OIPF

Release 1 IPTV Solution

V1.1 Errata 1

[2010-07-27]

Open IPTV Forum

Open IPTV Forum

Postal address

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

Internet
http://www.oipf.tv

Disclaimer

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

Copyright Notification

Contents

Foreword

This document has been produced by the Open IPTV Forum (OIPF). It contains the first set of errata for the Release 1 V1.1 IPTV Solution specifications.

1 References

[OVIEW]	Open IPTV Forum, “Release 1 Specification, Volume 1 - Overview”, V1.1, October 2009.
[MEDIA]	Open IPTV Forum, “Release 1 Specification, Volume 2 - Media Formats”, V1.1, October 2009.
[META]	Open IPTV Forum, “Release 1 Specification, Volume 3 - Content Metadata”, V1.1, October 2009.
[PROT]	Open IPTV Forum, “Release 1 Specification, Volume 4 – Protocols”, V1.1, October 2009.
[DAE]	Open IPTV Forum, “Release 1 Specification, Volume 5 - Declarative Application Environment”, V1.1, October 2009.
[PAE]	Open IPTV Forum, “Release 1 Specification, Volume 6 - Procedural Application Environment”, V1.1, October 2009.
[CSP]	Open IPTV Forum, “Release 1 Specification, Volume 7 - Authentication, Content Protection and Service Protection”, V1.1, October 2009.

2 Release 1 IPTV Solution V1.1 Errata Summary

Errata issues with the IPTV Solution specifications are categorised into one of the following:

- **Editorial ("E")** – where amendments do not affect any normative requirement in the specification.
- **Technical ("T")** - where amendments imply a technical change, but not one that causes any incompatibilities with an earlier revision of the V1.1 specification.
- **Critical ("C")** – where amendments imply a technical change that introduces some element of incompatibility with the published V1.1 specification.

Errata to the IPTV Solution specifications can have one of the following status settings:

- **Acknowledged** – the issue is acknowledged as an erratum and its resolution is under way.
- **Resolved** – the issue has been resolved and the erratum is in preparation.
- **Implemented** – the erratum is specified in the relevant normative section of the present document.

As an erratum is noted, its status can be expected to progress through these states in the indicated order, being updated in successive revisions of the present document. Issues that are notified but subsequently not deemed to be errata are not maintained in this document.

Table 1 below lists the issues addressed, indicating which specification volume(s) are impacted.

The subsequent sections contain he detailed errata for each V1.1 specification volume.

Issue number	Issue	Category	Impacted Volume(s)	Impacted Section(s)	Constituent Errata Issue Reference(s)	Status	Date
1	Informative list of main changes since V1.0	E	1	New Annex	3.1	Implemented	4/12/2009
2	AC-3 normative reference	E	2	1.1.1	4.1	Implemented	4/12/2009
3	HE-AAC normative reference and metadata	E	2	1.1.1, 8.1.1, 10.1	4.2	Implemented	4/12/2009
4	Parental control in DAE	C	5	7.3.2.2, 7.9.1, 7.9.1.2	7.1	Implemented	4/12/2009
5	Scheduled recording APIs	T	5	7.10.1.1, 7.10.2.2	7.2	Implemented	11/12/2009
6	Applications management APIs	T	5	7.2.2.1, 7.2.4.2, 7.2.5.3	7.3	Implemented	11/12/2009
7	Application signalling normative reference	E	3 5	1.1.1 5.2.7, 8.3, 9, Annex H	5.1 7.5	Implemented Implemented	18/2/2010 09/03/2010
8	Application type notation	T	3	3.2.3.3.1	5.2	Implemented	14/12/2009
9	Deprecation of OIPFApplicationSpecificDescriptor and DAEApplicationDescriptor	C	3 1	Annexes B.14, B.15 Annex A.4.16	5.3 3.2	Implemented	24/2/2009
10	Clarification of FEC protocol usage	T	4	New 9.3	6.1	Implemented	14/1/2010
11	GBA authentication	C	4 7	5.6.3.2.2 5.4.4.2	6.2 9.1	Implemented	22/1/2010
12	SIP and SIP/SDP for Content on Demand	C	4	6.2.2.1.1, 7.1.1.2.1	6.3	Implemented	11/2/2010
13	Public Service Identifiers	C	4	5.2.1.1.1, 5.2.2.1.1, 5.2.2.1.2, 5.3.4.2.1	6.4	Implemented	11/2/2010
14	UDP keep-alive messages	T	4	Annex G.5.2	6.5	Implemented	11/2/2010
15	Vol. 3 section 4.2.3 sub-section numbering	E	3	4.2.3	5.4	Implemented	11/2/2010
16	AES usage for MPEG-2 TS scrambling	C	7	2.1.1, 4.1.5.3, 4.2.3.6.1	9.2	Implemented	11/2/2010

Issue number	Issue	Category	Impacted Volume(s)	Impacted Section(s)	Constituent Errata Issue Reference(s)	Status	Date
17	Restart using DHCP option 61 and removal of HNI-IGI Restart message	T	4 5	3.1, 5.5.1.9, 5.5.1.10, 12.1.1.1.1, Annex G.1.1, new Annex G.3 7.3.3.1	6.6 REF Ref2680179	Implemented Implemented	18/2/2010 21/04/2010
18	Method duplication and omission in the metadata APIs.	C	5	7.5.7.2, 7.14.4.2	7.4	Implemented	09/03/2010
19	Media resource management	C	5	4.4.5, 7.13.1.1, 7.14.1.1	7.6	Implemented	09/03/2010
21	DOM level 2 style support	C	5	Annex B	7.7	Implemented	09/03/2010
22	ApplicationDestroyRequest	T	5	7.2.6	7.8	Implemented	09/03/2010
23	Parental rating change events	T	5	7.13.5, 7.14.6	7.9	Implemented	09/03/2010

Table 1 V1.1 Errata issues summary

3 Errata for Volume 1 - Overview

3.1 Summary of changes compared to V1.0

Volume 1 will contain a new informative annex, as in the remainder of this sub-section, which summarises the changes since V1.0.

This annex summarises the major changes implemented in Version 1.1 of the IPTV Solution specification, compared to the original version published in January 2009.

Section 3.1.1 lists the major changes that impact more than one specification volume. Subsequent sections list the major changes to both normative and informative sections in each of volumes 1-7.

3.1.1 Cross-volumes issues

3.1.1.1 Application signalling

The method for signalling interactive applications via Service Provider Discovery extensions, specified in section 3.2.1 of Vol. 3, is deprecated. It is replaced by Application Announcement and Signalling based on ETSI TS 102 809 V1.1.1 (originally DVB blue book A137r1), specified in the new section 3.2.3.

The text in volume 5 corresponding to 3.2.1 of volume 3 was the "Approach A" and "Approach B" in sections 5.2.1 and 5.2.2 respectively. In V1.1, this text has been replaced with a single unified approach found in section 5.2.

3.1.1.2 Non-native HNI-IGI

The facility has been added to enable the OITF to provide access to all HNI-IGI interface functions, including IMS APIs, via an extended set of DAE APIs. Thus in cases where IMS functionality is to be accessed from within a DAE application, the OITF does not need to implement the HNI-IGI interface natively.

3.1.1.3 Multicast delivery of applications using FLUTE

This feature was foreseen in the Release 1 Architecture, but was not documented adequately in the IPTV Solution V1.0. This was rectified in V1.1, adding relevant specification content to Volumes 3, 4 and 5.

3.1.1.4 Software upgrade framework

A DAE application is able to request that the OITF triggers an update of its installed software. The software update process is proprietary to the manufacturer of the device that implements the OITF.

3.1.2 Volume 1 – Overview

V1.1 of Volume 1 contains the following major changes compared to V1.0:

- The informative overview of the Release 1 IPTV Solution has been expanded substantially; and
- Annex A has been updated to incorporate all XML schema changes implemented in Vols. 3, 5 and 7.

3.1.3 Volume 2 - Media Formats

V1.1 of Volume 2 contains the following major change compared to V1.0:

- Stipulation of the mandatory support for the decoding of both MPEG-2 TS and MP4 file format for unprotected content in the OITF.

3.1.4 Volume 3 – Content Metadata

V1.1 of Volume 3 contains the following major changes compared to V1.0:

- The Service Provider discovery extensions for DVB SD&S (section 3.2.1) are deprecated; and
- Service Provider related application signalling and application usage schema have been extended to include applications providing non-native HNI-IGI functionality.

