이선스 발급 방법 중 가장 효과적인 호환방법은 클라이언트와 서버간의 호환방법으로 보이나, 이 방식은 현 서비스 시스템의 프로토콜 체계를 변경해야 하는 부담과 프로토콜이 공개되는 것에 따른 보안성 우려가 존재한다. 또한 서버간 호환방법은 프로토콜의 노출 우려보다는 서비스 사업자의 정보가 공개되는 것에 대해 전반적으로 부정적인 입장에 있고, 대안으로 제시될 수 있는 클라이언트간 호환 방법은 보안상 가장 취약한 구조이기 때문에 표준으로 추진하기에는 한계가 있는 모델이다.

이러한 전자책 DRM 라이선스 발급 호환성에 대한 가능성 모델 중에서, 본 논문은 암호화 키 전달에 대해서는 클라이언트-서버 방식을 적용하고, 권리정보 전달 방식에 대해서는 서버간 발급대행 방식을 사용한 하이브리드 기술적 모델을 소개하도록 한다.

IV. 전자책 DRM 라이선스 발급 제안 모델

1. 제안 모델 개요

그림 7은 본 논문에서 제시하는 클라이언트-서버간 호환방식에 대한 개요도로, IDPF EPUB 기반의 전자책 DRM 표준을 준수하는 전자책 DRM 클라이언트가 표준 전자책 DRM 라이선스 발급 프로토콜을 기반으로 라이선스와 관련된 전자책 시스템의 정보를 요청하고, 전자책 DRM 라이선스 발급 서버는 클라이언트로부터 전달된 전자책 시스템의 내용을 수정해서 발급하는 모델을 보여준다.

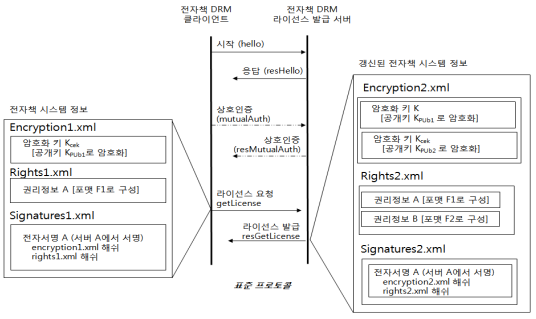

그림 7. 전자책 DRM 라이선스 발급 제안 모델
Fig. 7. License issuing model draft for eBook DRM

클라이언트-서버간 호환방식의 라이선스 발급 프로토콜은 표 3 에서와 같이 상호 인증서 등록 여부에 따라 3단계 프로토콜 또는 2단계 프로토콜로 나뉜다.

표 3. 전자책 DRM 라이선스 프로토콜 메시지 구성
Table 3. Components of the protocol messages

프로토콜 메시지 구성		기능
3 단계	시작 (Hello)	상호 인증서 등록여부 확인
	상호인증 (MutualAuth)	인증서 미등록시, 상호 인증을 통한 연동 가능 모듈임을 확인
	라이선스 요청 (GetLicense)	상호 연동 가능 모듈인 경우, 라이선스 요청 및 수신
2 단계	시작 (Hello)	상호 인증서 등록여부 확인
	라이선스 요청 (GetLicense)	이미 등록된 모듈인 경우 라이선스 요청 및 수신

2. 프로토콜 메시지

가. 시작(Hello) 메시지

본 논문에서 제안하고자 하는 전자책 DRM 라이선스 발급 프로토콜의 시작(Hello) 메시지는 클라이언트-서버간에 상호 인증서 등록여부를 확인하기 위한 용도로 사용된다. 메시지의 발송은 클라이언트에서 시작되며, 메시지의 내용은 클라이언트의 인증서 정보를 포함한다. 시작 메시지를 수신한 서버는 클라이언트의 인증서 정보가 서버에 등록되어 있는지 여부를 검사한다. 클라이언트의 인증서 등록여부에 따라 다음에 진행될 메시지의 종류가 결정되는데, 만약 인증서 정보가 서버에 등록되어 있다면 이는 이미 이전에 상호 인증 과정을 통해 인증이 완료된 클라이언트를 의미하며 상호 인증 과정 없이 직접 라이선스 요청 단계가 진행될 수 있다. 반면 인증서 정보가 서버에 등록되어 있지 않다면 클라이언트 모듈에 대한 신뢰성 확보를 위해 상호 인증 과정을 진행해야 한다. 상호 인증 과정의 진행 여부에 따라 프로토콜은 각각 3단계 또는 2단계 프로토콜로 분류되어 처리된다. 상호 인증 과정의 진행 여부에 대한 판단 정보는 시작 메시지의 응답 메시지(resHello)를 통해 클라이언트로 전송된다.

