

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 Simple Secure Streaming Specification

Version 1.1  
Final

Source	Marlin Developer Community
Date	March 14, 2012

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 © 2003 - 2012 by MDC, 415-112 North Mary Avenue #383 Sunnyvale, CA  
54 94085, USA. All rights reserved. Third-party brands and names are the property  
55 of their 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

## Contents

65			
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	Abbreviations .....	4
72	1.5	References .....	4
73	2	Conformance Test Items for MS3 Client.....	6
74	2.1	TLS Handshake .....	6
75	2.2	Stream Access Statement (SAS) Access.....	6
76	2.3	Triggering of MS3 Clients .....	6
77	2.3.1	Action Token .....	6
78	2.3.2	Compound URI .....	6
79	2.3.3	MS3 Manifest File .....	7
80	2.4	Handling of SAS and Content.....	7
81	3	Conformance Test Items for MS3 Service .....	8
82	3.1	TLS Handshake .....	8
83	3.2	Stream Access Statement (SAS) .....	8
84	3.3	Revocation Functions .....	8
85	3.4	Message Bindings .....	8
86	4	Conformance Test Items for Stream Access Statement (SAS) Evaluation .....	9
87	4.1	Variation 1.....	9
88	4.2	Variation 2.....	9
89	4.3	Variation 3.....	10
90	4.4	Variation 4.....	10
91			

# 1 Introduction

## 1.1 Document Organization

This document describes a Conformance Test Specification for client and service implementations for the Marlin Simple Secure Streaming Specification (MS3). It is organized as follows:

- (this) introduction, overview, conformance conventions and references
- Sections for each of the Conformance Test Items. These are:
  - Conformance Test Items for MS3 Client
  - Conformance Test Items for MS3 Service
  - Conformance Test Items for Stream Access Statement (SAS) Evaluation

## 1.2 Overview

This document describes Conformance Test Specification for client and service implementations of the Marlin Simple Secure Streaming Specification [MS3]. The goal for this specification is to help ensure interoperability between independent implementations of MS3 Clients and MS3 Services supporting secure HTTP streaming by testing functions specified in [MS3]. 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 Abbreviations

AES	Advanced Encryption Standard
C-URIT	URI Template for Content URL
C-URL	Content URL
MS3	Marlin Simple Secure Streaming
MIME	Multipurpose Internet Mail Extensions
NEMO	Networked Environment for Media Orchestration
SAS	Stream Access Statement
SHA-1	Secure Hash Function 1
S-URL	Stream Access Statement URL
TLS	Transport Layer Security

## 1.5 References

### Normative References

[HTTP/TLS]	HTTP Over TLS, IETF RFC 2818. <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a>
[MS3]	Marlin – Simple Secure Streaming Specification, version 1.1
[RFC 2119]	S. Bradner, <i>RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels</i> , IETF, March 1997, <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
[TLS]	The Transport Layer Security (TLS) Protocol version 1.2, IETF RFC 5246

121

[TLSAES]	AES Ciphersuites for TLS, IETF RFC 3268. <a href="http://www.ietf.org/rfc/rfc3268.txt">http://www.ietf.org/rfc/rfc3268.txt</a>
----------	---

## 2 Conformance Test Items for MS3 Client

This section describes common functions REQUIRED for Marlin MS3 Clients.

### 2.1 TLS Handshake

The following SHALL be tested for MS3 Client:

- From §3.1.1 of [MS3], MS3 Client SHALL only use TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA [TLSAES] cipher suite when performing TLS handshake with the MS3 Service.

The Conformance Test SHALL confirm the specifications above for the client.

### 2.2 Stream Access Statement (SAS) Access

The following SHALL be tested for MS3 Client:

- From §3 of [MS3], MS3 Client MUST establish a [TLS] session using the profile defined in §3.1 of [MS3].
- From §3.2 of [MS3], MS3 Client MUST issue an HTTP GET request to the service resource specified by the S-URL.
- From §3.2 of [MS3], MS3 Client MUST support expanding the C-URIT with template variables including the authenticator variable.

The Conformance Test SHALL confirm the specification above for the client.

### 2.3 Triggering of MS3 Clients

#### 2.3.1 Action Token

The support of Action Token is OPTIONAL for MS3 Client that implements [MS3].

The following SHALL be tested for MS3 Client that indicates support for Action Token.

- MS3 Client SHALL be capable of handling the Action Token and SHOULD initiate the protocol binding defined in §3.2 of [MS3] to resolve the URL carried in the <ms3:SASLocation> element. In the case of a compound URI encoding the MS3 Client SHALL parse the URI to derive the S-URL and C-URIT components.

The Conformance Test SHALL confirm to the specifications above for the client.

#### 2.3.2 Compound URI

The support of Compound URI is OPTIONAL for MS3 Client that implements [MS3].

The following SHALL be tested for MS3 Client that indicates support for Compound URI.