3.1.5 Volume 4 - Protocols

V1.1 of Volume 4 contains the following major changes compared to V1.0:

- Added distinction between native and non native HNI-IGI function;
- Addition of the RTSP usage profile for the unmanaged model and associated network support procedure in the unmanaged model (e.g. NAT-T, network and session keep-alive messages);
- Addition of the SIP Digest authentication method;
- Clarification for devices that implement both OITF and IG;
- Improvement of DHCP options usage (removal of well-known PSI definitions for DHCP Options 15 and 124/125);
- Reorganisation of section on DHCP Option 124/125, for SD&S entry point discovery;
- Added definition of a profile of the data model for TR-069 based remote management function;
- Many minor improvements around the HNI-IGI, e.g. MIME type definitions;
- Many minor improvements around the usage of RTCP; and
- Reorganisation of Annex G for improved readability and to point out the start-up procedure with and without Native HNI-IGI.

3.1.6 Volume 5 - DAE

V1.1 of Volume 5 contains the following major changes compared to V1.0:

- Re-organisation of section 7 for improved readability;
- Support for Scheduled Content service without SD&S;
- Many small improvements around the <video/broadcast> object;
- Many small improvements around download support;
- Extended support of W3C specifications compared to CEA-2014 revision A; and
- Inter-application communication based on W3C cross-document messaging.

3.1.7 Volume 6 - PAE

V1.1 of Volume 6 includes only minor editorial changes compared to V1.0.

3.1.8 Volume 7 - CSP

V1.1 of Volume 7 contains the following major changes compared to V1.0:

- Support of HDCP and DTCP System Renewability Message delivery independently from Marlin;
- Mandating of IMS Registration;
- Addition of Marlin Action Token in the MarlinPrivateData schema, to enable delivery of the Marlin Token in the Content Access Descriptor, triggering license acquisition; and
- Addition of IMS AKA Registration for consistency with Volume 4 [OIPF_PROT].

3.2 service-sdns XML schema update

As a consequence of errata issues no. 9 and 10 noted in sections 5.3 and 6.1 respectively, the complex types OIPFApplicationSpecificDescriptor *and* DAEApplicationDescriptor *are removed from the* urn:oipf:service:sdns:2009 *schema in annex A.4.16.*

Due to these changes the schema namespace is updated to be "urn:oipf:service:sdns:2009-1".

The modifiled schema is:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="urn:oipf:service:sdns:2009-1" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:tva="urn:tva:metadata:2007" xmlns:dvb="urn:dvb:metadata:iptv:sdns:2008-1" xmlns:dvbmhp="urn:dvb:mhp:2006"
xmlns:oipfbcg="urn:oipf:service:bcg:2008" xmlns:mis="urn:dvb:mhp:2009" targetNamespace="urn:oipf:service:sdns:2009-1"
elementFormDefault="qualified" attributeFormDefault="unqualified">
    <!-- schema filename is  service-sdns.xsd -->
    <xs:annotation>
        <xs:documentation xml:lang="en">
            This schema is copyrighted by the Open IPTV Forum ("OIPF") and distributed in conjunction
            with Release 1 of the IPTV Solution Specification.

            Disclaimer
            The Open IPTV Forum members accept no liability whatsoever for any use of this document.
            This specification provides multiple options for some features. The Open IPTV Forum Profiling
            specification will complement the Release 1 specifications by defining the Open IPTV Forum
            implementation and deployment profiles. Any implementation based on Open IPTV Forum
            specifications that does not follow the Profiling specifications cannot claim Open IPTV Forum
            compliance.

            Copyright Notification
            No part may be reproduced except as authorized by written permission.
            Any form of reproduction and/or distribution of these works is prohibited.
            Copyright 2009 © Members of the Open IPTV Forum
            All rights reserved.
        </xs:documentation>
    </xs:annotation>
    <xs:import namespace="urn:tva:metadata:2007" schemaLocation="imports/tva_metadata_3-1_v141.xsd"/>
    <xs:import namespace="urn:dvb:metadata:iptv:sdns:2008-1" schemaLocation="imports/sdns_v1.4r10_modded.xsd">
        <xs:annotation><xs:documentation>as distributed with ETSI TS 102 809 v1.1.1</xs:documentation></xs:annotation>
    </xs:import>
    <xs:import namespace="urn:dvb:mhp:2006" schemaLocation="imports/mhpiptv.xsd"/>
    <xs:import namespace="urn:dvb:mhp:2009" schemaLocation="imports/mis_xmlait.xsd">
        <xs:annotation><xs:documentation>as distributed with ETSI TS 102 809 v1.1.1</xs:documentation></xs:annotation>
    </xs:import>
    <xs:import namespace="urn:oipf:service:bcg:2008" schemaLocation="service-bcg.xsd"/>
    <xs:element name="ServiceDiscovery">
        <xs:annotation>
            <xs:documentation>The use of this element is deprecated                    </xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:choice>
                <xs:element name="BroadcastDiscovery" type="dvb:BroadcastOffering" maxOccurs="unbounded"/>
                <xs:element name="CoDDiscovery" type="dvb:CoDOffering" maxOccurs="unbounded"/>
                <xs:element name="ServicesFromOtherSP" type="dvb:ReferencedServices" maxOccurs="unbounded"/>
                <xs:element name="PackageDiscovery" type="dvb:PackagedServices" maxOccurs="unbounded"/>
                <xs:element name="ServiceProviderDiscovery" type="tns:ServiceProvider" maxOccurs="unbounded"/>
                <xs:element name="BCGDiscovery" type="dvb:BCGOffering" maxOccurs="unbounded"/>
                <xs:element name="ContentGuideDiscovery" type="tns:ContentGuideOffering" maxOccurs="unbounded"/>
                <xs:element name="CommunicationDiscovery" type="tns:CommunicationOffering"/>
            </xs:choice>
            <xs:attribute name="Version" type="dvb:Version" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="CommunicationOffering">
        <xs:annotation>
            <xs:documentation>The use of this complex type is deprecated                    </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
```

```
            <xs:extension base="dvb:OfferingBase">
                <xs:sequence>
                    <xs:element name="InitialAppLoc" type="xs:anyURI"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="ServiceProvider">
        <xs:annotation>
            <xs:documentation>The use of this complex type is deprecated                </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="ServiceProvider" maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Name" type="dvb:MultilingualType" maxOccurs="unbounded"/>
                        <xs:element name="Description" type="dvb:MultilingualType" minOccurs="0" maxOccurs="unbounded"/>
                        <xs:element name="Offering" type="tns:OfferingListType" minOccurs="0"/>
                        <xs:element name="ApplicationList" type="dvbmhp:ApplicationList" minOccurs="0"/>
                    </xs:sequence>
                    <xs:attribute name="DomainName" type="dvb:DomainType" use="required"/>
                    <xs:attribute name="Version" type="dvb:Version" use="required"/>
                    <xs:attribute name="LogoURI" type="xs:anyURI" use="optional"/>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="OfferingListType">
        <xs:annotation>
            <xs:documentation>The use of this complex type is deprecated                </xs:documentation>
        </xs:annotation>
        <xs:choice maxOccurs="unbounded">
            <xs:element name="Push" type="dvb:DVBSTPTransportModeType"/>
            <xs:element name="Pull">
                <xs:complexType>
                    <xs:complexContent>
                        <xs:extension base="dvb:PayloadList">
                            <xs:attribute name="Location" type="dvb:PullURL" use="required"/>
                        </xs:extension>
                    </xs:complexContent>
                </xs:complexType>
            </xs:element>
            <xs:element name="WebOfferingLoc" type="dvb:DescriptionLocation"/>
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="ContentGuideOffering">
        <xs:annotation>
            <xs:documentation>The use of this complex type is deprecated                </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="dvb:OfferingBase">
                <xs:sequence>
                    <xs:element name="BCG" maxOccurs="unbounded">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="Name" type="dvb:MultilingualType" maxOccurs="unbounded"/>
                                <xs:element name="Description" type="dvb:MultilingualType" minOccurs="0"
maxOccurs="unbounded"/>
                                <xs:element name="TransportMode" type="tns:TransportModeType"/>
                                <xs:element name="Logo" type="xs:anyURI" minOccurs="0"/>
                                <xs:element name="Type" type="tva:ControlledTermType" minOccurs="0"/>
                                <xs:element name="TargetProvider" type="dvb:DomainType" minOccurs="0"
maxOccurs="unbounded"/>
                                <xs:element name="BCGProviderName" type="dvb:MultilingualType" minOccurs="0"
maxOccurs="unbounded"/>
                            </xs:sequence>
                            <xs:attribute name="Id" type="tva:TVAIDType" use="required"/>
                            <xs:attribute name="Version" type="dvb:Version" use="optional"/>
```

