http://dx.doi.org/10.7236/JIIBC.2013.13.2.127
JIIBC 2013-2-17

전자책 DRM을 위한 자동화된 표준정합성 검사 시스템에 관한 연구

A Study on the Automated Compatibility Standard Test System for eBook DRM

김태현*, 강호갑**, 안창주**, 조성환***

Tae-Hyun Kim, Ho-Gap Kang, Chang-Ju Ahn, 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. 또한 동일 연구과제에서는 이들 4개의 표준이 전자책 DRM의 실질적인 호환성을 위해 적용될 수 있도록 전자책 DRM 라이선스 프로토콜에 대한 표준안도 2012년에 수립하였다. 기술 표준들은 해당 표준 명세서를 기반으로 개발된 구현물들이 표준에 부합되게 구현되었는지를 검사하는 표준정합성 검증과정이 필수적으로 요구된다. 본 논문은 전자책 DRM 표준기술 명세서를 기반으로 한 자동화된 표준 정합성 검증 방법 및 모델을 제시하고자 한다.

Abstract The study of the compatibility of EPUB DRM, granted by the Korea Copyright Commission, as a CT R & D project (Project Title: The Development of the standard reference software technology for 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). The research project also proposed standards of ebook DRM license protocols in order for the four standards to practically apply to ebook DRM compatibility. It is necessary for technology standards to require a compatibility standard test process for testing whether implementations which were developed on the basis of the standard specification, comply with standards. This study suggests an automated compatible standard test method and a test model under the ebook DRM standard technical specification.

Key Words : EPUB, Compliance Test, DRM, Interoperability

*정회원, DRM inside(교신저자)
**정회원, DRM inside
***정회원, 금강대학교
접수일자 2013년 2월 27일, 수정완료 2013년 3월 27일
게재확정일자 2013년 4월 12일

Received: 27 February 2013 / Revised: 27 March 2013 / Accepted: 12 April 2013
*Corresponding Author: thkim@drminside.com
CTO, DRM inside, Korea

I. 서 론

IDPF (International Digital Publishing Forum)[1]에서는 전자책 기술규격으로 2011년 10월, EPUB (Electronic Publication) 3.0 표준을 발표하여 PDF 형태가 주류를 이루고 있는 전자책 산업에 새로운 기술표준을 제시하고 있다[2]. 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 전자책 산업 표준으로 자리매김하고 있다. 그러나 아직까지는 IDPF의 EPUB 표준 보호 기술 명세서에서 권장하고 있는 W3C XML Encryption[2]과 Signature[3]의 적용 방법이 다양하고, 솔루션 제공업체들의 표준 이해 방식에 차이가 있어 EPUB를 구현한 방식들 간에 상호 연동이 될 수 있을 정도의 호환성을 지원하지 못하고 있다. 이에 대해 한국저작권위원회에서는 2011년 EPUB 표준 포맷을 기반으로 IDPF에서 권고하고 있는 W3C XML Encryption과 XML Signature 대한 프로파일 표준안을 마련하여 솔루션업체들의 표준 구현 부담을 줄일 수 있도록 하였고, ITU-T X.509[4]를 기반으로 IDPF EPUB에는 언급이 없었던 인증서 프로파일 표준에 대한 정의를 하였다. 또한 권리정보 표준에 대해서도 다양한 종류의 권리표현언어가 사용되더라도 전자책에서 사용될 때 공통된 표준 의미가 사용되도록 하기 위해 권리정보 용어에 대한 표준안을 마련하여 특히 문제로 인한 권리정보 표준의 부담을 줄였다. 이들 4개의 표준안들은 각각 '전자책 DRM 암호화 명세서'[7][10], '전자책 DRM 전자서명 명세서'[8][11], '전자책 DRM 인증서 명세서'[9][12], '전자책 DRM 권리용어 정의'[6][13] 라는 제목으로 ODPF[14]와 TTA[15]를 통해 2012년 국내 산업표준화가 완료되었다.[2]

추가적으로 2012년에는 4개의 표준들을 기반으로 전자책 DRM 라이선스 발급 프로토콜에 대한 표준화가 진행 중에 있어 전자책 산업은 이기종 DRM의 공존을 인정하면서도 진정한 의미의 호환을 바라볼 수 있는 계기가 마련되었다. 더욱이 위에서 언급한 표준들은 모두 산업계의 실적용을 위해 참조할 수 있는 레퍼런스 소프트웨어가 공개되어 있기 때문에 산업계의 적용도 매우 빠르고 용이하게 이루어질 것으로 예상된다.

