OpenCable™ Specifications
Home Networking

Home Networking Security Specification

OC-SP-HN-SEC-I02-110512

ISSUED

Notice

This OpenCable specification is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

Document Status Sheet

Document Control Number:	OC-SP-HN-SEC-I02-110512			
Document Title:	Home Networking Security Specification			
Revision History:	I01 – Released 12/17/09 I02 – Released 05/12/11			
Date:	May 12, 2011			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~WG ONLY~~	~~CL/Member~~	~~CL/Member/ NDA Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

1 SCOPE

1.1 Introduction and Purpose

This specification describes the security requirements for an OpenCable home networking host device, such that a registered privileged application allows the access streaming of the MSO Recorded Content from a server device to a client device within the home network. This specification is a required extension to the Home Networking specifications.

A privileged OCAP application optionally can register itself to be notified if MSO Recorded Content is requested to be streamed or a UPnP service action is invoked by another device. The registered OCAP application can grant or deny access to the content streaming or the UPnP service action, based on its internal logic. The internal logic as to how the registered OCAP application determines granting or denying the request is beyond the scope of this specification.

If no privileged OCAP application is registered, the security will default to the underlying approved Home Networking Content Protection (HNCP).

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"SHALL"	This word means that the item is an absolute requirement of this specification.
"SHALL NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific:

- For a specific reference, subsequent revisions do not apply.
- For a non-specific, non-Bundle reference, the latest version applies.
- For non-specific CableLabs references that are part of the [OC-BUNDLE], the versions mandated in a particular Bundle apply.

[DLNA vol 3] Networked Device Interoperability Guidelines - Expanded: October 2006, Volume:3 Link Protection, http://www.dlna.org/industry/certification/guidelines/, Digital Living Network Alliance.

[DTCP-IP] Digital Transmission Content Protection

[HNP] OpenCable Home Networking Protocol 2.0, OC-SP-HNP2.0, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].

[HOST-DVR] Host 2.X DVR Extension, OC-SP-HOST2-DVREXT, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].

[OC-BUNDLE] OC-SP-BUNDLE, OpenCable Bundle Requirements. See section 2.3.1 to acquire this specification.

[OCAP] OpenCable Application Platform (OCAP), OC-SP-OCAP, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].

[OCAP-HN] OCAP Home Networking Extension, OC-SP-OCAP-HNEXT, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].

[tru2way] tru2way Host Device License Agreement, http://www.opencable.com/downloads/tru2way_agreement.pdf, Cable Television Laboratories, Inc.

2.2 Informative References

This specification uses the following informative references.

2.3 Reference Acquisition

2.3.1 OpenCable Bundle Requirements

The OpenCable Bundle Requirements specification [OC-BUNDLE] indicates the set of CableLabs specifications required for the implementation of the OpenCable Bundle. The version number of [OC-BUNDLE] corresponds to the release number of the OpenCable Bundle that it describes. One or more versions of [OC-BUNDLE] reference this specification. Current and past versions of [OC-BUNDLE] may be obtained from CableLabs at http://www.cablelabs.com/opencable/specifications.

2.3.2 Other References

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Digital Living Network Alliance[SM], DLNA Administration, C/O VTM Attn: Membership Services, 3855 SW 153rd Drive Beaverton, Oregon 97006; Phone: +1-503.619.0422, Fax: +1-503.644.6708, http://www.dlna.org/home

