http://dx.doi.org/10.7236/JIWIT.2012.12.1.249
JIWIT 2012-1-33

ePUB 기반 전자책 DRM의 부분열람 제어 방법에 관한 연구

A Study of Partial Preview Control Method of ePUB-based eBook DRM

김은범*, 김경일**, 김태현***, 조성환****

Eun-Bum Kim, Kyung-Il Kim, Tae-Hyun Kim, Seong-Hwan Cho

요 약 ePUB은 국제전자출판포럼(IDPF)에서 2009년 표준으로 발표된 이후로 가장 널리 사용되고 있는 전자책 포맷 중 하나이다. ePUB은 ZIP Archive 형식으로 압축되어 있고, 내부적으로 OCF라 불리는 표준포맷으로 구조화되어 있다. 현재 국내외적으로 ePUB에 DRM을 적용하여 전자책 서비스가 활발하게 이루어지고 있으나 ePUB를 하나의 키로 암호화하고 있어 미리보기 기능 등과 같은 산업계의 다양한 요구 사항을 충족하지 못하고 있는 상황이다. 본 논문에서는 ePUB을 기반으로 한 전자책 콘텐츠를 단순하게 하나의 키로 암호화하지 않고, 다중 키 암호화 방식을 적용하여 보다 다양한 사업 모델의 적용이 가능한 방법을 제안하고자 한다. 다중 키 방식을 적용한 암호화 기법은 이를 위한 라이선스 발급 및 전송 기법, 그리고 eBook 리더에서 복호화하여 활용하는 기법과 병행하여 실제로 응용 가능한 형태로 제안한다. 제안된 다중 키 암호화 방식을 적용하게 되면 ePUB기반의 전자책 콘텐츠의 부분적 열람 기능이 가능하고, 이를 통하여 다양한 서비스 모델에 적용할 수 있으며, 단일 키 암호화 방식보다 보안성을 높일 수 있다.

Abstract ePUB is one of the most pervasive eBook formats since it was announced as a 2009 standard in IDPF(International Digital Publishing Forum). ePUB is compressed as a ZIP Archive format and structured as a standard format of OCF. Domestically and internationally, eBook services applying DRM into ePUB have currently been active, while it does not satisfy various needs from business because it does not support preview service which is due to the encryption of the whole ePUB as a single key. This study suggests a way to apply diverse business models by providing eBook content based on ePUB multiple key encryption method, not by encrypting it simply as a single key. The encryption method which applies a multiple key encryption method is suggested as a practically appliable form together with licence issuing and delivery method and decryption method in eBook readers. The multiple key encryption method suggested in this study will make it possible to support partial preview services of ePUB based eBook content. It will be applied to diverse service models and enhance the security level better then single key based encryption method.

Key Words : 전자책, ePUB, 저작권 보호기술, DRM, 다중키 암호화

Ⅰ. 서 론

ePUB(electronic publication)은 국제전자출판포럼(IDPF, International Digital Publishing Forum)에서 제정한 개방형 자유 전자책 표준이다. ePUB는 2007년 9월 이전에 있던 오픈 eBook 표준을 대체하기 위해 국제전자출판포

*정회원, (주)파수닷컴(교신저자)
**정회원, (주)파수닷컴
***정회원, DRM inside
****정회원, 금강대학교
접수일자 2012.1.19, 수정일자 2012.2.7
게재확정일자 2012.2.10

Received: 19 January 2012 / Revised: 7 February 2012 / Accepted: 10 February 2012
*Corresponding Author: icesnake@fasoo.com
Dept. Fasoo.com, Inc, Korea