```
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="TransportModeType">
    <xs:annotation>
        <xs:documentation>The use of this complex type is deprecated        </xs:documentation>
    </xs:annotation>
    <xs:choice maxOccurs="unbounded">
        <xs:element name="DVBSTP" type="dvb:DVBSTPTransportModeType"/>
        <xs:element name="HTTP" type="dvb:HTTPTransportModeType"/>
        <xs:element name="ContentGuideLoc" type="dvb:DescriptionLocation"/>
    </xs:choice>
</xs:complexType>
<xs:complexType name="Package">
    <xs:annotation>
        <xs:documentation>The use of this complex type is deprecated        </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="dvb:Package">
            <xs:sequence>
                <xs:element name="ApplicationList" type="dvbmhp:ApplicationList" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="IPService">
    <xs:annotation>
        <xs:documentation>The use of this complex type is deprecated        </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="dvb:IPService">
            <xs:sequence>
                <xs:element name="TimeToRenegotiate" type="xs:duration" minOccurs="0"/>
                <xs:element name="PurchaseItem" type="oipfbcg:PurchaseItemType" minOccurs="0"/>
                <xs:element name="ApplicationList" type="dvbmhp:ApplicationList" minOccurs="0"/>
                <xs:element name="FileFormat" type="tva:ControlledTermType" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="WebApplicationDescriptor">
    <xs:annotation>
        <xs:documentation>The use of this complex type is deprecated        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="location" type="dvb:DescriptionLocation"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="Application">
    <xs:annotation>
        <xs:documentation>The use of this complex type is deprecated        </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="dvbmhp:Application">
            <xs:sequence>
                <xs:element name="fluteSessionDescriptor" type="tns:FLUTESessionDescriptor" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="OIPFApplication">
    <xs:complexContent>
        <xs:extension base="mis:Application">
            <xs:sequence>
```