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Broadcast Content	The MSO Content streaming directly from an HFC network, using the tuner of an OCHN Device to receive the content. The difference between Live Content and Broadcast Content is that the Broadcast Content can be received in the future.
Buffered Content	Content that is recorded to the Buffered Storage. The content may or may not be presented to the user. For example, the content is buffered in the background with no presentation.
Buffered Recording	A type of content recording, where the content is stored on a Buffered Storage.
Buffered Storage	A type of media storage, where the stored content does not survive a power-cycle and the storage is limited. The content is overwritten as the end of the buffer is reached.
Buffering	The act of storing content into a Buffered Storage for future possible use by the Subscriber.
Digital Storage	A type of media storage, such as a hard drive or a circular buffer, that is used for stream buffering or permanent storing of the content. There are two types of Digital Storage: Permanent Storage and Buffered Storage.
DVR Content Protection	The encryption method used to secure MSO-provided controlled content on the DVR as specified by [HOST-DVR].
Home Networking Interface Mapping Protocol	An OCAP implementation that provides a network interface compliant with [HNP].
Live Content	The MSO Content streaming directly from an HFC network using the tuner of either an OC-DMP Device or an OC-DMS Device to receive the content. The Live Content can be immediately rendered using either the OC-DMP Device's Tuner or the OC-DMS Device's Tuner.
MSO Content	The content that arrives to Subscriber's home through HFC network. There are three types of MSO Content: Broadcast Content, Live Content, and On-Demand Content.
Non-buffered Content	Content that is being rendered by the OC-DMP Device, received on the tuner of either OC-DMP Device or OC-DMS Device, and is NOT stored in a Buffered Storage.
OpenCable Digital Media Player	An OCHN Device that is attached to the home network and receives and renders content to the display. This device is not discoverable by other devices in the home network. The UPnP Control Point resides in the OC-DMP.
OpenCable Digital Media Server	An OCHN Device containing one or more tuners and Digital Storage, which is attached to the home network and provides content to the OC-DMP.
OCHN Device	OpenCable Home Network Device is an OCAP device.
On-Demand Content	The MSO Content streaming directly to an HFC network, where the Trick-mode of the content occurs at the headend.
OpenCable Bundle	The OpenCable Bundle defines a set of specifications required to build a specific version of an OpenCable device. See [OC-BUNDLE].

Permanent Recording	A type of content recording, where the content is stored on Permanent Storage; therefore, it survives a power-cycle. Although the storage is limited, the recorded content is not overwritten.
Permanent Storage	A type of media storage, where the stored content survives a power-cycle.
Render	Presentation of any content either from Digital Storage or tuner to the display device on the OC-DMP Device for viewing by the Subscriber.
Resources	Could reference to one of these resources: Tuner, Digital Storage, Circular Buffer, and bandwidth.
Series-based	A collection of programs that are related through an MSO-defined metadata.
Stream Buffered Content	MSO Content streaming from a Buffered Storage where the content is being rendered on the OC-DMP Device.
Subscriber	An MSO user interacting with the Local or OC-DMS Devices within Home Network.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

API	Application Program Interface
BCM	Basic Connection Management
CA	Conditional Access
CDS	Content Directory Service
DTCP-IP	Digital Transmission Content Protection over IP
DCP	DVR Content Protection
HDCP	High-Bandwidth Digital Content Protection
HNCP	Home Network Content Protection
HNIMP	An OCAP implementation that provides a network interface compliant with [HNP]
IMA	Initial Monitor Application
LOCP	Local Output Content Protection
MOCA®	Multimedia over Coax Alliance
OC-CP	OCHN Control Point
OC-DMP	OpenCable Digital Media Player
OC-DMS	OpenCable Digital Media Server
OCHN	OpenCable Home Network
OSH	OCAP Security Handle
RSD	Reserved Service Domain
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SRS	Scheduled Recording Service

5 OVERVIEW

For the purposes of this specification, Home Network Security applies to several areas:

- RSD Security – refers to authentication and authorization of devices for requesting resources (e.g., QoS) within the home network. The RSD Security is beyond the scope of this specification.
- Link Layer Protection – refers to content encryption and CCI enforcement using an approved Home Networking Content Protection technology (HNCP).
- UPnP service action invocation – refers to authentication of UPnP service action invocation by a remote/client device.
- Usage Rights – refers to a set of usage rights that an MSO privileged application applies to the content. Details of how usage rights are defined and enforced are beyond the scope of this specification. An MSO privileged application, as enabled by this specification, can choose to apply its own proprietary usage rights prior to starting an activity, in addition to the approved HNCP technology.
- Passwords – setting link layer network security passwords.

This specification provides a set of tools such that a registered MSO privileged application can apply its set of use rights for each UPnP service action invocation, streaming of MSO Recorded Content, in addition to setting password for link layer.

Encrypting and/or signing of the UPnP service actions are beyond the scope of this version of this specification.

5.1 Assumptions

The assumption for this specification is that the server device providing the MSO Recorded Content to another client/remote device is an OpenCable Home Networking certified device (OC-DMS), which either has a native application or an OCAP MSO privileged application that can communicate through its own proprietary mechanism to other MSO applications with other remote/client devices (i.e., Rendering, Player, or Control Point Devices).

