

# Standardization Strategy for e-Book DRM Interoperability

2012. 10. 24

Hogab Kang

DRM inside



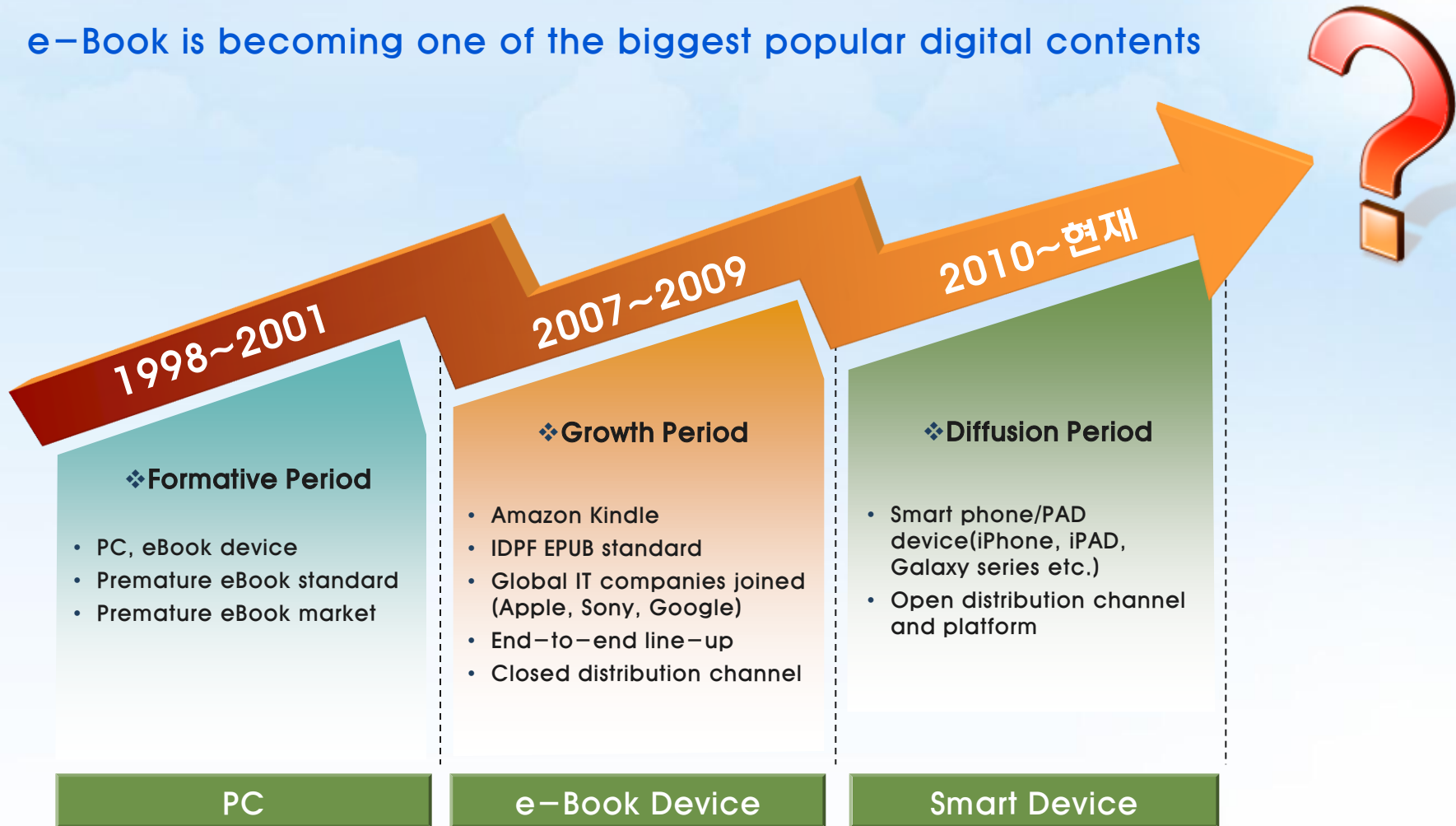
# Contents

- 1 e-Book Market Trend
- 2 DRM Interoperability Issues
- 3 e-Book DRM Standardization
- 4 Project for e-Book DRM Interoperability



## e-Book Market Trend

- ❖ e-Book is becoming one of the biggest popular digital contents



Wholesaler market volume in U.S (IDPF report)

2008 : \$ 53.3M

2009 : \$165.8M

Wholesaler market volume in U.S (GigaOM pro report)

2011 : \$ 2B

2016 : \$ 6B



# e-Book Delivery Format and Protection

❖ EPUB is becoming de-facto standard, but DRMs(Digital Rights Management) are various

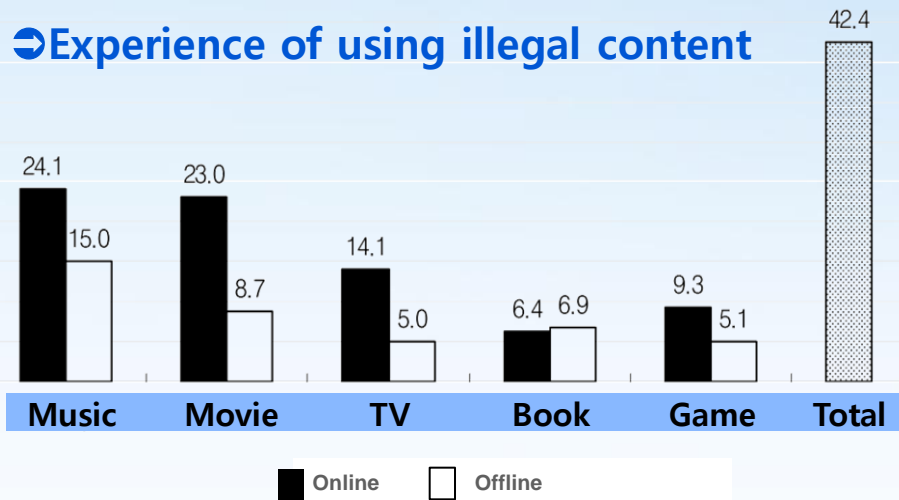
	Company	Service	Format	DRM	Number of Contents
Global	Amazon	Amazon.com	AZW	자체 DRM	600,000+
	Sony	Sony eBook Store	EPUB	Adobe DRM	600,000+
	Google	Google Editions	EPUB	Adobe DRM	12,000,000
	Apple	iBook Store	EPUB	FairPlay	90,000+
	Barnes&Noble	eBook Store	EPUB	Adobe DRM	1,000,000+
	Borders	Borders eBook Store	EPUB	Adobe DRM	1,500,000+
Korea	Kyobo	Internet Kyobo	EPUB	Fasoo.com	130,000
	Interpark	Biscuit	EPUB	Markany	80,000
	KT	Qook Book Cafe	EPUB	Incubetech	60,000
	KEPUB	K-EPUB	EPUB	Hancom	75,000
	KPC	KPC	EPUB	Markany	10,000

# How many illegal copies are in eBook market?

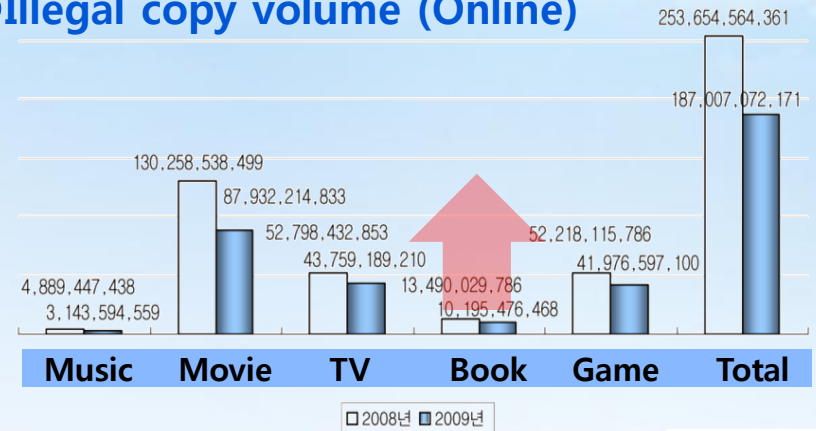
- ❖ e-Book is vulnerable to illegal copy due to relatively small content size

## ⇒ Experience of using illegal content

(단위 : %)

