

HbbTV Specification Errata 2

August 2nd 2012



Copyright 2011-2012 HbbTV Association

Some material contained herein is the copyright of, or has been supplied by the Digital TV Group

Table of Contents

1	Introduction.....	7
2	Conventions.....	7
3	Summary.....	7
4	Technical Changes to TS 102 796.....	15
4.1	General.....	15
4.1.1	RTSP.....	15
4.2	Clause 1 - Scope.....	15
4.2.1	Signalling of broadcast-independent applications.....	15
4.3	Clause 2 – References.....	15
4.3.1	Permit either TLS 1.2 (RFC 5246) or TLS 1.0 (RFC2246) or 1.1 (RFC4346).....	15
4.3.2	CI+ Usage.....	16
4.3.3	Open IPTV Forum Errata.....	16
4.3.4	URL Entry.....	16
4.3.5	Encoding of numbers in XML.....	16
4.3.6	Cookie size.....	16
4.3.7	Application domain.....	16
4.3.8	Supported Audio Formats.....	16
4.3.9	Clarification of query strings in URIs passed to createApplication.....	16
4.3.10	XML Capabilities - String Matching.....	17
4.4	Clause 6 – Service and Application Model.....	17
4.4.1	Failure to start an application.....	17
4.4.2	Revised Section 6.3.....	17
4.4.5	Changes to clause 6.2.2.6.....	18
4.4.7	No application started from recorded broadcast content.....	19
4.4.8	AIT Updates.....	19
4.4.9	What to do after Application loading via DSMCC fails.....	20
4.4.10	Error reporting for application failure.....	23
4.4.12	Impact of linking outside application domain on broadcast AV.....	23
4.4.13	Usage of the video/broadcast extension for recording and time shift.....	23
4.4.14	Potential (Security) Issues when transitioning between trust levels.....	24
4.4.15	Behaviour of HbbTV on protected channels - #2 - starting applications.....	25
4.4.16	Definition of "an MPEG program which is not a broadcast service".....	25
4.4.17	Applications exiting on non-broadcast services.....	26
4.4.18	State transition of 6.2.2.7 not mentioned in A.2.4.1.....	26
4.5	Clause 7 – Formats and Protocols.....	26
4.5.1	External application authorization descriptor.....	26
4.5.2	Clarification of subtitle support for broadband streaming.....	26
4.5.3	Permit either TLS 1.2 (RFC 5246) or TLS 1.0 (RFC2246) or 1.1 (RFC4346).....	27
4.5.4	Application visibility in the AIT.....	27
4.5.5	app_id for trusted applications.....	28
4.5.6	Restriction when using the AVC Baseline Profile.....	28
4.5.7	Clarify that both HTTP and HTTPS are supported.....	28
4.5.8	Version.macro should be version.micro.....	28
4.5.9	Clarification on HTTP range header.....	28
4.5.10	Clarification on HTTP redirect methods.....	28
4.5.11	Clarification on HTTP progressive streaming for live content.....	29

4.5.12	Incorrect application type.....	29
4.5.13	Missing text for ApplicationSpecificDescriptor.....	29
4.5.14	Open IPTV Forum Errata.....	29
4.5.15	Clarification of Deferred Association Tag Support.....	29
4.5.16	Clarification of HE-AAC Container Format.....	30
4.5.17	DLNA MP4 File Format Restrictions.....	30
4.5.18	User-Agent Examples.....	30
4.5.19	Use of a Single PID for AIT Signalling.....	30
4.5.20	data_broadcast_id descriptor.....	30
4.5.21	Object carousel caching.....	31
4.5.22	Usage of the video/broadcast extension for recording and time shift.....	31
4.5.23	Tables in 7.3.1.1.....	31
4.5.24	MPEG2TS VoD seeking behaviour.....	32
4.5.25	Application type when more than one AIT is signalled.....	32
4.5.26	Application Domain.....	32
4.5.27	Seeks in MPEG-2 transport streams.....	32
4.5.28	WAV Audio.....	32
4.5.29	Data Services.....	33
4.5.30	Clarification on XML AIT Restrictions.....	33
4.5.31	Receiver mix audio description.....	33
4.5.32	DSM-CC Reference Length.....	34
4.6	Clause 8 – Browser Application Environment.....	34
4.6.1	Stream event listeners and state changes in the video/broadcast object.....	34
4.6.2	Clarify format of XHR responseText on DSM-CC carousel Directories/Stream Event and DVB URL examples.....	35
4.6.3	Intrinsic events and DSMCC stream events.....	35
4.6.4	CI+ Usage.....	35
4.6.5	property 'Name' of StreamEvent.....	36
4.6.6	XHR access to DSM-CC violates XHR specification.....	36
4.7	Clause 9 – System Integration.....	36
4.7.1	Video / broadcast and AV Control object colours.....	36
4.7.2	Textual service identifier in DVB URL.....	36
4.7.3	DVB URL and Starting Applications.....	36
4.7.4	Encoding of numbers in XML.....	37
4.8	Clause 10 – Capabilities.....	38
4.8.1	Clarification on using the keyset object.....	38
4.8.2	Require to store cookies in persistent memory.....	38
4.8.3	URL Entry.....	39
4.8.4	Supported character set.....	40
4.8.5	Broadcast parental access control.....	40
4.8.6	Clarification of valid syntax for application/oipfCapabilities property & method.....	40
4.8.7	Clarification on equivalent fonts.....	41
4.8.8	Mismatch between some VK key codes and W3C spec.....	42
4.8.9	Resolutions greater than 1280x720.....	42
4.8.10	Missing VK_RECORD key.....	42
4.8.11	Clarification of text entry.....	42
4.8.12	Font reference and character set.....	43
4.8.13	Inconsistency between 7.3.1.1 and 10.2.1.....	43

4.8.14	Requirement on platform to include a mechanism to enable / disable subtitles, both for broadcast and for broadband.....	43
4.8.15	Graphics Model Comparison.....	43
4.9	Clause 11 – Security.....	44
4.9.1	CI+ Usage.....	44
4.9.2	SSL / TLS Root Certificates.....	44
4.10	Annex A – OIPF DAE Specification Profile.....	45
4.10.1	Clarify security exceptions for restricted APIs.....	45
4.10.2	CI+ Usage.....	45
4.10.3	Clarification about setChannel().....	47
4.10.4	Clarify what “fail” means.....	47
4.10.5	Access to ProgrammeCollection.....	47
4.10.6	Broadcast-independent applications and tuning failures.....	47
4.10.7	video/broadcast object's setVolume/getVolume methods should be NI.....	48
4.10.8	OnPlayPositionChanged.....	48
4.10.9	AV Control queue clarification.....	48
4.10.10	Open IPTV Forum Errata.....	48
4.10.11	charCode defined as both included and not included.....	48
4.10.12	The video/broadcast object stop method and broadcast-independent applications... ..	48
4.10.13	Usage of the video/broadcast extension for recording and time shift.....	49
4.10.14	onParentalRatingError.....	49
4.10.15	getChannelConfig "trusted" or broadcast-related".....	49
4.10.16	Clarifying supported properties on the ScheduledRecording and Recording classes.....	49
4.10.17	Clarification about A.2.6.1.....	50
4.11	New Annex D – Server root certificate selection policy (informative).....	50
5	Editorial Changes to TS 102 796.....	52
5.1	General.....	52
5.1.1	DAE Reference Error.....	52
5.1.2	PlayStateChangedEvent in HbbTV Spec.....	52
5.2	Clause 2.1 – Normative References.....	52
5.3	Clause 4 - Overview.....	52
5.3.1	Behaviour of HbbTV on protected channels - #1 - communication with the CAM.....	52
5.4	Clause 5 – User experience.....	52
5.4.1	Default Background Colour.....	52
5.4.2	Reference to figure 13.....	53
5.4.3	URL Entry.....	53
5.4.4	Behaviour of HbbTV on protected channels - #3 - system messages and HbbTV applications.....	53
5.4.5	Duplication in Cases E and F.....	54
5.5	Clause 6 – Service and application model.....	54
5.5.1	Application lifecycle example.....	54
5.6	Clause 7 – Formats and Protocols.....	55
5.6.1	Typo in reference to TS 102 809.....	55
5.6.2	Application profile bits.....	55
5.6.3	Signalling of broadcast-independent applications.....	55
5.7	Clause 8 – Browser Application Environment.....	56
5.7.1	Add reference to XML event description file.....	56
5.8	Clause 9 – System Integration.....	56

5.8.1 Incorrect references into the OIPF DAE specification.....	56
5.9 Annex A - OIPF DAE Specification Profile.....	56
5.9.1 Typo in Annex A.....	56
6 Changes and Issues with Referenced Specifications.....	56
6.1 Open IPTV Forum Specifications.....	56
6.1.1 Media Resource Management.....	56
6.1.2 Open IPTV Forum Errata	56
6.1.3 AV Control automatic transition clarification.....	57
6.1.4 Window object.....	57

1 Introduction

The present document has been integrated with HbbTV 1.5 and the text of ETSI TS 102 796 V1.1.1 and proposed to ETSI to become version 1.2.1 of TS 102 796. For avoidance of doubt, the contents of this document have not been reviewed or approved by ETSI and may be changed as part of that process.

This is a temporary document that will have no meaning once ETSI publish TS 102 796 V1.2.1. This document should not be referenced except in documents that will be updated as necessary to reference ETSI TS 102 796 V1.2.1 once that is published.

Test cases will not be developed referencing this document. Test cases for HbbTV receivers implementing TS 102 796 V1.1.1 plus errata (excluding requirements added by HbbTV 1.5) will reference TS 102 796 V1.2.1.

2 Conventions

In this document, text quoted from other documents or to be added to other documents is indented. Fine-grained changes in text from other documents is shown using the underline and strikethrough convention.

3 Summary

The following table summarises the changes included in this document.

Reference	Short Description	Category	Clauses Impacted	Errata Version
94	External application authorization descriptor	Implementation	7.2.3.1	
102	Stream event listeners and state changes in the video/broadcast object	Ambiguity	8.2.1.1	
104	Clarify format of XHR responseText on DSM-CC carousel Directories/Stream Event and DVB URL examples	Ambiguity	8.2.2	
105	Clarification of valid syntax for application/oipfCapabilities property & method	Ambiguity	10.2.4	
106	Clarification of subtitle support for broadband streaming	Ambiguity	7.2.1, 7.3	
108	Clarification of security exception for APIs restricted to broadcast-related applications required	Ambiguity	A.1	
110	Add reference to XML event	Editorial	8.2.1.1	

Reference	Short Description	Category	Clauses Impacted	Errata Version
	description file			
121	Permit either TLS 1.2 (RFC 5246) or TLS 1.0 (RFC2246) or 1.1 (RFC4346)	Implementation	2.1, 7.3.2.3	
124	Use of “Partially obscured” in 10.1.2	Ambiguity	10.1.2	
127	Intrinsic events and DSMCC stream events	Error	8.2.1.3	
128	Application visibility in the AIT	Ambiguity	7.2.3.1	
129	Failure to start an application	Ambiguity	6.2.2.5.3	
131	video presentation by the A/V control object	Ambiguity	10.1.3	
132	app_id for trusted applications	Ambiguity	7.2.3.1	
133	CI+ Usage	Ambiguity, Error	2.2, 8.2.3, 11.4.1, 11.4.2, A.1	
137	Restriction when using the AVC Baseline Profile	Implementation	7.3.1.3	
138	DAE reference error	Editorial	Many	
139	PlayStateChangedEvent in HbbTV Spec	Editorial	Many	
140	Editorial change of table 14 for font reference	Editorial	10.2.1	
141	Http redirect and application boundaries	Ambiguity	6.3	
142	Clarification about setChannel()	Ambiguity	A.1	
143	Clarify that both HTTP and HTTPS are supported	Ambiguity	6.3, 7.2.3.2	
144	Version.macro should be version.micro	Editorial	7.2.3.1	
145	Clarify what “fail” means	Ambiguity	A.2.4.2	
146	Access to ProgrammeCollection	Ambiguity	A.1	
147	Fixing conditions under which broadcast-independent applications can become broadcast-related	Error	6.2.2.6	

Reference	Short Description	Category	Clauses Impacted	Errata Version
148	Calling setChannel() with a null parameter	Ambiguity	A.2.4.1	
151	broadcast-indepenent applications and tuning failures	Ambiguity	A.2.4.2	
152	Remove security restrictions to create embedded objects	Ambiguity	A.1	
158	Clarification on using the keyset object	Editorial	10.2.2	
159	Clarification on HTTP range header	Ambiguity	7.3.2.1	
160	Clarification on HTTP redirect methods	Ambiguity	New section 7.3.2.5	
161, 183, 673	Require to store cookies in persistent memory	Ambiguity	10.2.1	1 – 161, 183 2 - 673
163	Clarification on HTTP progressive streaming for live content	Ambiguity	7.3.2.1	
165	Clarification on equivalent fonts	Ambiguity	10.2.1	
166, 303	What to do after Application loading via DSMCC fails	Error	6.2.2.2, 6.2.2.3	
167, 449	Error reporting for application failure	Ambiguity	6.2.2.4, 6.2.2.5	1 – 167 2 - 449
168	Supported character set	Ambiguity	10.2.1	
184	video/broadcast object's setVolume/getVolume methods should be NI	Implementation	A.1	
185	Use of a Single PID for AIT Signalling	Implementation	7.2.3.1	
186	Clarification of Deferred Association Tag Support	Implementation	7.2.2	
188	Description of addStreamEventListener method	Ambiguity	8.2.1.1	
191	property 'Name' of StreamEvent	Editorial	8.2.1.2	
197	Restrict application domain to not	Error	6.3	