럼에서 공식 표준으로 채택되었다[1]. 이러한 전자서적의 형태는 기존의 일반 서적에 비해 보다 다양한 방법의 사업 기회를 부여할 수 있다. 특히 ePUB은 그 형식이 완벽하게 공개되어 있는 개방형 표준이고, 구조화되어 있어 이를 응용하여 보다 많은 사업 모델을 만들어 내는 것이 가능할 것이다. 예를 들면, 전자책 콘텐츠 서비스 제공자들은 자신들이 보유한 콘텐츠를 많은 독자들에게 알리기 위하여 홍보를 한다. 홍보를 하는 방법은 여러 가지가 있겠지만 전자서적 콘텐츠의 일부분만을 독자들에게 공개하고 나머지 대부분 내용들은 공개하지 않음으로써 독자들의 궁금증을 불러 일으켜 구매 동기를 유발시킬 수 있을 것이다. 또한 더 많은 회원들을 확보하기 위해 사이트 회원들에 한해서만 일부 페이지를 열람할 수 있는 기능들을 제공하고 비회원들에게는 모든 내용을 볼 수 없게 할 수도 있다. 독자들의 관점에서 볼 때는 콘텐츠에 대한 구매 결정을 하기 위해 해당 콘텐츠에 대한 일 부분의 정보를 얻고자 할 수도 있다. 이와는 별개로 콘텐츠의 원저작자의 관점에서 볼 때는 자신이 개발한 콘텐츠 내용의 일부분조차 허가되지 않은 독자들에게 공개되는 것을 원하지 않을 수 있다. 이와 같이 다양하게 있을 수 있는 사업 모델들의 요구 사항들을 ePUB 기반의 전자서적의 DRM(Digital Right Management)[2] 기술을 응용하여 해결할 수 있는 방법을 제안하고자 한다. 본 논문에서는 ePUB 기반의 전자책 DRM에 대한 특정한 방법을 제안하고자 하여 ePUB의 개요와 산업화 현황에 대하여 기술하고, 현재 적용된 ePUB DRM 기술의 한계와 발전 방향에 대하여 소개하고, 이에 대한 다중 키 암호화 방식을 제안하여 보다 다양한 ePUB 기반의 전자책 서비스에서 응용이 가능하도록 한다.

II. ePUB의 개요

1. ePUB 표준화 현황

2007년 9월, ePUB은 이전의 전자서적 표준을 대체하는 국제전자출판포럼(IDPF)의 공식 표준이 되었다. 2009년 8월, IDPF는 ePUB 표준의 유지관리 작업을 시작한다고 발표하였고, 이후 작업 그룹은 초기 버전의 유지보수와 오류수정 등을 통하여 최신 버전을 유지하면서 2010년 4월, 당시까지의 오류 수정을 종료하고 ePUB 2.0.1을 발표하였다. ePUB 3.0에 대한 편집초안은 2010년 11월 12일에 출판 되었고 최초의 공개초안은 2011년 2월 15일에 게시되었으며, 2011년 5월 23일에 IDPF의 최종 제안 규격이 승인되었다. 그리고 2011년 10월 10일에 IDPF는 최종 사양으로 ePUB 3.0을 발표하였다.

2. ePUB의 구성

ePUB이 명세는 [표 1] 같이 세 가지 정의로 구성되어 있다. ePUB 파일의 물리적인 구성 내용을 보면, 일단 ePUB은 .epub 확장자를 갖는 단일 파일 형태로 되어 있다. 이는 여러 개의 구성 요소(디렉터리 및 파일)를 ZIP 메커니즘을 사용하여 단일 파일 형태로 저장 또는 압축해 놓은 모양의 결과물로서 실제로 확장자를 .zip으로 바꾸면 압축을 해제할 수 있다. 루트에는 mimetype 파일과 META-INF 디렉터리가 존재하며, META-INF 디렉터리의 container.xml 파일에는 실 콘텐츠데이터들에 대한 정보를 담고 있는 content.opf 파일의 위치가 기술되어 있다.

표 1. ePUB 2.0.1의 기술규격
Table 1. Three Specification of ePUB 2.0.1

OPS[3] (Open Publication Structure 2.0)	ePUB 출판 형식의 가장 상위 레벨의 구조로서 ePUB 출판물의 모듈화 구성 명세 정의 및 스타일 시트에 대한 정의, XHTML이나 XML의 제한적 사용에 대한 명세서
OPF[4] (Open Packaging Format 2.0)	OCF 표준에 부합하며 OCF내에 발행된 메타데이터, 읽는 순서, 정보 탐색의 동작에 대한 메커니즘에 대한 명세서
OCF[5] (Open Container Format 2.0)	ePUB 출판 구성물의 컨테이너 기술에 대한 일반적인 기술 명세서

OPF의 구현은 container.xml에서 기술된 내용을 기반으로 하고 있으며, 주로 OEBPS(Open e-Book Publication Structure) 디렉터리 내에 content.opf로 실체화되어 있다. content.opf는 메타데이터와 독자들이 읽을 내용이 기술되어 있는 파일의 순서, 콘텐츠들이 표현될 스타일 그리고 ePUB 리더(장치 또는 응용프로그램이 될 수 있음) 등의 장치에서 활용할 수 있는 탐색 정보들로 구성되어 있다. ePUB을 정의하는 구성 요소 중 OCF에서는 ePUB을 물리적으로 구성하는 mimetype 파일에 대한 포맷과, META-INF 디렉터리에 들어갈 rootfile들에 대한 기술 명세서를 다룬다.

