

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

Conformance Test Specification for Marlin EPUB Extension Specification

Version 1.0
Final

Source	Marlin Developer Community
Date	August 2, 2011

29 **Notice**

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

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

51 Any copyright notices shall not be removed, varied, or denigrated in any
52 manner.

53 Copyright © 2011 by MDC, 415-112 North Mary Avenue #383 Sunnyvale, CA 94085,
54 USA. All rights reserved. Third-party brands and names are the property of their
55 respective owners.

56 **Intellectual Property**

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

59 **Contact Information**

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

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

64

65	Contents	
66		
67	1 Introduction	4
68	1.1 Document Organization	4
69	1.2 Overview	4
70	1.3 Conformance Conventions	4
71	1.4 References	4
72	2 Conformance Test Items for EPUB Publication	5
73	2.1 Signalling of Protection Scheme	5
74	2.2 Inclusion of Marlin License	5
75	2.3 Inclusion of Rights URL	5
76	2.4 Resource Encryption	5
77	2.5 Associating Encrypted Resources to a Marlin License	5
78	2.6 Digital Signature	6
79		

1 Introduction

1.1 Document Organization

This document describes the Conformance Test Specification for implementations of the Marlin - EPUB Extension Specification. It is organized as follows:

- (this) introduction, overview, conformance conventions and references
- Conformance Test Items for EPUB Publication

1.2 Overview

This document describes Conformance Test Specification for Marlin - EPUB Extension Specification. The goal for this specification is to help ensure a interoperable protected file format of EPUB Publication which can be used by independent Marlin implementations. In other words, this Conformance Test Specification does not ensure 100% coverage of the specification. It is expected that the tests are expanded upon as implementers verify interoperability with each other.

1.3 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 [RFC 2119].

1.4 References

Normative References

[MCS]	Marlin - Core System Specification, Version 1.3
[MEPUB]	Marlin - EPUB Extension Specification, version 1.0
[MFFS]	Marlin File Formats Specifications, Version 1.1
[MURIT]	URI Templates for Marlin, Version 1.0
[RFC 2119]	S. Bradner, <i>RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels</i> , IETF, March 1997, http://www.ietf.org/rfc/rfc2119.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
[xmllenc]	<i>XML Encryption Syntax and Processing, W3C Recommendation</i> http://www.w3.org/TR/xmllenc-core/

2 Conformance Test Items for EPUB Publication

This section describes the REQUIRED common test items for EPUB Publications protected by Marlin.

2.1 Signalling of Protection Scheme

The following SHALL be tested per [MEPUB] §4.1.1:

- The EPUB Publication SHALL include a <Marlin> element with namespace declaration URL “http://marlin-drm.com/epub”, in the rights.xml file within the META-INF directory at the root level of the EPUB container file system.
- The <Marlin> element MUST contain a child element <Version> with value 1.0.

The Conformance Test SHALL confirm the specifications above.

2.2 Inclusion of Marlin License

The following SHALL be tested per [MEPUB] §4.1.2, if the rights.xml file contains a Marlin License:

- The Marlin License is placed under the <Marlin> element.
- The Octopus objects SHALL be encoded and bundled in a <oct:Bundle> element as defined in [MCS] §3.3.

The Conformance Test SHALL confirm the specifications above.

2.3 Inclusion of Rights URL

The following SHALL be tested per [MEPUB] §4.1.3, if the rights.xml file contains Rights URL:

- The Rights URL is placed in a <RightsURL> element under the <Marlin> element.
- The Rights URL MUST be a URL according to [RFC2396] or a URI template as defined in [MURIT].

The Conformance Test SHALL confirm the specifications above.

2.4 Resource Encryption

The following SHALL be tested per [MEPUB] §3.1:

- For each encrypted resource in an EPUB Publication, the following SHALL be tested:
 - If a resource conforms to the ISO Base Media File Format (ISO/IEC 14496-12) before encryption, it MUST have an encrypted form which conforms to MIPMP ([MFFS] §2.3).
 - For other type of encrypted resources, the encryption MUST be performed on a per file basis, with the algorithm of AES 128 bit key in Cipher Block Chaining (CBC) mode described in [xmllenc] §5.2. (This encryption method is called Generic File Encryption)

The Conformance Test SHALL confirm the specifications above for the Marlin Import Agent.

2.5 Associating Encrypted Resources to a Marlin License

The following SHALL be tested per [MEPUB] §4.2.1:

- The EPUB Publication SHALL include one or more <enc:EncryptedData> elements, in the encryption.xml file within the META-INF directory at the root level of the EPUB container file system.

- Each <enc:EncryptedData> element SHALL have one <enc:CipherData> child and one <ds:KeyInfo> child.
 - For each encrypted resource in an EPUB Publication, the following SHALL be tested:
 - If a resource is encrypted with Generic File Encryption, the EncryptionMethod algorithm identifier MUST be “http://www.w3.org/2001/04/xmlenc#aes128-cbc”. 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 MIPMP, the EncryptionMethod algorithm identifier MUST be “http://marlin-drm.com/epub/algorithm/mipmp”. 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.
 - If a resource is encrypted with PDCF, the EncryptionMethod algorithm identifier MUST be “http://marlin-drm.com/epub/algorithm/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 Conformance Test SHALL confirm the specifications above.

2.6 *Digital Signature*

The following SHALL be tested per [MEPUB] §4.3, if the signatures.xml file within the META-INF directory at the root level of the EPUB container file system contains digital signatures:

- The signature profile conforms the XML Digital Signature Profile described in [MCS] §12.2.
- If a resource in an EPUB Publication uses a HMAC signature:
 - The key used for computing the signature MUST be the Marlin Content Key by which the resource is encrypted.
 - The Marlin Content ID SHALL be the specified in the <ds:KeyName> element to indicate the key.
- If a resource in an EPUB Publication requires a public key signature:
 - The key used for computing the signature MUST be an entity which its certificate is issued by a subordinate Content License CA as specified in section 9.4.5.2 of [MCS].

The Conformance Test SHALL confirm the specifications above.