Reference	Short Description	Category	Clauses Impacted	Errata Version
	more than one FQDN			
200	onPlayPositionChanged		A.1	
201	WAV audio	Ambiguity	7.3.1.1	2
214	AV Control automatic transition clarification	Ambiguity	A.2.5	
215	AV Control queue clarification	Ambiguity	A.2.5	
224	No application started from recorded broadcast content	Ambiguity	6.2.2.1	
225	MIME-type for XML StreamEvent object files	Error	9.3.1	2
228	HE-AAC Container Format Clarification	Ambiguity	7.3.1.1	
232	AIT Updates	Ambiguity	6.2.2.3	
238 1218	Capabilities for CI+ and DRM	Ambiguity	10.2.4, A.1	1 – 238 2 - 1218
244	charCode defined as both included and not included	Ambiguity	A.1	
253	Incorrect references into the OIPF DAE specification	Editorial	9.1.1.2, 9.1.2	
254	Incorrect application type	Error	7.2.3.2	
255	Missing text for ApplicationSpecificDescriptor	Error	7.2.3.2	
256	Typo in Annex A	Editorial	A.1	
260	ISMA reference	Error	2.1	
273, 385	URL Entry	Ambiguity	5.3.5, 6.2.2.6, 6.2.3, 10.2.3.1	
275	Identical carousels and the org_id	Editorial	6.3	
291	Broadcast parental access control	Ambiguity	10.2.6.1	
294	XHR's responseText for DSMCC Directory and Stream Event	Ambiguity	8.2.2	
301	Broadcast event subscriptions	Ambiguity	8.2.1.1	

Reference	Short Description	Category	Clauses Impacted	Errata Version
308	DLNA MP4 File Format Restrictions	Implementation	7.3.1.2	
315	Alignment of broadcast video and the application plane	Ambiguity	10.1.2	
349	Default background colour	Error	5.3.3.1, 10.1.1	
350	Use of DVB URL to start applications	Ambiguity	9.2	
351	User-Agent examples	Error	7.3.2.4	
352	Textual service identifier in DVB URL	Ambiguity	9.2	
353	Clarify behaviour of stream events with video/broadcast state changes	Ambiguity	8.2.1.1, A.2.4.2	
354	Video plane transparency	Ambiguity	10.1.2	
356	The video/broadcast object stop method and broadcast-independent applications	Error	A.2.4.2	
357	References to 6.2.2.7	Error	6.2.2.6	
358	XML-AIT lifecycle on manual service change	Ambiguity	6.2.2.2	
359	Supported Audio Formats	Ambiguity	2.1, 7.3.1.1	Partly in 1 and partly in 2
360	Resolutions greater than 1280x720	Ambiguity	10.2.1	
370	Usage of the video/broadcast extension for recording and time shift	Ambiguity	6.2.2.4, 7.2.3.1, A.1, A.2.4.3	
391	Reference to figure 13	Editorial	5.3.4	
397	data_broadcast_id descriptor	Ambiguity	7.2.3.1	
398	Object carousel caching	Ambiguity	7.2.5.1	
401	Typo in reference to TS 102 809	Editorial	7.2.3.1	
402	Impact of linking outside application domain on broadcast AV	Ambiguity	6.3	
409	Open IPTV Forum Errata	Ambiguity, Error	Numerous	2

Reference	Short Description	Category	Clauses Impacted	Errata Version
441	Encoding of numbers in XML	Ambiguity	2.1, 9.3.1	
462	Data services	Ambiguity	New 7.2.6, 7.2.3.1	2
494	Seeks in MPEG-2 transport streams	Error	7.3.2.1	2
598	Tables in 7.3.1.1	Editorial	7.3.1.1	
621 1166	Clarification of query strings in URIs passed to createApplication	Ambiguity	9.2	2
635	Missing VK_RECORD key	Error	10.2.2	2
688	Clarification of text entry	Ambiguity	10.2.1	2
722	Application type when more than one AIT is signalled	Implementation	7.2.3.1	2
735	XHR access to DSM-CC violates XHR specification	Error	8.2.2	2
739	getChannelConfig "trusted" or broadcast-related"	Ambiguity	A.1	2
768	Clarifying supported properties on the ScheduledRecording and Recording classes	Ambiguity	A.1	2
776	MPEG2TS VoD seeking behaviour	Error	7.3.2.1	2
832	XML capabilities for audio-only services	Error	10.2.4	2
856	SSL/TLS root certificates for server authentication	Error	11.2, 7.3.2.3, new annex D	
919	Application domain	Error	6.3, 6.2.2.6, 7.2.3.2	2
936	Potential (Security) Issues when transitioning between trust levels	Ambiguity	6.2.2.4	2
953	Error property for SecurityErrors	Implementation	A.1	2
955	Clarification on XML AIT restriction	Ambiguity	7.2.3.1	2
973	Definition of "an MPEG program which is not a broadcast service"	Ambiguity	6.2.2.2	2
975	APIs used to present live content	Ambiguity	7.3.2.1	2
977	behaviour of HbbTV on protected	Ambiguity	A.1, 4.3	2

Reference	Short Description	Category	Clauses Impacted	Errata Version
	channels - #1 - communication with the CAM			
978	behaviour of HbbTV on protected channels - #2 - starting applications	Ambiguity	New section 6.2.2.8	2
979	behaviour of HbbTV on protected channels - #3 - system messages and HbbTV applications	Ambiguity	New section 5.5.	2
1014	xmlCapabilities clarification	Inconsistency	10.2.4	2
1019	more on XML StreamEvent object files	Ambiguity	8.2.1.1	2
1053	Meaning of "M-M" in table A.1	Error	A.1	2
1103, 1230	Unicode characters	Implementation	10.2.1	2
1117	Maximum DSM-CC reference length	Ambiguity	New 7.2.5.4	2
1121	an stream event descriptor	Editorial	8.2.1.1	2
1145	Leftover references to setVolume() and getVolume()	Inconsistency	A.2.4.2	2
1158	Application exist on non-broadcast service	Ambiguity	6.2.2.3	2
1205	Channel type for data services	Ambiguity	7.2.6	2
1208	requirement on platform to include a mechanism to enable / disable subtitles, both for broadcast and for broadband	Ambiguity	New section 10.2.7	2
1233	Clarification about A.2.6.1	Inconsistency	A.2.6.1	2
1234	Glyph variants	Error	10.2.1	2
1242	XML capabilities - string matching	Error	10.2.4	2
1243	Error in DRM example	Error	10.2.4	2
1248	Wording in change 3 of issue 370	Ambiguity	A.1	2
1249	Omission in capability string in 10.2.4	Error	10.2.4	2
1251	Application profile bits	Editorial	7.2.3.1	2

Reference	Short Description	Category	Clauses Impacted	Errata Version
1252	Inconsistency between 7.3.1.1 and 10.2.1	Ambiguity	10.2.1	2
1256	Signalling of broadcast-independent applications	Editorial	1, 7.2.3.2	2
1282	Duplication in Cases E and F	Editorial	5.3.4	2
1285	state transition of 6.2.2.7 not mentioned in A.2.4.1	Ambiguity	6.2.2.7, A.2.4.1	2
1286	Window object	Other	A.2.8.1	2
1288	RTSP	Other	Various	2
1292	E-AC3 “not included”	Ambiguity	7.2.3.1	2

Key to categories

Ambiguity	Feature where different implementations may behave in different ways. This includes under-specified features as well as inconsistencies within the specification.
Editorial	Purely editorial change
Error	Clear technical error in the specification. Cannot be implemented as written.
Implementation	Feature removed, simplified or modified in order to simplify implementation and testing.

The following changes included in previous versions of this document are now included in release 1 version 1.2 of the Open IPTV Forum specifications and have been removed from this document.

Reference	Short Description	Category	Clauses Impacted	Errata Version
97	Changing the MIME type of an instantiated embedded object	Ambiguity	New A.2.9.	1
100-986	Video / broadcast and AV Control object colours	Ambiguity	9.1.1.1	1 – 100 2 - 986
125, 465	Behaviour of video and audio for a stopped video/broadcast object	Ambiguity	A.2.4.1	1 – 125 2 - 465
136	Execution timing of GetComponent() function	Ambiguity	A.1	

Reference	Short Description	Category	Clauses Impacted	Errata Version
149	video/broadcast state transitions triggered by external events	Ambiguity	A.2.4.1	
206	Open IPTV Forum Errata	Ambiguity	2.1, 7.3.1.4, A.1, A.2.1	
217	Mismatch between some VK key codes and W3C spec	Error	10.2.2, A.1, new A.2.11	1
257	When audio stops ...	Ambiguity	A.2.1	
498	Issue with onPlayStateChange() and playState for A/V control object	Ambiguity	New A.2.15	2
686	onParentalRatingError	Ambiguity	New A.2.13	2
782	Handling receiver mix audio description	Ambiguity	New A.2.16, new 7.1.2	2
1001	property naming - parentalRating vs. parentalRatings	Implementation	A.1, A.2	2

4 Technical Changes to TS 102 796

4.1 General

4.1.1 RTSP

All references to RTSP are removed.

4.2 Clause 1 - Scope

4.2.1 Signalling of broadcast-independent applications

The following line shall be deleted from under “The main uses of the broadband connection are the following:”

- Discovery of broadcast-independent applications.

4.3 Clause 2 – References

4.3.1 Permit either TLS 1.2 (RFC 5246) or TLS 1.0 (RFC2246) or 1.1 (RFC4346)

The following additional normative references shall be added;

- [21] IETF RFC 2246 : "The Transport Layer Security (TLS) Protocol Version 1.0".

[22] IETF RFC 4346 : "The Transport Layer Security (TLS) Protocol Version 1.1".

[23] IETF RFC 5746 : "Transport Layer Security (TLS) Renegotiation Indication Extension".

4.3.2 CI+ Usage

Informative reference i.3 (ETSI TS 102 757) shall be removed.

4.3.3 Open IPTV Forum Errata

All references to the Open IPTV Forum specifications shall be updated to reference release 1 version 1.2.

4.3.4 URL Entry

The following additional informative reference shall be added;

[i.5] W3C, "How to Add a Favicon to your Site",
<http://www.w3.org/2005/10/howto-favicon>

4.3.5 Encoding of numbers in XML

The following additional normative reference shall be added;

[25] XML Schema Part 2: Datatypes Second Edition
NOTE: Available at <http://www.w3.org/TR/xmlschema-2/>

4.3.6 Cookie size

The following additional normative reference shall be added.

[27] IETF RFC6265 : "HTTP State Management Mechanism"

4.3.7 Application domain

The following additional normative reference shall be added.

[28] IETF RFC 6454 "The Web Origin Concept"

4.3.8 Supported Audio Formats

The following additional normative reference shall be added.

[29] IEC 62481-2, Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 2: Media Formats, ed1.0 (2007-08)

4.3.9 Clarification of query strings in URIs passed to createApplication

The following additional normative reference shall be added.

[31] IETF RFC 3986 : "Uniform Resource Identifier (URI): Generic Syntax"

4.3.10 XML Capabilities - String Matching

The following additional normative reference shall be added.

[32] W3C Recommendation “Exclusive XML Canonicalization Specification Version 1.0”, 18 July 2002

NOTE: Available at <http://www.w3.org/TR/xml-exc-c14n/>

4.4 Clause 6 – Service and Application Model

4.4.1 Failure to start an application

In clause 6.2.2.5.3, the second bullet point shall be changed as follows;

Available only through broadband: the terminal shall not display an error message for applications which were either unless the application was launched as autostart (e.g. following a channel selection or AIT update) or which were launched by another application.

4.4.2 Revised Section 6.3

Clause 6.3 shall be replaced completely as follows;

Every application is associated with an application boundary. This is defined as follows:

- An application boundary is a set of URL origins and object carousels
- If the origin of a URL is the same as one of the origins in the application boundary, that URL is said to be inside the application boundary.
 - The origin for URLs shall be as defined in “The Web Origin Concept” specification [28]
- If an object carousel is identical to one of the carousels in the application boundary, that carousel is said to be inside the application boundary
 - The requirements for two object carousels to be identical shall be as defined in clause B.2.10 of TS 102 809 [3].

NOTE: For carousels delivered by different transport streams, the terminal compares the two `carousel_ids`. The use of the broadcaster’s `organization_id` in the 24 MSBs of the two `carousel_ids` is a means to obtain unique `carousel_ids` and is not visible to the terminal.

- For applications loaded via HTTP or HTTPS, the application boundary shall include the origin of the URL used to launch the application e.g. as signalled in the AIT or XML AIT or passed as argument of `createApplication()`.

NOTE: This means that the default boundary is the tuple (scheme, host, port) of the application URL before any redirect, where the port component is the default port if not otherwise specified.

