OpenCable™ Specifications
Home Networking

Home Networking Security Specification

OC-SP-HN-SEC-I05-130418

ISSUED

Notice

DISCLAIMER

This document is published by Cable Television Laboratories, Inc. ("CableLabs®").

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various agencies; technological advances; or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein. CableLabs makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the document or any information or opinion contained in the report. Any use or reliance on the information or opinion is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any cable member to purchase any product whether or not it meets the described characteristics. Nothing contained herein shall be construed to confer any license or right to any intellectual property, whether or not the use of any information herein necessarily utilizes such intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	OC-SP-HN-SEC-I05-130418			
Document Title:	Home Networking Security Specification			
Revision History:	I01 – Released 12/17/09 I02 – Released 05/12/11 I03 – Released 01/12/12 I04 – Released 05/31/12 I05 – Released 04/18/13			
Date:	April 18, 2013			
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

This page intentionally left blank.

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 running in a server device allows:

- Streaming of the MSO Recorded Content from a server device to a client device within the home network
- Streaming of Live Content
- Content Copy operations

This specification is a required extension to the Home Networking specifications.

A privileged OCAP application can register itself to be notified if MSO Recorded Content or Live Content is requested to be streamed or a UPnP service action is invoked by another device. Additionally, it will be notified if Copy Operations are requested over the home network. The registered OCAP application can grant or deny access to the content streaming or the UPnP service action, based on its internal logic.

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.

[CCCP] OpenCable CableCARD Copy Protection 2.0 Specification, OC-SP-CCCP2.0, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].

[DLNA vol 1] Digital Living Network Alliance Home Networked Device Interoperability Guidelines; expanded: October 2006, Volume 1: Architectures and Protocols.

[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.

[DLNA vol 4] DLNA Networked Device Interoperability Guidelines, Volume 4, DRM Interoperability (DTCP-IP), June 09, 2009, V 0.9.

[DTCP] DTCP Specification Volume 1, Revision 1.7.

[DTCP-IP] DTCP Volume 1, Supplement E Mapping DTCP to IP, Revision 1.4.

[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].

[MPEG-DASH] ISO/IEC 23009-6 Information Technology—MPEG systems technologies – Part 6: Dynamic adaptive streaming over HTTP (DASH).

[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

[MPEG-4] ISO/IEC 14496-14:2003, Information technology - Coding of audio-visual objects - Part 14: MP4 file format.

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
- Digital Transmission Licensing Administrator, www.dtcp.com

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 HNIMP OC-DMS 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.
Client Device	A DLNA compliant device in the DMP class. Includes OC-DMP.
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.
DLNA Premium DMP	A DLNA DMP device that is capable of running an RUI that can authenticate and verify entitlements for premium services.
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. Types of MSO Content include: Broadcast Content, Live Content, On-Demand Content, Recorded 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 HNIMP OC-DMP 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 Renderer	An OC-DMR is a device that complies with DLNA DMR guidelines and OpenCable requirements for renderers.
OpenCable Digital Media Server	An HNIMP OC-DMS containing one or more tuners and Digital Storage, which is attached to the home network and provides content to the OC-DMP.
OpenCable Control Point	OpenCable Control Point is a logical entity that includes UPnP control point functionality, as well as extensions as specified in this specification for a UPnP control point.

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
CCI	Copy Control Information
CDS	Content Directory Service
DTCP-IP	Digital Transmission Content Protection over IP
DCP	DVR Content Protection
EMI	Encryption Mode Indicator
fMP4	Fragmented MP4
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
MP4	MPEG-4
NAH	Network Authorization Handler
OC-CP	OpenCable Control Point
OC-DMP	OpenCable Digital Media Player
OC-DMR	OpenCable Digital Media Renderer
OC-DMS	OpenCable Digital Media Server
PCP-UR	Protected Content Packet - Usage Rule
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:

- 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.

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 an OC-DMS HNIMP authorizing a client device when it is requested to stream or copy Live MSO Content and interest is registered by an MSO privileged application. Second, it refers to the process of authorizing invocation of UPnP service actions on the OC-DMS when 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 provides an API to allow an MSO privileged application to register as an authorization agent that can allow or deny streaming of MSO Recorded and Live Content, copy of MSO Recorded Content, or a UPnP service action request on the OC-DMS.