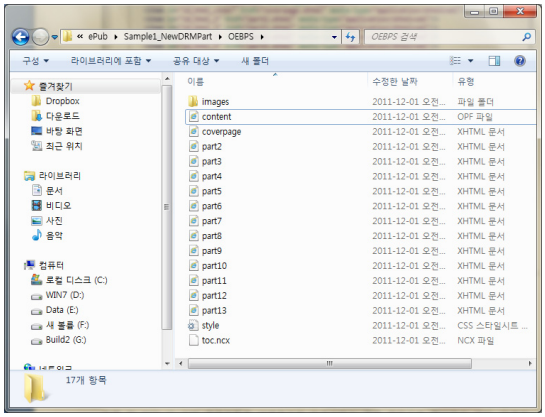

그림 1. ePUB 내부의 OEBPS 구성
Fig. 1. OEBPS Structure inside ePUB

3. ePUB의 저작권 관리 권고 사항

IDPF에서는 ePUB의 저작권 관리 시스템에 대해서 강제하는 규격은 없으며, W3C의 보안 XML 규격을 기준으로 하는 권고 사항들이 존재한다. ePUB에서 권고하는 저작권 보호(DRM)에 대한 정의를 보면 ZIP Archive 형식으로 묶여진 하나의 .ePUB 파일은 암호화 대상이 아니며, ZIP Archive내에 구성되는 각각의 파일들을 암호화할 수 있다. 이중에서 META-INF, OPF, Mimetype 은 암호화하면 안 되며 그 외에 콘텐츠들은 개별적으로 암호화하는 것을 원칙으로 정의하고 있다. 암호화의 단위는 각각의 파일이 된다. 따라서 OEBPS 디렉터리 내에 content.opf 파일을 제외한 모든 파일들이 각각 개별적으로 암호화될 수 있다. 추가적으로 암호화될 수 있는 파일들은 OEBPS/Images내의 모든 파일들과 OEBPS내의 모든 XHTML파일들과 NCX 파일들과 CSS 파일들 이다. IDPF의 ePUB의 표준 규격을 준수하면서 해당 전자책 콘텐츠에 암호화를 수행하게 되면 META-INF 디렉터리에 Encryption.xml을 생성해야 하는데, 이는 W3C 보안 XML 표준 규격에 준하여 암호화를 수행하는 키 정보, 알고리즘 정보들을 담고 있어야 한다. 또한 콘텐츠의 위, 변조 방지를 위해 전자 서명용 Signatures.xml 파일과, 콘텐츠 사용자의 권한 제어를 위해 Rights.xml 파일에 대한 생성을 권고하고 있다. 암호화, 전자 서명, 권한 제어에 대해서는 적용되는 알고리즘을 지정하고 있지는 않으며 특정 알고리즘 및 권한 표현 언어를 사용할 수 있다는 권고 사항을 제안하고 있다. 본 제안에서는 암호화 알고리즘이나 전자서명의 방법에 대해서는 다루지 않는다.

Ⅲ. 국내외 ePUB DRM 현황

국내외 전자책 시장에서 전자책 콘텐츠의 불법 복제 방지 및 저작권 보호를 위해 사용되고 있는 전자책 DRM 기술을 종합하여 요약하면 다음과 같다.

표 2. 국내외 ePUB DRM 기술 현황[6]
Table 2. Domestic/Global ePUB DRM Tech.

기술 공급자	DRM 기술 정책	파일 포맷	고객사
아마존[9]	폐쇄적 운영	AZW	아마존
파수닷컴 [10]	전자책 서비스 사업자 및 단말기 제조업체에 DRM 기술 공급	비공개 포맷	교보문고[11] NHN
인큐브테크 [16]		ePUB	한국이퍼브[13], 쿡북카페
유니닥스 [17]		PDF	교보문고[11]
마크애니 [18]		비공개 포맷	인터파크[12], 한국출판콘텐츠 조선일보
어도비[15]		ePUB	소니, 반스앤노블, 아이리버, 네오럭스
다산지엔지		BCB	북큐브

표 3. 국내외 ePUB 암호화 기술 현황[6]
Table 3. Domestic/Global ePUB Encryption Tech.

