

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

Marlin IPTV End-point Service Conformance Test
Specification for IP Multicast Services
Version 1.0.2
Final

Source	Marlin Developer Community
Date	3 March, 2010

29 **Notice**

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

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

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

54 Copyright © 2003 - 2010 by MDC, 415-112 North Mary Avenue #383 Sunnyvale, CA
55 94085, USA. All rights reserved. Third-party brands and names are the property
56 of their respective owners.

57 **Intellectual Property**

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

60 **Contact Information**

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

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

65	Contents	
66		
67	1 Introduction	4
68	1.1 Scope.....	4
69	1.2 References	4
70	1.3 Terminology and Definitions	4
71	1.3.1 Abbreviations	4
72	2 Conformance Test Items.....	6
73	2.1 Overview.....	6
74	2.2 Phase1 Test Items.....	8
75	2.2.1 Challenge Message	8
76	2.2.2 Response & Challenge Message	8
77	2.2.3 Plain Command Message (Error)	8
78	2.3 Phase2 Test Items.....	8
79	2.3.1 Response & Request Message	8
80	2.3.2 Reply Message	8
81	2.3.3 Plain Command Message (Error)	9
82	2.4 Phase3 Test Items.....	9
83	2.4.1 Request Message	9
84	2.4.2 Reply Message	9
85	2.4.3 Encrypted Command Message (Error)	9
86	2.5 Phase4 Test Items.....	9
87	2.5.1 Encrypted Command Message (Commit).....	9
88	2.5.2 Encrypted Command Message (ACK).....	10
89	2.6 Optional Test Items	10
90	Appendix A Sample SAC Messages (Non-Normative)	12
91	A.1 Overview.....	12
92	A.2 Assumed Test Environment.....	12
93	A.2.1 Overview	12
94	A.2.2 Assumed test procedure	12
95	A.2.3 Prerequisite.....	12
96	A.3 Test Message	13
97	A.3.1 Overview	13
98	A.3.2 Fixed Values	13
99	A.3.2.1 Random Numbers	13
100	A.3.2.2 Device Information.....	14
101	A.3.2.3 Usage Rule Reference	14
102	A.3.2.4 Content Key	15
103	A.3.2.5 ExtractInfo	16
104	A.3.2.6 Trusted Time	16
105		

Introduction

Scope

This document specifies Marlin IPTV End-point Service (IPTV-ES) conformance test specification (CTS) for IP Multicast services. The Marlin IPTV-ES specification supports VOD and Download services in addition to IP Multicast services. The CTS for the VOD and Download services are not within the scopes of this document. They are specified in separate documents.

The CTS is provided to check the interpretation of the Marlin IPTV End-point Service specification [IPTV-ES]. With the CTS, the interoperability between Marlin IPTV-ES Servers and Devices is ensured. Handling of Certificate Revocation List (CRL), Device Revocation List (DRL) and certificates is also tested with the CTS. On the other hand, this CTS does not ensure 100% coverage of the Marlin IPTV End-point Service Specification such as handling Marlin IPTV-ES Content. It is expected that the tests are supplemented by implementers to verify the entire conformance to the specification.

Because of its purpose, the CTS specified in this document covers all the valid cases including erroneous cases defined in [IPTV-ES] such as an error message sent from Marlin IPTV-ES Server when authentication of the Marlin IPTV-ES Device is failed on the SAC establishment. With regard to valid error parameters of SAC messages, one typical error value is picked up and involved in the CTS test messages. On the other hand, The CTS does not include invalid cases such as invalid values in SAC messages, which are not defined in [IPTV-ES].

References

[IPTV-ES]	Marlin IPTV End-point Service Specification, Version 1.0.2.
[IEEE1363-2000]	IEEE Standard Specifications for Public-Key Cryptography.
[TESTITEM]	Marlin IPTV End-point Service Conformance Test Item Specification for IP Multicast services, Version 1.0.1.
[VODTESTITEM]	Marlin IPTV End-point Service Conformance Test Item Specification for VOD services, Version 1.0.1.
[CTK]	Marlin IPTV End-point Service Common Test Key Data Sheets
[SAMPLE]	Marlin IPTV End-point Service Conformance Test Sample Messages and Sequences for IP Multicast services, Version 1.0.1.