If there is an MSO privileged application registered, the OC-DMS consults with the application prior to granting access to network activities such as:

- streaming of MSO Recorded Content
- streaming of Live Content
- copying of MSO Recorded Content to a device over the home network
- invocation of a UPnP service action on the OC-DMS

The details of how an MSO privileged application determines to grant or deny streaming or action invocation requests are application-specific. This specification describes the tools and APIs provided to the MSO privileged application to be utilized for the MSO Authorization Process.

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

6.2 MSO 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.

For the purpose of this specification, a content item marked with the msoContentIndicator property field set to true is called MSO Content.

6.3 Content Protection

Selected MSO Content is 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.

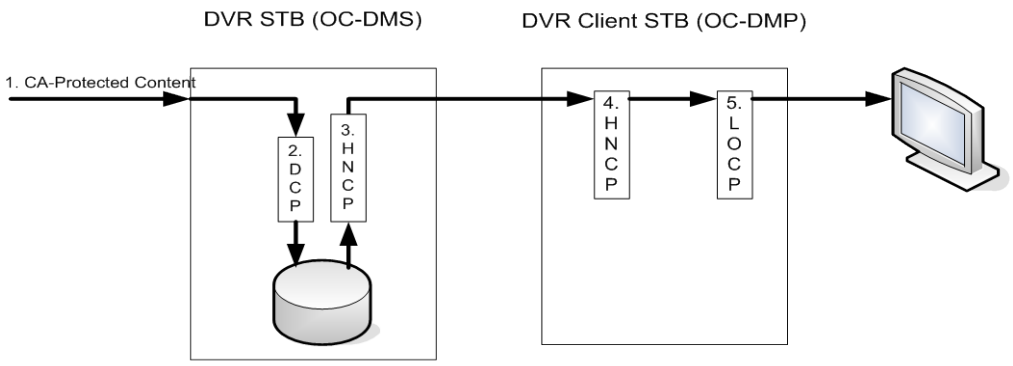

Figure 1 - Example of Content Protection

The steps shown in Figure 1 are described below:

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

Step 2. The MSO Content that is to be recorded 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. If an OC-DMP or OC-DMS request streaming of the MSO Recorded Content, 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. For Digital Output, 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.

When content streaming is initiated by an OC-DMP or OC-DMR, 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

When the OC-DMS supports multiple content protection systems for the same content binary, a res element indicating support for each content protection system is listed in a single CDS content item (rather than multiple CDS content items 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 Content traversing across the home network using an approved HNCP technology, as indicated by a res@protocolInfo property in the CDS object.

If the MSO 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]).

For streaming of MSO live content or in-progress recordings, the HNIMP OC-DMS SHALL always apply DTCP-IP Protected Frame encapsulation for the content irrespective of the Copy Control Information (CCI) values for the content sent from the CableCARD to the Host and SHALL apply encryption based on the CCI of the content. See [CCCP] for definition of CCI bit assignments for transmission from CableCARD to Host.

For streaming of completed recordings that contain any content identified as restricted based on CCI values, the HNIMP OC-DMS SHALL apply DTCP-IP encapsulation for the streamed content and apply encryption based on

the CCI values of the content. If a recording has multiple CCI values, the HNIMP OC-DMS SHALL apply DTCP-IP encapsulation and encryption according to the CCI associated with the content at the media time being streamed. For streaming of completed recordings whose E-EMI value is copy-free without EPN assertion, the HNIMP OC-DMS SHALL NOT apply DTCP-IP encapsulation.

When streaming DTCP-IP encapsulated content, 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]. This requirement is compliant with [DTCP-IP] section V1SE.10.2.2.

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 Network Authorization Handler

The Network Authorization Handler (NAH) is an MSO privileged application that can register to receive notification of content access requests and authorize any of the following activities (see NetAuthorizationHandler & NetAuthorizationHandler2 in [OCAP-HN]):

- Streaming of MSO Content (Recorded or Live)
- Copy of MSO Recorded Content
- Invocation of UPnP service actions

6.6.1 Registration

An MSO privileged application can choose to register as the NAH in order to be notified by the HNIMP OC-DMS if streaming or copy of MSO Content is requested to be started. In addition, the MSO privileged application can choose to register as the NAH in order to be notified by the HNIMP OC-DMS if a specific UPnP service action (i.e., based on the action name) is received.