전자책 DRM 기술 명세서에 대한 표준화가 완료되면 표준 명세서를 기반으로 구현된 개발물들은 표준에 맞게 개발되었는지를 검사하는 표준정합성 검증이 필요하다. 표준정합성 검증은 주로 검증 시나리오에 따라 검사관이 수작업을 통해 검증을 하고 있지만, 반복적으로 이루어지는 검증 작업의 효율성 개선 측면과 검증 결과에 대한 신뢰성 보장 측면, 그리고 비용적인 면을 감안해 보았을 때 수작업 보다는 자동화된 툴을 통한 검증 방법이 필수적으로 요구된다. 현재 IDPF에서는 EPUB 2.0 및 3.0 표준을 준수하는 EPUB 콘텐츠에 대한 자동 검증 사이트[16]를 시범 운영하고 있다. 그러나 이 사이트는 대부분 EPUB 표준 항목에 대한 문법적(syntax)인 검사를 하고 있을 뿐이며, 의미적(semantics)인 검사를 하는 데에는 한계가 있는 것으로 분석되었다. 또한 콘텐츠 자체에 대한 데이터 검증만을 하고 있고, 기능 검증이나 프로토콜 검증과 같은 검증 자료를 필요로 하는 자동 검증은 구현되어 있지 않은 상태여서 공식적인 검증 사이트로 활용하기에는 한계가 있다.

본 논문에서는 2011년 한국 저작권위원회 주관으로 진행된 4개의 전자책 DRM 표준들과, 2012년에 개발된 전자책 DRM 라이선스 발급 프로토콜을 분석하고 이들 표준들에 대한 적용 결과물들을 검증해 주는 자동화된 표준 정합성 검증 모델을 다룬다.

II. 전자책 DRM 표준 명세서

전자책 DRM을 위한 자동화된 표준정합성 검사의 대상이 되는 표준 기술명세서는 암호화, 전자서명, 인증서, 권리표현 부분에 대한 것으로 2012년 ODPF와 TTA에 각각 등록이 되어 있으며, 라이선스 획득 프로토콜은 표준안 개발이 완료되어 표준화가 진행 중에 있다. 표 1은 전자책 DRM 표준정합성 검증 대상이 되는 표준들의 구성을 보여준다.

표 1. 전자책 DRM 표준 정합성 대상 표준 구성
Table 1. Standards for eBook DRM compatibility standard test

표준 제목	표준문서/등록기관	등록일
전자책 DRM 암호화 명세서	ODPF KR 02-2:2012[7]/ ODPF	2012.x.x
	TTAK.OT-10.0332[10]/ TTA	2012.12.21
전자책 DRM	ODPF KR 02-3:2012[8]/ ODPF	2012.x.x

전자서명 명세서	TTAK.OT-10.0333[11]/ TTA	2012.12.21
전자책 DRM 인증서 명세서	ODPF KR 02-4:2012[9]/ ODPF	2012.x.x
	TTAK.KO-10.0624[12]/ TTA	2012.12.21
전자책 DRM 권리용어 정의	ODPF KR 02-1:2012[6]/ ODPF	2012.x.x
	TTAK.KO-10.0625[13]/ TTA	2012.12.21
전자책 DRM 라이선스 획득 프로토콜	-	-

1. 전자책 DRM 암호화 명세서

이 표준은 IDPF EPUB 표준에서 암호화 방식으로 권고하고 있는 W3C XML Encryption에 대한 프로파일을 규정하고 있다. 프로파일의 규정 근거는 구현범위에 대한 축소와 보안성 강화에 있다. 현재 W3C 표준에서 사용될 수 있는 암호화 알고리즘과 키 길이, 키 저장 방식은 매우 다양한 종류와 방식으로 사용될 수 있기 때문에 W3C Encryption 표준을 그대로 사용할 경우 보안 취약성이 있는 알고리즘과 키 길이가 사용될 수 있어 보안적인 허점이 존재할 가능성이 존재한다. 또한 표준 명세서를 기반으로 솔루션을 제작해야하는 산업체 입장에서는 다양한 구현 가능성이 존재하는 W3C 표준을 포괄적으로 적용할 수 있는 제품을 만들기가 매우 어렵다는 문제가 존재한다. 이에 따라 데이터 암호화와 키 암호화 부분에서 표 2와 같이 프로파일을 정의하고 있다.