- For applications loaded via object carousel, the application boundary shall include the carousel from which the first page of the application was loaded
- A `simple_application_boundary_descriptor` may be present in the AIT or an `applicationBoundary` element may be present in the XML AIT. As described in clause 7.2.3.1 and 7.2.3.2 of this specification, these may include :

- one or more HTTP or HTTPS URLs prefixes. The application boundary shall be extended to include also the origins of such prefix if this will not result in having origins from more than one host in the boundary. Otherwise the additional origin shall be ignored.

NOTE: this means that the boundary cannot be extended to cover more than one FQDN

- one or more DVB URL prefixes. The application boundary shall be extended to include also object carousels referenced by such prefixes.

Launching a new application by using the method `createApplication()` (with an arbitrary new start page) or killing the current application and starting a new one via application signalling shall result in losing the association with the current application boundary (i.e. the new application will have a new boundary as defined in this section)

Documents loaded from outside the application boundary shall be untrusted (in the sense of the word “trusted” as defined in section 11), for example documents loaded in an `<iframe>` element or documents loaded as a result of following a link or an HTTP redirect. Following a link or an HTTP redirect from outside the application boundary back inside the application boundary shall restore the trust level to the original trust level of the application.

NOTE: An application being broadcast-related or broadcast-independent is not impacted by this change in trust level.

For files requested with `XMLHttpRequest`, the Same-Origin Policy shall be extended using the application boundary i.e. any origin in the application boundary will be considered of same origin.

4.4.3

4.4.4

4.4.5 Changes to clause 6.2.2.6

In section 6.2.2.6, in the second bulleted list, the first item shall be modified as follows;

The broadcast-independent application has an org_id and app_id (whether obtained ~~was initially referenced~~ through a broadcast AIT or an XML AIT)~~(and hence has an org_id and an app_id)~~.

In clause 6.2.2.6, the second bullet point in the first bulleted list shall be revised as shown;

- Optionally from a terminal specific application like an Internet TV Portal or following manual URL input as described in clause 5.3.5.

In clause 6.2.2.6, the two instances of “Access to broadcast resources shall be lost as described in clause 6.2.2.7” shall be replaced with “Access to broadcast resources shall be lost and the object shall transition to the unrealized state”.

In clause 6.2.2.6, the following two paragraphs shall be merged into one paragraph and revised as shown;

Where the URL refers to an HTML page directly, the broadcast-independent application

shall be created without an org_id or app_id ~~and with an application domain being the fully qualified domain name of the referenced page (the first page to be loaded)~~. Where the URL refers to an XML AIT, the broadcast-independent application shall be created with the org_id and app_id specified in the XML AIT. In both cases, the application shall be associated with and an application domain boundary derived from the contents of the XML AIT as specified defined in clause 6.3.

In clause 6.2.2.6, the last two points in the second bulleted list shall be revised as shown;

- The URL of the entry point document of the broadcast-independent application has the same origin as at least one of exactly matches the URLs signalled in the broadcast signalling for that org_id and app_id up to the beginning of any query or fragment string signalled.
- The URL of the page currently loaded in the broadcast-independent application is inside the application domain boundary of the broadcast application as defined in clause 6.3.

4.4.6

4.4.7 No application started from recorded broadcast content

The following shall be added at the end of the first bulleted list in clause 6.2.2.1;

- Starting applications in response to the playback of recorded or downloaded content is not supported.

4.4.8 AIT Updates

The following text shall be added after the figure in clause 6.2.2.3.

In the above figure, the following clarifications shall apply;

1. For the purposes of deciding whether an application is already running or is still signalled, only the organization_id and application_id fields from the AIT shall be used. Other information (e.g. the URL of the first page) shall not be used.

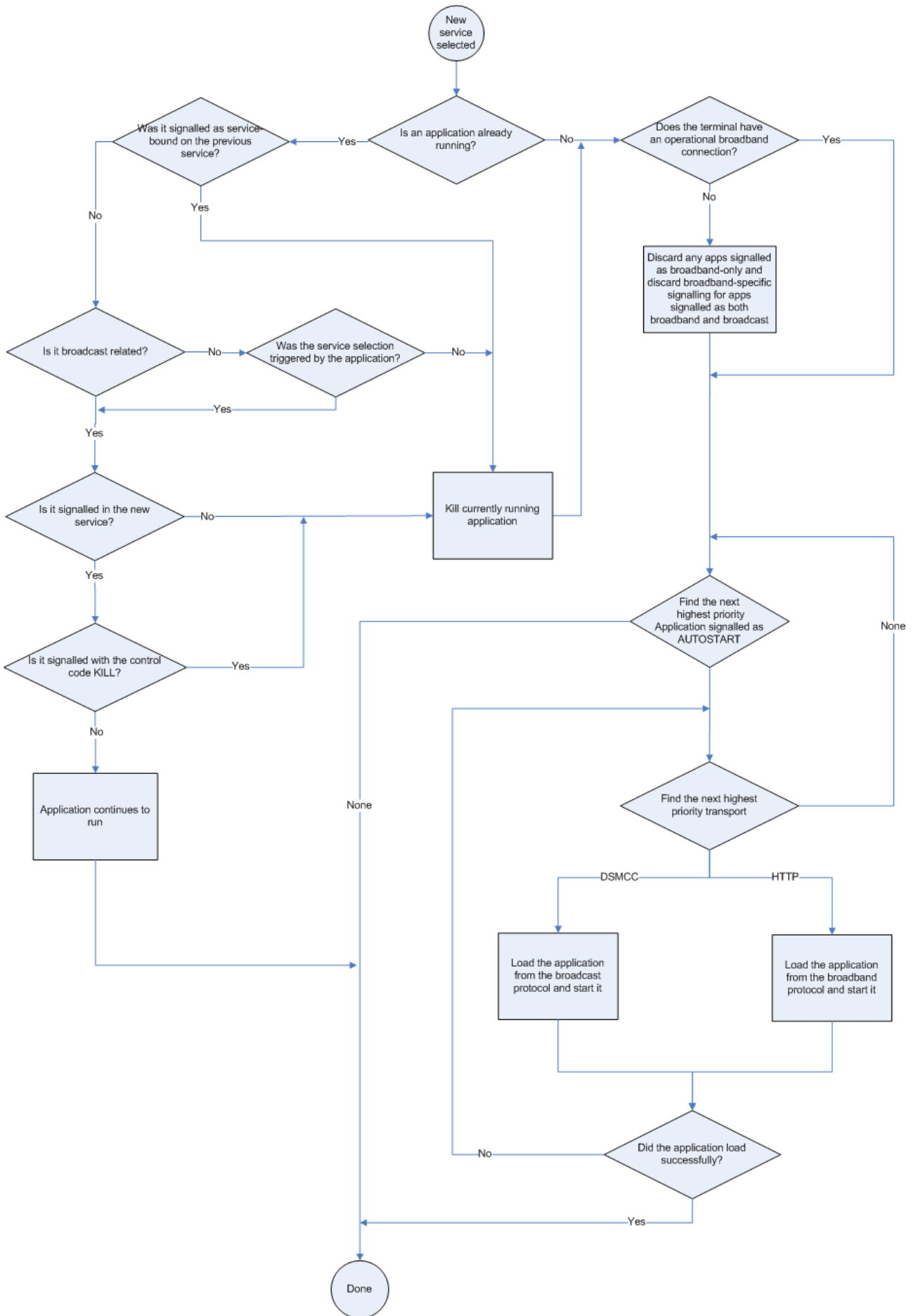
2. Other than organization_id and application_id, the only other field in the AIT which is relevant when the AIT is updated is the application control code. Changes in other fields shall be ignored for already running applications.

NOTE: As a result of the above, changes to fields in the AIT other than organization_id, application_id and application control code will only take effect for newly started applications. In order for those changes to effect an already running application, the application needs to exit and re-start. It is up to the broadcaster and/or application provider to arrange for this to happen.

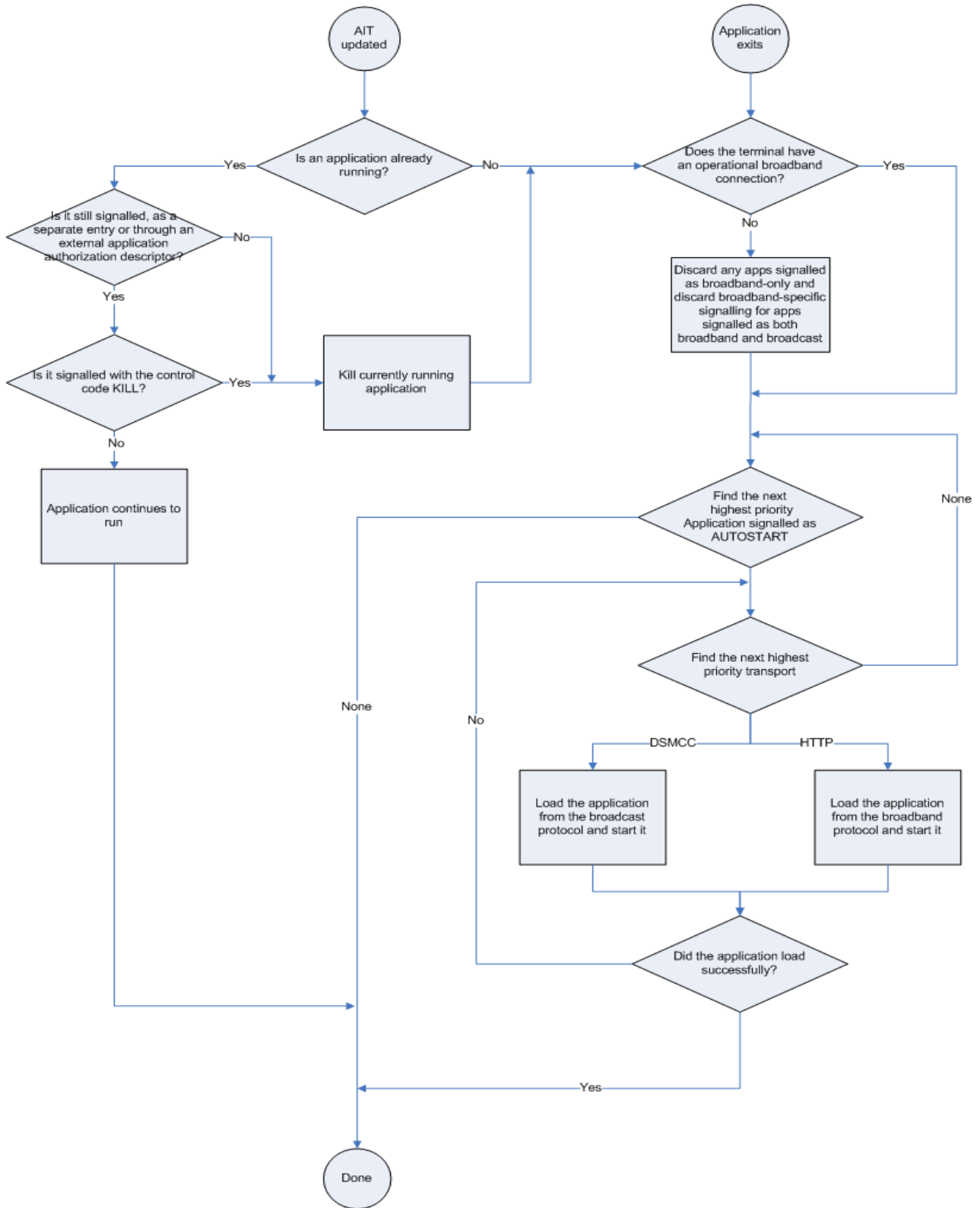
NOTE: A change in the version number of an AIT subtable is an indication to the terminal to retrieve a new version of the AIT. It does not imply or require any changes in the content of the AIT itself. For example, adding an application to the AIT would be an update to the AIT without changing the AIT entries for any existing applications.

4.4.9 What to do after Application loading via DSMCC fails

In clause 6.2.2.2, figure “Behaviour when selecting a broadcast service” shall be revised as follows;



In clause 6.2.2.3, figure “Behaviour while a broadcast service is selected” shall be revised as follows;



4.4.10 Error reporting for application failure

The last paragraph of clause 6.2.2.5.3 shall be modified as follows;

If the application cannot ultimately be loaded from either broadcast or broadband, ~~an error shall be returned if the~~ and the application was launched by a call to createApplication(), an ApplicationLoadError shall be dispatched. Once the initial page of an application has been successfully loaded, the present document does not specify how terminals should behave if a page from that application subsequently fails to load.

The following text shall be added at the end of clause 6.2.2.4;

When one application requests a second application be started, the first application shall continue to run until the initial HTML document of the second application has been loaded - i.e. until after an ApplicationLoadError event would be generated (if any listener was registered). Only then shall the first application be stopped.

Failing to parse the initial page of an application SHALL be regarded as a loading failure when evaluating if the application successfully loads in figure 13 and 14.

4.4.11

4.4.12 Impact of linking outside application domain on broadcast AV

In clause 6.3, immediately after the following paragraph (which is modified by 4.2.2 above);

Documents loaded from outside the application domain shall be untrusted, for example documents loaded in an <iframe> element or documents loaded as a result of following a link. Following a link from outside the application domain back inside the application domain shall restore the trust level to the original trust level of the application.

The following note shall be added.

NOTE: An application being broadcast-related or broadcast-independent is not impacted by this change in trust level.

4.4.13 Usage of the video/broadcast extension for recording and time shift

The following text shall be added to the end of clause 6.2.2.4.