6 CONTENT SECURITY

6.1 MSO Authorization Process

The MSO Authorization Process in this specification refers to two distinct processes. First, it refers to the process of a server device (i.e., OC-DMS) authorizing a control point (i.e., OC-CP) when it is requested to stream MSO Recorded Content, if the interest is registered by an MSO privileged application. Note that an OC-CP can be part of an OC-DMR, OC-DMP, or OC-DMS. Second, it refers to the process of authorizing invocation of UPnP service actions on the OC-DMS, if the interest is registered by an MSO privileged application. The HNIMP OC-DMS provides APIs and behavior requirements, as defined by [OCAP-HN] and [HNP].

The HNIMP OC-DMS SHALL allow an MSO privileged application to register an interest for authorization of control point streaming the MSO Recorded Content or invoking a UPnP service action on the OC-DMS.

The OC-DMS SHALL allow an MSO privileged application to register interests in streaming MSO Recorded Content or invocation of UPnP service specific actions independently.

If there is an MSO privileged application registered, the OC-DMS SHALL consult with the MSO privileged application as to whether to grant the access or not, prior to streaming of the MSO Recorded Content to the OC-CP or invocation of the UPnP service action on the OC-DMS. The details of how an MSO privileged application determines whether the streaming or invocation requests are to be granted or denied are application-specific. This specification describes the tools and APIs provided to the MSO privileged application to be utilized for the MSO Authorization Process.

The MSO Recorded Content traversing across the home network is protected by the approved HNCP technology. The MIME type for the ContentItems for MSO Recorded Content in the Content Directory indicates one of the approved HNCP technology, for example, DTCP-IP MIME type (see [DTCP-IP]).

6.2 MSO Recorded Content

In this specification, MSO Content refers to the content that has arrived from the cable headend. It is up to the MSO privileged application whether to allow the MSO Content to be shared among home network devices. Once the MSO privileged application decides to create a content item entry for the MSO Content, the content is then protected by the approved HNCP technology, complying with the Licensing rules of the HNCP. The HNIMP OC-DMS SHALL mark the MSO Content with the value of one in the msoContentIndicator property field in the CDS. For the purpose of this specification, content item marked with the msoContentIndicator property field set to one is called MSO Recorded Content.

6.3 Content Protection

The MSO Content MAY be protected across the path from the headend to the recipient device by various content encryption mechanisms. This section describes how the content is protected across the path while passing through equipment and network devices.

The MSO Content arriving on the HFC network from the cable headend MAY be protected with the MSO Conditional Access (CA). If this controlled content is stored onto a DVR box (i.e., OC-DMS), it is protected using DVR Content Protection (DCP), as specified by the [HOST-DVR] specification. Once an OC-DMS requests to stream the MSO Recorded Content across the home network, the OC-DMS first decrypts the DCP encrypted content and then re-encrypts it with the approved HNCP technology. The OC-DMP Device decrypts from the approved HNCP technology and re-encrypts it for the Local Output Content Protection (LOCP). Figure 1 depicts an example of the encryption and decryption of the content.

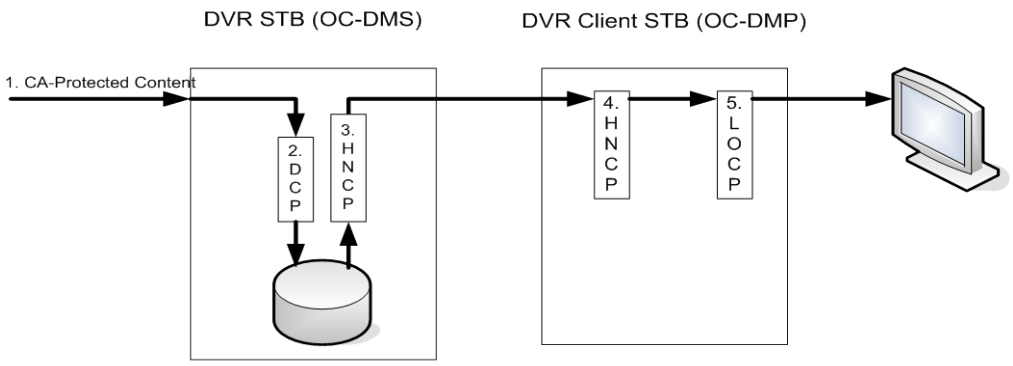

Figure 1 - Example of Content Protection

The steps shown in Figure 1 are described below:

Step 1. The MSO Content MAY arrive CA or otherwise protected at the OC-DMS.