- From §4.2 of [MS3], MS3 Client SHALL use the Compound URI to uniquely associate an SAS with corresponding content when `contentId` is not specified in the SAS and content.
- From §3.4.2 of [MS3], MS3 Client SHALL be capable of parsing the compound URI at the fragment (“#”) delimiter to derive distinct S-URL and C-URIT parameters. Subsequent processing of the resultant C-URIT SHALL decode percent-encoded characters and adhere to the expansion rules defined in §3.3 of [MS3].
- From §3.4.2 of [MS3], MS3 Client MAY support the “ms3” URI scheme. An MS3 Client supporting the “ms3” URI scheme SHALL process the S-URL in a manner equivalent to the “https” URI scheme.
- From §3.4.2 of [MS3], if C-URIT includes the placeholder for Authenticator, the MS3 Client SHALL use the associated S-URL to retrieve the SAS bearing

166 the Authenticator. The supplied Authenticator SHALL replace the placeholder  
 167 in the C-URIT.  
 168 • From §4.2 of [MS3], MS3 Client SHALL support capability query for the SAS  
 169 MIME Type.  
 170 • From §4.2 of [MS3], MS3 Client SHALL support and process the container  
 171 parameter query. If the Client does not support the media format designated  
 172 in the container parameter, it SHALL return a negative response when  
 173 queried.  
 174 The Conformance Test SHALL confirm the specifications above for the client.

### 175 **2.3.3 MS3 Manifest File**

176 The support of MS3 Manifest File is OPTIONAL for MS3 Client that implements  
 177 [MS3].  
 178 The following SHALL be tested for MS3 Client that indicates support for MS3  
 179 Manifest File.  
 180 • From §3.4.3 of [MS3], if the MIME type  
 181 application/vnd.marlin.drm.StreamAccessDescriptor is signaled, the MS3  
 182 Client SHALL treat the payload as a Stream Access Descriptor.  
 183 • From §4.3 of [MS3], MS3 Client SHALL uniquely associate the SAS acquired  
 184 from S-URL with the corresponding content acquired from C-URIT when  
 185 `contentId` is not specified in the SAS and content.  
 186 • From §4.3 of [MS3], MS3 Client SHALL return “probably” or “maybe” to the  
 187 capability query MS3 Manifest file MIME Type.  
 188 The Conformance Test SHALL confirm the specifications above for the client.  
 189

## 190 **2.4 Handling of SAS and Content**

191 The following SHALL be tested for MS3 Client:  
 192 • From §4 of [MS3], the use of content obtained from the C-URL by MS3 Client  
 193 SHALL be subject to the constraints expressed in the SAS obtained from the  
 194 corresponding S-URL.  
 195 • From §3.5.1 of [MS3], MS3 Client SHALL only cache an SAS for a  
 196 reasonable retention period so as to enable content rendering. After playback  
 197 has ended or stopped (e.g. by user interaction), a conformant MS3 Client  
 198 SHALL discard the corresponding SAS.  
 199 • From §3.5.2 of [MS3], when the bit 0(LSB) of the `controlFlags` is set to 1  
 200 in the SAS, MS3 Client SHALL NOT retain the downloaded content, either in  
 201 encrypted or plaintext form corresponding to the SAS except for a reasonable  
 202 retention period to allow for buffering so as to preserve the fidelity of the  
 203 content rendering.  
 204 • From §3.5.2 of [MS3], when a bit flag in `outputControlFlags` is set to 1,  
 205 the Client SHALL set the output control parameter as specified by the  
 206 corresponding bit-field in the `outputControlValue`. When a bit flag in  
 207 `outputControlFlags` is set to 0, the MS3 Client SHALL set the  
 208 corresponding output control parameter as specified by the default in §3.5.3 of  
 209 [MS3].  
 210 • From §3.5.2 of [MS3], the output control requirements MUST be enforced or  
 211 the corresponding content SHALL NOT be consumed.  
 212 The Conformance Test SHALL confirm the specifications above for the client.  
 213

## 3 Conformance Test Items for MS3 Service

This section describes the functions REQUIRED for MS3 Service.

### 3.1 TLS Handshake

The following SHALL be tested for MS3 Service:

- From §3.1.1 of [MS3], MS3 Service SHALL only use TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA [TLSAES] cipher suite when performing TLS handshake with the MS3 Client.
- From §3.1.3 of [MS3], MS3 Service SHALL validate the MS3 client certificate.

The Conformance Test SHALL confirm the specifications above for the service.

### 3.2 Stream Access Statement (SAS)

The following SHALL be tested for MS3 Service:

- From §3.5.2 of [MS3], when the content is not encrypted, the `keycount` in the SAS SHALL be set to 0.
- From §3.5.2 of [MS3], the `contentIds` in the SAS (if present) SHALL be the SHA-1 hash of the content identifiers.

The Conformance Test SHALL confirm the specification above for the service.

### 3.3 Revocation Functions

The following revocation functions SHALL be tested for MS3 Service:

- From §3.1.3 of [MS3], when any CAs in the MS3 Client X.509v3 certificate chain is revoked, the MS3 Service does not provide its service to the client.
- From §3.1.3 of [MS3], when the MS3 Client uses an X.509v3 certificate that has been revoked, the MS3 Service does not provide its service to the client.

