

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36

Marlin - EPUB Extension Specification

Version 1.1
Draft

Source	Marlin Developer Community
Date	November 13, 2014

37 Notice

38 THIS DOCUMENT IS PROVIDED "AS IS" WITH NO REPRESENTATION OR
39 WARRANTY, EXPRESS OR IMPLIED, CONCERNING THE
40 COMPLETENESS, ACCURACY, OR APPLICABILITY OF ANY
41 INFORMATION CONTAINED IN THIS DOCUMENT. THE MARLIN
42 DEVELOPER COMMUNITY ("MDC") ON BEHALF OF ITSELF AND ITS
43 PARTICIPANTS (COLLECTIVELY, THE "PARTIES") DISCLAIM ALL
44 LIABILITY OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED,
45 ARISING OR RESULTING FROM THE RELIANCE OR USE BY ANY PARTY
46 OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. THE
47 PARTIES COLLECTIVELY AND INDIVIDUALLY MAKE NO
48 REPRESENTATIONS CONCERNING THE APPLICABILITY OF ANY
49 PATENT, COPYRIGHT (OTHER THAN THE COPYRIGHT TO THE
50 DOCUMENT DESCRIBED BELOW) OR OTHER PROPRIETARY RIGHT OF
51 THIS DOCUMENT OR ITS USE, AND THE RECEIPT OR ANY USE OF THIS
52 DOCUMENT OR ITS CONTENTS DOES NOT IN ANY WAY CREATE BY
53 IMPLICATION, ESTOPPEL OR OTHERWISE, ANY LICENSE OR RIGHT TO
54 OR UNDER ANY PATENT, COPYRIGHT, TRADEMARK OR TRADE
55 SECRET RIGHTS WHICH ARE OR MAY BE ASSOCIATED WITH THE
56 IDEAS, TECHNIQUES, CONCEPTS OR EXPRESSIONS CONTAINED
57 HEREIN.

58 Use of this document is subject to the agreement executed between you and
59 the Parties, if any.

60 Any copyright notices shall not be removed, varied, or denigrated in any
61 manner.

62 Copyright © 2014 by MDC, 415-112 North Mary Avenue #383 Sunnyvale, CA 94085,
63 USA. All rights reserved. Third-party brands and names are the property of their
64 respective owners.

65 Intellectual Property

66 A commercial implementation of this specification requires a license from the Marlin
67 Trust Management Organization.

68 Contact Information

69 Feedback on this specification should be addressed to: [editor@marlin-](mailto:editor@marlin-community.com)
70 [community.com](mailto:editor@marlin-community.com)

71 Contact information for the Marlin Trust Management Organization can be
72 found at: <http://www.marlin-trust.com/>

74	Contents	
75	MARLIN - EPUB EXTENSION SPECIFICATION	1
76	1 INTRODUCTION	4
77	1.1 Document Organization	4
78	1.2 Conformance Conventions	4
79	1.3 References	4
80	1.3.1 Normative references	4
81	1.3.2 Informative references	5
82	1.4 Terms and Definitions.....	5
83	2 OVERVIEW	6
84	3 CRYPTOGRAPHIC PROFILES.....	7
85	3.1 Encryption.....	7
86	3.1.1 Generic File Encryption.....	7
87	3.1.2 Marlin-defined Encryption Algorithm Identifiers	7
88	3.2 Signature.....	7
89	4 MARLIN EPUB EXTENSION.....	8
90	4.1 Rights Management File	8
91	4.1.1 Signalling of Protection Scheme	8
92	4.1.2 Inclusion of Marlin License.....	8
93	4.1.3 Inclusion of Rights URL	8
94	4.2 Encryption File	10
95	4.2.1 Associating Encrypted Resources to a Marlin License	10
96	4.3 Digital Signatures File.....	11
97		

1 Introduction

This document describes how to use Marlin [MBNS] with content packaged as EPUB Publication. This enables Marlin protection of EPUB contents.

1.1 Document Organization

This document is organized as follows:

- (This) introduction, including abbreviations, definitions and references.
- Overview of this document
- Cryptographic Profiles
- Marlin EPUB Extension

1.2 Conformance Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this specification are to be interpreted as described in IETF RFC 2119 [RFC2119].

