Conformance Test Specification for Marlin Simple Secure Streaming Specification

Version 1.1
Final

Source	Marlin Developer Community
Date	March 14, 2012

Notice

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

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

Intellectual Property

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

Contact Information

Feedback on this specification should be addressed to: editor@marlin-community.com

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

Contents

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

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

[TLSAES]	AES Ciphersuites for TLS, IETF RFC 3268. http://www.ietf.org/rfc/rfc3268.txt

121

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

the Authenticator. The supplied Authenticator SHALL replace the placeholder in the C-URIT.

- From §4.2 of [MS3], MS3 Client SHALL support capability query for the SAS MIME Type.
- From §4.2 of [MS3], MS3 Client SHALL support and process the container parameter query. If the Client does not support the media format designated in the container parameter, it SHALL return a negative response when queried.

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

2.3.3 MS3 Manifest File

The support of MS3 Manifest File is OPTIONAL for MS3 Client that implements [MS3].

The following SHALL be tested for MS3 Client that indicates support for MS3 Manifest File.

- From §3.4.3 of [MS3], if the MIME type application/vnd.marlin.drm.StreamAccessDescriptor is signaled, the MS3 Client SHALL treat the payload as a Stream Access Descriptor.
- From §4.3 of [MS3], MS3 Client SHALL uniquely associate the SAS acquired from S-URL with the corresponding content acquired from C-URIT when `contentId` is not specified in the SAS and content.
- From §4.3 of [MS3], MS3 Client SHALL return “probably” or “maybe” to the capability query MS3 Manifest file MIME Type.

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

2.4 Handling of SAS and Content

The following SHALL be tested for MS3 Client:

- From §4 of [MS3], the use of content obtained from the C-URL by MS3 Client SHALL be subject to the constraints expressed in the SAS obtained from the corresponding S-URL.
- From §3.5.1 of [MS3], MS3 Client SHALL only cache an SAS for a reasonable retention period so as to enable content rendering. After playback has ended or stopped (e.g. by user interaction), a conformant MS3 Client SHALL discard the corresponding SAS.
- From §3.5.2 of [MS3], when the bit 0(LSB) of the `controlFlags` is set to 1 in the SAS, MS3 Client SHALL NOT retain the downloaded content, either in encrypted or plaintext form corresponding to the SAS except for a reasonable retention period to allow for buffering so as to preserve the fidelity of the content rendering.
- From §3.5.2 of [MS3], when a bit flag in `outputControlFlags` is set to 1, the Client SHALL set the output control parameter as specified by the corresponding bit-field in the `outputControlValue`. When a bit flag in `outputControlFlags` is set to 0, the MS3 Client SHALL set the corresponding output control parameter as specified by the default in §3.5.3of [MS3].
- From §3.5.2 of [MS3], the output control requirements MUST be enforced or the corresponding content SHALL NOT be consumed.

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

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.

This MS3 Client SHALL ignore the extension.

4.3 Variation 3

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 critical flag. 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`
  - There is an unknown extension with critical flag.

This MS3 Client SHALL refuse the SAS.

4.4 Variation 4

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

- `keys`
  - No AES key is required.
  - `keyCount` is set to 0.
  - Marlin `contentId` is empty.
- `authenticator`
  - `authenticatorSize` is set to 1.
  - `authenticator` is specified.
- `controlFlags`
  - LSB(0) is set to 1 to indicate that the content (unencrypted) 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.