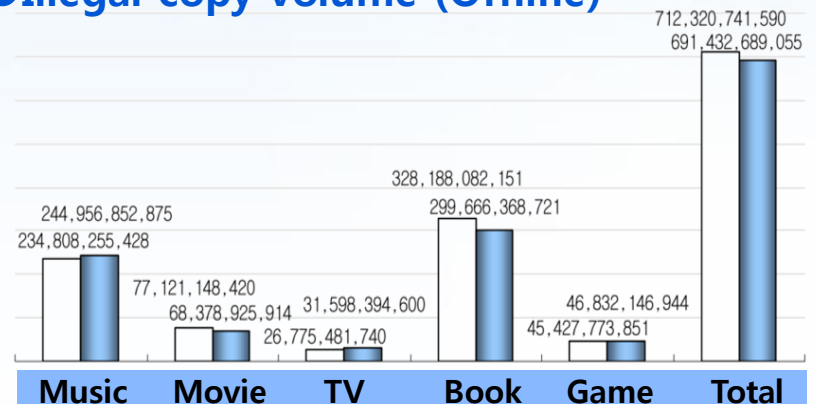


## ⇒ Illegal copy volume (Online)



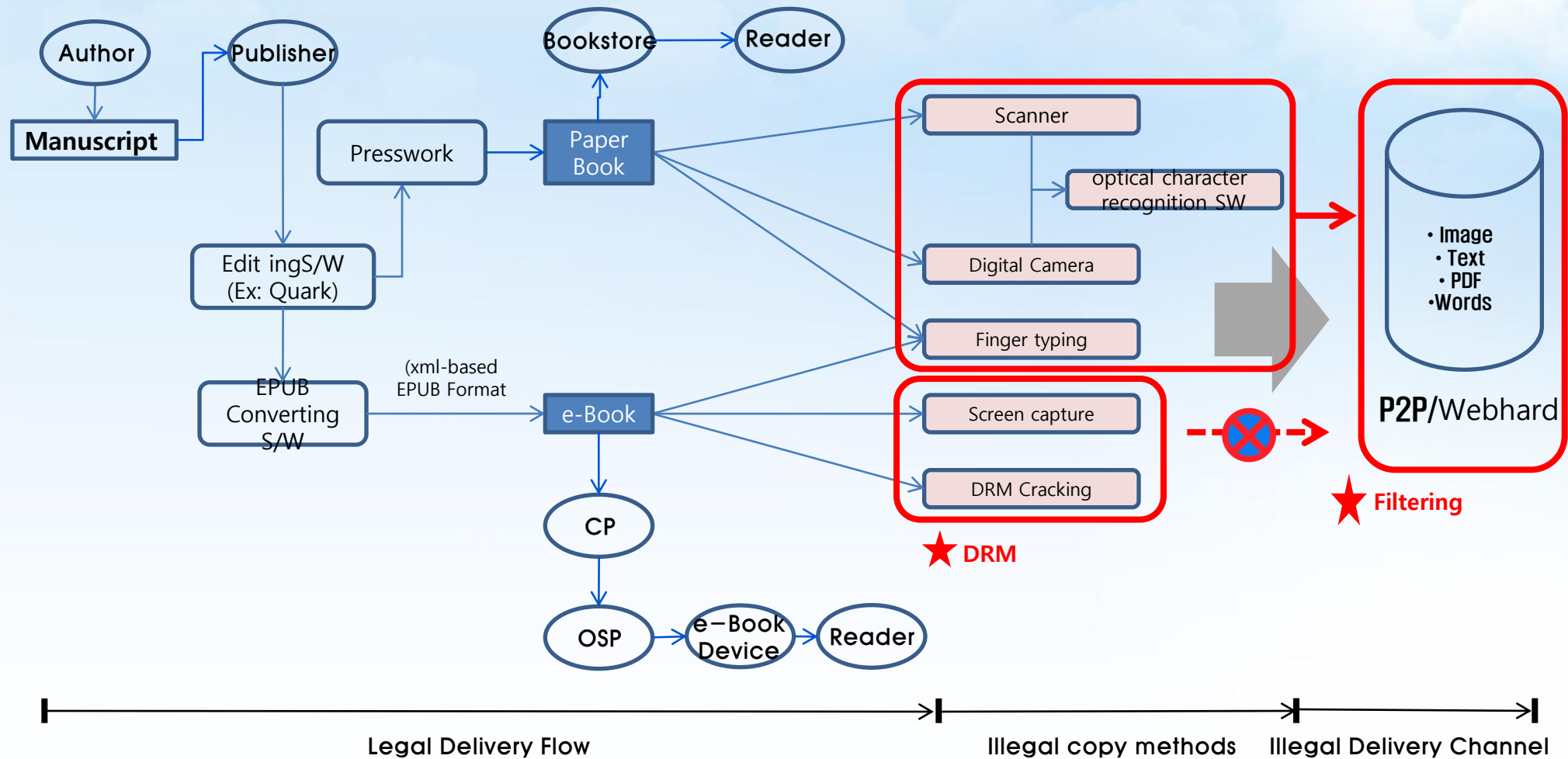
## ⇒ Illegal copy volume (Offline)

Unit : KRW



※ Source : Annual report on copyright protection 2012, By Copyrights protection center, Korea

# Illegal Path of Books and Protection Methods





## 2 DRM Interoperability Issues

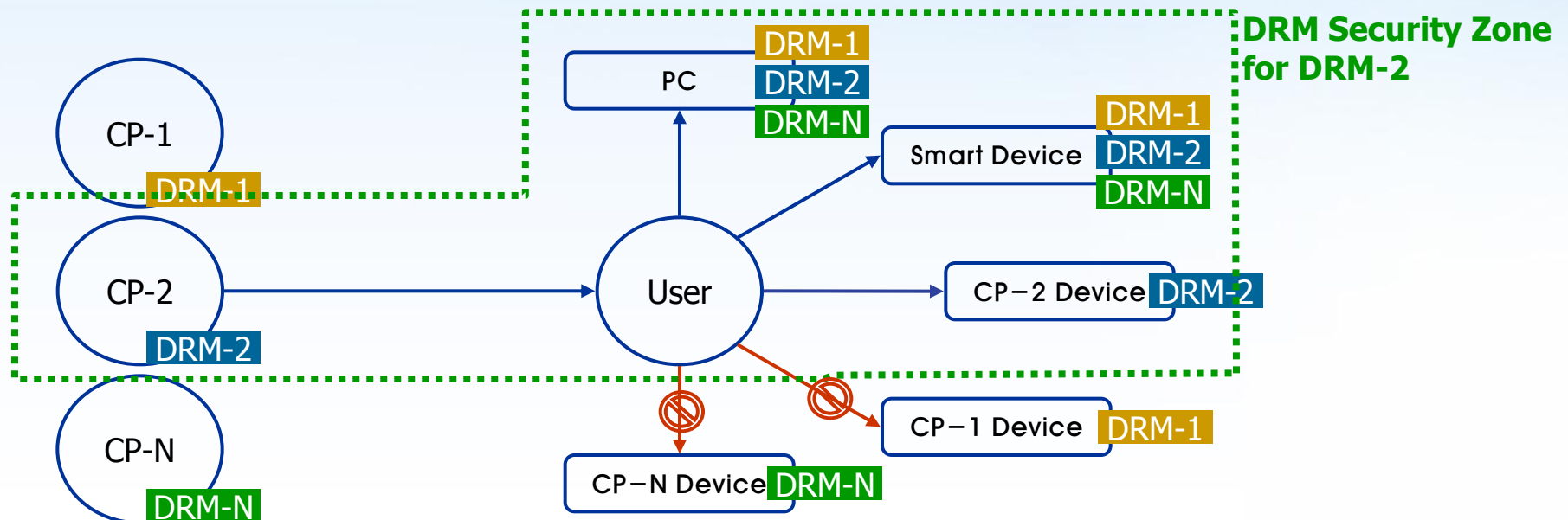


❖ User : Fairuse

- Restriction on private copy due to the lack of DRM interoperability
- Constraint on choose option of service and device

- ❖ OSP : Independence & Flexibility

- “DRM Security Zone” issues
- Pros : “Customer Lock-in” effect
- Cons : Dependent on a particular DRM technology



