OIPF

Test Specification Overview

[V1.0.0] - [2010-11-15]

Open IPTV Forum

Open IPTV Forum

Postal address

Open IPTV Forum support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 43 83
Fax: +33 4 92 38 52 90

Internet
http://www.oipf.tv

Disclaimer

The Open IPTV Forum members accept no liability whatsoever for any use of this document.

Copyright Notification

Revision History

Version	Date	Description
V1.0.0	2010-11-15	First publication of Test Specification Overview for Release 1 v1.1

Contents

Index of Figures

1 OVERVIEW

1.1 Purpose

The Purpose of this document is to guide the reader in understanding the Test Specifications produced by the Open IPTV Forum.

The document explains the Specification Conformance Test Plan and the Solution Interoperability Test Plan and aims at verifying that all the client requirements are fulfilled during the development of the system. This also explains the preconditions, priority and results for any test specification defined.

The requirements for specifying the test cases are derived from the following sources:

- Open IPTV Forum Service and Platform Requirements version 1.1
- Open IPTV Forum Functional Architecture v1.2
- Open IPTV Forum Release 1 Solution Specification, version 1.1

1.2 Scope

This document describes the Test Specifications produced by the Open IPTV Forum as well as providing an introduction to the test cases.

2 REFERENCES

2.1 Normative References

Normative references refer to those documents that provide information that serves as an integral part of this specification and should be read and understood along with this work.

[RFC2616]	IETF, RFC 2616, “Hypertext Transfer Protocol -- HTTP/1.1”
[RFC2119]	IETF, RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels
[RFC2782]	IETF, RFC 2782, “A DNS RR for specifying the location of services (DNS SRV)”
[TVA-UNID]	ETSI, TS 102 822-3-2 V1.4.1 (2007-11), “Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems (“TV-Anytime”); Part 3: Metadata; Sub-part 2: System aspects in a uni-directional environment”
[TVA-BID]	ETSI, TS 102 822-6-1 V1.4.1 (2007-11), “Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network; Sub-part 1: Service and transport”
[DVBSI]	ETSI, TS 300 468 v1.8.1 (2007-10), “Digital Video Broadcasting: Specification for Service Information (SI) in DVB systems”
[BCG]	ETSI, TS 102 539 V1.2.1 (2008-04), “Digital Video Broadcasting: Carriage of Broadband Content Guide (BCG) information over Internet Protocol”
[SDNS]	DVB, Bluebook A086r8 , “Digital Video Broadcasting: Transport of MPEG-2 Based DVB Services over IP Based Networks”
[TS102034]	ETSI, TS 102 034 V1.3.1 (2007-10), “Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Networks”.
[CEA2014A]	CEA, CEA-2014-A, (Including the August 2008 Errata) “Web-based Protocol Framework for Remote User Interface on UPnP Networks and the Internet (Web4CE)”
[FLUTE]	IETF, RFC 3926, “FLUTE – File Delivery over Unidirectional Transport”
[TS102809]	ETSI, TS 102 809 V1.1.1, (2010-01), “Digital Video Broadcasting (DVB); Signalling and carriage of interactive applications and services in Hybrid broadcast/broadband environments”
[TR-069]	Broadband Forum, TR-069 Amendment 2, “CPE WAN Management Protocol v1.1”

2.2 Open IPTV Forum References

[REQS]	Open IPTV Forum, “Open IPTV Forum Service and Platform Requirements V1.1”, May 2008.
[ARCH]	Open IPTV Forum, “Functional Architecture - V1.2”, December 2008.
[SCT]	Open IPTV Forum, “Specification Conformance Test Plan for Release 1”, October 2010.
[SIT]	Open IPTV Forum, “Solution Interoperability Test Plan for Release 1”, October 2010.
[MEDIA]	Open IPTV Forum, “Release 1 Specification, Volume 2 - Media Formats V1.1”, October 2009
[META]	Open IPTV Forum, “Release 1 Specification, Volume 3 - Content Metadata V1.1”, October 2009
[PROT]	Open IPTV Forum, “Release 1 Specification, Volume 4 - Protocols V1.1”, October 2009
[DAE]	Open IPTV Forum, “Release 1 Specification, Volume 5 - Declarative Application Environment V1.1”, October 2009
[PAE]	Open IPTV Forum, “Release 1 Specification, Volume 6 - Procedural Application Environment V1.1”, October 2009
[CSP]	Open IPTV Forum, “Release 1 Specification, Volume 7 - Authentication, Content Protection and Service Protection V1.1”, October 2009

3 TERMINOLOGY AND CONVENTIONS

3.1 Conventions

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

All sections and appendixes, except “Scope”, are normative, unless they are explicitly indicated to be informative.

The following numbering scheme is used:

OIPF-<spec>-<vvv>-<number>

<spec>: { DAE | PAE | CSP | META | AVC | PROT }

<vvv>: Render | AppModel | Service (<spec> specific)

<number>: 3 digit sequential number per <vvv>

3.2 Definitions

Reference OITF	Accepted reference implementation of an OITF with decoding capability for all MPEG-2 TS and media formats. Includes diagnostic capability to determine media format(s) of consumed content.

3.3 Abbreviations

APDU	Application Protocol Data Unit
API	Application Programming Interface
AS	Application Server
ASM	Authentication and Session Management
ASP	Active Server Pages
A/V	Audio/Video
A/V Codec	Audio and Video Codec
BMP	Baseline Managed Profile
CDC	Connected Device Configuration
CDF	Content Delivery Function
CDN	Content Delivery Network
CI	Common Interface
CoD	Content on Demand
CSP	Content and Service Protection
CSPIF	CSP Interface
CSPG	Content and Service Protection Gateway
CSPG-CI+	CSPG-CI+ based
CSPG-DTCP	CSPG-DTCP-IP based
CVM	Customized Virtual Management
DAE	Declarative Application Environment
DB	Database
DRM	Digital Rights Management

DTCP	Digital Transmission Content Protection
EMP	Enhanced Managed Profile
FE	Functional Entity
FP	Foundation Profile
GEM	Globally Executable MHP
HTTP	Hyper text Transfer Protocol
IGMP	Internet Group Management Protocol
IG	IMS Gateway
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IUT	Implementation Under Test
MHP	Multimedia Home Platform
nPVR	Network Personal Video Recorder
OIP	Open Internet Profile
OIPF	Open IPTV Forum
PAE	Procedural Application Environment
PBP	Personal Basis Profile
PCO	Point of Control and Observation
PDU	Protocol Data Units
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SAA	Service Access Authentication
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRS	Software Requirement Specification
SUT	System Under Test
TCI	TTCN-3 Control Interface
TRI	TTCN-3 Runtime Interface
TTCN-3	Testing and Test Control Notation Version-3
UDP	User Datagram Protocol
W3C	World Wide Web consortium

4 INTRODUCTION

This document serves as the template for writing the test cases for the Specification Conformance Test Plan and the Solution Interoperability Test Plan. Later sections of this document describe the test methods, the test environment and the tables of test specifications. The detailed representation of the test environment is explained using figures in each section.

The test method contains a detailed explanation of the techniques and testing method for each aspect of the IPTV Solution Specification.

The test environment describes the environment which will be used to implement the test method along with the role of each component.

Specification table has various fields which enables the tester to develop test cases.

4.1 Structure of the Test Specifications

The Open IPTV Forum Test Specifications comprise three parts as described in the following sub-sections.

The Test Specification Overview, this document, describes the testing methodologies, test environment and introduces the test cases that are found in the Specification Conformance Test Plan and the Solution Interoperability Test Plan.

The Specification Conformance Test Plan contains test cases which verify the compliance of an implementation towards the OIPF Solution Specifications, [MEDIA], [META], [PROT], [DAE], [PAE] and [CSP].

The Solution Interoperability Test Plan contains test cases to verify the interoperability of an implementation against reference devices. The implementation (which is the device under test) and the reference devices form a complete end-to-end IPTV delivery system which is compliant to the OIPF specifications.

4.1.1 Test Specification Overview

The test specification overview table shall contain the test specification ID, the test object, the test specification description, the test cases and the precondition. The detailed test specification overview table is as following:

Test Specification ID	A unique identification number to identify the particular service, functions, or APIs under test.
Test Specification Version	The version number for the test specification. This value will be updated if the test case changes.
Test Object(s)	Name of the entity or entities under test.
Test Specification Description	Basic description of the test case.
Specification Section(s)	A reference to the particular section(s) of the specification documents. This will be help in consulting the details of the specification document form the basis of the test.
Test Cases	Lists of all the test items required for this Test Specification ID. The test items are the checklists to verify the functionalities of the test objects including the normal functions and exception handlings. These are further defined in the Specification Conformance Test Plan and Solution Interoperability Test Plan.
Precondition	Preconditions necessary to run the tests on the Test Object. This will also give information about the dependencies of the particular service.
Priority	Priority or relative importance of the test specification, specified as either **Mandatory** or **Optional**
Remark	Any additional information that is necessary such as modification of the test environment, specific test data requirement, etc.

4.1.2 Specification Conformance Test Plan

The format for the Test Specification ID shall be

OIPF-{AVC|META|PROT|DAE|PAE|CSP}-<feature>-<test number>

4.1.3 Solution Interoperability Test Plan

The format for the Test Specification ID shall be

OIPF-SIT-<feature>-<test number>

5 SPECIFICATION CONFORMANCE TEST

Specification Conformance Test is the activity of providing testing for the specifications of OIPF. The specifications to be tested are as follows:

1. Media Formats
2. Metadata
3. Protocols
4. Declarative Application Environment
5. Procedural Application Environment
6. Authentication, Content Protection and Service Protection

In this section, the test method and the test environment for each specification will be described and the features to be tested will be listed for each specification.

5.1 Media Formats

5.1.1 Prerequisites

None

5.1.2 Test Method

5.1.2.1 Consumer side testing

This involves the testing of functions that consume the A/V content. It tests the capability to access and consume various media formats and profiles as specified in [MEDIA]. The OITF consumes the content and it is target device.

The testing will be performed using a browser-based DAE environment, running on the target, with each test case represented by a DAE A/V application which refers to media content. A/V applications and content resides in A/V DB.

The A/V application will have an A/V plug in object for e.g. CEA-2014-A A/V streaming object or video/broadcast object. This object has information on the content location, media content and content delivery mechanism (for e.g. progressive download of images, streaming audio clip, downloading and viewing encrypted video).

Using a starting web-page (which the OITF is pre-configured to obtain from the test manager), the target sends a request for an A/V application to the A/V server. A/V server sends the A/V application to the target. The target sends the corresponding content request to the Stream Generator (acting as the Content Delivery FE) by accessing the A/V application. The stream is rendered on the target & analyzed for correctness.

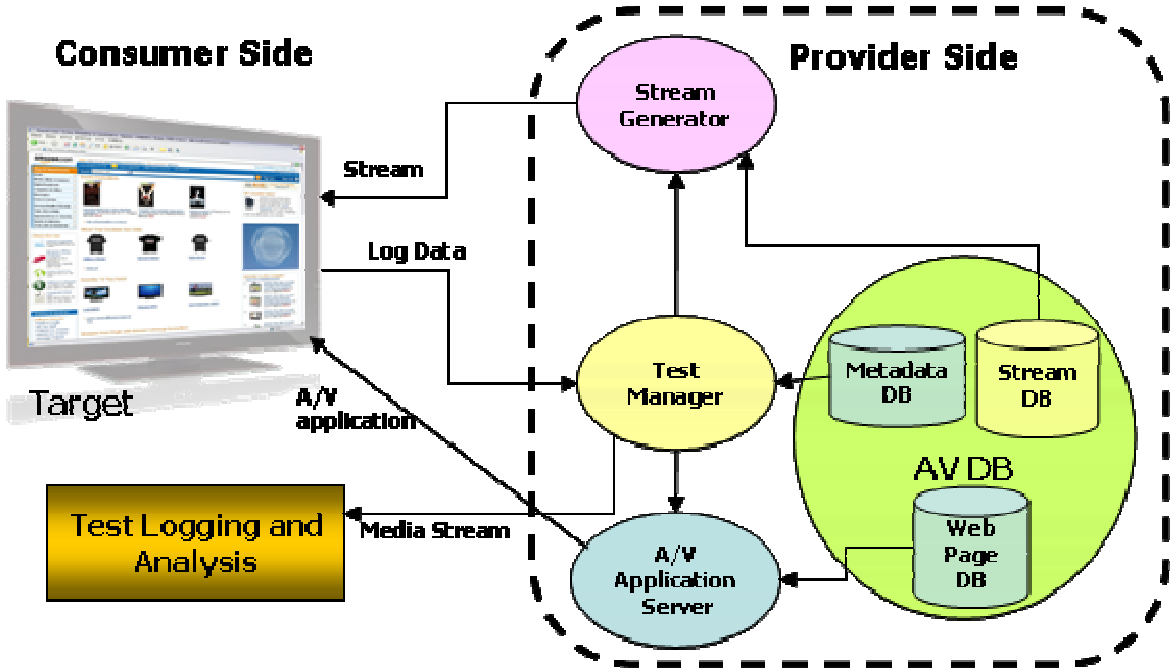

Figure 1 - Test Environment for Media Format Consumer Side Testing

5.1.2.2 Provider side testing

This pertains to the testing of the Multicast Content Delivery Function (MCDF) that streams content to the consumer. The transport protocol and CSP-G issues are not in the scope of Media Format conformance testing.

As shown in Figure 2, the MCDF (encoder) is the functional entity under test (Test Object). Content files will be conformant to [MEDIA]. Input to the test object will be content files present in the A/V DB e.g. MPEG, AAC, wav. The test manager will configure the MCDF to generate streams with the desired characteristics from a given set of content files in the A/V DB as per the test case (e.g. MPEG-2 TS request to the MCDF). Output from the test object is a transport stream (e.g. MPEG TS with desired structure) generated from the content files. A Reference OITF device will work as a client to request content streams from the test object as per the test case. Content streams delivered to the client will be logged and analyzed by the Test logger and Analysis module. Passive Analysis of the stream will be performed. The OITF shall be used to render the streams to verify overall compatibility of transport streams with the format specifications. Transport streams will be checked for proper syntax & related consistency checks. A compliance registry will keep track of the Test Object's claimed profile support and the Test Object's actual profile support.

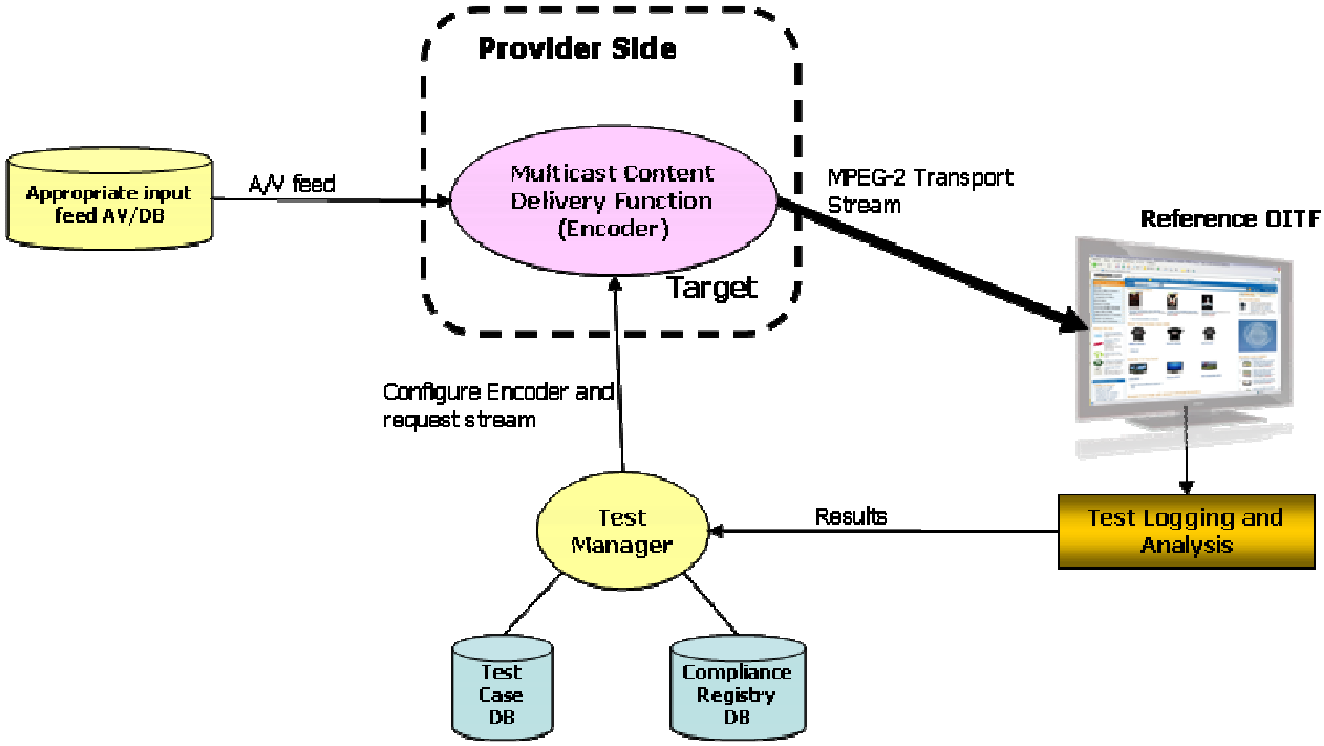

Figure 2 - Test Environment for Media Format Provider Side Testing

5.1.3 Test Environment

The test environments for Media Formats are displayed in Figure 1 and Figure 2. Each component in the environment is described below.

- Target:

  This is the entity at which the delivery or reception of the audio/ video content formats are tested.

- Stream Generator:

  Creates the test streams, e.g. MPEG-2 transport stream with a Conditional Access Table. After making a test stream, it sends the stream to the target. It can be configured by Test Manager to deliver the appropriate stream to the test target (i.e. the OITF).

- Test Manager:

  This entity controls the overall testing of the Audio/Video Content. It manages the requests and responses from various modules of the test environment and commands or configures the modules according to the test case under execution.

- Test Logging and Analysis:

  This entity is responsible for maintaining the test log. The Test Management interface will be used to record test management information generated by the test case. The decoding of streams is also logged by this entity. The analysis module can also perform the analysis of the stream delivered to the OITF.

- Audio/Video Application Server:

  This entity receives the request from the Test Manager for the Scheduled Content and fetches the appropriate application from the database.

- Audio/Video Content Database:

  This entity contains various applications corresponding to the different Scheduled Content requests. These applications link to the media contents (e.g. MPEG-2 content) in various formats and profiles (as are supported by the specifications), which are also stored in the database.

Note: The Test Logging and Analysis module can capture network traffic directed at the target upon the Test Manager's command.

5.1.4 Test Specification for Media Formats

5.1.4.1 Formats supported on provider side

Test Specification ID	OIPF-AVC-MN-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object supports MPEG-2 TS for Managed Networks.
Specification Section(s)	[MEDIA] §4.3, [MEDIA] §10.1
Test Cases	• Check the support of MPEG-2 TS on 25Hz system • Check the support of MPEG-2 TS on 30Hz system
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-AVC-TS-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object supports MPEG-2 TS
Specification Section(s)	[MEDIA] §4.1, [MEDIA] §10.1
Test Cases	• Check support of MPEG-2 TS on 25Hz system • Check support of MPEG-2 TS on 30Hz system • Check support of MPEG-2 TS on 25Hz system with PSI Carriage • Check support of MPEG-2 TS on 25Hz system with DVB-SI Carriage • Check support of MPEG-2 TS on 30Hz system with PSI Carriage • Check support of MPEG-2 TS on 30Hz system with DVB-SI Carriage • Check SD content Maximum Bit Rate on 25 Hz system • Check SD content Maximum Bit Rate on 30 Hz system • Check HD content Maximum Bit Rate on 25 Hz system • Check HD content Maximum Bit Rate on 30 Hz system
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

Test Specification ID	OIPF-AVC-AVCV-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object supports H.264/AVC encoding,
Specification Section(s)	[MEDIA] § 5, [MEDIA] §5.13, [MEDIA] §10.1, [MEDIA] §5.1.2.1, [MEDIA] §5.1.1.1, [MEDIA] §10.2.2.1, [MEDIA] §10.2.2.2, [MEDIA] §5.1.2.2, [MEDIA] §5.1.1.2
Test Cases	• Check support of H.264/AVC encoding for SD content on 25Hz system • Check support of H.264/AVC encoding for SD content on 30Hz system • Check support of H.264/AVC encoding for HD content on 25Hz system • Check support of H.264/AVC encoding for HD content on 30Hz system

Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

Test Specification ID	OIPF-AVC-MP2V-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object supports MPEG-2 encoding,
Specification Section(s)	[MEDIA] §5, [MEDIA] §5.13, [MEDIA] §10.1, [MEDIA] §5.1.2.1, [MEDIA] §5.1.1.1, [MEDIA] §10.2.2.1, [MEDIA] §10.2.2.2, [MEDIA] §5.1.2.2, [MEDIA] §5.1.1.2
Test Cases	• Check support of MPEG-2 encoding for SD content on 25Hz system • Check support of MPEG-2 encoding for HD content on 25Hz system
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

Test Specification ID	OIPF-AVC-CPTN-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object supports creation of subtitle information.
Specification Section(s)	[MEDIA] Sections 6, 6.1
Test Cases	• Check support of subtitling based on DVB specification. • Check support of subtitling based on CEA-708-C specification.
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

Test Specification ID	OIPF-AVC-TTXT-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object support Teletext information in EBU format.
Specification Section(s)	[MEDIA] §7, [MEDIA] §7.1
Test Cases	• Check support of Teletext in EBU format.
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

Test Specification ID	OIPF-AVC-AACAA-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object support MPEG-4 HE-AAC audio encoding.
Specification Section(s)	[MEDIA] §8, [MEDIA] §8.1.1, [MEDIA] §10.1
Test Cases	• Check support of MPEG-4 HE-AAC audio encoding.
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-AVC-ACA3A-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object support AC3 audio encoding.
Specification Section(s)	[MEDIA] Sections 8, 8.1.2, 10.2.3.1
Test Cases	• Check support of AC3 audio encoding.
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

Test Specification ID	OIPF-AVC-MP1L2A-001
Test Specification Version	1.0.0
Test Object(s)	Multicast Content Delivery Function (Encoder)
Test Specification Description	Verify the Test Object support MPEG-1 Layer II audio encoding.
Specification Section(s)	[MEDIA] §8, [MEDIA] §8.1.3, [MEDIA] §10.2.3.2
Test Cases	• Check support of MPEG-1 Layer II audio encoding.
Preconditions	• The Test Object is configured by the Test Manager. • Test Object should have access to appropriate input feed. • Reference OITF should be connected to the test network with Target Object.
Priority	Optional
Remark	

5.1.4.2 Format supported on OITF

5.1.4.2.1 Graphic Formats

Test Specification ID	OIPF-AVC-IMG-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to render JPEG formatted graphic images
Specification Section(s)	[MEDIA] §9.1.1
Test Cases	• Perform the necessary test cases according to the claimed media support of the Test Object o For all implementations

	o For 25Hz implementations o For 30Hz implementations o For implementations supporting high definition content
Preconditions	None
Priority	Mandatory
Remark	All test cases shall render the graphic image in order to pass

Test Specification ID	OIPF-AVC-IMG-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to render GIF formatted graphic images
Specification Section(s)	[MEDIA] §9.1.2
Test Cases	• Perform the necessary test cases according to the claimed media support of the Test Object o For all implementations o For 25Hz implementations o For 30Hz implementations o For implementations supporting high definition content
Preconditions	None
Priority	Mandatory
Remark	All test cases shall render the graphic image in order to pass

Test Specification ID	OIPF-AVC-IMG-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to render PNG formatted graphic images
Specification Section(s)	[MEDIA] §9.1.3
Test Cases	• Perform the necessary test cases according to the claimed media support of the Test Object o For all implementations o For 25Hz implementations o For 30Hz implementations o For implementations supporting high definition content
Preconditions	None
Priority	Mandatory
Remark	All test cases shall render the graphic image in order to pass

5.1.4.2.2 Video Tests

Test Specification ID	OIPF-AVC-VID-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to receive and present standard definition video content. Reference content streams contain PSI and DVB-SI information that is included in the test cases.
Specification Section(s)	[MEDIA] §5.1.2
Test Cases	• H.264/AVC video in an MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video in an MPEG-2 transport stream with PSI and DVB-SI for 30Hz implementations • MPEG-2 video in an MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations

	• H.264/AVC video in a time-stamped MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video in a time-stamped MPEG-2 transport stream with PSI and DVB-SI for 30Hz implementations • MPEG-2 video in a time-stamped MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video using MPEG-4 file format for 25Hz implementations • H.264/AVC video using MPEG-4 file format for 30Hz implementations
Preconditions	None
Priority	
Remark	All test cases shall present the video content in order to pass

Test Specification ID	OIPF-AVC-VID-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to receive and present high definition video content. Reference content streams contain PSI and DVB-SI information that is included in the test cases.
Specification Section(s)	[MEDIA] §5.1.1
Test Cases	• H.264/AVC video in an MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video in an MPEG-2 transport stream with PSI and DVB-SI for 30Hz implementations • MPEG-2 video in an MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video in a time-stamped MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video in a time-stamped MPEG-2 transport stream with PSI and DVB-SI for 30Hz implementations • MPEG-2 video in a time-stamped MPEG-2 transport stream with PSI and DVB-SI for 25Hz implementations • H.264/AVC video using MPEG-4 file format for 25Hz implementations • H.264/AVC video using MPEG-4 file format for 30Hz implementations
Preconditions	Standard definition video tests appropriate to implementation shall be executed prior to high definition tests
Priority	
Remark	Only required for implementations Test Object claiming high definition video capability. All test cases shall present the video content in order to pass

Test Specification ID	OIPF-AVC-VID-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to receive and present supplemental information such as teletext and subtitling that delivered with the video content in the MPEG-2 transport stream
Specification Section(s)	[MEDIA] §6, [MEDIA] §7
Test Cases	• Decoding and presentation of DVB formatted subtitles for 25Hz implementations • Decoding an presentation of DVB formatted subtitles for 30Hz implementations • Decoding an presentation of CEA-708 formatted subtitles for 25Hz implementations

	• Decoding an presentation of CEA-708 formatted subtitles for 30Hz implementations • Presentation of Teletext information service from a delivered transport stream
Preconditions	None
Priority	Optional
Remark	All test cases shall present the video content in order to pass

5.1.4.2.3 Audio Tests

Test Specification ID	OIPF-AVC-AUD-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to receive and present streamed audio
Specification Section(s)	[MEDIA] §8
Test Cases	• Playout of audio coded using the MPEG-4 AAC profile from an MPEG-2 transport stream. • Playout of audio coded using the MPEG-4 HE-AAC profile from an MPEG-2 transport stream. • Playout of audio coded as AC3 from an MPEG-2 transport stream. • Playout of audio coded as MPEG-1 Layer 2 from an MPEG-2 transport stream.
Preconditions	None
Priority	Mandatory
Remark	All test cases shall present the audio content in order to pass

Test Specification ID	OIPF-AVC-AUD-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Verify the OITF ability to receive and present memory based audio
Specification Section(s)	[MEDIA] §8
Test Cases	• Playout of audio coded using the MPEG-4 AAC profile from a file loaded into memory on the Test Object. • Playout of audio coded using the MP3 AAC profile from a file loaded into memory on the Test Object. • Playout of audio coded using the MP3X AAC profile from a file loaded into memory on the Test Object. • Playout of audio coded using the WAV AAC profile from a file loaded into memory on the Test Object.
Preconditions	None
Priority	Mandatory
Remark	All test cases shall present the audio content in order to pass

5.2 Metadata

The prerequisite for this section is the carriage mechanism of the BCG metadata formats (for Program & Channel information) and Service Discovery & Selection record formats , and the metadata transmission protocols - HTTP (for Unicast delivery) and DVBSTP (for Multicast delivery).

For testing access to BCG metadata for programme and channel information, the DAE Metadata API shall be tested under the DAE conformance testing. This involves the testing of DAE object extensions.

The ability to gather and access the metadata information from various metadata records (as per the supported schema and their extensions) will be tested under this section.

Metadata can be in two formats as listed below. The metadata records generated according to the base standards along with the OIPF extensions to these formats will be tested:

- Service Discovery and Selection (SD&S)

  Required for service provider discovery, service discovery and selection. Extensions have been added by OIPF, to allow metadata accessibility in CE-HTML format. Metadata records will be generated as per the SD&S schema and are checked for the support of various elements given in the schema.

- Broadband Content Guide (BCG)

  Carries program and channel information. The prime testing focus in this section is BCG format and extensions as given in [META]. In addition, various supported metadata records will be generated as per the BCG schema and will be checked.

In addition the following aspects of metadata control and delivery are applicable

- Metadata Control:

  Covers linking between SD&S and BCG metadata. Metadata will be generated in SD&S and BCG formats which will be linked with each other. At the target, an EPG will be constructed for each service in the SD&S records and using the link information to the BCG metadata for the service .

- Metadata delivery:

  Pertains to the carriage of metadata. Depending on the metadata formats the content will be delivered over the network using one of the defined mechanisms - HTTP or DVBSTP.

5.2.1 Prerequisites

None

5.2.2 Test Method

To test the metadata specifications, a Metadata server is used as described below. This server accesses metadata from the metadata database that contains metadata defined as per the OIPF extensions to both the SD&S records and BCG metadata content formats as well as CE-HTML pages. These extensions allow metadata as to be accessed as CE-HTML pages. To be conformant with the OIPF specifications, an implementation must support the metadata delivery as CE-HTML pages and for this, it must also support extensions as specified in [META] for SD&S records and BCG metadata..

The Metadata server accesses metadata from a database as described above and delivers it using unicast or multicast methods (e.g. HTTP or DVBSTP) supporting various modes such as push or pull.

The OITF (target) shall be configured to contact the Metadata server, which acts as the service provider discovery entry point (either using DHCP configuration or through data pre-configured on the IG or some other method as described in the OIPF specifications). At this point it can send requests to the metadata server for accessing SD&S records for service provider, service and content guide etc.

The test driver at the target OITF shall require the OITF to select the appropriate service provider, service and content information and hence, obtain the necessary information from the metadata server as SD&S, BCG records (with OIPF extension elements). From the information received, the target shall make a presentation of metadata from which it shall be observed whether metadata information required for the conformance has been obtained from the extended metadata format.

For BCG metadata, DAE applications can be make use of various objects such as “Channel List” or “video/broadcast” in which the metadata information can be extracted from the content stream or the network using the methods and properties of these objects as defined by the Metadata API of [DAE]. A script inside the DAE application can check for the correctness and availability of the information received from the metadata server or the content stream depending on the test case. Testing of metadata specifications would therefore also imply the testing of objects and methods of the Metadata API as described above.

The tester at the target will be able to log the output of the test case (i.e. the metadata information it could access).

5.2.3 Test Environment

The test environment for Metadata is displayed in Figure 3, and each component in the environment is described below.

- Metadata server:

  It delivers all required Service Discovery and Selection (SD&S) records and EPG data for Broadcast Content Guides (BCG) via HTTP and multicast delivery mechanisms. It will be used to provide metadata information to the target in the requested format for the current test object and test case.

- Test Manager:

  It will configure the metadata server to behave as service provider discovery /service discovery /application server FE in the desired delivery mode (unicast/multicast) to provide for the user with different metadata information as per the test case. It will co-ordinate with test driver for each test case and will configure the metadata server accordingly.

- Metadata database:

  It consists of metadata provided as CE-HTML pages and XML documents as per the schema in defined in [META], [TS102034] and [BCG].