```
                    <xs:element name="fluteSessionDescriptor" type="tns:FLUTESessionDescriptor" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="FLUTESessionDescriptor">
        <xs:sequence>
            <xs:element name="senderIP" type="xs:string"/>
            <xs:element name="numChannels" type="xs:unsignedInt"/>
            <xs:element name="destIP" type="xs:string"/>
            <xs:element name="TSI" type="xs:unsignedInt"/>
            <xs:element name="sessionTimeParam" type="xs:string"/>
            <xs:element name="lang" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="OIPFApplicationSpecificDescriptor">
        <xs:annotation>
            <xs:documentation>The use of this complex type is deprecated                </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="mis:ApplicationSpecificDescriptor">
                <xs:choice>
                    <xs:element name="DAEDescriptor" type="tns:DAEApplicationDescriptor"/>
                </xs:choice>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="DAEApplicationDescriptor">
        <xs:annotation>
            <xs:documentation>The use of this complex type is deprecated                </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="mis:OtherDescriptor">
                <xs:sequence>
                    <xs:element name="location" type="dvb:DescriptionLocation"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="OIPFIPServiceType">
        <xs:complexContent>
            <xs:extension base="mis:IPServiceType">
                <xs:sequence>
                    <xs:element name="TimeToRenegotiate" type="xs:duration" minOccurs="0"/>
                    <xs:element name="PurchaseItem" type="oipfbcg:PurchaseItemType" minOccurs="0"/>
                    <xs:element name="FileFormat" type="tva:ControlledTermType" minOccurs="0"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:schema>
```

4 Errata for Volume 2 – Media Formats

4.1 AC-3 normative reference

In section 1.1.1 "Standard References", the entry for "AC3" is changed to:

[AC3]	ETSI TS 102 366 V1.2.1 (2008-08), "Digital Audio Compression (AC-3, Enhanced AC-3) Standard".

4.2 HE-AAC normative reference and metadata

In section 1.1.1 "Standard References", the entry for "AAC" is changed to:

[AAC]	ISO/IEC 14496-3:2009, "Information Technology – Coding of audio-visual objects – Part 3: Audio".

In section 8.1.1 the new sub-section 8.1.1.3 "HE-AAC metadata" is added:

HEAAC format audio MAY contain metadata as specified in [AAC] or [TS101154], specifically:

- Dynamic Range Control parameters as defined in [AAC] section 4.5.2.7 or [TS101154] section 6.4.3 and Annex C.5
- Down-mix parameters as defined in [AAC] section 4.5.1.2.2 or [TS101154] Annex C.5.

In section 10.1 "Mandatory capabilities" the second bullet on audio capabilities is changed to:

- The OITF SHALL support the HEAAC audio format as defined in section 0. It SHALL support the decoding of HE-AAC audio in up to 5.1 channel surround format. If the OITF does not make use of 5.1 surround mode then it SHALL be capable of down-mixing the 5.1 surround audio stream to stereo. Down-mix parameters as defined in section 0 SHALL be used, if present in the encoded audio data. The OITF SHALL support the Dynamic Range Control metadata as defined in section 0, if present in the encoded audio data.
  Note that decoders supporting the MPEG-4 HE-AAC profile inherently also support the MPEG-4 AAC profile.

5 Errata for Volume 3 – Content Metadata

5.1 XMLAIT normative reference

In section 1.1.1 "Standard References", the entry for "XMLAIT" is changed to the relevant ETSI specification:

[XMLAIT]	ETSI TS 102 809 V1.1.1, (2010-01), "Digital Video Broadcasting (DVB); Signalling and carriage of interactive applications and services in Hybrid broadcast/broadband environments"

5.2 Application type notation

In section 3.2.3.3.1 the two bullets defining the application type notation are changed to:

- for DAE applications this value SHALL be either "`application/urn.oipf.cs.ApplicationTypeCS.2009.DAE.XHTML`" or "`application/urn.oipf.cs.ApplicationTypeCS.2009.DAE.SVG`"
- for PAE applications this value SHALL be "`application/urn.oipf.cs.ApplicationTypeCS.2009.PAE`"

5.3 Deprecation of OIPFApplicationSpecificDescriptor and DAEApplicationDescriptor

The DAEApplicationDescriptor specified in section B.15 is deprecated in the overall XML schema, as the equivalent functionality is provided by `SimpleApplicationLocationDescriptor` *in [XMLAIT].*

The OIPFApplicationSpecificDescriptor Extension specified in section B.14 is redundant by consequence and is thus deprecated in the overall XML schema.

5.4 Vol. 3 section 4.2.3 sub-section numbering

The sub-sections of section 4.2.3, "CRID Location Resolution" in volume 3 are numbered incorrectly. The correct numbering is:

4.2.3.1 Unmanaged networks

4.2.3.2 Managed networks

6 Errata for Volume 4 – Protocols

6.1 Clarification of FEC protocol usage

The following text is added as new section 9.3, titled "Application Layer Forward Error Correction", to specify the FEC protocol:

This section specifies the protocol for Application Layer FEC (AL-FEC) protection of streaming media for Scheduled Content services carried over RTP transport.

Application Layer FEC SHALL conform to [TS102 034] annex E. Only the base layer of DVB-IPTV AL-FEC SHALL be supported. Support of the AL-FEC enhancement layer is out of scope.

DVB AL FEC base layer is signalled in DVB SD&S, as defined in [TS102034], section 5.2.6.2

6.2 GBA authentication

Erratum 11 on GBA authentication consists of two amendments in Volume 4, detailed in the following sub-sections, and one amendment in Voume.7, detailed in section 9.1.

6.2.1 Credential retrieval

The text of section 5.3.6.2.2, "Credential Retrieval by an OITF for Re-use of GBA Authentication" in Volume 4 is replaced with the following:

The key Ks that is established during the GBA registration MAY be reused later for user authentication and service access by consumer network applications.

Each time an OITF needs to access a service that is offered by an AS (i.e. NAF) that requires GBA Authentication, a specific key Ks_NAF SHALL be derived by the IG and the server side GBA Single Sign-on function (the BSF). This generated key SHALL be conveyed to the OITF in the consumer network by the IG, and to the AS by the server side GBA Single Sign-on function (the BSF). The key Ks_NAF SHALL then be used for authentication between the OITF and the AS, using HTTP Digest authentication as specified by [UB_UA]. The OITF SHALL act as the UE as specified in [UB_UA].

As a pre-requisite to this procedure, the GBA procedure MUST have been successfully completed.

The complete procedure for retrieval of credentials by the OITF from the IG is specified in [CSP].

The HNI-IGI procedure for credential retrieval is as follows:-

Step 1: The OITF SHALL send an HTTP POST request to the IG. The request includes FQDN of the NAF. The content of the HTTP Request SHALL be as follows:

- **HTTP Request Headers:** Including the following:
  - <list of HTTP headers> - as per RFC 2616 [HTTP]
  - <X-HNI-IGI-Request> - set to Fetch-GBA-Credentials
  - <X-HNI-IGI-NAF-FQDN> - set to NAF FQDN extracted from the HTTP authentication realm as specified in [UB-UA].
- **HTTP Request Body:** Empty

Step 2: The IG SHALL generate Ks_NAF, which is computed as follows:

Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_ID), where KDF is the key derivation function as specified in Annex B of [GAA] and the key derivation parameters consist of the user's IMPI, the NAF_ID and RAND. The NAF_ID is constructed as follows: NAF_ID = FQDN of the NAF || Ua security protocol identifier as specified in 3GPP 33 220 [GAA]. The identifier for Ua security protocol HTTP Digest authentication according to 3GPP 33 220 [GAA] is (0x01, 0x00, 0x00, 0x00, 0x02).