# Reference Model for solving DRM Interoperability

Model	Approaching Methods and Representative Examples
Single DRM Technology	<ul style="list-style-type: none"> <li>• All vendors adopt only one DRM technology</li> <li>• Representative examples                             <ul style="list-style-type: none"> <li>–DCI(Digital Cinema Initiatives) : KDM standard for copy protection of Digital Cinema content</li> </ul> </li> </ul>
Operating of Multiple DRM Servers by OSP	<ul style="list-style-type: none"> <li>• The way providing the proper DRM content and License depending on the type of the user's terminal by operating multiple DRM servers</li> <li>• Representative examples                             <ul style="list-style-type: none"> <li>–Music industry in the past</li> </ul> </li> </ul>
Embedding Multiple DRM Clients into a Device by Device Manufacturer	<ul style="list-style-type: none"> <li>• The way building the plurality of DRM clients into a device when manufacturing of devices</li> <li>• Representative examples                             <ul style="list-style-type: none"> <li>–Music industry in the past</li> </ul> </li> </ul>
DRM Converting	<ul style="list-style-type: none"> <li>• To enable the use of protected content between two DRM technologies, DRM content is changed to target DRM from source DRM</li> <li>• Representative examples                             <ul style="list-style-type: none"> <li>–Microsoft PlayReady(suport DTCP, CPRM, HerixDRM, etc)</li> <li>–Marlin OMAv2 Gateway, OMArin</li> <li>–Sony Rootkit(Converting from Protected music CD to Microsoft WMDRM)</li> <li>–TiVo TO Go service</li> </ul> </li> </ul>
DRM Interoperable Interface	<ul style="list-style-type: none"> <li>• Providing standard export and import interface between different DRM technologies to ensure compatibility</li> <li>• Representative examples                             <ul style="list-style-type: none"> <li>–EXIM, CADII</li> </ul> </li> </ul>



**3**

## **e-Book DRM Standardization**

## ❖ IDPF(International Digital Publishing Forum)

- De-facto e-Book standard organization formed by more than 120 companies in digital publishing industry

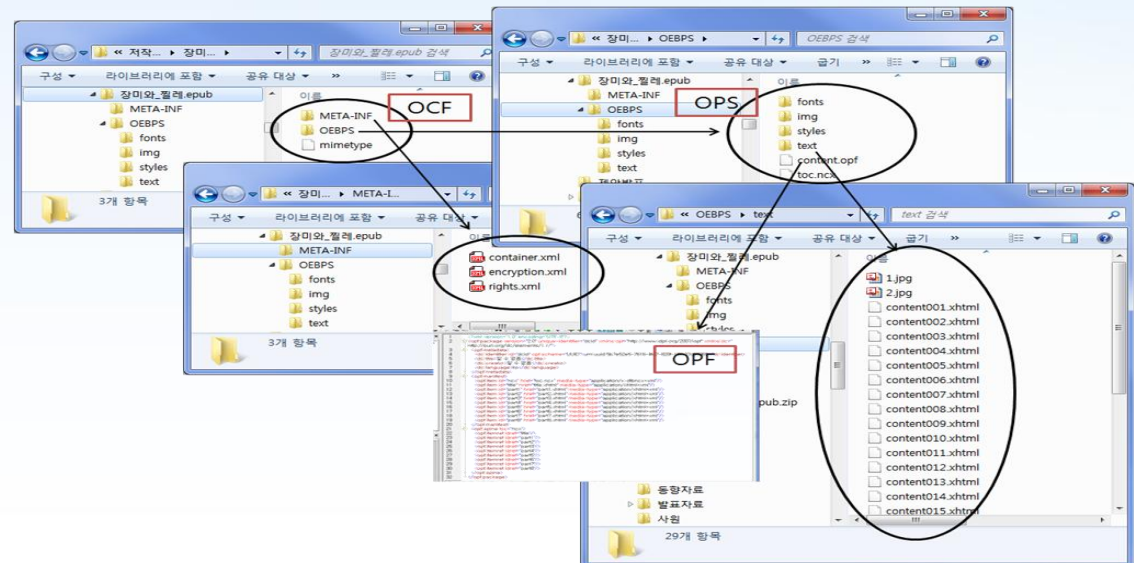
## ❖ Standardization Activities in IDPF

Year	Activities
1998	Open e-Book Forum(OeBF) formed by MS, Adobe, etc
1999	OEBF proposes a XML-based Open e-Book(OEBPS) format
2002	OEBPS 1.2 Update : Peanut Press, MobiPocket, SoftBook, NuvoMedia, Gemstar, ETI, MS
2005	OEBF was changed to IDPF
2006	OEBPS Working Group resumes a standard work for OEBPS 1.2 revision
2007	Enactment of EPUB standard <ul style="list-style-type: none"> <li>– Open Publication Structure (OPS) : XHTML or DTBook</li> <li>– Open Packaging Format (OPF)</li> <li>– OEBPS Container Format (OCF) : Zip container</li> </ul>
2010	Update of EPUB standard <ul style="list-style-type: none"> <li>– Open Publication Structure (OPS) v.2.0.1</li> <li>– Open Packaging Format (OPF) v.2.0.1</li> <li>– OEBPS Container Format (OCF) v.2.0.1</li> </ul>
2011	Update to EPUB 3.0
2012, May	EPUP Lightweight Content Protection : RfC(Request for Comments) for Use Cases & Requirements
2012, July	RFP for EPUB LCP solutions

- ❖ EPUB is an de-facto standard in e-Book industry with content protection measures published by IDPF

Standard item	Content
OCF (Open Container Format)	<ul style="list-style-type: none"> <li>• ZIP format</li> <li>• Mimetype : EPUB Identifier</li> <li>• META-INF : Information on keys, rights and locations of OPS and OPF( container.xml, encryption.xml, rights.xml and signatures.xml file )</li> </ul>
OPS (Open Publication Structure)	• EPUB contents + OPF file
OPF (Open Package Format)	• Information on TOC, metadata and location of contents

e-BookContent.EPUB  
  
e-BookContent.EPUB.zip





- ❖ EPUB provides specification on just encryption and digital signature for content protection, but did not define specification for rights

OCF Item	Content
META-INF/encryption.xml	<ul style="list-style-type: none"> <li>• W3C XML encryption standard referenced</li> <li>• Description for encryption target, algorithm and key information</li> </ul>
META-INF/signatures.xml	<ul style="list-style-type: none"> <li>• W3C XML signature standard referenced</li> <li>• Description for signed target, algorithm and validation certificates</li> </ul>
META-INF/rights.xml	<ul style="list-style-type: none"> <li>• No specification defined</li> <li>• Any kind of rights expression language can be used</li> </ul>

## Encryption.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<encryption xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmenc#">
    <xenc:EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmenc#aes128-cbc"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:RetrievalMethod URI="#EK" Type="http://www.w3.org/2001/04/xmenc#EncryptedKey"/>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherReference URI="OEBPS/content.html"/>
    </xenc:CipherData>
  </xenc:EncryptedData>
  <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmenc#" Id="EK">
    <xenc:EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmenc#rsa-oaep-mgf1p"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyName>dnQualifier=dnyE2kTAtuwcUmr2peYsQKu54k=,CN=CuName,O=SP Name,C=kr</ds:KeyName>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>YkOPSj+mvrQvTgQTQ8RPieicCULqQM0E8Etbd5fDhXYD6QmTC
      Cvte+V3Luzs28lCG1py9ES5JEZ412QY7YdNt4lKtnzVbmG2eLETO7KR2vH9tM2w1PaC
      akA32YL/SaDWtN6dcerF9RuVa0kNkk/M0dyRz+6K/09M=</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedKey>
</encryption>
```

## W3C XML Encryption

## Signatures.xml