6.6.2 Un-registration

Once an NAH is registered with HNIMP OC-DMS, an MSO privileged application can unregister the NAH. Once an NAH is unregistered by calling the org.ocap.hn.security.NetSecurityManager.setAuthorizationHandler method and setting the NetAuthorizationHandler parameter to null, the access to the MSO Content is defaulted to the approved HNCP technology, as described in Sections 6.6.3 and 6.6.4 of this specification.

6.6.3 MSO Content

The HNIMP OC-DMS SHALL grant access to the MSO Content when the registered NAH grants access. If no NAH is registered, or if the NAH has not registered interest to receive notification when MSO content is accessed, then OC-DMS SHALL grant access to all MSO Content in accordance to the underlying approved HNCP protection.

The HNIMP OC-DMS notifies the NAH when a streaming or copy operation on an MSO Content has been terminated as defined by Section 6.8.

If no NAH is registered with HNIMP OC-DMS, or is registered but has not indicated interest in receiving notifications about transport messages, the HNIMP OC-DMS SHALL grant the request for streaming of MSO Content based on the approved HNCP technology, as described in Section 6.5 of this specification. Additionally, if no NAH is registered, a copy request is granted according to the CCI bits.

MSO Content streaming and copy requests SHALL NOT be processed by the HNIMP OC-DMS until the beginning of “normal operation”, as specified in Section 20.2.1.2, "Boot Process – CableCARD device present" of [OCAP]. This requirement guarantees that the NAH will have the opportunity to authorize any streaming and copy requests made to the HNIMP OC-DMS.

6.6.4 UPnP Actions

If an NAH has registered interest to receive notification of UPnP actions, then the HNIMP OC-DMS SHALL notify the NAH when a requested UPnP service action is invoked. The HNIMP OC-DMS SHALL grant access to the UPnP service invocation when the registered NAH grants access.

If no NAH is registered, or if the NAH has not registered interest to receive notification of UPnP actions, then the OC-DMS SHALL grant access to all UPnP service actions.

UPnP action requests SHALL NOT be processed by the HNIMP OC-DMS until the beginning of "normal operation", as specified in Section 20.2.1.2, "Boot Process – CableCARD device present" of [OCAP]. This requirement guarantees that the NAH will have the opportunity to authorize any UPnP action requests made to the HNIMP OC-DMS.

6.7 Start of Content Streaming or Copy

An OC-DMP can stream MSO Content and a DLNA device can stream or copy MSO content from an OC-DMS using various transport protocols such as HTTP or RTP/RTSP, based on the protocol info indicated in the content item. This section describes OC-DMS requirements for identifying first transport request for HTTP and RTP/RTSP.

When an NAH is registered with the notifyTransportRequests parameter set to false [OCAP-HN], the OC-DMS notifies the registered NAH upon the receipt of the first transport request for streaming or copy of MSO Content from an OC-DMP as specified in [HNP].

6.7.1 HTTP Protocol

If an OC-DMP uses HTTP protocol to stream or copy MSO 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 no HTTP request was previously sent for the same content item from the same requesting device (as identified by the content URI or IP address of the requesting device), and if the stream has not been terminated previously as described by Section 6.8.
- If an 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 message is the first request and a ConnectionID was not already generated as a result of the CM::PrepareForConnection() action, the HNIMP OC-DMS SHALL generate a ConnectionID and populate that in the scid.dlna.org header in the HTTP response.

6.7.2 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.

6.7.3 Explanation of Authorization by NAH

Figure 2 and Figure 3 show an example scenario diagram of interaction between an OC-DMP/DLNA Premium DMP device and OC-DMS device for the MSO Authorization Process.

