제3절 e-Book DRM 보안정보 관리기술 현황

e-Book DRM의 보안정보 관리기술에는 정보를 암호화하는 암호화기술, 정보에 대한 신뢰성 및 무결성을 보장해 주는 전자서명 기술, 그리고 암호화 및 전자서명에 필요한 인증서 기술이 필요하다. IDPF에서는 이를 위해 W3C XML 표준 (Encryption, Signature)의 사용을 권고하고 있고 ITU-T에서는 전자서명 정보관리 기술로 X.509 기술을 권고하고 있다.

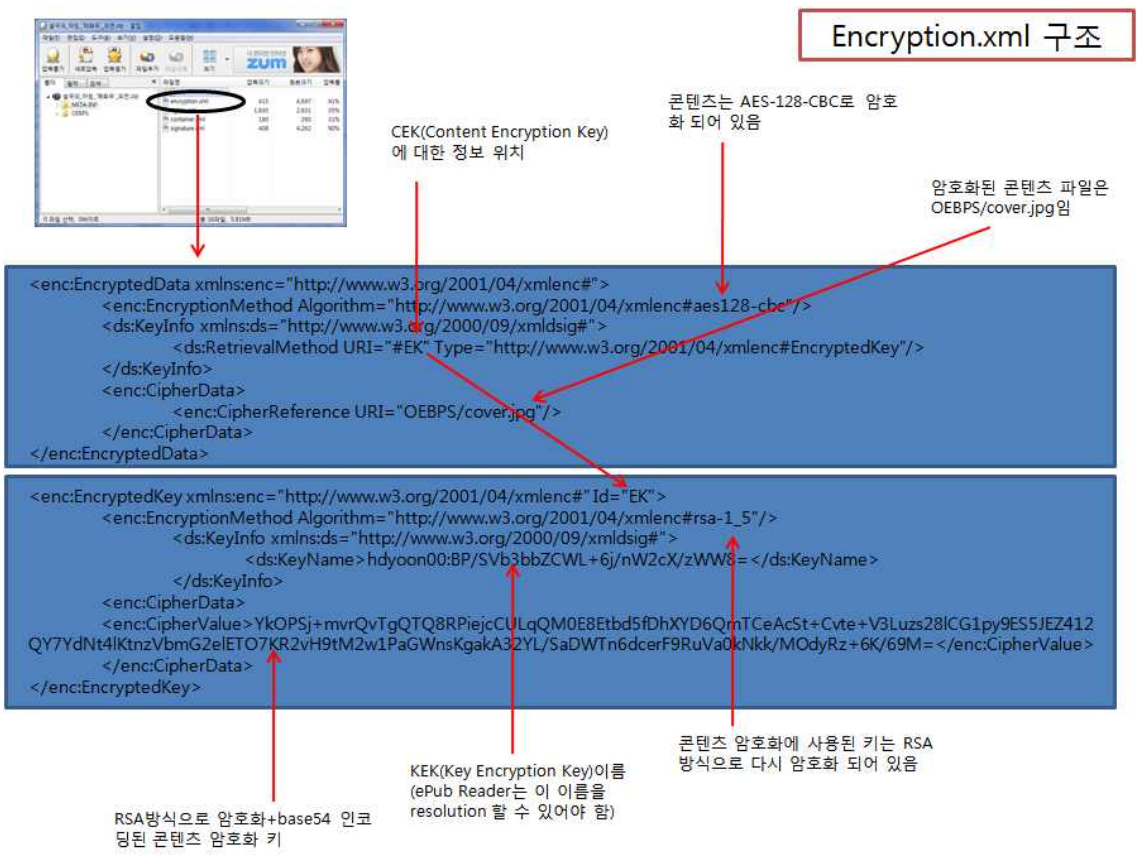
[표 9] e-Book DRM 보안정보 관리기술

구분	표준명	비고
암호정보 관리기술	W3C XML Encryption	IDPF EPUB 지정
전자서명정보 관리기술	W3C XML Signature	IDPF EPUB 지정
인증서정보 관리기술	X.509 Certificate	인증서 de-facto 표준

1. ePub에서의 encryption.xml 사용 예

IDPF의 EPUB 표준에서는 암호화된 데이터와 키에 대한 전달을 W3C XML Encryption 표준의 xenc:encryptedData와 xenc:encryptedKey를 사용할 것을 권고하고 있다.

다음은 W3C XML Encryption 방식을 사용하여 IDPF의 EPUB의 encryption.xml에서의 xenc:encryptedData와 xenc:encryptedKey 정보를 표현하는 한 예를 보여준다.



[그림 6] ePub에서의 encryption.xml 사용예