If the terminal initiates time-shifting of the currently selected broadcast service, an application may get out of sync with the presentation of the audio-video components of this service. An HbbTV application shall be terminated if it is not safe to run it on a time-shifted broadcast service. An application is safe to run in time shift mode, if it is signaled in the AIT with an `applicaton_recording_descriptor` and both the `trick_mode_aware_flag` and the `time_shift_flag` set to '1' as described in clause 7.2.3.1. If an application is killed due to a broadcast service being time-shifted, the procedure defined in clause 6.2.2.2 for selecting an autostart application to run shall be followed except that only applications that are time-shift safe shall be considered.

After starting time-shift a terminal shall:

- dispatch a `RecordingEvent` to signal a state change to state 11 “time-shift mode has started” of the PVR state machine
- update the `recordingState`, `playPosition` and `playSpeed` properties of the video/broadcast object

After stopping time-shift a terminal shall:

- dispatch a `RecordingEvent` to signal a state change to state 0 “unrealized” of the PVR state machine

The present document defines two implementation options for support of applications when video is time-shifted - depending on whether the terminal can or cannot maintain synchronization between applications and the A/V components of a service. Which of these two options is implemented by a terminal is indicated by the `timeShiftSynchronized` property.

When a terminal can maintain synchronization between applications and the A/V components of a service, all of the following shall apply;

- DSMCC stream event descriptors shall be recorded with the A/V components keeping the timing relation and shall be delivered during playback of the time-shift
- The AIT shall be monitored, any changes shall take effect preserving the correct timing with respect to the A/V components
- The service information shall be recorded with the A/V components keeping the timing relation and the properties of the video broadcast object (e.g. programmes, `AVComponent` as defined in clause 7.13.4 of the OIPF DAE specification [1]) changes at the proper time of the playback of the time-shift
- The `timeShiftSynchronized` property shall be set to true (see clause A.2.4.3)

If a terminal is not able to maintain synchronization between applications and the A/V components of a service

- The application may receive some (or all) broadcast resources from the live broadcast signal instead of the time shift playback.
- It shall set the `timeShiftSynchronized` property to false

Note: when an application accesses service information or receives stream events, it may check if it is synchronized with the A/V component of the service by reading the values of the properties `recordingState` and `timeShiftSynchronized`.

4.4.14 Potential (Security) Issues when transitioning between trust levels

The following text shall be added at the end of clause 6.2.2.4.

When an application selects a new broadcast channel, there is a period of time between the

channel change having been completed (when the onChannelChangeSucceeded event is triggered) and the AIT having been received and parsed. During this period, the application shall retain its type (broadcast-related or broadcast-independent) and trust level (trusted or untrusted). Hence, while a broadcast-independent application is transitioning to become broadcast-related, access to features limited to broadcast-related applications will continue to fail as they did before the transition started until the AIT has been received and parsed.

4.4.15 Behaviour of HbbTV on protected channels - #2 - starting applications

A new clause 6.2.2.8 shall be added as follows;

6.2.2.8 Behaviour on encrypted broadcast service

Some channels may have the broadcast content encrypted, preventing those terminals without the appropriate CAS and rights from decoding and presenting the content. In these cases, clause 6.2.2.2 and 6.2.2.3 remains applicable even when the terminal fails to decode some or all of the components.

In particular, terminals shall behave as follows:

- failure to decrypt the AIT is identical to having no AIT present on that channel,
- failure to decrypt the carousel containing the application is identical to failing to load the application from broadcast protocol,

NOTE : The present document is intentionally silent about requirements for terminals to support decryption of encrypted AITs, object carousels and other data components.

Applications associated with channels which may be encrypted are advised to check whether the content is being presented ([using the error parameter provided in the onPlayStateChange method of the video/broadcast object](#)) and to modify their behaviour accordingly. For instance, if the content is not being presented, the application may wish to display some advertising message indicating how the user may gain access to this channel. Applications should not remain hidden or show a mainly transparent screen.

4.4.16 Definition of "an MPEG program which is not a broadcast service"

In section 6.2.2.2, the paragraph beginning "Figure 13 shall not apply when selecting an MPEG program which is not a broadcast service" shall be replaced as follows;

Figure 13 shall not apply when selecting an MPEG program that is not a broadcast DVB service. If a transport stream does not include an SDT actual then none of the MPEG programs in that stream are broadcast DVB services. If the SDT actual in a transport stream does not include an entry corresponding to a PMT in that transport stream then the MPEG program described by that PMT is not a broadcast DVB service.

There is no requirement for a terminal to check again either for an SDT or that a service is listed in the SDT if it has already done so, e.g. in order to acquire the service name when creating the channel list.

NOTE: If broadcasters or operators change programs in a multiplex from being a broadcast service to a non-broadcast service or vice-versa, they should use new program numbers / service_ids and should not re-use the old program numbers / service_ids.

As a consequence of selecting such an MPEG program:

4.4.17 Applications exiting on non-broadcast services

The following text shall be added to clause 6.2.2.3 at the end of the paragraph beginning “If the only running broadcast-related application exits without starting a broadcast-independent application or without the terminal changing channel”;

If an application exits when an MPEG program that is not a broadcast DVB service is selected and that MPEG program does not include an AIT then the behaviour is implementation specific.

4.4.18 State transition of 6.2.2.7 not mentioned in A.2.4.1

In section 6.2.2.7, the paragraph beginning “If access to broadcast resources is suspended” shall be replaced with;

Suspension of access to broadcast resources shall be treated as a transient error as defined in table 11 – “State transitions for the video/broadcast embedded object” of the OIPF DAE specification [1]. The PlayStateChange Event that is dispatched shall have the error code 11.

In section 6.2.2.7, the paragraph beginning “When access to broadcast resources is restored following earlier suspension of access” shall be replaced with;

When access to broadcast resources is restored following earlier suspension of access, this shall be treated as recovery from a transient error as defined in table 11 – “State transitions for the video/broadcast embedded object” of the OIPF DAE specification [1].

4.5 Clause 7 – Formats and Protocols

4.5.1 External application authorization descriptor

In clause 7.2.3.1 “Broadcast signalling”, in Table 5 “Supported application signalling features”, the row for “5.3.5.7 External application authorization descriptor” shall be “NI” not “M”.

4.5.2 Clarification of subtitle support for broadband streaming

Clause 7.2.1 shall be modified as follows;

7.2.1 System, video, ~~and~~ audio and subtitle formats

The present document does not contain any requirements for system, video, ~~and~~ audio and subtitle formats for the broadcast channel.

These requirements are defined by the appropriate specifications for each market where the terminals are to be deployed.

In clause 7.3, Table 8: “System, video and audio formats” shall have an extra column and note added as follows;

Table 1: System, video and audio formats

System Format	Video Format	Audio Format	Subtitle format	MIME Type
TS	AVC_SD_25 AVC_HD_25	HEAAC E-AC3 (see note1)	See note2.	video/mpeg
MP4	AVC_SD_25 AVC_HD_25	HEAAC E-AC3 (see note1)	Not defined in the present document.	video/mp4

NOTE1: Terminals shall support E-AC3 for the broadband connection when it is supported for the broadcast connection. Otherwise it is not mandated.

NOTE2: Terminals shall support the same subtitle formats for the broadband connection as are supported for the broadcast connection.

4.5.3 Permit either TLS 1.2 (RFC 5246) or TLS 1.0 (RFC2246) or 1.1 (RFC4346)

The following changes shall be made to clause 7.3.2.3;

HTTP as defined in RFC 2616 [7] and HTTP over TLS as defined in RFC 2818 [8] ~~and RFC 5246 [9]~~ shall be supported for transporting application files over broadband. TLS 1.2 (RFC 5246 [9]) should be supported for HTTP over TLS, if not then TLS 1.1 (RFC4346 [22]) should be supported instead and if neither of those is supported then then TLS 1.0 (RFC 2246 [23]) shall be supported instead.

NOTE: TLS 1.2 provides a much higher security level than TLS 1.0 and 1.1 so manufacturer are recommended to support it. Note also that TLS 1.0 and 1.1 are obsoleted by the TLS 1.2 specification. It is expected that future versions of the present document will require support for TLS 1.2 and omit the possibility of only supporting TLS 1.0 or 1.1.

When using HTTP over TLS the server may send a client certificate request during the TLS handshake as defined in RFC 2818 [8]. The TLS stack implementation shall support negotiation and delivery of client certificates to the server as defined in RFC 5246 [9], RFC 4346 [22] and RFC 2246 [21]. The client certificate shall comply with RFC 5280 [10]. The provision of these certificates is outside the scope of the present document as explained in clause 11.3.

The terminal shall support the default cipher suite of TLS as defined by clause 9 in RFC 5246 [9] or RFC 2246 [21] or RFC 4346 [22] as appropriate.

In order to fix a known vulnerability in SSL and TLS renegotiation, the terminal shall support the Renegotiation Indication Extension as specified in RFC 5746 [23].

4.5.4 Application visibility in the AIT

In clause 7.2.3.1, in table 5: “Supported application signalling features”, in the row for “5.2.6 Application visibility”

- The status shall be changed to “M/NI”
- The notes column shall contain “VISIBLE_ALL shall be signalled. Values other than VISIBLE_ALL are not included in the present document.”

4.5.5 app_id for trusted applications

In clause 7.2.3.1, in Table 5 “Supported application signalling features”, the notes for the row “5.2.3 Application identification” shall be extended with the following:

Applications signalled with an application_id in the range of unsigned application shall be started as untrusted. Applications signalled with an application_id in ranges other than signed and unsigned are outside the scope of this specification. If not otherwise required by other specifications, these applications shall not be started and discarded by the platform"

4.5.6 Restriction when using the AVC Baseline Profile

In clause 7.3.1.3, the following text shall be deleted.

with the following modifications:

- AVC baseline profile @ level 2 shall also be supported.

4.5.7 Clarify that both HTTP and HTTPS are supported

In clause 7.2.3.2, “or HTTPS” shall be added to the following sentence as show.

The XML file shall be delivered with HTTP or HTTPS using the "application/vnd.dvb.ait+xml" MIME type as defined in clause 5.4 of TS 102 809 [3].

4.5.8 Version.macro should be version.micro

In clause 7.2.3.1, in table 5 “Supported application signalling features”, in the row for 5.2.5 “Platform profiles”, “version.macro” shall be “version.micro”.

4.5.9 Clarification on HTTP range header

In clause 7.3.2.1, the first sentence shall be extended as follows;

Unicast streaming using HTTP 1.1 shall be supported as defined in clause 5.2.2.2 of the OIPF protocols specification [4] with the addition that the ~~range~~Content-Range header shall be supported in seek operations thus allowing the application to seek to any arbitrary position within the streaming video without the need of downloading the complete video first.

4.5.10 Clarification on HTTP redirect methods

A new clause 7.3.2.5 shall be added as follows;

HTTP redirects as defined in [HTTP] in response to a HTTP request shall be supported as described in this clause.

- The terminal SHALL support responses with a status code of “302 Found” and “307 Temporary Redirect” by using the temporary URL given in the Location field.
- The terminal SHALL support at least one redirection.

4.5.11 Clarification on HTTP progressive streaming for live content

In clause 7.3.2.1, the following additional paragraph shall be added between the current first and second paragraphs.

HTTP chunked transfer coding shall be supported as defined by section 3.6.1 of RFC2616 [7].

NOTE: Live content delivered using HTTP chunked transfer encoding is presented using the A/V control object. There are no requirements for the <video/broadcast> object to present content delivered using HTTP.

4.5.12 Incorrect application type

In clause 7.2.3.2, in Table 7 "Contents of XML AIT for Broadcast-independent applications", the row for "applicationDescriptor/type" shall read as follows;

applicationDescriptor/ type/OtherApp	Shall be "application/vnd.hbbtv.xhtml+xml " for Hybrid Broadcast Broadband TV applications.	Mandatory. Mime types other than "application/vnd.hbbtv.xhtml+xml " are outside the scope of the present document.
---	---	--

4.5.13 Missing text for ApplicationSpecificDescriptor

In clause 7.2.3.2, in Table 7 "Contents of XML AIT for Broadcast-independent applications", the row for "applicationSpecificDescriptor" shall be modified as follows;

applicationSpecificDescriptor/ OtherDescriptor	Shall be HBBTVApplicationSpecificDescriptor as defined by the present document.	For future use.
---	---	-----------------

4.5.14 Open IPTV Forum Errata

In clause 7.3.1.4, the following changes shall be made to the final bullet point;

The terminal shall use metadata, where provided, to control the stereo down-mix from multichannel audio, and shall use it, or pass it through, when providing bitstream output. Such metadata may be provided as described in the OIPF Media Formats specification [2] ~~clause 4.6.8.3 of ISO/IEC 14496-3 [14], annex C of TS 101 154 [15] and clause 6.8 of TS 102 366 [16].~~

4.5.15 Clarification of Deferred Association Tag Support

The following text shall be added to clause 7.2.2.

The use of the deferred_association_tags_descriptor for the purpose of referencing an elementary stream (TS 102 809 section B.3.1.1 and B.3.2) is not required by the present document. However this signalling may be present in a broadcast transport stream and acted upon by receivers that support this. Consequently, authors/broadcasters/operators should not expect this signalling to be ignored if it is present in the broadcast transport stream.