- Test Driver:

  It is the application at the target that controls the metadata requests generated from the target by guiding the tester appropriately for each test case. It will co-ordinate with the Test Manager for each test case. To this end, it may also be required to configure the entities such as the IG at the client end. Additionally, it will log the test result output observed at the target and send it to the Test Manager for reporting purposes. The output will be the information presented to the user in the manner as required by the test case.

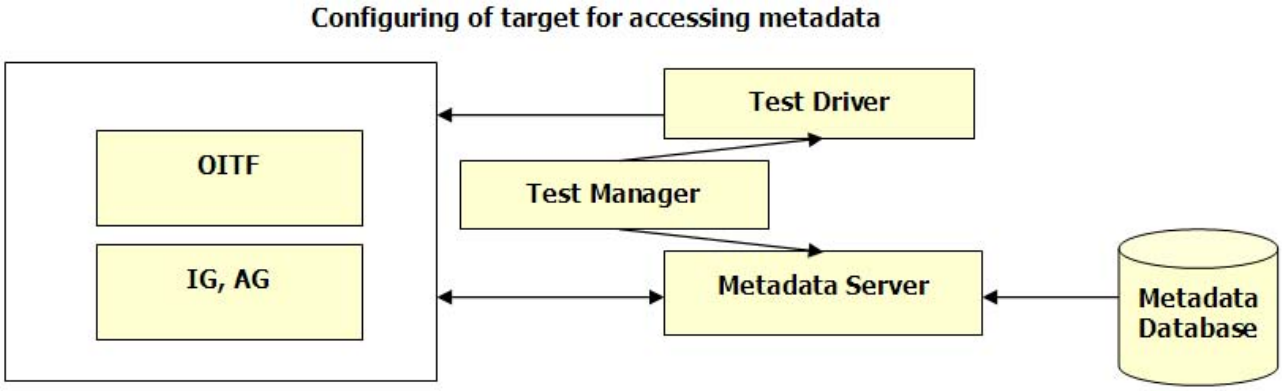

Figure 3 - Test Environment for Metadata

5.2.4 Test Specification for Metadata

The following information provides a complete overview of the test cases that need to be passed for DVB SD&S and BCG validation (metadata content, metadata control and delivery). However, the test cases provided in the SCT document focus only on the specific SD&S and BCG extensions defined by the OIPF.

5.2.4.1 Metadata Content

5.2.4.1.1 Schema Extension and Validation

Test Specification ID	OIPF-META-MC_SEV-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Schema extension and validation
Specification Section(s)	[META] §3.1
Test Cases	• Check that OITF XML schema is obtained by extending SD&S and BCG schemas. • Check that the extension rule adopted is the “forward compatibility” constraints specified for extending BCG Schema [TVA-UNID]. • Check that content that is purported to conform to the extension specified in this specification must pass a validation test using any widely-accepted XSD validation engine.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2 SD&S (Service Discovery and Selection)

5.2.4.1.2.1 Service Discovery and Selection as described in [SDNS]

5.2.4.1.2.1.1 Service Identification

Test Specification ID	OIPF-META-MC_SDNS_SI-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection – Service Identification – Service Provider (SP)
Specification Section(s)	[META] §3.2 [TS102034] §5.2.1.1
Test Cases	• Check that a SP shall be identified uniquely by the name of the DNS Domain it has registered and controls. • The organizations administrating the Internet DNS domain names shall be used as a globally unique registration mechanism that allows these textual SP identifiers to be globally unique names.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNS_SI-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection – Service Identification – Service name or ServiceID
Specification Section(s)	[META] §3.2 [TS102034] §5.2.1.2
Test Cases	• Each service shall be assigned one textual identifier that takes the form of an Internet DNS host name under the DNS domain that the SP controls. • Thus a service can be uniquely identified by a concatenation of a service name (managed uniquely by the SP) and the SP's domain name. • There are two basic mechanisms for uniquely identifying a service (Either form can be used for identifying a service globally and uniquely):

	o the triplet of numeric identifiers: original_network_id, transport_stream_id and service_id as defined in DVB SI; o a textual service identifier, as defined above.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.1.2 Fragmentation of SD&S Records

Test Specification ID	OIPF-META-MC_SDNS_FRAG-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Fragmentation of SD&S Records – SD&S Information data types
Specification Section(s)	[META] §3.2 [TS102034] §5.2.2.1
Test Cases	• Check that the following different information types are specified: o SD&S information relating to a SP. o four types of SD&S information relating to the service offering of a SP. o Broadband Content Guide Discovery record. o Regionalisation Discovery record to provide for local services. (N/A) o Firmware Announcement Information to allow for upgrade or changes to HNED firmware. (N/A) • A SP offering can be made up of Live Media Broadcast services ("TS Full SI" or "TS Optional SI" records) or CoD (via the BCG Discovery record). • The SP can also reference services provided by another SP or define a package if it chooses to group several services and present them as a single entity. • These different types of SD&S information shall be identified by an 8-bit value called payload ID.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNS_FRAG-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Fragmentation of SD&S Records
Specification Section(s)	[META] §3.2 [TS102034] §5.2.2.2
Test Cases	• Check that segments shall be supported to allow an SD&S record to be managed as a collection of smaller units. Segments are defined in the context of a single type of SD&S information, i.e. segments are defined for a declared payload ID. • Check that each segment shall be assigned a segment ID to identify a segment of data for the declared SD&S data type (payload ID). • Check that the segment ID is a 16-bit value. • Check that a segment is a well formed and valid XML record. • Check that an 8-bit value is used to define the current version of a segment, this version shall be keyed on payload ID together with segment ID. Thus when the data within a segment changes, its version number called segment version shall be incremented. The segment versions of the unchanged

	segments do not need to change. • Check that the segment version is modulo 256, and wraps round.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNS_FRAG-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Fragmentation of SD&S Records – Maximum Cycle time
Specification Section(s)	[META] §3.2 [TS102034] §5.2.2.3
Test Cases	• The length of time required to transmit all the segments making up the full set of SD&S Information for a SP is called the Cycle Time. Check that the Maximum Cycle Time shall be set to 30 s.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.1.3 Steps in service discovery

Test Specification ID	OIPF-META-MC_SISD-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Steps in service discovery
Specification Section(s)	[META] §3.2 [TS102034] §5.2.3
Test Cases	• Check that the service discovery process begins with the discovery of SPs offering DVB-IPTV services over the IP network and continues with the discovery of available services from each SP. • Check that the service discovery process shall bootstrap itself by determining the entry point(s) of the discovery information. • Check that the discovery of SPs offering DVB-IPTV services is done via the acquisition of the SP Discovery Information. SPs will publish their offering via the service discovery information.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.1.4 Service discovery entry points

Test Specification ID	OIPF-META-MC_SDEP-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery entry points
Specification Section(s)	[META] §3.2 [TS102034] §5.2.4
Test Cases	• Check that the service discovery process is bootstrap itself by determining the entry point(s) of the discovery information. The SD&S entry points must be one of the following:

	o A well known multicast address registered with IANA that is 224.0.23.14 (DvbServDisc) o A list of SD&S entry points addresses may be acquired via DNS according to the service location [RFC2782]. o When the HNED connects to the network to request its own address (e.g. during DHCP) it may be provided with domain names via DHCP option 15.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.1.5 Service Provider discovery information

Test Specification ID	OIPF-META-MC_SPDI-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service Provider discovery information
Specification Section(s)	[META] §3.2 [TS102034] §5.2.5
Test Cases	• Check that SP Discovery Record carries in a record containing the information listed in [TS102034] table 2. • Check that The SP Discovery Information may be multicast (push model) or retrieved on request (pull model). o One or both models shall be supported by the server. o Both models shall be supported by the client.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.1.6 DVB-IPTV service discovery information

Test Specification ID	OIPF-META-MC_SDI-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery information - DVB-IPTV Offering Record
Specification Section(s)	[META] §3.2 [TS102034] §5.2.6.1
Test Cases	• Check that DVB-IPTV Offering record contains at least the fields described in [META] Table 3, followed by fields relating to the actual SP offering. • Check that a SP offering could be made up of: • Live Media Broadcast services ("TS Full SI" or "TS Optional SI" records) • CoD (via the BCG Discovery record) • services provided by another SP.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDI-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery

	information – Broadcast discovery record TS Full SI
Specification Section(s)	[META] §3.2 [TS102034] §5.2.6.2.1
Test Cases	• Check that Broadcast discovery record TS Full SI provides all the necessary information to find available live media broadcast services which have embedded SI. • Check that Broadcast discovery record provides information on individual services is afterwards acquired from the transport stream itself through classical use of service information as defined in DVB-SI. • Check that this record implements the Broadcast Discovery Information (“TS Full SI”) and the linked Service(s) Location and Service(s) Description Location, and by inheritance the DVB-IPTV Offering. • Check that this record includes all attributes in table 3, and in addition contains the fields of table 4 in [TS102034] Section 5.2.6.2.1.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDI-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery information – Broadcast discovery record TS Optional SI
Specification Section(s)	[META] §3.2 [TS102034] §5.2.6.2.2
Test Cases	• Check that Broadcast discovery TS Optional SI record provides all the necessary information to create a list of available services with sufficient information for the user to make a choice and gives the necessary information on how to access the service. • Check that the "TS Optional SI" Broadcast Discovery Information implements the Broadcast Discovery Information (“TS Optional SI”) and the linked Service(s) Location and Service Description Location, and by inheritance the DVB-IPTV Offering. • Check that this record includes all attributes in [META] table 3, and in addition contains the fields of table 5 in [TS102034] Section 5.2.6.2.2.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	By default, the IP Service Discovery Information shall take precedence over the DVB SI tables when present in the transport stream.

Test Specification ID	OIPF-META-MC_SDI-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery information – Service from Other Services Providers record
Specification Section(s)	[META] §3.2 [TS102034] §5.2.6.4
Test Cases	• Check that a SP can reference individual services or a complete offering provided by another SP. • Check that supplying its textual service identifier references a service. • Check that supplying the SP's DNS domain name without a service list references an entire SP's offering. • Check that discovery information relating to a service, or SP, such as the location of the service will need to be acquired directly from the SP

	providing the service, and is not "pointed to" from this record. • Check that the "Services From other SPs" Record implements the Services From other SPs and linked Service ID, and by inheritance the DVB-IPTV Offering, • Check that the record includes all attributes in [TS102034] table 3, and in addition contains the following fields.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDI-005
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery information –Package discovery record
Specification Section(s)	[META] §3.2 [TS102034] §5.2.6.5
Test Cases	• Check that the Package Discovery Record implements the Package Discovery Information, linked Service ID and Description Location, and by inheritance the DVB-IPTV Offering. • Check that the record includes all attributes in table 3, and in addition contains the fields of table 8 in [TS102034] Section 5.2.6.5. • Check that a service may belong to more than one package. • Check that a service does not have to be part of any package. • Check that The package discovery information does not enable the discovery of new services. • Check that Discovery information relating to a service, or SP, such as the location of the service is needed to be acquired directly from the SP providing the service, and is not "pointed to" from this record. • Check that the Visible attribute of the referenced package is ignored when a package includes another package (using the PackageReference element).
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDI-006
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –Service discovery information –Broadband Content Guide record
Specification Section(s)	[META] §3.2 [TS102034] §5.2.6.6 [BCG]
Test Cases	• Check that the Broadband Content Guide Record provides a means to discover the locations of guides listing the content that is available, either live (e.g. through a Broadcast Offering) or via CoD or via CDSs. • Check that a provider discovered through this offers a service as described in [BCG]. • Check that the record includes all fields of table 9 in [BCG] Section 5.2.6.6. • Check that in the case where there are several references to BCGs in the ServiceList or SingleService, the preferred BCG is optionally signalled using a boolean attribute "preferred".
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory

Remark	

5.2.4.1.2.2 OIPF Service Discovery and Selection Extensions

Test Specification ID	OIPF-META-MC_SDNSE_SDE-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –OITF Service Discovery and Selection Extensions – Service Discovery Extensions - Bandwidth Renegotiation
Specification Section(s)	[META] §3.2.2.3
Test Cases	• Check that the MaxBitrate element in IPService Record of SD&S extended by OITF is mandatory in case of managed network. • Check that the MaxBitrate is used during session initiation or session modification for scheduled services to ensure that the necessary bandwidth is available in the network. • Check that the TimeToRenegotiate element that when present is used to determine when down-sizing of the reserved bandwidth for the content session is performed. • Check that When the TimeToRenegotiate element is provided with the IPService record then: o The MaxBitrate element is provided. o If the MaxBitrate of the new service is greater than the reserved bandwidth, network bandwidth reservation using the MaxBitrate of the new service is occur immediately to ensure sufficient bandwidth is made available for the new service. o If the MaxBitrate of the new service is equal to the reserved bandwidth, network bandwidth reservation procedures are not performed as sufficient bandwidth is already available for the new service. o If the MaxBitrate of the new service is less than the reserved bandwidth, network bandwidth reservation using the MaxBitrate of the new service is occur after the period (in seconds) provided by the TimeToRenegotiate element of the new service.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNSE_SDE-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –OITF Service Discovery and Selection Extensions – Service Discovery Extensions - Purchasing Broadcast Services
Specification Section(s)	[META] §3.2.2.4
Test Cases	• Check the optional PurchaseItem element which allows to include DRM control information in the Broadcast Discovery Record extended by OITF is available.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNSE_SDE-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –OITF Service Discovery and Selection Extensions – Service Discovery Extensions - Container Format Indication
Specification Section(s)	[META] §3.2.2.5
Test Cases	• Check the optional FileFormat element is available in the IPService Record of [SDNS] extended by OITF. • Check that this element provides a means to indicate file format.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.3 Application Announcement & Signalling

Test Specification ID	OIPF-META-MC_SDNSE_AAS-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –OITF Service Discovery and Selection Extensions –Application Announcement & Signalling – Service Provider Related Application Signalling
Specification Section(s)	[META] §3.2.3.1 [TS102809]
Test Cases	• If service provider related applications are signalling using the AbstractService element at the Service Provider Discovery Record level: o Check that the Service Provider Discovery Record SHALL embed applications information in the ApplicationList element defined in [TS102809] where they are referred to as “unbound applications.” • If service provider related applications are signalling using the Application Discovery Record at the service discovery level : o Check that the Service Provider Discovery Record SHALL embed application reference id values in the ApplicationList element defined in [TS102809] for signalling the broadcast independent applications with the Application Discovery Record. o Check that the actual information of applications SHALL be described in the Application Discovery Record. o Check that when OITF receives the Service Provider Discovery Record and the Application Discovery Record, OITF SHALL link the application reference id values in the Service Provider Discovery Record to the application identifier values in the Application Discovery Record. • Check if a service provider wants to signal the applications : ServiceDiscovery Application, Communication Application, EPG Application and VoD Application with these two approaches, the ApplicationUsage value defined in [META] part 3.2.3.3.3 SHALL be used with the application location value defined in [META] part 3.2.3.3.6.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNSE_AAS-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection –OITF Service Discovery and Selection Extensions –Application Announcement & Signalling – Broadcast Related Application Signalling
Specification Section(s)	[META] §3.2.3.2 [TS102809]
Test Cases	• If service broadcast related applications are signalling using either the extended IPService element in the Broadcast Discovery Record or the extended Package element in the Package Discovery Record o Check for signalling broadcast related applications with the extended IPService and Package elements, the Broadcast Discovery Record and the Package Discovery Record SHALL embed applications information in the ApplicationList element defined in [TS102809] where they are referred to as "Service bound application." • If service provider related applications are signalling using the Application Discovery Record at the service discovery level : o Check that Broadcast related applications SHALL NOT be signalled with the Service Provider Discovery Record. o Check that the extended IPService element in the Broadcast Discovery Record and the extended Package element in the Package Discovery Record SHALL embed application reference id values in the ApplicationList element defined in [TS102809]. o Check that the actual information about applications SHALL be contained in the Application Discovery Record. o Check that when OITF receives the application reference id values in the extended IPService or Package element, the OITF SHALL link the application reference id values in the extended IPService and Package elements to the application identifier values in the Application Discovery Record • Check if a service provider wants to signal the applications : Communication Application, EPG Application and VoD Application with these two approaches, the ApplicationUsage value defined in [META] part 3.2.3.3.3 SHALL be used with the application location value defined in [META] section 3.2.3.3.6.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MC_SDNSE_AAS-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection – OITF Service Discovery and Selection Extensions – Application Announcement & Signalling – Platform Specific Definitions
Specification Section(s)	[META] §3.2.3.3 [TS102809] [MEDIA]
Test Cases	• Check that to use [TS102809] in the OIPF specification, the following platform specific definitions are described: o application types, o application profiling, o profile versioning, o graphic formats used for application icons. These properties are contained in the Application descriptor

	• The Type Element of the Application descriptor defines the actual application environment that is used by the application [TS102809]. The ApplicationTypeCS defines the values to signal if an OIPF application is either a DAE or PAE application. Check that : o for DAE applications this value SHALL be either "application/urn.oipf.cs.ApplicationTypeCS.2009.DAE.XHTML" or "application/urn.oipf.cs.ApplicationTypeCS.2009.DAE.SVG" o for PAE applications this value SHALL be "application/urn.oipf.cs.ApplicationTypeCS.2009.PAE" • The mhpVersion element defines the actual profile and profile version of the platform which is required to run an application. If the mhpVersion element is used in the ApplicationDescriptor [TS102809], check that the below values SHALL be set: o profile: 1 o versionMajor: 1 o versionMinor: 1 o versionMicro: 0 • OIPF defines specific application usages for ServiceDiscovery, Communication and ContentGuide applications. This is signalled using the ApplicationUsageDescriptor as defined in [TS102809]. If the ApplicationUsage element is used in the ApplicationDescriptor, check that the below values SHALL be set. o A Service Discovery application SHALL be signalled with a value of "urn:oipf:cs:ApplicationUsageCS:2009:servicediscovery." o A Communication application SHALL be signalled with a value of "urn:oipf:cs:ApplicationUsageCS:2009:communication." o An EPG application SHALL be signalled with a value of "urn:oipf:cs:ApplicationUsageCS:2009:epg." o A VoD application SHALL be signalled with a value of "urn:oipf:cs:ApplicationUsageCS:2009:vod." o An HNI-IGI application SHALL be signalled with a value of "urn:oipf:cs:ApplicationUsageCS:2009:hni-igi." • Check that the graphic formats used for application icons are the same as defined in [MEDIA] • In addition to the transport protocols defined in [TS102809], OIPF defines a multicast transport method using FLUTE. o Check that in order to signal this transport method the Application element of [TS102809] is extended by the FLUTESessionDescriptor.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.4 OIPF BCG (Broadband Content guide) Extensions

5.2.4.1.2.4.1 Signalling and Media Transport Protocol Extension

Test Specification ID	OIPF-META-MC_BCGE_SMTPE-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection – OITF BCG Extensions – Signalling and Media Transport Protocol Extension - OnDemandProgramType Extension
Specification Section(s)	[META] §3.3.1.1
Test Cases	• Check that Content on Demand can be delivered in Open IPTV Forum using a combination of different signalling and media transport protocols. Information about the protocols used MAY be signalled in the OnDemandProgramType describe in [TS102034] table 9.

Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.4.2 DRM Control Information Extension

Test Specification ID	OIPF-META-MC_BCGE_DRMCIE-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection – OITF BCG Extensions – DRM Control Information Extension - PurchaseItemType Extension
Specification Section(s)	[META] §3.3.2.1
Test Cases	• Check that the elements used as DRM control parameters are hold by the PurchaseItemType OITF extension of the BCG (DRMControlInformation). • Check that the existing tva:DRMDeclaration element in the BCG is not used in Open IPTV Forum services.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.4.3 Open IPTV Forum Classification Schemes

Test Specification ID	OIPF-META-MC_BCGE_CSCH-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Service Discovery and Selection – OITF BCG Extensions – Open IPTV Classification Schemes
Specification Section(s)	[META] §3.3.3
Test Cases	• Check that Open IPTV Forum classification schemes wholly replace the BCG equivalent classification schemes: o VideoCodingFormat Classification Scheme o AudioCodingFormat Classification Scheme o AVMediaFormat Classification Scheme o Protocol Classification Scheme o Reference to Parental Guidance Classification Scheme
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.1.2.5 FLUTE FDT Extensions

Test Specification ID	OIPF-META-MC_FFDTE-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Content – Flute FDT Extensions
Specification Section(s)	[META] §3.4 [FLUTE]
Test Cases	• Check that when FLUTE is used for delivery of objects via multicast the FDT-Instance XML structure is extended using the extension mechanism defined in [FLUTE]. • Check that the FLUTE FDT-Instance element is extended with two attributes. o The Tags attribute contains a list of tags that the content is associated

	with. o The optional Priority attribute is used by the OITF to determine which content items can be discarded when there is a need to recover memory.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.2 Metadata Control and Delivery

5.2.4.2.1 Metadata Delivery Mechanism

5.2.4.2.1.1 Carriage of SD&S metadata

Test Specification ID	OIPF-META-MCD_MDM_CSDNSM-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of SD&S metadata
Specification Section(s)	[META] §4.1.1
Test Cases	• Check for the SD&S metadata information delivery over multicast, it is the DVBSTP Protocol which is used. • Check that the DVBSTP Syntax and usage are conform to the [SDNS] definition • Check for the SD&S metadata information delivery over unicast, it is the HTTP Protocol which is used. • Check that the HTTP Request and usage are conform to the [SDNS] definition
Preconditions	• Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MDM_CSDNSM-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of SD&S metadata - Additional PayloadID values
Specification Section(s)	[META] §4.1.1.1 [SDNS] §5.2.2.1 [BCG] §4.1.2.1
Test Cases	• Check for the carriage of Application discovery record defined in [TS102809], Payload ID “0xC1” is used. • Check that All other PayloadIDs SHALL be as specified in clause 5.2.2.1 of [SDNS] and clause 4.1.2.1 of [BCG].
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	This clause only applies when Metadata Content is transported with DVBSTP and HTTP.

Test Specification ID	OIPF-META-MCD_MDM_CSDNSM-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of

	SD&S metadata - Encoding metadata
Specification Section(s)	[META] §4.1.1.2 [SDNS] §5.5
Test Cases	Check that OITF can supported BiM encoding for SDNS and BCG delivery information
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MDM_CSDNSM-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of SD&S metadata – Update mechanism for SD&S
Specification Section(s)	[META] §4.1.1.3
Test Cases	• Check that OITF supports the signalling of change for SD&S metadata information delivery over multicast mode (DVBSTP). • Check that OITF supports the signalling of change for SD&S metadata information delivery over unicast mode (HTTP)
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.2.1.2 Carriage of BCG metadata

Test Specification ID	OIPF-META-MCD_MDM_CBCGM-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of BCG metadata
Specification Section(s)	[META] §4.1.2 [BCG] §4.1
Test Cases	• Check that OITF can support the Container Based delivery for the BCG metadata information delivery. • Check that OITF can support the Text Based delivery for BCG metadata information delivery. • Check that Container based delivery of BCG metadata is conform to clause 4.1 of [BCG]. • Check that OITF may support the SOAP Query mechanism for text-based delivery.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MDM_CBCGM-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of BCG metadata – Container Based delivery
Specification Section(s)	[META] §4.1.2.1 [BCG] §4.1.2.2.1 [BCG] §4.1.2.2.2

Test Cases	• Check that the DVBSTP Protocol is used for the BCG Container Based delivery over multicast. • Check that the HTTP Protocol is used for the BCG Container Based delivery over unicast. • Check the DVBSTP Protocol is used as defined in clause 4.1.2.2.1 of [BCG] • Check the HTTP Protocol is used as defined in clause 4.1.2.2.2 of [BCG]
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MDM_CBCGM-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of BCG metadata – Container Based delivery- Encoding BCG metadata
Specification Section(s)	[META] §4.1.2.1.1 [BCG]
Test Cases	• Check that the Encoding BCG metadata may be supported as described in [BCG]. • Check that BCG metadata can also be delivered without encoding.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MDM_CBCGM-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of BCG metadata – Container Based delivery- Update mechanism
Specification Section(s)	[META] §4.1.2.1.2 [TVA-UNID] [SDNS] §5.4.3
Test Cases	• Check that delivered BCG metadata have update manage through fragment updating method as described in TV-Anytime specification [TVA-UNID] • Check that OITF client is able to detect the changes of fragment version through the method described in clause 5.4.3 of [SDNS].
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.2.1.2.1 SOAP Query Mechanism

Test Specification ID	OIPF-META-MCD_MDM_CBCGM_SOAP-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of BCG metadata – SOAP Query Mechanism
Specification Section(s)	[META] §4.1.2.2 [TVA-BID] [BCG] [SDNS] §5.4.3
Test Cases	• Check that SOAP query methods are implemented on OITF as described in

	the clause 4.2 of [BCG]. • Check that mandatory SOAP methods defined in [TS102034] table 12 are implemented. • Check the good implementation of the request "get_data" SOAP method in the OITF. • Check conformity of the response of "get_data" SOAP method delivered by the Metadata Server • Check the good implementation of the request "describe_Get_data" SOAP method in the OITF. • Check conformity of the response of "describe_Get_data" SOAP method delivered by the Metadata Server
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MDM_CBCGM_SOAP-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Carriage of BCG metadata – SOAP Query Mechanism – SOAP Update mechanism for BCG
Specification Section(s)	[META] §4.1.2.2.3 [TVA-BID]
Test Cases	• Check that overall BCG XML document may have version number associated with it. • Check that BCG fragments may have an ID and version number associated with them. • Check that client may allowed to request fragment updates using SOAP Query mechanism.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

5.2.4.2.1.3 Event Information Tables (EIT)

- Broadcast Discovery
  - URI identifier of a BCG or ContentGuide Discovery record. Either:
    - *BroadcastDiscovery/SI/ServiceDescriptionLocation* or
    - *BroadcastDiscovery/ServicesDescriptionLocation*

In accordance with clause 5.2.6.2.2 of SD&S [SDNS], if present, SI/ServiceDescriptionLocation shall take precedence. Furthermore, if more than one BCG or ContentGuide Discovery record is specified, a single preferred record may optionally be signalled using the "preferred" attribute.

Test Specification ID	OIPF-META-EIT_TSOptionalSI-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Delivery Mechanism – Metadata embedded in a DVB Transport Stream
Specification Section(s)	[META] §4.1.3 [DVBSI] §5.2.4
Test Cases	• Check that an OITF is able to retrieve the Event Information Table (EIT) which is embedded in a DVB Transport Stream and contains metadata events (event name, start time, duration…). For Open IPTV Forum, EIT information is restricted to the following two main types of table:

	o actual TS, present/following event information = table_id = "0x4E"; o other TS, present/following event information = table_id = "0x4F";
Preconditions	Transport Streams with EIT tables available
Priority	Optional
Remark	

5.2.4.2.2 Metadata Control

5.2.4.2.2.1 Locating a BCG for a Service using SD&S

Test Specification ID	OIPF-META-MCD_MC_LBCGFS-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Control – Locating a BCG for a Service using SD&S
Specification Section(s)	[META] §4.2.1 [SDNS] §5.2.6.2.2
Test Cases	• Check that access to a BCG service is described in a BCG which is linked to from Broadcast Discovery Record • Check that the following SD&S elements should be used: o In Broadcast Discovery the URI identifier of a BCG record : – *BroadcastDiscovery/SI/ServiceDescriptionLocation* or – *BroadcastDiscovery/ServicesDescriptionLocation* – Check that if present, *SI/ServiceDescriptionLocation* shall take precedence. Furthermore, if more than one BCG record is specified, a single preferred record may optionally be signaled using the "preferred" attribute. o In BCG record: – Identifier of BCG : *BCGDiscovery/BCG@ID,* – One of delivery information of BCG metadata: ▪ *BCGDiscovery/TransportMode/DVBSTP* ▪ *BCGDiscovery/TransportMode/HTTP@Location* ▪ *BCGDiscovery/TransportMode/HTTP@SOAP*
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	[META] Figure 6 Indicates how to receive BCG metadata relating to a single service or a couple of services in Broadcast Discovery information. In order to signal BCG metadata for a single service or services' list, the value of "ServiceDescriptionLocation" or "ServicesDescriptionLocation" in Broadcast Discovery and "BCG@ID" in BCG must be the same. The transport address of BCG metadata is described in the children nodes of "TransportMode" element in the relevant BCG. With this address, the OITF can receive BCG metadata for a single service or a couple of services (either through push or pull container based mechanism, or through SOAP querying).

5.2.4.2.2.2 Linking SD&S Service Information with BCG

Test Specification ID	OIPF-META-MCD_MC_LSDNSSIBCG-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Control – Linking SD&S Service Information with BCG
Specification Section(s)	[META] §4.2.2 [SDNS] §5.2.1.2 [BCG] §6.6

Test Cases	• Check that access to the BCG record allows the OITF to receive all BCG metadata relating to a single or a couple of services. • Check that the following SD&S elements and BCG element should be used for create an EPG: • To create an EPG, for example, with the received BCG metadata and SD&S metadata, the following BCG metadata elements should be used: o ServiceInformationTable – *TVAMain/ProgramDescription/ServiceInformationTable/ServiceInformation@serviceId* ▪ Unique Identifier of Service whose syntax is defined in clause 5.2.1.2 of SD&S [SDNS] - equals the ServiceName attribute in the associated SD&S Broadcast Discovery record (See clause 6.6 in BCG [BCG]). o Schedule Element in ProgramLocationTable – *ProgramLocationTable/Schedule@serviceIDRef* ▪ Reference of a serviceId ▪ *serviceIDRef* value must be the same as the associated *serviceId* in *ServiceInformationTable* – *ProgramLocationTable/Schedule/ScheduleEvent/Program@crid* ▪ CRID information of a program in a service. Provides link to detailed program description, found in the ProgramInformationTable. – *ProgramLocationTable/Schedule/ScheduleEvent/PublishedStartTime* ▪ Advertised start time of a single program in a service – *ProgramLocationTable/Schedule/ScheduleEvent/PublishedDuration* ▪ Advertised duration of a single program. o ProgramInformationTable – *ProgramInformationTable/ProgramInformation@programId* ▪ CRID value of a single program ▪ *programId* value should be the same with one of CRID values in ProgramLocationTable
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	[META] Figure 7 describes how to find description information in BCG from a single service of Broadcast Discovery. Service information in SD&S and BCG metadata is linked as described in clause 6.6 of BCG [BCG] (BCG ServiceInformation@serviceId = SD&S BroadcastDiscovery ServiceName attribute). Once the *serviceId* value in *ServiceInformationTable* is found, a single service's schedule events can be retrieved from the *ProgramLocationTable*. Then, *Program@CRIDs* in *ScheduleEvent* values can be used to find detailed information of a single content by referencing *ProgramInformation@programId*.

5.2.4.2.2.3 CRID Location Resolution

Test Specification ID	OIPF-META-MCD_MC_CRIDLR-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Control – CRID Location Resolution – Unmanaged Network
Specification Section(s)	[META] §4.2.4.1 [BCG] [TVA-BID]

Test Cases	• Check that The terminal that supports BCG shall support content resolution: • Check that the terminal may support terminal-side resolution. If so, it shall be delivered using the container-based mechanisms, as specified by clause 5 of [BCG]. • Check that the terminal shall support server-side resolution using the protocol defined in [TVA-BID]. • Check that a service provider may provide content resolution information.
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-META-MCD_MC_CRIDLR-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Metadata Control and Delivery – Metadata Control – CRID Location Resolution – Managed Network
Specification Section(s)	[META] §4.2.4.2 [PROT]
Test Cases	• Check that the service provider have the choice between two approach for identifying each instance of one content : o one CRID per instance o one CRID for the content and x IMIs for each instance, the combination of CRID and IMI identifies the appropriate instance • Check that to enable either approach to be used for Content on Demand provided via managed networks, CoD session setup and initiation SHALL use the CRID and an Instance Metadata Identifier (where one exists) in conjunction with the process defined in clause 5.2.2 of the Protocol specification • Check the implementation of the URI CRID request
Preconditions	Test Manager has access to OIPF XML files and to XML validation tools.
Priority	Mandatory
Remark	CRID Location Resolution for scheduled content is undefined.