These capitalized key words are used to unambiguously specify requirements and behavior that affect the interoperability and security of implementations. When these key words are not capitalized they are meant in their natural-language sense.

All Elements of this specification are considered **Normative** unless specifically marked **Informative**. All Normative Elements are **Mandatory** to implement, except where such an element is specifically marked **OPTIONAL**. Finally, where **Normative** elements are described as **OPTIONAL**, they MAY be omitted from an implementation, but when implemented, they MUST be implemented as described.

1.3 References

1.3.1 Normative references

[8pus]	Octopus DRM Technology Platform Specifications, Version 1.0
[AES]	Advanced Encryption Standard (AES), FIPS PUB 197, November 26, 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[AES-MODES]	Recommendation for Block Cipher Modes of Operation, NIST Special Publication 800-38A, 2001 Edition http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
[MAF]	Marlin Adaptive Streaming Specification - Full Profile
[MAS]	Marlin Adaptive Streaming Specification - Simple Profile
[MBNS]	Marlin – Broadband Network Service Profile Specification, Version 1.2
[MCS]	Marlin - Core System Specification, Version 1.3
[MFFS]	Marlin File Formats Specifications, Version 1.1
[MURIT]	URI Templates for Marlin, Version 1.0
[OCF]	International Digital Publishing Forum, EPUB Open Container Format (OCF), Version 2.0, 3.0
[OMArin]	OMArin Specification, Version 1.0

[RFC2104]	H. Krawczyk, M. Bellare, and R. Canetti. <i>HMAC: Keyed-Hashing for Message Authentication</i> . IETF RFC 2104. February 1997. http://www.ietf.org/rfc/rfc2104.txt
[RFC2396]	T. Berners-Lee, R. Fielding, L. Masinter. <i>Uniform Resource Identifiers (URI): Generic Syntax</i> . IETF RFC 2396. August 1998. http://www.ietf.org/rfc/rfc2396.txt
[RFC2630]	Network Working Group. R. Housley, <i>Cryptographic Message Syntax</i> . Request for Comments: 2630. June 1999. http://www.ietf.org/rfc/rfc2630.txt
[RFC4051]	D. Eastlake 3 rd . <i>Additional XML Security Uniform Resource Identifiers (URIs)</i> . IETF RFC4051. April 2005. http://www.ietf.org/rfc/rfc4051.txt
[xmldsig]	<i>XML-Signature Syntax and Processing Version 1.1 W3C Recommendation</i> http://www.w3.org/TR/xmldsig-core1/
[xmenc]	<i>XML Encryption Syntax and Processing Version 1.1, W3C Recommendation</i> http://www.w3.org/TR/xmenc-core1/
[xml-exc-c14n]	Exclusive XML Canonicalization, Version 1.0, W3C Recommendation 18 July 2002 http://www.w3.org/TR/xml-exc-c14n/

1.3.2 Informative references

Marlin	http://www.marlin-community.com/
--------	---

1.4 Terms and Definitions

EPUB	Electronic Publication http://www.idpf.org/
EPUB Publication	As defined by EPUB, a logical document entity consisting of a set of interrelated resources and packaged in a container.
Generic File Encryption	As defined in §3.1.1, an encryption schema which may apply to any type of resources in an EPUB Publication.
Marlin Content ID	As defined in [8pus] §2.2, the ID that uniquely identifies a Marlin content object
Marlin Content Key	As defined in [MCS] §1.5, the symmetric key that encrypts the payload of the Marlin content.
Marlin License	As defined in [8pus] §2.2, the consolidated form of content governance objects that are used to protect the content and associate usage rules to the protected content.
MCENC	As defined in [MAF] and [MAS], the MP4 Common Encryption Format with Marlin extensions.
MIPMP	As defined in [MFFS] §2.3, Marlin File Format using IPMP for Marlin Broadband Content.
PDCF	As defined in [OMarlin] §4, Packetized DRM Content Format.