If elementary streams present in other services are to be referenced, then that elementary stream will also be required to be present in the current services PMT.

The use of the `deferred_association_tags_descriptor` to support the `BIOP_PROGRAM_USE` tap (TS 102 809 section B.3.1.2) is required by the present document.

4.5.16 Clarification of HE-AAC Container Format

The following text shall be added in a new “notes” column to table 9, in the HEAAC row;

NOTE: The HEAAC pure audio media format implies carriage of HE-AAC audio inside the MP4 system format container. This format shall comply with the requirements specified in section 8.6.35 of the DLNA media formats specification [29], except for 8.6.35.11.

4.5.17 DLNA MP4 File Format Restrictions

In the first paragraph of clause 7.3.1.2, the reference to the MP4 file format and to TS 102 366 shall be deleted. The following new text shall be inserted after that paragraph.

The MP4 File Format shall comply with clause 4 of the OIPF Media Formats specification [2] and the following additions:

- For E-AC3 it shall comply with TS 102 366 [16] in addition
- The size of the moov box should not exceed 2.5 MByte
- Note: Large moov boxes will slow down start up times especially for broadband connections with a small bandwidth
- The `largesize` field may be used. The size of a box should not exceed 4GByte.

4.5.18 User-Agent Examples

In clause 7.3.2.4, the two examples of user-agent strings shall be replaced with the following;

User-Agent: HbbTV/1.1.1 (+PVR+DL; Sonic; TV44; 1.32.455; 2.002;)

User-Agent: HbbTV/1.1.1 (;;;;;)

4.5.19 Use of a Single PID for AIT Signalling

In clause 7.2.3.1, in table 5 “Supported application signalling features”, in the row for clause 5.3.4 of TS 102 809, the first paragraph in the Notes cell shall be replaced with the following;

A maximum of one PID per service shall be used to carry the AIT sub-table defined by the Hybrid Broadcast Broadband TV application type.

4.5.20 `data_broadcast_id` descriptor

In clause 7.2.3.1, in table 5 “Supported application signalling features”, in the row for clause 5.3.5.2 of TS 102 809, an extra sentence shall be inserted as shown.

The value to be used for the `data_broadcast_id` field of the `data_broadcast_id_descriptor` for Hybrid Broadcast Broadband TV carousels shall be 0x0123. The id_specific_data are not defined. By supporting this optional feature, terminals can reduce the time needed to mount a carousel.

4.5.21 Object carousel caching

The following extra sentence shall be added to the end of the 1st paragraph in section 7.2.5.1.

Additionally a terminal may read and cache and monitor several carousels in parallel in order to decrease the loading time as experienced by the user.

4.5.22 Usage of the video/broadcast extension for recording and time shift

In clause 7.2.3.1, in table 5: “Supported application signalling features”, in the row for “5.3.5.4 Application recording descriptor”, the status column shall contain “M/NI” and the Notes column shall contain the following;

Support of the `application_recording_descriptor` is mandatory when the terminal has support for time-shift. Otherwise it is not included.

The semantics of the `application_recording_descriptor` for HbbTV are clarified below this table.

The following text shall be added after the table;

The semantics of `application_recording_descriptor` are as follows

- Applications that are safe to run in time-shift including trickmode shall set the `trick_mode_aware` flag and the `time_shift_flag` to ‘1’.
- The `scheduled_recording_flag` is not included.
- If applications are signalled with `trick_mode_aware` set to ‘0’ the `timeshift_flag` shall be ignored.
- The `dynamic_flag` and `av_synced_flag` shall be used as defined by [TS102809]
- `initiating_replay_flag` is not included.
- `label_count`, `label_length`, `label_char`, and `storage_properties` are not included.
- Applications shall list broadcasted data components in the component tag list. The elementary stream carrying the AIT does not need to be listed.

4.5.23 Tables in 7.3.1.1

In clause 7.3.1.1, the following changes shall be made;

The sentence just before table 8 shall be changed to:

Table 8 defines the subset of the combinations of system, video and audio formats specified in the OIPF Media Formats specification [2] that shall be supported.

The sentence just before table 9 shall be changed to:

Table 9 defines the subset of audio formats specified in the OIPF Media Formats specification [2] that shall be supported for audio-only services and audio clips.

The title of table 9 shall be changed to:

Table 9: Formats for audio-only services and audio clips

4.5.24 MPEG2TS VoD seeking behaviour

In clause 7.3.2.1, the following paragraph shall be added between the first paragraph and the existing second paragraph.

The accuracy of seeking to a particular point in time within an MPEG-2 transport stream is implementation dependent. Applications should avoid this except for small seeks relative to the current position in a stream that is already being played which are likely to be the least inaccurate. Seeking is likely to be more accurate in a constant bit-rate stream than a variable bit-rate one.

4.5.25 Application type when more than one AIT is signalled

In clause 7.2.3.1, in table 5: "Supported application signalling features", in the row for "5.3.5.1 Application signalling descriptor", the Notes column shall contain the following;

If more than one stream is signalled in the PMT for a service with an `application_signalling_descriptor`, then the `application_signalling_descriptor` for the stream containing the AIT for the HbbTV application shall include the HbbTV `application_type` (0x0010).

4.5.26 Application Domain

In clause 7.2.3.2, in Table 7 "Contents of XML AIT for Broadcast-independent applications", the row for "applicationBoundary" shall be modified as follows;

<code>applicationBoundary/</code>	Optional.	Mandatory. Only strict prefixes starting with " <code>dvb://</code> ", " <code>http://</code> " or " <code>https://</code> " shall be supported. Only prefixes forming at least a second-level domain shall be supported. Path elements shall be ignored.
-----------------------------------	-----------	--

4.5.27 Seeks in MPEG-2 transport streams

In clause 7.3.2.1, the first paragraph shall be extended with the following;

If the Content-Length header is not provided, terminals shall not make any assumptions on the size of the buffer on the server. Hence terminals which need to obtain some data from the stream, e.g. for initialisation, cannot assume that this data is still buffered on the server once they have completed their initialisation.

4.5.28 WAV Audio

In clause 7.3.1.1, the following text shall be added after table 9;

Playing WAVE audio from memory is not included in the present document. It should not be

implemented unless required by another specification.

4.5.29 Data Services

A new section 7.2.6 shall be added as follows;

7.2.6 Data Services

HbbTV services may exist that don't have any broadcast audio or video components (i.e. pure data services). Their broadcast signalling shall be as follows.

The SDT entry for the pure data service shall use a service_descriptor with a service_type of 0x0C. It shall also contain a data_broadcast_descriptor as defined in TS 102 809 v1.1.1 section 5.3.9.1 with the following restrictions:

- The data_broadcast_id shall be 0x0123
- The selector_bytes shall be present, and shall carry information about all HbbTV AUTOSTART applications that the service may carry
- The application name and text and other private data may be present

The signalling of the AIT and any HbbTV carousel remains the same as normal audio and video services.

Terminals shall process the data_broadcast_descriptor in the SDT and include, in the terminals service list, data services that signal applications that are supported. If the selector_bytes are not present, the service shall not be included in the terminals service list.

NOTE: The present document does not contain any requirements how broadcast channel lists are updated and managed. These requirements may be defined by the appropriate specifications for each market where the terminals are to be deployed.

Where an instance of the Channel class represents a data service, the value of the channelType property shall be 256.

In section 7.2.3.1, in table 5, in the last 2 columns in table 5 for the row "5.3.9 Service information", in the status column, "NI" shall be changed to "M", and in the Notes column, "As modified by 7.2.6 below" added.

4.5.30 Clarification on XML AIT Restrictions

In the first paragraph of section 7.2.3.2, the third sentence shall be modified as shown;

The XML file shall contain an application discovery record containing exactly one or more application elements, all with the same orgId and appId values but with different application types.

4.5.31 Receiver mix audio description

A new section 7.1.2 shall be added as follows;

7.1.2 Audio description

For the broadcast connection, signalling of audio description is defined by the appropriate specifications for each market where the terminals are to be deployed. Signalling of audio

description for MPEG-2 transport streams delivered by the broadband connection shall follow the specification for the broadcast connection (if any).

NOTE: Typically most countries will use one of the 3 mechanisms from section 8.4.2 of the OIPF DAE specification [1] but the present document does not require that.

For ISO format files, signalling is only defined to identify audio description streams when these are delivered using DASH. In this case, the signalling is defined in clause E.2.4, "Role Related Requirements".

Presenting a broadcast-mix audio description stream is supported since this is no different from presenting any other alternative audio stream.

Presenting receiver-mix audio description streams is not required by the present document.

To the extent that audio description is supported, it shall be exposed to applications as defined in clause 8.4.5 of the OIPF DAE specification [1].

4.5.32 DSM-CC Reference Length

A new clause 7.2.5.4 shall be added as follows;

7.2.5.4 Constraints

A resolved DSM-CC object reference shall be at most 64 bytes.

4.6 Clause 8 – Browser Application Environment

4.6.1 Stream event listeners and state changes in the video/broadcast object

In clause 8.2.1.1 "Adding and removing stream event listeners", the description of the method "void addStreamEventListener(String targetURL, String eventName, EventListener listener)" shall be changed as follows;

Add a listener for the specified DSM-CC stream event.

~~When the event is found, a StreamEvent event with "StreamEvent" type shall be dispatched and passed to the event listener.~~

When a broadcaster transmits an identical instance of the MPEG private data section carrying a stream event descriptor (including the version number), only one StreamEvent event shall be dispatched.

When a broadcaster transmits different events using the same event name id (i.e. with different version numbers), one StreamEvent event shall be dispatched for each different stream event descriptor received.

An event shall also be dispatched in case of error.

~~When a broadcaster transmits an identical instance of the MPEG private data section carrying an event (including the version number), only one event shall be dispatched. When a broadcaster transmits different events using the same event name (i.e. with different version numbers), one event shall be dispatched for each different event received.~~

Listeners can only be added while the video/broadcast object is in the Presenting or Stopped states. Calls to this function when the video/broadcast object is in another state shall have no

effect.

The terminal shall automatically unregister all listeners on the video/broadcast object in the following cases:

- A transition to the Unrealized state (e.g. when becoming broadcast-independent)
- A transition to the Connecting state that is due to a channel change

Listeners are not unregistered when transitioning to the Connecting state due to a transient error that does not result in a change of channel.

4.6.2 Clarify format of XHR responseText on DSM-CC carousel Directories/Stream Event and DVB URL examples

In clause 8.2.2, table 11 “Values of the responseText and responseXML properties” shall be modified as follows;

DSM-CC object	URL example	responseText	responseXML
File	/weather/data.xml	Returns the “text response entity body” as defined in XMLHttpRequest [12].	If the file has the extension “.xml”, returns the “XML response entity body” as defined in XMLHttpRequest [12]. <u>Otherwise, returns null.</u>
Directory	/weather	Comma-separated list of <u>names (File name, Stream Event name or Directory name) of all objects in the directory. These names shall not include path information.</u>	null
Stream Event	/weather/main/streamEvt1	Comma-separated list of <u>names of all events in the Stream Event object.</u>	null

Also in clause 8.2.2, the examples shall be modified with the following additional text;

Examples of `dvb:` URLs that may be used with the `XMLHttpRequest` object are:

`/weather/data.xml` (absolute path from the root of the carousel of the current page)

`../weather/data.xml` (relative path to the current page)

`dvb://1..1.B8/weather/data.xml` (0xB8 is the component tag)

4.6.3 Intrinsic events and DSMCC stream events

Clause 8.2.1.3 shall be removed

4.6.4 CI+ Usage

Clause 8.2.3 and all sub-clauses shall be removed.

4.6.5 property 'Name' of StreamEvent

In clause 8.2.1.2, in the descriptions of the properties, the “Name” property shall be called “name” to match with the signature definition.

4.6.6 XHR access to DSM-CC violates XHR specification

In clause 8.2.2, in the description about Headers not being relevant for carousel access, only the getAllResponseHeaders() method shall return an empty string. The getResponseHeader() method shall return null.

4.7 Clause 9 – System Integration

4.7.1 Video / broadcast and AV Control object colours

In clause 9.1.1.1, the second line shall be modified and a new third line added as follows;

- Stopping playback shall cause the video ~~plane to be made transparent~~ and the audio to stop.
- When not presenting video, the AV Control object shall be rendered as an opaque black rectangle.

4.7.2 Textual service identifier in DVB URL

The following text shall be added to clause 9.2;

Support for DVB URLs including the textual service identifier is not required in the present document.