5.3 Protocols

The testable functions and aspects for various protocols are given below.

- HTTP:
  - Service Functions: Scheduled Content, CoD and Content Download.
  - Service Access and Control Functions: These functions involve Service Provider Discovery, Service Discovery, Service Access, User Profile Management, Remote Management and User Registration and Network Authentication.
  - Communication Functions: These Functions involve Caller ID, Instant Messaging, IM Session and Presence.
  - Protocol System Infrastructure Functions
- SIP:
  - Service Functions: Scheduled Content and CoD.
  - Service Access and Control Functions: These functions involve Service Provider Discovery and Notification of Service Profile Changes.
  - Communication Functions: These Functions involve Caller ID, Instant Messaging, IM Session and Presence.
- RTSP:
  - Service Functions: CoD.
  - Service Access and Control Functions: Performance Monitoring.
- IGMP:
  - Service Functions: Scheduled Content.
  - Service Access and Control Functions: Service Discovery and Remote Management.
- RTP/ RTCP:
  - Service Functions: Scheduled Content and CoD.
  - Service Access and Control Functions: Performance Monitoring.
- UPnP and DLNA:
  - Protocol System Infrastructure Functions.

5.3.1 Prerequisites

None

5.3.2 Test Method

Testing is performed by the Coordinated Testing Method displayed in Figure 4 because the top of the IUT (Implementation under Test) is not accessible. The Test Management (Lower Tester) dictates the behaviour of the Testing Target and Driver (Upper Tester), to achieve the purpose of each test case, in a language which can be "spoken" from the Lower Tester PCO (Point of Control and Observation). By adopting the Coordinated Testing Method, the testing can be done by test cases written using the TTCN-3 environment.

The TTCN-3 test cases are written with respect to all functionalities of the protocol. Different test cases will be generated by varying the main functionality like Registration, Call Control etc. The Functionality Subgroups, such as Call Establishment, Call Release etc. also need to be varied. The script will be varied according to the Role such as the Originating Endpoint, Terminating Endpoint, Registrar, Registrant etc.

The testing procedure begins when the Driver User Agent on the Test Execution module triggers the Driver User Agent on the testing target. According to this trigger, an application or driver on the testing target triggers the REQUEST to the Test Execution Module. When the REQUEST is received at the remote end through the TRI, the TTCN-3 Runtime System sends a message to the Encoding Decoding System to decode the test message. The Encoding Decoding System then decodes this message and provides the TTCN-3 values to the Executable Test Suite entity. The test execution starts within the Test Control entity. During the test execution, the test events are logged in the Test Logging entity. This log will be analyzed using a protocol analyzer such as Wireshark to compare it with the expected output.

5.3.2.1 Coordinated Test Method

The lower tester is remote and accesses the SUT (System Under Test) through a network or a service provider. There is only one PCO, beneath the lower tester. The top of the IUT is not accessible. However, an upper tester must be incorporated into the SUT, to handle an explicit and standardized form of test coordination procedures, the Test Management. The Test Management dictates the behaviour of the Upper Tester, to achieve the purpose of each test case, in a language which can be "spoken" from the lower tester PCO.

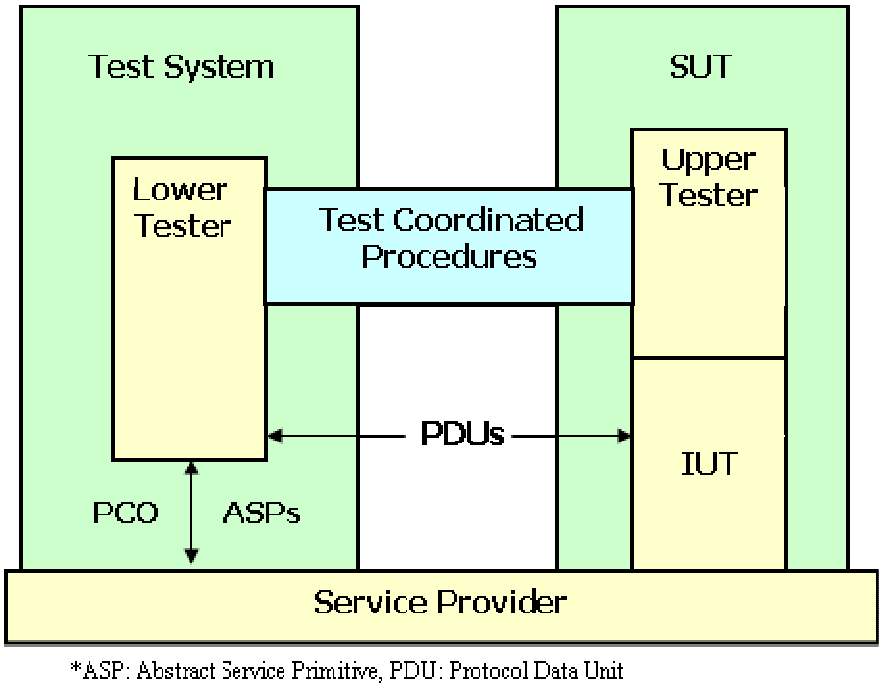

Figure 4 - Coordinated Test Method

The details of the test items are given below for each of the testable protocols:

- Service Functions:

  The service functions for the various protocols involved in Scheduled Content, CoD and Content Download.

- Service Access and Control Functions:

  These functions basically consist of Service Provider Discovery, Service Discovery, Service Access, User Profile Management and Usage, Remote Management, User Registration and Network Authentication, Notifications of Service Profile Changes and Performance Monitoring.

- Communication Functions:

  For different protocols, communication functions involve Caller ID, Instant Messaging, IM Session and Presence.

- Protocols System Infrastructure Functions:

  Some protocols like HTTP, UPnP and DLNA employ these functions over the endpoints.

5.3.3 Test Environment

The test environment for Protocol is displayed in Figure 5 and described below.

- Testing Target:

  This is the entity for which the protocol of the sent and received messages is to be tested.

- Test Execution:
  - TTCN-3 Runtime System:

    This entity interacts with the Test Management module entities via TCI, and manages the Executable Test Suite and Encoding Decoding System entities.

- Executable Test Suite:

  This entity handles the execution or interpretation of test cases, the sequencing and matching of test events, as defined in the corresponding TTCN-3 modules. It interacts with the TTTCN-3 Runtime System entity to send, attempt to receive (or match), and log test events during test case execution.

- Encoding/ Decoding System:

  This entity is responsible for the encoding and decoding of test data, as specified in the executing TTCN-3 module.

- Test Management:
  - Test Control:

    This entity is responsible for overall management of the test system. After the test system has been initialized, test execution starts within the Test Control entity. The entity is responsible for the proper invocation of TTCN-3 modules.

  - Test Logging and Analysis:

    This entity is responsible for maintaining the test log. It is explicitly notified of log test events by the Test Execution. The Test Logging entity has a unidirectional interface where any entity part of the Test Execution may post a logging request to the Test Logging entity. A Test Management internal interface may also be used to record test management information generated by the Test Control.

  - External Codec:

    The External Codec entities are optionally responsible for encoding and decoding data associated with message-based or procedure-based communications within the Test Execution module. Unlike the built-in codec, the external codec has a standardized interface which makes it portable between different TTCN-3 systems and tools.

- Driver User Agents:

  These are APIs that are present at the Testing Target as well as at the Test Execution module. These entities trigger the protocol messages.

- TRI:

  This is the interface between the Testing Target and the Test Execution module. This TTCN-3 Run-time Interface is required for interfacing the executable tests to the Testing Target. It provides a standardized adaptation for timing and communication of a software test system to a particular processing platform and the system under test

- TCI:

  This is the interface between the Test Execution module and the Test Management module. This TTCN-3 Control Interface is required for controlling the execution of test cases and activities like management, logging and analysis etc.

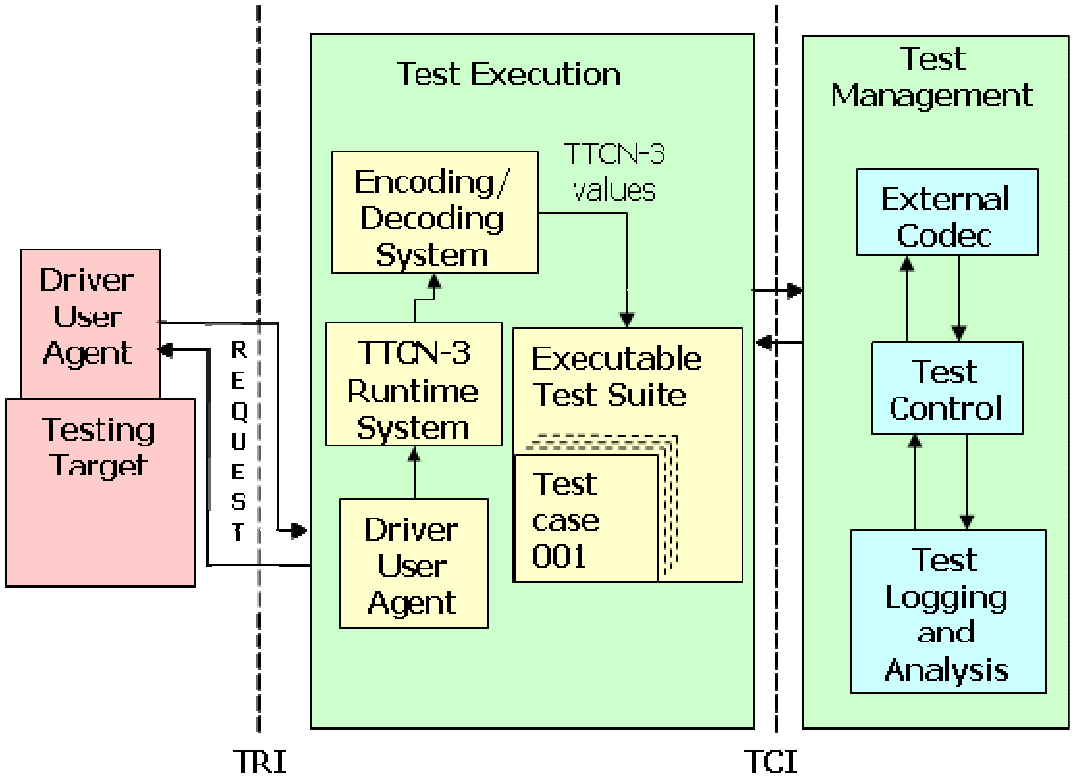

Figure 5 - Test Environment for Protocols

5.3.4 Test Specification for Protocols

5.3.4.1 HTTP Protocol

5.3.4.1.1 Service Provider Discovery

Test Specification ID	OIPF-PROT-HTTP_SPDM-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG
Test Specification Description	Service Provider Discovery in HTTP protocol using managed network
Specification Section(s)	[PROT] §5.3.1.1
Test Cases	• Check request for subscription (HTTP POST) from OITF to IG with the purposes below: o Subscription initiation o Refresh subscription o Subscription cancellation • Check response for subscription (HTTP status code) from IG to OITF • Check initial pending IG request (HTTP PENDING_IG) from OITF to IG • Check response with XML information (HTTP status code) from IG to OITF • Check pending IG request (HTTP Pending IG with SIP response) from OITF to IG
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SPDUS-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Service Provider Discovery FE
Test Specification Description	Service Provider Discovery using SD&S records via unicast in HTTP protocol
Specification Section(s)	[PROT] §5.3.1.2
Test Cases	• Check service providers information request (HTTP GET) from OITF to service provider discovery server, that could be IPTV Service Provider Discovery FE or IG, depending on the OITF deployment • Check service providers information response (HTTP status code) from service provider discovery server, that could be IPTV Service Provider Discovery FE or IG, depending on the OITF deployment, to OITF delivered as SD&S record for searching Service Discovery Information in: o Push mode (via multicast) o Pull mode (via unicast) o DAE Application (via web)
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SPDDAE-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Application FE
Test Specification Description	Service Provider Discovery using DAE Applications in HTTP protocol without using managed network
Specification Section(s)	[PROT] §5.3.1.2
Test Cases	• Check retrieval of Service Provider Discovery Information from IPTV Application FE, as Service Provider Discovery FE, to OITF using DAE Application
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.1.2 Service Discovery

Test Specification ID	OIPF-PROT-HTTP_SDUS-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Service Discovery FE
Test Specification Description	Service Discovery using SD&S records via unicast in HTTP protocol without using managed network
Specification Section(s)	[PROT] §5.3.2.2
Test Cases	• Check service information request (HTTP GET) from OITF to IPTV Service Discovery FE • Check service information response (HTTP status code) from IPTV Service Discovery FE to OITF delivered as SD&S record for searching Service Access Information in: o Push mode (via multicast) o Pull mode (via unicast)

	o DAE Application (via web)
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SDDAE-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Application FE
Test Specification Description	Service Discovery using DAE Applications in HTTP protocol without using managed network
Specification Section(s)	[PROT] §5.3.2.1
Test Cases	• Check retrieval of Service Discovery Information from IPTV Application FE, as Service Discovery FE, to OITF using DAE Application
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.1.3 Service Access

Test Specification ID	OIPF-PROT-HTTP_SAUC-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Metadata Control FE
Test Specification Description	Service Access Container-Based Delivery via unicast in HTTP protocol without using managed network
Specification Section(s)	[PROT] §5.3.3.2
Test Cases	• Check Broadband Content Guide information request (HTTP GET) from OITF to IPTV Metadata Control FE • Check Broadband Content Guide information response (HTTP status code) from IPTV Metadata Control FE to OITF delivered as SD&S record
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SAUQ-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Metadata Control FE
Test Specification Description	Service Access Query mechanism vis unicast in HTTP protocol without using managed network
Specification Section(s)	[PROT] §5.3.3.2
Test Cases	• Check Broadband Content Guide information request (HTTP POST) from OITF to IPTV Metadata Control FE for the SOAP methods below: o get_Data o describe_Get_Data

	o submit_Data o describe_Submit_Data • Check Broadband Content Guide information response (HTTP status code) from IPTV Metadata Control FE delivered as XML document that could be: o SOAP method error response o SOAP method successful response
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SADAE-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Application FE
Test Specification Description	Service Access using DAE Applications in HTTP protocol without using managed network
Specification Section(s)	[PROT] §5.3.3.1
Test Cases	• Check performance of the Service using DAE Application
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.1.4 Scheduled Content

Test Specification ID	OIPF-PROT-HTTP_SCSI-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG
Test Specification Description	Scheduled Content Session Initiation in HTTP protocol using managed network
Specification Section(s)	[PROT] §5.2.1.1.1
Test Cases	• Check request for session initiation (HTTP POST) from OITF to IG • Check response for session initiation (HTTP status code) from IG to OITF • Check acknowledgement of the last response (HTTP PENDING_IG) from OITF to IG
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SCSM-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG
Test Specification Description	Scheduled Content Session Modification Session in HTTP protocol using managed network

Specification Section(s)	[PROT] §5.2.1.1.2
Test Cases	• Check request for session modification (HTTP POST) from OITF to IG with the purposes below: o Change of service. o Change of bandwidth. • Check response for session modification (HTTP status code) from IG to OITF • Check acknowledgement of the last response (HTTP PENDING_IG) from OITF to IG
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SCSR-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG
Test Specification Description	Scheduled Content Session Refresh in HTTP protocol using managed network
Specification Section(s)	[PROT] §5.2.1.1.4, [PROT] §5.5.1.4.1
Test Cases	• Check refresh message (HTTP PENDING_IG) from OITF to IG • Check response for refreshing (HTTP status code) from IG to OITF • The OITF performance should be tested: o Repeat the refreshing o Terminate the session
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-HTTP_SCST-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG
Test Specification Description	Scheduled Content Session Termination in HTTP protocol using managed network
Specification Section(s)	[PROT] §5.2.1.1.3, [PROT] §5.5.1
Test Cases	• Check request for session termination (HTTP POST or HTTP PENDING_IG) from OITF to IG • Check response for session termination (HTTP status code) from IG to OITF originated by the OITF or IPTV Control FE request.
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.2 SIP Protocol

5.3.4.2.1 Service Provider Discovery

Test Specification ID	OIPF-PROT-SIP_SPDM-002
Test Specification Version	1.0.0
Test Object(s)	IG, Authentication and Session Management FE, IPTV Service Provider Discovery FE
Test Specification Description	Service Provider Discovery in SIP protocol using managed network
Specification Section(s)	[PROT] §6.3.1
Test Cases	• Check request for subscription (SIP SUBSCRIBE) from IG to IPTV Service Provider Discovery FE via Authentication and Session Management FE with the purposes below: o Subscription initiation. o Refresh subscription. o Subscription cancellation • Check response for subscription (SIP status code) from IPTV Service Provider Discovery FE to IG via Authentication and Session Management FE • Check request for notifying (SIP NOTIFY) from IPTV Service Provider Discovery FE to IG via Authentication and Session Management FE • Check response for notifying (SIP status code) IG to IPTV Service Provider Discovery FE via Authentication and Session Management FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.2.2 Scheduled Content

Test Specification ID	OIPF-PROT-SIP_SCSI-002
Test Specification Version	1.0.0
Test Object(s)	IG, Authentication and Session Management FE, IPTV Control FE
Test Specification Description	Scheduled Content Session Initiation in SIP protocol using managed network
Specification Section(s)	[PROT] §6.2.1.1.1, [PROT] §6.2.1.2.1
Test Cases	• Check request for session initiation (SIP INVITE) from IG to IPTV Control FE via Authentication and Session Management FE • Check response for session initiation (SIP status code) from IPTV Control FE to IG via Authentication and Session Management FE • Check acknowledgement of the last response (SIP ACK) from IG to IPTV Control FE via Authentication and Session Management FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-SIP_SCSM-002
Test Specification Version	1.0.0
Test Object(s)	IG, Authentication and Session Management FE, IPTV Control FE
Test Specification Description	Scheduled Content Session Modification in SIP protocol using managed network
Specification Section(s)	[PROT] §6.2.1.1.1, [PROT] §6.2.1.2.2
Test Cases	• Check request for session modification (SIP re-INVITE or SIP UPDATE) from IG to IPTV Control FE via Authentication and Session Management FE with the purposes below: o Change of service. o Change of bandwidth. • Check response for session modification (SIP status code) from IPTV Control FE to IG via Authentication and Session Management FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-SIP_SCST-002
Test Specification Version	1.0.0
Test Object(s)	IG, Authentication and Session Management FE, IPTV Control FE
Test Specification Description	Scheduled Content Session Termination in SIP protocol
Specification Section(s)	[PROT] §6.2.1.1.2, [PROT[§6.2.1.2.3
Test Cases	• Check request for session termination (SIP BYE) from IG to IPTV Control FE via Authentication and Session Management FE originated by an OITF request • Check response for session termination (SIP status code) from IPTV Control FE to IG via Authentication and Session Management FE originated by an OITF request • Check request for session termination (SIP BYE) from IPTV Control FE to IG via Authentication and Session Management FE originated by an internal indication
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.3 IGMP and Multicast Protocol

5.3.4.3.1 Service Discovery

Test Specification ID	OIPF-PROT-IGMP_SDJS-004
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Service Discovery Joining Service in IGMP protocol without using managed network
Specification Section(s)	[PROT] §8.2.1.2
Test Cases	• Check joining operation (IGMPv3 Membership Report or IGMPv2 Membership Report) from OITF to Transport Processing Function FE

Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-IGMP_SDLS-004
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Service Discovery Leaving Service in IGMP protocol without using managed network
Specification Section(s)	[PROT] §8.2.1.2
Test Cases	• Check leaving operation (IGMPv3 Membership Report or IGMPv2 Leave group) from OITF to Transport Processing Function FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-DVBSTP_SDMD-004
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Service Discovery FE
Test Specification Description	Service Discovery DVB SD&S records via multicast in DVBSTP protocol without using managed network
Specification Section(s)	[PROT] §8.2.1.1
Test Cases	• Check multicast delivery of SD&S information in DVBSTP protocol from IPTV Service Discovery FE to OITF
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.3.2 Service Access

Test Specification ID	OIPF-PROT-IGMP_SAJC-004
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Service Access to Join Container-Based Delivery in IGMP protocol without using managed network
Specification Section(s)	[PROT] §8.2.1.2
Test Cases	• Check join operation (IGMPv3 Membership Report or IGMPv2 Membership Report) from OITF to Transport Processing Function FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages

Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-IGMP_SALC-004
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Service Access Leaving Container-Based Delivery in IGMP protocol without using managed network
Specification Section(s)	[PROT] §8.2.1.2
Test Cases	• Check leave operation (IGMPv3 Membership Report or IGMPv2 Leave group) from OITF to Transport Processing Function FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-DVBSTP_SAMD-004
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Metadata Control FE
Test Specification Description	Service Access DVB SD&S records via multicast in DVBSTP protocol without using managed network
Specification Section(s)	[PROT] §8.2.1.1
Test Cases	• Check multicast delivery of Broadband Content Guide information in DVBSTP protocol from IPTV Metadata Control FE to OITF
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.3.3 Scheduled Content

Test Specification ID	OIPF-PROT-IGMP_SCJS-004
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Scheduled Content Joining Service in IGMP protocol without using managed network
Specification Section(s)	[PROT] §8.1
Test Cases	• Check join operation (IGMPv3 Membership Report or IGMPv2 Membership Report) from OITF to Transport Processing Function FE
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-IGMP_SCLS-004
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Scheduled Content Leaving Service in IGMP protocol without using managed network
Specification Section(s)	[PROT] §8.1
Test Cases	• Check leave operation (IGMPv3 Membership Report or IGMPv2 Leave group) from Transport Processing Function FE to OITF
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.4 RTP/RTCP Protocol

5.3.4.4.1 Scheduled Content

Test Specification ID	OIPF-PROT-RTP_SC-005
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE
Test Specification Description	Scheduled Content Delivery in RTP protocol without using managed network
Specification Section(s)	[PROT] §9.1.1
Test Cases	• Check streamed content encapsulated in RTP from Transport Processing Function FE to OITF (Single Program Transport Stream, SPTS)
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Mandatory
Remark	

5.3.4.5 UDP Protocol

5.3.4.5.1 Scheduled Content

Test Specification ID	OIPF-PROT-UDP_SC-007
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function FE without using managed network
Test Specification Description	Scheduled Content Delivery in UDP protocol
Specification Section(s)	[PROT] §9.1.1
Test Cases	• Check streamed content encapsulated in UDP from Transport Processing Function FE to OITF
Preconditions	• The Testing Target is configured with the Test Manager • The Encoding/ Decoding System and the Test Suite Converter are configured with the Testing Target as well as the Test Manager • Driver is installed on the Testing Target which triggers the messages
Priority	Optional
Remark	

5.3.4.6 Remote Management

5.3.4.6.1 Remote Management for Open Internet Profile and Baseline Managed Profile

The Remote Management for the Open Internet Profile and Baseline Managed Profile is based on the DAE APIs. Therefore, the test cases are part of the DAE section.

5.3.4.6.2 Remote Management for Enhanced Managed Profile

Pre-requisites:

> *Information on BBF Conformance and Interoperability test plan to be provided when the OIPF/BBF liaison is in place.*

OIPF Remote Management for Enhanced Managed Profile devices SHALL be supported via the Broadband Forum (BBF) TR-069 based approach [TR-069].

The BBF has specified the CPE WAN Management Protocol (CWMP) designed for the communication between a CPE and an Auto-Configuration Server (ACS). The ACS is a server within the Service Provider's network that controls and manages a CPE which has a TR-069 client. The BBF has also defined a set of hierarchical CPE object models for InternetGatewayDevice object, VoIP, STB devices, etc.

In the framework of an OIPF deployment based on the Enhanced Managed Profile, it is assumed that the RMS, WG, IG and AG functional entities are implemented in line with the Broadband Forum TR-069 approach and that the compliance rules of the BBF for conformance and interoperability apply. A RMS (Remote Management Server) OIPF functional entity is called an ACS (Auto-Configuration Server) in BBF terminology. The Remote Management test cases use the ACS abbreviation.

As the OITF functional entity defined by the OIPF will be integrated in retail devices, it is intended that an OITF support limited functions mainly for Capabilities inventory, Performance monitoring and Diagnostics. Consequently, an OITF device does not fulfil all the requirements that are requested in TR-069 [TR-069]. The OIPF has defined a subset of the RPC methods defined in the TR-069 protocol, as well as a specific OITF data model derived from the TR-135 and TR-106 data models. Therefore, the test cases for an OITF functional entity focus on the set of RPC methods of the protocol and the parameters of the OIPF-specific data model.

Test Specification ID	OIPF-PROT-TR069-RPC-001
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Check that the OITF implements the limited set of RPC methods of [TR-069] that are required in the framework of OIPF. Check that an ACS compliant with [TR-069] is able to remotely manage an OITF
Specification Section(s)	[PROT] §5.3.5.1.2
Test Cases	• Check that the OITF implements the following RPC methods and respects the calling arguments and type as defined in [TR-069] o Inform o GetRPCMethods o SetParameterValues o GetParameterValues o SetParameterAttributes o GetParameterAttributes • Check that the DeviceIdStruct that is used for the DeviceId argument of the Inform method is obtained from the ManufacturerOUI, the ProductClass "OIPF" and the serialNumber, and that the DeviceID is unique for each OITF
Preconditions	• OITF is connected to a gateway that provides access to a managed network and the OITF has already been provisioned with the address of the ACS • The ACS and the OITF are able to communicate using underlying protocols used by TR-069 protocol
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-TR069-TR106-002
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Test of the OITF specific Data Model derived from TR-106 Data Model o Check that all the READ parameters in the parameters lists defined in the table 66 can be read and are consistent with the semantics given by the parameters o Check that all the WRITE parameters in the parameters lists defined in the table 66 can be written in the OITF and provide the expected result
Specification Section(s)	[PROT] §5.3.5.1.2 [PROT] Annex K OITF-specific TR-135 and TR-106 Remote Management Objects (Normative), table 66
Test Cases	• Check that the **Device.DeviceSummary** and **Device.DeviceInfo.** readable parameters can be read and are consistent with the OITF description • Check that the **Device.ManagementServer.URL** writable parameter can be written and used to set-up the URL of the ACS • Check that the **Device.ManagementServer.Username** and the **Device.ManagementServer.Password** writable parameters can be written and used to set-up the username and password used to authenticate the CPE when making a connection to the ACS • Check that the **Device.ManagementServer.PeriodicInformEnable**, **Device.ManagementServer.PeriodicInformInterval** and **Device.ManagementServer.PeriodicInformTime** writable parameters can be written and used to indicate whether or not the CPE MUST periodically send an Inform message to the ACS, with indication of duration and interval of time • Check that the **Device.ManagementServer.ParameterKey**, **Device.ManagementServer.ConnectionRequestURL**, **Device.ManagementServer.ConnectionRequestUsername** and **Device.ManagementServer.ConnectionRequestPassword** parameters to associate the OITF with an ACS are accurately implemented • Check that the **Device.GatewayInfo.** readable parameters can be read and are consistent with the WAN Gateway (the connected Internet Gateway Device) • Check that the **Device.LAN.** readable parameters can be read and are consistent with the IP configuration of the OITF
Preconditions	• OITF is connected to a gateway that provides access to a managed network and the OITF has already been provisioned with the address of the ACS • The ACS and the OITF are able to communicate using underlying protocols used by TR-069 protocol
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-TR069-TR135-003
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Test of the OITF specific Data Model derived from TR-135 Data Model o Check that all the READ parameters in the parameters lists defined in the table 65 can be read and are consistent with the semantics given by the parameters o Check that all the WRITE parameters in the parameters lists defined in the table 65 can be written in the OITF and provide the expected result

Specification Section(s)	[PROT] §5.3.5.1.2 [PROT] Annex K OITF-specific TR-135 and TR-106 Remote Management Objects (Normative), table 65
Test Cases	• Check that the **.STBService.{i}.Capabilities.** readable parameters can be read and are consistent with the OITF capabilities • Check that the **.STBService.{i}.Components.** readable parameters can be read and are consistent with the OITF components description • Check that the **.STBService.{i}.Components.FrontEnd.{i}.DVBT.Modulation.SNR** readable parameter can be read and is consistent with the signal quality value of the DVBT reception the OITF • Check that the **.STBService.{i}.AVStreams.** readable parameters can be read and are consistent with the OITF AV Streams description • Check that the **.STBService.{i}.Components.FrontEnd.{i}.IP.RTCP.** writable parameter can be written and used to enable or disable RTCP receiver report generation • Check that the **.STBService.{i}.ServiceMonitoring**. writable parameters can be written to configure the service monitoring and that the provided Sample statistics are consistent with the settings • Check that the **.STBService.{i}.ServiceMonitoring.** writable parameters can be written to reset the Total statistics and that the provided Total statistics are consistent with the settings
Preconditions	• OITF is connected to a gateway that provides access to a managed network and the OITF has already been provisioned with the address of the ACS • The ACS and the OITF are able to communicate using underlying protocols used by TR-069 protocol
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-TR069-IGConf-004
Test Specification Version	1.0.0
Test Object	IG
Test Specification Description	Configuration of the IG via Configuration File
Specification Section(s)	[PROT] §5.3.5.1.3
Test Cases	Check that the IG can be configured with an IPTV configuration file with the list of users with their IMPU, Alias and Passwords and also configure whether user authentication is to be performed by the IG
Preconditions	• IG is connected to a WAN gateway that provides access to a managed network and the IG has already been provisioned with the address of the ACS • The ACS and the IG are able to communicate using underlying protocols used by TR-069 protocol
Priority	Mandatory
Remark	

5.3.4.7 Communication Services for Protocols

5.3.4.7.1 General Communication Services

Test Specification ID	OIPF-PROT-CS-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Test Protocol Communication Service for OITF

Specification Section(s)	[PROT] §5.5.1.4
Test Cases	• Verifies OITF supports the sending of HNI-IGI Pending IG request without an ongoing SIP dialogue • Verifies OITF supports the sending of HNI-IGI Pending IG request without an ongoing SIP dialogue • Verifies OITF supports the refreshing of HNI-IGI PENDING_IG request by the reception of a HTTP OK from the IG • Verifies OITF supports the refreshing of HNI-IGI PENDING_IG request by the resending of HNI-IGI PENDING_IG • Verifies OITF supports the sending of HNI-IGI SIP Request to terminate the session • Verifies OITF supports the reception of HTTP 200 OK response after the sending of a HNI IGI SIP Request to terminate the session (a SIP bye) • Verifies OITF supports the sending of a HNI IGI SIP Request to terminate the session (a SIP SUBSCRIBE (with X-OITF-Expiry set to 0) • Verifies OITF supports the reception of HTTP 200 OK response from the IG as a result of cancelling of HNI-IGI PENDING_IG request when there exists an outstanding HNI-IGI PENDING_IG request a HNI IGI SIP Request to terminate the session (a SIP SUBSCRIBE (with X-OITF-Expiry set to 0)
Preconditions	• Test Object should be connected to reference IG and reference managed network.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-CS-002
Test Specification Version	1.0.0
Test Object(s)	IG
Test Specification Description	Test Protocol Communication Service for IG
Specification Section(s)	[PROT] §5.5.1.4
Test Cases	• Verifies IG supports setting up a pending HNI-IGI PENDING_IG request without an ongoing SIP dialogue • Verifies IG supports responding to a pending HNI-IGI PENDING_IG request without an ongoing SIP dialogue • Verifies IG supports the refreshing of HNI-IGI PENDING_IG request • Verifies IG supports the cancelling of HNI-IGI PENDING_IG request due to disconnection of TCP connection • Verifies IG supports the cancelling of HNI-IGI PENDING_IG request due to TCP time out • Verifies IG supports the cancelling of HNI-IGI PENDING_IG request with an outstanding HNI-IGI PENDING_IG request an HNI-IGI SIP Request to terminate the session • Verifies IG supports the response to cancelling of HNI-IGI PENDING_IG request with an outstanding HNI-IGI PENDING_IG request an HNI-IGI SIP Request to terminate the session • Verifies IG supports the cancelling of HNI-IGI PENDING_IG request with an outstanding HNI-IGI PENDING_IG request a HNI IGI SIP Request to terminate the session (a SIP SUBSCRIBE (with X-OITF-Expiry set to 0) • Verifies IG supports the response to cancelling of HNI-IGI PENDING_IG request with an outstanding HNI-IGI PENDING_IG request a HNI IGI SIP Request to terminate the session (a SIP SUBSCRIBE (with X-OITF-Expiry set to 0).
Preconditions	• Test Object should be connected to Reference OITF and reference managed network.