The Conformance Test SHALL confirm the specification above for the service.

### 3.4 Message Bindings

The following SHALL be tested for MS3 Service:

- From §3.2 of [MS3], when the HTTP GET request from the MS3 Client contains an entity header, the MS3 Service SHALL ensure that the MS3 protocol version supported by the client is 1.0 or above.
- From §3.2 of [MS3], if the MS3 Service grants access to the MS3 Client, the MS3 Service SHALL return a successful HTTP 200 (OK) response via the secure TLS channel.
- From §3.2 of [MS3], a successful HTTP response returned by the MS3 Service to convey the SAS MUST contain a Content-Type entity header to signal the MIME type `application/vnd.marlin.drm.StreamAccessStatement`.

The Conformance Test SHALL confirm the specification above for the service.

## 4 Conformance Test Items for Stream Access Statement (SAS) Evaluation

This section describes variations of Marlin SAS RECOMMENDED to be used for the SAS evaluation test of MS3 Client. The SAS evaluation test is to confirm whether MS3 Clients can evaluate the SAS as expected.

### 4.1 Variation 1

This variation assumes the Marlin content is encrypted and it is streamed to MS3 clients. The LSB(0) of the `controlFlags` is set to 1, indicating that content must not be stored. The SAS includes:

- `keys`
  - ✧ An AES key to decrypt the marlin content.
  - ✧ `keyCount` is set to 1.
  - ✧ The key is linked to a Marlin `contentId`.
- `authenticator`
  - ✧ `authenticatorSize` is set to 0.
  - ✧ `authenticator` is empty.
- `ControlFlags`
  - ✧ LSB(0) is set to 1 to indicate that the content (both encrypted and plain) must not be stored.
- `usageRule`
  - ✧ All bit-flag of `OutputControlFlags` are set to 0, thus use default output control.
- `extensions`
  - ✧ No extension is defined.

This MS3 Client SHALL accept the SAS.

### 4.2 Variation 2

This variation assumes the Marlin content is encrypted and it is streamed to MS3 clients. The LSB(0) of the `controlFlags` is set to 1, indicating that content must not be stored. There is an unknown extension with non-critical flag. The SAS includes:

- `keys`
  - ✧ An AES key to decrypt the marlin content.
  - ✧ `keyCount` is set to 2.
  - ✧ The keys are linked to two Marlin `contentIds`.
- `authenticator`
  - ✧ `authenticatorSize` is set to 0.
  - ✧ `authenticator` is empty.
- `ControlFlags`
  - ✧ LSB(0) is set to 1 to indicate that the content (both encrypted and plain) must not be stored.
- `usageRule`
  - ✧ All bit-flag of `OutputControlFlags` are set to 0, thus use default output control.
- `extensions`
  - ✧ There is an unknown extension with non-critical flag.

298 This MS3 Client SHALL ignore the extension.  
 299

### 300 **4.3 Variation 3**

301 This variation assumes the Marlin content is encrypted and it is streamed to MS3  
 302 clients. The LSB(0) of the `controlFlags` is set to 1, indicating that content must not  
 303 be stored. There is an unknown extension with critical flag. The SAS includes:

- 304 • `keys`
  - 305 ✧ An AES key to decrypt the marlin content.
  - 306 ✧ `keyCount` is set to 1.
  - 307 ✧ The key is linked to a Marlin `contentId`.
- 308 • `authenticator`
  - 309 ✧ `authenticatorSize` is set to 0.
  - 310 ✧ `authenticator` is empty.
- 311 • `ControlFlags`
  - 312 ✧ LSB(0) is set to 1 to indicate that the content (both encrypted and plain)  
 313 must not be stored.
- 314 • `usageRule`
  - 315 ✧ All bit-flag of `OutputControlFlags` are set to 0, thus use default  
 316 output control.
- 317 • `extensions`
  - 318 ✧ There is an unknown extension with critical flag.

319  
 320 This MS3 Client SHALL refuse the SAS.  
 321

### 322 **4.4 Variation 4**

323 This variation assumes the Marlin content is not encrypted and it is streamed to the  
 324 MS3 client upon successful client authentication. The LSB(0) of the `controlFlags`  
 325 is set to 1, indicating that content must not be stored. The SAS includes:

- 326 • `keys`
  - 327 ✧ No AES key is required.
  - 328 ✧ `keyCount` is set to 0.
  - 329 ✧ Marlin `contentId` is empty.
- 330 • `authenticator`
  - 331 ✧ `authenticatorSize` is set to 1.
  - 332 ✧ `authenticator` is specified.
- 333 • `controlFlags`
  - 334 ✧ LSB(0) is set to 1 to indicate that the content (unencrypted) must not be  
 335 stored.
- 336 • `usageRule`
  - 337 ✧ All bit-flag of `outputControlFlags` are set to 0, thus use default  
 338 output control.
- 339 • `extensions`
  - 340 ✧ No extension is defined.

341  
 342 This MS3 Client SHALL accept the SAS.  
 343