Terminology and Definitions

Abbreviations

IPTV-ES	IPTV End-point Service
CTS	Conformance Test Specification
CRL	Certificate Revocation List
DRL	Device Revocation List
CTK	Common Test Key

Conformance Test Items

Overview

The Marlin IPTV End-point Service Specification [IPTV-ES] defines the SAC protocol between Marlin IPTV-ES Servers and Devices, the Service protocols over the SAC, Marlin IPTV-ES Trust Management, and Marlin IPTV-ES encrypted content formats. The CTS is for the conformity and the interoperability of the implementations of the Marlin IPTV-ES Servers and Devices, therefore the tests specified in this Conformance Test Specification are as follow:

- SAC protocol sequence tests including certificate handling tests
- Service protocol sequence tests for IP Multicast services
- CRL handling tests
- DRL handling tests

With regard to the service protocol sequence tests, test items only for the IP Multicast services are specified in this document.

Each of test items specified in this document is categorized into four phases of the Marlin IPTV-ES SAC protocol as shown in Figure 0-1 and Figure 0-2. Each of the phases consists of a pair of SAC messages, one is from a Marlin IPTV-ES Device to a Marlin IPTV-ES Server and the other is from the Marlin IPTV-ES Server to the Marlin IPTV-ES Device. Each of test items is for checking conformant processing of one SAC message on both ends. A test item is specified with its phase, test description, prerequisites, and the expected result.

Test items are labelled as Mandatory or Optional. Mandatory test items are for testing functions necessary for all IP Multicast service capable Marlin IPTV-ES Servers and Devices. Optional test sequences are for testing functions that might not be implemented in a certain implementation. See section 0 for mandatory/optional test items.

The test items are specified in [TESTITEM]. Some test items are not applicable for Marlin IPTV-ES Server or Device. The applicability is shown in Test Target column and non-applicable parts are greyed out in [TESTITEM].