The IG SHALL return an HTTP 200 OK to the OITF that includes the Ks_NAF, the B-TID, the lifetime of the key Ks_NAF, and optionally the intended identity. The lifetime indicates the expiry time of the key Ks_NAF and is equal to the lifetime of the key Ks (which was specified by the BSF during the GBA bootstrapping procedure). The content of the HTTP 200 OK response is as follows:

- **HTTP Response Headers:** It includes the following:
  - <list of HTTP headers> - as per RFC 2616 [HTTP]
  - <X-HNI-IGI-KS_NAF> - set to the computed Ks_NAF
  - < X-HNI-IGI-B_TID> - set to the B-TID
  - <X-HNI-IGI-LifeTime> - set to life time of the key Ks_NAF
  - <X-HNI-IGI-Intended-Identity> - set to the intended identity. This header is optional and its use is described in [CSP].

6.2.2 IG configuration

The text of section 5.3.5.1.3, "Configuration of the IG via Configuration File" in Volume 4 is replaced with the following:

CPE WAN Management protocol based on Broadband Forum TR-069 [TR069] SHALL be used to configure the IPTV application in the IG. An IPTV configuration file SHALL be used to populate the IG with the list of users with their IMPU, Alias and Passwords and also configure whether user authentication is to be performed by the IG. If GBA Authentication is supported by the IG, the IG SHALL be configured whether it has to provide an intended identity or not in the GBA authentication procedure as described in section 5.3.6.2.2. The file is downloaded to the IG during the IG power up procedure.

The configuration data SHALL be defined in XML and shall include the XML schema to be enforced against the configuration data.

6.3 SIP and SIP/SDP for Content on Demand

In section 6.2.2.1.2, "Protocol over NPI-4, NPI-19, NPI-26" the format of the RTSP DESCRIBE message is changed, to use a MIME type for the Content-type header. The text of section 6.2.2.1.2 in Volume 4 is replaced with the following:

The OPTIONS message SHALL conform to [TS124503] and SHALL be forwarded through the ASM, IPTV Control and CDN Controller FE to the appropriate Cluster Controller, in the same way as for the INVITE message.

In certain cases, the CDN Controller MAY forward the SIP OPTIONS message to a default Cluster Controller.

On receiving the SIP OPTIONS message, the Cluster Controller SHALL issue an RTSP DESCRIBE to the CDF. In certain cases, the Cluster Controller MAY issue an RTSP DESCRIBE to a default CDF. The Content-type header of DESCRIBE message SHALL be set to "application/sdp".

The SDP body included in the RTSP 200 OK response received from the CDF SHALL be included by the Cluster Controller in a SIP 200 OK response to the OPTIONS message. The SIP 200 OK message SHALL be forwarded all the way back to the IG.

This is the only case for which an OPTIONS message will be sent to a Cluster Controller.

Note: If, in a future release, other reasons warrant that the Cluster Controller receive the OPTIONS message, then support for discrimination between the various reasons for sending the OPTION will be required.

In section 7.1.1.2.1, "Missing SDP parameters Retrieval" the format of the RTSP DESCRIBE message is changed, to use a MIME type for the Accept header. The text of section 7.1.1.2.1 in Volume 4 is replaced with the following:

When the Cluster controller receives a SIP OPTIONS message to retrieve missing parameters, it SHALL send an RTSP DESCRIBE message to an appropriate CDF. The "Accept" header SHALL be set to "application/sdp".

The CDF SHALL reply with a RTSP 200 OK with the Content-type header set to "application/sdp".

6.4 Public Service Identifiers

The Public Service Identifiers (PSI) allocated by OIPF have been harmonised to use the prefix "OIPF_". This results in the following changes in volume 4:

In Table 5, in section 5.2.1.1.1 the Public Service Identifier (PSI) of the Scheduled Content service is amended to:

OIPF_IPTV_SC_Service@<domain name>

In Table 10, in section 5.2.2.1.1, and in Table 12, in section 5.2.2.1.2, the Public Service Identifier (PSI) of the CoD services is amended to:

OIPF_IPTV_CoD_Service_*@<domain name>

In Table 21, in section 5.3.4.2.1 the Public Service Identifier (PSI) of the IPTV Service Profile FE is amended to:

OIPF_IPTV-ServiceProfile@<domainname>

6.5 UDP keep-alive messages

In section G.5.2 on "NAT Traversal and keep-alive messages for CoD" of volume 4, text is added to specify the format of keep-alive messages for the case when the transport format of MPEG-2 TS over UDP is applied. The following paragraph is added as the second-last paragraph of section G.5.2:

If the transport format of MPEG-2 TS encapsulated in UDP (direct UDP) is used, keep-alive messages with the following format SHALL be sent in order to keep the NAT bindings open: a UDP packet with body filled with bytes of value 20. The sender and destination IP/port settings follow the same rules as for RTP keep-alive messages.

6.6 Restart using DHCP option 61 and removal of HNI-IGI Restart message

The HNI-IGI Restart Auxiliary message is deprecated and removed, since it is redundant. At boot time the OITF does not have knowledge of whether it is booting for the very first time or it is restarting, so it cannot give an indication of an OITF restart event. Moreover, the only piece of information that this message carries is the DeviceID, and this is already included in DHCP Option 61, thus HNI-IGI Restart Auxiliary message is redundant.

The implied Vol.4 specification amendments are detailed in the following sub-sections.

6.6.1 Consumer Network to Provider Network Interfaces (UNI)

In section 3.1, "Consumer Network to Provider Network Interfaces (UNI)", the HNI-IGI restart message is removed from the list of natively implemented interactions. The fourth paragraph is replaced by the following text:

The interactions that must be implemented natively consist of user registration (Sec. 5.3.6.1 and 6.3.2.2) including service provider discovery (5.3.1.1), and GBA procedures (Sec. 5.3.6.2) performed at OITF startup.

6.6.2 DHCP option usage, common options

In section 12.1.1.1.1, "Common options", the definition of "Client identifier" is added. The following text replaces the third bullet describing the usage of option 61: Client identifier:

- Option 61: Client identifier. In this specification, the DHCP Client Identifier used in OITF devices is the deviceID, defined as follows:.
    - deviceID - Identifies the device. It SHALL be unique within the home network and SHALL NOT change between restarts. The deviceID SHALL be the SHA-1 hash of the MAC address of the interface used to connect to the IPTV service as bytes concatenated with the domain name received via DHCP option 15 in ASCII characters:
        - deviceID=SHA-1(X)
          where: X: = (MAC address as bytes) + (domain name in ASCII characters) and the '+' denoted the concatenation operation. SHA-1 SHALL be used as specified in [SHA-1]. The

domain name SHALL be set to the domain name received via DHCP option 15 (see Section 12.1.1.1.2, "Option 15.")

6.6.3 OITF Restart HNI-IGI Auxiliary Message

Section 5.5.1.9, "OITF Restart HNI-IGI Auxiliary Message" is removed.

6.6.4 References to DeviceID

All references to "S. 5.5.1.9" *and* "X-HNI-IGI-OITF-DeviceID" *or* "DeviceID" *or similar are replaced with* "section 6.3.2.1" *and* "deviceID", *respectively.*

6.6.5 Error Recovery in the IG

In section 5.5.1.10, "Error Recovery in the IG", clause 2) is replaced with the following text:

2) In case the GW is integrated into the IG (referred to as IG-GW), the IG-GW SHALL detect that an OITF is restarted upon receipt of an DHCP server discovery request (DHCPDISCOVER message) and IP address request (DHCPREQUEST message), and where the IG-GW internal state indicates that the OITF is powered on. In such a case, the IG-GW SHALL terminate all active SIP sessions, the IG-GW SHALL de-register all users that are logged in from the restarted OITF as stored in the IG-GW state. Note that the IG-GW is able to keep a mapping between the SIP dialogs ongoing, the IMPUs of registered users, and the IP addresses and DeviceIDs of the devices being used. Following deletion of stale SIP state and de-registration of users, the IG-GW SHALL act on the OITF start up high level procedure Requests.