4.7.3 DVB URL and Starting Applications

The text in clause 9.2 relating to the DVB URL shall be modified as follows;

The dvb: URL scheme as defined in TS 102 851 [11] shall be supported and extended as follows:

- It shall be possible to use dvb: URLs including path references to refer to DSM-CC file objects and to DSM-CC stream event objects signalled in the current service. It shall be possible to append to URLs referring to DSM-CC file objects an optional query component or fragment component, e.g. to pass parameters to an application. Since ‘?’ and ‘#’ are reserved characters as defined in RFC3986[31], if the name of a DSM-CC file object that is part of an HbbTV application contains such characters, they shall be percent-encoded (as defined in RFC3986[31]) when used in URLs.
- It shall be possible to use dvb: URLs referring to applications signalled in the current service as defined in table 4 of TS 102 851 [11] and optionally appended fragment component with the Application.createApplication() method. Use of dvb: URLs referring to applications from another service will cause createApplication() to fail as if the initial page could not be loaded. ~~Parameters~~ Any query component and fragment component assigned to this DVB URL shall be ~~parsed and~~ attached to the application location URL signalled inside the corresponding AIT as follows:

- If only one URL contains a query component then the resulting URL shall use that query component.
- If both URLs contain a query components then the query component of the DVB application URL is appended to the application location URL using an ampersand sign '&'. The terminal shall not attempt to parse or process the query components.
- If only one URL contains a fragment componnt then the resulting URL shall use that fragment component.
- If both URLs contain a fragment component, the fragment component of the DVB application URL takes precedence and overwrites the one in the application location URL
- The window.location.href property shall take the value of the resulting URL, including any parametersquery component. Any fragment component shall be available in the window.location.hash property and the query component in the window.location.search property.

Examples for a resulting URL include:

- URL signaled in the AIT: <http://www.example.com/app1?param1=value1>

createApplication URL: dvb://current.ait/1.1?param2=value2#foo

Resulting URL: <http://www.example.com/app1?param1=value1¶m2=value2#foo>

- URL signaled in the AIT: <http://www.example.com/app1?param1=value1#test>

createApplication URL: dvb://current.ait/1.1#foo

Resulting URL: <http://www.example.com/app1?param1=value1 #foo>

- The application is signaled in a DSMCC Carousel with a Component Tag of 4 and a Base URL of /index.php?param1=value1 and the current service location is dvb://1.2.3

createApplication URL: dvb://current.ait/1.1?param2=value2#foo

Resulting URL: <dvb://1.2.3.4/index.php?param1=value1¶m2=value2#foo>

4.7.4 Encoding of numbers in XML

The following text shall be added to clause 9.3.1.

For the XML schema defined in clause 8.2 of TS 102 809 [3] the following restrictions shall apply.

The value of the `stream_event_id` attribute of the type `StreamEventType` shall represent a positive/unsigned integer with a maximum value of 65535. The lexical representation of the value shall be as defined by clause 3.3.23 “unsignedShort” of [25]

The value of the `component_tag` attribute of the type `DsmccObjectType` shall represent a positive/unsigned integer with a maximum value of 255. The lexical representation of the value shall be as defined by clause 3.3.24 “unsignedByte” of [25]

Stream event XML files shall be served with a MIME type of "application/vnd.dvb.streamevent+xml"

4.8 Clause 10 – Capabilities

4.8.1 Clarification on using the keyset object

The following note shall be added to the end of clause 10.2.2.

NOTE: Applications must set the NAVIGATION bit of the keyset object even if the navigation keys are only used for focus based navigation (including the CSS nav-* properties) and not used in javascript event handlers.

4.8.2 Require to store cookies in persistent memory

In clause 10.2.1, the following additional row shall be added to table 14 “Minimum terminal capabilities”.

Cookie support	<p>Cookies with an expiry date shall be stored in persistent memory. Terminals shall respect the expiry date of the cookie.</p> <p>Terminal SHALL follow [RFC6265] when implementing cookies support.</p> <p>Since section 6.1 of [RFC6265] does not fix strict limits, this specification fix the following minimum capabilities that terminals SHALL support:</p> <ul style="list-style-type: none"> * At least 4096 bytes per cookie (as measured by the sum of the length of the cookie's name, value, and attributes). * At least 20 cookies per domain * At least 100 cookies total * At least 5120 bytes for the "Set-Cookie" header <p>NOTE: as implied by the RFC6265, if a cookie or a "Set-Cookie" header is bigger than the maximum size supported by the terminal, it will be discarded, not truncated.</p>	
----------------	--	--

4.8.3 URL Entry

The following additional text shall be added to the end of clause 10.2.3.1.

For the presentation of applications on manufacturer portals or in favourite lists the terminal may use a title and an icon specified in the HTML head section and the URL of the initial page of the application.

- The application name is defined by the HTML title element
- The application may have multiple title elements to provide a name in different languages using the lang attribute.
- The linking to an application icon is done by an HTML link element with the following attributes. See also [i.5]
 - rel – shall have the value ‘icon’
 - type – shall contain the mime type of the image format
 - href – shall be the URL of the image

- The image format and mime types of the icon shall be as defined in section 7.1.1
- An application may have multiple icons for different aspect ratios, e.g. 4 by 3 and square. It is recommended that an application provides at least one icon with a square aspect ratio.

4.8.4 Supported character set

In clause 10.2.1, in table 14 “Minimum terminal capabilities”, in the row “Supported proportional font”, the 4 references to the Tiresias screenfont shall have “ v8.03” added.

4.8.5 Broadcast parental access control

In clause 10.2.6.1, text shall be inserted as follows;

Terminals shall support parental access control for the broadcast channel as required for the markets in which the products are to be sold or deployed. The details of this are outside the scope of the present document. Typically the end user may have to enter the appropriate PIN in order to obtain access to TV content above the parental rating threshold. The following shall apply if access to broadcast TV content is blocked as a result:

4.8.6 Clarification of valid syntax for application/oipfCapabilities property & method

The following changes shall be made to clause 10.2.4;

- 1) The clause shall be renamed to “Hybrid Broadcast Broadband TV reported capabilities and option strings”.
- 2) The following text shall be inserted at the start of the clause;

For a terminal supporting only the base level of features, the XML Document object provided by the xmlCapabilities property of the application/oipfCapabilities embedded object shall describe an XML document that when canonicalized according to the W3C XML Canonicalization specification [32] shall be equal to the canonicalized form of the following XML::

```
<profilelist>
  <ui_profile name="OITF_HD_UIPROF+DVB_S+TRICK_MODE">
    <ext>
      <parentalcontrol schemes="dvb-si">true</parentalcontrol>
    </ext>
  </ui_profile>
  <video_profile name="TS_AVC_SD_25_HEAAC" type="video/mpeg" />
  <video_profile name="TS_AVC_HD_25_HEAAC" type="video/mpeg" />
  <video_profile name="MP4_AVC_SD_25_HEAAC" type="video/mp4" />
  <video_profile name="MP4_AVC_HD_25_HEAAC" type="video/mp4" />
  <audio_profile name="MPEG1_L3" type="audio/mpeg"/>
  <audio_profile name="HEAAC" type="audio/mp4"/>
</profilelist>
```

“DVB_S” can be replaced by the appropriate string(s) for the supported broadcast delivery system(s).

Other parental control schemes in addition to than “dvb-si” may be listed in the “<parentalcontrol>” element.

Only the video format profiles supported for broadband shall be listed.

As mentioned in table 8, the terminal may also support E-AC3 audio, in which case the following elements shall be added after the elements listed in the profilelist element in the above XML:

```
<video_profile name="TS_AVC_SD_25_E-AC3" type="video/mpeg" />
<video_profile name="TS_AVC_HD_25_E-AC3" type="video/mpeg" />
<video_profile name="MP4_AVC_SD_25_E-AC3" type="video/mp4" />
<video_profile name="MP4_AVC_HD_25_E-AC3" type="video/mp4" />
```

3) The text “The strings defined in this clause shall be used to indicate which options are supported by a terminal. They shall be used in the HTTP User-Agent header for applications data retrieval through HTTP and as parameters of a JavaScript API to dynamically query the options supported by the terminal.” shall be revised as follows;

The strings defined in table 16 shall be used to indicate which options are supported by a terminal. They shall be used:

- 1) in the HTTP User-Agent header for applications data retrieval through HTTP
- 2) in the ui_profile element’s name property of the xmlCapabilities property of the application/oipfCapabilities embedded object
- 3) as parameters of the hasCapability() method of the application/oipfCapabilities embedded object to dynamically query the options supported by the terminal.

4) The following additional row shall be added to the end of Table 16: “Hybrid Broadcast Broadband TV Option Strings”

“+DRM”	Support for the DRM feature – specifically that the XML capabilities include a <drm> element as defined below. NOTE: “+DRM” has a specific meaning in OIPF which it does not have in the present document.
--------	---

5) The following text shall be added at the end of clause 10.2.4.

The support of the DRM feature shall be indicated by the addition of one or more <drm> elements as defined in Annex F of the OIPF DAE specification [1] to the end of the profilelist element in the above XML. For example:

```
<drm DRMSystemID="urn:dvb:casystemid:12345">TS_PF</drm>
```

The support of CI+ shall be indicated using the <drm> element defined in Annex F of the OIPF DAE specification [1] and providing the protectionGateways attribute with “ci+” string. For example:

```
<drm DRMSystemID="urn:dvb:casystemid:12345" protectionGateways="ci+">TS_PF</drm>
```

4.8.7 Clarification on equivalent fonts

The following text shall be added to clause 10.2.1 immediate after table 14 “Minimum terminal capabilities”;

An equivalent font is one for which all the following are true:

- The line height of both fonts is the same.
- The widths of the glyphs for corresponding character points are the same in both fonts (where the character point is defined in both fonts).

- The kerning tables contain the same values for both fonts where both of the character points in the pair are present in both fonts.
- Either the appearance of the glyphs is visually similar or they are valid glyph variants as defined by unicode.

4.8.8 Mismatch between some VK key codes and W3C spec

The following text shall be added to the end of Section 10.2.2 User Input;

Note that VK_* key codes are defined as properties of KeyEvent interface and do not have a “global” Javascript scope.

For example, if an application wants to check if a user pressed the “Enter” key, it should use Javascript like the following code fragment:

```
if(e.keyCode == KeyEvent.VK_ENTER)
//handle the user input.
```

Furthermore constant values for VK_* key codes defined by CEA2014-A Annex F are OPTIONAL.

4.8.9 Resolutions greater than 1280x720

In clause 10.2.1, in table 14 “Minimum terminal capabilities”, in the row “Screen resolution” shall be replaced with the following;

	Value	Characteristic
Hybrid Broadcast Broadband TV application graphic plane resolution	1280 pixels horizontally by 720 pixels vertically with a 16:9 aspect ratio.	The terminal shall have at least this graphics resolution. If it is physically higher than this then the resolution shall appear to the applications to be exactly 1280x720 pixels.

4.8.10 Missing VK_RECORD key

In clause 10.2.2, in the table “key events and their status”, the following row shall be added.

Button (for conventional remote controls)	Key event	Status
Record	VK_RECORD	Mandatory if the PVR feature is supported, otherwise optional.

4.8.11 Clarification of text entry

In clause 10.2.1, in the table “Minimum terminal capabilities”, in the row for “text entry method”, the second paragraph shall be revised as shown.

For multi-tap or other methods which use multiple supported key events to generate a single characters,

4.8.12 Font reference and character set

In Table 14 in 10.2.1, in the rows for “Supported proportional font” and “Supported non-proportional font”, the references to

the Unicode character range "Basic Euro Latin Character set" as defined in annex D of TS 102 809 [3].

shall be replaced with

the Unicode character range "Generic Application Western European Character Set" as defined in annex C of TS 102 809 [3] but excluding the unicode character codes 0149 and 066B.

4.8.13 Inconsistency between 7.3.1.1 and 10.2.1

In Table 14 in 10.2.1, in the row for “Audio format for unicast streaming using HTTP and file download”, the reference to AC3 shall be changed to E-AC3.

4.8.14 Requirement on platform to include a mechanism to enable / disable subtitles, both for broadcast and for broadband

A new section 10.2.7 shall be added as follows;

10.2.7 Subtitles

Terminals shall support a method for the user to enable and disable subtitles and to select at least one preferred subtitle language. Terminals shall use this information when playing content to determine whether to present subtitles and to select between multiple subtitles when they are available.

Applications may change the terminal derived subtitle component selection and presentation status. The terminal shall maintain such changes made by an application until one of the following occurs:

- the application terminates,
- the application makes a further change,
- the video broadcast object or the A/V control object (as appropriate) is destroyed,
- the user makes a change using the terminal’s subtitle selection mechanism.
- in the case of a video/broadcast object, the broadcast channel is changed either by an application as defined in the present document or by a mechanism outside the scope of the present document (e.g. the end-user pressing P+ or P- on a remote control)

If the subtitle components available in the content change and the previously selected component is no longer available, then the terminal may re-evaluate the subtitle component selection based on the user preferences.

4.8.15 Graphics Model Comparison

All of clause 10.1 and sub-clauses shall be replaced with the following;

This clause is replaced by Annex H, “Display Model” of the OIPF DAE specification [1].

4.9 Clause 11 – Security

4.9.1 CI+ Usage

In clause 11.4.1, the following changes shall be made;

Terminals supporting CI+ for protected content via broadcast shall support the following mapping from the application/oipfDrmAgent embedded object to the CI+ protocol as defined by clause 4.2.3 ‘CI+ based Gateway’ of the OIPF CSP specification [5]:

- 4.2.3.1 Mandatory
- 4.2.3.2 Mandatory
- 4.2.3.3 Mandatory
- 4.2.3.4 Mandatory, except for ~~4.2.3.4.1.1.5-6-7, 4.2.3.4.1.1.9-10, 4.2.3.4.1.2 and 4.2.3.4.3~~ which are Not Included
- 4.2.3.5 N/A
- 4.2.3.6 Not Included
- 4.2.3.7 Mandatory using URI (Usage Rule Information) as defined in section 5.7 of CI Plus [13] if the PVR feature is supported otherwise Not Included, the PVR resource as defined in section 15 of CI Plus [13] is Not Included
- 4.2.3.8 Mandatory using URI (Usage Rule Information) as defined in section 5.7 of CI Plus [13] if the PVR feature is supported otherwise Not Included, the PVR resource as defined in section 15 of CI Plus [13] is Not Included
- 4.2.3.9 Not Included
- 4.2.3.10 N/A

Terminals supporting CI+ shall accept CI+ CICAMs that do not support the OIPF extensions defined by clause 4.2.3 ‘CI+ based Gateway’ of the OIPF CSP specification [5]. Specifically, the failure for any reason to set up the SAS connection with the Open IPTV Forum private_host_application_ID shall not stop other CI+ functionality, that does not depend upon this connection, from working normally.