Priority	Mandatory
Remark	

5.3.4.7.2 Caller ID

Test Specification ID	OIPF-PROT-CID-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Test Protocol Caller ID for OITF
Specification Section(s)	[PROT] §5.4.1.1.1, [PROT] §5.4.1.2.1
Test Cases	• Verifies OITF support receiving Caller ID in an instant message (SIP MESSAGE) on the HTTP PENDING_IG response • Verifies OITF support responding to the reception of Caller ID in an instant message (SIP MESSAGE) with a HTTP POST • Verifies OITF supports receiving Caller ID as part of an incoming call (SIP INVITE) on the HTTP PENDING_IG response • Verifies OITF supports the response of receiving Caller ID as part of an incoming call (SIP INVITE) with an HTTP POST
Preconditions	• Test Object should be connected to reference IG and reference managed network.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-CID-002
Test Specification Version	1.0.0
Test Object(s)	IG
Test Specification Description	Test Protocol Caller ID for IG
Specification Section(s)	[PROT] §5.4.1.1.1, [PROT] §5.4.1.2.1
Test Cases	• Verifies IG supports receiving Caller ID in an instant message (SIP MESSAGE) • Verify IG supports forwarding to the OITF the received Caller ID from an incoming call (SIP INVITE) • Verify IG supports forwarding to the OITF the received Caller ID from an incoming call (SIP INVITE). • Verify IG supports forwarding to the OITF the received Caller ID from an incoming call (SIP INVITE)
Preconditions	• Test Object should be connected to Reference OITF and reference managed network.
Priority	Mandatory
Remark	

5.3.4.7.3 Instant Message

Test Specification ID	OIPF-PROT-IM-001
Test Object(s)	OITF
Test Specification Description	Test Protocol Instant Message for OITF
Specification Section(s)	[PROT] §5.4.2.2
Test Cases	• Verifies OITF supports receiving instant message (SIP MESSAGE) on the HTTP PENDING_IG response • Verifies OITF supports responding to the reception of instant message (SIP MESSAGE) on the HTTP PENDING_IG response with a HTTP POST
Preconditions	• Test Object should be connected to reference IG and reference managed network.

Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-IM-002
Test Specification Version	1.0.0
Test Object(s)	IG
Test Specification Description	Test Protocol Instant Message for IG
Specification Section(s)	[PROT] §5.4.2.2
Test Cases	• Verifies IG supports receiving instant message (SIP MESSAGE) • Verifies IG supports forwarding the instant message (SIP MESSAGE) to OITF
Preconditions	• Test Object should be connected to Reference OITF and reference managed network.
Priority	Mandatory
Remark	

5.3.4.7.4 Chat using MSRP

Test Specification ID	OIPF-PROT-CHAT-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Test Protocol Chat using MSRP for OITF
Specification Section(s)	[PROT] §5.4.3
Test Cases	• Verifies OITF supports initiating MSRP based chat session by the sending of HTTP POST • Verifies OITF supports reception of HTTP 200 OK as the response to the initiation of MSRP based chat session • Verifies OITF supports sending of the HTTP PENDING_IG as a final response to the initiating MSRP based chat session • Verifies OITF supports the reception of MSRP based chat session initiation message • Verifies OITF supports responding to MSRP based chat session initiation message with an HTTP POST to the IG • Verifies OITF supports the reception of the SIP ACK resulting from MSRP based chat session initiation message • Verifies OITF supports sending MSRP based chat message • Verifies OITF supports receiving the response to sending MSRP based chat message • Verifies OITF supports receiving MSRP based chat message • Verifies OITF supports sending the response to receiving MSRP based chat message • Verifies OITF supports sending a chat status message • Verifies OITF supports receiving the response to sending a chat status message • Verifies OITF supports terminating a chat session • Verifies OITF supports the response to requesting terminating a chat session
Preconditions	• Test Object should be connected to reference IG and reference managed network.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-CHAT-002
Test Specification Version	1.0.0
Test Object(s)	IG
Test Specification Description	Test Protocol Chat using MSRP for IG
Specification Section(s)	[PROT] §5.4.3
Test Cases	• Verifies IG supports receiving MSRP based chat session initiation from OITF over HNI-IGI • Verifies IG supports the response to receiving MSRP based chat session initiation from OITF over HNI-IGI • Verifies IG supports the initiating (SIP INVITE) of the chat session towards the remote user • Verifies IG supports the response of initiating (SIP INVITE) of the chat session towards the remote user • Verifies IG supports sending the chat invitation to the OITF • Verifies IG supports sending the received chat initiation message from the OITF to the reference managed network • Verifies IG supports receiving the response to sending the received chat initiation message from the OITF to the reference managed network • Verifies IG supports the receiving the chat message from the OITF • Verifies IG supports the response to receiving the chat message from the OITF • Verifies IG supports receiving a chat message from the OITF and sending a chat message (MSRP) to the remote user • Verifies IG supports the acknowledgment of sending a chat message (MSRP) to the remote user • Verifies IG supports sending a chat status message (MSRP SEND ACTIVITY) to the remote user • Verifies IG supports receiving the response to sending a chat status message (MSRP SEND ACTIVITY) to the remote user • Verifies IG supports receiving a chat status message from the OITF • Verifies IG supports the response to receiving a chat status message from the OITF • Verifies IG supports receiving a chat message (MSRP SEND) from the remote user • Verifies IG supports the response to receiving a chat message (MSRP SEND) from the remote user • Verifies IG supports sending the received chat message to the OITF • Verifies IG supports the response of sending the received chat message to the OITF • Verifies IG supports receiving a chat status message (MSRP RECEIVE ACTIVITY) from the remote user • Verifies IG supports responding to the receiving a chat status message (MSRP RECEIVE ACTIVITY) from the remote user • Verifies IG supports sending the received chat status message to the OITF • Verifies IG supports the response to sending the received chat status message to the OITF • Verifies IG supports receiving a termination of a chat session from the remote user • Verifies IG supports the response to forwarding a termination of a chat session from the remote user • Verifies IG supports receiving a termination of a chat session from the OITF • Verifies IG supports the response to receiving a termination of a chat session from the OITF • Verifies IG supports sending termination of a chat session to the remote user

	• Verifies IG supports the response to sending termination of a chat session to the remote user
Preconditions	• Test Object should be connected to Reference OITF and reference managed network.
Priority	Mandatory
Remark	

5.3.4.7.5 Presence

Test Specification ID	OIPF-PROT-PRES-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Test Protocol Presence for OITF
Specification Section(s)	[PROT] §5.4.4
Test Cases	• Verifies OITF supports subscribing to a presence event • Verifies OITF supports the receiving the response to subscribing to a presence event • Verifies OITF supports receiving a notification for the subscribed event • Verifies OITF acknowledges the receiving of a notification for the subscribed event • Verifies OITF supports cancelling subscription to a presence event • Verifies OITF supports the receiving the response to cancelling a presence event • Verifies OITF supports refreshing the subscription to a presence event • Verifies OITF supports the receiving the response to refreshing the subscription to a presence event • Verifies OITF supports publishing presence information • Verifies OITF supports receiving the response to publishing presence information • Verifies OITF supports refreshing the publish presence information periodically • Verifies OITF supports receiving the response to refreshing the publish presence information periodically
Preconditions	• Test Object should be connected to reference IG and reference managed network.
Priority	Mandatory
Remark	

Test Specification ID	OIPF-PROT-PRES-002
Test Specification Version	1.0.0
Test Object(s)	IG
Test Specification Description	Test Protocol Presence for IG
Specification Section(s)	[PROT] §5.4.4
Test Cases	• Verifies IG supports receiving a HNI-IGI request for subscribing to a presence event (OITF→IG) • Verifies IG supports the response for receiving a HNI-IGI request for subscribing to a presence event (OITF→IG). • Verifies IG supports initiating a subscription (SIP SUBSCRIBE) for a presence event • Verifies IG supports the acknowledgment to initiating a subscription (SIP SUBSCRIBE) for a presence event • Verifies IG supports receiving a notification (SIP NOTIFY) of a presence event

	• Verifies IG supports responding to a notification (SIP NOTIFY) of a presence event • Verifies IG supports sending a notification of a received presences event on the HNI-IGI interface (IG→OITF) • Verifies IG supports cancelling subscription to a presence event (OITF→IG) • Verifies IG supports the response of cancelling subscription to a presence event (OITF→IG) • Verifies IG supports the response of cancelling subscription to a presence event (IG→Network) • Verifies IG supports the response of cancelling subscription to a presence event (IG→Network) • Verifies IG supports refreshing subscription to a presence event (OITF→IG) • Verifies IG supports the response to refreshing subscription to a presence event (OITF→IG) • Verifies IG supports refreshing subscription to a presence event and (IG-Network) • Verifies IG supports the response from refreshing subscription to a presence event (IG-Network) • Verifies IG supports publishing presence information (OITF→IG) • Verifies IG supports the response of publishing presence information (OITF→IG) • Verifies IG supports publishing presence information and (IG→Network). • Verifies IG supports the response of publishing presence information (IG→Network)
Preconditions	• Test Object should be connected to Reference OITF and reference managed network.
Priority	Mandatory
Remark	

5.3.4.8 Content on Demand

5.3.4.8.1 Managed Model

Test Specification ID	OIPF-PROT-CoD-001
Test Specification Version	1.0.0
Test Object	OITF, IG
Test Specification Description	Test Protocol for Content on Demand Managed Model
Specification Section(s)	[PROT] §5.2.2.1, [PROT] §5.2.2.1.2, [PROT] §6.2.2.1.2
Test Cases	• Validates OITF supports retrieval of missing parameters to form SDP (FEC info including bandwidth or Transport Protocol). OITF sends HTTP POST request. • Validates OITF supports retrieval of missing parameters to form SDP (FEC info including bandwidth or transport Protocol). OITF receives the response for the HTTP Post request. • Validates OITF supports HNI-IGI session initiation - OITF sends HTTP POST. • Validates OITF supports HNI-IGI session initiation. OITF receives response to HTTP POST (HTTP 200 OK). • Validates OITF supports HNI-IGI session initiation. OITF sends HTTP Pending Request to acknowledge the final response • Validates OITF supports HNI-IGI session refresh. • Validates OITF supports HNI-IGI session termination. - OITF sends HTTP POST • Validates OITF supports HNI-IGI session termination. OITF receives

	response to HTTP POST request to terminate session - HTTP 200 OK. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Streaming is done with MPEG2TS over RTP/UDP. OITF receives content encapsulated in the RTP packets. o Media stream is protected. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Streaming is done with MPEG2TTS over RTP/UDP. OITF receives content encapsulated in the RTP packets. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Streaming is done with MPEG2TS over UDP. OITF receives content encapsulated in the UDP packets. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Streaming is done with MPEG2TTS over UDP. OITF receives content encapsulated in the UDP packets. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Streaming is done with MPEG2TS over RTPUDP. OITF receives content encapsulated in the RTP packets. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Streaming is done with MPEG2TTS over RTPUDP. OITF receives content encapsulated in the RTP packets. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Check Media stream is protected. • Validates OITF supports session initiation - HTTP POST o Check HTTP Request Header, HTTP Request Body with SDP Parameter for RTSP control channel and SDP parameter for the content delivery channel. o Check multiple media stream to be protected or single media stream protected by multiple FEC stream • Validates OITF supports modify playback • Validates OITF supports pause playback.. • Validates OITF supports handling of media control for retrieving playback information. - OITF supports RTSP GET_PARAMETER. • Validates OITF supports RTSP commands - OITF receives RTSP 200 OK response message from reference CDF. • Validates OITF supports handling the Beginning and Ending of stream. – OITF receiving of RTSP ANNOUNCE “2101” End of Stream Reached from reference CC/CDF.

	• Validates OITF supports handling the Beginning and Ending of stream. - OITF receiving of RTSP ANNOUNCE “2101” End of Stream Reached from reference CC/CDF - OIFT sends RTSP 200 OK. • Validates OITF supports Session refresh HNI-IGI session refresh. • Check refresh message (HTTP Pending_IG) from OITF to reference IG, and check response for refreshing (HTTP status code) from reference IG to OITF • Verify Test Object sends refresh messages periodically to keep alive the session successfully. • Validates IG supports retrieval of missing session parameters to form SDP - IG Receives HTTP Post • Validates IG supports retrieval of missing session parameters to form SDP - Send SIP OPTION to reference network • Validates IG supports retrieval of missing session parameters to form SDP - Receiving SIP 200 OK Response Message from the reference network • Validates IG supports retrieval of missing session parameters to form SDP - The IG forwards the SIP 200 OK info to the OITF by sending a 200 OK HTTP • Validates IG Support the CoD Retrieval HTTP POST - Validation Unsuccessful • Validates IG Support the CoD Retrieval HTTP POST - Validation Unsuccessful. IG sends a HTTP non-200 OK message • Validates IG supports session initiation - Receiving HTTP POST from reference OITF • Validates IG supports session initiation - IG send SIP INVITE • Validates IG supports session initiation - IG receives Response to SIP INVITE - SIP 200 OK • Validates IG supports session initiation - IG sends HTTP 200 OK to OITF • Validates IG supports session initiation - Reception of to HTTP Pending Request • Validates IG supports session refresh. Check refresh message (HTTP Pending_IG) from OITF to IG, and check response for refreshing (HTTP status code) from IG to OITF • Validates IG supports session termination - HTTP Post Request to terminate session • Validates IG supports session termination - IG sends SIP BYE to reference network
Preconditions	Test Object(s) should be connected and reference managed network.
Priority	Mandatory
Remark	

5.3.4.8.2 Unmanaged Model

Test Specification ID	OIPF-PROT-CoD-002
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Test Protocol Content on Demand for OITF Unmanaged Model
Specification Section(s)	[PROT] §5.2.2.2.2, [PROT] §7.1.1.1.1, [PROT] §7.1.1.1.2, [PROT] §7.1.1.1.3
Test Cases	• Verify OITF support HTTP Progressive Streaming • Verify OITF support RTSP Streaming - Session Set-up - OITF sends RTSP Describe message • Verify OITF support RTSP Streaming - Session Set-up - OITF receives RTSP 200 OK response • Verify OITF support RTSP Streaming - RTSP SETUP Message • Verify OITF support RTSP Streaming - OITF Receives response to RTSP SETUP (RTSP 200 OK Message)

	• Verify OITF support RTSP Streaming - OITF send RTSP PLAY and PAUSE • Verify OITF support RTSP Streaming - OITF receives RTSP 200 OK response to the RTSP PLAY and PAUSE message • Verify OITF support RTSP Session Teardown - OITF send RTSP TEARDOWN • Verify OITF support RTSP Session Teardown - OITF receives RTSP 200 OK response from reference CC/CDF. • Verify OITF supports RTSP GET PARAMETER Message • Verify OITF supports RTSP GET PARAMETER Response Message - OITF receives RTSP 200 OK • Verify OITF supports RTSP ANNOUNCE Message • Verify OITF supports RTSP ANNOUNCE Response Message - OITF receives RTSP 200 OK • Verify OITF supports RTSP OPTIONS Message • Verify OITF supports RTSP OPTION Response Message - OITF receives RTSP 200 OK • Verify OITF supports receiving RTSP 301 Response message • Verify OITF supports receiving RTSP 302 Response message • Verify OITF supports receiving RTSP 4xx Response message • Verify OITF supports receiving RTSP 2xx Response message
Preconditions	Test Object should be connected to reference network.
Priority	Mandatory
Remark	

5.3.4.9 Content Download

Test Specification ID	OIPF-PROT-CoD-003
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Test Protocol for Content Download for OITF
Specification Section(s)	[PROT] §5.2.3
Test Cases	• Verify OITF support Content Download. OITF sends HTTP GET with the Range HTTP Header
Preconditions	Test Object should be connected to reference IG and reference managed network.
Priority	Mandatory
Remark	

5.4 Declarative Application Environment (DAE)

The scope of DAE testing falls into two basic areas as described below.

- Basic test for browser supporting the DAE environment. This refers to the top-level presentation capabilities of the browser
  - W3C technologies like XHTML and CSS
  - Other browser-based technologies such as CE-HTML.
- DAE specification test (inclusive of specific services that can be invoked from the browser)
  - Streaming
  - Download and Playback
  - Channel List and Channel Switch
  - PVR
  - Remote UI
  - Metadata and Application
  - IMS APIs

5.4.1 Prerequisites

The prerequisites required before testing the DAE are to check compliance with W3C and CEA-2014-A.

5.4.1.1 CEA-2014-A tests applicable for OIPF testing of the Remote User Interface

Configuration information that details the type of configurations that may be tested are:

- UI Control Point
- 3-Box model
- Box Model
- 2-Box model

Test materials for testing of Remote UI Client and Remote UI Server implementations with UI profiles (at default resolution settings) as defined in CEA-2014-A such as:

HD_UIPROF	High Definition UI profile
SD_UIPROF	Standard Definition UI profile
MD_UIPROF	Mobile Device UI profile

OIPF defines additional profiles, and these need to be tested in addition to the CEA tests.

OITF_SDEU_UIPROF	SD
OITF_SD60_UIPROF	
OITF_SDUS_UIPROF	
OITF_HD_UIPROF	
OITF_FULL_HD_UIPROF	

5.4.1.1.1 Conventions

R	Required
O	Optional
S	Should (recommended)
CR	Conditionally Required
	Not required, not applicable

5.4.1.1.2 Mandated sections of the CEA-2014-A specification

The following sections are indicated in [DAE] (section 4.1) as mandatory for OIPF terminals with respect to the i-box guidelines. Note that changes described in section 10.2 of [DAE] can have additional guidelines.

- 5.1.2
- 5.2
- 5.3
- 5.4
- 5.5
- 5.6
    - 5.6.1
- 5.7
    - 5.7.1
    - 5.7.3
- 5.8
- 5.9
- 5.10

To provide a complete overview, all sections of the CEA-2014-A test specification are listed.

However, the DAE specification also indicates that all of CEA-2104-A can be implemented as an optional feature.

5.4.1.1.3 CEA-2014-A Remote UI Server and Client Types

Each Remote UI Client or Server type is denoted by a *level*, and the following levels have been defined:

- **Level 0** - a Remote UI Client or Server type which is not discoverable in a UPnP network
- **Level 1** - a Remote UI Client or Server type which is discoverable in a UPnP network, and can be controlled by an (external) UI Control Point through HTTP commands
- **Level 2** - a Level 1 type Remote UI Client or Server which adds optional support for SOAP-based invocation of UPnP actions.

5.4.1.1.4 Test Guidelines Overview

The following tables in this document list the CEA-2014-A test cases that need to be tested for an OIPF compliant device. These selected test cases need to be executed as a pre-requisite for OIPF certification (based on the OIPF profile supported).

The table needs to be read as follows:

- Column 1: CEA-2014-A Test Specification test case number.
- Column 2, 3 and 4: Mentions if that particular test case is a mandatory or optional requirement for a CEA-2014-A Remote UI Client (Level 0, Level 1 and Level 2)
- Column 5, 6 and 7: Mentions if that particular test case is a mandatory or optional requirement for a CEA-2014-A Remote UI Server (Level 0, Level 1 and Level 2)
- Column 8: Mentions if that particular test case is a mandatory or optional requirement for a CEA-2014-A UI Control Point
- Column 9, 10 and 11: Mentions if that particular test case is a mandatory or optional requirement for a OIPF Profile (OIP, BMP and EMP)
- Column 12: Gives the description of the test case.

Some tables have an additional column “OIPF Annex B changes”. This column mentions if the particular test case has any modification in [DAE] Annex B.

5.4.1.1.5 CEA-2014-A Section 5.1.1

The test cases mentioned for this section are optional, since these are the CEA-2014-A specific discovery mechanisms that are optional in OIPF.

Note: [DAE] section 4.1.1 indicates that the XML UI listing is being used in an AG device. This means that the control point requirements on the XML UI listing should also be used by an OIPF device that is interacting with an AG device.

Note: [PROT] section 10 also contains UPnP based mechanism; so some of the practice of these tests could be used to define tests for the guidelines in this chapter.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.1.1.a				R	R	R		O	O	O	Requires Remote UI Servers support either Level 0, 1 or 2 requirements.
5.1.1.b					O	O		O	O	O	Indicates Remote UI Servers may also support UPnP CDS discovery mechanisms.
5.1.1.1.a				R				O	O	O	Requires Remote UI Servers reside on internet domain
5.1.1.1.b				R				O	O	O	Requires Remote UI Servers provide a URL to an XML UI Listing
5.1.1.2.a					R	R		O	O	O	Requires Remote UI Servers be discoverable via UPnP.
5.1.1.2.b					R	R		O	O	O	Requires Remote UI Servers include a <uiServerInfo> element in its UPnP Device Description.
5.1.1.2.c					R	R		O	O	O	Describes how Remote UI Servers provide a URL to retrieve an XML UI Listing.
5.1.1.2.d					R			O	O	O	Requires Remote UI Servers use *urn:schemas-ce-org:* device and service types.
5.1.1.2.e					R	R		O	O	R	Requires Remote UI Servers list Remote UI UPnP multicast notification state variables.
5.1.1.3.a						R		O	O	O	Requires Level 2 Remote UI Servers support Level 1 Remote UI Server requirements (excluding device/service names).
5.1.1.3.b						R		O	O	O	Requires Remote UI Servers use *urn:schemas-upnp-org:* device/service types.
5.1.1.3.c						R		O	O	O	Requires Remote UI Servers comply with UPnP Remote UI Server specifications. Clarifies delivery of XML UI Listing for UPnP Remote UI compliant servers.

5.4.1.1.6 CEA-2014-A Section 5.1.1.4 Content Directory Service

Not applicable in OIPF Terminal testing.

Note: Requirements are applicable to RUI servers which support advertising RUI applications via the UPnP ContentDirectory service.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.1.1.4.a					O	O		O	O	O	Indicates Remote UI servers can advertise Remote UI applications via UPnP CDS service. Requires UPnP device to be DLNA compliant.
5.1.1.4.b					R	R		O	O	O	Describes Remote UI Server encapsulation of XML UI elements within UPnP CDS <item> elements.
5.1.1.4.c					R	R		O	O	O	Describes Remote UI Server encapsulation of XML UI elements within UPnP CDS <item> elements.

5.4.1.1.7 CEA-2014-A Section 5.1.1.5 XML UI Listing

Not applicable in OIPF Terminal testing.

Note: [DAE] section 4.1.1 indicates that the XML UI listing is being used in an AG device. This means that the control point requirements on the XML UI listing also should be used by an OIPF device that is interacting with an AG device.

Also the CEA-2014-A i-Box model is using the XML UI Listing therefore OIPF devices should use these requirements.

Current tests are based on the server side of the XML UI Listing, and therefore apply to the OIPF service. This might change in the future.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.1.1.5.a				R	R	R					Requires XML UI Listings comply with UPnP Remote UI Server specification XML Schema requirements.
5.1.1.5.b				R	R	R					Requires Remote UI Servers provide CE-HTML compliant applications with <uri> elements using *http:* or *https:* transport schemes.
5.1.1.5.c				R	R	R					Requires Remote UI applications in XML UI listing to have a <protocol>-element with *shortname*-attribute of *"CE-HTML-1.0"*.
5.1.1.5.d				R	R	R					Requires <protocolInfo>-element describe the Remote UI application's capability requirements per 5.2.1.e.
5.1.1.5.e				R	R	R					Requires each Remote UI application <uri>-element to have a corresponding <profilelist>-element which provides the capability requirements of the served-up application.
5.1.1.5.f				R	R	R					Requires Remote UI Servers provide a "filtered" XML UI listing based on Remote UI client capabilities provided in the http-get request's User-Agent header.
5.1.1.5.g				R	R	R					Requires Remote UI Servers not generate an XML UI Listing exceeding 64KB.

5.4.1.1.8 CEA-2014-A Section 5.1.1.6 Embedded/Non-embedded UI ControlPoint Requirements

Not applicable in OIPF Terminal testing.

UPnP control point requirements.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.1.1.6.a							R	O	O	O	Requirement states UI Control Points will adhere to HTTP requirements of Sec 5.3 when fetching XML UI Listings.
5.1.1.6.b							R	O	O	O	Requirements states UI Control Points insure Remote UI Client capabilities match the target Remote UI Servers URL when commanding a connection.

5.4.1.1.9 CEA-2014-A Section 5.1.2 General Remote UI Client Requirements

UPnP control point side requirements.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.1.2.a	R	R	R					R	R	R	Requires Remote UI Clients support either Level 0, 1 or 2 Remote UI Client requirements.
5.1.2.b	R	R	R					R	R	R	Requires Remote UI Clients that can connect to an i-Box Remote UI Server support the https: scheme and SSL or TLS encryption.
5.1.2.c	R	R	R					R	R	R	Requires Remote UI Clients support Remote UIs that are offered through <protocol> elements with a *shortname*-attribute of CE-HTML-1.0.
5.1.2.c	S	S	S					O	O	O	Requires Remote UI Clients should support <protocol>-elements with a *shortname*-attribute of *CE-HTML-1.0_SAVED* per section 5.8.
5.1.2.d	O	O	O					O	O	O	Requirement indicates Remote UI Clients may support Remote UIs that are offered through <protocol>-elements with a *shortname*-attribute of *XRT*.
5.1.2.e	O	O	O					O	O	O	Requirement indicates Remote UI Clients may support Remote UIs that are offered through <protocol>-elements with a *shortname*-attribute of *URC-HTTP*.
5.1.2.f	O	O	O					O	O	O	Requirement indicates that Remote UI Clients may support other UI protocols.
5.1.2.2.a		R	R					O	O	O	Requires Remote UI clients include a <uiClientInfo> Remote UI Client capabilities element their UPnP Device Description.
5.1.2.2.b		R						O	O	O	Requires Remote UI clients use *urn:schemas-ce-org:* device and service types.
5.1.2.2.c		R	R					O	O	O	Requires Remote UI clients accept connection commands from UI Control Points.
5.1.2.2.d		R	R					O	O	O	Describes how Remote UI Clients are required to return results of connection requests issued from UI Control Points.
5.1.2.2.e		R	R					O	O	O	Describes how Remote UI Clients are required to handle failed connection requests from UI Control Points.
5.1.1.2.f		R	R								Requires Remote UI Clients accept disconnect commands from UI Control Points. Describes how Remote UI clients are required to handle failed disconnects requests.
5.1.2.3.a			R					O	O	O	Requires Level 2 Remote UI Clients support Level 1 Remote UI Client requirements excluding device/service names.
5.1.2.3.b			R					O	O	O	Requires Remote UI Servers use *urn:schemas-upnp-org:* device and service types.
5.1.2.3.c			R					O	O	O	Requires Level 2 Remote UI Clients comply with UPnP Remote UI Client specifications. Clarifies support of required UPnP Remote UI actions.

5.4.1.1.10 CEA-2014-A Section 5.1.2.4 Non-embedded UI Control Point Requirements

This section lists requirements of UPnP control points that discover remote UI clients on the home network. This is optional for i-box models, but [DAE] states that an OIPF terminal can optionally implement this feature. When this feature is implemented, all test cases listed in this section must be executed successfully.

Conditionally required for OIPF terminal testing.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.1.2.4.a							R	CR	CR	CR	Requires non-embedded UI Control Points to discover Level 1 and Level 2 Remote UI Clients.
5.1.2.4.b							R	CR	CR	CR	Requires non-embedded UI Control Points issue connection commands to Remote UI Clients as described in 5.1.2.2.c. Requires UI Control point to do Remote UI application capability matching on behalf of the Remote UI Client.
5.1.2.4.c							O	O	O	O	Requirement states UI Control Points may include a <profilelist>-element when commanding a connection.

5.4.1.1.11 CEA-2014-A Section 5.2 Capability Exchange

Mandatory for OIPF terminal testing.

Note that the RUIS server requirements can be applied to OIPF services, but are not identified in the table.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.2.1.a	R	R	R					R	R	R	Yes	Requirement describes usages of Remote UI Client capability elements in Remote UI Client capability description. Defines how Remote UI Client may extend pre-defined UI profile capabilities.
5.2.1.b	R	R	R					R	R	R	Yes	Requirement defines Remote UI Client named UI profiles. States the minimum capability settings for each pre-defined UI profile.
5.2.1.c	S	S	S					O	O	O		Requirement states Remote UI Clients should include audio and video profile capability elements based on DLNA media profiles.
5.2.1.d	CR	CR	CR					R	R	R		Requires Remote UI Clients that support DLNA audio or video profile capabilities support http streaming.
5.2.1.e				R	R	R						Requirement describes how Remote UI Servers are required to structure XML UI Listings.
5.2.1.f				R	R	R						Require a Remote UI Server to support the SD_UIPROF profile with no extensions.

5.2.1.g				S	S	S						Recommends Remote UI Servers publish multiple versions of each Remote UI application with different UI profiles.
5.2.2.a	R	R	R					R	R	R		Requires Remote UI Clients connecting to a Remote UI application to select one of the named UI profiles the application supports and to provide the named profile during connection.
5.2.2.b	R	R	R					R	R	R		Requires Remote UI Clients connecting to a Remote UI application indicate it supports the audio and video profiles required by the Remote UI Server application.
5.2.2.c				R	R	R						Requires Remote UI Servers return Remote UI content matching the Remote UI client's capabilities provided during connection, and to return an error if it cannot supply matching content.
5.2.2.d	R	R	R					R	R	R		Requires Remote UI Clients not change their capabilities while connected to a Remote UI Server.
5.2.2.e				R	R	R						Requires Remote UI Servers insure any content linked to by a CE-HTML page will also match the connecting Remote UI client capabilities.
5.2.2.f				S	S	S						Requires a Remote UI Servers insure any content linked to by a CE-HTML page conforms to MIME-types listed in this requirement.
5.2.2.g	R	R	R					R	R	R		Requires Remote UI Clients replace browser windows contents due to: following a link, submitting a form or changing the location of an <iframe>-element.
5.2.2.h	R	R	R					R	R	R		Requires a Remote UI Clients support a "*Back*" Browser button. Requires Remote UI Clients take into account changes to a window object's location property.
5.2.2.i				R	R	R						Describes required behaviour for Remote UI Servers which are unable to provide Remote UI content that matches the connecting Remote UI client's capabilities.

5.2.2.j	O	O	O					O	O	O		States a Remote UI Client may attempt to recover from a failed connection (due to no matching content) by attempting to connect to the SD_UIPROF version of the Remote UI Server application.

