

Superseded by a later version of this document.

OpenCable™ Specifications

OpenCable Unidirectional Receiver

OC-SP-OCUR-I01-060109

ISSUED

Notice

This OpenCable specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

© Copyright 2005-2006 Cable Television Laboratories, Inc.
All rights reserved.

Document Status Sheet

Document Control Number:	OC-SP-OCUR-I01-060109			
Document Title:	OpenCable Unidirectional Receiver			
Revision History:	D01 – Released June 2, 2005 D02 – Released November 18, 2005 I01 – Released January 9, 2006			
Date:	January 09, 2006			
Status:	Work in Progress	Draft	Issued	Closed
Distribution Restrictions:	Author Only	CL/Member	CL/Member/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:

DOCSIS®, eDOCSIS™, PacketCable™, CableHome®, CableOffice™, OpenCable™, CableCARD™, and CableLabs® are trademarks of Cable Television Laboratories, Inc.

Contents

1	INTRODUCTION	1
1.1	OpenCable Overview	1
1.2	OpenCable Unidirectional Cable Receiver (OCUR) Overview.....	2
1.3	Compliance Notation	3
2	REFERENCES	4
2.1	Normative References	4
2.2	Informative References.....	5
2.3	Reference Acquisition	5
3	TERMS AND DEFINITIONS.....	7
4	ABBREVIATIONS AND ACRONYMS	8
5	OVERVIEW OF CORE SERVICES AND FUNCTIONALITIES	10
5.1	OCUR components	10
5.1.1	Core Services (Informative).....	11
5.1.2	Core Functions and Features (Informative).....	11
5.2	General Compliance (Normative).....	11
6	SECURITY	13
6.1	Conditional Access	13
6.2	Certificate Storage and Management	13
6.3	Analog Program Copy Protection.....	13
6.4	Digital Program Copy Protection	13
6.5	DRI Content Protection.....	13
6.6	HMS Association Recording	13
7	UNIDIRECTIONAL PHYSICAL LAYER CHARACTERISTICS.....	15
7.1	RF Interface.....	15
7.1.1	Maximum Individual Carrier Amplitude	15
7.2	Communication Channels	15
7.2.1	Forward Application Transport (FAT) Channel	15
7.2.2	NTSC Channels.....	15
7.2.3	CA Signaling on Forward Data Channel.....	16
7.3	Physical Layer Specifications.....	16
7.3.1	In-Band Downstream Channel, FDC Characteristics and RF Performance.....	16
8	CARD INTERFACE.....	21
8.1	OCUR Functionality with Unscrambled Content	21
8.2	OCUR Functionality without a Card	21
8.3	Man Machine Interface (MMI) Support.....	21
8.4	Software Download	22
8.5	Digital Receiver Interface (DRI) Output	22

9 VIDEO	23
9.1 Analog Video	23
9.2 Digital Video.....	23
9.2.1 MPEG-2 Transport	23
9.2.2 FAT Delivered Service/System Information.....	23
9.2.3 Service/System Information provided by Card	23
9.2.4 Digital Television (DTV) Closed Captioning	23
9.2.5 Digital Television (DTV) Content Advisory Information	23
9.2.6 Digital Television (DTV) Emergency Alert Service (EAS).....	25
10 OCUR POWERING STATES	26
Card Background Mode Power Management.....	26
11 OCUR DIAGNOSTICS	27
11.1 Memory Resources	27
11.2 Software Versions	27
11.3 Firmware Version (OCUR)	28
11.4 MAC Addresses.....	28
11.5 OCUR Network Addresses	28
11.6 Status of FDC.....	28
11.7 Status of FAT	28
11.8 Current Channel Status	29
11.9 DRM Pairing Message.....	29
12 MECHANICAL	30
ANNEX A OCUR-HMS CONTENT PROTECTION REQUIREMENTS	
(NORMATIVE).....	33
ANNEX B MECHANISM FOR DRM REVOCATION.....	37

Figures

Figure 1.2-1 - OpenCable OCUR Environment.....	2
Figure 1.2-2 - OpenCable Content Protection Transitions	3
Figure 5.1-1 - Block Diagram of the OCUR (Informative)	10

Tables

Table 6.6–1 - HMS Association Record	14
Table 7.3–1 - Analog and FAT Channel: RF Performance Parameters (0° - 40° C).....	16
Table 7.3–2 - FDC Channel: RF Performance Parameters (0° - 40° C)	18
Table 7.3–3 - Adjacent Channel Characteristics.....	19
Table 9.2–1 - Content advisory conversion table.....	24
Table 12–1 - Environmental / Mechanical Requirements	30
Table B–1 - Code File Naming	37
Table B–2 - Code File Structure.....	37
Table B–3 - PKCS #7 Signed Data	38
Table B–4 - SRM Structure	40
Table B–5 - Code File Structure.....	40

This page left blank intentionally.