Terminals supporting an embedded CA solution should support a mapping from the application/oipfDrmAgent to the embedded CA system to provide the same functionality as defined above.

Clause 11.4.2 and all sub-clauses shall be removed.

4.9.2 SSL / TLS Root Certificates

Clause 11.2 shall be completely replaced with the following;

11.2 TLS and SSL Root Certificates

A list of root certificates is maintained at <http://www.hbbtv.org/spec/certificates.html>. The policy by which this list has been derived is outlined in Annex D.

Terminals shall trust all root certificates identified as mandatory and may support those

certificates identified as optional on that list, subject to the conditions in this section.

Terminals should not trust any other root certificates.

NOTE: Including root certificates that are not on the list increases the risk of a man in the middle attack if those root certificates have not been audited to a similar or greater level than those on the list.

Terminals shall cease to trust any root certificates with RSA keys of less than 2048 bits after 31st December 2013.

Terminals shall support a means by which the device manufacturer can remove or distrust root certificates after manufacture. This may be handled either via a firmware upgrade mechanism or preferably via a specific root certificate update mechanism that could allow more timely updates.

A manufacturer may choose to remove or distrust a mandatory root certificate in the Terminal in response to a security threat.

Terminals should support a means of securely adding new root certificates after manufacture in order to maintain interoperability with servers over time.

4.10 Annex A – OIPF DAE Specification Profile

4.10.1 Clarify security exceptions for restricted APIs

The following changes shall be made to Table A.2 “Key to security column”;

1) the row for “broadcast-related” shall have the following text added to the description.

If other applications or web pages try to use this API, the terminal shall throw an error with the name property set to SecurityError (see clause 10.1.1 of the OIPF DAE specification [2]).

Note that for embedded objects, broadcast-independent applications may acquire instances of them without restrictions, either through the object factory or by using HTMLObjectElements. Security restrictions are enforced only when the application attempts to access properties or execute functions on the objects.

2) The row for “trusted” shall have the following text added to the description.

Note that for embedded objects, untrusted applications may acquire instances of them without restrictions, either through the object factory or by using HTMLObjectElements. Security restrictions are enforced only when the application attempts to access properties or execute functions on the objects.

3) In the row for “trusted”, the reference to an error with the message property set to SecurityError” shall be changed “an error with the name property set to SecurityError”.

4.10.2 CI+ Usage

The following changes shall be made to table A.1, “Section-by-section profile of the OIPF DAE specification”

1) In the row for “Applications started by the DRM agent”, the status column shall be changed from “M-M(*)” to “NI” and the notes column replaced with the following;

Terminals should not start Hybrid Broadcast Broadband TV applications triggered by the

DRM agent in order to avoid killing a currently running Hybrid Broadcast Broadband TV application which is trying to present the protected content.

Instead, it is recommended that applications trying to present the protected content should handle DRM-specific UI.

Note that CI+ application MMI (see clause 5.5.2 of the present document) has some conceptual similarities with this but uses a different presentation technology.

2) In the rows for “The DRMControlInformation class” and “The DRMControlInfoCollection class”, the status column shall be changed from “M-D, M-M” to “M-D+M-M” and the notes column replaced with the following;

Mandatory if both Download and DRM features are supported – even if the supported DRM systems do not use the <DRMControlInformation> element inside the content access download descriptor.

If the Download feature is supported and the terminal supports CI+ and if the terminal is capable of providing downloaded content to the CI+ CAM then these classes shall be supported – even if the CAS brought by a CI+ CAM do not use the <DRMControlInformation> element inside the content access download descriptor.

3) In the row for “Content Service Protection API”, the note shall be changed to read “Mandatory if the DRM feature is supported or if the terminal supports CI+”.

4) In the row for “Extensions to video/broadcast for DRM rights errors” (OIPF DAE reference 7.13.6), the “NI” shall be changed to “M-C,” and a note added as follows - “Mandatory if the terminal supports CI+”.

5) In the row for “Extensions to A/V object for playback through Content-Access Streaming Descriptor”, the “M-M” shall be changed to “O-M” and the notes column replaced with “The description of how a particular DRM technology integrates the present document may make this mandatory”

6) In the row for “Extensions to A/V object for parental rating errors”, “NI” shall be changed “O-M” and a note added as follows “The description of how a particular DRM technology integrates the present document may make this mandatory”.

7) In the row for “Content Access Streaming Descriptor Format”, the “M-M” shall be changed to “O-M” and the notes column replaced with “The description of how a particular DRM technology integrates the present document may make this mandatory”

8) In the row for “Abstract Content Access Descriptor Format”, the status shall be changed from “M-D, M-M” to “M-D, O-M” and the notes replaced with the following;

Shall be supported if the download feature is supported. The description of how a particular DRM technology integrates with the present document may make this mandatory

The clause A.1, in Table A.3: “Key to status column”, the additions shown underlined below shall be made;

Status	Meaning
M	Mandatory.
M-C	Mandatory if CI+ is supported for protected content via broadcast. Support of the related section/sub-section in table A.1 is not expected if CI+ support is not indicated according to clause 10.2.4.
M-D	Mandatory if the download feature supported otherwise not included.
M-M	Mandatory if the DRM feature is supported otherwise not included. Support of the related section/sub-section in table A.1 is not expected if the support of the DRM feature is not indicated according to clause 10.2.4. NOTE: A device supporting CI+ is not expected to support all the APIs required for the DRM feature
O-M	Optional in the present document but may be made mandatory by the definition of how a particular DRM solution integrates with HbbTV.
M-P	Mandatory if the PVR feature is supported otherwise not included.
M-R	Mandatory if the RTSP feature is supported otherwise not included.
NI	Not included.
NOTE:	Any of the above may be post-fixed with (*) where only some parts of the section or sub-section are required in the present document.

4.10.3 Clarification about setChannel()

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for clause 7.13.1 of the OIPF DAE specification, the reference to the optional contentAccessDescriptorURL parameter shall be changed from “is not included” to “may be ignored”.

4.10.4 Clarify what “fail” means

In clause A.2.4.2, in the third item in the bulleted list, “fail” shall be replaced as shown below;

The following methods shall always ~~fail~~throw a “Security Error” (as defined in clause 10.1.1 of the OIPF DAE specification) : getChannelConfig, bindToCurrentChannel, prevChannel, nextChannel, addStreamEventListener and removeStreamEventListener.

4.10.5 Access to ProgrammeCollection

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for clause 7.16.3, “ProgrammeCollection”, the entry in the Security column shall be “broadcast-related”.

4.10.6 Broadcast-independent applications and tuning failures

In the bulleted list in A.2.4.2, text shall be added to the first item as following;

- The following properties and methods shall have no restrictions: createChannelObject, playState, onChannelChangeSucceeded, onChannelChangeError, onPlayStateChange, width and height.

The last item in that bulleted list shall have a reference to the connecting state added as follows;

- The object shall always be in the unrealized or connecting states.

4.10.7 video/broadcast object's setVolume/getVolume methods should be NI

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, the row for OIPF clause 7.13.1 shall have the following text added;

The setVolume() and getVolume() methods are not included.

4.10.8 OnPlayPositionChanged

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for OIPF clause 7.14.3, the status column shall be changed to "M(*)" and the Notes column to:

Only the onPlayPositionChanged property and event are required except where the RTSP feature is supported, in which case the onPlaySpeedChanged property and event shall also required.

4.10.9 AV Control queue clarification

In clause A.2.5, the paragraph “Calling stop() or modifying the data property shall cause any queued media item to be discarded” shall be changed as follows;

Calling stop(), ~~or~~ modifying the data property or entering the error state shall cause any queued media item to be discarded.

4.10.10 Open IPTV Forum Errata

In table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for “the Application class”, clause 7.2.2 of that document, the following text shall be replaced;

- a property "privateData" (which shall have the same semantics as the private property)
- with
- the property “privateData”

4.10.11 charCode defined as both included and not included

In Table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for “Annex I charCode attribute support”, the “M” shall be changed to “NI”.

4.10.12 The video/broadcast object stop method and broadcast-independent applications

In clause A.2.4.2, the following change shall be made;

The following methods shall have no effect: setFullScreen, ~~and~~ release, and stop.

4.10.13 Usage of the video/broadcast extension for recording and time shift

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for “Extensions for recording and timeshift”;

- The “status” column shall be changed from “M-P” to “M(*), M-P”.
- The “notes” column shall read as follows;
 - Terminals that support time shift of broadcast video shall support the following events and properties even if they do not support the full PVR option;:
 - RecordingEvent
 - recordingState
 - playPosition
 - playSpeed

A new clause A.2.4.3 shall be added as follows;

A.2.4.3 Extensions to the Configuration class for time-shift

The following property is added to the Configuration class.

readonly Boolean timeShiftSynchronized
--

Returns a boolean indicating if the terminal is capable of maintaining synchronization between applications and A/V components during time-shift. A definition of synchronization between applications and A/V components can be found in clause 6.2.2.4.

4.10.14 onParentalRatingError

The definition of when the onParentalRatingError function of the <video/broadcast> object is called shall be amended so that it is called when one more parental ratings are found and none of them are valid. Where valid shall mean “A valid parental rating is defined as one which uses a parental rating scheme that is supported by the OITF and which has a parental rating value that is supported by the OITF.”

NOTE: This solution is aligned with clause 7.13.5 of release 2.1 of the Open IPTV Forum DAE specification

4.10.15 getChannelConfig "trusted" or broadcast-related"

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for “Conveyance of channel list”, the entry in the “Security” column shall be changed from “Trusted” to “Broadcast-related”

4.10.16 Clarifying supported properties on the ScheduledRecording and Recording classes

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for the ScheduledRecording class, the contents of the Notes column shall be replaced with the following;

Only the following properties shall be supported:

- startPadding
- endPadding
- name
- description
- startTime
- duration
- parentalRatings
- channel

All other properties are not included.

The parentalRating property has been renamed to parentalRatings in errata 2 to the Open IPTV Forum DAE specification [25].

In clause A.1, in table A.1 “Section-by-section profile of the OIPF DAE specification”, in the row for the Recording class, the contents of the Notes column shall be replaced with the following;

Only the following properties shall be supported:

- state
- id
- recordingStartTimer
- recordingDuration

Since the Recording class implements the ScheduledRecording interface, the properties required to be supported from that interface as defined above are also required

- All other properties are not included.

4.10.17 Clarification about A.2.6.1

In clause A.2.6.1, the following two items should be removed;

- The window.download method is not included, even in terminals supporting A/V content download.
- Direct keycodes are not included. Only the virtual keycodes (e.g. VK_) are required.

And the following item re-written as shown

- Support for [Req. 5.4.1.o] of CEA2014-A (use of accesskey attribute for standardized keycodes) is not included.

4.11 New Annex D – Server root certificate selection policy (informative)

D.1 Introduction

This informative annex describes the policy that is adopted for the selection of root certificates for inclusion in terminals compliant with this specification. A list of such certificates is published at <http://www.hbbtv.org/spec/certificates.html>.

D.2 Background

There are over 150 root certificates in web browsers at the time of publication.

- This list changes frequently over time.
- The larger the list of root certificates the more likely it is to change.

The security of TLS against man-in-the-middle attacks is dependent on the weakest root certificate trusted by a terminal.

The security of various key lengths changes with time as computing power increases. Specifically 1024 bit RSA keys are no longer recommended for use.

Service providers need to know which root certificates are trusted by terminals to achieve interoperability. Service providers are often not in control of the servers delivering their content (e.g. delivery via a CDN).

Service providers may also wish to make use of third party web services that are not under their control.

Maintaining an independent list of root certificates that are validated requires significant resources.

D.3 Policy

The Mozilla list of approved root certificates has been selected as the authoritative source for the mandatory and optional list of root certificates for inclusion in terminals compliant with this specification. This was chosen because:

- The approved root certificate list is publicly available.
- The process for inclusion in the list is open.
- Anyone can take part in the acceptance process.
- The acceptance process itself happens in public.
- Metadata is provided to differentiate root certificates for web server authentication, e-mail and code signing,
- The procedure for requesting a root certificate for inclusion in the list requires a test website be provided which uses that certificate.

The Mozilla list of approved root certificates is published on their website at <http://www.mozilla.org/projects/security/certs/>. Each certificate marked as approved for web server authentication is automatically an optional root certificate as specified in section 11.2. This specification will rely upon the Mozilla list for verifying the trustworthiness of Certificate Authorities.

A list of root certificates that are mandatory will be maintained which will be a subset of the certificates specified above.

