나. e-Book DRM 기술 분석

1) 개요

IDPF의 e-Book 보안은 OCF(Open Container Format)에서 옵션 사항으로 다루고 있으나 기술규격 측면에선 매우 미흡한 수준에 머무르고 있다. OCF에 정의된 전자서명, 암호화, 저작권 정보에 대한 메타데이터는 다음과 같다.

- Digital Signatures(META-INF/signatures.xml) : W3C XML Signature 방식을 이용하여 e-Book 파일들에 대한 전자서명 값 표기
- Encryption (META-INF/encryption.xml) : e-Book 파일들을 암호화할 경우 이에 대한 암호화 영역, 암호화 알고리즘 및 키에 대한 정보 표기
- Right Management (META-INF/rights.xml) : 적용되는 DRM 정책에 대한 정보 표기 (현재 포맷이 정해져 있지 않다.)

2) encryption.xml

선택 가능한 항목인 encryption.xml 파일은 콘테이너 파일시스템의 최상위단에 있으면서 EPUB 콘테이너의 콘텐츠들에 대한 모든 암호화 정보를 담고 있다. 이 파일은 최상위 엘리먼트로 encryption을 가지고 있는 XML 문서이다. encryption 엘리먼트는 W3C XML Encryption에서 정의하고 있는 EncryptedKey와 EncryptedData 타입의 자식 엘리먼트를 가진다. 각각의 EncryptedData 항목은 컨테이너안에 있는 하나 또는 그 이상의 파일이 어떻게 암호화 되어 있는지를 묘사한다. 결론적으로 컨테이너안에 어떠한 리소스가 암호화 되어 있다면, encryption.xml은 리소스가 암호화되어 있다는 것을 알리기 위해 반드시 존재해야하고, 이것이 어떻게 암호화되었는지에 대한 정보를 제공해야 한다.

3) signatures.xml

선택 가능한 항목인 signatures.xml 파일은 콘테이너 파일시스템의 최상위단에 있으면서 콘테이너와 콘텐츠들에 대한 전자서명 정보들 담고 있다. 이 파일은 최상위 엘리먼트로 signature를 가지고 있는 XML 문서이다. signature 엘리먼트는 W3C XML Signature에서 정의하고 있는 Signature 타입의 자식 엘리먼트를 가진다. 서명은 출판물과 어떤 다른 대안의 단위 출판물에 대한 전체 또는 일부의 전자서명에 적용될 수 있다. XML Signature는 XML말고도 다른 형태의 어떠한 데이터에도 적용가능하다.

4) rights.xml

rights.xml에 대한 포맷은 정해진 표준이 없지만 이에 사용될 수 있는 REL로는 “Rights and Rules Coordinated Requirements”에서 정의하는 요구사항을 준수할 것을 권장하고 있다.