   Note: this specification does not specify how error recovery works in case he GW is not integrated into the IG.

6.6.6 System Infrastructure, OITF with Native HNI-IGI Support

In section G.1.1, "OITF with Native HNI-IGI Support", Step 4 is removed and subsequent steps re-numbered accordingly, and step 4 is removed from Figure 21. The new text for G.1.1 becomes:

Figure 21 shows the high-level procedural flow for OITF starts up i.e. up to the point where all OITF functions are available. The following is a description of the steps:

Step 1: The local device start up procedure (which is implementation dependent).

Step 2: The OITF SHALL discover the IG through a UPnP procedure (Section 10.1.1.1, "Procedure for IG Discovery").

Step 3: The OITF SHALL use the DHCP option 124/125 to query the DHCP server to obtain the SP Discovery entry point. (See Section 12.1.1.3, "Option 124/125".) If the deployment includes an IG, the DHCP server SHOULD[1] be configured to return the IG address in the DHCP option 125, either as a FQDN or as an IP address. In other words, in such a deployment the IG acts as the SP Discovery entry point (see Section G.3, "IG Startup and Shutdown procedures" for how an IG acts in this role).

Step 4: The OITF SHALL retrieve the list of subscription identities (IMPUs) (Section 5.3.6.3, "User ID Retrieval for managed network services.")

Step 5: The OITF SHALL registers the user identity with the IG (Section 5.3.6.1, "Procedure for User Registration and Authentication in the Managed Model on the HNI-IGI Interface.") An OITF without native support for HNI-IGI SHALL NOT perform this step *at this stage* (see step 9 below).

Step 6: The OITF SHALL perform GBA authentication (Section 5.3.6.2.1, "Initial GBA registration.")

Step 7: The OITF SHALL perform service provider discovery (Section 5.3.1, "Service Provider Discovery.") The service provider information MAY be returned directly by the IG.

[1] The DHCP server MAY, e.g., return the FQDN or IP address of the SP Discovery FE in the network instead.

Step 8: The OITF (or the DAE application, whichever applies) SHALL prompt the user to choose an SP. For any device, the timing and method of presentation as well as the relative positioning of the different SPs to the user is out of scope of the IPTV Solution specifications.

Step 9: The OITF (or the retrieved DAE application, whichever applies) SHALL perform service discovery (see Section 5.3.2, "Service Discovery".)

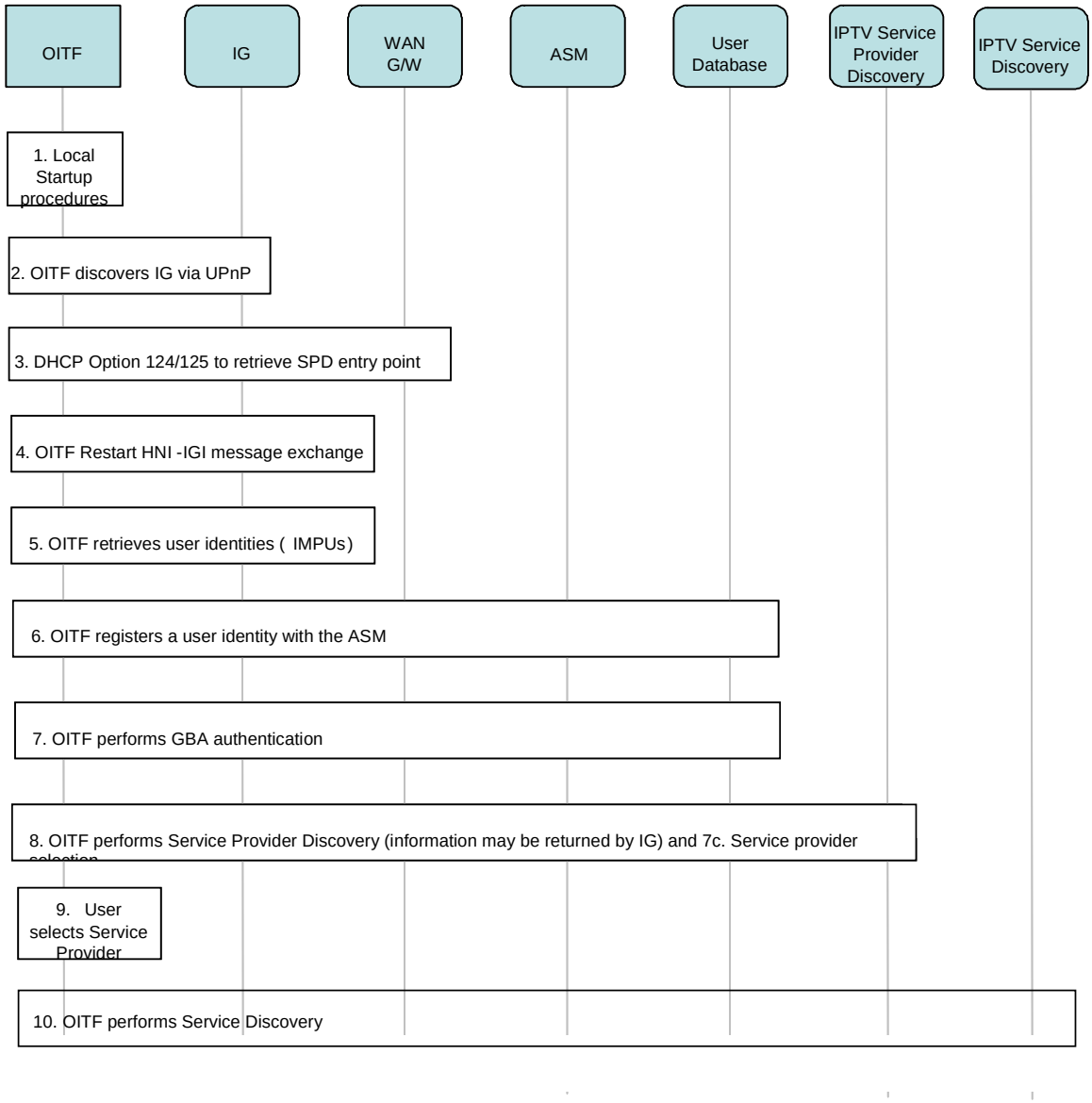

Figure 21: High level Start up procedural flow for an OITF with native HNI-IGI support

6.6.7 OITF Re-start High Level Procedures for an IG integrating GW

New section G.3 is added with the following contents:

This section details how stale SIP state can be detected in an IG integrating the GW, i.e. IG-GW, when an OITF restarts. This procedure is valid for both native and non-native HNI-IGI interfaces.

Figure G.3.1 depicts how the IG-GW is able to establish a mapping between the SIP state (SIP dialog, IMPU and IP address) and the network state (IP address and deviceID).

The ability of the IG-GW to detect stale SIP state upon restart is based on the fact that when an OITF restarts, it re-initiates the DHCP server discovery (sends a DHCPDISCOVER message) and IP address request (DHCPREQUEST) procedures. This is an indication that the OITF has re-started. This is depicted in Figure G.3.2.

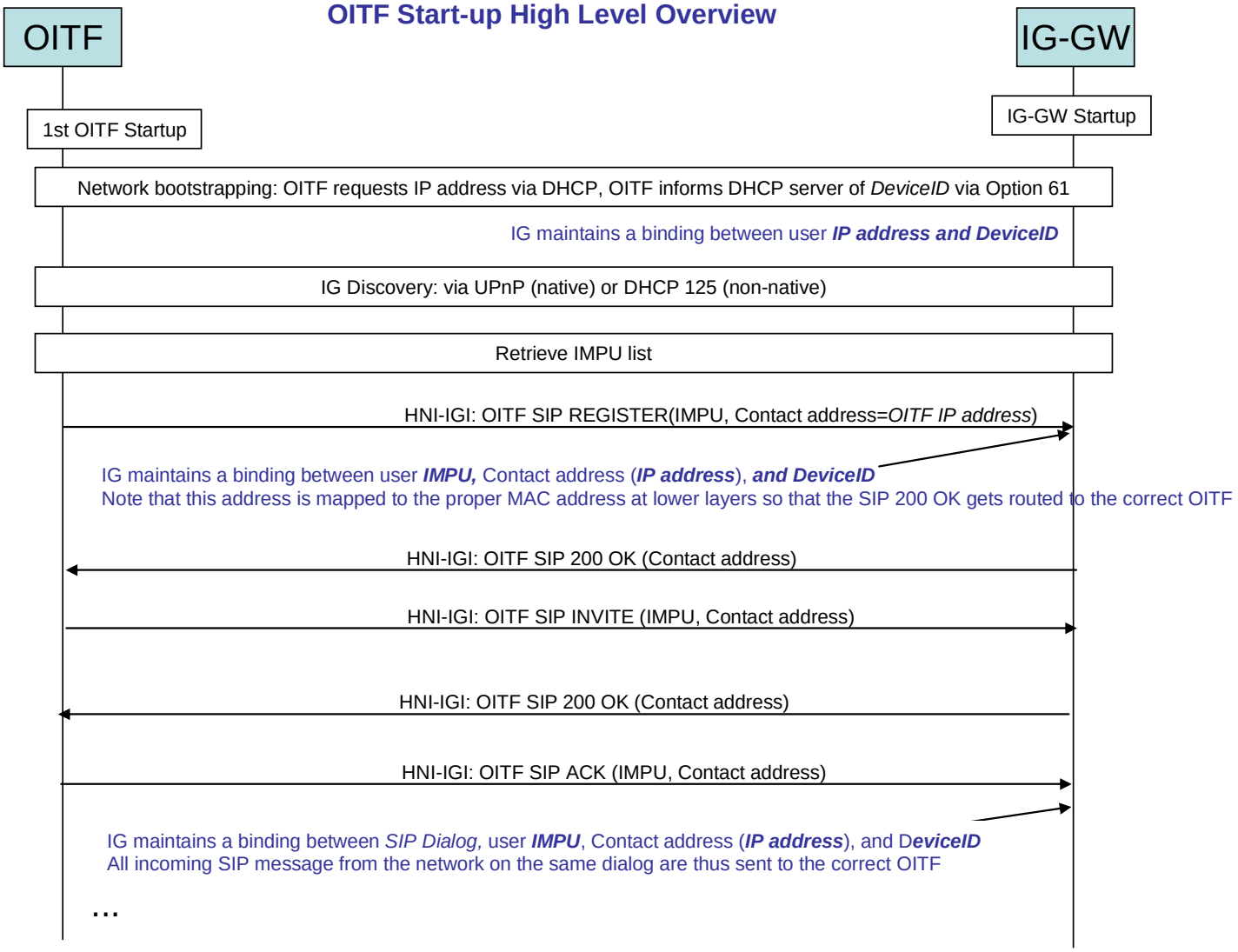

Figure G.3.1: Overview OITF Start-up

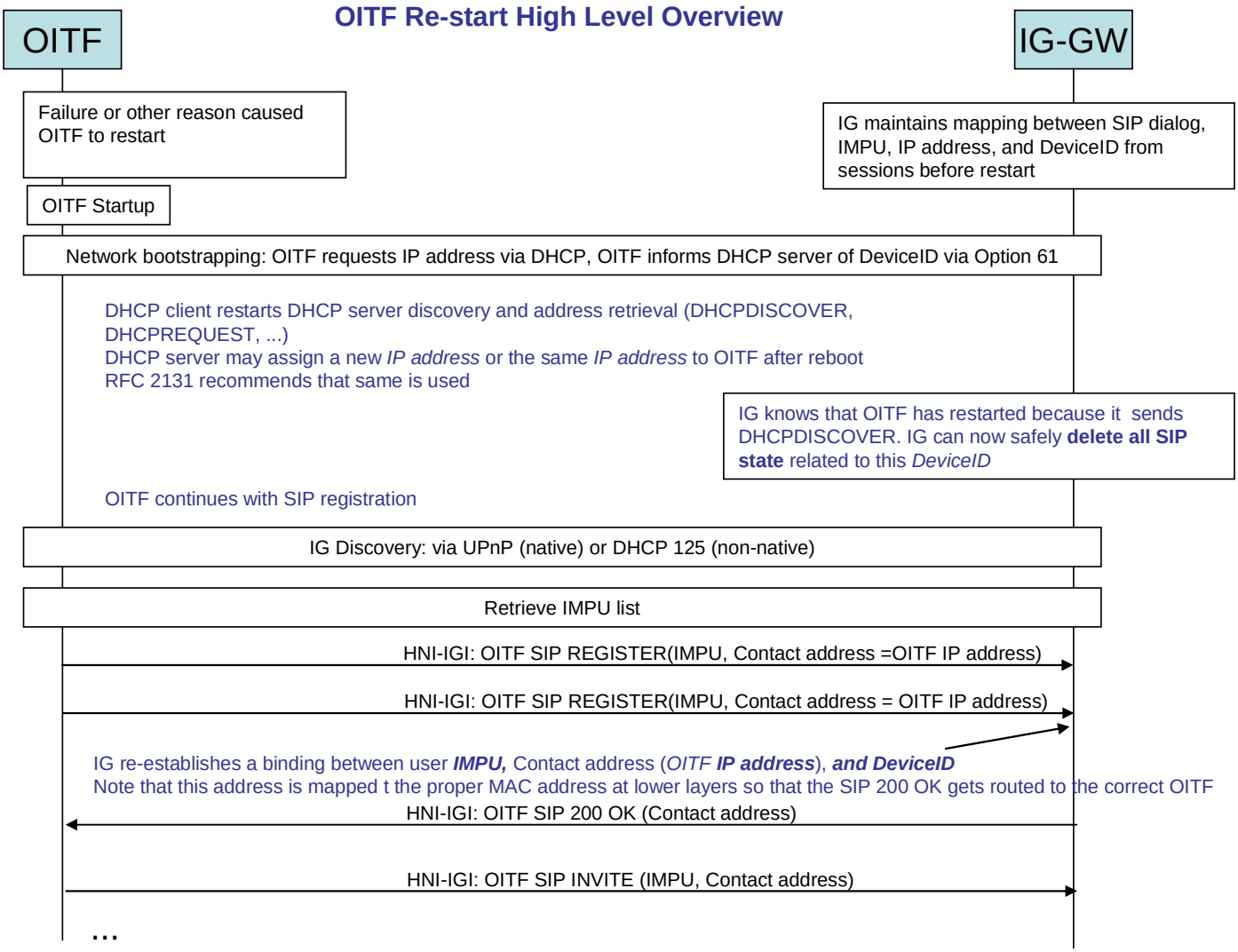

Figure G.3.2: Overview OITF Restart

7 Errata for Volume 5 – Declarative Application Environment

7.1 Parental control API

The following methods are removed from section 7.3.2.2:

getBlockUnrated()

setParentalControlPINEnable()

getParentalControlPINEnable()

The following methods and properties are moved from section 7.3.2.2 to section 7.9.1:

isPINEntryLocked

setParentalControlPIN

unlockWithParentalControlPIN

verifyParentalControlPIN

setBlockUnrated

The definition of setParentalControlStatus() in section 7.9.1.2 is changed to:

`Integer` **`setParentalControlStatus`**`( String pcPIN, Boolean enable )`		
Description	As defined in [CSP], the OITF shall prevent the consumption of a programme when its parental rating doesn't meet the parental rating criterion currently defined in the OITF. Calling this method with `enable` set to `false` will temporarily allow the consumption of any blocked programme. Setting the parental control status using this method SHALL set the status until the consumption of any of all the blocked programmes terminates (e.g. until the content item being played is changed), or another call to the `setParentalControlStatus()` method is made. Setting the parental control status using this method has the following effect: for the `Programme` and `Channel` objects as defined in Sections 7.16.2 and 7.13.12, the `blocked` property of a programme or channel SHALL be set to `true` for programmes whose parental rating does not meet the applicable parental rating criterion, but the `locked` property SHALL be set to `false`. This operation to temporarily disable parental rating control SHALL be protected by the parental control PIN (i.e. through attribute pcPIN). The return value indicates the success of the operation.	
Arguments	*pcPIN*	The parental control PIN.
	enable	Flag indicating whether parental control should be enabled.

7.2 Scheduled recording APIs

In sections 7.10.1.1 and 7.10.2.2 the following text on the bitfield values is amended:

These bitfield values can be 'OR'ed together to repeat a recording.

7.3 Applications management APIs

In sections 7.2.2.1 the property "private" is renamed to "privateData".

This renaming also applies to the examples in 7.2.4.2 and 7.2.5.3, where this property is used.

7.4 On-demand content

Add the following methods (copied from section 7.5.5.2 with slight modifications) to section 7.5.7.2:

`Object item( Integer index )`		
Description	Return the item at position index in the current page, or `undefined` if no item is present at that position. This function SHALL only return objects that are instances of `CODAsset`, `CODFolder`, or `CODService`. Applications SHALL be able to access items in the collection using array notation instead of calling this method directly.	
Arguments	*index*	The index into the collection.

`void getPage( Integer page, Integer pageSize )`		
Description	Retrieve one page of the services contents. The application SHALL be notified by an event targeted at the services parent content catalogue when the data is available. Calls to this method SHALL cancel any outstanding requests.	
Arguments	*page*	The number of the page for which data should be retrieved, indexed from zero.
	pageSize	The size of the page.

`void abort()`	
Description	Abort the current request for a new page of contents. Any results for SHALL be removed (i.e. the value of the `length` property will be 0 and any calls to the `item()` method SHALL return `undefined`),

Modify section 7.14.4.2 as follows

`Object item( Integer index )`		
Description	Return the item at position index in the collection of currently available results, or `undefined` if no item is present at that position. This function SHALL only return objects that are instances of `Programme`, `CODAsset`, `CODFolder`, or `CODService`.	
Arguments	*index*	The index into the result set.

7.5 Application signalling

In the list of normative references, replace the reference to [MHP] with the following;

[TS 102 809]	ETSI TS 102 809 "Digital Video Broadcasting (DVB); Signalling and carriage of interactive applications and services in Hybrid broadcast/broadband environments"