- The list will be updated periodically.
- The list will only include certificates that use algorithms mandated by section 7.3.2.3.
- The mandatory list of certificates will be determined based on the requirements of service providers and the Certificate Authorities that are in widespread use.
- The list will be compiled relying upon published statistics to determine how widespread a Certificate Authority is.
- Certificate Authorities may be excluded from the mandatory list if they impose requirements that are deemed unreasonable.
- A revision history of changes to the mandatory list will be maintained and published

This policy is subject to change.

5 Editorial Changes to TS 102 796

5.1 General

5.1.1 DAE Reference Error

In many places, the OIPF DAE specification is referred to as reference [2] when it is in fact reference [1] in the list of normative references.

5.1.2 PlayStateChangedEvent in HbbTV Spec

In many places, the OIPF “PlayStateChange event” is referred to by the wrong name - “PlayStateChanged event” or even “PlayStateChangedEvent”.

5.2 Clause 2.1 – Normative References

In clause 2.1, the note after reference 6 shall be changed from;

NOTE: Available at .

to <http://www.isma.tv>

NOTE: Available at http://www.mpegif.org/m4if/bod/ISMA/ISMA_2.0.pdf

5.3 Clause 4 - Overview

5.3.1 Behaviour of HbbTV on protected channels - #1 - communication with the CAM

The following text shall be added at the end of clause 4.3 ("Terminal capabilities and extensions");

Additionally the present document defines some aspects that are mandatory for terminals supporting CI+ [13].

5.4 Clause 5 – User experience

5.4.1 Default Background Colour

In clause 5.3.3.1, the following paragraph shall be modified as shown;

Applications will start with a window covering the entire display in order that they can position the "Red Button" notification where they wish. ~~By default, the background colour of this window should be set to an opaque colour. Therefore, Since the browser rendering canvas default color is device-dependent,~~ applications should explicitly set the background of their <body> element to transparent using (for example) the following CSS rule (or an equivalent mechanism):

```
body {  
    background-color: transparent;
```

}

5.4.2 Reference to figure 13

In clause 5.3.4, in case D, the reference to figure 13 shall be replaced with one to figure 7.

5.4.3 URL Entry

The underlined sentence shall be added into the middle of section 5.3.5 as shown.

Broadcast-independent applications are started via a running application or an Internet TV Portal. An Internet TV Portal is an application which provides a type of start page where broadcast-independent applications are sorted and offered in an appropriate and useful way to the end user. The Internet TV Portal may be opened by pressing a dedicated Internet TV Button on the RCU. The type of interactive applications that are listed in the Internet TV Portal is the responsibility of the manufacturer. There may be an option for the user to add broadcast independent applications via manual URL entry or similar means like apps on mobile phones. The structure and the design of the start page is the responsibility of the manufacturer and out of the scope of the present document. Broadcast-independent applications are described in more detail in clause 6.2.2.6.

5.4.4 Behaviour of HbbTV on protected channels - #3 - system messages and HbbTV applications

A new clause 5.5 shall be added as follows;

5.5 User interface issues

5.5.1 Advertising broadcast applications

The user interface displayed on channel change (and when the “Info” button is pressed) is the responsibility of the terminal manufacturer but typically includes the title and synopsis of the current event. It is recommended that the presence of HbbTV applications signalled in the broadcast is indicated to the user in this UI.

5.5.2 Co-existence with CI and CI+ MMI

A CAM may request the terminal to display an MMI screen or dialogue at any time. The terminal has to respect the mandatory requirements of the CI and CI+ specifications (see sections 12.3.3 and 12.6.1.1 of [13]). Working within those constraints, the terminal should endeavour to present a consistent and uncomplicated user interface at all times. On occasion, this may result in the HbbTV application at least losing focus and possibly being terminated.

If any interaction between the CAM and the user is required, application authors are strongly recommended to use the oipfDrmAgent APIs to allow communication between the CAM and the HbbTV application, which can then act as a proxy for any interaction with the user.

5.5.3 Encrypted channels

Terminals may wish to display a message to the user that the channel is encrypted and cannot be displayed (see 6.2.2.4). If they do so, they should be aware that applications may wish to present some relevant information for this scenario. Hence any native UI should not remain on screen permanently or should give the user a way to remove it.

5.4.5 Duplication in Cases E and F

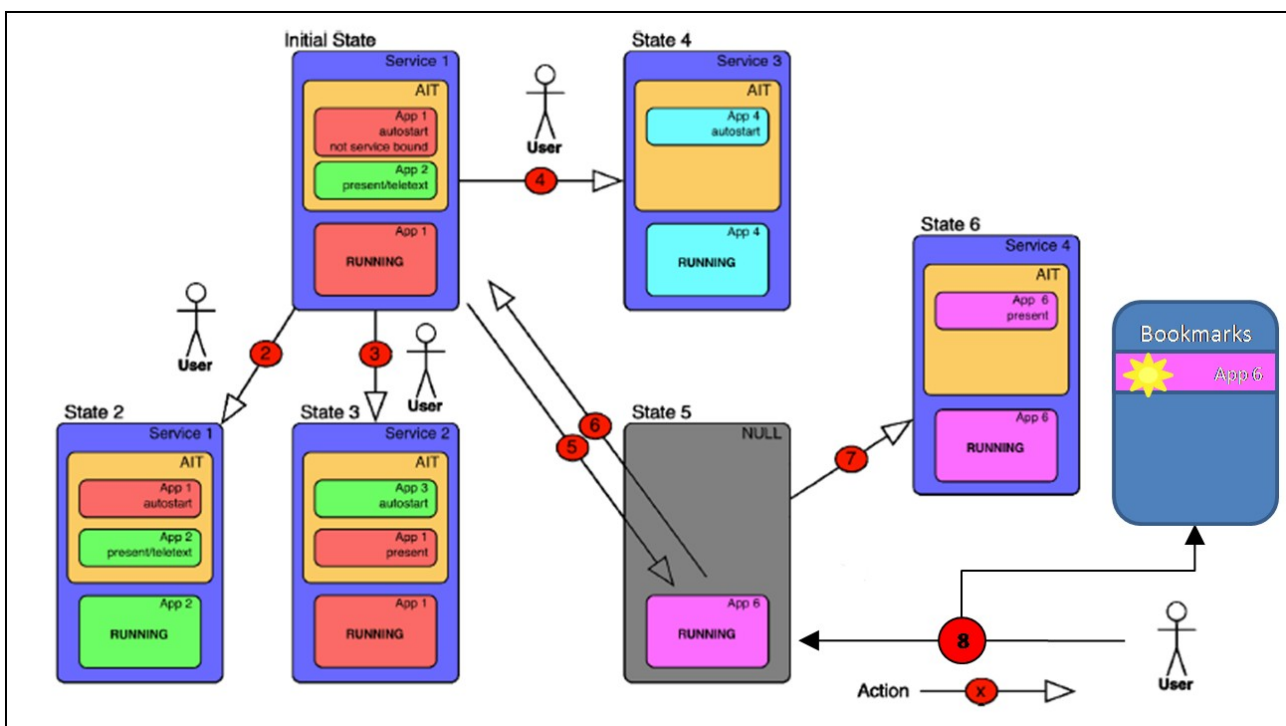
In clause 5.3.4, the first sentence of case E shall be replaced with the following;

If no digital teletext application is signalled and standard teletext is not available, nothing should happen.

5.5 Clause 6 – Service and application model

5.5.1 Application lifecycle example

In clause 6.2.3, figure 15 and the following table shall be updated as shown.



Starting state	Action	Resulting state
Initial State: Application 1 is running	2: User presses "TEXT" key	State 2: Application 2 will be started due to TELETEXT signalling.
Initial State: Application 1 is running	3: User selects service 2	State 3: Application 1 keeps running assuming it is not service-bound.
Initial State: Application 1 is running	4: User selects service 3	State 4: Application 1 will be killed and Application 4 will be started due to AUTOSTART signalling.
Initial State: Application 1 is running	5: Application call to createApplication() with an XML AIT to start a broadcast-independent application	State 5: Broadcast-independent application 6 is running. Any former presentation of service components will be stopped. The application has an application identifier as it was started from an XML AIT. See also action #7.
State 5: Application 6 is running	6: User selects Service 1	State 1: Application 6 will be stopped and Application 1 will be started due to AUTOSTART signalling.
State 5: Application 6 is running	7: User Application 6 selects service 4	State 6: Presentation of service 4 starts. Application 6 is signalled on service 4. It

		transitions to broadcast-related and keeps running. Due to signalling, presentation of service components starts.
	<u>8: User enters URL of XML AIT or initial page to start application and to store it in his bookmarks. Terminal takes application title and logo for bookmark entry as signalled in HTML header.</u>	State 5: same as for action 5.

5.6 Clause 7 – Formats and Protocols

5.6.1 Typo in reference to TS 102 809

In clause 7.2.3.1, in table 5, “Supported application signalling features”, in the row for clause 5.2.4 of TS 102 809, the reference to TS 102 809 has a duplicated character '8'.

5.6.2 Application profile bits

In clause 7.2.3.1, in table 5 “Supported application signalling features”, in the row for 5.2.5 “Platform profiles”,

- “Content download” shall be changed to “A/V content download”
- The sentence “The following bits can be combined for applications that require additional features:” shall be replaced with “The following bits can be combined to express profiles corresponding to additional features that applications may require:”
- The following text shall be added “As defined in clause 5.2.5.1 of [TS 102809], terminals shall be able to run all applications where the signalled application profile is one of the profiles supported by the terminal. All terminals shall support the basic profile (0x0000) in addition to profiles corresponding to the other features supported by the terminal.”

5.6.3 Signalling of broadcast-independent applications

In section 7.2.3.2, the following text shall be replaced;

Broadcast-independent applications do not require any signalling. If they are signalled then this shall be done using the XML encoding of the AIT as defined in clause 5.4 of TS 102 809 [3].

with

The present document does not define any signalling, announcement or discovery of broadcast-independent applications. Clause 5.3.5 of the present document defines how they can be started. Broadcast-independent applications shall be identified either by the URL of the first page of the application or by the URL of a XML AIT as defined by clause 5.4 of TS 102 8093 and profiled in this clause.

5.7 Clause 8 – Browser Application Environment

5.7.1 Add reference to XML event description file

In clause 8.2.1.1, the description of the targetURL argument of the addStreamEventListener method shall have text added as follows.

The URL of the DSM-CC StreamEvent object or an HTTP or HTTPS URL referring to an XML event description file (as defined in clause 8.2 of [3]) describing the event.

The description of the targetURL argument of the removeStreamEventListener method shall have text added as follows.

The URL of the DSM-CC StreamEvent object or an HTTP or HTTPS URL referring to ~~an~~the event description file describing the event.

5.8 Clause 9 – System Integration

5.8.1 Incorrect references into the OIPF DAE specification

In clause 9.1.1.2, the reference to clause 8.1.3.1 of the OIPF DAE specification shall be to 8.2.3.1.

In clause 9.1.2, the reference to clause 8.1.1.1 of the OIPF DAE specification shall be to clause 8.2.1.1.

5.9 Annex A - OIPF DAE Specification Profile

5.9.1 Typo in Annex A

In the row for OIPF clause 5.3.1.2, “Out of Session even the notification” shall be “Out of Session event notification”

6 Changes and Issues with Referenced Specifications

6.1 Open IPTV Forum Specifications

6.1.1 Media Resource Management

Clause A.2.1 shall be replaced with the following;

In clause 4.4.5 of the OIPF DAE specification [1], the statement that, “If insufficient resources are available to present the media, the attempt to play the media shall fail except for” shall have an extra exception in addition to those listed in that document - suspension of access to broadcast resources (see clause 6.2.2.7 of the present document).

6.1.2 Open IPTV Forum Errata

Clause A.2.4.1 shall be completely replaced with the following;

This clause describes a set of changes to the state machine for the video/broadcast object

defined in clause 7.13.1.1 of the OIPF DAE specification [1].

- Calling the setChannel() method from any state of the video/broadcast object with a null argument shall cause the application to transition to a broadcast-independent application (as described in clause 6.2.2.6). This is in addition to what is required by OIPF – e.g. causing the video/broadcast object to transition to the unrealized state and releasing any resources used for decoding video and/or audio. Hence the setChannel(null) and release() methods do not have the same behaviour in the present document.
- Suspension of access to broadcast resources as defined in clause 6.2.2.7 of the present document shall be treated as a transient error.

6.1.3 AV Control automatic transition clarification

The following text shall be added to clause A.2.5 between the paragraph starting “Play control keys” and the paragraph starting “The following value shall”,

The timing of automatic transitions from the error state to the stopped state is implementation dependent; applications should not rely on the AV Control object remaining in the error state after an error has occurred and should listen for play state change events in order to detect errors.

If the AVControl object's play() method returns true then at least one play state change event shall be generated.

The error property shall be available in the stopped state. After an automatic transition from the error state to the stopped state, the value of the error property shall be preserved.

The end of clause A.2.5 shall be updated as follows;

The following values shall be added to the list of valid values for the error property:

7 - content blocked due to parental control.

undefined - no error has occurred

6.1.4 Window object

In clause A.2.8.1;

- The id property shall be removed
- The onblur, onfocus and frameElement properties shall be added
- The clause shall start with “The window object shall be supported as defined in annex B of the OIPF DAE specification [1] except as follows.”