5.4.1.1.12 CEA-2014-A Section 5.2.3 Browser Area

General requirements on the browser area. Section referred to as mandatory in OIPF.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.2.3.a	O	O	O					O	O	O	Requirement states Remote UI Client rules for scaling of Remote UI content smaller or equal to the Remote UI Clients advertised capabilities.
5.2.3.b	S	S	S					O	O	O	Requirement states Remote UI Client rules for scrolling/cropping of Remote UI content larger than the Remote UI Clients advertised capabilities.
5.2.3.c	R	R	R					R	R	R	Requires Remote UI Clients map content with absolute positions using the stated size of the Remote UI Clients browser area.
5.2.3.d	R	R	R					R	R	R	Requires Remote UI Clients browser area to be visible at all times.
5.2.3.e	S	S	S					O	O	O	Requires Remote UI Clients use square-pixels. Requires Remote UI Clients preserve the aspect ratio of content..
5.2.3.f	O	O	O					O	O	O	Indicates that Remote UI Clients may use screen area outside of the Browser area for their own purposes.

5.4.1.1.13 CEA-2014-A Section 5.3 Http Headers

Section indicated as Mandatory for OIPF terminal testing.

Note that some Server tests can be used for OIPF services, but are not identified in the table.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.3.a	R	R	R	R	R	R		R	R	R	Yes	Requirement indicates Remote UI Clients and Remote UI Servers support the listed http request/response headers. Defines CEA-2014-A specific usage of http headers.
5.3.b	R	R	R					R	R	R		Requires Remote UI Clients support HTTP Cookie headers, and recommends support for HTTP Refresh header.
5.3.c				R	R	R						Requirement indicates optional Remote UI Server support for HTTP Cookie headers.
5.3.d	O	O	O					O	O	O		Requirement indicates optional Remote UI Client support for

												Content-* headers.
5.3.e	R	R	R	R	R	R		R	R	R		Requirement indicates Remote UI Clients and Remote UI Servers are required to conform to DLNA media transport guidelines for connections involving DLNA AV media types.
5.3.e	R	R	R	R	R	R	R	R	R	R		Requirement indicates Remote UI Clients, Remote UI Servers and UI Control Points are required to ignore unsupported HTTP headers.
5.3.g	R	R	R					R	R	R		Defines Remote UI Clients requirements for HTTP persistent connection timeouts.
5.3.h	R	R	R	R	R	R	R	R	R	R		Requirement set limits on aggregate header data length generated by Remote UI Clients and Remote UI Servers.
5.3.i	R	R	R	R	R	R	R	R	R	R		Requirement sets limits on individual header lines generated by Remote UI Clients and Remote UI Servers.
5.3.j	R	R	R	R	R	R	R	R	R	R		Requirement sets maximum allowable integer value for use in Remote UI Client and Remote UI Server headers.

5.4.1.1.14 CEA-2014-A Section 5.4 XHTML profile (CE-HTML)

Mandatory for OIPF terminal testing.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.4.a-1	R	R	R					R	R	R		Requires Remote UI Clients support and Remote UI applications conform to XHTML 1.0 Strict or Transitional, with stated extensions and restrictions.
5.4.a-2	R	R	R					R	R	R		Requires Remote UI Clients support and Remote UI applications conform to ECMA-262 (ECMAScript 3rd edition).
5.4.a-3.a	R	R	R					R	R	R	Yes	Requires Remote UI Clients support and Remote UI applications conform to DOM level 2 Core
5.4.a-3.b	R	R	R					R	R	R		Requires Remote UI Clients support and Remote UI applications conform to DOM level 2 Style, with stated restrictions.
5.4.a-3.c	R	R	R					R	R	R	Yes	Requires Remote UI Clients support and Remote UI applications conform to DOM

												level 2 Events, with stated extensions.
5.4.a-3.d 5.4.a-3.e	R	R	R					R	R	R	Yes	Requires Remote UI Clients support and Remote UI applications conform to DOM level 2 HTML, with stated extensions and restrictions.
5.4.a-4								n/a	n/a	n/a	n/a	Reference to CEA-2014-A scripting object interfaces defined in other sections.
5.4.a-5	R	R	R	O	O	O		R	R	R		Requirement defines ECMAscript access to element properties using format: document.[*element-id].[property]*.
5.4.a-6	R	R	R					R	R	R	Yes	Requirement refers to W3C recommendations for resolving conflicting name and id element attributes.
5.4.a-7	R	R	R	R	R	R		R	R	R	Yes	Requires Remote UI Clients support and Remote UI applications conform to CSS TV Profile 1.0 (a variant of CSS 2.0), with stated extensions and restrictions.
5.4.a-8	R	R	R					R	R	R		Requires Remote UI Clients to support and Remote UI applications to conform to the given image formats.
5.4.a-9	R	R	R					R	R	R		Requirement defines CEA-2014-A specific <op>-element which a Remote UI Client expands to a custom name string for a VK_* key.

5.4.1.1.15 CEA-2014-A Section 5.4.1 Key Events

Mandatory for OIPF terminal testing.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.4.1.a	R	R	R					R	R	R	Yes	Requirement defines extension to DOM level 2 Events for keydown, keyup and keypress events. Requirement also defines key code literal constants (VK_*) for use in ECMAScript.
5.4.1.b	R	R	R					R	R	R		Requires Remote UI Clients generate key events for an element with input-focus for all keys indicated in the Remote UI client capabilities.
5.4.1.c	R	R	R					R	R	R		Requirement directs key events to the window object if no element has input focus.
5.4.1.d	R	R	R					R	R	R		Requires key events be “bubbled” consistent with DOM level 2 Event. Defines the Window object

												as target if key event is not handled by a DOM tree node's EventListener.
5.4.1.e	R	R	R					R	R	R		Requirement states not to generate key event for keys associated with forms element(s) input management such as (VK_CLEAR, VK_BACKSPACE, etc).
5.4.1.f	R	R	R					R	R	R	Yes	Requirement defines Remote UI Client requirements for handling navigation keys within form element input fields.
5.4.1.g	R	R	R					R	R	R		Requirement defines Remote UI Client special key event handling of VK_ENTER on form elements.
5.4.1.h	R	R	R					R	R	R		Requirement defines Remote UI Client special key event handling for button elements within a form.
5.4.1.i	R	R	R					R	R	R		Requires Remote UI Clients be capable of generating a full set of alpha-numeric and punctuation input key events for form element input fields with CSS property *input-format: alpha-numeric*.
5.4.1.j	R	R	R					R	R	R		Requires Remote UI Clients generate numeric input key events for form element input fields with CSS property *input-format: numeric.*
5.4.1.k	R	R	R					R	R	R		Requirement extends *onchange* event for forms elements to generate a change event on every value change.
5.4.1.l	R	R	R					R	R	R		Requires Remote UI Clients implement typematic (key repeat) event behaviour.
5.4.1.m 5.4.1.n	R	R	R					R	R	R	Yes	Requires Remote UI Clients provide key-based navigation to <a>, <area>, <form>, <iframe> and AV Player objects. Defines generation/handling of DOM 2 focus events..
5.4.1.o	R	R	R					R	R	R		Requires Remote UI Clients accept VK_* literal key codes for the value of the accesskey attribute of XHTML element(s).

5.4.1.1.16 CEA-2014-A Section 5.4.2 Window Scripting Object

Mandatory for OIPF terminal testing.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.4.2.a-1								O	O	O	Yes	Requirement defines Remote UI Clients support of required methods and properties of the Window object.
5.4.2.a-1.w	R	O	O					R	R	R	Yes	Requirement summarizes CEA-2027 related window methods and properties. Note: Support of CEA-2027 properties/methods is optional for CEA-2014-A certification.
5.4.2.a-2	R	R	R					R	R	R	Yes	Requirement states Remote UI Clients treatment of the Window object as a global and identifies “this.” and “” as aliases of the Window object.
5.4.2.a-3	O	O	O					O	O	O	Yes	Requirement defines UIContentFrame as an alias of window for CEA-2027 compatibility. Note: This requirement is CEA-2027 related and is optional for CEA-2014-A certification.
5.4.2.a-4	R	R	R					R	R	R	Yes	Requirement defines Remote UI Clients support of required methods and properties of the Window.location object.
5.4.2.a-5	O	O	O					O	O	O	Yes	Requirement defines Remote UI Clients support of required methods and properties of the Window.history object.
5.4.2.b-1	R	R	R					R	R	R		Requirement defines Remote UI Clients support of required methods and properties of the Window object.
5.4.2.b-2	R	R	R					R	R	R		Requirement summarizes CEA-2027 related window methods and properties. Note: Support of CEA-2027 properties/methods is optional for CEA-2014-A certification.
5.4.2.c-1	R	R	R					R	R	R		Requirement states Remote UI Clients treatment of the Window object as a global and identifies “this.” and “” as aliases of the Window object.
5.4.2.c-2	R	R	R					R	R	R		Requirement defines UIContentFrame as an alias of window for CEA-2027 compatibility. Note: This requirement is CEA-2027 related and is optional for CEA-2014-A certification.

5.4.1.1.17 CEA-2014-A Section 5.5.1 NotifSocket Scripting Object

Mandatory for OIPF terminal testing.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.5.1.a	R	R	R					R	R	R	Requirement defines Remote UI Clients support of properties and methods of NotifSocket scripting object.

5.4.1.1.18 CEA-2014-A Section 5.5.1 XMLHttpRequest Scripting Object

Mandatory for OIPF terminal testing.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.5.2.a	R	R	R					R	R	R	Requirement requires i-Box Model Remote UI Clients support the XMLHttpRequest object.

5.4.1.1.19 CEA-2014-A Section 5.6.1 Multicast Notifications

Required for OIPF terminal testing, See [DAE] chapter 4.1.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.6.1.a-1 to 5.6.1.a-12		R	R		R	R		R	R	R	Requirement(s) defines Remote UI Server and Remote UI Client support of UPnP Multicast events for non i-Box model devices.
5.6.1.a-13		R	R		R	R		R	R	R	Requirement defines support of named UPnP Multicast State variables to send notification messages.
5.6.1.b					S	S		O	O	O	Requirement defines Remote UI Server requirements for retransmission of multicast notification messages.
5.6.1.c					S	S		O	O	O	Requirement defines Remote UI Server requirements control rate of sending unique multicast notification messages.
5.6.1.d					R	R		O	O	O	Requirement defines Level 1 and 2 Remote UI Server requirements UPnP multicast event variables.
5.6.1.e											Requirement defines UPnP Service Description schema changes to support multicast states variables. Obsolete with the publication of UPnP Device Architecture 1.1.

5.4.1.1.20 CEA-2014-A Section 5.6.2 Polling based Notifications

[DAE] Annex B indicates that this section of the CEA-2014-A specification is optional for an OITF (conditional required).

This means that when implemented the test cases must be successfully executed.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.6.2.a – 1.a	R							CR	CR	CR	Yes	Requirement defines method to request Remote UI Client begin/end polling for Remote UI Servers for notifications.
5.6.2.a – 1.b	R							CR	CR	CR	Yes	Requirement indicates Remote UI Clients must provide HTTP headers per Sec 5.3 when polling for notifications.
5.6.2.a – 1.c	R							CR	CR	CR	Yes	Requirement defines format of a Remote UI Server's response to a Remote UI Client's http-get polling request.
5.6.2.b	R							CR	CR	CR		Requirement states Remote UI Client requirements for polling for notifications in the background.
5.6.2.c	R			R				CR	CR	CR		Requirement indicates Remote UI Clients should limit the number of active notification subscriptions.
5.6.2.d	S							O	O	O		Requirement defines method to request Remote UI Client begin/end polling for Remote UI Servers for notifications.
5.6.2.e	S											Requirement indicates Remote UI Clients must provide HTTP headers per Sec 5.3 when polling for notifications.

5.4.1.1.21 CEA-2014-A Section 5.6.3 Notification Content and Window

[DAE] Annex B indicates that this section of the CEA-2014-A specification is optional for an OITF (conditional required).

This means that when implemented the test cases must be successfully executed.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.6.3.a	R							CR	CR	CR	Requirement indicates Remote UI Clients ignore notification messages with identical Notification IDs.
5.6.3.b				R	R	R					Requirement indicates a Remote UI Servers provide CE-HTML compliant content.
5.6.3.c	R	R	R					CR	CR	CR	Requirement indicates Remote UI Client performing http-get to fetch notification URLs provide HTTP headers per Sec 5.3.
5.6.3.d	S	S	S					O	O	O	Requirement indicates Remote UI Clients position notification windows above other displayed content.

5.6.3.e	S	S	S					O	O	O	Requirement defines sizing of notification windows.
5.6.3.f				S	S	S					Requirement defines Remote UI Servers handling of the <notificationscripts> Remote UI Client capability element.
5.6.3.g	S	S	S					O	O	O	Requirement defines Remote UI Client handling of _blank attribute in <a>, <form> and <area> elements in notification window content.
5.6.3.h	R	R	R					CR	CR	CR	Requirement defines Remote UI Client handling of the _close attribute in <a>. <form> and <area> elements in notification window content..
5.6.3.i	R	R	R					CR	CR	CR	Requirement defines Remote UI Client handling of cancellation of notification messages.

5.4.1.1.22 CEA-2014-A Section 5.7.1 Streamed A/V content

This section applies to CEA-2014-A RUI Clients which optionally support the A/V Player object; however this is required for OIPF terminals.

Note: CEA-2014-A does not define any media format. OIPF mandates a list of media formats.

	RUIC Level			RUIS Level			UICP	OIPF			OIPF Annex B changes	Description
	0	1	2	0	1	2		OIP	BMP	EMP		
5.7.1.a-1	R	R	R					R	R	R		Requirement defines <object> element attributes and child-elements for AV player scripting objects.
5.7.1.a-2	S	S	S					R	R	R		Requirement defines Remote UI Clients DOM HTMLObjectElement interface support for AV Player scripting object.
5.7.1.a-3	S	S	S					R	R	R		Requirement defines Remote UI Clients support for AV Player video window-mode and requirements for scaling of video content.
5.7.1.a-4	R	R	R					R	R	R		Requirement defines Remote UI Clients support of limited set of CSS properties for the AV Player window.
5.7.1.b	R	R	R					R	R	R		Requirement defines Remote UI Clients support opacity/z-index support for XHTML overlays on an AV Player window.
5.7.1.c	R	R	R					R	R	R		Requirement defines Remote UI Clients support of the methods and properties of the AVPlayer object.
5.7.1.d	R	R	R					R	R	R		Requirement defines Remote UI Clients support for AV Player scripting object methods and properties specific to video playback.

5.7.1.e	R	R	R					R	R	R		Requirement indicates Remote UI Clients may position the Browser area anywhere over the AV Player running in fullscreen mode.
5.7.1.f	R	R	R					R	R	R	Yes	Requirement defines Remote UI Client AVPlayer objects handling of navigation keys..
5.7.1.g	R	R	R					R	R	R		Requirement recommends Remote UI Server applications dynamically create AVPlayer objects to avoid patent issues.
5.7.1.h	O	O	O					O	O	O		Requirement defines <object> element attributes and child-elements for AV player scripting objects.
5.7.1.i	R	R	R					R	R	R		Requirement defines Remote UI Clients DOM HTMLObjectElement interface support for AV Player scripting object.
5.7.1.j	O	O	O					O	O	O		Requirement defines Remote UI Clients support for AV Player video window-mode and requirements for scaling of video content.

5.4.1.1.23 CEA-2014-A Section Local video player

This section applies to CEA-2014-A RUI Clients which optionally support the Local Video Player object, which is also optional for OIPF terminals

This means that when implemented the test cases must be successfully executed.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.7.2.a	R	R	R					R	R	R	Requirement defines Remote UI Client support for Local Video Player scripting object.
5.7.2.b	R	R	R					R	R	R	Requirement defines limited set of supported CSS properties for Remote UI Clients Local Video Player scripting object.
5.7.2.c	R	R	R					R	R	R	Requirement defines Remote UI Clients support of XHTML content overlays on Local Video Player.
5.7.2.d	O	O	O					O	O	O	Requirement states Remote UI Clients Local Video Player should not directly or indirectly block execution of CE-HTML scripts.
5.7.2.e	O	O	O					O	O	O	Requirement recommends Remote UI Server applications dynamically create Local Video Player objects to avoid patent issues.

5.4.1.1.24 CEA-2014-A Section 5.7.3 Full screen video

Note: This section applies to CEA-2014-A RUI Clients which support either the A/V Player object or the Local Video Player object; however this is required for OIPF terminals.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.7.3.a	R	R	R					R	R	R	Requirement defines Remote UI Clients handling of full-screen mode for AV Player and Local Video Player scripting objects.
5.7.3.b	R	R	R					R	R	R	Requirement indicates full-screen video objects must cover the entire Remote UI Clients Browser Area.
5.7.3.c	R	R	R					R	R	R	Requirement indicates Remote UI Client will switch to non-full-screen mode when video full-screen objects are no longer visible.
5.7.3.d	O	O	O					O	O	O	Requirement indicates that Remote UI Client may rescale the Browser Area when switching to full-screen mode.

5.4.1.1.25 CEA-2014-A Section 5.8 Save and Restore

All tests are Conditionally Required, e.g. required only when implemented and indicated in the profile.

Note: This section applies to RUI Clients and RUI Servers which support Save-Restore of UI pages.

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.8.a	R	R	R					CR	CR	CR	Requirement describes Remote UI Clients <save-restore> capability element and UI Control Point usage scenarios.
5.8.b	R	R	R					CR	CR	CR	Requirement defines methods and properties of Remote UI Clients Save-Restore scripting object.
5.8.b-1	R	R	R					CR	CR	CR	Requirement indicates Remote UI Servers should provide a URL to accept saved UI information posted from Remote UI clients.
5.8.b-2	R	R	R					CR	CR	CR	Requirement indicates Remote UI Server applications should support the save-restore mechanism by including the save-restore <object> element and scripts necessary to support the save-restore mechanism.
5.8.b-2.c	R	R	R					CR	CR	CR	Requirement describes Remote UI Clients support for UI Control Point save-state requests and the labelling of saved state information.
5.8.c					S	S					Requirement defines Remote UI Servers listing of saved-state information from Remote UI clients.
5.8.d				S	S	S					Requirement defines the Remote UI Servers response to a Remote UI Client request to restore save-state information.
5.8.e		R	R				S				Requirement defines Remote UI Clients support for a UI Control Point to request the Remote UI Client fetch and restore saved-state information.

5.8.f					R	R					Requirement defines Remote UI Clients processing when restoring saved-state information
5.8.f-3						R					Requirement defines request to Remote UI Servers to delete saved-state information.
5.8.g					R	R					Requirement describes Remote UI Clients <save-restore> capability element and UI Control Point usage scenarios.
5.8.h		R	R				S				Requirement defines methods and properties of Remote UI Clients Save-Restore scripting object.
5.8.i		R	R								Requirement indicates Remote UI Servers should provide a URL to accept saved UI information posted from Remote UI clients.
5.8.j					R	R	S				Requirement indicates Remote UI Server applications should support the save-restore mechanism by including the save-restore <object> element and scripts necessary to support the save-restore mechanism.

5.4.1.1.26 CEA-2014-A Section 5.9 Cookie Support

Mandatory for all DAE based devices

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.9.a	R	R	R					R	R	R	Requirement defines Remote UI Clients support of “cookies” per applicable IETF RFC including the “expires” field from the original Netscape specification.
5.9.b	R	R	R					R	R	R	Requirement defines minimum lifetime of “cookies” at Remote UI Clients.
5.9.c		R	R		R	R		O	O	O	Requirement defines Remote UI Clients substitution of Remote UI application <uiID> in domain name field of cookies from Level 1/2 servers during save restore.
5.9.d	R	R	R					R	R	R	Requirement indicates Remote UI Clients be capable of storing a minimum of 20 cookies per Remote UI application.
5.9.e	R	R	R					R	R	R	Requirement indicates Remote UI Clients support cookies of at least 4KB in length.
5.9.f	R	R	R					R	R	R	Requirements indicate Remote UI Clients not accept cookies that contain un-encoded semi-colon and comma characters.
5.9.g	O	O	O					O	O	O	Requirement indicates Remote UI Server applications should only store cookies necessary to its operation.

5.4.1.1.27 CEA-2014-A Section 5.10 Robustness Guidelines

Mandatory for all DAE based devices

	RUIC Level			RUIS Level			UICP	OIPF			Description
	0	1	2	0	1	2		OIP	BMP	EMP	
5.10.a	R	R	R	R	R	R	R	R	R	R	Requirement indicates URLs conform to DLNA and UPnP maximum length requirements.
5.10.b				R	R	R					Requirement indicates Remote UI servers insure image content served conform to Remote UI Client resolution capabilities.
5.10.c				S	S	S					Requirement indicates Remote UI Servers put “reasonable” limits on usage of alpha blending and overlapping elements.
5.10.d	R	R	R	R	R	R	R	R	R	R	Requirement indicates Remote UI devices ignore unknown XML elements including child-elements, and ignore undefined XML attributes and values.
5.10.e	R	R	R	R	R	R	R	R	R	R	Requirement indicates Remote UI devices not depend on ordering of XML elements unless a schema specifies a specific ordering.
5.10.f				S	S	S					Requirement indicates Remote UI Servers applications limit usage of XMLHttpRequest and NotifSocket objects to a maximum of 10 each.
5.10.g				S	S	S					Requirement indicates Remote UI Server applications avoid usage of animated GIF graphics as backgrounds and limit usage of alpha blending in animated GIF graphics.

5.4.2 Test Method

For conformance testing against the DAE specifications, test cases will be developed to test the DAE functionality under in the target device. Test applications are loaded and executed over the browser-based DAE environment with the help of native UI on the test target (referred to as the test driver, described below in the test environment section).

DAE test cases will be applications, which are a collection of mark-up pages and scripts as per the OIPF DAE specifications [DAE]. Mark-up pages will be generated in various supported formats to test for various kinds of layout capabilities as well as DAE services. Scripts will make use of various APIs specified in the DAE specification and references therein. These applications will exercise various services and capabilities of the DAE environment. These applications will be stored in a database referred to as the web-page DB.

The test cases will be supported with other test data stored in various data bases such as the user profile DB for storing user profiles, the license DB for storing license information, the stream DB for storing media content and the metadata DB for content metadata storage etc. These databases are located in a central repository (hereafter referred to as the test case database - TC DB).

These data will be utilized by various components of the test environment during the test case execution, as listed below in the test environment section. These various components are the ones interacting with the test target using various standardized interfaces as defined by the Open IPTV Forum to implement the IPTV solution, e.g. the web-server for sending test applications to the target. A central entity referred to as Test Manager (described below in the test environment section) will control these components to interact with the test target (as per the test case under execution).

In addition, the test manager will co-operate with other test-environment specific components (for example, the test report generator) which may aid in the test execution, validation and/or reporting.

To perform a sequence of test cases, the test driver, which is a native UI on target, shows the various test cases to be executed. The tester selects one test case from the list. A request for that test case is sent to the test manager from the target for execution of that test case. The test manager then sends a message to the web server to obtain the particular test application from the web-page DB. The target then requests the web server for the test application and obtains it after proper authentication.

The application for testing the streaming functionality shall contain appropriate mark-up (content descriptors and embedded streaming objects) and scripts for obtaining content from the stream generator.

The test manager will observe this request (through packet capture/protocol analysis over the network) and will send a message to the stream generator to prepare the required test stream. The stream generator will obtain the test contents from the stream DB.

The test application will now request the stream generator for the content stream and obtain it. The test driver will be provided with a user-input facility to log output of the application at the target end and may also log the test result status as pass or fail. The test driver will send these logs to the test manager for further analysis, if required. The test driver will further forward the analyzed results to the test report generator for the generation of a test report for the executed test case.

The details for each of the testable aspect (for each category of aspect the broad testing approach will be adapted) of the DAE module:

- Rendering:

  Rendering of application layout and visual look should be as per the visual models supported. Evaluation of the test case result shall be performed, either

  a) manual – by user determination, or
  b) automated - by comparison to a snapshot image of the expected output.

  Rendering aspects deal with the static visual output rendered by the browser as well as the animations that can be offered by SVG and Javascript usage.
  Check for support of relevant standards like SVG, CSS, XHTML etc. Use available test suites and appropriate test cases therein. Launch an application with desired layout and match the output with the expected output.

- Application Model:

  This includes Application Lifecycle, Signalling, Security and Event Notifications. Creating a number of applications with specified interactions leads to the desired side-effects, which can be monitored by a tester, e.g. creation and termination of an application based on user-generated input events. These may also include tests for application level security and performance issues regarding resource constraints under multiple application loads, responsiveness to user input in such a case, application load time as a function of size & other application level performance issues.

- Service APIs:

  Services & functionalities are offered in the DAE environment using APIs (e.g. the standard DOM API) for objects (existing, such as XMLHttpRequest, or extended by the OIPF specifications such as, video/broadcast, CEA A/V streaming, local system etc). Using suitable tools, simulated components (as necessary) for the test environment, the functionality offered by these can be tested under various data sets (e.g. different DOM structured applications, metadata, certificates etc.) for these components parameters, and environment conditions. For example, for testing the streaming object, the content server can be setup using Darwin/Helix server or VLC player to send content at various resolutions. Test results can be checked using the API return values along with expected final page layout changes and page loading.

- Interactivity:

  This refers to the interaction of the browser with the user (through events based on user navigation and interactions) and the network side application servers (sending requests).Support for DOM events shall be a part of this. For user interactions, event can be generated as desired to navigate the UI presentation such as traversing an EPG application. Support for desired the navigation feature support must be done and delivery of the event to the right target can be tested. If possible, automated playback mechanism should be used, using timing and description of events (key event like VK_UP) so as to provide the applications with the desired inputs to the target UI elements at desired times to enable browser UI/animation responsiveness/performance checking offered by the OITF.

- Application and Service Security and User Authentication:

  Security issues concerning the client side security requirements, such as privileged API usage, security check for untrusted servers, application retrieval through the same FQDN, will be tested for support of secure application fetching using proper authentication. Details on user authentication, content and service access protection implementation details are provided in the CSP section (refer Section 5.6).
  The issues described under this testing cannot be tested through a script API test and may require tapping the communication to and from OITF to ensure that the OITF implements the security checks properly while trying for applications access or making applications with a pass criterion which indicated blocked access to private functionality. The pass criteria can be implemented as error/exception check.

5.4.3 Test Environment

The test environment for DAE is displayed in Figure 6, and each component is described below.

- Test Manager:

  It sends a message to the Authentication and Session Management server which initiates the session and provides to the Test Manager the user's current profile. It sends a message to the stream generator to make a test stream. It sends a request to the web server to send the desired test web pages to the target under test. It will interact with the Test Driver on the target for this purpose. It will log the output from the target and send the information to the test report generator which will generate a report based on the pass/fail criteria.

- Authentication and Session Management:

  It initiates the session. It responds to the test manager's query about user authentication with the user's current profile.

- Stream Generator:

  It generates a test stream. After generating a test stream, it sends the stream to the target. It is configurable by the Test Manager to deliver the appropriate stream to the test target (i.e. the OITF).

- Test Case Database:

  It consists of stream database, web page database and user database. The following items are stored in stream database; Test data, AV Content, applications. The web pages are stored in the web page database. The user's current profile is stored in the user database.

- Web Server:

  It sends web pages to the target.

- Test driver on target:

  It allows the fetching of the DAE application for a particular test case (rendering tests, service API etc.) making use of the native UI on the target.

- DAE Application for streaming: APIs for making DAE application that implements streaming functionality.
- Additionally, a number of servers might be used as appropriate for per the test case, e.g. CSP Server for authenticating the OITF for content access.

All the network communication of interest can be tapped using packet capture /protocol analysis tools (e.g. a customized Wireshark application for monitoring HTTP request response flow) and can also be presented in the log of the output.