클라이언트와 서버 인증서에 대한 정보는 인증서의 공개키 부분에 대한 SHA1 해쉬값으로 표기된다. 3단계 프로토콜을 진행하기 위한 서버의 응답 메시지는 클라이언트에 대한 인증서 체인 요청 정보만이 추가되지만, 2단계 프로토콜을 진행하기 위한 응답 메시지는 라이선스 요청 메시지를 처리를 위한 세션키 정보 및 서버의 전자서명 정보가 추가된다. 2단계 프로토콜을 진행하기 위한 서버 전자서명은 클라이언트에서 서버의 신뢰성을 확인하기 위한 정보로 사용된다.

표 4. 시작 메시지 내용 요약
Table 4. Brief description of Hello message

메시지 종류	내 용
시작 요청	<hello> 모듈 버전 정보 암호화 인증서 정보 전자서명용 인증서 정보 </hello>
시작 응답	<resHello> 모듈 버전 정보 (공통) 암호화 인증서 정보 (공통) 전자서명용 인증서 정보 (공통) 클라이언트 인증서 요청 정보 (3단계 용) 세션키 정보 (2단계 용) 전자서명 (2단계 용) </resHello>

표 4는 전자책 DRM 라이선스 발급 프로토콜의 시작 메시지의 요청과 응답에 사용되는 정보들의 요약을 보여준다.

나. 상호인증(MutualAuth) 메시지

본 논문에서 제안하는 전자책 DRM 라이선스 발급 프로토콜의 상호인증(MutualAuth) 메시지는 클라이언트-서버간에 인증서와 전자서명을 교환함으로써 신뢰된 모듈간의 정보 교환임을 사전에 확인하기 위한 용도로 사용된다.

이 메시지의 요청은 시작 메시지를 받은 서버의 응답 메시지(resHello)에 의해 결정이 되며, 메시지의 발송은 클라이언트에서 이루어진다. 상호인증 메시지는 클라이언트의 암호화용 인증서와 전자서명을 포함한다. 이때 전자서명에는 전자서명을 확인할 수 있는 인증서 체인을 모두 첨부하여 전송하는데, 이는 상호인증 정보를 수신한 서버가 클라이언트의 전자서명 정보를 통해 클라이언트의 인증서를 발행한 루트 CA 인증서를 확인 할 수 있고, 해당 루트 CA가 전자책 DRM 라이선스 발급의 호환을 위해 사업적으로 합의된 CA 인증서와 동일한지 여부를 확인함으로써 클라이언트에 대한 신뢰성을 확보하는 용도로 사용된다. 전자서명에 대한 검증과정이 통과되면 라이선스 발급서버는 세션키가 포함된 상호인증 응답 메시지를 회신한다. 세션키는 인증이 완료된 클라이언트의 공개키로 암호화 하여 보안성을 확보한다.

표 5는 전자책 DRM 라이선스 발급 프로토콜의 상호인증 메시지의 요청과 응답에 사용되는 정보들의 요약을 보여준다.

표 5. 상호인증 메시지 내용 요약
Table 5. Brief description of MutualAuth message

메시지 종류	내 용
상호인증	<mutualAuth> 서버 인증서 요청 정보 클라이언트 암호화 인증서 전자서명 </mutualAuth>
상호인증 응답	<resMutualAuth> 세션키 전자서명 </resMutualAuth>

다. 라이선스 요청(GetLicense) 메시지

본 논문에서 제안하고자 하는 전자책 DRM 라이선스 발급 프로토콜의 라이선스 요청(GetLicense) 메시지는 전자책 DRM에서 사용될 키 정보 및 권리정보를 요청하고 수신하기 위한 용도로 사용된다.