표 2. 전자책 DRM 암호화 명세서 요약
Table 2. Summary of eBook DRM encryption standard

항목	주요 규정 내용		구분
데이터 암호화	대칭키	알고리즘 AES-128 이상	강제
		알고리즘 AES-128-CBC	권장
	RetrievalMethod를 통해서만 참조		강제
키 암호화	비대칭키	알고리즘 RSA-2048 이상	강제
		알고리즘 OAEP 방식	권장
	대칭키	알고리즘 AES-128 이상	강제

2. 전자책 DRM 전자서명 명세서

이 표준은 IDPF EPUB 표준에서 전자서명 방식으로 권고하고 있는 W3C XML Signature에 대한 프로파일을 규정하고 있다. 프로파일의 규정 근거는 구현범위에 대한 축소와 보안성 강화에 있다. 현재 W3C 표준에서 사용될 수 있는 암호화 알고리즘과 키 길이, 키 저장 방식은 매우 다양한 종류와 방식으로 사용될 수 있기 때문에 W3C Signature 표준을 그대로 사용할 경우 보안 취약성이 있는 알고리즘과 키 길이가 사용되어 보안적인 허점이 존재할 가능성이 존재한다. 또한 표준 명세서를 기반으로 솔루션을 제작해야하는 산업체 입장에서는 다양한 구현 가능성이 존재하는 W3C 표준을 포괄적으로 적용할 수 있는 제품을 만들기가 매우 어렵다는 문제가 존재한다. 이에 따라 데이터 서명정보, 키 정보, 서명대상정보 부분에서 표 3과 같이 프로파일을 정의하고 있다.

표 3. 전자책 DRM 전자서명 명세서 요약
Table 3. Summary of eBook DRM signature standard

항목	주요 규정 내용		구분
서명정보	알고리즘	RSA-SHA356	강제
	변환	알고리즘 C14NWithoutComment	
	해쉬	알고리즘 SHA256	
키 정보	X.509 인증서 사용		강제
서명대상정보	변환	알고리즘 C14NWithoutComment	강제
	해쉬	알고리즘 SHA256	

3. 전자책 DRM 인증서 명세서

이 표준은 IDPF의 EPUB를 기반으로 한 전자책 DRM을 구현함에 있어 키 전달과 전자서명을 위해 사용되는 인증서에 대한 규정을 하고 있다. 인증서 명세서는 ITU-T의 X.509 프로파일로 구성되어 있다. 프로파일에 대한 규정 근거는 다른 표준과 동일하게 구현범위에 대한 축소와 보안성 강화에 있다. 현재의 X.509 포맷은 사용할 수 있는 알고리즘 및 형식이 매우 다양하기 때문에, 범용 표준으로 적용하기에는 구현 및 검증이 매우 복잡하다. 또한 알고리즘의 종류 및 비도 등이 구체적이지 않아 보안에 취약한 알고리즘과 비도가 사용될 가능성도 존재한다. 이에 따라 데이터 서명정보, 키 정보, 서명대상정보 부분에서 표 4와 같이 프로파일을 정의하고 있다.

표 4. 전자책 DRM 인증서 명세서 요약
Table 4. Summary of eBook DRM certificate standard

항목	주요 규정 내용		구분
저장 방식	인코딩	ASN.1 DER	강제
	파일포맷	ASCII 파일 : PEM	
		이진 파일 : DER	
기본 필드	버전	V3	강제
	서명알고리즘	sha256withSHAEncryption	
	일련번호	64비트 크기 양의 정수	
	발급자	DnQualifier 사용	
	대상자	DnQualifier 사용	
	공개키비도	키 길이 : 2048 비트	
		지수 : 65537	
	유효기간	기존 표준과 동일	
확장 필드	키사용	인증용, 서명용, 인증서 발급용 구분	강제
	기본제한	CA 구분	강제
	인증기관 ID	ROOT CA ID 식별	선택
	타 확장	Critical mark 사용금지	강제

4. 전자책 DRM 권리용어 정의

이 표준은 IDPF의 EPUB를 기반으로 한 전자책 DRM을 구현함에 있어 EPUB 표준에서 규정하지 않고 있는 권리표현언어에 대한 호환성을 지원하기 위해 권리용어에 대한 정의를 규정하고 있다. 권리용어정의는 표 5에 열거되어 있는 것과 같이 사용용도 10개, 사용제한 12개, 사용조건 1개에 대한 용어를 정의하고 있다.