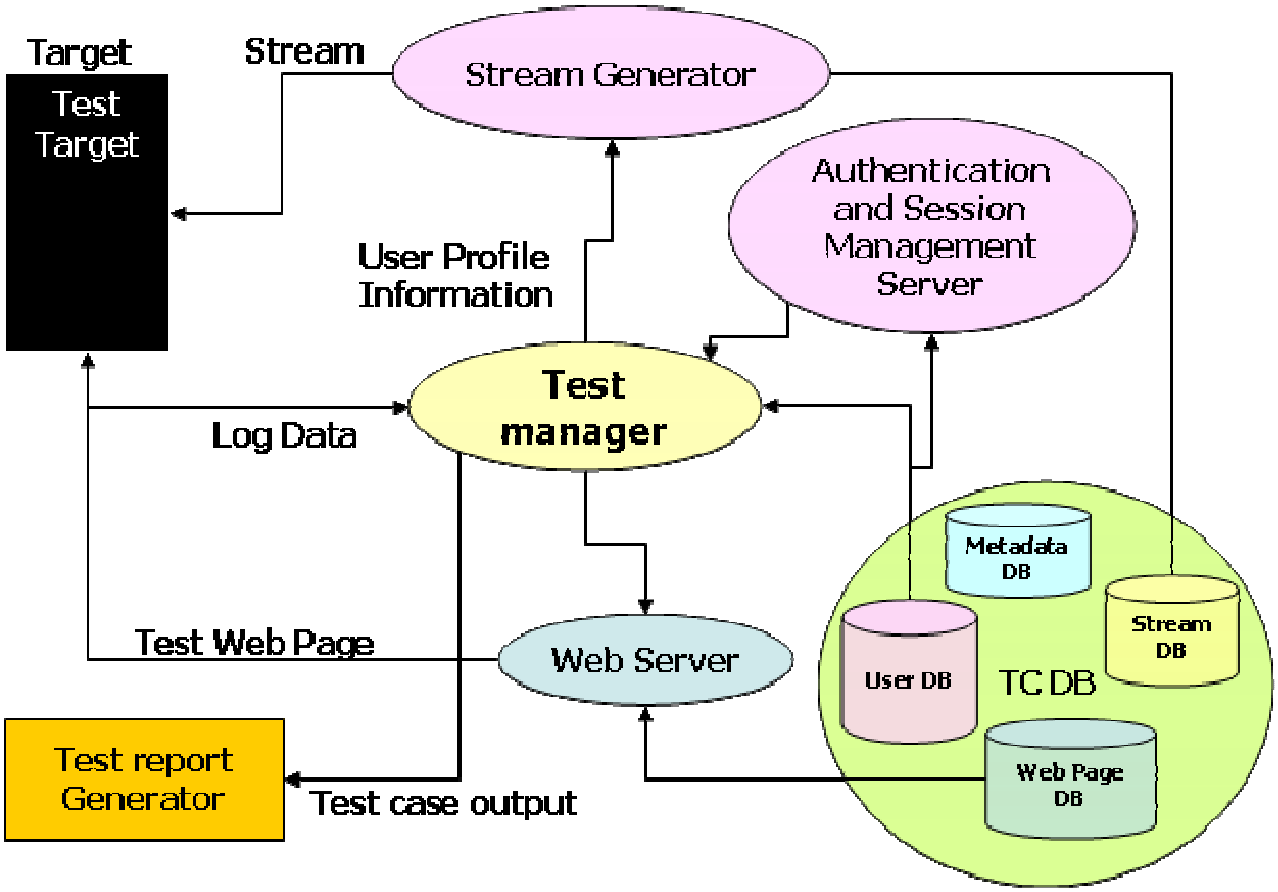

Figure 6 - Test Environment for DAE

5.4.4 Test Specification for DAE

5.4.4.1 DAE Overview

5.4.4.1.1 Application Definition

Test Specification ID	OIPF-DAE-Overview-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Application definition
Specification Section(s)	[DAE] §4.3, [DAE] §4.4 (partly)
Test Cases	• Check that the applications are organized in an implicit tree structure and that the applications that are created while the DAE environment is running are created as children of the system node. • Check that the applications are organized in an implicit tree structure and that the applications that are created while the DAE environment is running are created as children of the system node or as a sibling of the application • Check for modes to display multiple applications • Check for notification given by various methods available like show(), hide(), activate(), deactivate() to the execution environment • Check that the mode by which multiple applications are displayed on the OITF are determined prior to initialization of the DAE execution environment. • Check for the transparency of the background of any area of the browser area outside the DOM window • Check for the transparency of the background of the DOM window object associated within an application • Check that the DOM Window object associated with an application covers

	the entire area available to DAE applications • Check that the restrictions of size or location of windows are not enforced for windows associated with applications within the browser area • Check that the Active Application List is updated
Preconditions	• Test manager initiates an authenticated session of OITF. • OITF should be connected to the test network and have access to the resources located on the Test Case Database. • Test Manager sends request to load initial application on OITF
Priority	Mandatory
Remark	

5.4.4.1.2 Resource Management

Test Specification ID	OIPF-DAE-Overview-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Resource Management features
Specification Section(s)	[DAE] §4.4
Test Cases	• Check that the OITF restores interrupted presentations automatically when interrupted by audio from memory • Check that the OITF does not restore automatically a media presentation if it is interrupted due to resource loss caused by another request to play an audio or video presentation
Preconditions	• Test manager initiates an authenticated session of OITF. • OITF should be connected to the test network and have access to the resources located on the Test Case Database
Priority	Mandatory
Remark	

5.4.4.1.3 Content Download

Test Specification ID	OIPF-DAE-Overview-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Content Download features
Specification Section(s)	[DAE] §4.6
Test Cases	• Check that the OITF continues downloading as a background process even if the browser does not have an active session with the server that originated the download request anymore after a device power-down until it succeeds • Check that the OITF continues downloading as a background process even if the browser does not have an active session with the server that originated the download request anymore after a device network failure, until it succeeds • Check that the OITF continues downloading as a background process even if the browser does not have an active session with the server that originated the download request anymore (e.g. has switched to another DAE application), until it succeeds • * Check that the OITF passes the data inside the content access download descriptor into the XMLHttpRequest.response XML property in Javascript for further processing, if the OITF encounters an HTTP response message with the Content-Type of the "application/vnd.oipf.ContentAccessDownload+xml", as the result of an XMLHttpRequest • Check that if the OITF receives an HTTP 404 "File Not Found" status code, the OITF SHALL stop his attempts to resume the download, and go to a

	"Failed Download" state.
Preconditions	• Test manager initiates an authenticated session of OITF. • OITF should be connected to the test network and have access to the resources located on the Test Case Database • * OITF encounters an HTTP response message with the Content-Type of the "application/vnd.oipf.ContentAccessDownload+xml", as the result of an XMLHttpRequest
Priority	Mandatory
Remark	

5.4.4.1.4 Scheduled Content

Test Specification ID	OIPF-DAE-Overview-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Scheduled Content features
Specification Section(s)	[DAE] §4.8
Test Cases	• Check that if the OITF conveys the channel list information to a service through an HTTP POST message that is sent upon the first connection to a service that requires tuner control
Preconditions	• Test manager initiates an authenticated session of OITF. • OITF should be connected to the test network and have access to the resources located on the Test Case Database. • OITF supports conveying the channel list information to a service using Javascript by using method "getChannelConfig()" • OITF does NOT support conveying the channel list information to a service through an HTTP POST message that is sent upon the first connection to a service that requires tuner control
Priority	Mandatory
Remark	

5.4.4.2 DAE Application Model

5.4.4.2.1 Application Lifecycle

Test Specification ID	OIPF-DAE-Application-Model-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Application lifecycle
Specification Section(s)	[DAE] §5.1
Test Cases	• Check for the access of HTML, JavaScript and SVG files by an application from same FQDN • Check that the OITF includes the ability for applications to discover the applications provided by the AG through the remote UI • Check that the child applications do not inherit the permissions issued to the parent application. • Check that when an API is exported by an application to other applications, security checks are carried out in the context of the calling application • Check for *destroyApplication()*. • Check that when an application is terminated, all associated resources are freed and any network connections are terminated. • Check that when methods on an Application object are called from pages not running as part of an application, the OITF throws an error.
Preconditions	• Test Manager has initiated an authenticated session.

	• OITF is connected to the test network and have access to the resources located on the Test Case Database. • Test Manager sends request to test web server to send the test page to OITF.
Priority	Mandatory
Remark	

5.4.4.3 Application Announcement and Signalling

5.4.4.3.1 Broadcast related Applications

Test Specification ID	OIPF-DAE-Application-Model-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Application announcement and signalling- Broadcast related applications
Specification Section(s)	[DAE] §5.2.3
Test Cases	• Check that the OITF follows the Procedure for Starting Broadcast Related Applications when no previous linear TV service is running • Check that the OITF follows the Procedure for Starting and Stopping Broadcast Related Applications when signalling is updated • Check that the OITF follows the Procedure for exiting an application by a user controllable mechanism, if supported by the OITF • Check that the OITF follows the Procedure for exiting an application, the OITF stops presenting any broadcast
Preconditions	• OITF supports an exit mechanism for stopping an application which is directly accessible by the end-user • Test manager initiates the authenticated session of OITF. • Broadcast Discovery information is delivered to OITF • OITF is connected to the test network and have access to the resources located on the Test Case Database. • The broadcast scheduled content service must have an application which can be stopped by the end user. This application must have at least one child applications. This application must have at least one sibling as well
Priority	Mandatory
Remark	

5.4.4.3.2 Service provider related Applications

Test Specification ID	OIPF-DAE-Application-Model-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Application announcement and signalling- Service provider related applications
Specification Section(s)	[DAE] §5.2.4
Test Cases	• Check that the OITF provides a mechanism to show the service discovery application and starts the service provider related applications when a service provider is selected • Check that the OITF loads the EPG application in the browser, if there is a mechanism supported by the OITF to show the EPG application • Check that the OITF loads the CoD application in the browser, if there is a mechanism supported by the OITF to show the CoD application • Check that the OITF loads the Communication Service application in the browser, if there is a mechanism supported by the OITF to show the Communication Service application • Check that the OITF follows the Procedure for exiting an application by a

	user controllable mechanism, if supported by the OITF • Check that the OITF follows the Procedure for exiting an application if a different service provider is selected • Check that the OITF follows the Procedure for exiting an application if the selected service provider updates the list of applications in their SD&S service provider discovery record, an application is removed and the OITF detects this update
Preconditions	• Test manager initiates the authenticated session of OITF. • Service Provider Discovery information is delivered to OITF • OITF is connected to the test network and have access to the resources located on the Test Case Database. • The service provider service must have a few applications which are signalled with the status code AUTOSTART
Priority	Mandatory
Remark	

5.4.4.3.3 Broadcast independent Applications

Test Specification ID	OIPF-DAE-Application-Model-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	To test DAE Application announcement and signalling- Broadcast independent applications
Specification Section(s)	[DAE] §5.2.5
Test Cases	• Check that the OITF follows the Procedure for Starting and Stopping applications for applications which are independent of both broadcasters and service provider
Preconditions	• OITF supports a mechanism for starting and stopping an application which is directly accessible by the end-user • Test manager initiates the authenticated session of OITF. • OITF is connected to the test network and have access to the resources located on the Test Case Database. • The database must have an application which is independent of broadcasters and service providers which can be started or stopped by a user operation. This application must have at least one child applications. This application must have at least one sibling as well.
Priority	Mandatory
Remark	

5.4.4.3.4 Switching between Applications

Test Specification ID	OIPF-DAE-Application-Model-005
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Check that the OITF switches between applications
Specification Section(s)	[DAE] §5.2.2, [DAE] §5.2.5
Test Cases	• Check that the OITF follows the Procedure for Starting and Stopping applications for applications which are independent of both broadcasters and service provider
Preconditions	• OITF supports a mechanism for starting and stopping an application which is directly accessible by the end-user • Test manager initiates the authenticated session of OITF. • OITF is connected to the test network and have access to the resources located on the Test Case Database.

	• The database must have an application which is independent of broadcasters and service providers which can be started or stopped by a user operation. This application must have at least one child applications. This application must have at least one sibling as well.
Priority	Mandatory
Remark	

5.4.4.3.5 Signalling Format

Test Specification ID	OIPF-DAE-Application-Model-006
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Check for the signalling format used to signal DAE application
Specification Section(s)	[DAE] §5.2.7
Test Cases	• Check for the signalling format used to signal DAE application • Check the response of the application if it is signalled with the control codes like AUTOSTART, PRESENT etc
Preconditions	• Test manager initiates the authenticated session of OITF. • OITF should be connected to the test network and have access to the resources located on the Test Case Database.
Priority	Mandatory
Remark	

5.4.4.3.6 Event Notification

Test Specification ID	OIPF-DAE- Application-Model-007
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Check for the event notification in DAE
Specification Section(s)	[DAE] §5.3
Test Cases	• Check for XMLHTTPRequest scripting object for in-session Event notification • Check for NotifSocket scripting object for in-session event notification • Check for out of session event notification for multicast • Check for polling based out of session event notification (OPTIONAL). • HNI-IGI transactions for out-going request messages. (OPTIONAL) • HNI-IGI transactions for in session incoming request messages • HNI-IGI transactions for out of session incoming request messages. (OPTIONAL) • HNI-IGI transactions for out of session incoming request messages Check that OITF transactions when an unsolicited message arrives from the network. (OPTIONAL)
Preconditions	• Test manager initiates the authenticated session of OITF. • DAE application is active on OITF. • OITF is connected to the test network and have access to the resources located on the Test Case Database.
Priority	Mandatory
Remark	

5.4.4.4 Formats

5.4.4.4.1 CE-HTML

Test Specification ID	OIPF-DAE-Formats-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Check for the Format support in DAE
Specification Section(s)	[DAE] §6.1, [DAE] Annex B
Test Cases	• Check for the exceptions support in XHTML profile called CE-HTML • Check in JPEG that support for lossless and hierarchical modes and arithmetic coding of DCT coefficients is OPTIONAL
Preconditions	• Test manager initiates the authenticated session of OITF. • CEA-2014-A i-Box model is supported. • Test manager send request to test web server to send a test page to OITF, which has hasFeature() method of DOM embedded. • OITF is connected to the test network and have access to the resources located on the Test Case Database.
Priority	Mandatory
Remark	

5.4.4.4.2 Media Format

Test Specification ID	OIPF-DAE-Formats-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Check for the Format support in DAE
Specification Section(s)	[DAE] §6.2
Test Cases	• Check in JPEG that support for lossless and hierarchical modes and arithmetic coding of DCT coefficients is OPTIONAL
Preconditions	• Test manager initiates the authenticated session of OITF. • Externally defined formats are supported by the OITF. • Test manager send request to test web server to send initial test page on OITF. • OITF is connected to the test network and have access to the resources located on the Test Case Database.
Priority	Optional
Remark	

5.4.4.4.3 SVG

Test Specification ID	OIPF-DAE-Formats-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Check for the Format support in DAE
Specification Section(s)	[DAE] §6.3
Test Cases	• Check that SVG tiny 1.2 extensions are supported • Check for the extensions required to support DOM access from parent CE-HTML document to child SVG Tiny 1.2 document • Check for the extensions required to support DOM access from child SVG Tiny 1.2 document to parent CE-HTML document • Check for the extensions required to support DOM access from parent SVG Tiny 1.2 document to child CE-HTML document • Check for the extensions required to support DOM access from child

	CE-HTML document to parent SVG Tiny 1.2 document • Check for the extensions required to support DOM access from SVG Tiny 1.2 document to CE-HTML document • Check for the extensions required to accomplish setting and moving focus through SVG Tiny 1.2 document and CE-HTML document • Check for the extensions required to pass an event that occurred in the CE-HTML document to a script in SVG Tiny 1.2 document • Check for following document event methods: createEvent(), dispatchEvent(), addEventListener(), removeEventListener(), addEventListenerNS() and removeEventListenerNS(). • Check that the script code of SVG Tiny 1.2 is able to call functions in DOM nodes. • Check that the DAE applications do not rely upon codec support for the use of audio and video elements from SVG Tiny 1.2. • Check that the DAE applications does not rely upon support for the use of Connection from SVG Tiny 1.2.
Preconditions	• Test manager initiates the authentication session of OITF. • OITF support SVG Tiny 1.2 documents. • DAE application is active on OITF. • OITF is connected to the test network and have access to the resources located on the Test Case Database.
Priority	Mandatory
Remark	

5.4.4.5 APIs

5.4.4.5.1 Object factory API

Test Specification ID	OIPF-DAE-API_Object_Factory-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to check and create an instance of DAE defined embedded objects will be tested in this section
Specification Section(s)	[DAE] §7.1
Test Cases	• Check for support of mime types through *isObjectSupported()* API of *OipfObjectFactory* object • Check *OipfObjectFactory* object APIs given below for creation of visual objects o Test for *createVideoBroadcastObject()* API o Test for *createVideoMpegObject()* API o Test for *createStatusViewObject()* API • Check *OipfObjectFactory* object APIs given below for creation of non visual objects o Test for *createApplicationManagerObject()* API o Test for *createCodManagerObject()* API o Test for *createConfigurationObject()* API o Test for *createDownloadManagerObject()* API o Test for *createDownloadTriggerObject()* API o Test for *createDrmAgentObject()* API o Test for *createGatewayInfoObject()* API o Test for *createIMSObject()* API o Test for *createNotifSocketObject()* API o Test for *createParentalControlManagerObject()* API o Test for *createRecordingSchedulerObject()* API o Test for *createRemoteManagementObject()* API o Test for *createSearchManagerObject()* API

	o Test for *createCapabilitiesObject()* API o Test for *createMDTFObject()* API
Preconditions	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.2 Applications Management APIs

Test Specification ID	OIPF-DAE-API_App_Mgmt-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF DAE application capability will be tested in this section
Specification Section(s)	[DAE] §7.2
Test Cases	• Check for current visualization mode of application using *getApplicationVisualizationMode()* API of *application/oipfApplicationManager* object • Check that the application part of specified document is retrieved by *getOwnerApplication()* API of *application/oipfApplicationManager* object • Check that children applications of an application are retrieved by *getChildApplications()* API of *application/oipfApplicationManager* object • Check that the hint to execute garbage collection is given by *gc()* API of *application/oipfApplicationManager* object • Check that the application are made visible by *show()* API of *Application* class • Check that the applications are made invisible by *hide()* API of *Application* class • Check that the applications are activated by *activateInput()* API of *Application* class • Check that the applications are deactivated by *deactivateInput()* API of *Application* class • Check that the applications are created by *createApplication()* API of *Application* class • Check that the application are destroyed by *destroyApplication()* API of *Application* class • Check for access of Application object in array notation through *item()* API of *ApplicationCollection* class • Check current available memory to application by using *getFreeMem()* API of *ApplicationPrivateData* class • Check that the keyset which DAE application requests to receive is set by *setValue()* API of *KeySet* class
Preconditions	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.3 Configuration and Setting APIs

Test Specification ID	OIPF-DAE-API_Config_Setting-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF Configuration and Setting functionality will be tested in this section

Specification Section(s)	[DAE] §7.3
Test Cases	• Check that parental control pin is set through *setParentalControlPIN()* API of the *Configuration* object • Check that parental control pin is set through *setParentalControlPINEnable()* API of the *Configuration* object • Check that status of parental control pin is retrieved through *getParentalControlPINEnable()* API of the *Configuration* object • Check that target is unlocked by parental control pin through *unlockWithParentalControlPIN()* API of the *Configuration* object • Check that specified parental control pin is correct through *verifyParentalControlPIN()* API of the *Configuration* object • Check that non parental rated programmes are blocked by the terminal through *setBlockUnrated()* API of the *Configuration* object • Check that the system text for given key is retrieved through *getText()* API of the *Configuration* object • Check that the system text for given key is set through *setText()* API of the *Configuration* object • Check that the screen size is set through *setScreenSize()* API of the *LocalSystem* object • Check that the type of PVR support is set through *setPvrSupport()* API of the *LocalSystem* object • Check for access of *NetworkInterface* object in array notation through *item()* API of *NetworkInterfaceCollection* object • Check for access of *AVOutput* object in array notation through *item()* API of *AVOutputCollection* object
Preconditions	• OITF supports <ConfigurationChanges> element with value “true” • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.4 Content download APIs

Test Specification ID	OIPF-DAE-API_Content_Download-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF content download functionality will be tested in this section
Specification Section(s)	[DAE] §7.4
Test Cases	• Check passing of content access descriptor to an underlying download manager by *application/oipfDownloadTrigger* object through API *registerDownload()* • Check OITF is triggered to initiate download, from given URL of given content, for *application/oipfDownloadTrigger* object through API *registerDownloadURL()* • Check for possibility of download of given size for *application/oipfDownloadTrigger* object through API *checkDownloadPossible()* • *Check passing of CRID and IMI to the underlying download manager through *registerDownloadFromCRID()* API of *application/oipfDownloadTrigger* object • **Check that the in-progress, stalled or queued download is paused through *pause()* API of *application/oipfDownloadManager* object • **Check that the paused download is resumed through *resume()* API of *application/oipfDownloadManager* object • **Check that the downloaded content is removed through *remove()* API of

	application/oipfDownloadManager object • **Check that the collection of downloads of given id are retrieved through *getDownloads()* API of *application/oipfDownloadManager* object • **Check that filtered list of downloads is created using *createFilteredList()* API of *application/oipfDownloadManager* object • Check that when the ID of a download is TV-Anytime CRID, then the values of name, description and parentalRating properties are set by the DAE based on the metadata provided for the item matching that CRID • Check for access of *Download* object in array notation through *item()* API of *DownloadCollection* class • Check for access of DRM Control information in array notation through *item()* API of *DRMControlInfoCollection* class
Preconditions	• OITF indicates “true” for <download> element • *OITF supports <clientMetadata> with value “true” and “type” attribute with value “bcg” and supports download management APIs • **OITF supports download management APIs i.e. attribute "manageDownloads" of the <download> element a value unequal to ‘none’ • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.5 Content On Demand Metadata APIs

Test Specification ID	OIPF-DAE-API_CoD_Metadata-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF content metadata will be tested in this section
Specification Section(s)	[DAE] §7.5

Test Cases	• Check for the Content catalogue APIs
	  o Test for *item()* API of *CatalogueCollection* class
	  o Test for *getPurchaseHistory()* API of *ContentCatalogue* class
	• Check that requested CoD folder content list, which is made available on demand in paging model, is fetched from the appropriate source, and application is notified on availability
	• Check for the *CODFolder* class APIs
	  o Test for *item()* API
	  o Test for *getPage()* API
	  o Test for *abort()* API
	• Check for the *CODAsset* class APIs
	  o Test for *isReady()* API
	  o Test for *lookupMetadata()* API
	• Check for the *CODService* class APIs
	  o Test for *isReady()* API
	  o Test for *lookupMetadata()* API

Preconditions	• OITF supports <clientMetadata> with value “true” and “type” attribute with value “bcg” and may apply to “type” attribute with value “dvb-si” • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.6 Content Service Protection API

Test Specification ID	OIPF-DAE-API_Content_Protection-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF DRM protection will be tested in this section
Specification Section(s)	[DAE] §7.6
Test Cases	• Check *sendDRMMessage()* API of *application/oipfDrmAgent* object to send message to DRM agent
Preconditions	• OITF supports DRM protection by providing one or more <drm> elements • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.7 Gateway Discovery and Control APIs

Test Specification ID	OIPF-DAE-API_Gateway_Discover_Control-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF Gateway Discovery and control functionality will be tested in this section
Specification Section(s)	[DAE] §7.7
Test Cases	• Check for IG supported method through *isIGSupportedMethod()* API of *application/oipfGatewayInfo* object
Preconditions	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.8 IMS Related APIs

Test Specification ID	OIPF-DAE-API_IMS-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF IMS functionality will be tested in this section
Specification Section(s)	[DAE] §7.8

Test Cases	• Check for following *application/oipfIMS* object APIs
	  o Test for *getRegisteredUsers()* API
	  o Test for *registerUser()* API
	  o Test for *deRegisterUser()* API
	  o Test for *getAllUsers()* API
	  o Test for *setUser()* API
	  o Test for *subscribeImsNotification()* API
	  o Test for *unSubscribeImsNotification()* API
	• *Check for following *application/oipfIMS* communication services class APIs
	  o Test for *openChatSession()* API and *sendMessageInSession()* API
	  o Test for *closeChatSession()* API
	  o Test for *sendMessage()* API
	  o Test for *setStatus()* API
	  o Test for *subscribeToStatus()* API
	  o Test for *getContacts()* API

	o Test for *allowContact()* API o Test for *blockContact()* API o Test for *createContactList()* API o Test for *getContacts(string)* API o Test for *addToContactList()* API o Test for *removeFromContactList()* API o Test for *deleteContactList()* API o Test for *allowAllContacts()* API o Test for *blockAllContacts()* API • Check that list of users represented by the *UserDataCollection* object can be accessed in array notation through API *item()* • Check that list of features associated to user represented by the *FeatureTagCollection* object can be accessed in array notation through API *item()* • Check for following *ContactCollection* APIs o Test for *item()* API o Test for *remove()* API o Test for *add()* API
Preconditions	• OITF supports control of its IMS functionality by a server by stating <ims>true</ims> in its capability description • *OITF supports Communication Services functionality by a server by stating <communication_services>true</communication_services> in its capability description • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.9 Parental Rating and Parental Control APIs

Test Specification ID	OIPF-DAE-API_Parental_Rating_Control-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF parental rating and control functionality will be tested in this section
Specification Section(s)	[DAE] §7.9
Test Cases	• Check that *setParentalControlStatus()* API is used by *application/oipfParentalControlmanager* object for setting the status of parental control • Check that *getParentalControlStatus()* API is used by *application/oipfParentalControlmanager* object for getting the status of parental control • Check blockage status of non parental rated programmes through *getBlockUnrated()* API of *application/oipfParentalControlmanager* object • Check that the index of the parental rating scheme is retrieved through *indexof()* API of *ParentalRatingScheme* class • Check that string representation of rating for parental rating scheme can be accessed in array notation through *item()* API of *ParentalRatingScheme* class • Check for retrieval of URI of icon representing rating of parental scheme through *iconURI()* API of *ParentalRatingScheme* class • Check for access of parental rating schemes in array notation through *item()* API *ParentalRatingSchemeCollection* object • Check for creation and addition of new *ParentalRatingScheme* object to *ParentalRatingSchemeCollection* through *addParentalRatingScheme()* API • Check for getting reference of *ParentalRatingScheme* object associated

	with given scheme name through *getParentalRatingScheme()* API • Check that parental rating values can be accessed in array notation through *item()* API of *ParentalRatingCollection* object • Check for creation and addition of *ParentalRating* object for a given parental rating scheme and parental rating, for a programme or channel, to *ParentalRatingCollection* through *addParentalRating()* API
Preconditions	• OITF has indicated <parentalcontrol> element with value “true” in capability profile • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.10 Scheduled Recording APIs

Test Specification ID	OIPF-DAE-API_Scheduled_Recording-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF Scheduled recording functionality will be tested in this section
Specification Section(s)	[DAE] §7.10
Test Cases	• Check for following application/oipfRecordingScheduler object APIs o Test for *record()* API o Test for *recordAt()* API o Test for *getScheduledRecordings()* API o Test for *getChannelConfig()* API o Test for *remove()* API o Test for *createProgrammeObject()* API • Check for access of scheduled recordings in array notation through *item()* API of *ScheduledRecordingCollection* object • *Check for extension to *application/oipfRecordingScheduler* for control of recording through following APIs o Test for *getRecording()* API o Test for *remove()* API o Test for *stop()* API o Test for *refresh()* API • Check that the values of *Recording* object properties are obtained from the metadata of recorded programme and are copied from programme used for the scheduling a recording by the *record()* API of *application/oipfRecordingScheduler* object • Check for access of Recording object in array notation through *item()* API of *RecordingCollection* object • Check that *PVREvent* objects are generated and it indicates the changes in the status of active recording • Check for following *BookmarkCollection* APIs o Test for *item()* API o Test for *addBookmark()* API o Test for *removeBookmark()* API
Preconditions	• OITF indicates <recording> with value “true” in its capability profile • *OITF indicates <recording> element with attribute “manageRecordings” with value “true” in its capability profile • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.11 Remote Management APIs

Test Specification ID	OIPF-DAE-API_Remote_Mgmt-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF remote management functionality will be tested in this section
Specification Section(s)	[DAE] §7.11
Test Cases	• Check for application/oipfRemoteManagement object APIs o Test *getParameter()* API o Test *setParameter()* API o Test *triggerSoftwareUpdate()* API
Preconditions	• OITF indicates the <remote_diagnostics> with value "true" in capability description • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.12 Metadata API

Test Specification ID	OIPF-DAE-API_Metadata-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF Metadata functionality will be tested in this section
Specification Section(s)	[DAE] §7.12
Test Cases	• Check that the MetadataSearch object is created using createSearch() API of application/oipfSearchManager object • Check that the channel line up is retrieved using getChannelConfig() API of application/oipfSearchManager object • Check for the following MetadataSearch class APIs o Test for *addRatingConstraint()*API o Test for *addCurrentRatingConstraint()* API o Test for *addChannelConstraint()* API o Test for *orderBy()* API o Test for *createQuery()* API o Test for *findProgrammesFromStream()* API • Check for following the *Query* class APIs o Test for *and()* API o Test for *or()* API o Test for *not()* API • Check that the metadata search results are fetched from the appropriate source, and application is notified on availability • Check for the following *SearchResults* class APIs o Test for *item()* API o Test for *getResults()* API o Test for *abort()* API o Test for *update()* API
Preconditions	• OITF supports <clientMetadata> with value "true" and "type" attribute with value "bcg" • OITF that supports <clientMetadata> with value "true" and "type" attribute with value "dvb-si", for these OITFs adherence is optional

	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.13 Scheduled content and hybrid tuner APIs

Test Specification ID	OIPF-DAE-API_Sched_Content_Hybrid_Tuner-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF *video/broadcast* functionality will be tested in this section
Specification Section(s)	[DAE] §7.13
Test Cases	• Check for the following *video/broadcast* object APIs o Test for *getChannelConfig()* API o Test for *bindToCurrentChannel()* API o Test for *createChannelObject()* API o Test for *setChannel()* API o Test for *prevChannel()* API o Test for *nextChannel()* API o Test for *setFullScreen()* API o Test for *setVolume()* API o Test for *getVolume()* API o Test for *release()* API • Check support for CSS properties of video/broadcast object like width, height, position, float, top, left, right, bottom, vertical-align, padding and padding-* properties, margin and margin-* properties, border and border-* properties, visibility, and display • Check for the <overlaylocaltuner> support • Check support for CSS opacity property and CSS3 RGBA colour values, for any non-video XHTML element on top of video object • *Check for extension to *video/broadcast* object for recording and time shift through following APIs o Test for *recordNow()* API o Test for *stopRecording()* API o Test for *pause()* API o Test for *resume()* API o Test for *setSpeed()* API o Test for *seek()* API o Test for *stopTimeshift()* API o Test for *setChannel()* API • Check for extension to *video/broadcast* object for playback through following APIs o Test for *getComponents()* API o Test for *getCurrentActiveComponents()* API o Test for *selectComponent()* API o Test for *unselectComponent()* API • **Check for extension to *video/broadcast* object for channel scan through following APIs o Test for *startScan()* API o Test for *stopScan()* API • ****Check for creation of channel list from SD&S fragments through *createChannelList()* API as extension of *video/broadcast* object • Check for creation of filtered list of channels through *createFilteredList()* API of *ChannelConfig* class

	• Check for following *ChannelList* class APIs
	  o Test for *item()* API
	  o Test for *getChannel()* API
	  o Test for *getChannelByTriplet()* API
	  o Test for *getChannelBySourceID()* API
	• *****Check for extension to metadata of *Channel* class through following APIs
	  o Test for *getField()* API
	  o Test for *getLogo()* API
	• Check for following *FavouriteListCollection* class APIs
	  o Test for *getFavouriteList()* API
	  o Test for *item()* API
	• ***Check for extension of *FavouriteListCollection* class through following APIs
	  o Test for *createFavouriteList()* API
	  o Test for *remove()* API
	  o Test for *commit()* API
	• Check for following *FavouriteList* class APIs
	  o Test for *item()* API
	  o Test for *getChannel()* API
	  o Test for *getChannelByTriplet()* API
	  o Test for *getChannelBySourceID()* API
	• ***Check for extension of *FavouriteList* class through following APIs
	  o Test for *insertBefore()* API
	  o Test for *remove()* API
	  o Test for *commit()* API

Preconditions	• OITF supports <video_broadcast> with value “true” • * OITF supports <recording> with value “true” • **OITF supports <clientMetadata> with value “true” and “type” attribute with value “eit-pf” or “dvb-si” • ***OITF supports <extendedAVControl> with value “true” • ****OITF indicates support for broadcast video using SD&S • *****OITF supports <clientMetadata> with value “true” and “type” attribute with values “bcg”, “sd-s”, “eit-pf” or “dvb-si” • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.14 Media Playback APIs

Test Specification ID	OIPF-DAE-API_Media_Playback-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF media playback functionality will be tested in this section
Specification Section(s)	[DAE] §7.14

Test Cases	• Check that the resources are freed when play state of A/V object is set to 6 (error), due to unavailability of scarce resources, or is set to 0 when stopped
	• Check that when 'data' attribute and/or the 'type' attribute of the HTMLObjectElement representing the A/V object has different values, the object goes to state 0
	• Check that when available content has reached to the end the A/V control object is set to state 5 (finished)
	• Check that when available content has reached to the beginning the A/V control object is set to state 2 (paused)
	• Check that the request is rejected when seek is performed beyond the available content
	• Check that the visibility of an A/V object does not affect its state or its use of scarce resources
	• Check that when play, on streaming content, is called in stopped, connecting or buffering state, the A/V object goes to pause state
	• Check that when play, on downloaded content, is called before sufficient data is downloaded, A/V object is set to error state
	• Check that when play, on downloaded content, is called before sufficient data is downloaded , A/V object is set to error state
	• Check that when play, on recorded content, is called before sufficient data is recorded, A/V object is set to error state
	• Check that initiating playback of the A/V stream uses information given by Content Access Descriptor referred to by the 'data' attribute,
	• Check for passing DRM-information of selected content and DRM system ID as a part of <DRMControlInformation>-elements of a content-access descriptor to the DRM agent
	• Check for extension to *A/V object* for playback through following APIs
	  o Test for *getComponents()* API
	  o Test for *getCurrentActiveComponents()* API
	  o Test for *selectComponent()* API
	  o Test for *unselectComponent()* API
	• Check for changing the played content item through *setSource()* API as extension to *A/V* object for playing media
	• *Check for extension to *A/V* object for UI feedback of buffering A/V content through following APIs
	  o Test for *getAvailablePlayTime()* API
	  o Test for *setBufferingStrategy()* API
	• Check for <object> element restrictions for memory audio
	• Check for <object> element is accessible through the Javascript A/V media object
	• Test for *play()* and *stop()*

Preconditions	• OITF supports A/V object • *OITF supports buffering of A/V content • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.15 Miscellaneous APIs

Test Specification ID	OIPF-DAE-API_Miscellaneous-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF miscellaneous functionality will be tested in this section