1 INTRODUCTION

1.1 OpenCable Overview

The goal of the OpenCable specifications is to define the first of a new generation of host devices that are interoperable across cable systems in North America. Information is presented in this document in order to help define the range of capabilities and applications to be supported by an OpenCable Unidirectional Receiver (OCUR). Information on the OpenCable Project can be obtained from the OpenCable website at <http://www.opencable.com>.

The OpenCable specifications:

1. Provide for integrated environments for broadcast services (analog and digital) and real-time interactive multimedia services, including IP data services (program synchronous and asynchronous), IP voice communications, video telephony, and on-demand interactive applications. Multiple models of OpenCable Host Devices are expected to co-exist within any given system, allowing the network operator to offer various services.
2. Require openness and interoperability. OpenCable takes advantage of “open” computing and network architectures, wherever possible, to minimize costs and maximize the ability to include new technologies as they become available and affordable. “Open” is defined as adherence to an international standard, North American standard, or published *de facto* industry standard. In all cases, the acquisition of the necessary software, hardware, and intellectual properties will be achievable at fair and reasonable costs. All standard interfaces will be in the public domain or, if such technology standards are to be defined, they will be available for license at a fair and reasonable cost. Closed proprietary systems are to be avoided.
3. Require portability. Retail availability of cable navigation devices is required in compliance with the FCC’s 1996 Telecom Reform Act. The OpenCable system permits “point-of-deployment decisions” for network, security, and operator-programmed user interfaces to enable the anticipated variety of retail devices.
4. Define a renewable and replaceable core encryption system called the CableCARD™ device.
5. Provide cable Multiple System Operators (MSOs) the ability to inform the navigation device (Host) of the services (video, Internet, etc.) that are offered.
6. Present a migration path from uni-directional to bi-directional networks and from broadcast to real-time interactive applications. Media servers and the related hardware (e.g., disk storage, switch fabric, modulators) will support the incremental addition of the required components to preserve any existing investment while taking advantage of more cost-effective solutions. In addition, the system software will be designed to scale efficiently as more interactive applications are added and service offerings expand. Of particular note are “authentication” and “name” services, database services, fault tolerance, and recovery mechanisms.
7. Allow efficient application and network design by:
 - Improving quality of service and/or reducing the bit rate of a digital stream through improved compression and transmission technologies; for example, by using improved MPEG-2 encoders and higher constellation digital modulation techniques.
 - Optimizing the use of network capacity. During the broadcast applications phase, bandwidth is allocated to accommodate broadcast digital program streams. As systems migrate to real-time interactive applications, the system will make efficient use of the network resources by dynamically allocating bandwidth.
 - Developing applications designed to use network resources efficiently, varying their behavior according to the network’s resource availability.
 - Minimizing the network resources required when the consumer “turns on” the terminal device.

8. Maximize compatibility with existing and/or newly-installed operational and customer support systems. All interfaces developed specifically for this effort will be integrated into the current and/or newly-installed billing support systems.
9. Co-exist with the embedded base of existing set-top devices.

1.2 OpenCable Unidirectional Cable Receiver (OCUR) Overview

This document describes the requirements for a unidirectional receiver (OCUR) Host profile.

The OCUR corresponds to a digital cable receiver with a tuner, a Card interface and an IP interface. It is intended to enable multi-user, multi-room scenarios where multiple OCURs can provide digital cable audio-visual programming over an IP connection to a Home Media Server (HMS) as shown in Figure 1.2-1.

REQ1539 The OCUR is connected to the home media server through the Digital Receiver Interface. The OCUR SHALL output content only on the DRI; no other analog or digital outputs are permitted.