기술 공급자	암호화	전자서명	REL
아마존[9]	비공개	비공개	비공개
파수닷컴 [10]	SEED, AES-128, 3DES RSA 1024	RSA 1024	XML 1.0, 2.0
인큐브테크 [16]	SEED-CBC, AES256	SHA-1	XrML[7]
유니닥스 [17]	3DES	SHA-1	비공개
마크애니 [18]	비공개	비공개	비공개
어도비[15]	AES-128	비공개	비공개
다산지엔지	비공개	비공개	비공개

국내외 DRM 기술을 분석한 결과, 대부분의 업체들은 독자적인 포맷과 암호화 기술을 사용하고 있으며, DRM 기술 사양에 대한 공개를 하지 않고 있다. 국내의 일부

DRM 기술은 ePUB 표준을 준수하여 제작된 전자책 콘텐츠 파일을 통째로 암호화하는 방식을 사용하고 있는데 이 방식은 IDPF에서 제안한 ePUB 표준에 전혀 부합하지 않는다.

Ⅳ. 전자책 부분열람 제어를 위한 제안기술

ePUB은 하나의 파일이며 하나의 전자책 콘텐츠로 볼 수 있다. 이러한 이유로 ePUB 파일에 DRM을 적용하고자 할 때 하나의 CEK(Content Encryption Key)를 사용하여 암호화하는 방식을 사용하고 있다. ePUB 표준에서 권고하는 DRM을 적용하든 독자적인 기술 표준으로 DRM을 적용하든 하나의 ePUB 파일에 하나의 CEK로 암호화를 수행하는 것이 기존의 방법이었다. 하지만 실제로는 ePUB은 ZIP Archive내 여러 개의 파일들의 집합으로써, 여러 개의 파일이 하나의 콘텐츠를 표현하고 있는 방식으로 볼 수 있다. 기존의 방식과 같이 ePUB을 단일키로 암호화하게 되면 전자책 콘텐츠의 부분적 열람 기능을 완전하게 구현할 수 없다. 구현하더라도 부분적으로 암호화를 적용하거나 아니면 원본 형태로 유지하는 제한적인 기능을 구현할 수밖에 없다. 하지만 ePUB의 구조 내에 존재하는 구성요소들의 각 파일들에 대응하는 복수개의 키를 생성하여 암호화하는 다중 키 암호화 방식을 적용하면 원천적으로 전자책의 모든 내용에 대하여 보안을 적용한 상태에서 권한 제어를 통하여 부분적 열람 기능을 구현할 수 있어 보안성을 높일 수 있으며, 또한 이러한 열람 제어 기술을 응용하여 보다 다양한 전자책 서비스 방법을 구현할 수 있다.

본 논문에서 제안하는 기술은 IDPF에서 제정한 ePUB 표준 규격에 준수하여 ePUB 기반 전자책의 모든 내용을 암호화하고 사용자 그룹의 권한에 따라 내용의 부분적 접근을 제어하는 기술에 관한 것이다. 암호화 모듈에서는 ZIP Archive 형식으로 존재하는 ePUB 파일내의 암호화가 가능한 모든 파일들을 대상으로 암호화를 수행한다. 전자책 본문(표지 포함)에 해당하는 내용을 암호화할 때 XHTML 파일 단위로 각각 다른 CEK를 생성하여 암호화를 수행한다. 이는 사용자 그룹별로 콘텐츠 내용에 대한 부분적인 접근 권한을 제어하기 위함이다. 하나의 ePUB을 암호화하는 과정에서는 여러 개의 CEK가 생성된다. CEK는 암호화하는 과정에서 생성한 Encryption.xml에 은닉하여 배포하지 않고, Encryption.xml에는 CEK를 얻을 수 있는 경로만을 링크하여 기록한다. 생성된 CEK들은 키 관리 서버에 의해서 관리된다. 사용자가 리더를 통해서 암호화된 ePUB을 열람하고자 할 때는 CEK를 얻어야 한다. ePUB 리더는 ePUB내에 존재하는 Encryption.xml로부터 CEK를 얻을 수 있는 키 관리 및 라이선스 발급 모듈의 경로를 구하고, 이에 사용자 자신의 고유한 식별 정보(ID, Public Key)를 전달하면서 함께 CEK를 요청한다. 키 관리 및 라이선스 발급 모듈에서는 전달받은 사용자 식별 정보를 통해 사용자의 ePUB 접근 권한을 판단한다. 사용자가 ePUB 파일 내용 전체를 열람할 수 있는 권한을 가지고 있다면 모든 CEK를 전달하며, 일부분에 대한 내용만 열람할 수 있는 권한을 가진다면 해당하는 부분만 열람이 가능하도록 CEK를 선택하여 전달하고 나머지 CEK들은 전달하지 않는다. CEK의 전달은 일반적으로 행하여지는 바와 같이 사용자 고유의 식별 정보에 의해 암호화되어 라이선스 내에 포함된다. 이때 각 CEK들이 ePUB 파일 내용의 어떤 부분을 복호화할 수 있는지 식별할 수 있는 정보를 같이 포함하도록 한다. 리더는 라이선스를 전달받아 라이선스로부터 자신의 개인키로 CEK와 해당 CEK가 ePUB 파일 내용 중에 어떠한 부분을 복호화 할 수 있는지를 식별하는 정보를 추출한다. 상기 정보들을 추출하여 해당하는 내용만을 복호화하여 출력한다. 여기에서는 이러한 시스템을 구현하기 위해 암호화 모듈(Packager), 라이선스 발급 모듈, ePUB 리더를 제안한다.