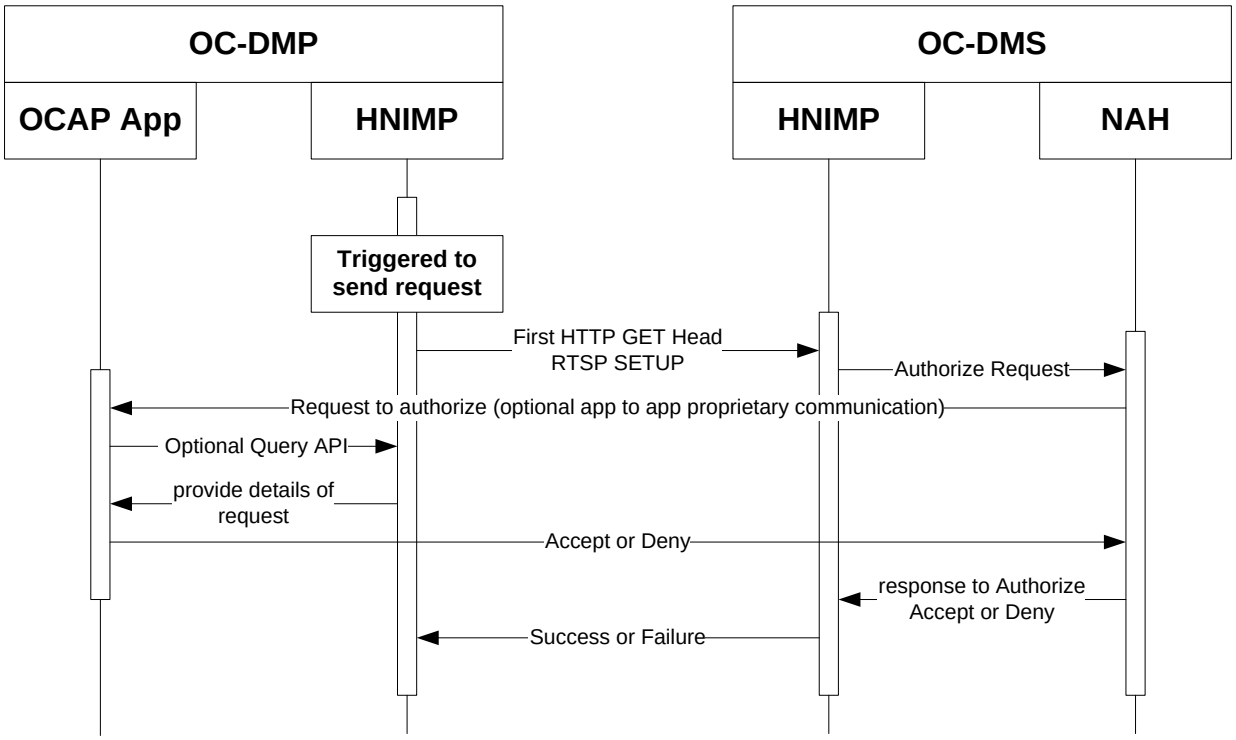

Figure 2 - Authorization Trigger Example

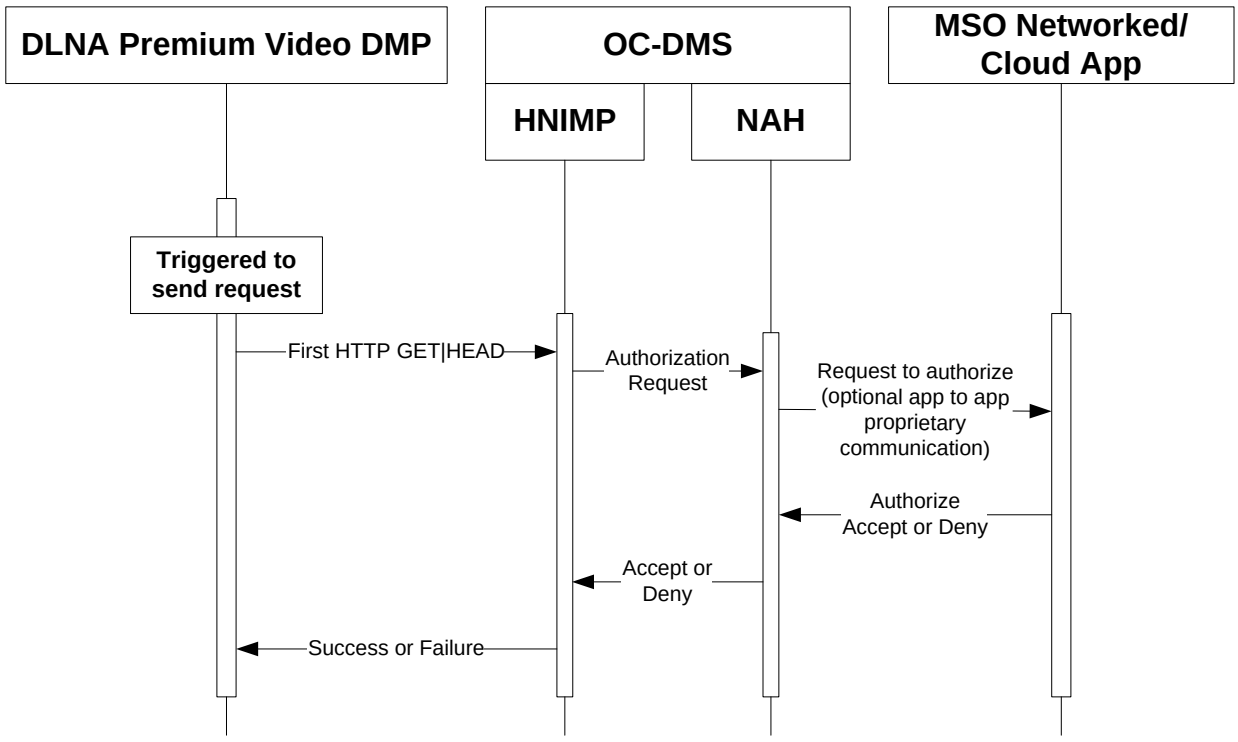

Figure 3 - Authorize Using Network or Cloud

The steps shown in Figure 2 are described below:

Step 1. A trigger occurs on the OC-DMP/DLNA Premium DMP to request MSO Content.

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

Step 3. The HNIMP OC-DMS invokes notifyActivityStart if an NAH is registered; otherwise it grants access according to the approved HNCP technology.

Step 4. Optionally, OC-DMS NAH (through a proprietary mechanism) communicates with either an application on OC-DMP or, in the case of a DLNA Premium DMP, an application on the network to see if the device and/or the request 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 NAH on OC-DMP and OC-DMS, the NAH, or other mechanisms determined by NAH on the OC-DMS, determines whether the request is granted or denied.

Step 8. The OC-DMS NAH 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 granted to the device. If the request is denied, the streaming of the MSO Recorded Content cannot be granted.

6.8 Termination of Content Streaming or Copy

The HNIMP OC-DMS notifies the registered NAH when an OC-DMS stops the playback or copy of the MSO Content. The streaming or copy operation of the content can be stopped either implicitly or explicitly, as described below.

6.8.1 Implicit Termination of Content Streaming or Copy

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

- HTTP: For a period of time as defined by [DLNA vol 1] for HTTP inactivity timeout, if no HTTP request has arrived for the ContentItem from a requesting device (as determined by the IP address), the OC-DMS SHALL consider the content streaming or copy operation to be terminated.
- RTSP: When the OC-DMS receives a RTSP::TEARDOWN message for a streaming or copy session established earlier, the OC-DMS SHALL consider the content streaming or copy operation to be terminated.

In addition, the OC_DMS SHALL consider a content streaming or copy operation 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 pass the activity identifier to the notifyActivityEnd method that was returned from the corresponding call to the notifyActivityStart method.

6.8.2 Explicit Termination of Content Streaming or Copy

Explicit termination of a Content Streaming or Copy request is accomplished by invocation of CM::ConnectionComplete(). If the NAH is registered for the CM::ConnectionComplete() action, OC-DMS notifies the NAH upon receipt of this action as required in 6.9.

6.8.3 MSO Content Streaming Termination Process Example

Figure 4 depicts an example scenario diagram of interaction between an OC-DMP and an OC-DMS for the MSO Termination Process.