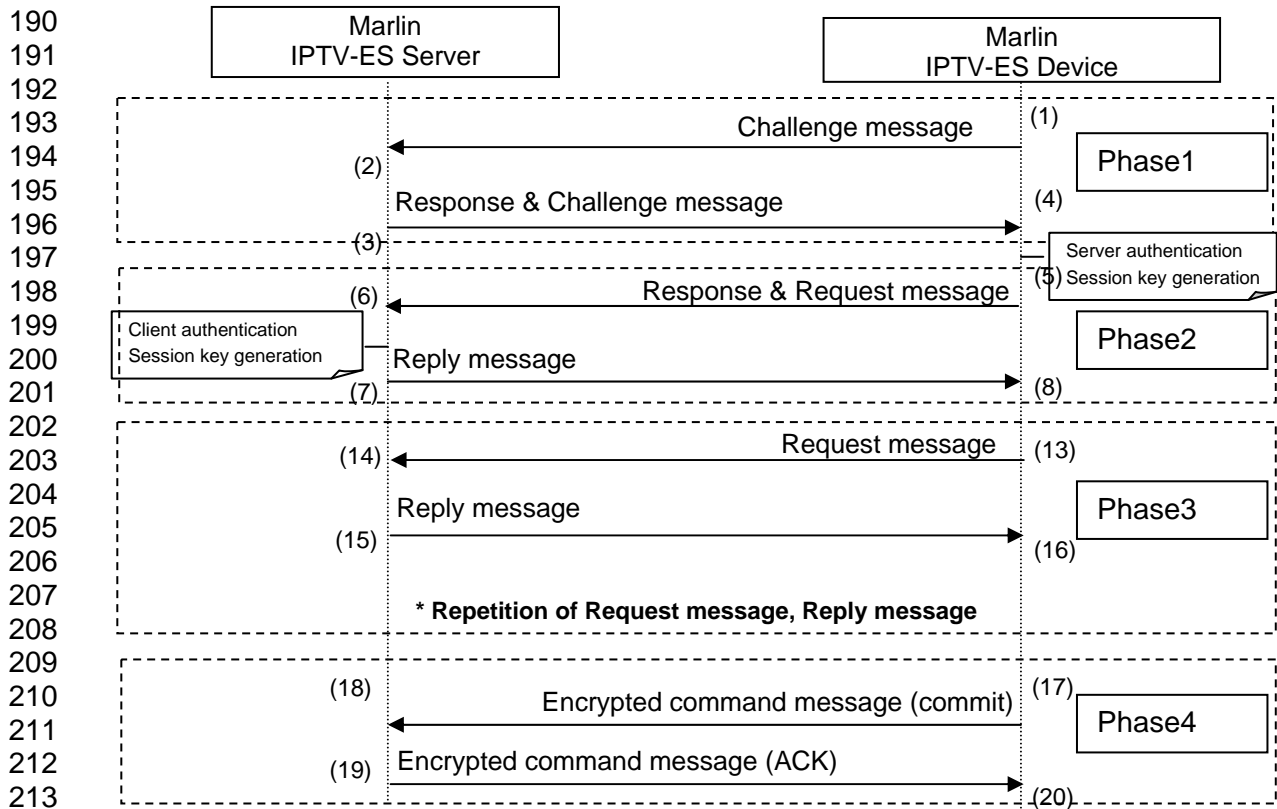


Figure 0-1 Basic Sequence Structure of the Case where Multiple Requests are sent over the SAC

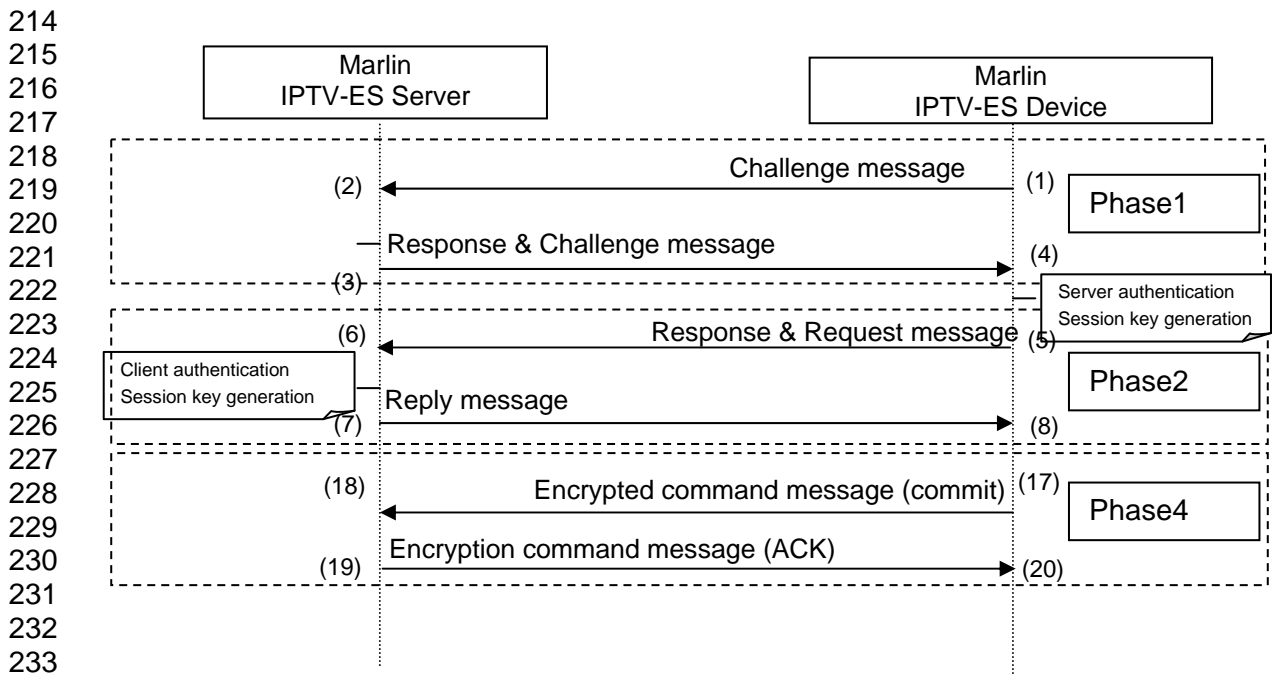


Figure 0-2 Basic Sequence Structure of the Case where Only One Request is sent over the SAC

236 ***Phase1 Test Items***

237 **ChallengeMessage**

238 Challenge Message is sent by Marlin IPTV-ES Devices to Marlin IPTV-ES Servers as
239 the first SAC message in the SAC protocol. The Challenge Message contains
240 SinkCertificate that the receiving Marlin IPTV-ES Server verifies. Therefore, test
241 items on verification of SinkCertificate and processing DRLs are included in this test
242 item group. One test item representing all the erroneous Challenge Message is
243 specified.
244 See the test item specifications in the Sheet "Phase1_C->S" of [VODTESTITEM].
245