2 Overview

This specification works with the EPUB Open Container Format [OCF]. This specification will use the existing extensibility features of [OCF] to include Marlin specific information, which will allow Marlin DRM Clients to recognize a Marlin-protected EPUB Publication, locate and/or acquire a relevant Marlin License, decrypt the encrypted contents and/or check the integrity of the contents in an EPUB Publication.

Figure 1 provides an overview of the resulting EPUB Publication files.

EPUB Publication

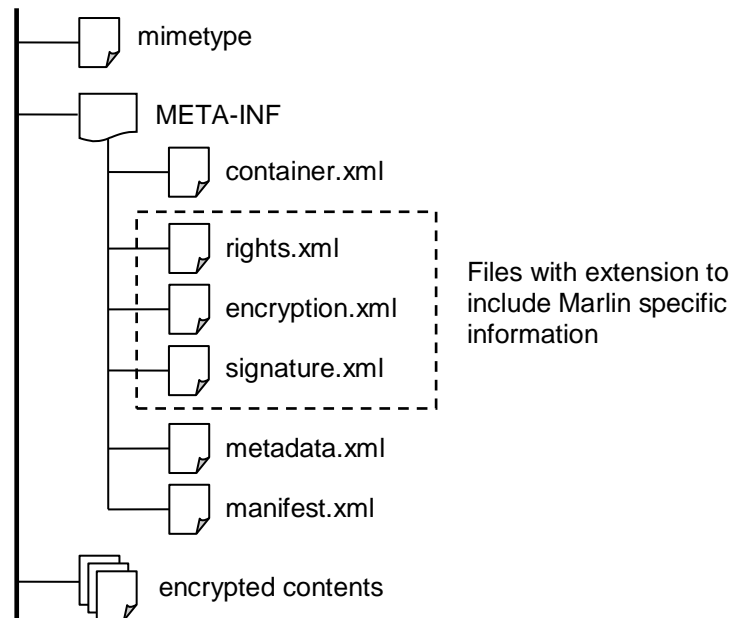


Figure 1: Overview

3 Cryptographic Profiles

As defined in [OCF], an EPUB Publication is a logical document entity consisting of a set of interrelated resources and packaged in an EPUB container. [OCF] has chosen [xmllenc] and [xmldsig] to be adopted for the encryption and signature of resources within an EPUB Publication. This section defines the cryptographic profile which complies with [xmllenc] and [xmldsig], to be used to protect of resources within an EPUB Publication.

3.1 Encryption

For EPUB Publication resources which conforms to the ISO Base Media File Format (ISO/IEC 14496-12) and requires encryption, any or a combination of the following encryption methods MUST be used:

- MCENC
- MIPMP
- PDCF
- Generic File Encryption (, defined in §3.1.1)

For other types of EPUB Publication resources that require encryption, Generic File Encryption as defined in §3.1.1 SHALL be used.

3.1.1 Generic File Encryption

Generic File Encryption MAY apply to any type of resources in an EPUB Publication. The encryption is performed on a per file basis, with one of the 128-bit AES algorithms listed in [xmllenc] §5. The algorithm of AES 128 bit key in Cipher Block Chaining (CBC) mode described in [xmllenc] §5.2 is RECOMMENDED as long as the vulnerability of the CBC block encryption algorithm, which is mentioned in [xmllenc] §6.9, can be mitigated or accepted in some reasonable way.

A DRM Client compliant to this specification MUST support Generic File Encryption with AES 128 bit key in CBC mode defined in [xmllenc] §5.2.

3.1.2 Marlin-defined Encryption Algorithm Identifiers

This section defines the identifiers which MUST be used to identify encryption algorithms besides Generic File Encryption, in the [xmllenc] based encryption framework of an EPUB Publication (in specific word the encryption file described in §4.2).

- MCENC:
<http://marlin-drm.com/epub/algorithm/mcenc>
- MIPMP:
<http://marlin-drm.com/epub/algorithm/mipmp>
- PDCF:
<http://marlin-drm.com/epub/algorithm/pdcf>

3.2 Signature

For any or all resources in an EPUB Publication that requires a digital signature, the XML Digital Signature Profile described in [MCS] §12.2 MUST be used.