1. 암호화 모듈

암호화 모듈(Packager Module)은 ePUB 파일의 구조를 분석하고 암호화 대상 구성 요소들을 선별한다. 암호화 대상 구성 요소들은 각각 하나의 스트림 단위로 나뉘어 분리된다. 각 스트림들은 무작위로 생성된 대칭키 방식의 키(CEK)로 암호화 된다. 이때 각 스트림별로 하나의 CEK가 생성되어, 여러 개의 스트림이 존재한다면 해당 개수만큼 CEK가 생성되어 해당 스트림을 암호화한다. 이후 해당 스트림에 대한 식별 정보와 CEK는 쌍으로 키 관리 저장소에 저장한다. 스트림 식별 정보는 해당 ePUB 파일에 대한 식별 정보를 포함한다. 이 작업은 암호화 대상이 되는 모든 스트림을 암호화할 때 까지 반복하여 수행한다. 암호화된 스트림들은 다시 ePUB의 구성

요소로 구조화되어 ePUB 형식 파일로 저장한다.

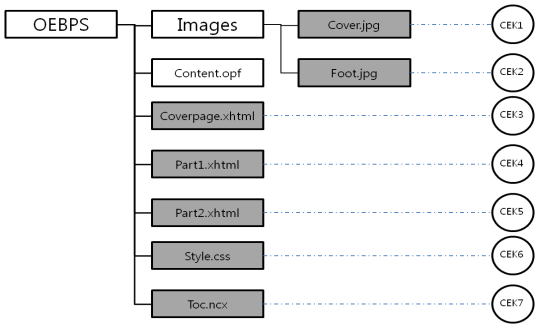

그림 2. OEBPS 구성 요소들에 대한 CEK 생성과 대응
Fig. 2. CEK Creation and Matching for OEBPS Subsets

2. 키 관리 및 라이선스 발급 모듈

키 저장소(Key Store)에 관리되고 있는 CEK(Content Encryption Key)들은 ePUB 리더 모듈에서 독자들의 열람 요구사항이 있을 경우 라이선스 발급 모듈(License Issuing Module)에 의해 사용자들에게 전달된다.

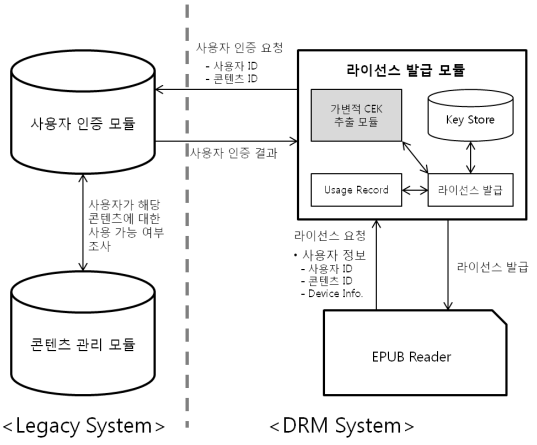

그림 3. 라이선스 발급 모듈에 대한 처리의 흐름
Fig. 3. Processing Flow of License Issuing Module

ePUB 리더에서 라이선스 발급 요구 사항이 접수되면 라이선스 발급 모듈은 사용자 정보를 받아 권한 판단을 한다. 권한 판단은 사용자 인증 모듈에서 수행하여 인증에 대한 결과를 라이선스 발급 모듈이 받아 해당 권한에 맞는 라이선스를 만들어 ePUB 리더에게 발급한다. 라이선스에는 ePUB을 복호화 할 수 있는 CEK들이 포함되어 전달되어지는데 이때 CEK들은 사용자 정보(사용자의 공개키, 공인 인증서 등)에 의해 암호화된다. CEK는 해당 ePUB 콘텐츠에 따른 사용자의 접근권한에 따라 가변적으로 포함된다.