이 메시지의 요청은 클라이언트에서 이루어지는데, 클라이언트는 라이선스 발급 서버로부터 라이선스를 발급받을 수 있는 자격이 있음을 증명하기 위해서 해당 서비스 사이트에 대한 암호화된 회원정보를 추가하고, 열람을 원하는 전자책에 대한 전자책 시스템 정보를 포함하여 메시지를 전송한다. 클라이언트로부터 라이선스 요청 메시지를 수신한 서버는 암호화된 서비스 회원인증 정보를 통해 클라이언트가 회원 자격이 있음을 확인하고, 요청한 전자책 시스템의 키 정보를 클라이언트의 공개키로 암호화하여 회신 메시지에 포함해서 전달한다. 이때 클라이언트에 맞는 권리정보도 함께 포함해서 전달한다. 이 절차는 라이선스 발급 서버에서 직접 처리하거나, 연동을 허가한 대상 서버로부터 권리정보 생성 모듈을 전달 받아 라이선스 발급을 대행 처리한다.

표 6은 전자책 DRM 라이선스 발급 프로토콜의 라이선스 요청 메시지의 요청과 발급에 사용되는 정보들의 요약을 보여준다.

표 6. 라이선스 요청 메시지 내용 요약
Table 6. Brief description of GetLicense message

메시지 종류	내 용
라이선스 요청	<getLicense> 서비스 회원 인증 정보 EPUB META/INFO 정보 HMAC </mutualAuth>
라이선스 발급	<resGetLicense> 수정된 EPUB META/INFO 정보 HMAC </resGetLicense>

3. 프로토콜에 대한 보안성 확인

본 모델에서는 클라이언트와 서버간의 표준 프로토콜 공개를 전제로 하고 있다. 프로토콜 공개에 따른 보안성의 위험 요소별 프로토콜의 안전성 분석은 표 7과 같다.

표 7. 프로토콜의 보안 위험 요소별 안전성 분석
Table 7. Risk factors and safety

보안위험 요소	안정성
클라이언트 위조를 통한 불법 라이선스 획득	서버는 인증서 및 전자서명을 기반으로 상호인증 과정을 통해 해당 인증서의 주인을 신뢰된 방법으로 식별할 수 있고, 전자서명을 통해 인증서를 발급한 루트 CA의 신뢰성 및 비즈니스 협의 기관임을 확인할 수 있다. 따라서 위조된 인증서를 가진 클라이언트에 대한 접근이 불가능하다.
서버위조를 통한 사용자 회원정보 획득	클라이언트에서 인증되지 않은 서버로는 데이터 전송을 하지 않기 때문에 위조된 서버와의 통신이 발생할 수 없다.
Man-in-the-middle 공격	데이터 전송은 인증된 상대방의 공개키를 기반으로 전달되기 때문에 중간에 내용을 가로채더라도 의미 없는 데이터이다.
replay 공격	각 프로토콜에 메시지에 nonce 값을 사용함으로써 replay 공격을 무력화한다.

V. 결론

본 논문은 전자책 DRM에 있어서의 호환성을 지원하는라이선스 요청 및 발급 방법에 대해 조사하고 각 방식에 대한 장단점 및 시사점을 분석한 후, 보안성과 구현가능성을 고려한 라이선스 발급 모델을 제시하였다. 제안한 모델은 2011년 6월부터 2013년 3월까지 2년간에 걸쳐 진행되고 있는 한국저작권위원회 CT R&D 연구과제(과제명 : 국제표준의 EPUB 기반 전자책 DRM 표준 레퍼런스 소프트웨어 기술 개발)의 2011년 연구 결과물(4개의 표준 명세서 - "전자책 DRM 암호화 명세서", "전자책 DRM 전자서명 명세서", "전자책 DRM 인증서 명세서", "전자책 DRM 권리용어 정의")을 기반으로 하고 있다. 본 논문에서 제시하는 전자책 DRM 라이선스 발급 프로토콜 명세서는 2012년 표준안으로 개발되어 전자출판물 표준화포럼[2]과 한국정보통신표준협회[9]를 통해 국내 산업 표준으로 진행될 예정이다. 또한 과제를 통해 개발된 전자책 DRM 라이선스 발급 프로토콜의 구현물은 Java 기반의 공개소스로 개발되어 라이선스 없이 누구나 사용될 수 있도록 제공될 예정이다.

전자책에 관련된 국제표준 단체인 IDPF에서는 최근 EPUB 3.0을 기준으로 단일 DRM으로 진행하려던 당초 계획을 수정하여 복수 DRM이 사용될 수 있는 플랫폼 환경으로 변화를 추구하고 있다. 이는 국내 산업현장에서와 마찬가지로 해외 전자책 시장의 상황도 단일 표준의 DRM이 산업표준으로 적용되기는 어려운 현실임을 보여주는 것이다. 이런 의미에서 본 연구는 표준 포맷이 존재함에도 불구하고 사용자들에게 여전히 불편한 사용 환경을 가져다주었던 라이선스 발급에 대한 호환성 지원 방안을 마련하게 됨에 따라 국내 전자책 시장의 성장에 큰 기여를 할 것으로 기대하며, 아울러 국내의 연구결과에 많은 관심을 보이고 있는 IDPF의 표준화 방향에서도 국내 표준의 성공사례가 좋은 영향으로 작용 것으로 기대된다.