표 5. 전자책 DRM 인증서 권리용어 요약
Table 5. Summary of eBook DRM rights terms definition

항목	정의 항목
사용용도	보기, 재생, 인쇄, 가상인쇄, 물리적인쇄, 대여, 양도, 추출, 복제, 이동
사용제한	절대적기간, 상대적기간, 횟수, 사용자, 사용자그룹, 네트워크, 프린터, 지리적위치, 소프트웨어, 하드웨어, 선행제한, 대안제안
사용조건	동의

5. 전자책 DRM 라이선스 획득 프로토콜

이 표준은 전자책 DRM 클라이언트가 전자책 DRM 라이선스 발급 서버로부터 표준화된 라이선스(권리정보, 암호화 정보, 전자서명 정보)를 발급받기 위한 프로토콜을 정의하고 있다. 라이선스 획득 프로토콜 명세서는 HTTP 기반의 통신 프로토콜로 구성되어 있다. 라이선스 획득 프로토콜의 규정 근거는 전자책 서비스 사업자들 간에 라이선스 발급 과정을 표준화하여 최종 소비자의 사용 편리성을 높이는 것에 목적을 두고 있다. 전자책 DRM에 관련된 포맷이 EPUB 표준과 위에서 서술한 인증서 표준, 전자서명 표준, 인증서 표준을 준수하여 제작되었다고 하더라도, 이에 대한 정보를 전달과정이 표준화 되어 있지 않다면 전자책 DRM 단말기는 서비스 사업자간에 호환성을 보장하기 어렵다는 문제가 상존한다. 이에 따라 표 6에서와 같이 3단계(시작-상호인증-라이선스 요청/발급) 또는 2단계(시작-라이선스 요청/발급) 메시지로 구성된 프로토콜을 정의하고 있다.

표 6. 전자책 DRM 라이선스 프로토콜 메시지 구성
Table 6. 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

III. 전자책 DRM 표준 정합성 검증 구성

전자책 DRM 표준 기술명세서를 기반으로 제작된 개발물들은 전자책 DRM 패키저, 전자책 DRM 뷰어, 전자책 라이선스 발급 서버 및 클라이언트로 구분된다. 이러한 전자책 DRM 개발물들을 대상으로 하는 정합성 검증은, 패키저를 통해서 제작된 전자책 DRM 콘텐츠에 대해서는 콘텐츠의 구성 포맷과 형식이 표준과 부합하는지 여부를 검사하는 데이터 검증이 있고, 뷰어에 대해서는 정합 또는 비정합 DRM 콘텐츠를 입력하여 정상적으로 처리하는지 여부를 확인하는 기능 검증이 있으며, 라이선스 발급 서버와 클라이언트에 대해서는 라이선스 발급을 위한 표준 프로토콜의 준수 여부를 검증하

는 프로토콜 검증이 있다. 표 7은 전자책 DRM 표준 정합성에 대한 검증 항목과 검증자료에 대한 내용을 보여준다.

표 7. 전자책 DRM 표준 정합성 검증 종류
Table 7. Type of eBook DRM compatibility standard test

검증 종류		내용
검증 항목	데이터 검증	전자책 DRM 콘텐츠 검사
	기능 검증	전자책 DRM 콘텐츠 뷰어 검사
	프로토콜 검증	전자책 DRM 라이선스 발급 클라이언트 및 서버 검사

1. 데이터 검증

전자책 DRM 표준정합성 검증에 있어서의 데이터 검증은 패키징된 전자책 DRM 콘텐츠가 전자책 DRM 암호화 표준, 전자서명 표준, 인증서 표준을 준수하여 제작되었는지 여부를 검증하는 과정이다. 데이터 검증 과정은 표 8에서와 같이 암호화 부문 8개, 전자서명 부문 7개, 인증서 부문 11개로 구성되어 있다.

표 8. 전자책 DRM 표준 정합성 데이터 검증 항목
Table 8. Data validation items for eBook DRM compatibility standard