246 **Response & Challenge Message**

247 Response & Challenge Message is sent by Marlin IPTV-ES Servers to Marlin IPTV-
248 ES Devices responding to Challenge Message. The Response & Challenge Message
249 contains SourceCertificate that the receiving Marlin IPTV-ES Device verifies.
250 Therefore, test items on verification of SourceCertificate and processing CRLs are
251 included in this test item group.
252 See the test item specifications in the sheet "Phase1_S->C" of [VODTESTITEM].
253

254 **Plain Command Message (Error)**

255 When the Marlin IPTV-ES Server fails in verification of Challenge Message, the
256 Marlin IPTV-ES Server sends Plain Command Message with Error Command to the
257 Marlin IPTV-ES Device. One test item of Plain Command Message as the response
258 to the erroneous Challenge Message is specified.
259 See the test item specification in the sheet "Phase1_S->C" of [VODTESTITEM].
260

261 ***Phase2 Test Items***

262 **Response & Request Message**

263 Response & Request Message is sent by Marlin IPTV-ES Devices to Marlin IPTV-ES
264 Servers responding to Response & Challenge Message. Erroneous Response &
265 Request Message, which error is at the SAC layer, representing all the other
266 erroneous Response & Request Message is specified. Since the Response &
267 Request Message contains Get Permission Request or Packed Message Request for
268 IP Multicast services, test items about the two sorts of Requests are specified.
269 Erroneous Requests for each of the two sorts representing the other erroneous
270 cases are also specified.
271 See the test item specifications in the sheet "Phase2_C->S" of [TESTITEM].
272

273 **Reply Message**

274 Reply Message is sent by Marlin IPTV-ES Servers to Marlin IPTV-ES Devices
275 responding to Response & Request Message in Phase2. Since the Reply Message
276 contains Get Permission Reply or Packed Message Reply for IP Multicast services,
277 test items about the two sorts of Replies are specified. Reply with Error Status for
278 each of the two sorts representing the other erroneous cases are also specified.
279 See the test item specifications in the sheet "Phase2_S->C" of [TESTITEM].
280

Plain Command Message (Error)

When the Marlin IPTV-ES Server fails in verification of Response & Request Message, the Marlin IPTV-ES Server sends Plain Command Message with Error Command to the Marlin IPTV-ES Device. One test item of Plain Command Message as the response to the erroneous Response & Request Message is specified. See the test item specification in the sheet "Phase2_S->C" of [TESTITEM].

Phase3 Test Items

Request Message

Request Message may be sent to Marlin IPTV-ES Servers after receiving Reply Message by Marlin IPTV-ES Devices. Erroneous Request Message, which error is at the SAC layer, representing all the other erroneous Request Message is specified. Since the Request Message contains Get Permission Request or Packed Message Request for IP Multicast services as well as Response & Request Message, test items about the two sorts of Requests are specified. Erroneous Request for each of the two sorts representing the other erroneous cases are also specified. See the test item specifications in the sheet "Phase3_C->S" of [TESTITEM].

Reply Message

Reply Message is sent by Marlin IPTV-ES Servers to Marlin IPTV-ES Devices responding to Request Message in Phase3. Since the Reply Message contains Get Permission Reply or Packed Message Reply for IP Multicast services, test items about the two sorts of Replies are specified. Reply with Error Status for each of the two sorts representing the other erroneous cases are also specified. See the test item specifications in the sheet "Phase3_S->C" of [TESTITEM].

Encrypted Command Message (Error)

When the Marlin IPTV-ES Server fails in verification of Request Message, the Marlin IPTV-ES Server sends Encrypted Command Message with Error Command to the Marlin IPTV-ES Device. One test item of Encrypted Command Message as the response to the erroneous Request Message is specified. See the test item specification in the sheet "Phase3_S->C" of [TESTITEM].