하나의 ePUB 파일에는 XHTML 파일 단위로 여러 개의 내용으로 분리되어 있어 각 XHTML 파일마다 접근권한을 개별적으로 부여할 수 있다. 특정 ePUB 콘텐츠에 특정 사용자가 일부분만을 접근할 수 있는 권한을 갖는다면 그에 해당되는 일부분(XHTML 파일 단위)에 대한 CEK만 포함하여 전달한다. 전체를 접근할 수 있는 권한을 갖는다면 전체 내용을 모두 복호화 할 수 있도록 해당 ePUB 콘텐츠의 모든 CEK들이 라이선스에 포함된다. 또는 해당 콘텐츠의 모든 내용에 접근할 수 없는 사용자의 권한이라고 판단되면 라이선스 발급을 거부할 수 있다.

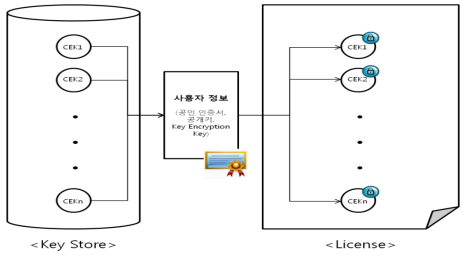

그림 4. 키 저장소로부터 라이선스의 발급
Fig. 4. License and Key Repository

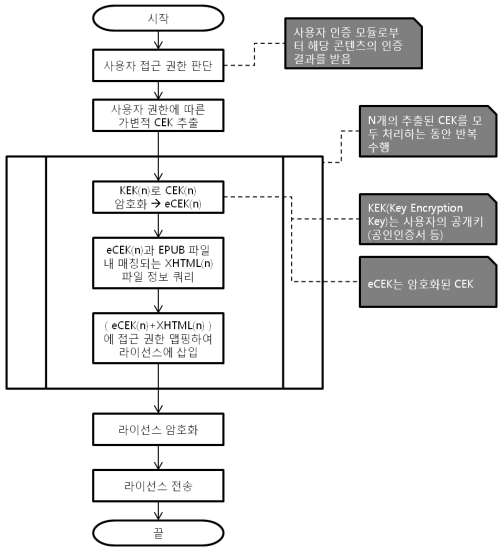

그림 5. 라이선스 발급과 전달의 처리
Fig. 5. License Deliverying Process

3. ePUB 리더 모듈

사용자는 ePUB 뷰어를 통해 ePUB 콘텐츠를 열람할 수 있다. ePUB 뷰어는 응용 프로그램일수도 있고, 단말 장치일 수 도 있다. ePUB 뷰어는 ePUB의 내용을 사용자가 읽을 수 있게 보여 주어야 하는데, ePUB 구조를 분석하고 이를 읽을 수 있는 스트림 형식의 데이터로 추출해 주는 모듈을 ePUB 리더 모듈(ePUB Reader Module)이라 정의한다. ePUB 리더 모듈에서는 암호화된 ePUB 파일을 읽어 평문의 스트림 데이터로 변환해 ePUB 렌더러 모듈(ePUB Renderer Module)에 전달한다.

ePUB 리더 모듈은 암호화된 ePUB 파일을 읽기 위해서 키 관리 및 라이선스 관리 모듈로부터 CEK와 사용 권한을 취득해야 한다. CEK와 사용 권한은 라이선스라고 호칭되는 하나의 구조화된 데이터에 존재하며 이는 ePUB 리더의 요청에 의해 키 관리 및 라이선스 발급 모듈에 의해 생성되어 전달된다.