항목	검증 항목	표준근거
암호화	암호화 정보 파일 추출	EPUB OCF3.0[17] 3.1
	문법 정합성	EPUB OCF3.0 3.5.2
	데이터 암호화 알고리즘	TTAK.OT-10.0332 5.2.1
	데이터 암호화 키 정보	TTAK.OT-10.0332 5.2.2
	암호화된 데이터 정보	TTAK.OT-10.0332 5.2.3
	키 암호화 알고리즘	TTAK.OT-10.0332 5.3.1
	키 암호화 키 정보	TTAK.OT-10.0332 5.3.2
	암호화된 키 정보	TTAK.OT-10.0332 5.3.3
전자서명	전자서명 정보 파일 추출	EPUB OCF3.0 3.1
	문법 정합성	EPUB OCF3.0 3.5.6
	전자서명 알고리즘	TTAK.OT-10.0333 5.2.1
	전자서명 대상 정보	TTAK.OT-10.0333 5.2.2
	전자서명에 사용된 인증서 검증	TTAK.OT-10.0333 5.2.3
	신뢰할 수 있는 인증서 체인 검증	TTAK.KO-10.0624 5.4
	전자서명 검증	ITU-T X,509
인증서	표현방식	TTAK.KO-10.0624 5.1
	시리얼번호	TTAK.KO-10.0624 5.2.2
	전자서명 알고리즘	TTAK.KO-10.0624 5.2.3
	전자서명 무결성	ITU-T X,509
	공개키 무인	TTAK.KO-10.0624 5.2.4[6]
	발급자, 수신자 정보	TTAK.KO-10.0624 5.2.4[6]
	기간 검증	TTAK.KO-10.0624 5.2.5
	공개키 정보	TTAK.KO-10.0624 5.2.7
	CA 식별자 정보	TTAK.KO-10.0624 5.2.10
	상위 인증서 정보	TTAK.KO-10.0624 5.2.10
	말단 인증서 정보	TTAK.KO-10.0624 5.2.10

2. 기능 검증

전자책 DRM 표준정합성 검증에 있어서의 기능 검증은 전자책 DRM 표준에 따라 제작된 전자책을 열람하고자 하는 장치 또는 응용프로그램(이하 전자책 처리기)이 표준을 준수하여 제작되었는지 여부를 검증하는 과정이다. 기능 검증은 표 9에서와 같이 복호화 처리 부문 13개, 전자서명 부문 16개, 인증서 부문 8개의 검증 데이터를 대상으로 진행된다.

표 9. 전자책 DRM 표준 정합성 기능 검증 항목
Table 9. Function validation items for eBook DRM compatibility standard

항목	검증 항목	분류
복호화 처리	기본 복호화 처리	정합성 검증
	복수데이터 단일키 처리	
	복수데이터 복수키 처리	
	데이터 암호화 알고리즘 오류	비정합성 검증
	키 암호화 알고리즘 오류	
	키 미존재	
	키 정보 오류	
	키 표기 방법 오류	
	암호화된 데이터 정보 오류 (5개)	
전자서명 처리	기본 전자서명 처리 기능	정합성 검증
	복수 전자서명 지원	
	전자서명 데이터 오류	비정합성 검증
	전자서명 대상 오류	
	서명 인증서 미존재	
	전자서명 오류 (5개)	
	인증서 체인 오류 (5개)	
	유효하지 않은 CA	
인증서 처리	기본 인증서 처리	정합성 검증
	표현방식 처리 오류	비정합성 검증
	전자서명 알고리즘 오류	
	인증서 유효기간 오류	
	공개키 무인 오류	
	공개키 종류 오류	
	전자서명 검사 오류	
	인증서 종류별 정보 유효성 오류	

3. 프로토콜 검증

전자책 DRM 표준정합성 검증에 있어서의 프로토콜 검증은 라이선스 발급을 요청하는 전자책 DRM 클라이언트와 발급 주체가 되는 라이선스 발급서버가 각각 프로토콜 표준에 맞게 구현이 되었는지 여부를 검증하는 과정이다.

표 10. 전자책 DRM 표준 정합성 프로토콜 검증 항목
Table 10. Protocol validation items for eBook DRM compatibility standard

항목		검증 항목	표준근거
클라이언트	2단계	hello 메시지	LAP[18] 2.2.3.2
		getLicense 메시지	LAP 2.2.3.6
	3단계	hello 메시지	LAP 2.2.3.2
		mutualAuth 메시지	LAP 2.2.3.4
		getLicense 메시지	LAP 2.2.3.6
서버	2단계	reponseHello 메시지	LAP 2.2.3.3
		responseGetLicense 메시지	LAP 2.2.3.7
	3단계	responseHello 메시지	LAP 2.2.3.3
		responseMutaulAuth 메시지	LAP 2.2.3.5
		responseGetLicense 메시지	LAP 2.2.3.7

IV. 전자책 DRM 표준 정합성 자동 검증 시스템

Ⅱ 절에서 설명된 표준 정합성 항목들에 대해서 자동화된 검증 시스템은 데이터 검증을 위해서는 가상의 전자책 뷰어가 존재하여야 하고, 프로토콜 검증을 위해서는 대상이 되는 가상의 전자책 DRM 클라이언트와 서버가 존재하여야 한다. 또한 기능 검증을 위한 정합/비정합 검증 자료도 필요하다. 그리고 검증 결과에 대해 공식적인 보고서를 자동으로 출력해 줄 수 있는 보고서의 생성기능도 요구된다. 이 시스템은 단독 응용프로그램으로 제작되어 검증을 원하는 업체에 제공되거나 또는 웹 응용프로그램으로 제작되어 네트워크를 통해 검증이 이루어질 수도 있다. 그림 1은 전자책 DRM을 위한 자동화된 표준정합성 검사 시스템에 대한 개념도를 보여준다.