```
<?xml version="1.0" encoding="utf-8"?>
<signatures xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="sig">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010718"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#Manifest1">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010718"/>
        </ds:Transforms>
      </ds:Reference>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
      <ds:DigestValue>3V0uQz+ikh8LpdZCxfmKJUofMQ0dDRoToiJ6sB7ZKY=</ds:DigestValue>
    </ds:SignedInfo>
    <ds:SignatureValue>XR4iR9Zlr+MOZT4eyvircWzJ2arphipnvi3zMDbloPpVnqxI/1HxJfF1Y
    W+mumazeHStOfLiaTW/lkGY8bJ7cb8y65XcsZkmZJUqLoRhD6kHYi4Yt6gPR/Jy
    IdxFVNgDAGiacRDp38g0iR7bttm/e+6aKqyOOMP84//+on9NyAskdMhTVObHgnC1
    qwVeD93HxSw0ptLMMz59j/7apr2NlU5z7AadKFgrOz+td4QUP4E+WB3YM6zJ11R7
    udVfd/mxtSwcwg4g69iBnKAn1zRR68IH07GrxuFizLa7rPih/u3Reftoe3TcR
    HYk+RMA72BJG8sUnmVUCWQ=</ds:SignatureValue>
  </ds:Signature>
</signatures>
```

## W3C XML Signature

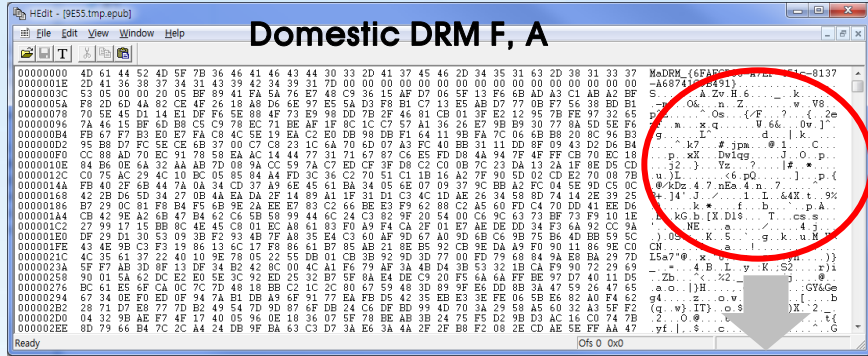
## rights.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<o-ex:rights xmlns="http://odrl.net/1.1/ODRL-EX"
  xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:dd="http://odrl.net/1.1/ODRL-DD"
  xmlns:eb="http://e-book.copyrights.or.kr/1.0/rel/EBR-DD"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://e-book.copyrights.or.kr/1.0/rel/EBR-DD EBR-DD-10.xsd">
  <o-ex:context>
    <o-dd:uid>RightsObjectID</o-dd:uid>
  </o-ex:context>
  <o-ex:agreement>
    <o-ex:asset>
      <o-ex:context ebr:type="partial">
        <!-- item id at the manifest content.opf file -->
        <o-dd:uid>partial content ID</o-dd:uid>
      </o-ex:context>
    </o-ex:asset>
    <o-ex:permission>
      <o-dd:display/>
      <o-dd:print/>
    </o-ex:permission>
    <o-ex:constraint>
      <o-dd:group>
        <o-ex:context>
          <o-dd:uid>멤버쉽 A</o-dd:uid>
        </o-ex:context>
      </o-dd:group>
    </o-ex:constraint>
  </o-ex:agreement>
</o-ex:rights>
```

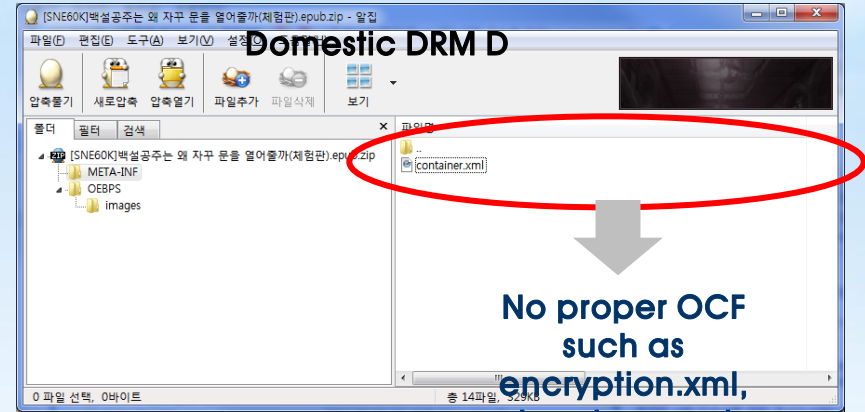


# Is EPUB standard enough for interoperability?

- ❖ Although based on EPUB standard, each DRM uses different approaches for encryption
- ❖ Cryptographic algorithms are various
- ❖ No standard for rights.xml



Proprietary encryption of EPUB



No proper OCF such as encryption.xml, signatures.xml, rights.xml

Each solution can't understand other proprietary measures



Key information in rights.xml

Each DRM uses different REL



## **Project for e-Book DRM Interoperability**

## ❖ Each of content providers uses different DRM technologies

- KEPUB : Hancom DRM
- KPC : Markany DRM
- Kyobo : Fasoo.com DRM



- Why e-Book contents is not compatible although there is EPUB standard?

## ❖ Inconvenience of Digital Library & Viewer

- KEPUB partners use 'crema' library and viewer developed by KEPUB
- Each of KPC partners uses their own proprietary e-Book library and viewer
- Kyobo uses Kyobo's proprietary e-Book library and viewer



- Where are my purchased e-Book contents?
- What are lists of e-Book contents?
- Do I use something else in spite of my favorite viewer?

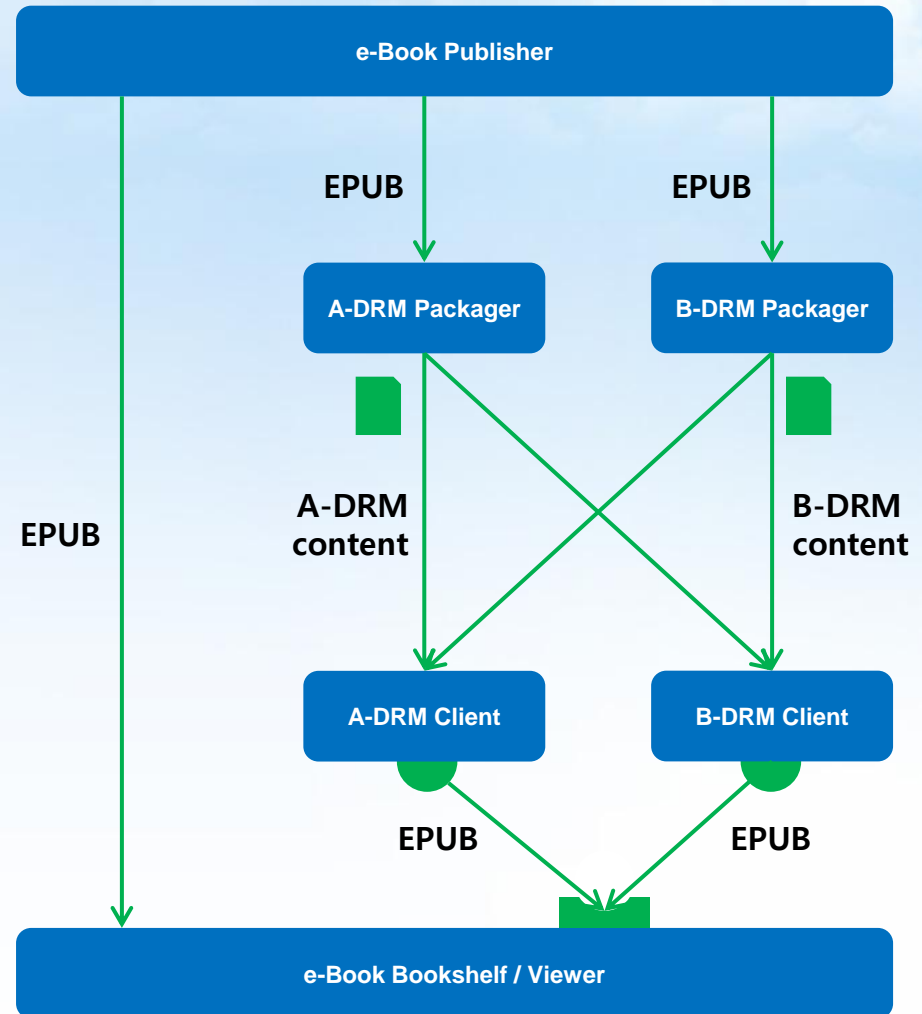
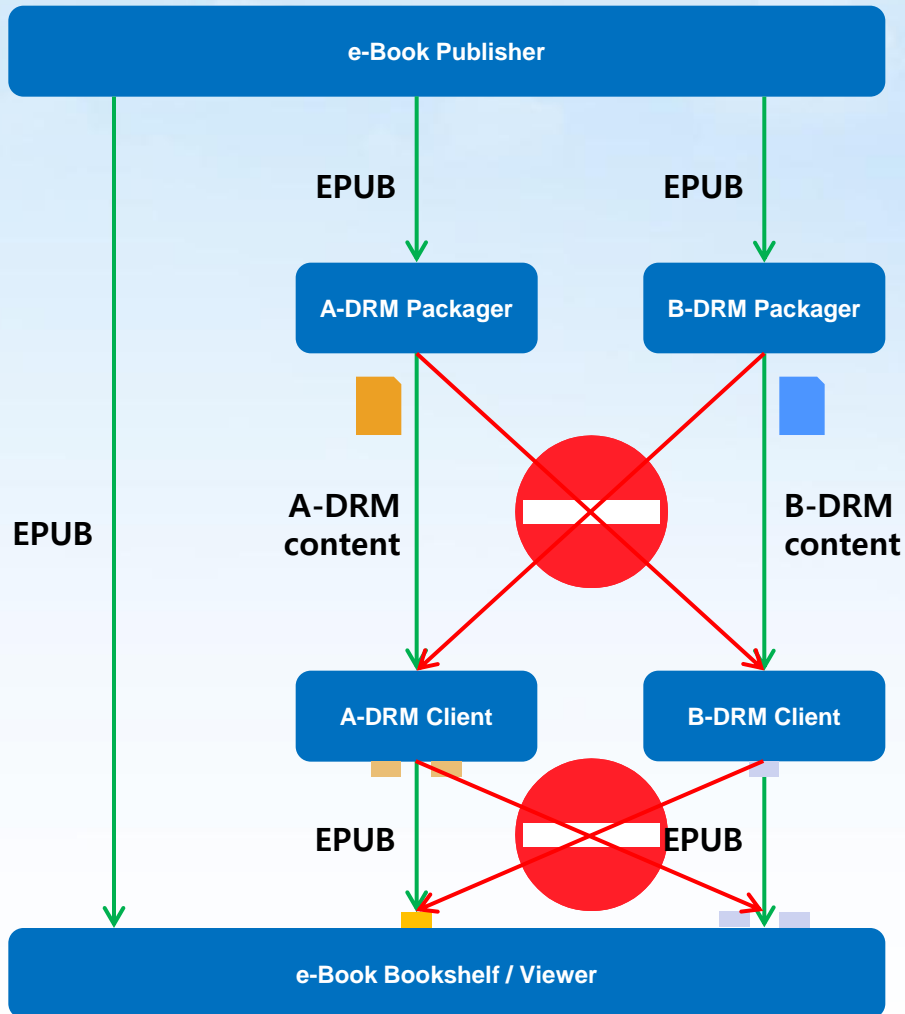
## ❖ Supply of e-Book Content