참 고 문 헌

[1] IDPF, Available: http://www.idpf.org

[2] W3C, W3C XML Encryption, 2002

[3] W3C, W3C XML Signature, 2008

[4] Ho-Gap Kang et al., "A Study of ePub-based Standard Framework Supporting Mutual Comparability of eBook DRM", Vol 11, No. 6, The Jounak of The Institute of Webcasting, Internet and Telecommunication, pp.235-245, 2011

[5] ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology.

[6] ODPF, Available: http://odpf.or.kr

[7] TTA, Available: http://www.tta.or.kr/

[8] Tae-Hyun Kim et al., "A Study of ePUB-based Interoperability Method of Rights Information Supporting Mutual Comparability of eBook DRM", Vol 12, No. 2, The Jounak of The Institute of Webcasting, Internet and Telecommunication, pp.205-214, 2012

[9] ODPF KR 02-1:2012, Definitions of Right Terms for EPUB DRM

[10] ODPF KR 02-2:2012, Encryption specification for EPUB DRM

[11] ODPF KR 02-3:2012, Digital signature specification for EPUB DRM

[12] ODPF KR 02-4:2012, Certificate specification for EPUB DRM

[13] TTAK.OT-10.0332, Encryption specification for EPUB DRM

[14] TTAK.OT-10.0333, Digital signature specification for EPUB DRM

[15] TTAK.KO-10.0624, Certificate specification for EPUB DRM

[16] TTAK.KO-10.0625, Definitions of Right Terms for EPUB DRM

※ 본 논문은 문화체육관광부의 저작권기술개발사업에 의거 한국저작권위원회의 정부지원금을 받아 연구되었습니다.
(This research project was supported by Government Fund from Korea Copyright Commission.)

저자 소개

김 태 현(정회원)

- 1993년 : 중앙대학교 전자계산학과 졸업(학사)
- 2011년 : 성균관대학교 대학원 전기전자 및 컴퓨터공학과(공학석사)
- 1992년 ~ 2000년 : (주)삼성SDS 정보기술연구소
- 2000년 ~ 2004년 : (주)파수닷컴 개발실장
- 2005년 ~ 현재 : 디알엠인사이드 전략기획실장

<주관심분야 : 저작권보호기술(DRM), 정보보안기술, 리버스 엔지니어링, 전자책>

강 호 갑(정회원)

- 1985년 : 성균관대학교 전자공학과 졸업(학사)
- 1988년 : 성균관대학교 대학원 전자공학과(공학석사)
- 2010년 : 성균관대학교 대학원 전자전기공학과(공학박사)
- 1991년 ~ 2000년 : (주)삼성SDS 정보기술연구소
- 2000년 ~ 2003년 : (주)파수닷컴 연구소장
- 2005년 ~ 현재 : 디알엠인사이드 연구소장

<주관심분야 : 저작권보호기술(DRM), 디지털콘텐츠 유통, 디지털시네마>

김 윤 호(정회원)

- 1985년 : 서울대학교 계산통계학과(학사)
- 1987년 : 서울대학교 대학원 계산통계학과(이학석사)
- 1996년 : 서울대학교 대학원 전산과학박사
- 1997년 ~ 현재 : 상명대학교 소프트웨어대학 컴퓨터과학부 교수

<주관심분야 : 분산시스템, 저작권보호기술, 디지털콘텐츠>

조 성 환(정회원)

- 1980년 : 성균관대학교 전자공학과(학사)
- 1982년 : 성균관대학교 대학원 전자공학과(공학석사)
- 1991년 : 성균관대학교 대학원 전자공학과(공학박사)
- 1982년 ~ 1985년 : 해군사관학교 전기 및 전자공학과 전임강사
- 1997년 : 미국 Columbia 대학 CATT Visiting Scholar
- 1985년 ~ 2002년 : 동서울대학 컴퓨터공학과 부교수
- 2002년 ~ 현재 : 금강대학교 교수

<주관심분야 : 영상통신, 무선네트워크, 저작권보호기술(DRM)>