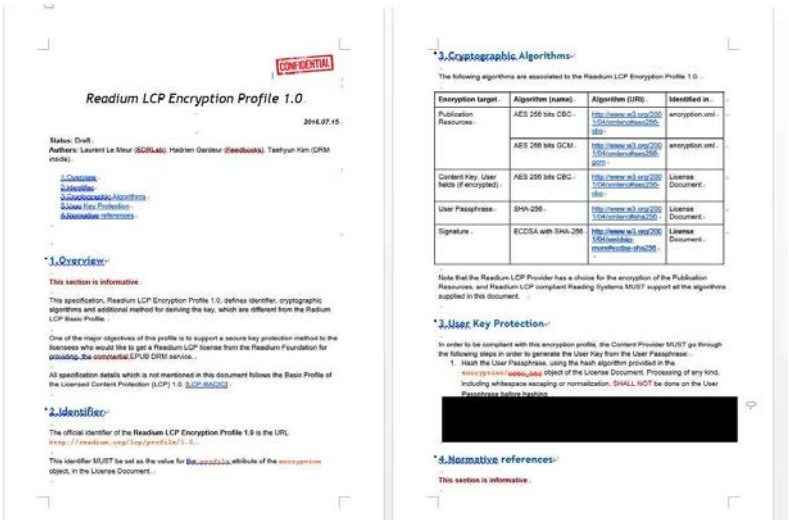
1. Readium LCP 확장 기술 개발

컨소시엄 기존 Readium LCP 표준에서 비밀번호 기반의 키 관리 방식의 보안적인 문제점을 방지하기 위해 비밀키를 사용할 수 있는 Readium LCP Encryption Profile 명세서를 작성하여 Readium에 기고하였으며, 비밀번호 방식의 근본적인 문제점을 해결하기 위한 방안으로 인증서기반의 키 관리를 할 수 있는 Certificate based Key Protection(CPK) Profile 명세서를 작성하여 EDRLab에 제공하였다. 또한 이들 두 명세서를 Readium SDK에 연동 구현화한 제품화단계의 산출물을 가지고 프랑스에서 열린 EPUB Summit 회의장과 일본 전시회(Content Tokyo 2016)에 참가하여 데모 시연을 하였다.

가. 표준안 설계

1) Readium LCP encryption profile

- Readium LCP encryption profile 1.0에 대한 기술 명세서 작성
- 프로파일 v1.0에서 사용되는 암호화 알고리즘 그리고 User Key를 보호하기 위한 비밀키 방법을 기술하고 있음
- 표준명세서 작성 후 LCP 명세서 author 들 간에 google doc 문서 공유 (https://docs.google.com/document/d/1ZIv64jTZIQoDcayE41KnLSZtnhxKbdZE_V6wRbzPYB0/edit)
- 본 문서는 LCP 라이선스 계약 업체에게만 제공되는 비공개 기술 문서로 EDRLab에서 별도로 관리될 예정임


CONFIDENTIAL

Readium LCP Encryption Profile 1.0

2016.07.15

Status: Draft

Authors: Laurent Le Meur (EDRLab), Hadrien Gardeur (Feedbooks), Taehyun Kim (ORM inside)

1. Overview

This section is informative.

This specification, Readium LCP Encryption Profile 1.0, defines identifier, cryptographic algorithms and additional method for deriving the key, which are different from the Radium LCP Basic Profile.

One of the major objectives of this profile is to support a secure key protection method to the licensees who would like to get a Readium LCP license from the Readium Foundation for providing the confidential EPUB DRM service.

All specification details which is not mentioned in this document follows the Basic Profile of the Licensed Content Protection (LCP) 1.0.

2. Identifier

The official identifier of the Readium LCP Encryption Profile 1.0 is the URL

3. Cryptographic Algorithms

The following algorithms are associated to the Readium LCP Encryption Profile 1.0.

Encryption target	Algorithm (name)	Algorithm (URI)	Identified in
Publication Resources	AES 256 bits CBC	http://www.w3.org/2001/04/xmlenc#aes256-cbc	encryption.xml
	AES 256 bits GCM	http://www.w3.org/2009/xmlenc11#aes256-gcm	encryption.xml
Content Key, User fields (if encrypted)	AES 256 bits CBC	http://www.w3.org/2001/04/xmlenc#aes256-cbc	License Document
User Passphrase	SHA-256	http://www.w3.org/2001/04/xmlenc#sha256	License Document
Signature	ECDSA with SHA-256	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256	License Document

Note that the Readium LCP Provider has a choice for the encryption of the Publication Resources, and Readium LCP compliant Reading Systems MUST support all the algorithms supplied in this document.

3. User Key Protection

In order to be compliant with this encryption profile, the Content Provider MUST go through the following steps in order to generate the User Key from the User Passphrase.

1. Hash the User Passphrase, using the hash algorithm provided in the object of the License Document. Processing of any kind, including whitespace escaping or normalization, SHALL NOT be done on the User Passphrase before hashing

4. Normative references

This section is informative.

☞ 자세한 내용은 별첨 Readium LCP Encryption Profile1.docx 문서 참조