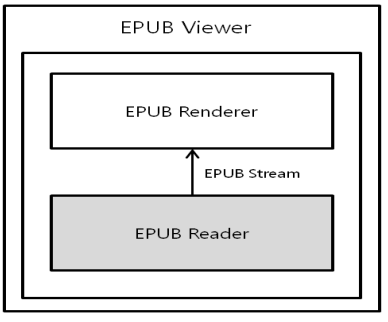

그림 6. ePUB 뷰어의 구조
Fig. 6. Structure of ePUB Viewer

라이선스는 위(키 관리 및 라이선스 발급 모듈)에서 언급한 바와 같이 ePUB 리더 모듈에서 공인된 사용자 정보(공인 인증서 등)와 콘텐츠 정보, 단말 장치 정보를 먼저 제공함으로써 얻을 수 있다. 해당 정보들을 전송하고 라이선스를 얻게 되면 ePUB 리더 모듈은 라이선스를 분석하고 암호화된 문서를 복호화하기 위해 CEK와 그에 맵핑된 암호화된 구성 요소 정보(XHTML, Image, CSS, NCX 등)를 추출한다. 또한 해당 구성 요소에 접근할 수 있는 권한 정보도 추출한다. 라이선스 분석 작업을 마친 후 CEK를 추출할 수 없는 경우에는 해당 콘텐츠를 처리할 수 없어 그대로 종료를 하고, 한 개라도 추출했다면 ePUB 파일 구조 분석을 실시한다. OPF 파일을 먼저 분석하고 OPF 분석에 의한 결과의 순서대로 구성 요소들을 나열한다.

우선 스타일 시트 복호화 및 분석과 TOC(Table Of Contents)복호화 및 분석을 한 후 리소스 구성 요소들(Image 등)을 복호화한다. 다음으로 본문의 내용을 담고 있는 XHTML 파일들을 분석하고 복호화한다. XHTML 파일들은 특히 각각의 사용 권한(읽기, 인쇄, 편집, 원본 추출등)들과 맵핑된다. 이러한 작업들을 CEK들이 모두 사용되었거나 모든 구성 요소들을 다 처리하였을 때 까지 반복하여 수행한다. 복호화된 스트림들은 ePUB 렌더러로 전달되어 렌더러에서 허용된 권한으로 제한되어 사용한다.

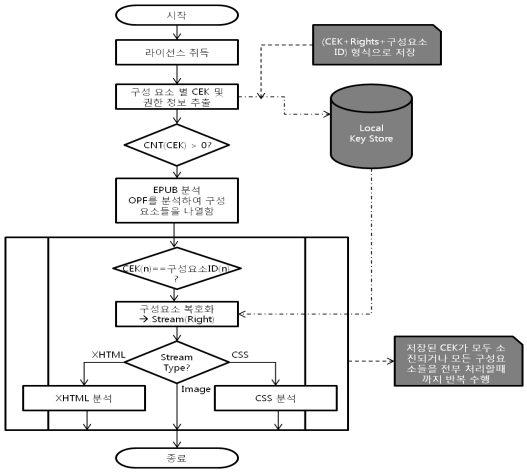

그림 7. 암호화된 ePUB 콘텐츠의 복호화 과정
Fig. 7. Decryption process of Encrypted ePUB Content

V. 결론

기존의 ePUB 저작권 보호 시스템은 하나의 CEK로 ePUB 파일 전체를 구조화 없이 암호화하는 방법을 취했거나, ePUB의 구조를 유지하면서 내부 구성 요소들을 하나씩 암호화한다고 하여도 하나의 CEK를 사용하여 암호화 했다. 이는 전자책 한 권을 하나의 콘텐츠로 인식하여 다양한 비즈니스 모델을 적용하기에 제약 사항이 존재하였다. 하지만 여기에서 제안하는 방법은 ePUB의 구조를 유지하면서 여러 개의 CEK를 생성하여 ePUB 내부의 구성 요소들 각각에 저마다 다른 CEK를 적용하여 암호화하고 또 그에 따른 사용 권한도 각각 맵핑하도록 하고 있