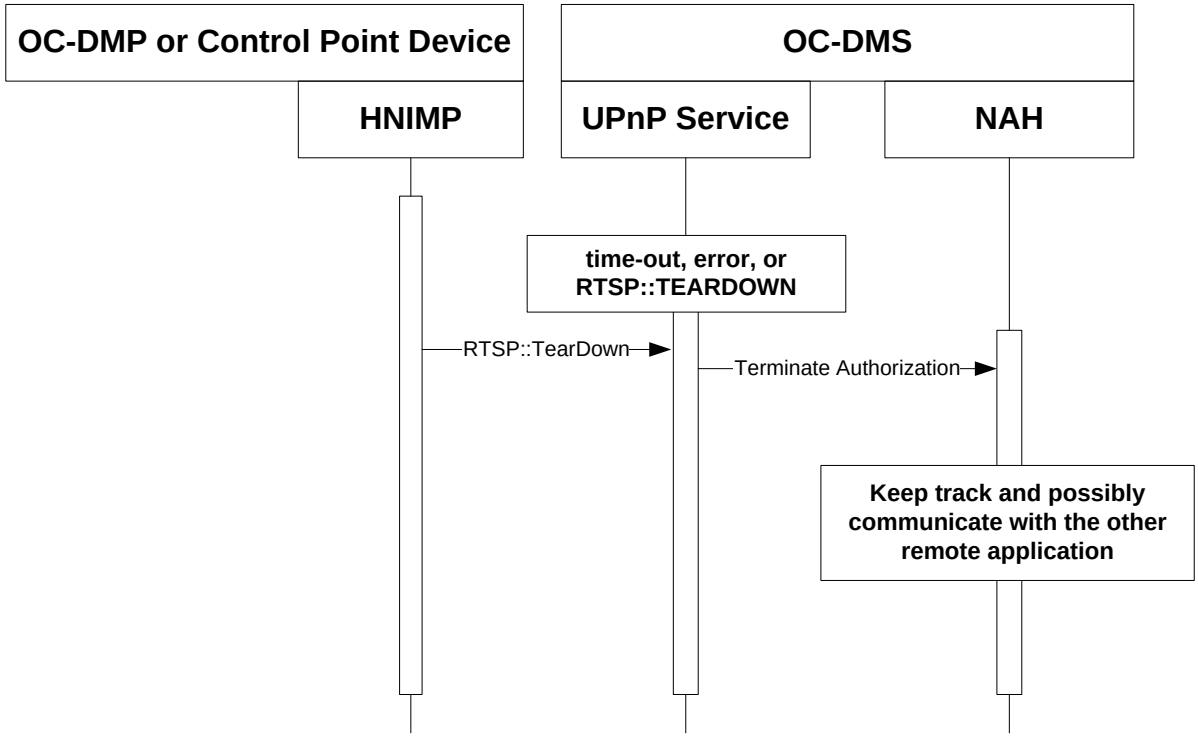

Figure 4 - Termination Trigger Example

The steps shown in Figure 4 are described below:

Step 1. Either the OC-DMP invokes an action to cause the OC-DMS to terminate the steaming session or a time-out occurs. Three cases cause the termination of a streaming session: 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 NAH notifyActivityEnd method if an NAH is still registered.

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

6.9 UPnP Service actions

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

6.10 Revocation

An NAH may revoke the authorization for a streaming or copy request in the middle of the streaming or copy operation. When this occurs, the NAH invokes the org.ocap.hn.security.NetSecurityManager.revokeAuthorization method to notify the HNIMP OC-DMS that it can no longer stream the request arriving from this device for this content item.

When the org.ocap.hn.security.NetSecurityManager.revokeAuthorization method is called, the OC-DMS SHALL stop streaming or copy operation of the content to the OC-DMP or OC-DMR requesting the content for which the authorization has been revoked.

6.11 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 NAH, using org.ocap.hn.security.NetSecurityManager.setNetworkPassword and org.ocap.hn.security.NetSecurityManager.getNetworkPassword APIs, respectively.

6.12 Requirements for Copy Support

As specified in [HNP], an OC-DMS HNIMP optionally supports the ability for an external DLNA device to copy MSO recorded content from the OC-DMS. The subsequent sections describe OC-DMS content security requirements to support this scenario.