Specification Section(s)	[DAE] §7.15

Test Cases	• Check for *application/oipfMDTF* object APIs
	  o Test for *addFLUTEListener()* API
	  o Test for *addFLUTEListenerTags()* API
	  o Test for *getFLUTEListeners()* API
	  o Test for *getTags()* API
	  o Test for *removeFLUTEListener()* API
	• **Check that the *application/oipfStatusView* embedded object provides overall consistent graphical view for status of downloads
	• **Check for following *application/oipfStatusView* object APIs
	  o Test for *getMinimumItemWidth()* API
	  o Test for *getMinimumItemHeight()* API
	• ***Check that at least additional monitor state namely "list_of_recorded_content" is supported by *application/oipfStatusView* object
	• ****Check for support of given capability by OITF through *HasCapability()* API of *application/oipfCapabilities* object
	• *****Check for *debug()* API, used by application developer for debugging

Preconditions	• *OITF indicates <mdtf> element with value "true" in capability profile • **OITF supports content download • **OITF supports at least the minor states "list_of_recent_downloads" and "list_of_downloaded_content" • ***OITF supports recoding functionality • ****OITF supports *application/oipfCapabilities* object • *****OITF supports global (Window) object • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.5.16 Shared Utility classes and features

Test Specification ID	OIPF-DAE-API_Shared_Utility-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various APIs used to provide OITF shared utilities will be tested in this section
Specification Section(s)	[DAE] §7.16
Test Cases	• Check for access of strings in array notation through *item()* API of *StringCollection* object • *Check that the value of given field contained in metadata for the programme is retrieved through *getField()* method of *Programme* class • **Check that the descriptor content from DVB SI EIT programme descriptor is retrieved through *getSIDescriptor()* method of *Programme* class • Check for access of *Programme* objects in array notation through *item()* API of *ProgrammeCollection* object
Preconditions	• *OITF supports <clientMetadata> with value "true" and "type" attribute with value "bcg", "eit-pf" or "dvb-si" • **OITF supports <clientMetadata> with value "true" and "type" attribute with value "eit-pf" or "dvb-si" • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory

Remark	

5.4.4.6 System Integration Aspects

5.4.4.6.1 Mapping from APIs to Protocols

Test Specification ID	OIPF-DAE-Map_PROT_Interactivity-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	This section tests the APIs which maps Protocols from DAE
Specification Section(s)	[DAE] §8.2
Test Cases	• Check that the content is downloaded which is described in the "contentAccessDescriptor" through registerDownload() API • Check mapping of following APIs of CEA-2014-A AV object to the HNI-IGI protocol interfaces o *play()* o *stop()* o *seek()* o *play(0)* • Check that the OITF obtains the Broadcast Discovery Record by utilizing UNIS-7 • Check setChannel() API of video/broadcast object for initiation of broadcast session • Check setChannel() API of video/broadcast object for switching between channels • Check release() API that causes OITF to perform an IGMP Leave on the active broadcast session of video/broadcast object • Check registerUser() API for IMS registration of user • Check deRegisterUser() API for IMS de-registration of user • Check subscribeImsNotification() API for application subscription to notifications • Check unSubscribeImsNotification() API for notifying that application will not receive unsolicited notifications • Check mapping of following DAE APIs with the unmanaged network o *play()* o *stop()* o *seek()* o *play(0)* • Check setChannel() API of video/broadcast object for initiation of broadcast session • Check setChannel() API of video/broadcast object for switching between channels • Check release() API that causes OITF to perform an IGMP Leave on the active broadcast session of video/broadcast object
Preconditions	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.6.2 URI Schemes and Usage

Test Specification ID	OIPF-DAE-URI_Schemes_Usage_Interactivity-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Testing various URI schemes and their usage

Specification Section(s)	[DAE] §8.3
Test Cases	• Check for the support of corresponding protocols to given URL scheme
Preconditions	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.7 Capabilities

5.4.4.7.1 DAE capability and Default UI

Test Specification ID	OIPF-DAE-Capability_UI_Profile_Rendering-005
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Various DEA capabilities and default UI profiles
Specification Section(s)	[DAE] §9.1, [DAE] §9.2
Test Cases	• Check that OITF supports loading of multiple simultaneous applications and running in browser • Check that OITF supports at least 2 DAE applications being visible at one time, in notification and main browser window • *Check for the HD output support for 1280x720 graphics • Check for the support of unrestricted scaling of IP delivered video • Check that OITF supports at least one bit of per-pixel alpha • Check that OITF supports decoding of one stream containing audio and video • Check support for Tiresias Screenfont or equivalent with the “Generic Application Western European Character set” • Check in OITF that it supports some means for input text • Check that SSL/TLS implementation has supports for o Key length up to 2048 bits for asymmetric encryption o Key length at least 128 bits for AES symmetric encryption o Key length at least 168 bits for 3DES symmetric encryption • Check that at least 100 cookie’s are supported with maximum of 20 per domain • Check that the maximum size of any individual cookie is 4K • Check that VK_0 – VK_9 key events are available to DAE applications • Check that VK_UP, VK_DOWN, VK_LEFT, VK_RIGHT, VK_ENTER, VK_BACK, VK_RED, VK_GREEN, VK_YELLOW, VK_BLUE key events are available to DAE applications • **Check that VK_PLAY, VK_PAUSE, VK_STOP, VK_NEXT, VK_PREV, VK_PLAY_PAUSE, VK_FAST_FWD, VK_REWIND keys events are available to DAE application • Check that OITF supports at least one of the following UI base profile "OITF_SDEU_UIPROF", "OITF_SD60_UIPROF", "OITF_SDUS_UIPROF", "OITF_HD_UIPROF", "OITF_FULL_HD_UIPROF" • Check that server and OITF supports the concatenation of a series of UI profile name fragments in any order • ***Check that the OITF supporting extension to capabilities is advertised using mechanism defined in [DAE] section 8.1
Preconditions	• *OITF supports HD output • **OITF supports VK_PLAY, VK_PAUSE, VK_STOP, VK_NEXT, VK_PREV, VK_PLAY_PAUSE, VK_FAST_FWD, VK_REWIND keys • ***OITF supports an extension to the capabilities which is defined using a combination of a base UI Profiles and a (number of) UI Profile fragment(s)

	• The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.7.2 CEA-2014 Capability Negotiation and Extensions

Test Specification ID	OIPF-DAE-CEA_Negotiation_EXTN_Rendering-005
Test Specification Version	1.0.0
Test Object(s)	OITF, Server
Test Specification Description	Various CEA-2014-A capabilities negotiation will be tested under this section
Specification Section(s)	[DAE] §9.3
Test Cases	• Check that the control over OITF local tuner functionality by the server is indicated in capability exchange mechanism by element video_broadcast • Check that OITF support for overlay over local tuner video broadcast is indicated by <overlaylocaltuner> having either value none|on-off|global|per-pixel • Check for the rendering of broadcasted content over IP on OITF is indicated in capability exchange mechanism by element video_broadcast • Check that OITF support for overlay over IP video broadcast is indicated by <overlayIPbroadcast> having either value none|on-off|global|per-pixel • Check that control for recording functionality of OITF by server, is indicated in capability exchange mechanism by element <recording> having either value true|false • Check that for recording OITF uses supported method for conveyance of channel list to server • Check that support for content download to a client is indicated by <download> element in client capability • Check that OITF support for parental control is indicated by <parentalcontrol> element in capability profile by either value true|false • Check that OITF support for extended A/V API is indicated by <extendedAVControl> element in capability profile by either value true|false • Check that OITF support for client side metadata processing and APIs is indicated by <clientMetadata> element in capability profile by either value true|false • Check support for modification in OITF configuration and settings by applications is indicated by <configurationChanges> element in OITF capability profile by either value true|false • Check that OITF support for IMS API is indicated by <ims> element in client capability profile by value either true|false • Check that OITF support for handling DRM protected content is indicated by <drm> element • Check that OITF support for streaming A/V content to client is indicated by non-empty list of <audio_profile> and/or <video_profile> elements in the RUI client capability description • Check for support for new attribute namely “DRMSystemID” for <audio_profile> and <video_profile> elements • Check that client provides the list of supported audio and video profiles through <audio_profile> and/or <video_profile> with “type” attribute having value as application/vnd.oipf.ContentAccessStreaming+xml • Check that OITF support for remote diagnostics is indicated by <remote_diagnostics> element in capability profile by either value true|false • Check OITF support for SVG • Check that OITF support for 3rd party polling mechanism is indicated by

	<pollingNotifications> element by either value true|false • Check OITF support for multicast delivery terminating function is indicated by <mdtf> element by either value true|false • Check support for extensions to the capability profile elements defined in [Req. 5.2.1.a] of [CEA2014A]
Preconditions	• OITF support for new elements is defined by schema described in [DAE] Annex F • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.4.4.8 Security

5.4.4.8.1 Application / Service Security and User Authentication

Test Specification ID	OIPF-DAE-App_Service_Security-006
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Performs necessary security checks for application and user authentication
Specification Section(s)	[DAE] §10
Test Cases	• Check that OITF authenticates the server during a TLS handshake through a valid X.509v3 certificate (granted by a certificate authority that is trusted by the OITF) • Check that OITF matches the hostname or (sub) domain name of the HTML document's URI with the hostname or (sub) domain name as specified in the X.509v3 certificate • Check that OITF support the Online Certificate Status Protocol (OCSP), to determine the current validity of the X.509v3 certificate • Check that OITF supports a private certificate extension for X.509v3 certificates called "permissions" • Check that OITF throws an error with the message value "SecurityError" when server does not have the necessary access privileges but user may override this decision • Check that the server specifies the use of TLS for each HTML document that accesses privileged functionality • Check that the server has exposed a valid X.509v3 certificate during the TLS certificate handshake • Check that server can request an OITF for certain permissions to access privileged functionality through a private certificate extension • Check for the security requirement of tuner control and lineup (if it is supported) o Check that authenticated server, which has necessary privilege, obtains the channel line up of (local) tuner from OITF o *Check that OITF does not convey the Client Channel Listing to the server through HTTP POST or getChannelConfig() and throws an error as defined in [DAE] section 10.1.1 o *Check that OITF denies the requests to switch a local tuner to another channel by throwing an error as defined in [DAE] section 10.1.1 • Check for the security requirement for recording (if it is supported) o Check that authenticated server, which has necessary privilege, schedules the broadcast recording on OITF o *Check that OITF denies server request to access application/oipfRecordingScheduler object and throws an error as defined in [DAE] section 10.1.1

	o *Check that OITF does not convey the Client Channel Listing to the server through HTTP POST or getChannelConfig() o Check that authenticated server, which has necessary privilege, schedules recording of current broadcast on OITF o *Check that OITF denies the request to start recording of current broadcast and throws an error as defined in [DAE] section 10.1.1 o Check that OITF restricts the visibility and control over scheduled recordings to those scheduled recordings that were initiated through a server from the same FQDN that scheduled the recordings • Check for the security requirement for content download (if it is supported) o Check that authenticated server, which has necessary privilege, initiates a download on OITF o *Check that OITF does not start the content download even after receiving a content-access description document, when the server is unauthentic • Check for the security requirement for DRM related functionality (if it is supported) o Check that authenticated server, which has necessary privilege, interacts with the DRM agent of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when an application loaded from the server attempts to access properties or methods of DRM agent object • Check for the security requirement for IMS functionality (if it is supported) o Check that authenticated server, which has necessary privilege, interacts with IMS functionality of OITF o *Check that OITF throws an error as defined in section 10.1.1, when an application loaded from the server tries to access any classes, properties or methods defined in [DAE] section 7.8 • Check for the security requirement for metadata processing functionality (if it is supported) o Check that authenticated server, which has necessary privilege, interacts with search manager of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when an application loaded from the server attempts to access properties or methods of search manager o Check that authenticated server, which has necessary privilege, accesses extensions to video/broadcast for EIT p/f information of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when an application loaded from the server attempts to access programme properties of video/broadcast • Check for the security requirement for configuration and setting functionality (if it is supported) o Check that authenticated server, which has necessary privilege, interact with configuration functionality of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access any of the classes, properties or methods defined in [DAE] section 7.3. • Check for the security requirement for APIs for OITF under control of service provider for accessing extended tuner control APIs (if it is supported) o Check that authenticated server, which has necessary privilege, interact with extended tuner control APIs of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access any of the classes, properties or methods defined in [DAE] section 7.13.7 • Check for the security requirement for APIs for OITF under control of service provider for accessing extended PVR APIs (if it is supported) o Check that authenticated server, which has necessary privilege,

	interact with extended PVR APIs of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access any of the classes, properties or methods defined in [DAE] section 7.10.4 • Check for the security requirement for APIs for OITF under control of service provider for accessing download manager (if it is supported) o Check that authenticated server, which has necessary privilege, interact with download manager of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access any of the classes, properties or methods defined in [DAE] section 7.4.3 • Check for the security requirement for APIs for OITF under control of service provider for accessing all downloads o Check that authenticated server, which has necessary privilege, manages downloads which are not initiated by current application on OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access this property defined in [DAE] section 7.4.3 • Check for the security requirement for remote diagnostic and management API (if it is supported) o Check that authenticated server, which has necessary privilege, interact with remote diagnostic and management functionality of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access any of the classes, properties or methods defined in [DAE] section 7.11.1 • Check for the security requirement for parental control manager (if it is supported) o Check that authenticated server, which has necessary privilege, interact with parental control manager functionality of OITF o *Check that OITF throws an error as defined in [DAE] section 10.1.1, when loaded application from server tries to access any of the classes, properties or methods defined in [DAE] section 7.9.1
Preconditions	• *Server does not have the necessary privileges or it is not properly authenticated • The Testing Target is configured with the Test Manager • OITF is authenticated on the network and has launched the first page
Priority	Mandatory
Remark	

5.5 Procedural Application Environment (PAE)

No test areas are defined for the Procedural Application Environment

5.6 Authentication, Content Protection and Service Protection (CSP)

The test area for CSP can be divided into the following parts:

- User Authentication
- Content Protection (DRM functionality)
  - Terminal Centric Approach
  - Gateway Centric Approach
    - CI+ based Gateway Centric Approach

- OITF side testing
- CSPG-CI+ side testing

- DTCP-IP based Gateway Centric Approach
  - OITF side testing
  - CSPG-DTCP side testing

5.6.1 User Authentication

5.6.1.1 Prerequisites

None

5.6.1.2 Test Method

As referred to in Figure 7, the Test Manager configures the OITF driver and the Test driver according to the test case requirement. The configuration done enables the proper sequence of messages between the Test Target and the Test Server. Test drivers are used to trigger the message flow between the OITF and the Test Server. The sequence of this message flow will be controlled by the Test Manager. Testing will also require some network analysing tools. The test case will be the message flow sequence between the OITF and the Test Server. For this, a DAE application will run on the OITF functioning as the OITF Driver, as described below. It will inform the Test Manager about the current test case under execution. The Test Manager will then appropriately configure the Test Server for sending response messages as required by the test case.

For User Authentication, interactions done over the UNIS-14 interface between the OITF and the SAA will be tested. A request for authentication will be triggered from the OITF and then the SAA checks the details from the user database and responds accordingly. The details in the user database can be varied to create various scenarios for user authentication, e.g. in case of HTTP digest authentication, the OITF will send a user name, password and a particular value based on the user name and password on the basis of which authentication will be done. The OITF Driver can request the Test Manager to provide a DAE application which can be an HTML page which will ask the user for their user ID and password. This ID and password will be checked asynchronously by a PHP script running on the SAA (simulated authentication server). If the authentication is successful then the user is considered a valid user.

The testable aspects of User Authentication are interactions between the OITF and the SAA and between the SAA and the user database for adherence to a specific User Authentication Protocol.

- Checking the message flow for the request and response sequence and the specific fields within these request/response messages according to the protocol used.

5.6.1.3 Test Environment

The test environment for CSP User Authentication is displayed in Figure 7 and each component in the environment is described below.

- Test Manager:

  It controls the test environment according to the test case. For this, it configures the OITF driver and the Test driver (for the Test Server) to manage the sequence of messages according to the test case to be executed.

- Test Target:

  It contains the OITF functionality.

- Test Server:

  It contains the SAA Simulator.

- OITF Driver:

  It triggers the OITF target to check the authentication procedures with the SAA simulator. It will be a DAE application.

- Test Driver:

  It triggers the Test Server to control the authentication procedures with the SAA simulator and User Database.

- OITF Test Target:

  It contains the OITF functionality. Initial requests for testing will be triggered from here.

- SAA Simulator:

  It contains the SAA functionality. It will communicate with the OITF and the user database for user authentication.

- User Database Simulator:

  It contains the user database functionality. It helps the SAA in retrieving details about the user being authenticated.

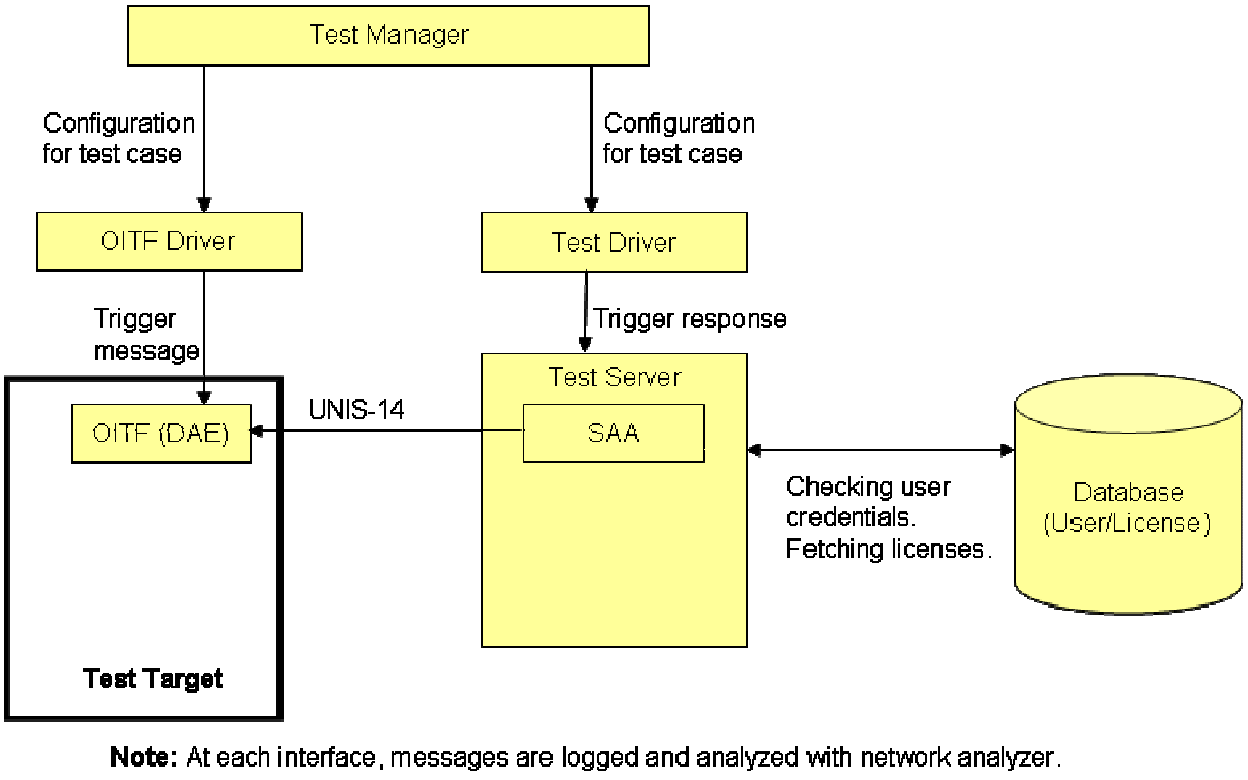

Figure 7 - Test Environment for CSP – User Authentication

5.6.1.4 Test Specification for CSP – User Authentication

Test Specification ID	OIPF-CSP-HTTP-001
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Check that the OITF support basic HTTP capabilities
Specification Section(s)	[CSP] §5.2.3
Test Cases	• Verifies OITF supports service initiation through an HTTP GET request • Verifies OITF support for re-direction during service initiation • Verifies OITF support for HTTP URL Parameters at service redirection • Verifies OITF support for Cookies • Verifies OITF support for HTML forms • Verifies OITF support for HTTP POST forms • Verifies OITF supports TLS • Verifies OITF supports SSL
Preconditions	• Test Object is connected to reference network • Test Object is successfully powered on
Priority	Mandatory
Remark	

Test Specification ID	OIPF-CSP-AUTH-001
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Check that the OITF support Authentication Capabilities
Specification Section(s)	[CSP] §5.4.4
Test Cases	• Verifies OITF initiates initial GBA request after successful user registration • Verifies OITF initiates Initial GBA procedure after successful user registration • Verifies OITF retrieval for the GBA keys needed for an HTTP session • Verifies OITF initiates an HTTP session using GBA authentication. Requested service supports GBA • Verifies OITF performs HTTP Digest using GBA authentication. Requested service supports GBA.
Preconditions	• Test Object is connected to reference network • Test Object is successfully powered on
Priority	Mandatory
Remark	

Test Specification ID	OIPF-CSP-AUTH-002
Test Specification Version	1.0.0
Test Object	IG
Test Specification Description	Check that the IG support Authentication Capabilities
Specification Section(s)	[CSP] §5.4.4
Test Cases	Verifies IG supports the GBA authentication procedure when triggered by OITF to perform it
Preconditions	• Test Object is connected to reference network • Test Object is successfully powered on
Priority	Mandatory
Remark	

Test Specification ID	OIPF-CSP-IMS-001
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Check that the OITF support IMS registration
Specification Section(s)	[CSP] §5.5
Test Cases	• Verifies OITF initiation of an HNI-IGI registration Request (IMS AKA) • Verifies OITF initiation of an HNI-IGI registration Request (SIP DIGEST)
Preconditions	• Test Object is connected to reference network • Test Object is successfully powered on
Priority	Mandatory
Remark	

Test Specification ID	OIPF-CSP-IMS-002
Test Specification Version	1.0.0
Test Object	IG
Test Specification Description	Check that the IG support IMS registration
Specification Section(s)	[CSP] §5.5
Test Cases	• Verifies IG support performing IMS-AKA registration

	• Verifies IG support performing SIP Digest Based authentication • Verifies IMS registration (IMS-AKA) at IG power up • Verifies IMS registration (SIP Digest) at IG power up
Preconditions	• Test Object is connected to reference network • Test Object is successfully powered on
Priority	Mandatory
Remark	

Test Specification ID	OIPF-CSP-SESSION-001
Test Specification Version	1.0.0
Test Object	OITF
Test Specification Description	Check that the OITF support session management
Specification Section(s)	[CSP] §5.6
Test Cases	• Verifies OITF support for Cookie Session – Storing Cookie • Verifies OITF support for Cookie Session – Updating Cookie • Verifies OITF support for cookie deletion by a user • HTTP Authentication Session – Sharing Authentication Parameters (HTTP Basic) • HTTP Authentication Session – Sharing Authentication Parameters (HTTP Digest) • HTTP Authentication Session – Sharing Authentication Parameters (GBA Credentials)
Preconditions	• Test Object is connected to reference network • Test Object is successfully powered on
Priority	Mandatory
Remark	

5.6.2 Terminal Centric Approach

5.6.2.1 Prerequisites

None

5.6.2.2 Test Method

As shown in Figure 8, the Test Manager configures the OITF driver and the Test driver according to test case requirements. The configuration done enables the proper sequence of messages between the Test Target and the Test Server. Test drivers are used to trigger the message flow between the OITF and the Test Server. The sequence of this message flow will be controlled by the Test Manager. Testing will also require some network analysing tools. The test case will be the message flow sequence between the OITF and the Test Server. For this, a DAE application will run on the OITF functioning as the OITF Driver, as described below. This application will contain JavaScript routines each invoking appropriate CSP agent API calls for triggering the message flow from the OITF for each test case. It will inform the Test Manager about the current test case under execution. The Test Manager will then appropriately configure the Test Server for sending response messages as required by the test case. The OITF Driver will have a JavaScript in which sequence for a particular test case is described. For DRM testing, the DAE application can trigger the test cases through its sendDRMmessage API and can check the result for success or failure through the notification handler (a callback function).

For the terminal centric DRM approach, the License Server will be simulated as the test server. The interactions between the CSP client and the License Server uses the UNIS-CSPT interface, which needs to be tested as per the specification of the content protection solution used. For example, when using the Marlin Protocol for the case of License Evaluation, various message exchanges will be tested. Messages can be of different types, such as the request to acquire the License Evaluation action token, the Configuration token etc. It can be achieved by varying the value of the first parameter in the DAE sendDRMmessage(…) API. For the license evaluation, there can again be different test cases generated. In the license database, we can vary the format of licenses to inject invalid licenses and ensure that the CSP client responds with a proper error message. The message flow is that the License Server interacts with the License database and fetches the license which will be delivered to OITF. This license is given by the OITF to the CSP client, using CSP-1 interface.

- Various scenarios for the testable aspects of the Terminal Centric DRM Approach, using the Marlin protocol could be:
  - Marlin Registration
    - Node Acquisition
    - Link Acquisition
  - License Acquisition
  - License Evaluation
  - Marlin Deregistration

5.6.2.3 Test Environment

The test environment for CSP Terminal Centric Approach is displayed in Figure 8, and each component in the environment is described below.

- Test Manager:

  It controls the test environment according to the test case. For this, it configures the OITF driver and the Test driver (for the Test Server) to manage the sequence of messages according to the test case to be executed.

- Test Target:

  It constitutes the OITF and the CSP client.

- Test Server:

  It constitutes the SAA Simulator and the CSP-T Server.

- OITF Driver:

  It triggers the OITF target to send the sequence of authentication/DRM messages to the SAA simulator or the CSP-T Server as per the test case. It will be a DAE application and it will communicate with the test manager for obtaining the DRM message sequence specification from the test manager.

- Test Driver:

  It triggers the Test Server to send the sequence of authentication/DRM messages to the OITF, User Database and the License Database as per the test case.

- OITF Test Target:

  It contains the OITF functionality. Initial requests for testing will be triggered from here.

- SAA Simulator:

  It contains the SAA functionality. It will communicate with the OITF and the user database for user authentication.

- User Database Simulator:

  It contains the user database functionality. It helps the SAA in retrieving details about the user for authentication.

- CSP-T Server:

  It contains the CSP-R Server functionality. For example, it can be used to simulate the Marlin Broadband Server (Bluewhale) functionality as per the case test case requirements for testing the Terminal Centric DRM approach.

- CSP Client:

  It is the CSP Agent functionality in the Residential Network.

- License Database:

  It provides the required licenses required to view the protected content.

  .

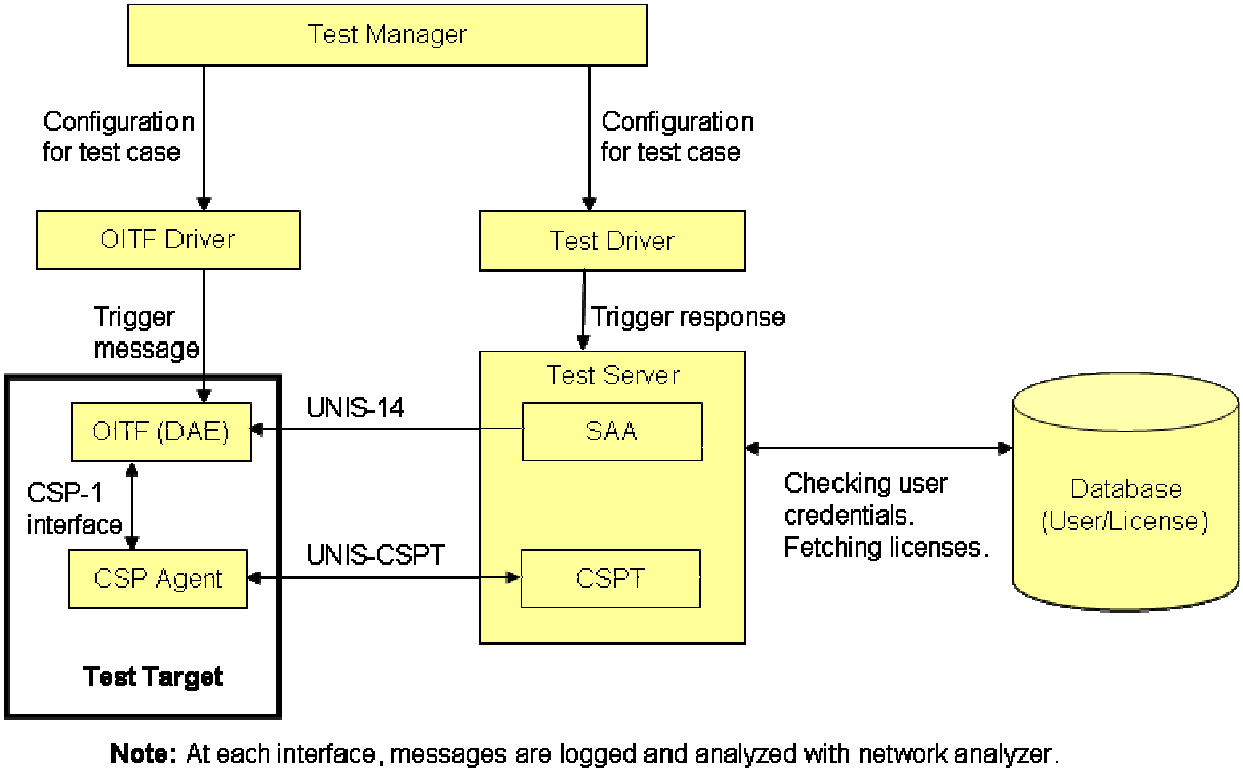

Figure 8 - Test Environment for CSP – Terminal Centric Approach

5.6.3 CI+ based Gateway Centric Approach

5.6.3.1 Prerequisites

None

5.6.3.2 Test Method

This involves the testing of the interface and integration with the CSPG-CI+ module including:

- Playing protected A/V content.
- Command interface to the CSPG-CI+.

The tests will be performed using a DAE application running on the target. The DAE application allows:

- Playing protected content using the A/V plug-in object, e.g. the CEA-2014-A A/V streaming object or the video/broadcast object.
- Sending messages to the CSPG-CI+ module and catching events from the CSPG-CI+ module using the application/oipfDrmAgent object.

The following parts cannot be tested, as they are not defined in the Open IPTV Forum specification:

- CSPG-CI+ protected content played from a native application.
- Use of CSPG-CI+ specific metadata, as defined in [CSP] section 4.2.3.10

5.6.3.2.1 OITF side testing of the CSPG-CI+ module,

The CSPG-CI+ module plugged in to the OITF is a CSPG-CI+ test module which has an IP connection to the CSP-G test server (this connection is made via the IP connection of the OITF).

To avoid the need for a complete CAS system, the behaviour of the CSPG-CI+ Test module is driven by the Test Manager, using the IP connection established between a CSP-G test server and a CSPG-CI+ test module. Note: In test descriptions, all requests from the Test Manager to the CSPG-CI+ Test Module, and reports from the CSPG-CI+ to the Test Manager are proxied through the CSP-G Test Server.

The Test DAE application, Web Test Server or CSP-G Test Server report the test results to the Test Manager.