4 Marlin EPUB Extension

This section defines the Marlin specific extensions of EPUB Open Container Format [OCF]. An EPUB Publication protected using the mechanism defined in this document SHALL have a rights management file (§4.1) and an encryption file (§4.2) within its META-INF directory. A digital signature file (§4.3) MAY also be included in the META-INF directory to hold digital signatures for resources.

4.1 Rights Management File

As defined in [OCF], a rights.xml file within the META-INF directory at the root level of the EPUB container file system holds digital rights management (DRM) information.

4.1.1 Signalling of Protection Scheme

An EPUB Publication protected using the mechanism defined in this document SHALL include in the rights.xml file a <Marlin> element with namespace declaration URL "http://marlin-drm.com/epub". The <Marlin> element MUST contain a child element <Version> with value 1.1 to signal this protection scheme version.

```
<Marlin xmlns="http://marlin-drm.com/epub">
  <Version>1.1</Version>
</Marlin>
```

4.1.2 Inclusion of Marlin License

An EPUB Publication protected using the mechanism defined in this document MAY include its Marlin License in the rights.xml file, under the <Marlin> element. The Octopus objects SHALL be encoded and bundled in a <oct:Bundle> element as defined in [MCS] §3.3.

The following is an example:

```
<Marlin xmlns="http://marlin-drm.com/epub">
  <Version>1.1</Version>
  <oct:Bundle xmlns:oct="http://www.octopus-drm.com/profiles/base/1.0">
    <!-- Octopus objects -->
    ...
  </oct:Bundle>
</Marlin>
```

4.1.3 Inclusion of Rights URL

An EPUB Publication protected using the mechanism defined in this document MAY include the following Rights URLs in the rights.xml file, in a <RightsURL> element under the <Marlin> element.

- Rights Issuer URL
- Silent Rights URL
- Preview Rights URL

A Rights URL MUST be a URL according to [RFC2396] or a URI template as defined in [MURIT]. A DRM Client MUST support [MURIT]. Note that the minimal mandatory processing required by [MURIT] is to remove the template placeholders (i.e., delimited by a "{" and "}" character) from the URL or replace it with a "~".

4.1.3.1 Rights Issuer URL

Information of a Rights Issuer URL is to be included in a <RightsIssuer> element under the <RightsURL> element. The <RightsIssuer> element SHALL have a <URL> child to hold the Rights Issuer URL.

The following is an example:

```
<Marlin xmlns="http://marlin-drm.com/epub">
  <Version>1.1</Version>
  <RightsURL>
    <RightsIssuer>
      <URL>http://www.xyz.com/book/get-token?cid=8A9CF56D</URL>
    </RightsIssuer>
  </RightsURL>
</Marlin>
```

4.1.3.2 Silent Rights URL

Information of a Silent Rights URL is to be included in a <SilentRights> element under the <RightsURL> element. The <SilentRights> element SHALL have a <URL> child to hold the Silent Rights URL and a <Method> child to hold the silent-method as described in [OMArin] §4.2.1.

The following is an example:

```
<Marlin xmlns="http://marlin-drm.com/epub">
  <Version>1.1</Version>
  <RightsURL>
    <SilentRights>
      <URL>http://www.xyz.com/book/get-token-silent?cid=8A9CF56D</URL>
      <Method>on-demand</Method>
    </SilentRights>
  </RightsURL>
</Marlin>
```

4.1.3.3 Preview Rights URL

Information of a Preview Rights URL is to be included in a <PreviewRights> element under the <RightsURL> element. The <PreviewRights> element SHALL have a <URL> child to hold the Preview Rights URL and a <Method> child to hold the preview-method as described in [OMArin] §4.2.2.