6.12.1 DLNA DTCP-DIS Compliance for Copy Support

If an OC-DMS supports Copy functionality for copy controlled content, the OC-DMS SHALL comply with all the guidelines identified for DLNA DMS Device class in DLNA DTCP-DIS Guidelines [DLNA vol 4] for copy functionality applicable for Download System Usage. This covers the scenario of a DLNA device initiating download of content from OC-DMS to the DLNA device.

6.12.2 Media Management

The OC-DMS SHALL set DIS-DTCP-copy flag, defined in [DLNA vol 4], for MSO Recorded Content items according to the Copy Control Information (CCI) Encryption Mode Indicator (EMI) values for a content item as specified below. See [CCCP] for definitions of CCI and EMI.

Table 1 - Mapping of CCI Values to DIS-DTCP flags

CCI EMI Value	DIS-DTCP-copy flag
Copy Free	True
Copy Never	False
No More Copies	False
Copy One Generation	True

6.12.3 Copy Authorization

The OC-DMS SHALL comply with the DIS-DTCP-copy flag prior to allowing the copy operations by a client. If the DIS-DTCP-copy flag prohibits a content item from being copied, the OC-DMS SHALL return HTTP status code 403 (Forbidden) in the HTTP response to the GET request.

6.13 MP4 Containers and Embedded Copy Control Information

When MSO content is encapsulated using MPEG-4 (MP4) containers, there is no place holder for embedded copy control information.

The copy control information in this case is indicated using the Extended Encryption Mode Indicator (E-EMI) field of the Protected Content Packet (PCP) Header. The following requirements must be satisfied:

1. HNIMP OC-DMS and HNIMP OC-DMP SHALL support PCP-UR. The HNIMP OC-DMS and HNIMP OC-DMP will indicate support for PCP-UR using the DTCP CAPABILITY_REQ subfunction (Section: AKE_ID dependent field in [DTCP]). If the HNIMP OC-DMP does not support PCP-UR capability, content protection cannot be supported and the message exchange between HNIMP OC-DMS and HNIMP OC-DMP SHALL be terminated with an appropriate error status.
2. Once support for PCP-UR is asserted at both the HNIMP OC-DMS and HNIMP OC-DMP, DTCP-IP message exchange successfully completes AKE and generation of Content Key ([DTCP]).

3. When protected content is sent from the HNIMP OC-DMS to the HNIMP OC-DMP, PCP headers in the corresponding packets SHALL be set as described in [DTCP-IP] (Section: PCP-UR field).
4. The E-EMI (Encryption Mode Indicator in [DTCP-IP]) SHALL be set to match the copy control information of the corresponding MSO content.

6.14 Adaptive Streaming Over HTTP

Figure 5 describes the message exchange sequence between the HNIMP OC-DMP and HNIMP OC-DMS devices when MSO content that requires HNCP is represented in a manifest file.