Phase4 Test Items

Encrypted Command Message (Commit)

Encrypted Command Message with Commit Command is sent by Marlin IPTV-ES Devices to Marlin IPTV-ES Servers to terminate the SAC session. Two patterns of Encrypted Command Messages with Commit Command are specified, since SequenceNumber in the Encrypted Command Messages are different according to whether Phase3 is included in the SAC session. Two erroneous Encrypted Command Messages representing all the other erroneous Encrypted Command Message with Commit Command are also specified corresponding to the two normal Encrypted Command Messages. See the test item specifications in the sheet "Phase4_C->S" of [VODTESTITEM].

Encrypted Command Message (ACK)

Encrypted Command Message with ACK Command is sent by Marlin IPTV-ES Servers to Marlin IPTV-ES Devices responding to Encrypted Command Message with Commit Command. Two patterns of Encrypted Command Messages with ACK Command are specified, since SequenceNumber in the Encrypted Command Messages are different according to whether Phase3 is included in the SAC session. Two erroneous Encrypted Command Messages representing all the other erroneous Encrypted Command Message with ACK Command are also specified corresponding to the two normal Encrypted Command Messages. See the test item specifications in the sheet "Phase4_S->C" of [VODTESTITEM].

Optional Test Items

Test items shown in Table 0-1 are OPTIONAL for Marlin IPTV-ES Device or Server implementations described in the Tested Objects column of Table 0-1. The test item numbers in the Optional Test Items column indicate test items specified in [TESTITEM]. All the other test items are MANDATORY.

Tested Objects	Optional Test Items
Marlin IPTV-ES Devices that do not support GeneralizedTime in notBefore/notAfter of Server certificates.	<ul style="list-style-type: none">• 2.1.1.2• 2.1.1.3• 2.1.2.2• 2.1.2.3
Marlin IPTV-ES Devices that do not support GeneralizedTime in thisUpdate/nextUpdate of CRLs.	<ul style="list-style-type: none">• 2.2.3.1• 2.2.3.2• 2.2.4.1• 2.2.4.2• 2.2.4.3• 2.2.4.4
Marlin IPTV-ES Devices that do not support Get Permission Request message.	<ul style="list-style-type: none">• 3.1.1.1• 4.1.1.1• 4.2.1.1
Marlin IPTV-ES Devices that do not support Get Trusted Time Request message.	<ul style="list-style-type: none">• 3.1.2.1• 4.1.2.1• 4.2.2.1
Marlin IPTV-ES Devices that do not support Packed Message Request with a certain combination of request messages specified in each Test Item. Note that combinations of request messages supported by the tested Marlin IPTV-ES Device are not optional.	<ul style="list-style-type: none">• 3.1.3.1• 3.1.4.1• 3.1.5.1• 3.1.6.1• 4.1.3.1• 4.1.4.1• 4.1.5.1• 4.1.6.1• 4.2.3.1
Marlin IPTV-ES Devices that do not support Get Permission Request message in Request messages.	<ul style="list-style-type: none">• 5.1.1.1• 6.1.1.1• 6.2.1.1
Marlin IPTV-ES Devices that do not support Get Trusted Time Request message in Request message.	<ul style="list-style-type: none">• 5.1.2.1• 6.1.2.1• 6.2.2.1
Marlin IPTV-ES Devices that do not	<ul style="list-style-type: none">• 5.1.3.1

support Packed Message Request message with a certain combination of request messages specified in each Test Item in Request messages. Note that combinations of request messages supported by the tested Marlin IPTV-ES Device are not optional.	<ul style="list-style-type: none"> • 5.1.4.1 • 5.1.5.1 • 5.1.6.1 • 6.1.3.1 • 6.1.4.1 • 6.1.5.1 • 6.1.6.1 • 6.2.3.1
Marlin IPTV-ES Devices that do not support Request messages.	<ul style="list-style-type: none"> • 6.3.1.1 • 7.1.1.1 • 8.1.1.1
Marlin IPTV-ES Servers that do not support GeneralizedTime in notBefore/notAfter of Client certificates	<ul style="list-style-type: none"> • 1.1.1.2 • 1.1.1.3 • 1.1.2.2 • 1.1.2.3
Marlin IPTV-ES Servers that do not support GeneralizedTime in thisUpdate/nextUpdate of DRLs	<ul style="list-style-type: none"> • 1.2.2.3 • 1.2.2.4 • 1.2.2.5 • 1.2.2.6

Table 0-1 Optional Test Items

Sample SAC Messages (Non-Normative)

Overview

Sample SAC messages for the test items specified in [SAMPLE] are provided as references.