Step 2. If the MSO Content that is to be recorded arrives encrypted from the headend, it is decrypted, and re-encrypted with DVR Content Protection (DCP) scheme. It is up to the registered MSO privileged application whether to allow the content to be shared within home network devices or not. Once the MSO application decides to create a content item entry for the MSO Recorded Content, the content is protected by the approved HNCP technology, as described in the next step.

Step 3. The MSO Recorded Content is then DCP decrypted and encrypted with the approved HNCP technology.

Step 4. The MSO Recorded Content traverses across the home network protected by the approved HNCP technology, and is decrypted at the OC-DMP or the OC-DMR.

Step 5. The MSO Recorded Content is then encrypted with one of the Local Output Content Protection (LOCP); for example, HDCP, and sent to the Display Device, where it can be decrypted by the Display Device.

The OC-DMS protects the content prior to the storage onto the DVR using a DVR Content Protection (DCP) encryption, as required by the Compliance and Robustness rules of the [tru2way] license agreement and the [HOST-DVR] specifications.

When requested, the OC-DMS SHALL decrypt the MSO Recorded Content from DVR Content Protection and SHALL re-encrypt by one of the approved HNCP technologies, as described by the Compliance and Robustness rules of the [tru2way] license agreement.

6.4 Link Layer Protection

In the case of multiple link layer protection, the res elements are listed in a single CDS object (rather than multiple CDS objects with different res elements). This allows the OC-DMP or OC-DMR to select the most optimal content protection for their respective devices.

The HNIMP OC-DMS SHALL protect the MSO Recorded Content traversing across the home network using an approved HNCP technology, as indicated by res element in the CDS object.

If the MSO Recorded Content is marked by link layer protection DTCP-IP, the HNIMP OC-DMS SHALL populate the res@protocolInfo with the parameters, as defined in DLNA Link Protection guidelines (see [DLNA vol 3]).

The HNIMP OC-DMS SHALL advertise the DTCP-IP port number as specified in the comment of [DLNA vol 3] requirement [8.3.1.1].

6.5 Approved Home Networking Content Protection

The approved HNCP technology is DTCP/IP as described in [DTCP-IP] specification.

The approved HNCP technology may be amended and extended in the future as approved by CableLabs.

6.6 OCAP Security Handler

The OCAP Security Handler (OSH) is a logical MSO privileged application that can be registered to get notification for authorization of the following activities independently:

- Streaming MSO Recorded Content
- Invoking UPnP service action

If OSH has registered interest to receive notification, then HNIMP OC-DMS SHALL notify OSH when streaming of the MSO Recorded Content has been requested to be started or stopped. The HNIMP OC-DMS SHALL only grant access to the MSO Recorded Content when the registered OSH grants access. If OSH is not registered at all, or if OSH has not registered interest to receive notification, then OC-DMS SHALL grant access to streaming of all MSO Recorded Content in accordance to the underlying approved HNCP protection.

If OSH has registered interest to receive notification, then HNIMP OC-DMS SHALL notify OSH when one or more specific UPnP service actions are invoked. The HNIMP OC-DMS SHALL only grant access to the UPnP service invocation when the registered OSH grants access. If OSH is not registered at all, or if OSH has not registered interest to receive notification, then OC-DMS SHALL grant access to all UPnP service actions.

The HNIMP OC-DMS SHALL provide the following information to OSH when an MSO Recorded Content Item is requested to be streamed and OSH has registered interests to receive notification for the MSO Recorded Content:

- IP Address of the requesting device invoking the activity
- MAC Address of the requesting device invoking the activity
- Content URI

The HNIMP OC-DMS SHALL notify the OSH when an MSO Recorded Content stream has been terminated as defined by Section 6.9.

If an OSH is registered and has overloaded the method by a UPnP service action name, the HNIMP OC-DMS SHALL notify the OSH when a UPnP service action identified by the argument is invoked, as defined by the [OCAP-HN] specification.