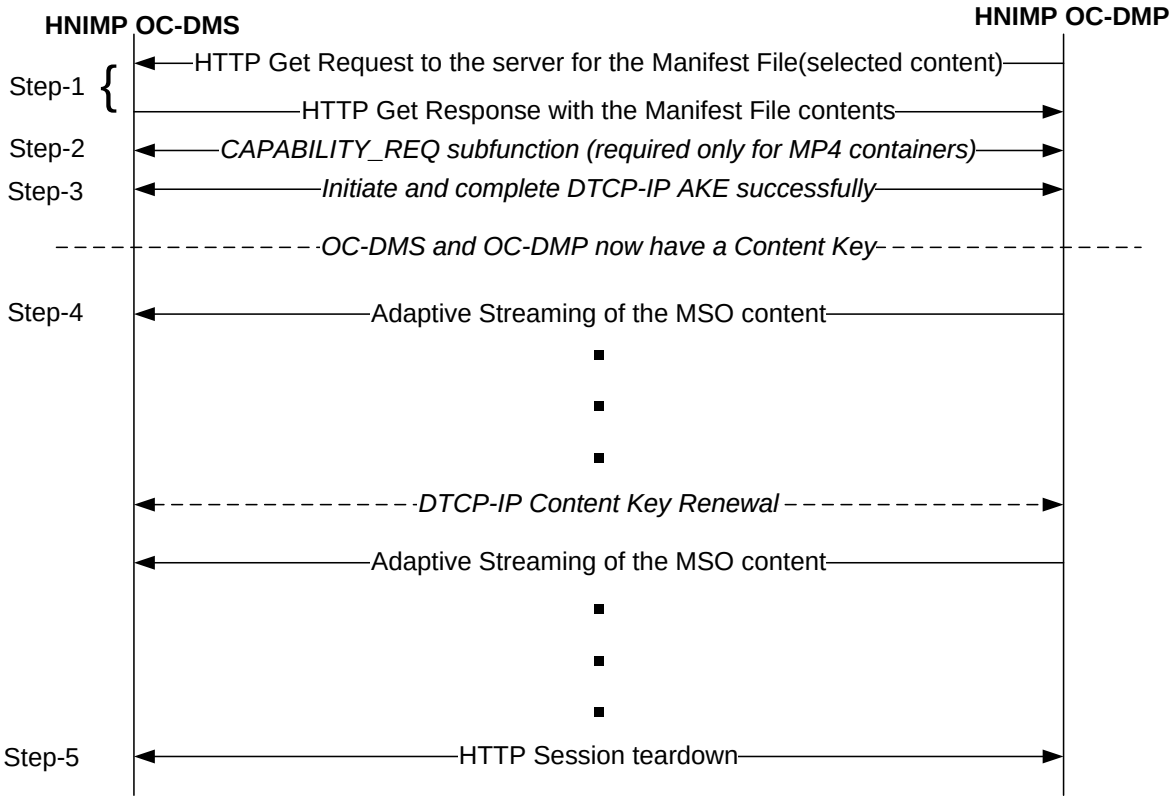

Figure 5 - Adaptive Streaming over HTTP

Step 1: As described in Section 6.6.3, when an HNIMP OC-DMP selects a MSO content and performs a HTTP GET for the corresponding manifest file, the NAH at the HNIMP OC-DMS gets notified and, based on the selected content, it will appropriately grant/deny access. If access is granted, then the manifest file that represents the MSO content is sent by HNIMP OC-DMS in the corresponding HTTP GET Response message to the HNIMP OC-DMP. The OC-DMP parses the received manifest and determines (a) if HNCP is required and (b) the format used to encapsulate the MSO content, namely MPEG2-TS, MP4 or fragmented MP4 (fMP4)

Step 2: When HNCP is required for the selected MSO content and the MSO content is contained in MP4 or fMP4 format (AVC_TS_MP_HD_AC3_ISO), a DTCP-IP CAPABILITY_REQ is initiated between the HNIMP OC-DMP and HNIMP OC-DMS devices. See Section 6.13.

Step 3: On successful completion of Step 2, the DTCP-IP Authentication and Key Exchange procedure (Full Authentication in [DTCP]) is initiated by the HNIMP OC-DMP. On successful completion of this step, the HNIMP OC-DMS and HNIMP OC-DMP derive a DTCP-IP Content Key that is used to encrypt the MSO content sent from the OC-DMS and decrypt the received content at the HNIMP OC-DMP.

Step 4: Adaptive streaming of the selected MSO content to the HNIMP OC-DMP starts and continues until one of the conditions described in Sections 6.8 or 6.10 is satisfied.

Step 5: The HNIMP OC-DMP or HNIMP OC-DMS terminates the adaptive streaming session at any time by tearing down the corresponding HTTP connection.

Appendix I Revision History

The following ECN was 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

The following ECN was incorporated into version I03 of this specification:

EC Identifier	Accepted Date	Title of EC
HN-SEC-N-10.1610-4	1/12/12	Add Copy and Live Streaming to HN Security Specification

The following ECN was incorporated into version I04 of this specification:

EC Identifier	Accepted Date	Title of EC
HN-SEC-N-12.1781-2	5/31/12	Authorization of HTTP Streaming Request from DLNA devices

The following ECNs were incorporated into version I05 of this specification:

EC Identifier	Author	Accepted Date	Title of EC
HN-SEC-N-13.1814-1	Venkatesan	4/18/13	HNP Enabling DTCP-IP link protection for content streamed using HTTP Adaptive Streaming
HN-SEC-N-13.1827-1	Millard	4/18/13	NetAuthorizationHandler Registration Clarification