Assumed Test Environment

Overview

Test items specified in this document can be performed with the sample test messages of SAC protocol and test sequences. The test messages utilize the Common Test Keys (CTK) as credentials of tested Marlin IPTV-ES Servers and Devices.

Test messages are messages exchanged between Marlin IPTV-ES Servers and Devices over the SAC defined in [IPTV-ES]. The test messages are assumed to be fed as inputs to the Marlin IPTV-ES Server or Device in test sequences. Note that how to feed the messages into Marlin IPTV-ES Servers or Devices depends on the specific implementation which is tested. After feeding a test message, output from the Marlin IPTV-ES Server or Device is obtained and compared with the corresponding test message indicated in each test sequence. Note that how to obtain an output from the Marlin IPTV-ES Server or Device depends on the specific implementation.

Assumed test procedure

Assumed test procedure using the test messages on Marlin IPTV-ES Device side is as follows:

1. Initiate a SAC at a Marlin IPTV-ES Device side.
2. Capture Device's SAC message and compare it with Device's corresponding SAC test message.
3. Feed Server's appropriate SAC test message to the Device and check the message is successfully processed.
4. Repeat the step 2 and 3 until the SAC is successfully done.

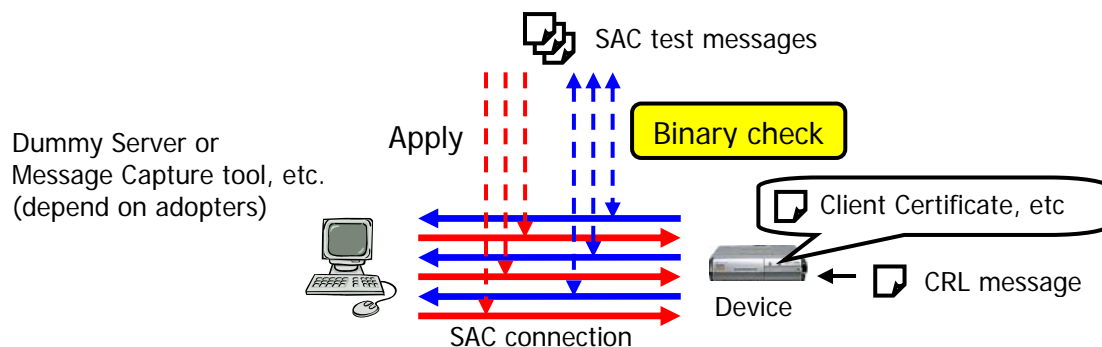


Figure A-1 Assumed test procedure on Marlin IPTV-ES Device side.

Assumed test procedure on Marlin IPTV-ES Server side is the same as on Marlin IPTV-ES Device side.

Prerequisite

In order for testing with the test messages, a tested Marlin IPTV-ES Server or Device is required the following functionalities:

- Use the indicated certificate and private key as its credential.

- Set the indicated CRL or DRL before a test sequence
- Adjust the clock to the indicated value before a test sequence.
- Use fixed values in some cryptographic calculations. The details are described in chapter 0.
- Use the indicated ContentKeyvalue and ExtractInfovalue in GetPermission Reply messages.
- Use the indicated Datetimevalue in GetTrustedTime Reply messages.
- Use the indicated Device Information on Devices.

Test Message

Overview

Test messages are SAC messages exchanged between Marlin IPTV-ES Servers and Devices. Test messages including wrong or invalid parameter values are not included in the Conformance Test Specification.

Two test messages are provided for parameters which may have variations. For example, 6 values of the Status parameter of the plain command message are defined in [IPTV-ES]. In this case two test messages, one of which contains *Success* (0000h) and the other contains *Message error* (8002h), are provided.

Fixed Values

The values specified in this section are used in the test messages.

Random Numbers

By definition, some SAC messages such as messages encrypted by a session key are not identical per generation by using (pseudo) randomized value. Test messages assume using fixed values instead in order to make binary comparison of a test message and an output message from Marlin IPTV-ES Server/Device. The following values are assumed to be fixed:

- 1 Sink Random in Challenge message defined in [IPTV-ES].
- 2 Source Random in Response & Challenge message defined in [IPTV-ES].
- 3 The parameter *u* of Operation 1, defined on page 36 in [IEEE1363-2000], for EC-DSA.
- 4 The party's own private key *s* of Input, defined on page 29 in [IEEE 1363-2000], for EC-DH.