- e-Book service providers attempt a cross-selling service in order to resolve the lack of e-Book contents
- Need to install multiple DRM technologies for cross-selling



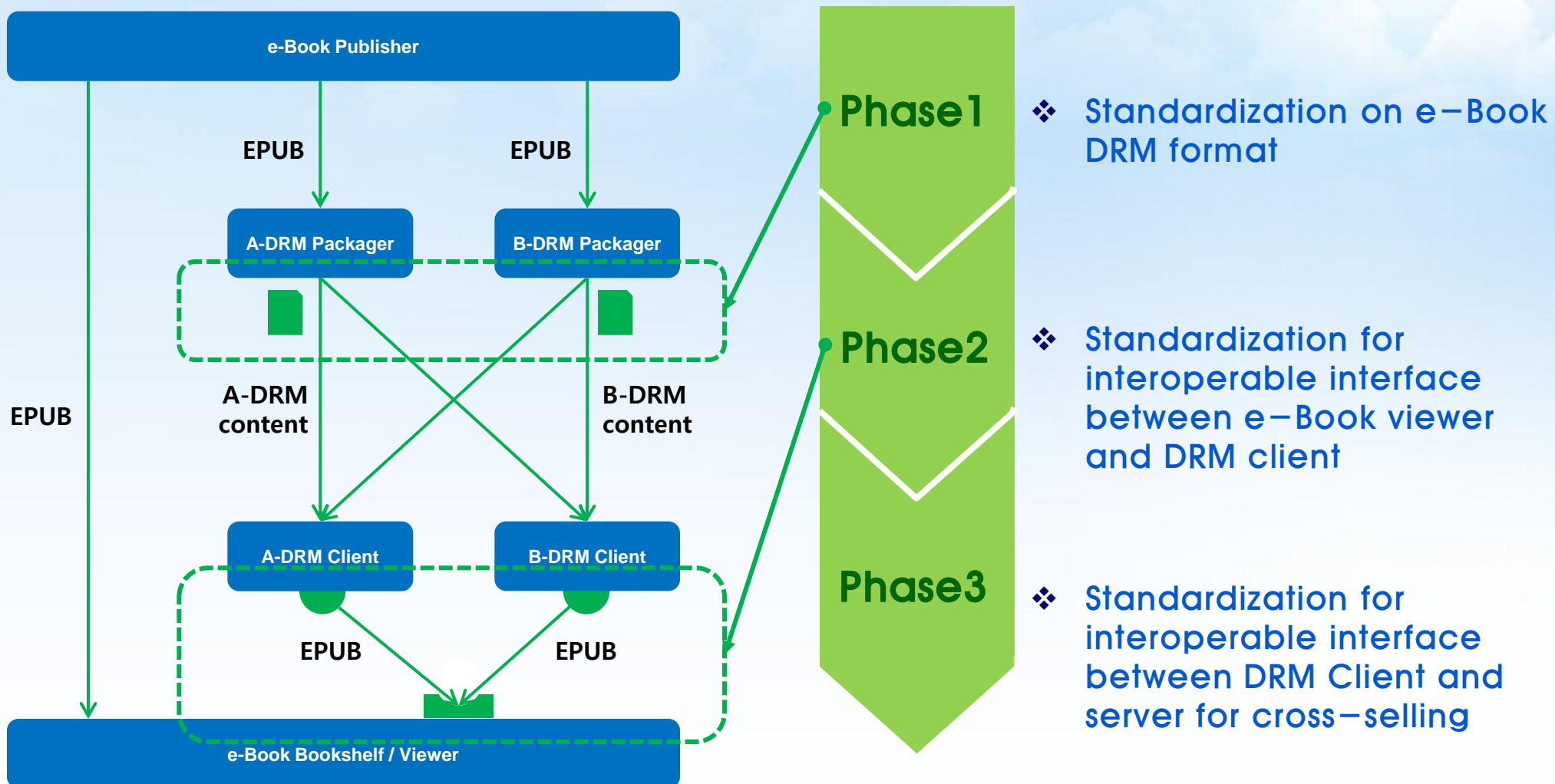
- Should I integrate your DRM technology to my DRM technology for cross-selling?
- Should I have the device porting burdens(time, cost, resources, etc) for supporting your DRM technology?
- My viewer is ragged because of supporting for multiple DRM technologies...

# Problems and Improvement Factors





# Strategy for e-Book DRM Interoperability



- ❖ Define simple profiles of existing EPUB
- ❖ Define how to resolve to process different right information

EPUB Item	Interoperable Issues	Current e–Book DRM	Recommended e–Book DRM
Content encryption	Algorithm	EPUB (W3 XML Encryption) or DRM proprietary	Profiled EPUB (W3 XML Encryption)
	Format		
	Metadata		
Key	Encryption algorithm		
	Delivery format		
	Metadata		
	Private key/secure key management	DRM proprietary	DRM proprietary
Signature	Algorithm, Keys	EPUB (W3 XML Signature)	Profiled EPUB (W3 XML Signature)
Rights	Expression language	DRM proprietary	REL Standard or DRM proprietary
	Enforcement		
License request protocol		DRM proprietary	Standard protocol

- ❖ 2-year project, "Development of the Interoperable e-Book DRM Standard and Reference S/W based of IDPF EPUB"
- ❖ 5 companies are joined and supported by KCC(Korea Copyright Commission)

**Goal: Multi-DRMs-allowable eBook solution market**

1<sup>st</sup> year (2011)

Development of Profiles of EPUB protection specification

2<sup>nd</sup> year (2012)