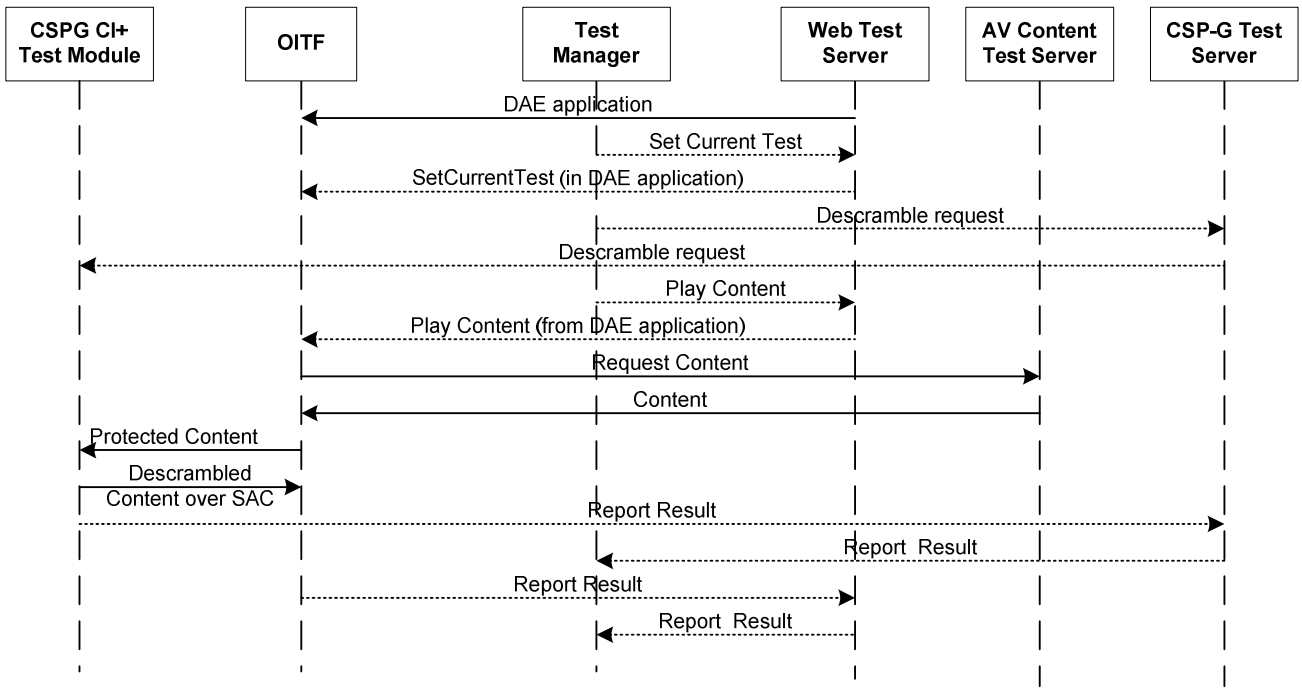

Figure 9 - Sequence diagram of a descrambling test

As an example, Figure 9 presents the sequence diagram for a descrambling test. This is a simplified view of the exchanges between the different elements, as it does not show all CI+ exchanges between the OITF and the CSPG-CI+ gateway.

The CSPG-CI+ Test Module is connected to the CSP-G Test Server (via the OITF). The Test Manager controls the behaviour of the CSP-G CI+ Test Module via the CSP-G Test Server.

The Test Manager drives the test via the Web Test Server and the Test DAE application by setting which test must be performed.

In this sequence:

- The DAE application requests playing of the protected content (as requested by Test Manager).
- The OITF gets the protected content from the A/V Content Test Server and passes it to CSPG-CI+ test module.
- The CSPG-CI+ test module descrambles the content (as requested by Test Manager).
- The DAE application and CSPG-CI+ test module report the test results to the Test Manager.

Note that even if no specific CAS system has to be specified, content has to be scrambled. The content is scrambled using a fixed CW. This scrambling is signalled in the Transport Scrambling Control Bits by setting them to 01 (Scrambling with the DEFAULT content key). The TEST_CAS_SYSTEM_ID is signalled as usual in the PMT of the MPEG2-TS stream.

5.6.3.2.2 CSPG-CI+ testing

The OITF is a Reference OITF supporting CSPG-CI+.

The CSPG-CI+ manufacturer will be provided with test data from the test database to adapt:

- Test AV content in clear, to protect it with the CAS system in the CSPG-CI+ module.
- Test web pages, to adapt them with CAS or CSPG-CI+ specific messages.
- Metadata files, to adapt them with CAS or CSPG-CI+ specific messages

The CSPG-CI+ manufacturer will provide the adapted test data and the optional Head-End Server (CSP-G Server).

5.6.3.3 Test Environment

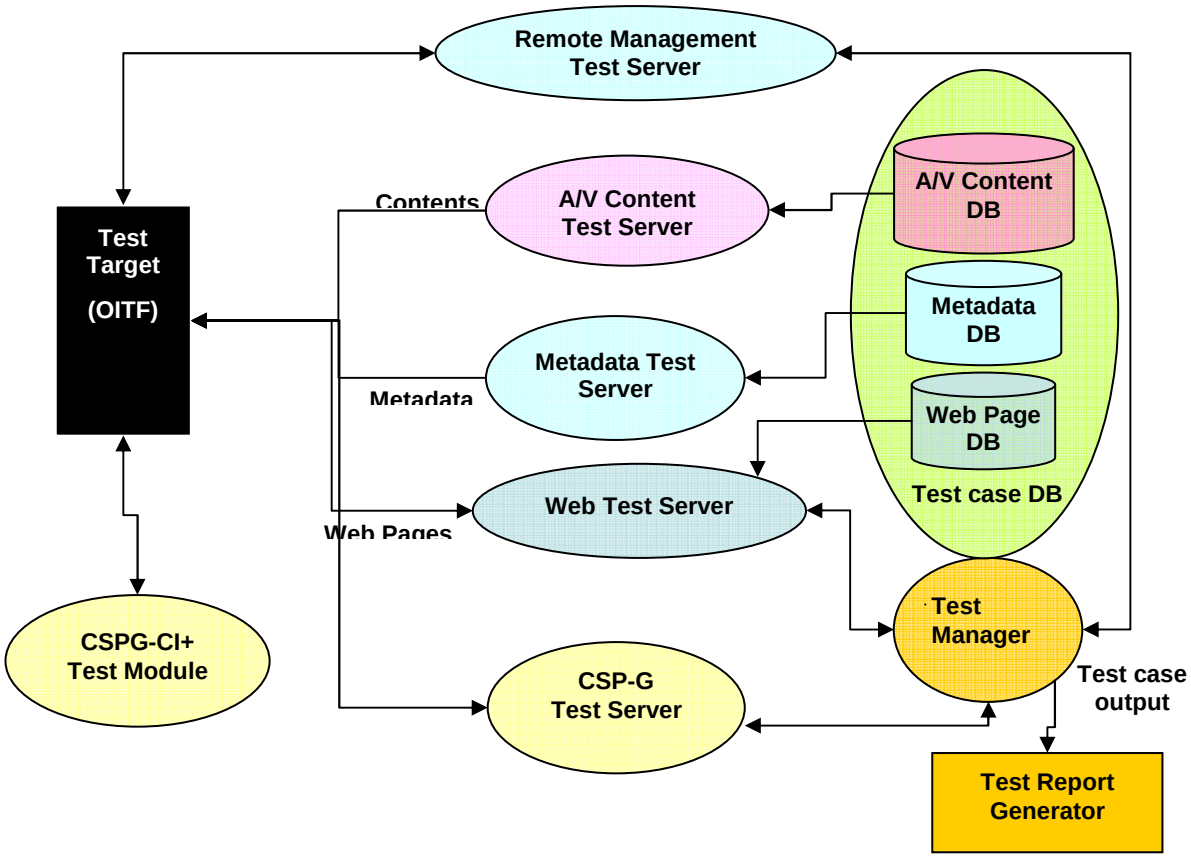

Figure 10 - Test Environment for CSP – CSPG-CI+ OITF side testing

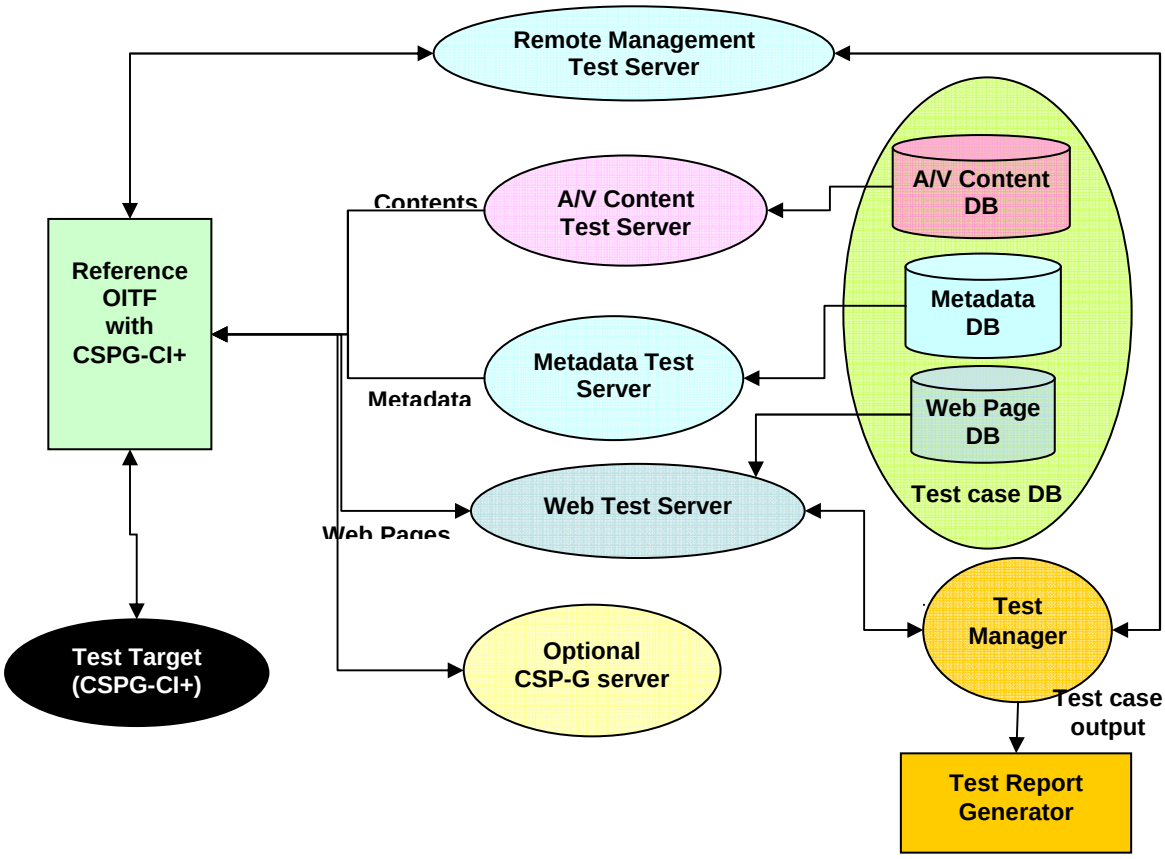

Figure 11 - Test Environment for CSP – CSPG-CI+ testing

The test environment for OITF side testing of CSPG-CI+ is displayed in Figure 10, and the test environment for CSPG-CI+ testing is displayed in Figure 11. Each component in these test environments is described below.

- Test Case Data Base:

  It consists of the A/V content database, web page database and metadata database.

  - A/V content database:

    The A/V content streams are stored in the A/V content database.

  - Web page database:

    The web pages are stored in the web page database.

  - Metadata database:

    The metadata files are stored in the metadata database

- Web Test Server:

  It provides the DAE web pages from the web page database to the target.

- A/V Content Test Server:

  The A/V Content Test Server (acting as the Content Delivery FE) delivers content (i.e., scheduled content or CoD) to the target. It can be configured by the Test Manager to deliver appropriate content to the test target (i.e. the OITF).

- Remote Management Test Server:

  The Remote Management Test Server allows managing the OITF through TR-069 stacks and protocols. It is configurable by the Test Manager.

- Metadata Test Server:

  It provides metadata to the target. It can be configured by the Test Manager to deliver appropriate metadata to the test target (i.e. the OITF) or the Reference OITF.

- CSPG-CI+ Test Module

  It consists of a CI+ module implementing CSPG-CI+ functions and triggering CSPG-CI+ events and functions. It embeds the test CAS function and is conformant with the OIPF specific requirements (SAS resource management including OIPF_APPLICATION_ID and OIPF CSPGCI+ dedicated APDUs).

- Standard DVB-CI Module

  A standard DVB-CI module is needed to test operations in the CI+ mode only. It is not represented on the figure. The CSPG-CI+ Test Module could also be pre-configured to work in DVB-CI mode only for the same purpose.

- CSP-G Test Server

  It communicates via the test target (OITF) with the CSPG-CI+ test module for the testing of the CI+ low speed communication functionality. It stands for the CI+ CSP-G Server.

- Optional CSP-G Server

  It communicates via the OITF with the Test Target (CSPG-CI+). It is provided, if necessary, by the CAS vendor.

- Test Target (OITF):

  This is the tested OITF entity for CSPG-CI+ OITF side testing.

- Reference OITF with CSPG-CI+:

  This is the reference OITF entity for CSPG-CI+ side testing. It includes a native application which allows testing of specific CSPG-CI+ APDUs, which are not interfaced to DAE applications.

- Test Target (CSPG-CI+):

  This is the tested CSPG-CI+ module for CSPG-CI+ testing. It is associated with the CSPG-CI+ Server.

- Test Manager

  This entity controls the overall testing. It configures the different test servers and checks the results.

- Test Report Generator (TRG):
  This entity is responsible for maintaining the test logs. The test management interface will be used to record management information generated by the Test Manager.

5.6.3.4 Test Specification for CSP – CI+ based gateway Centric Approach

5.6.3.4.1 OITF - Discovery and capabilities

Test Specification ID	OIPF-CSP-OITF-CI+-001
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – CSPG-CI+ discovery and signalling in capabilities -
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3 [DAE] §7.7, [DAE] §9.3.10 [PROT] §5.3.1, [PROT] §6.3.1, [PROT] Annex K, [PROT] Annex D.2
Test Cases	• CSPG-CI+ discovery using DAE Gateway Discovery and Control APIs • Signalling of CSPG-CI+ support using CEA-2014-A capability negotiation and extensions • Signalling CSPG-CI+ capabilities using TR-069 • Signalling CSPG-CI+ capabilities in UE Profile in IMS Service Discovery Procedure.
Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to metadata and web pages
Priority	Optional
Remark	

5.6.3.4.2 OITF - CI+ low-speed communication resource

Test Specification ID	OIPF-CSP-OITF-CI+-002
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – Support for CI+ low speed communication resource
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	CI+ low-speed communication resource
Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to test A/V contents, metadata and web pages
Priority	Optional
Remark	

5.6.3.4.3 OITF - Operation in CI+ mode only

Test Specification ID	OIPF-CSP-OITF-CI+-003
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – Operation in CI+ mode only
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	Operation in CI+ mode only

Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to test A/V contents, metadata and web pages
Priority	Optional
Remark	Either a standard DVB-CI module is needed or the CSPG-CI+ Test Module is pre configured to work in DVB-CI mode only

5.6.3.4.4 OITF - Integration to DAE application

Test Specification ID	OIPF-CSP-OITF-CI+-004
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – Integration to DAE application
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	• Management of DRM messages • Management of rights events • Management of parental control events
Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to test A/V contents, metadata and web pages
Priority	Optional
Remark	

5.6.3.4.5 OITF - Protected content handling

Test Specification ID	OIPF-CSP-OITF-CI+-005
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – Protected content handling
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	• Scheduled content sent in multicast mode • On demand content sent in unicast streaming mode • On demand content sent in unicast HTTP mode • On demand content downloaded
Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to test A/V contents, metadata and web pages
Priority	Optional
Remark	

5.6.3.4.6 OITF – Metadata handling

Test Specification ID	OIPF-CSP-OITF-CI+-006
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – Metadata handling
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	• Content Access Download Descriptor with metadata for CSPG-CI+ • Content Access Streaming Descriptor with metadata for CSPG-CI+

Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to test A/V contents, metadata and web pages
Priority	Optional
Remark	

5.6.3.4.7 OITF – Personal Video Recorder and Time-Shifting

Test Specification ID	OIPF-CSP-OITF-CI+-007
Test Specification Version	1.0.0
Test Object(s)	OITF
Test Specification Description	Support for CI+ based gateway-centric approach – Personal Video Recorder and Time-Shifting
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	• Personal Video Recorder with CI+ PVR resource • Personal Video Recorder with CI+ URI • Time shifting with CI+ PVR resource • Time shifting with CI+ URI
Preconditions	• The Test Object/Testing Target OITF is connected to the test network • Test Object should have access to test A/V contents, metadata and web pages
Priority	Optional
Remark	

5.6.3.4.8 CSPG-CI+ - Discovery and capabilities

Test Specification ID	OIPF-CSP-CSPG-CI+-001
Test Specification Version	1.0.0
Test Object(s)	CSPG-CI+
Test Specification Description	Support for CI+ based gateway-centric approach – Discovery and capabilities
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	CSPG-CI+ discovery
Preconditions	• Reference OITF supporting CSPG-CI+ is successfully connected to the test bench. • Reference OITF should have access to test A/V contents, metadata and web pages • The test target CSPG-CI+ module is inserted in the CI slot.
Priority	Mandatory
Remark	

5.6.3.4.9 CSPG-CI+ - Protected content handling

Test Specification ID	OIPF-CSP-CSPG-CI+-002
Test Specification Version	1.0.0
Test Object(s)	CSPG-CI+
Test Specification Description	Support for CI+ based gateway-centric approach – Protected content handling
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	MPEG-2 TS handling
Preconditions	• Reference OITF supporting CSPG-CI+ is successfully connected to the test bench. • Reference OITF should have access to test A/V contents, metadata and web pages

	• The test target CSPG-CI+ module is inserted in the CI slot.
Priority	Mandatory
Remark	

5.6.3.4.10 CSPG-CI+ - APDU handling

Test Specification ID	OIPF-CSP-CSPG-CI+-003
Test Specification Version	1.0.0
Test Object(s)	CSPG-CI+
Test Specification Description	Support for CI+ based gateway-centric approach – APDU handling
Specification Section(s)	[CSP] §4.2.1, [CSP] §4.2.2, [CSP] §4.2.3
Test Cases	• DRM message APDUs • Rights info/error event APDU • Parental control info/error APDUs • Parental control APDUs • Access info APDU
Preconditions	• Reference OITF supporting CSPG-CI+ is successfully connected to the test bench. • Reference OITF should have access to test A/V contents, metadata and web pages • The test target CSPG-CI+ module is inserted in the CI slot.
Priority	Mandatory
Remark	

5.6.4 DTCP-IP based Gateway Centric Approach

No test areas are defined for this function.

6 SOLUTION INTEROPERABILITY TEST

6.1 Test Method

Solution Interoperability Test validates the interworking of the test device with other functions that comprise the IPTV solutions. Important issues such as message sequencing, the execution order of methods and inter-function dynamics can be addressed. In this type of testing, the whole of IPTV system should be modelled for its behaviour either in the form of simulators or reference nodes..

The test environment consists of a Test manager and several simulators. The Test Manager includes various supporting tools required for testing such as the Test Report Generator, Protocol Analyzer, etc. Each simulator represents a device or system which is provided as part of an IPTV system. The simulator which represents the functionality of the test device is replaced with the actual target device and tested is coordinated by the Test Manager. The Test Manager performs test cases for the target device, and reports the test results and controls the simulators to set the conditions and to get logs from the simulators if necessary.

The test cases for Solution Interoperability Test will be developed based on the usage scenarios. Most test cases will be performed through the OITF simulators using DAE or PAE applications.

The test items for solution interoperability are as follows:

1) Device Startup
2) Service Selection
3) User Login and Authentication
4) EPG
5) Scheduled Content Selection
6) On Demand Content Selection
7) Parental Control
8) Communication Services
    - Caller ID
    - Instant Messaging
    - Presence

An additional sub-section will also be used for administration operation scenario testing.

For each usage scenario, test cases may be written for multiple use cases impacting different functional entities.

6.2 Test Environment

The test environment for Solution Interoperability Test is shown in Figure 12, and the components in the environment are described below.

- Test Manager:

  It works with the OITF simulator. It can have a connection to Target Device for getting log messages. It controls the simulators to set the conditions and gets the logs from the simulators. It routes the requests and responses to the OITF. It should provide a report after testing.

- Target Device:

  It is the actual device under test. It should be requested from the Test Manager and the test is performed within the Test Environment. The functionality of the device under test is checked by checking responses at the OITF simulator.

- Simulators:

  They are a part of Test Environment. A simulator is replaced by the actual device to be tested. Each simulator has to perform as a device itself inside the Test Environment.

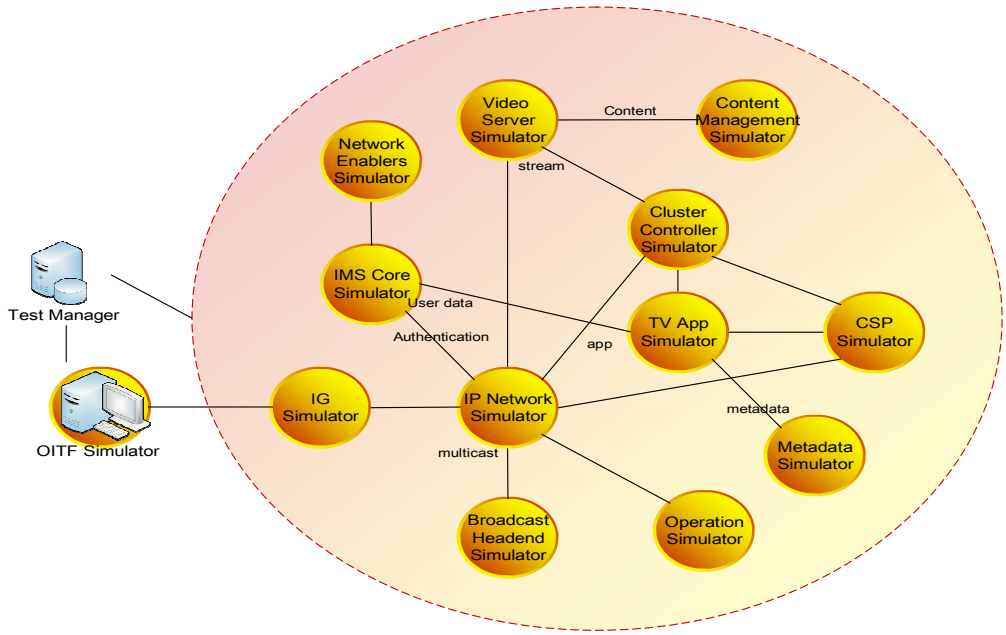

Figure 12 - Test Environment for Solution Interoperability Test

6.3 Test Specification for Solution Interoperability Test

6.3.1 Device Startup

Test Specification ID	OIPF-SIT-STRT-GW-001
Test Specification Version	1.0.0
Test Object(s)	WG, AG, IG, Network Attachment, ASM
Test Specification Description	Startup of gateway functions located in the residential network.
Specification Section(s)	
Test Cases	• Startup and initialization of the WG. • Startup and initialization of the AG. • Startup and initialization of the IG.
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-STRT-OITF-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, AG,WG, CSPG-DTCP
Test Specification Description	Startup of the OITF
Specification Section(s)	
Test Cases	• Startup and initialization of the OITF in a managed network with native HNI-IGI support • Startup and initialization of the OITF in a managed network with non-native HNI-IGI • Startup and initialization of the OITF in an unmanaged network
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-STRT-OITFIG-001
Test Specification Version	1.0.0
Test Object(s)	OITF/IG, AG,WG, CSPG-DTCP
Test Specification Description	Startup of a device containing both the OITF and IG functions
Specification Section(s)	
Test Cases	• Startup and initialization of the integrated OITF/IG in a managed network with no HNI-IGI support
Precondition	None
Priority	Mandatory
Remark	

6.3.2 Service Selection

Test Specification ID	OIPF-SIT-SPSEL-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, IPTV Service Provider Discovery, ASM
Test Specification Description	Validates the ability to retrieve Service Provider Discovery information
Specification Section(s)	
Test Cases	• OITF request the information about the IPTV Service Providers and it is delivered as a Web page for Unmanaged networks • OITF request the information about the IPTV Service Providers and it is delivered as a Web page for Managed networks • OITF request the information about the IPTV Service Providers based on a XML data– SD&S records, such as a DVB IP Service Provider(s) Discovery Record, for Unmanaged networks • OITF request the information about the IPTV Service Providers based on a XML data– SD&S records, such as a DVB IP Service Provider(s) Discovery Record, for Managed networks
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-SVCSEL-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Application, Transport Processing Function, IG, IPTV Service Discovery
Test Specification Description	Verifies the ability to retrieve and select service access information
Specification Section(s)	
Test Cases	• OITF request the information about the IPTV Services and it is delivered as a Web page for Unmanaged networks • OITF request the information about the IPTV Services and it is delivered as a web page for Managed networks • OITF request the information about the IPTV Services based on a XML data– SD&S records, for Unmanaged networks • OITF request the information about the IPTV Services based on a XML data– SD&S records, for Managed networks
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-SVCACC-001
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function, IPTV Metadata Control, IPTV Application
Test Specification Description	Check the retrieval of the Content Guide after the selection of an IPTV service.
Specification Section(s)	
Test Cases	• The OITF request the Content Guide via multicast for Managed Networks • OITF request Content Guide (via unicast) as Metadata for Managed Networks • OITF request Content Guide (via unicast) as Web page for Managed Networks • OITF request Content Guide (via unicast) as Metadata for Unmanaged Networks • OITF request Content Guide (via unicast) as Web page for Unmanaged Networks • OITF request Content Guide (via unicast) as Metadata for Managed Networks • OITF request Content Guide (via unicast) as Web page for Managed Networks
Precondition	None
Priority	Mandatory
Remark	

6.3.3 User Login and Authentication

No interoperability test cases are defined for this function.

6.3.4 EPG

No interoperability test cases are defined for this function.

6.3.5 Scheduled Content Selection

Test Specification ID	OIPF-SIT-SCHD-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, ASM, IPTV Control, IPTV Service Profile, Transport Processing Function
Test Specification Description	Verifies delivery of Scheduled Content in a managed network
Specification Section(s)	
Test Cases	• User requests to watch Scheduled Content in a Managed Network to be delivered over RTP • User requests to watch Scheduled Content in a Managed Network to be delivered over UDP. • User requests to watch different Scheduled Content (channel zapping) in a Managed Network • User requests to watch different Scheduled Content with different bandwidth requirements (channel zapping) in a Managed Network (SD->HD) • User requests to watch different Scheduled Content with different bandwidth requirements (channel zapping) in a Managed Network (HD→SD) • User requests to stop watching Scheduled Content in a Managed Network by terminating session (e.g.: selecting alternative IPTV service)
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-SCHD-002
Test Specification Version	1.0.0
Test Object(s)	OITF, Transport Processing Function
Test Specification Description	Verifies delivery of Scheduled Content in an unmanaged network

Specification Section(s)	
Test Cases	• User requests to watch Scheduled Content in an Unmanaged Network to be delivered over RTP. • User requests to watch different Scheduled Content (channel zapping) in a Unmanaged Network over RTP. • User requests to stop watching Scheduled Content in an unmanaged Network.
Precondition	None
Priority	Mandatory
Remark	

6.3.6 On Demand Content Selection

Test Specification ID	OIPF-SIT-COD-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG ASM, IPTV Control, CDNC, CC, CDF
Test Specification Description	Content on Demand in a managed network
Specification Section(s)	
Test Cases	• User requests to watch Content on Demand in a Managed Network • User requests to pause a Content on Demand using trick-play in a Managed Network • User requests to fast forward a Content on Demand using trick-play in a Managed Network • User requests to fast rewind a Content on Demand using trick-play in a Managed Network • Content on Demand is played until End of Stream is reached in a Managed Network • Content on Demand is Fast Forwarded until End of Stream is reached in a Managed Network • Content on Demand is Fast Rewind until Beginning-of-Stream is reached in a Managed Network • Content on Demand session is terminated in a managed network; User presses the STOP button • OITF Support the retrieval of CoD Playback information .in a Managed Network
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-COD-002
Test Specification Version	1.0.0
Test Object(s)	OITF, IPTV Application, IPTV Service Profile, CDNC, CC, CDF
Test Specification Description	Content on Demand in an unmanaged network
Specification Section(s)	
Test Cases	• User requests to watch Content on Demand in an Unmanaged Network • User requests to pause a Content on Demand using trick-play in an Unmanaged Network • User requests to fast forward a Content on Demand using trick-play in an Unmanaged Network • User requests to fast rewind a Content on Demand using trick-play in an Unmanaged Network • Content on Demand is played until End of Stream is reached in an Unmanaged Network • Content on Demand is Fast Forwarded until End-of-Stream is reached in an Unmanaged Network • Content on Demand is Fast Rewind until Beginning of Stream is reached in a Unmanaged Network

	• Content on Demand session is terminated in a Unmanaged Network; User presses the STOP button • OITF Support the retrieval of CoD Playback information in an Unmanaged Network.
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-COD-003
Test Specification Version	1.0.0
Test Object(s)	OITF, CDF
Test Specification Description	HTTP progressive delivery of Content on Demand
Specification Section(s)	
Test Cases	• User requests to watch Content on Demand in a Managed or Unmanaged Network using HTTP Streaming. • User requests to pause Content on Demand streaming in a Managed or Unmanaged Network using HTTP Streaming. • User requests to fast forward Content on Demand streaming in a Managed or Unmanaged Network using HTTP Streaming. • User requests to fast rewind Content on Demand streaming in a Managed or Unmanaged Network using HTTP Streaming.
Precondition	None
Priority	Mandatory
Remark	

6.3.7 Parental Control

No interoperability test cases are defined for this function.

6.3.8 Communication Services

6.3.8.1 Caller ID

Test Specification ID	OIPF-SIT-CID-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, ASM
Test Specification Description	Verifies indication of incoming Caller ID on OITF
Specification Section(s)	
Test Cases	• Verify incoming Called ID display message • Verify IMS Telephony based Caller ID (Voice included in SDP)
Precondition	None
Priority	Mandatory
Remark	

6.3.8.2 Instant Messaging

Test Specification ID	OIPF-SIT-IM-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, ASM
Test Specification Description	Verifies general instant messaging functionality
Specification Section(s)	
Test Cases	• Verify Originating Message

	• Verify Incoming Message
Precondition	None
Priority	Mandatory
Remark	

Test Specification ID	OIPF-SIT-IM-002
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, ASM
Test Specification Description	Verifies instant message exchange according to the MSRP protocol
Specification Section(s)	
Test Cases	• Initiating chatting session + setup MSRP path • Sending MSRP Chatting • Sending "Iscomposing "chat State • Receiving MSRP Chatting • Receiving MSRP chat state "IsComposing" • Terminating an IM Session Originating side MSRP Chat • Remote Terminating an IM Session (MSRP Chat) • Remote Initiating IM Session (MSRP Chat)
Precondition	None
Priority	Mandatory
Remark	

6.3.8.3 Presence

Test Specification ID	OIPF-SIT-PRES-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, ASM
Test Specification Description	Verifies establishment and operation of presence functions
Specification Section(s)	
Test Cases	• Subscription to Presence • Cancel Presence Subscription • Refresh Subscription to Presence • Publish Presence Information • Refresh Publish Presence Information
Precondition	None
Priority	Mandatory
Remark	

6.3.9 Administrative Operations

Test Specification ID	OIPF-SIT-ADMIN-UPGR-001
Test Specification Version	1.0.0
Test Object(s)	OITF, IG, IPTV Applications
Test Specification Description	Verify the possibility for a OITF to be upgraded from capabilities defined in the BMP profile to those defined in the EMP profile.
Specification Section(s)	
Test Cases	• Check the OITF Profile Upgrade from BMP to EMP
Precondition	None
Priority	Mandatory
Remark	