[TS 102 851]	ETSI TS 102 851, "Digital Video Broadcasting (DVB); Uniform Resource Identifiers (URI) for DVB Systems"

In volume 5, replace all uses of the [A137] reference with [TS 102 809].

In section 5.2.7 "Signalling format",

- In the row "5.4.4.14 ApplicationSpecificDescriptor", the "Status in this specification" column shall contain "Ignored".
- The following extra rows are added;

5.4.4.19 TransportProtocolDescriptorType	Abstract base type	Required
5.4.4.20 HTTPTransportType	Type for applications accessed by HTTP	Required
5.4.4.21 OCTransportType	Type for applications accessed by DSM-CC object carousel	Ignored
5.4.4.22 ComponentTagType	Encodes a DVB component tag	Ignored
5.4.4.23 SimpleApplicationLocationDescriptorType	Encodes the location of the start page of an application relative to one of the transport types.	Required
5.4.4.24 SimpleApplicationBoundaryDescriptorType	Encodes an application boundary.	Required

In section 8.3, replace the reference to section C.4.3 of [A137] with 6.3.3 of [TS 102851].

In section 9, replace the references to Annex D of [A137] with Annex C of [TS102809].

In Annex H, replace references to [A137] with [TS102851] and clause C.2 of [A137] with section 6.1 of [TS102851].

7.6 Media resource management

In section 4.4.5, 1) insert the following paragraph at the start of the section;

If insufficient resources are available to present the media, the attempt to play the media SHOULD fail except for the specific case of starting to play audio from memory (see below). For the video/broadcast object, this shall be indicated by a `ChannelChangeError` event with a value of 11 for the error state. For an AV Control object, the `error` property shall take the value 3.

2) Replace the paragraphs beginning "Where applications make conflicting requests for limited media decoding resources," and " If audio from memory interrupts any other media presentation then the interrupted presentation SHALL be restored automatically by the OITF when the interrupting presentation ends." with the following;

In the specific case of a request to play audio from memory while broadcast or broadband streaming audio is being played and where the terminal does not support mixing the audio from memory with the already playing audio, the following shall apply;

- The audio from memory shall have priority and shall interrupt the already playing audio.
- The interrupted presentation shall be resumed automatically by the terminal when the interrupting audio ends.

In section 7.13.1.1, replace "Section 4.4.4 describes the effect on scarce resources when a video/broadcast object is removed from the DOM tree." with the following;

When a video/broadcast object is destroyed (e.g. by the video/broadcast object being garbage collected), or when the release() method is called, control of broadcast video shall be returned to the terminal. If an application has modified the set of components being presented (e.g. changing the audio or subtitle stream being presented) then the same set of components will continue to be presented.

When a video/broadcast object is destroyed due to a page transition within an application, terminals may delay this operation until the new page is fully loaded in order to avoid display glitches if a video/broadcast object is also present in the new page. Presentation of broadcast video or audio shall not be interrupted in either case.

Insert the following at the end of section 7.14.1.1;

9)When an AV Control object is destroyed (e.g. by the AV Control object being garbage collected, or because of a page transition within the application), presentation of streamed audio or video shall be terminated.

7.7 DOM-2 style support

In annex B, in the section of changes to section 5.4, following the item "The W3C CSS working group made an official statement that the following DOM 2 Style features are considered to be problematic and have therefore been classified as obsolete." and the two sub-bullet points, insert the following;

In addition, the DocumentCSS and DOMImplementationCSS interfaces of DOM level 2 Style are also OPTIONAL.

7.8 ApplicationDestroyRequest

In section 7.2.6, in the description of ApplicationDestroyRequest, replace;

If an application registers a listener for this event, and there is a need for the OITF to terminate the current application, once the listener has been invoked, a reasonably short watchdog timer (e.g. 2 seconds) SHALL be started. If the application did not quit by itself (by invoking destroyApplication() for itself) during these 2 seconds, then the application shall be killed forcingly by the OITF.

With

Non-responsive applications SHOULD be forcibly terminated by the OITF, including the case where listeners for ApplicationDestroyRequest events do not return promptly. The determination of when an application is "non-responsive" is terminal-specific.

7.9 Parental rating change events

The `ParentalRatingChange` event was dispatched to the video/broadcast and AV control objects only when the content being played exceeded the parental control threshold set for the OITF. No event was generated when previously-blocked content became unblocked (i.e. when the parental rating of a new programme was lower than that of the preceding programme). This erratum modifies this behaviour to generate the event in both cases.

The text of section 7.13.5 is amended to:

`function onParentalRatingChange( String contentID, ParentalRating rating, String DRMSystemID, Boolean blocked )`

- The function that is called whenever the parental rating of the content being played inside the embedded object changes.

These events may occur at the start of a new content item, or during playback of a content item (e.g. during playback of linear TV content).

The specified function is called with three arguments `contentID`, `rating`, and `DRMSystemID` which are defined as follows:

- `String contentID` – the content ID to which the parental rating change applies. If the event is generated by the DRM system, it SHALL be the unique identifier for that content in the context of the DRM system (i.e. in the case of Marlin BB it is the Marlin contentID). Otherwise it MAY be `null` or `undefined`.
- `ParentalRating rating` – the parental rating value of the currently playing content. The `ParentalRating` object is defined in Section
- `String DRMSystemID` –the DRM System ID of the DRM system that generated the event as defined by element DRMSystemID in Table 8 of Section 3.3.2 of [META]. The value SHALL be `null` if the parental control is not enforced by a particular DRM system.
- `Boolean blocked` – flag indicating whether consumption of the content is blocked by the parental control system as a result of the new parental rating value.

The text of section 7.14.6 is amended to:

`function onParentalRatingChange( String contentID, ParentalRating rating, String DRMSystemID, Boolean blocked )`

The function that is called whenever the parental rating of the content being played inside the A/V Control object changes.

These events may occur at the start of a new content item, or during playback of a content item (e.g. during playback of A/V streaming content).

The specified function is called with three arguments `contentID`, `rating`, and `DRMSystemID` which are defined as follows:

- `String contentID` – the content ID to which the parental rating change applies. If the event is generated by the DRM system, it SHALL be the unique identifier for that content in the context of the DRM system (i.e. in the case of Marlin BB it is the Marlin contentID). Otherwise, it MAY be `null` or `undefined.`
- `ParentalRating rating` – the parental rating value of the currently playing content. The ParentalRating object is defined in Section 7.9.
- `String DRMSystemID` –the DRM System ID of the DRM system that generated the event as defined by element DRMSystemID in Table 8 of Section 3.3.2 of [META]. The value SHALL be `null` if the