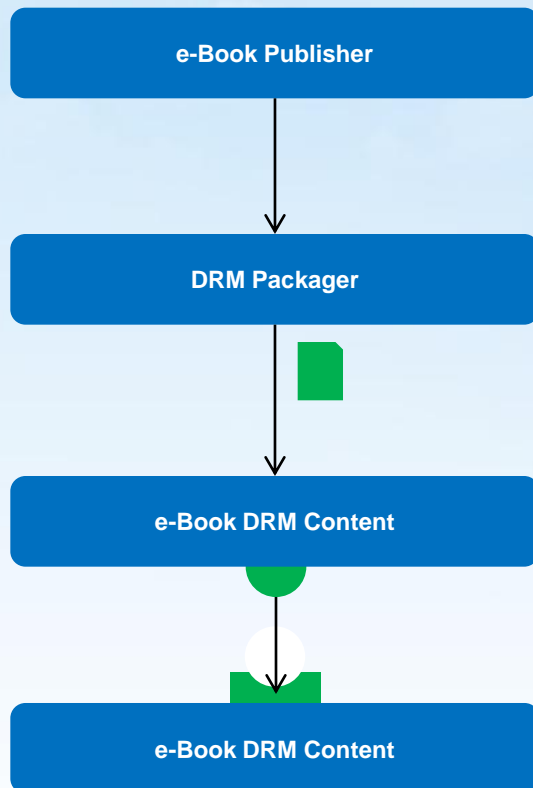
Development of the interoperable eBook protection environment

Standards	Reference S/W	Standards	Compliance test
Encryption/Signature profile standard	eBook Packager/Depackager	Interoperability of authentication process	Test scenarios
Rights terminology	Development API	Interoperability of key information delivery process	Test materials (valid/Invalid)
Certificate profile standard	Open reference S/W	Interoperability of rights information delivery process	Automated test module



# *Standard Requirements for e-Book DRM Interoperability*

- ❖ **Compliance with international standards**
  - Standard should be comply with the IDPF EPUB which is recognized as de-facto standard in e-Book industry
- ❖ **Royalty Free**
  - Standard should not use technology which is possible of patent infringement or royalty burden
- ❖ **Reliability**
  - Standard should ensure the reliability of the technology using internationally proven standard technology
- ❖ **Seamless Interworking Method to Legacy DRMs**
  - Standard should not impose a large change burden of legacy DRM technology
- ❖ **Security Robustness**
  - Standard should ensure an adequate level of security and not be tampered
- ❖ **Effective Competition**
  - Standard should not undermine existing DRM market order, and ensure effective competition between legacy commercial DRMs
- ❖ **Business-Independence**
  - Standard should ensure differentiated business model of e-Book service providers, and be able to support the DRM policy.
- ❖ **Economic Feasibility**
  - Standard should minimize the burden of e-Book service providers



- ❖ **Development of e–Book DRM Format based on EPUB**
  - Profile specification of encryption.xml, signature.xml for simple implementation and DRM interoperability
  - Dictionary of rights terms for rights.xml
  - Profile specification of Device Certificate based on X.509
- ❖ **Development of Reference Software**
  - There is a possibility that incompatible or arbitrary interpretation by the developer's ability is taken to errors although EPUB–based e–Book DRM standard format is to be.
  - In order to avoid such errors, reference software is needed to develop and opened to developer of e–Book DRM technology
- ❖ **Development of Interoperable Interface between e–Book Viewer and DRM Client**
  - Need a e–Book DRM API standard in order that e–Book Viewer and DRM technology can be independent of each other



- ❖ Still IDPF EPUB rule was used, which is based on W3C Encryption.
- ❖ Profiles was defined on enc:EncryptedData and enc:EncryptedKey of the W3C Encryption.
- ❖ Content encryption algorithm is strongly recommended to use AES-128-CBC (recommended by NIST in 2010)
- ❖ Key encryption algorithm is strongly recommended to use RSA-2048 (recommended by NIST in 2010)
- ❖ “Encryption specification for e-Book DRM” is approved to ODPF and TTA standard

TTA Standard

정보통신단표준  
TTA, xcc-xx, xxxxx/R1

제정일: 20xx년 xx월 xx일  
개정일: 20xx년 xx월 xx일

**전자출판물 DRM 암호화표준(안)**

(Encryption standard for electronic publishing DRM)

정보통신(한국)단표준

4. W3C XML Encryption 프로파일

이 절에서는 W3C XML Encryption에서 정의하고 있는 EncryptedData와 EncryptedKey 엘리먼트에 대한 프로파일을 정의한다.

4.1. Namespace

본 문서에서 사용하는 프로파일의 namespace는 아래와 같다.

Namespace	URI	내용
enc	http://www.w3.org/2001/04/xmenc#	W3C Encryption
ds	http://www.w3.org/2000/09/xmldsig#	W3C Digital Signature

4.2. EncryptedData

- EncryptedData는 속성으로 id와 MimeType만을 가져야 한다.
- EncryptedData의 자식엘리먼트는 기존 W3C Encryption 표준과 동일하다.

엘리먼트/속성	소속명	필수/선택	비고
enc:EncryptedData	0..n	-	
@enc:id	0..1	O	동일 xml 문서 내에서 연립될 때 사용되는 ID
@enc:MimeType	0..1	O	암호화된 데이터에 대한 미디어 타입 (RFC 2045 MIME에 의해 정의됨)
enc:EncryptionMethod	0..1	O	암호화 알고리즘 기술
ds:KeyInfo	0..1	O	암호화에 사용된 키 정보 기술
enc:CipherData	1	M	암호화된 데이터 기술
enc:EncryptionProperties	0..1	O	암호화된 데이터의 추가정보 기술

정보통신(한국)단표준

4. W3C XML Encryption 프로파일

이 절에서는 W3C XML Encryption에서 정의하고 있는 EncryptedData와 EncryptedKey 엘리먼트에 대한 프로파일을 정의한다.

4.1. Namespace

본 문서에서 사용하는 프로파일의 namespace는 아래와 같다.

Namespace	URI	내용
enc	http://www.w3.org/2001/04/xmenc#	W3C Encryption
ds	http://www.w3.org/2000/09/xmldsig#	W3C Digital Signature

4.2. EncryptedData

- EncryptedData는 속성으로 id와 MimeType만을 가져야 한다.
- EncryptedData의 자식엘리먼트는 기존 W3C Encryption 표준과 동일하다.

엘리먼트/속성	소속명	필수/선택	비고
enc:EncryptedData	0..n	O	
@enc:id	0..1	O	동일 xml 문서 내에서 연립될 때 사용되는 ID
@enc:MimeType	0..1	O	암호화된 데이터에 대한 미디어 타입 (RFC 2045 MIME에 의해 정의됨)
enc:EncryptionMethod	0..1	O	암호화 알고리즘 기술
ds:KeyInfo	0..1	O	암호화에 사용된 키 정보 기술
enc:CipherData	1	M	암호화된 데이터 기술
enc:EncryptionProperties	0..1	O	암호화된 데이터의 추가정보 기술