The HNIMP OC-DMS SHALL consult with the OSH as to whether or not to grant invocation of the UPnP service action as defined by the argument of registered OCAP application.

6.7 Registration

An MSO privileged application can choose to register interests regarding whether OSH is to be notified by the HNIMP OC-DMS if streaming of the MSO Recorded Content is requested to be started. In addition, the MSO privileged application can choose to register an OSH to be notified by the HNIMP OC-DMS, if an interested UPnP service action (i.e., based on the action name) is invoked by overloading the same method and specifying the action name as defined by the UPnP specification.

6.7.1 Default Behavior

If no OSH is registered with HNIMP OC-DMS, or is registered but has not set the interest flag, the HNIMP OC-DMS SHALL grant streaming of MSO Recorded Content based on the approved HNCP technology, as described in Section 6.7.1 of this specification.

If no OSH is registered with HNIMP OC-DMS, or is registered but has not overloaded the method with any UPnP service actions, the HNIMP OC-DMS SHALL grant access to all UPnP service actions.

NOTE: If OSH is not registered with the Initial Monitor Application (IMA), all the requests to access MSO Recorded Content arriving prior to the registration are granted access according to HNCP technology.

6.7.2 Un-registration

Once an OSH is registered with HNIMP OC-DMS, an MSO privileged application can unregister the OSH. Once an OSH is unregistered (org.ocap.hn.security.NetSecurityManager.setAuthorizationHandler set to null), the access to

the MSO Recorded Content is defaulted to the approved HNCP technology, as described in Section 6.7.1 of this specification. In addition, if an MSO privileged application unregisters OSH, the access to all UPnP service actions is granted.

6.8 Start Streaming MSO Recorded Content

When OSH is registered with the notifyTrasportRequests parameter set to FASLE [OCAP-HN], the OC-DMS notifies registered OSH upon the receipt of the first transport request for playback of MSO Recorded Content from an OC_DMP as specified in [HNP].

The OC-DMP is capable of streaming MSO Recorded Content using various transport protocols from an OC-DMS, such as HTTP or RTP/RTSP, according to the protocol info indicated in the content item. This section describes OC-DMS requirements for identifying first transport request for HTTP and RTP/RTSP.

6.8.1 HTTP Protocol

If a Control Point uses the HTTP protocol to stream the MSO Recorded Content, the HNIMP OC-DMS SHALL consider the HTTP request to be the first transport request according to the following rules:

- If no scid.dlna.org header is present in the request and the HTTP request is not on the same content item from the same requesting device's IP address, and if the stream has not been terminated previously as described by Section 6.9.
- If scid.dlna.org header is present in the request, but does not match a currently open connection that has already been authorized by a call to the notifyActivityStart method.

When an HTTP is the first request, the HNIMP OC-DMS SHALL create an scid.dlna.org value for the response, if it is not already by the Connection Manager::PrepareForConnection().

6.8.2 RTP/RTSP

If a Control Point chooses RTP/RTSP protocol to stream the MSO Recorded Content, the HNIMP OC-DMS SHALL consider RTSP::SETUP message as the first transport request.

6.8.3 MSO Content Streaming Authorization Process Scenario

Figure 2 shows an example scenario diagram of interaction between an OC-DMP device and OC-DMS device for MSO Authorization Process, if the parameter is set for checking only on the first try.