Test messages with two sets of the fixed values are provided. The fixed values are shown in Table A-1.

Name	Value in hexadecimal
Sink Random (1)	EAF70A8BB240D5A5A1DEECA18A456B1E
Sink Random (2)	E1C27CC1E9A42A879E4474571F5756B6
Source Random (1)	D87EF0D2FA04C378E84770170B6BCC44
Source Random (2)	30CD21877EC40DE55BE00291126C6627
Device's fixed value for EC-DSA (1)	37623966E806F02BC4F1165B37723D196E9D11E9B7242A9B6C42C00F
Server's fixed value for EC-DSA (1)	4055AE329781A8A62369A232E1A5DD05B476DD6BFFD1B27E43C5268A
Device's fixed	29D482F1F2FE281BC262F54B3B43B4FD4A1E5EC8649AAF3F74

value for EC-DSA (2)	9BBC95
Server's fixed value for EC-DSA (2)	472D3F32AEC53629036198AC5B0C414E986D6EB97F92FB345600EE0B
Device's fixed value for EC-DH (1)	23AA180BB579923647D4BEC94EF96F8A9EC968E6E39016D69575DBC9
Server's fixed value for EC-DH (1)	503A377714506E5616C9500113E2986099BEAF1DF14D0D80DC078741
Device's fixed value for EC-DH (2)	3E457A1E366CB28C439B33674F363ABCFEE1AC6B8E2F87B062495F55
Server's fixed value for EC-DH (2)	C72BF867D9FE5C80A12B71DC18C98DCF66423AB896FA64255A2ACB7A

Table A-1 Fixed Random Numbers

Device Information

The Device Information value used in Get Permission Request messages is shown in Table A-2.

Name	Value in hexadecimal
VersionMajor	01
VersionMinor	00
Capabilities	00
Manufacturer	1FFF
ManufacturerModel	0000
ManufacturerModelVersionMajor	00
ManufacturerModelVersionMinor	00
Reserverd	000000

Table A-2 Fixed Device Information

Usage Rule Reference

The UsageRuleReference value used in Get Permission Request messages is shown in Table A-3.

Name	Value in hexadecimal
URR1-1	FFFF0000000100000000000000000000
URR1-2	FFFF0000000000000000000000000000
URR2-1	FFFF0000010100000000000000000000
URR2-2	FFFF0000010000000000000000000000
URR3-1	FFFF0000020100000000000000000000
URR3-2	FFFF0000020000000000000000000000
URR4-1	FFFF0000030100000000000000000000
URR4-2	FFFF0000030000000000000000000000
URR5-1	FFFF0000040100000000000000000000
URR5-2	FFFF0000040000000000000000000000
URR6-1	FFFF0000050100000000000000000000
URR6-2	FFFF0000050000000000000000000000

URR7-1	FFFF0000060100000000000000000000
URR7-2	FFFF0000060000000000000000000000
URR8-1	FFFF0000070100000000000000000000
URR8-2	FFFF0000070000000000000000000000
URR9-1	FFFF0000080100000000000000000000
URR9-2	FFFF0000080000000000000000000000
URR10-1	FFFF0000090100000000000000000000
URR10-2	FFFF0000090000000000000000000000
URR11-1	FFFF00000A0100000000000000000000
URR11-2	FFFF00000A0000000000000000000000
URR12-1	FFFF00000B0100000000000000000000
URR12-2	FFFF00000B0000000000000000000000
URR13-1	FFFF00000C0100000000000000000000
URR13-2	FFFF00000C0000000000000000000000
URR14-1	FFFF00000D0100000000000000000000
URR14-2	FFFF00000D0000000000000000000000
URR15-1	FFFF00000E0100000000000000000000
URR15-2	FFFF00000E0000000000000000000000
URR16-1	FFFF00000F0100000000000000000000
URR16-2	FFFF00000F0000000000000000000000
URR17-1	FFFF0000100100000000000000000000
URR17-2	FFFF0000100000000000000000000000