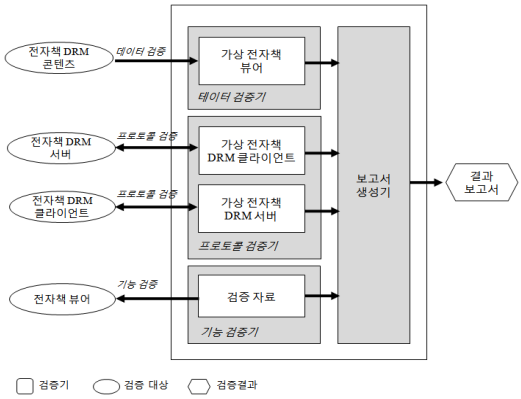

그림 1. 전자책 DRM 표준 정합성 자동검증 시스템 개념도
Fig. 1. Overview of automated compatibility standard test system for eBook DRM

1. 가상 전자책 뷰어

가상 전자책 DRM 뷰어는 데이터 검증에 사용된다. 데이터 검증에서는 검증대상이 되는 전자책 DRM 콘텐츠를 입력 받아 데이터 검증 항목에 대해 자동으로 검증을 완료한 후의 결과를 보고서 형식으로 출력하는 역할을 수행한다. 가상 전자책 뷰어는 암호화된 콘텐츠의 키 정보를 획득하기 위해서는 가상 전자책 DRM 클라이언트를 이용한다.

2. 가상 전자책 DRM 클라이언트

가상 전자책 DRM 클라이언트는 서버 프로토콜 검증에 사용된다. 검증은 검증 대상이 되는 전자책 DRM 서버에 실제 구동환경과 동일하게 서버 프로토콜 검증항목에 대한 메시지를 전송하고 응답된 메시지를 분석하여 보고서를 생성하는 역할을 수행한다.

3. 가상 전자책 DRM 서버

가상 전자책 DRM 서버는 클라이언트 프로토콜 검증용으로 사용되는데, 검증대상이 되는 전자책 DRM 클라이언트로부터 메시지를 전달받고, 이에 대한 결과를 응답 메시지 또는 결과 보고서 형태로 전송하는 역할을 수행한다. 이때 전자책 DRM 클라이언트는 클라이언트 프로토콜 검증항목에 기술된 메시지들을 모두 가상 서버에 전송하여 메시지의 표준정합성을 검증 받는다.

4. 검증 자료

검증 자료는 검증 대상이 되는 전자책 DRM 클라이

언트 또는 전자책 뷰어의 표준정합성 검증을 하기 위해 제공되는 정합 또는 비정합 전자책 DRM 콘텐츠를 의미한다. 검증자료는 기능검증 항목을 검증할 수 있도록 정상적인 전자책 DRM 콘텐츠(정합)와 비정상적인 전자책 DRM(비정합) 콘텐츠로 구성되어 있다. 정합 검증 자료는 열람을 용도로 제작된 검증 대상 소프트웨어가 표준에 부합하는 전자책 DRM 콘텐츠들을 정상적으로 처리하는지 여부를 검사하는 용도로 사용되고, 비정합 검증 자료는 검증 대상 프로그램이 비정상적인 전자책 DRM 콘텐츠들에 대해서도 비정상 종료와 같은 프로그램 오류 없이 작동하는지 여부를 검사하는 용도로 사용된다.

5. 보고서 생성기

보고서 생성기는 가상 전자책 DRM 클라이언트 또는 서버로부터 데이터 검증, 프로토콜 검증에 대한 결과를 기반으로 검사자가 원하는 형태의 포맷으로 결과 보고서를 자동으로 생성해 주는 기능을 수행한다.

V. 구현

전자책 DRM을 위한 자동화된 표준화 검증 시스템은 웹 환경에서 네트워크를 통해 검증을 할 수 있도록 구현되었다. 개발에 사용된 소프트웨어 환경은 표 11과 같다.