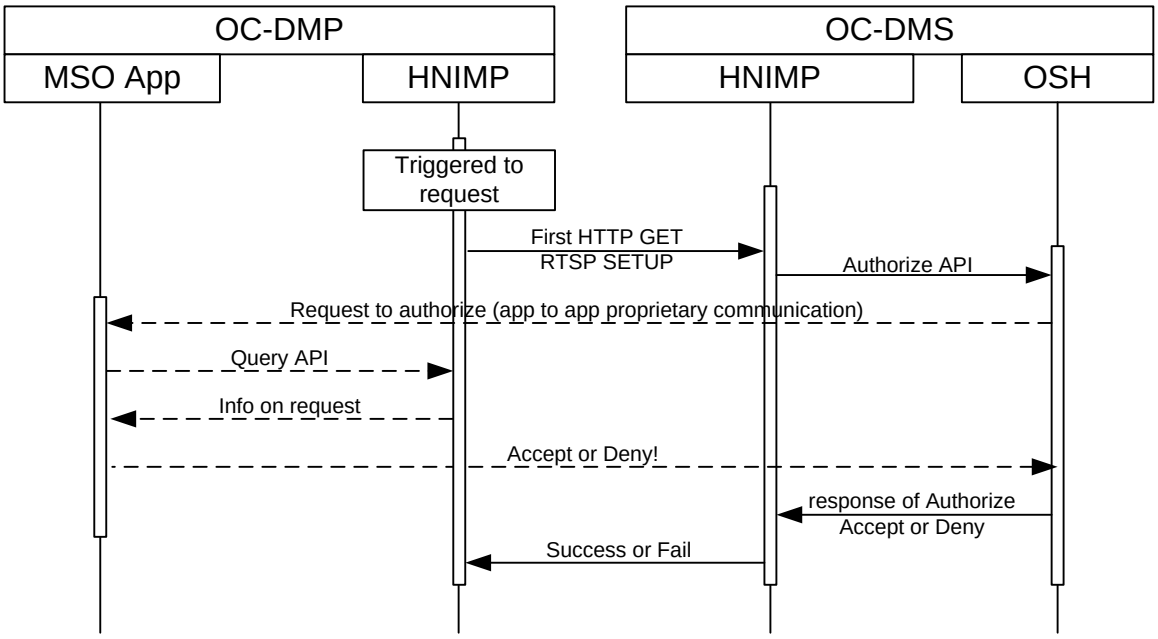

Figure 2 - Authorization Trigger Example

The steps shown in Figure 2 are described below:

Step 1. A trigger occurs on the OC-DMP to request an MSO Recorded Content.

Step 2. The OC-DMP sends its first HTTP GET request or RTSP SETUP request to the OC-DMS implementation.

Step 3. The HNIMP OC-DMS invokes (org.ocap.hn.security.NetAuthorizationHandler.notifyActivityStart), if an OSH is registered; otherwise grants access according to the approved HNCP technology.

Step 4. Optionally, OC-DMS OSH (through a proprietary mechanism) communicates with the application on OC-DMP to see if the device is authorized. The details of this communication and design are beyond the scope of this specification.

Step 5. Optionally, the MSO privileged application on the OC-DMP can query the HNIMP OC-DMS to discover whether a request has been initiated on its behalf.

Step 6. If requested by Step 5, the HNIMP OC-DMP responds with information about the home networking request that has been sent out.

Step 7. Optionally, through an application to application communication between the OSH on OC-DMP and OC-DMS, the OSH, or other mechanisms determined by OSH on the OC-DMS, determines whether the request is granted or denied.

Step 8. The OC-DMS OSH responds to the HNIMP OC-DMS with either accept or deny.

Step 9. If the request is accepted, the streaming of the MSO Recorded Content can be can be granted to OC-DMP device. If the request is denied, the streaming of the MSO Recorded Content can not be granted.

6.9 Stopped Streaming Content

The HNIMP OC-DMS notifies the registered OSH when an OC-DMS stops the playback of the MSO Recorded Content. The streaming of the content can be stopped either implicitly or explicitly. If UPnP service action causes the termination of the streamed content, the OSH needs to register for the UPnP action (i.e., CM::ConnectionComplete()) to receive notification of the termination.

6.9.1 Implicit Termination of Streaming Content

The HNIMP OC-DMS determines the termination of streaming content as follows:

For HTTP streaming when, for a period of time as determined by the HNIMP OC-DMS, no HTTP request has arrived for the ContentItem from IP Address of the requesting device, the OC-DMS SHALL consider the content streaming to be terminated. The time-out period is configured by the HNIMP OC-DMS.

For RTSP streaming, when RTSP::TEARDOWN is invoked, the OC-DMS SHALL consider the content streaming to be terminated.

In addition, the OC_DMS SHALL consider the content streaming to be terminated when

the content is deleted (while it was being streamed), or

a fatal error has occurred that required closing the streaming of the session.

The HNIMP OC-DMS SHALL match activity end occurrences with activity start occurrences and pass the activity identifier to the notifyActivityEnd method that was returned from the corresponding call to the notifyActivityStart method.