Table A-3 Fixed Usage Rule Reference

433

434 **Content Key**

435 The Content Key value used in Get Permission Reply messages is shown in Table A-
436 4.

Name	Value in hexadecimal
ContentKey	D16798F89B68E3A40FA3C8B301FCEBCD

Table A-4 Fixed Content Key

437

438

439 **Content Key ID**

440 The Contentn Key ID values used in Get Permission Reply messages are shown in
441 Table A-5.

Name	Value in hexadecimal
ContentKeyID1-1	FFFF000000011C200000000000000001
ContentKeyID1-2	FFFF000000021C200000000000000001
ContentKeyID1-3	FFFF0000000100000000000000000002
ContentKeyID1-4	FFFF0000000200000000000000000002
ContentKeyID2-1	FFFF000001011C200000000000000001
ContentKeyID2-2	FFFF000001021C200000000000000001
ContentKeyID3-1	FFFF000002011C200000000000000001
ContentKeyID3-2	FFFF000002021C200000000000000001
ContentKeyID4-1	FFFF000003011C200000000000000001
ContentKeyID4-2	FFFF000003021C200000000000000001
ContentKeyID5-1	FFFF000004011C200000000000000001
ContentKeyID5-2	FFFF000004021C200000000000000001
ContentKeyID6-1	FFFF000005011C200000000000000001
ContentKeyID6-2	FFFF000005021C200000000000000001
ContentKeyID7-1	FFFF000006011C200000000000000001

ContentKeyID7-2	FFFF000006021C200000000000000001
ContentKeyID8-1	FFFF000007011C200000000000000001
ContentKeyID8-2	FFFF000007021C200000000000000001
ContentKeyID9-1	FFFF000008011C200000000000000001
ContentKeyID9-2	FFFF000008021C200000000000000001
ContentKeyID10-1	FFFF000009011C200000000000000001
ContentKeyID10-2	FFFF000009021C200000000000000001
ContentKeyID11-1	FFFF00000A011C200000000000000001
ContentKeyID11-2	FFFF00000A021C200000000000000001
ContentKeyID12-1	FFFF00000B011C200000000000000001
ContentKeyID12-2	FFFF00000B021C200000000000000001
ContentKeyID13-1	FFFF00000C011C200000000000000001
ContentKeyID13-2	FFFF00000C021C200000000000000001
ContentKeyID14-1	FFFF00000D011C200000000000000001
ContentKeyID14-2	FFFF00000D021C200000000000000001
ContentKeyID15-1	FFFF00000E011C200000000000000001
ContentKeyID15-2	FFFF00000E021C200000000000000001
ContentKeyID16-1	FFFF00000F011C200000000000000001
ContentKeyID16-2	FFFF00000F021C200000000000000001
ContentKeyID17-1	FFFF000010011C200000000000000001
ContentKeyID17-2	FFFF000010021C200000000000000001

Table A-5 Fixed Content Key ID

ScrambleKey

The Scramble Key values used in ECM samples are shown in Table A-6.

Name	Value in hexadecimal
ScrambleKeyOdd	077F092139C2B80A0B43BC4B7D73279E
ScrambleKeyEven	5280D4E367D9A7B2DCC667D12C9A183D

Table A-6 Fixed Scramble Key

ExtractInfo

The ExtractInfo value used in Get Permission Reply messages is shown in Table A-7.

Name	Value in hexadecimal		
	NotBefore	NotAfter	RenderingObligation
ExtractInfo1	FFFFFFFF	0209A720	0000
ExtractInfo2	FFFFFFFF	0209A721	0000

Table A-7 Fixed ExtractInfo

Trusted Time

The Datetime values used in Get Trusted Time Reply messages and in ECM samples are shown in Table A-8.

Name	Value in hexadecimal
TrustedTime1	0136FAA0 (2008/10/01 00:00:00)
TrustedTime2	02800500 (2049/10/01 00:00:00)
TrustedTime3	02981A00 (2052/10/01 00:00:00)

Table A-8 Fixed Trusted Time

455
456
457

PrivateData in ECM

The PrivateData values used in ECM samples are shown in Table A-9.

Name	Value in hexadecimal
PrivateData1	0000000000000000192F00000
PrivateData2	0000000000000000292F00000

Table A-9 Fixed Scramble Key

458
459
460
461
462
463
464

ECM Sample

A set of ECM samples are provided together with associated SAC message samples. See the ECM data sheet of [SAMPLE] for the ECM samples and sequences which name starts with SEQ_5 in the Sequence data sheet of [SAMPLE] for the SAC message samples.