표 11. 전자책 DRM 인증서 명세서 요약
Table 11. Summary of eBook DRM rights terms definition

항목		사용 기술/환경
데이터 검증기		OpenSSL, LibXML, ZibArchieve
프로토콜 검증기	서버	OpenSSL, LibXML
	클라이언트	OpenSSL, LibXML, ZibArchieve
기능 검증기		Javascript
보고서 생성기		XML, XSTL
공통환경		Java servlet, VC++, Apache tomcat

1. 데이터 검증

데이터 검증은 웹 환경에서 검증대상이 되는 EPUB 콘텐츠를 업로드하면 표준정합성 검증서버의 전자책 DRM 가상 클라이언트가 자동으로 데이터 검증을 실시하고 결과를 보고서 형식으로 출력해 주는 과정으로 진행된다. 그림 2는 데이터 검증을 위한 표준정합성 검증서버 초기 화면을 보여준다.

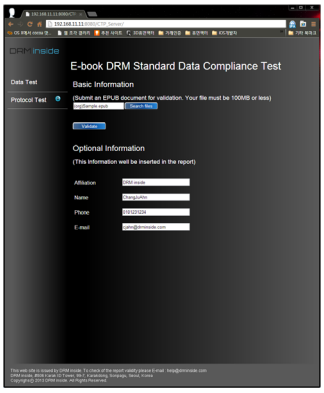

그림 2. 데이터 검증 화면
Fig. 2. Data validation screen

2. 프로토콜 검증

가. 서버검증

프로토콜 검증에서 서버 검증은 웹 환경에서 검증대상이 되는 전자책 DRM 라이선스 발급 서버에 대한 접속 정보를 입력하고 검증을 요청하면 표준정합성 검증서버의 전자책 DRM 가상 클라이언트가 검증 대상 서버에 대해서 자동으로 프로토콜 메시지를 전송하고 응답 메시지를 분석하여 결과를 보고서 형식으로 출력해 주는 과정으로 진행된다. 그림 3은 서버 프로토콜 검증을 위한 표준정합성 검증서버 초기 화면을 보여준다.

나. 클라이언트 검증

프로토콜 검증에서 클라이언트 검증은 클라이언트가 직접 표준정합성 검증서버에 접속하여 테스트를 시행하거나, 클라이언트가 전송하게 될 프로토콜 메시지를 표준정합성 검증 서버에 입력하고 메시지에 대한 검증을 요청할 수 있다. 표준정합성 검증 서버의 전자책 DRM 가상 서버는 클라이언트로부터 직접 메시지를 수신 받게 되는 경우 응답 메시지를 프로토콜 규격에 따라 전송해 주고, 웹을 통해 클라이언트 메시지에 대한 검증을 요청한 경우 이에 대한 검증 결과를 보고서 형식으로 출력해 주는 과정으로 진행된다. 그림 3은 클라이언트 프로토콜 검증을 위한 표준정합성 검증서버 초기 화면을 보여준다.

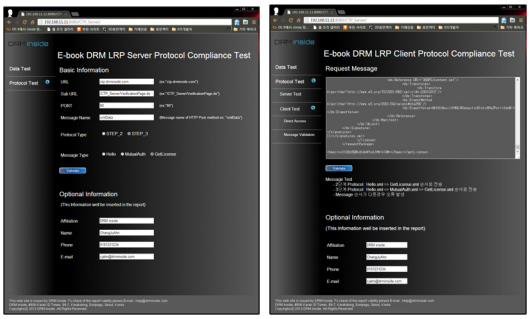

그림 3. 프로토콜 검증 화면
Fig. 3. Protocol validation screen

3. 기능 검증

기능 검증은 웹 환경에서 제공되는 정합 또는 비정합 검증용 데이터를 다운받아 검증하고자 하는 전자책 뷰어 또는 전자책 관련 응용프로그램에 입력을 하는 과정으로 진행된다. 이때 발생되는 검사 결과에 대해서 검사자는 웹 화면을 통해 입력을 하고 집계된 결과를 보고서 형식으로 출력해 주는 과정으로 진행된다. 그림 4는 기능 검증을 위한 정합 또는 비정합 자료를 제공하는 화면을 보여준다.