6.9.2 MSO Content Streaming Termination Process Example

Figure 3 depicts an example scenario diagram of interaction between an OC-DMP and an OC-DMS for the MSO Termination Process.

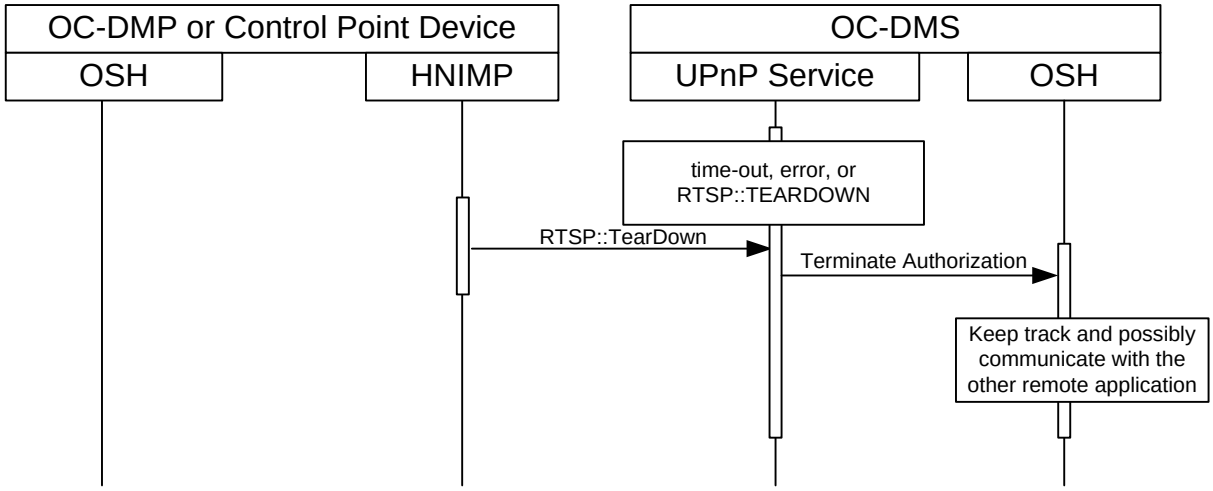

Figure 3 - Termination Trigger Example

The steps shown in Figure 3 are described below:

Step 1. Either the OC-DMP invokes an action on the OC-DMS to cause the Termination API to be called, or a time-out occurs. There are three cases when the Termination API is called: 1) no activity from the OC-DMP for a period of time, 2) CM::ConnectionComplete(), or 3) RTSP::TEARDOWN.

Step 2. The HNIMP OC-DMS invokes the OSH Terminate API (org.ocap.hn.security.NetAuthorizationHandler.notifyActivityEnd) if an OSH is still registered.

Step 3. The OSH updates its internal states and possibly communicates with other applications (this is purely an OSH proprietary design implementation).

6.10 UPnP Service actions

If an OC-DMP invokes any UPnP actions on the OC-DMS, and if the OSH has been registered for that action, the HNIMP OC-DMS SHALL invoke OSH Authorization API (org.ocap.hn.security.NetAuthorizationHandler. notifyAction).

6.11 Revocation

It is possible in the middle of streaming content that OSH revokes the streaming request authorization. When this occurs, the OSH invokes the revocation API to notify the HNIMP OC-DMS that it can no longer stream the request arriving from this device for this content item.

When the HNIMP OC-DMS receives this revocation API (org.ocap.hn.security.NetSecurityManager.revokeAuthorization), the OC-DMS SHALL stop streaming the content to the OC-DMP requesting the content for which the authorization has been revoked.

6.12 Network Password

An MSO privileged application can set and get the password for MOCA or wireless Ethernet link layer home network interface.

The HNIMP OC-DMS SHALL set and get the password for the MOCA or wireless Ethernet link layer home network interface when requested by OSH, using org.ocap.hn.security.NetSecurityManager.setNetworkPassword and org.ocap.hn.security.NetSecurityManager.getNetworkPassword APIs, respectively.

Appendix I Revision History

The following ECNs were incorporated into version I02 of this specification:

EC Identifier	Accepted Date	Title of EC
HN-SEC-N-11.1669-2	5/12/11	OCAP HN SEC Reference edits for OpenCable bundle inclusion