부록 A

저자권 관련 DRM encryption.xml 파일 샘플

1. 사용자 개인기 종속적인 encryption.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<encryption xmlns="urn:ietf:params:xml:enc:1.0:xmenc" xmlns:container="http://www.w3.org/2001/04/xmenc#" id="EK">
  <enc:EncryptedData xmlns:enc="http://www.w3.org/2001/04/xmenc#" id="EK">
    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#rsa-mle10"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:RetrievalMethod URI="#EK Type" http://www.w3.org/2001/04/xmenc#RetrievalKey"/>
    </ds:KeyInfo>
    <enc:CipherData>
      <enc:CipherReference URI="#EK Type" http://www.w3.org/2001/04/xmenc#RetrievalKey"/>
    </enc:CipherData>
  </enc:EncryptedData>
  <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmenc#" id="EK">
    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#rsa-mle10"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyName href="#EK Type" http://www.w3.org/2001/04/xmenc#RetrievalKey"/>
    </ds:KeyInfo>
    <enc:CipherData>
      <enc:CipherReference URI="#EK Type" http://www.w3.org/2001/04/xmenc#RetrievalKey"/>
    </enc:CipherData>
  </enc:EncryptedKey>
</encryption>
```

TTA 한국정보통신기술협회  
Telecommunications Technology Association

23

DRM inside

- ❖ Still IDPF EPUB rule was used, which is based on W3C Signature
- ❖ Profiles was defined on ds:Signature of the W3C Signature
- ❖ Signature algorithm is fixed to use RSA2048withSHA256 (recommended by NIST in 2010)
- ❖ Hash algorithm for message digest is fixed to use SHA256
- ❖ Canonicalization and transform algorithm is fixed to use c14n-20010315 (without comment)
- ❖ “Signature specification for e-Book DRM” is approved to ODPF and TTA standard

TTA Standard

정보통신산업표준  
TTA-icc-xx-xxxx/R1

제정일: 20xx년 xx월 xx일  
개정일: 20xx년 xx월 xx일

**전자출판물 DRM  
전자서명 표준(안)**

(Digital signature standard for  
electronic publishing DRM)

**TTA** 한국정보통신기술협회  
Telecommunications Technology Association

### 4. W3C XML Signature 프로파일

이 문서는 W3C XML Signature에서 정의하고 있는 ds:Signature 엘리먼트에 대한 프로파일을 정의한다.

#### 4.1. Namespace

본 문서에서 사용하는 프로파일의 namespace는 아래와 같다.

Namespace	URI	내용
ds	http://www.w3.org/2000/09/xmldsig#	W3C Digital Signature

#### 4.2. ds:Signature

- Signature의 자식 엘리먼트는 기존 W3C Signature 표준과 동일하다.

엘리먼트/속성	종형성	필수/선택	비고
ds:Signature	1	M	
@ds:Id	0..1	O	동일 xml 문서 내에서 연립될 때 사용되는 ID
ds:SignatureInfo	1	M	전자서명 생성에 대한 정보 기술
ds:SignatureValue	1	M	전자서명 값 기술
ds:KeyInfo	0..1	O	전자서명 확인에 사용될 정보
ds:Object	0..1	O	전자서명 대상에 대한 정보

#### 4.2.1. ds:SignatureInfo


- ds:SignatureInfo의 자식 엘리먼트는 기존 W3C Signature 표준과 동일하다.
- ds:CanonicalizationMethod 속성값은 Algorithm 속성값을 가져야 한다. 그 속성값은 "http://www.w3.org/TR/2001/REC-xml-c14n-20010315" 이어야 한다.
- ds:SignatureMethod 속성값은 Algorithm 속성값을 가져야 한다. 그 속성값은 "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" 이어야 한다.

엘리먼트/속성	종형성	필수/선택	비고
ds:SignatureInfo	1	M	
@ds:Id	0..1	O	동일 xml 문서 내에서 연립될 때 사용되는 ID
ds:CanonicalizationMethod	1	M	경우와 방법
ds:SignatureMethod	1	M	경우와 알고리즘
ds:SignatureMethod	1	M	전자서명 방법
ds:SignatureMethod	1	M	전자서명 알고리즘
ds:Reference	1..n	M	서명 대상에 대한 정보

```
<?xml version="1.0" encoding="utf-8"?>
<signatures xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
  <Signature Id="sig" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignatureInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#Manifest1">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>uZ6s8EPHqQnFw23ceMTMkKcBMCzrgTPg74KQ=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#Manifest2">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>w6U/2FHzooH09uQUkLD24Az3eikxBQDZTlacOSIs=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#Manifest3">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>NvRyKHZomxYcW7TrvLUkLD24Az3eikxBQDZTlacOSIs=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#Manifest4">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>K9MzFuZxZ2725wAJ0S24Az3eikxBQDZTlacOSIs=</ds:DigestValue>
      </ds:Reference>
    </ds:SignatureInfo>
    <ds:SignatureValue>eMmnyGkGRtCc1KvDHz7LlV3LxUzF2wWkUdMEwsZegFHzagCXQeNzFCET
Rk4DfmxX9gd555sLkToQkhyZPUFGCzQIM450x8c2wdcgusZ2eYn7Gf8n
nwPR4yV7REwnUUDgIENLPouLw5K9hGmU1U0CUsU3U7wWTeboIEE7Lo
ISUzCLN9GaiShuTFamaXlcbseDLsJ38c+vv3vGdH5AJ1xp/E2TE+1o6S19oA
nd3eLi3THRETDPIJ11nvOenl8J3ZshVC2MM7205UFS9eSpts1bt89FJ78hZoz1
huVv1x8C1C4GUES1WfQ==</ds:SignatureValue>
  </Signature>
</signatures>
```

- ❖ X.509 certificate is strongly recommend for the standard digital signature and key encryption method
- ❖ Profile was defined for ITU–T X.509 standard on certificate field values for simplicity of the implementation.
- ❖ Signature algorithm is fixed to use RSA2048withSHA256.
- ❖ Key strength is fixed according to NIST 800–131 recommendation.
- ❖ “Certificate specification for e–Book DRM” is approved to ODPF and TTA standard

TTA Standard	정보통신단체표준	제정일: 20xx년 xx월 xx일
	TTAx-xx-xx-xxxx/R1	개정일: 20xx년 xx월 xx일
	전자출판물 DRM 인증서표준(안)	
	(Certificate standard for electronic publishing DRM)	


**한국정보통신기술협회**  
 Telecommunications Technology Association

정보통신영문단재표준

5. 프로파일 요약

표 1) 전자출판용 DRM에 사용되는 인증서 프로파일

항목	제안내용
인코딩 방식	ASN.1 DER
파일 포맷	ASCII파일; PEM
인증서 버전	v3
전자서명 알고리즘	sha256withRSAEncryption
서리화 번호	64비트 보다 작은 양의 정수
SubjectPublicKeyInfo	Modulus : 2048 비트, exponent : 65537
Validity Field	UTC Time(년도 월 일 시간)
KeyUsage	<ul style="list-style-type: none"> <li>Key Usage 필드가 인증서의 서명된 부분안의 x509v3 Extension 섹션에 존재하여야 함</li> <li>서명용 인증서에 대해서는 "Certificate Sign(KeySign)" 플래그가 true이어야 함</li> <li>선택 인증서에 대해서는 "Certificate Sign(KeySignCert)"와 "CPLSign(CPLSign)" 플래그가 나타날 수도 있음(Optional)</li> </ul>
Basic Constraint	<ul style="list-style-type: none"> <li>Basic Constraint 필드가 인증서의 서명된 부분안의 x509v3 Extensions 섹션에 존재하여야 함</li> <li>서명용 인증서의 경우 인증서 기판 속성이 true 이어야 함</li> <li>선택 인증서에 대해서는 "Basic Constraint"와 "Key Encipherment" 표시가 true이어야 함</li> <li>Basic Constraint 필드가 인증서의 서명된 부분안의 x509v3 Extensions 섹션에 존재하여야 함</li> <li>서명용 인증서의 경우 인증서 기판 속성이 true 이어야 함</li> <li>선택 인증서에 대해서는 "Basic Constraint"와 "Key Encipherment" 표시가 true이어야 함</li> </ul>
공개키 Thumbprint	<ul style="list-style-type: none"> <li>Subject 필드에 정확히 1개의 DnQualifier가 존재하여야 함</li> <li>해당 DnQualifier의 값이 인증서 안에 있는 Subject 공개키의 Base64로 인코딩된 Thumbprint이어야 함</li> <li>Issuer 필드 안에 정확히 한 개의 DnQualifier가 존재하여야 함</li> <li>해당 DnQualifier의 값이 발급자 공개키의 Base64로 인코딩된 Thumbprint 이어야 함</li> </ul>
Unrecognized Extensions	<ul style="list-style-type: none"> <li>서명용 인증서에 대해서 : Basic Constraints 가 critical로 마크된 것 이어야 함</li> <li>KeyUsage는 critical로 마크된 것 이어야 함 (Optional)</li> <li>선택 인증서에 대해서 : "Basic Constraints" 필드는 critical로 마크될 수 있음 (Optional)</li> </ul>

정보통신(연구)사업 결과보고서

## 4. 전자출판물 DRM 인증서 프로파일

전자출판물 DRM 인증서 표준은 ITU-T X.509 표준을 준수하며 다음과 같은 계약조건을 가진 프로파일로 정의한다.

### 4.1. 표현 방법

#### 4.1.1. 데이터 형식

전자출판물 DRM 인증서의 데이터 형식은 ITU-T X.509의 Annex-A, "Public-Key and Attribute Certificate Frameworks" 표준을 준수해야 한다.

#### 4.1.2. 데이터 표기 방식

전자출판물 DRM 인증서에 대한 데이터표기 방식은 ITU-T X.509에서 지정한바와 동일하게 ASN.1 표기 방식을 사용해야 한다.

### 4.1.3. 인코딩 방식

ASN.1 형식으로 표기된 전자출판물 DRM 인증서 데이터는 DER 방식으로 인코딩되어야 한다.

### 4.1.4. 파일저장 포맷

전자출판물 DRM 인증서에 대한 파일 저장 포맷은 이진표기 방식을 사용하고자 할 경우 DER 방식, ASCII표기 방식을 사용하고자 할 경우 PEM 방식을 사용해야 한다.

### 4.1.5. 파일 확장명

전자출판물 DRM 인증서에 대한 파일 확장명은 DER 방식일 경우 .der 표기하고 PEM 방식일 경우 .pem으로 사용할 것을 권장한다.

## 4.2. 인증서 데이터 영역