다. 이와 같이 함으로써 다양한 요구사항들을 유연하게 적용할 수 있어 보다 많은 비즈니스 모델을 구현할 수 있게 한다. 이를테면 서비스 업체는 정회원, 준회원, 비회원이라는 사용자 정책을 유지하고 정회원에게는 콘텐츠의 모든 내용의 열람을 허용하고, 준회원에게는 미리 보기 서비스만을 제공하기 위해 특정 페이지 부분을 지정하여 열람할 수 있게 해줄 수도 있으며 비회원에게는 열람이 가능하지 않도록 막을 수도 있다. 또한 그에 따른 접근 권한도 부분적으로 줄 수 있다. 어떠한 페이지는 모든 사용자들에게 인쇄를 허락하지만 어떠한 페이지는 특정 사용자에게만 인쇄를 허락할 수 있고, 어떤 페이지는 모든 사용자들에게 인쇄를 할 수 없게 정책을 결정할 수도 있다. 이러한 비즈니스 모델은 전자책이기에 충분히 있을 수 있는 사용 시나리오 이다. 또한 기간적 대여를 한 전자책을 일정 기간 동안은 모든 페이지에 대해 복호화 및 열람이 가능한 라이선스를 발급하였다가, 기간이 지나면 특정 페이지만을 열람하도록 제한할 수 있다. 어떠한 사용자는 특정 전자책에서도 모든 내용 전체가 필요하지 않고 일부 내용만을 열람하기를 원할 수도 있는데 이러한 요구 사항들에 대해서도 대응이 가능하다. 이러한 다양한 요구 사항들을 모두 수용할 수 있어 서비스 업체 또는 저작권자들이 보다 다양한 비즈니스 모델을 창출해 낼 수 있게 하고, 사용자들의 합리적인 사용에 대한 요구사항들에 대응할 수 있게 한다.

또 다른 차별성으로 콘텐츠의 보안성 향상을 들 수 있다. 하나의 CEK로 암호화하였을 경우에는 만약의 경우 이 CEK가 누출된다면 이 전자책은 더 이상 저작권 보호를 받을 수 없다. 하지만 이 방법은 여러 개의 CEK로 암호화되어 하나의 CEK로 암호화된 경우보다 보안성이 그만큼 높다고 할 수 있다.

참 고 문 헌

[1] Wikipedia, ePUB, Available: http://en.wikipedia.org/wiki/ePUB

[2] Wikipedia, DRM, Available: http://en.wikipedia.org/wiki/Drm

[3] IDPF, OPS, Available: http://idpf.org/ePUB/20/spec/OPS_2.0.1_draft.htm

[4] IDPF, OPF, Available: http://idpf.org/ePUB/20/spec/OPF_2.0.1_draft.htm

[5] IDPF, OCF, Available: http://idpf.org/ePUB/20/spec/OCF_2.0.1_draft.doc

[6] 강호갑, 김태현외, “전자책 DRM의 상호호환성을 지원하는 ePub 기반 표준 프레임워크에 관한 연구”, p235-245, 제 11권 제6호, 한국인터넷방송통신학회 논문지, 2011.

[7] XrML, ContentGaurd, Available: http://www.xrml.org/

[8] ISO/IEC, ISO/IEC IS 21000-5. Rights Expression Language

[9] Amazon, Available: http://www.amazon.com/

[10] Fasoo.com, Available: http://www.fasoo.com/

[11] 교보문고, Available: http://www.kyobobook.co.kr/

[12] 인터파크, Available: http://www.interpark.co.kr/

[13] 한국이퍼브, Available: http://k-ePUB.tistory.com/

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

[15] Adobe, Available: http://www.adobe.com/

[16] 인큐브테크, Available: http://www.incube.co.kr/

[17] 유니닥스, Available: http://www.unidocs.co.kr/

[18] 마크애니, Available: http://www.markany.com/

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

저자 소개

김 은 범(정회원)

- 2000 호서대학교 대학원 전자계산학과(이학석사)
- 2003 ~ 2004 (주)벅스뮤직 정보기술연구소 과장
- 2006 ~ 현재 (주)파수닷컴 수석연구원
- E-mail : icesnake@fasoo.com

김 경 일(정회원)

- 1993 연세대학교 전자공학과 졸업(학사)
- 2004 The University of Texas at Austin, MBA(석사)
- 1994 ~ 2001 로커스 ㈜
- 2005 ~ 2006 넷피아닷컴
- 2006 ~ 2006 와이더댄
- 2006 ~ 현재 ㈜파수닷컴 전략사업본부 CP사업부장
- E-mail : kikim@fasoo.com

김 태 현(정회원)

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

<관심분야 : 저작권보호기술(DRM), 정보보안기술, 디지털시네마>

- Email : thkim@drminside.com

조 성 환(정회원)

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

<관심분야 : 영상통신, 무선네트워크, 저작권보호기술(DRM)>

- E-mail : shcho@ggu.ac.kr