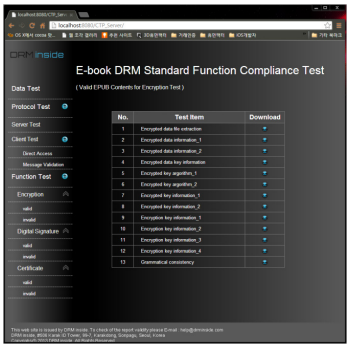

그림 4. 기능검증 자료화면
Fig. 4. Test materials screen

4. 보고서 생성

표준정합성 검증서버에서의 모든 검증 결과는 XML 형태로 저장된 이후에, XSLT에 의해 HTML로 자동 출력된다. 그림 5는 XLST에 의해 변환된 검증결과 보고서 화면을 보여준다.

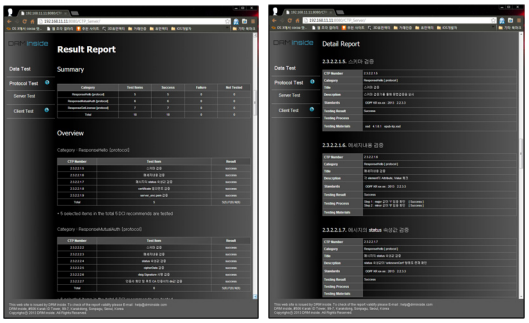

그림 5. 보고서 화면
Fig. 5. Report screen

VI. 결론

본 논문은 2012년 TTA와 ODPF에 등록된 4건의 전자책 DRM 표준들과 이들 표준을 기반으로 제작된 전자책 DRM 라이선스 획득 프로토콜에 대한 개략적인 기술을 분석한 후, 이들 표준들을 기반으로 구현된 전자책 DRM 콘텐츠, 뷰어, 클라이언트, 서버에 대한 표준정합성 검증 방법에 대한 방안을 제시하였다. 제안한 모델은 현재 문화체육관광부의 CT R&D 연구과제(과제명 : 국제표준의 EPUB 기반 전자책 DRM 표준 레퍼런스 소프트웨어 기술 개발)를 통해 개발이 이루어지고 있다. 전체 연구는 2011년 6월부터 2013년 3월까지 2년간에 걸쳐 진행되고 있으며, 현재 전자책 DRM 표준 정합성 검증 표준에 대해서는 검증 규격 명세서 및 자동검증 사이트 개발에 대한 마무리 작업이 진행되고 있다. 본 연구를 통해 개발된 전자책 DRM 표준정합성 검증 표준은 향후 전자출판물표준화포럼의 DRM프로젝트그룹에서 국내 대부분의 DRM 업체들이 참여한 가운데 기술검토 후 TTA의 PG421(디지털콘텐츠 프로젝트그룹) DRM 실무반을 통해 국내 산업 표준으로 진행될 예정이다.

현재 진행 중인 연구가 마무리되게 되면 전자책 DRM 표준을 기반으로 제작되는 콘텐츠 및 관련 소프트웨어들의 개발과 검증이 매우 용이해져 보다 많은 업체들이 전자책 DRM 표준 기술 적용에 참여 할 수 있으리라 기대된다. 또한 전자책 DRM 국제 표준화 단체인 IDPF에서는 연구기간동안의 교류를 통하여 본 연구 결과를 IDPF EPUB 표준의 표준 정합성 검증 시나리오 및 검증 시스템에 활용하기 위한 방안이 모색 중에 있

는바, 본 연구 결과가 국제 전자책 표준에 대한 기여할 수 있기를 기대해 본다.

참 고 문 헌

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

[2] Tae-Hyun Kim et al., "A Study of License acquisition Method Supporting Mutual Compatibility of EPUB-based eBook DRM", Vol 13, No. 1, The Journal of The Institute of Internet, Broadcasting and Telecommunication, pp.205-214, 2013

[3] W3C, W3C XML Encryption, 2002

[4] W3C, W3C XML Signature, 2008

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

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

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

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

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

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

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

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

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

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

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

[16] IDPF EPUB Validator, Available: http://validator.idpf.org/

[17] IDPF OCF3.0 Available: http://idpf.org/epub/30/spec/epub30-ocf.html

[18] ODPF KR xx-x:2013, License Acquisition Protocol

※ 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 : DRM인사이드 전략기획실장
<주관심분야 : 저작권보호기술(DRM), 정보보안기술, 리버스 엔지니어링, 디지털시네마>

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 : DRM인사이드 연구소장
<주관심분야 : 저작권보호기술(DRM), 디지털시네마>

안 창 주(정회원)

• 2012년 : 경기과학기술대학교 컴퓨터 정보 시스템과 (전문학사)
<주관심분야 : 저작권보호기술(DRM)>

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)>