```

        부록 II
        인증서 샘플

1. Root 인증서 샘플

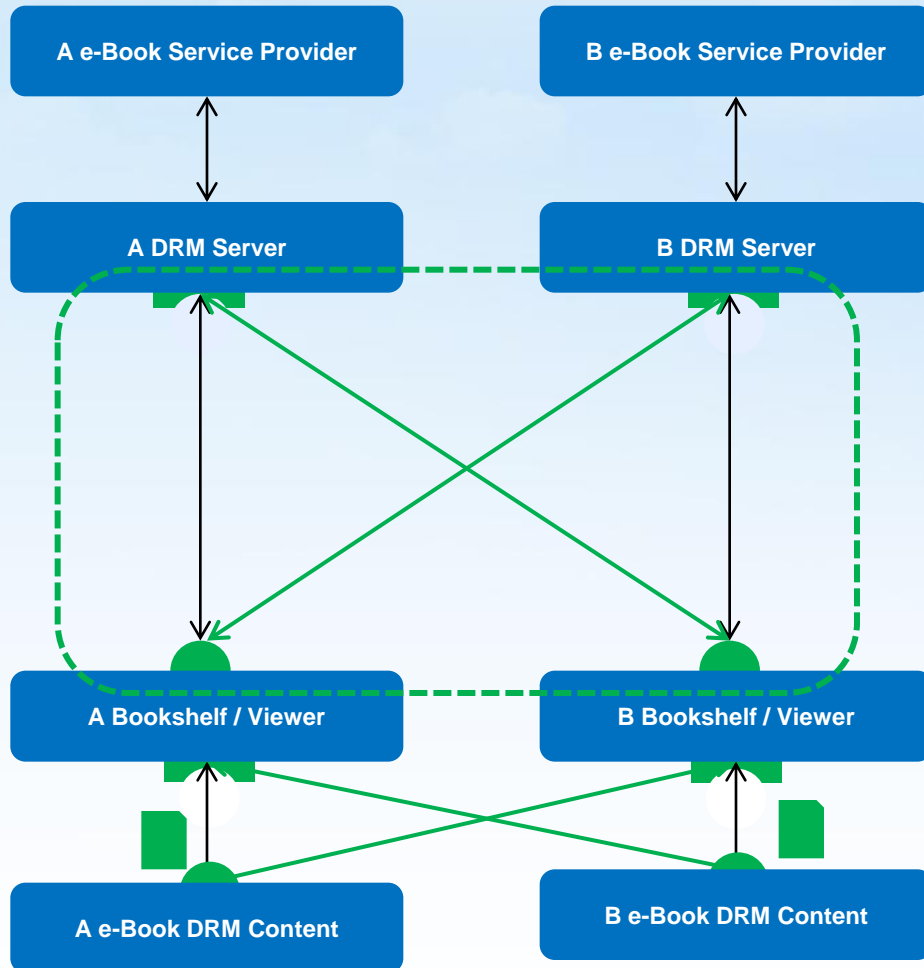
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 60000 (0xead0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=company, or=C, OU=CTP, Text=company, or,CN=
            O=C-KD8, ca=admin/znQualif=23/NrX/RyK/ZamX/cvI7Rv3Ht2DXjYe
    Validity:
        Not Before: 406 04:33:58 2006 GMT
        Not After: 406 04:33:58 2010 GMT
    Subject: O=company, or=C, OU=CTP, Text=company, or,CN=
        O=C-KD8, ca=admin/znQualif=23/NrX/RyK/ZamX/cvI7Rv3Ht2DXjYe
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:02:11:04:96:46:b0:43:63:a2:27:4b:e6:
                0b:07:1a1:04:51:a1:23:08:03:9c:e7:52:b4:
                02:90:50:b3:41:b1:c8:93:02:1f:13:cb:ad:a0:
                04:6f:49:6e:54:4d:ae:58:0b:0c:51:3f:42:20:43:
                0c:7b:0f:50:fa:1e:fa:02:a2:07:47:8f:0c:b2:0d:
                06:4f:08:3f:8f:c3:74:96:38:03:1f:1e:90:4a:
                61:cb:0b:a6:5c:79:a0:38:07:2:95:81:70:a5:a4:
                16:24:78:1a:3c:7b:93:93:1:2:04:0a:4a:
                35:07:4b:a5:4b:a4:ce:07:08:1b:c9:5c:50:86:cf:
                08:a8:a8:07:0b:0a:0b:03:3c:72:ba:0e:4a:47:83:
                79:09:00:37:52:ab:0c:07:77:fa:11:71:7f:3f:
                7c:90:0a:ca:1:95:cb:0a:45:18:3b:00:aa:00:0b:
                5c:7b:07:0c:11:b3:99:03:1a:0b:db:7b:58:0f:58:
                5c:1:8d:0b:0f:4b:a2:2f:75:27:82:a0:0a:0c:c8:
                ca:f9:91:7f:54:41:b3:96:c1:0c:18:dc:4c:6e:90:
                07:51:43:08:45:07:78:00:04:4c:ae:0b:19:58:14:
                28:31:0b:c4:29:5d:68:3c:1b:7d:46:df:ca:d9:
                55:c5
            Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Key Usage:
        Certificate Sign
    X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:3
    X509v3 Subject Key Identifier:
        A3:33:71:47:26:07:88:a9:1b:61:0c:82:ED:1B:F7:7E:14:F6:0D:76
    X509v3 Authority Key Identifier:
        keyid:A3:33:71:47:26:07:88:a9:1b:61:0c:82:ED:1B:F7:7E:14:F6:0D:76
        DnName: O=company, or=C, OU=CTP, Text=company, or,CN=O=C-KD8, ca=admin/znQualif=23/NrX/RyK/ZamX/cvI7Rv3Ht2DXjYe
        Serial: CA:00
    Signature Algorithm: sha256WithRSAEncryption
        78:38:10:7a:c0:47:98:f1:99:8a:cc:09:08:ae:6c:8c:8b:
        e7:09:08:5c:13:00:1e:7e:08:08:08:08:08:08:08:08:
        a2:1d:5b:7f:83:b6:61:3f:9f:83:5c:82:ae:02:5d:0d:ba:c0:
        ff:a0:08:93:33:ad:ac:bb:7c:82:9f:0a:03:06:aa:0b:ce:2e:
        8c:5cae:34:b:30:24:3b:31:7d:07:22:05:b1:5:fa:9d:92

```

- ❖ Hard to define specific rights expression language due to patent matter
- ❖ Defined only rights information dictionary for interoperability allowing any kind of syntax for rights information
- ❖ Defined 10 permissions, 12 constraints and 1 condition
- ❖ “Rights information dictionary for e–Book DRM” is approved to ODPF and TTA standard

Category	Name	Category	Name	Category	Name
Permission (10)	View	Constrain (12)	Absolute period	Condition (1)	Agreement
	Play		Relative period		
	Print		Count		
	Virtual print		User		
	Physical print		Group		
	Lend		Network		
	Transfer		Printer		
	Except		Geographical location		
	Copy		Software		
	Move		Hardware		
			Prerequisite		
			Alternative		





#### ❖ Interoperable Interface of Library

- e-Book content purchased from A company can look at B' s library(reverse case is also possible)

#### ❖ Interoperable Interface of e-Book Viewer

- e-Book content purchased from A company can look at B' s viewer(reverse case is also possible)

#### ❖ Interoperable Interface of DRM License Issuing

- in order that e-Book content purchased from A company can look at B' s viewer, the interoperable license request interface between B' s DRM client and A' s DRM license server is needed





*Thank you*

감사합니다

Hogab Kang  
[hgkang@drminside.com](mailto:hgkang@drminside.com)