parental control is not enforced by a particular DRM system.

- `Boolean blocked` – flag indicating whether consumption of the content is blocked by the parental control system as a result of the new parental rating value.

7.10 Restart using DHCP option 61 and removal of HNI-IGI Restart message

Section 7.3.3.1 is revised to the following

`readonly String` **`deviceID`**

Private OITF Identifier. Unique identifier SHALL take the value `undefined` except when accessed by applications meeting either of the following criteria:

- The application is signalled in an SD&S service provider discovery record with an application usage of `urn:oipf:cs:ApplicationUsageCS:2009:hni-igi` where the SD&S service provider discovery record was obtained by the OITF through the procedure defined in section 5.3.1.2 of [PROT].
- The URL of the application was discovered directly through the procedure defined in section 5.3.1.2 of [PROT].

In these two cases, it SHALL take the same value as defined for the DHCP client identifier in DHCP option 61 in section 12.1.1.1 of [PROT].

8 Errata for Volume 6 – Procedural Application Environment

There are no errata for Volume 6.

9 Errata for Volume 7 – Authentication, Content Protection and Service Protection

9.1 GBA authentication

Erratum 11 on GBA authentication consists of two amendments in Volume 4, detailed in section 6.2, and one amendment in Voume.7, detailed below.

The contents of section 5.4.4.2, "Re-use of GBA Authentication – Using HTTP Digest Authentication" in Volume 7, are replaced by the following:

The key Ks that was established during the GBA registration MAY be used later on for authentication between OITF functions and services (i.e., Application Servers). Each time an OITF needs to access a service offered by an AS (i.e., NAF) that requires GBA Authentication, a specific key Ks_NAF SHALL be derived by the IG and the server side GBA Single Sign-on function (the BSF). This generated key SHALL be conveyed to the OITF function in the residential network by the IG, and to the AS by the server side GBA Single Sign-on function (the BSF). The key Ks_NAF SHALL then be used for authentication between the OITF function and the AS, using HTTP Digest authentication as specified by [3GPP24.109].

If the OITF has registered to an IG which supports GBA Authentication, the OITF SHALL act as a User Equipment in [3GPP24.109] and therefore SHALL signal in its User Agent that it supports GBA Authentication.

When a SAA (acting like a NAF in [3GPP24.109]) requests GBA Authentication, the OITF SHALL retrieve GBA Credentials for the specified NAF from the IG as specified in [OIPF_PROT], and SHALL perform HTTP Digest authentication as specified by [3GPP24.109].

If the OITF retrieves an X-HNI-IGI-Intended-Identity HTTP header from the IG, it SHALL use it as intended user identity and SHALL add an "X-3GPP-Intended-Identity" HTTP header to the outgoing HTTP requests to the Application Server; as specified in [3GPP24.109]. The Application Server MAY verify that the intended identity belongs to the user (i.e. the identity matches one of the user's public identities indicated in the user security setting that was retrieved from the BSF).

As a pre-requisite to this procedure, the GBA registration (cf. 5.4.4.1) MUST have been successfully completed.

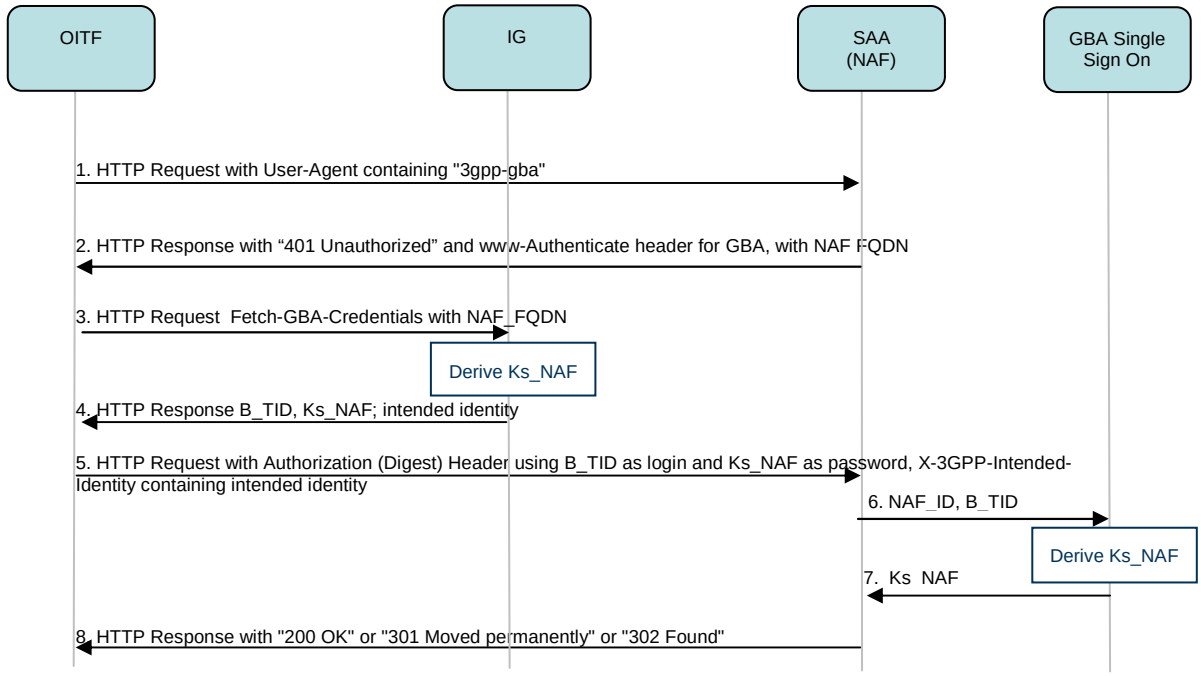

Figure 25 Authentication between an OITF and an SAA Based on GBA Keys

Figure 25 shows the message sequence for authentication between an OITF function and an SAA based on the previously established GBA key. It contains the following steps:

1. OITF function sends a request for a resource (e.g., service) to the SAA (NAF). It is assumed here that the resource requires authentication. The User-Agent string in the HTTP request contains "3gpp-gba" indicating to the SAA that it supports GBA authentication.

2. The SAA (NAF) returns a 401 Unauthorized message, the realm indicates that 3GPP bootstrapping is used and provides the NAF FQDN as defined in [3GPP24.109].

3. OITF sends a request including the NAF_FQDN to the IG to retrieve GBA credentials, and IG generates Ks_NAF. Note: according to [3GPP33.220], the NAF_ID is constructed as follows: NAF_ID = FQDN of the NAF || Ua security protocol identifier. The identifier for Ua security protocol HTTP Digest authentication according to [3GPP24.109] is (0x01,0x00,0x00, 0x00,0x02). The request format is specified in [OIPF_PROT], section 5.3.6.2.2, step 1.

   Ks_NAF is computed as Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_ID), where KDF is the key derivation function as specified in Annex B of [3GPP33.220], and the key derivation parameters consist of the user's IMPI, the NAF_ID and RAND.

4. IG returns Ks_NAF, B-TID, the lifetime of the key Ks_NAF and optionally the intended identity to OITF. The lifetime indicates the expiry time of the key Ks_NAF and is equal to the lifetime of the key Ks (which was specified by the BSF during the GBA bootstrapping procedure). The response format is specified in [OIPF_PROT], section 5.3.6.2.2, step 2.

5. The OITF function repeats the request with an Authorisation header, using B-TID as username and Ks_NAF as password. If a non empty intended identity is returned from the IG, the OITF adds an X-3GPP-Intended-Identity HTTP Header containing the intended identity. If no intended identity is returned from the IG, the OITF shall not add an X-3GPP-Intended-Identity.

6. SAA (NAF) sends B-TID and its NAF_ID to the GBA Single Sign-on function in provider network, the GBA Single Sign-on function retrieves Ks and calculates Ks_NAF.

7. The GBA Single Sign-on function in provider network returns Ks_NAF, together with its lifetime, to SAA (NAF).

   Note the key lifetime returned by the GBA Single Sign-on function is equal to the lifetime of the corresponding Ks. But the SAA (NAF) may choose a shorter key lifetime based on local policy and/or application-specific needs.

8. If Ks_NAF has expired, the SAA (NAF) shall send a suitable bootstrapping renegotiation request to the OITF, according to [3GPP33.220]. Otherwise the SAA (NAF) uses Ks_NAF to authenticate the request. Upon successful authentication, the SAA (NAF)/service serves the request or redirects the OITF to the service. The response may contain session management information (cookie, URL parameter).

The message format for steps 3 and 4 are specified in the section 5.3.6.2.2 of [OIPF_PROT].

9.2 AES usage for MPEG-2 TS scrambling

The specification for the usage of the AES scrambling algorithm for MPEG-2 TS was incomplete as no methods for initialisation vector (IV) setting and termination block handling were specified. This erratum resolves these issues by adopting the IIF Default Scrambling Algorithm specification of ATIS-IIF.

The following amendments to volume 7 are made:

In section 2.1.1, "Standard References", the following is added:

[ATIS-IDSA]	ATIS-0800006, IIF Default Scrambling Algorithm (IDSA)

In section 4.1.5.3, "PMT Table", a second paragraph is added:

In case DVB-SimulCrypt is used with other CA systems as defined in [DVB-SC] and/or with the gateway-centric approach then the content_key_index field in the IEC62455 ECM as defined in [MRL BBTS] SHALL match the

scrambling_mode of the other CA system. If the scrambling algorithm is AES then the next_initial_vector field in the IEC62455 ECM SHALL be set to 0 as specified in [ATIS-IDSA].

In section 4.2.3.6.1 "Protection of MPEG-2 Transport Streams" the third scrambling mode is replaced by that defined in ATIS IDSA, hence Table 19 Scrambling Modes is amended to:

scrambling_mode	Description
0x01	DVB-CSA1
0x02	DVB-CSA2
0x70	AES 128-bit key using the Cipher Block Chaining (CBC) encryption mode with the IV setting and the residual termination block process as specified in [ATIS-IDSA].

Table 19 Scrambling Modes