The following is an example:

```
<Marlin xmlns="http://marlin-drm.com/epub">
  <Version>1.1</Version>
  <RightsURL>
    <PreviewRights>
      <URL>http://www.xyz.com/book/get-token-preview?cid=8A9CF56D</URL>
      <Method>instant</Method>
    </PreviewRights>
  </RightsURL>
</Marlin>
```

4.1.3.4 Rights URL Processing

The following processing rules for handling the Rights URLs defined above SHALL be complied with:

- If the rights.xml file contains either a Silent Rights URL or a Preview Rights URL and there is no local available Marlin License, then an attempt to request a Marlin Action Token or a Marlin License SHALL be made automatically silently (without further user interaction).
- If the rights.xml file contains both a Silent Rights URL and a Preview Rights URL, the URL appearing first in the <RightsURL> element SHALL be prioritized and used to attempt to request a Marlin Action Token or a Marlin License first.
- If the rights.xml file contains a Rights Issuer URL parameter and there is no local available Marlin License and the context is a user-initiated session, requesting user consent and then getting a Marlin Action Token or a Marlin License SHALL be attempted by sending a HTTP GET request to the Rights Issuer URL. If the context is not a user-initiated session, then it is RECOMMENDED to abandon the rights acquisition effort.
- When requesting rights to the Rights Issuer URL, either of a Marlin Action Token, a Marlin License or a HTML which is defined by a Marlin-adopting system SHALL be returned and appropriately handled.

4.2 Encryption File

As defined in [OCF], an encryption.xml file within the META-INF directory at the root level of the EPUB container file system holds all encryption information on the contents of the container.

4.2.1 Associating Encrypted Resources to a Marlin License

An EPUB Publication protected using the mechanism defined in this document SHALL include in the encryption.xml file one or more <enc:EncryptedData> elements. Each <enc:EncryptedData> element SHALL have one <enc:CipherData> child and one <ds:KeyInfo> child, describing the relationship between an encrypted resource in that EPUB Publication and a Marlin License. If a resource is encrypted with Generic File Encryption, the <ds:KeyInfo> element SHALL have a <ds:KeyName> child, holding the Marlin Content ID by which the encrypted resource specified in <enc:CipherData> is associated with its Marlin License. If a resource is encrypted with MCENC, MIPMP or PDCF, the <ds:KeyInfo> element SHALL have a <ds:RetrievalMethod> child, holding the same URI in the URI attribute, as the URI attribute of <enc:CipherReference> for the encrypted resource.

The following is an example of encryption.xml file:

```
<?xml version="1.0"?>
<encryption xmlns="urn:oasis:names:tc:opendocument:xmlns:container"
  xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <!-- Encrypted book file -->
  <enc:EncryptedData Id="ED1">
    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
    <ds:KeyInfo>
      <!-- KeyName is the ContentID of the content file specified in enc:CipherData -->
      <ds:KeyName>urn:marlin:organization:xyz:1234:content-b-0:0001</ds:KeyName>
    </ds:KeyInfo>
    <enc:CipherData>
      <enc:CipherReference URI="OEBPS/book.html"/>
    </enc:CipherData>
  </enc:EncryptedData>
  <!-- Video content in MIPMP format -->
  <enc:EncryptedData Id="ED2">
    <enc:EncryptionMethod Algorithm="http://marlin-drm.com/epub/algorithm/mcenc"/>
    <ds:KeyInfo>
      <!-- RetrievalMethod is the same URI specified in enc:CipherReference -->
      <ds:RetrievalMethod URI="OEBPS/video/program.mp4">
    </ds:KeyInfo>
```

```
<enc:CipherData>
  <enc:CipherReference URI="OEBPS/video/program.mp4"/>
</enc:CipherData>
</enc:EncryptedData>
</encryption>
```

288
289

290 **4.3 Digital Signatures File**

291 As defined in [OCF], a signatures.xml file within the META-INF directory at the root level of
292 the EPUB container file system holds digital signatures of the container and its contents.

293

294 The signature profile (§3.2) allows HMAC signature and public key signature to be used. If a
295 resource in an EPUB Publication requires a HMAC signature, the key used for computing the
296 signature MUST be the Marlin Content Key by which the resource is encrypted. The Marlin
297 Content ID SHALL be the specified in the <ds:KeyName> element to indicate the key. If a
298 resource in an EPUB Publication requires a public key signature, the key used for computing
299 the signature MUST be an entity which its certificate is issued by a subordinate Content
300 License CA as specified in section 9.4.5.2 of [MCS].

301
302