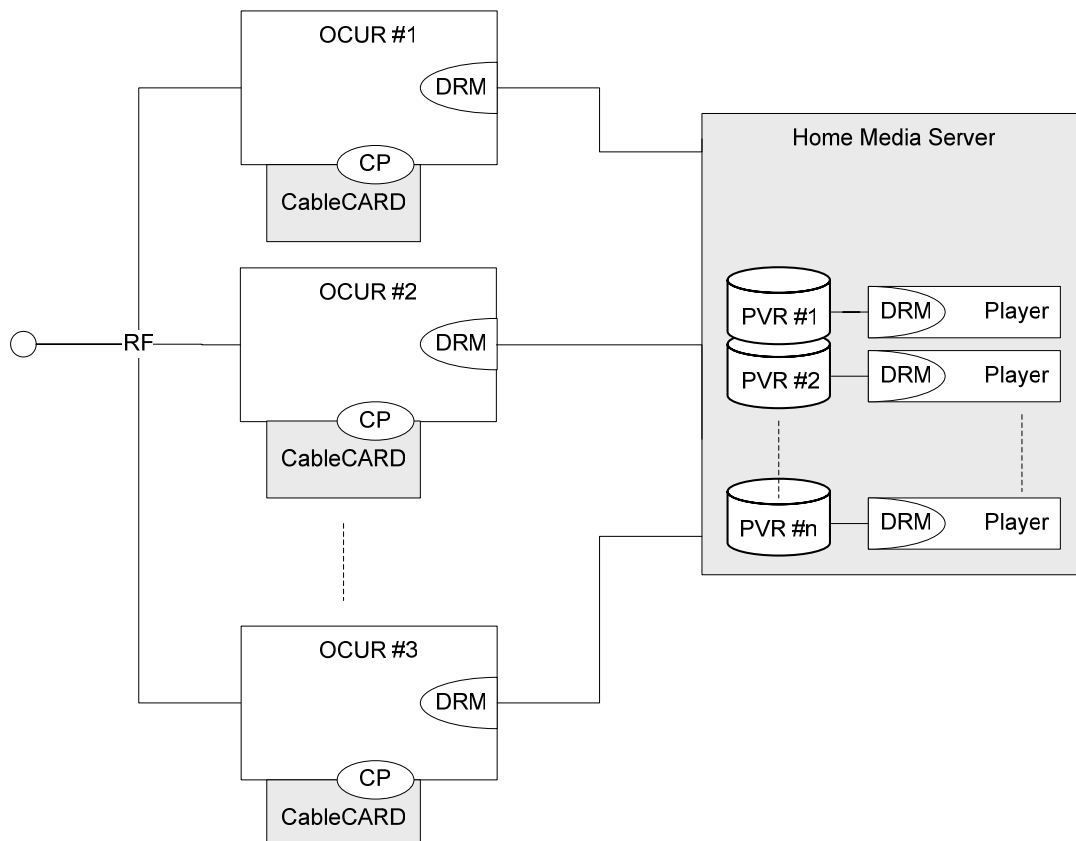


Figure 1.2-1 - OpenCable OCUR Environment

The overall protection of the cable audio-visual programming distribution across the home network is achieved through the means of a CableLabs-approved Digital Rights Management (DRM) system. All approved DRM systems need proximity control.

The OpenCable OCUR creates another content protection transition, similar to the CA-decryption/OpenCable Copy Protection encryption done within the Card, as defined in the OpenCable Digital Receiver Interface Specification [DRI]. The OCUR removes the OpenCable Copy Protection encryption, which protects the interface between the Card and any OpenCable Host device, and replaces it with a DRM

protection that provides a layer of encryption at the content level persistent until the authorized consumption of that service.

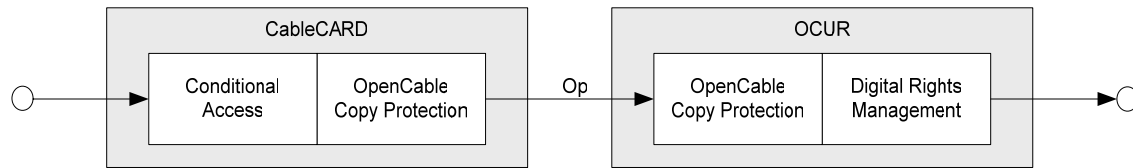


Figure 1.2-2 - OpenCable Content Protection Transitions

The OpenCable OCUR securely bridges the OpenCable Copy Protection signaling to the Digital Rights Management system by exporting and enforcing the encoding rules associated to the service, as defined by the OpenCable Copy Protection Specification [CCCP].

The goals and objectives of the OCUR are:

- To receive non-scrambled analog and digital services.
- To be sold through retail channels directly to the customer.
- To receive digital premium (scrambled) cable services using a CableLabs qualified Card.
- To enable a multi-room, multi-user home media server scenario.
- To bridge the OpenCable Copy Protection mechanism with any CableLabs-approved Digital Right Management system.

Information on the OpenCable Project can be obtained from the OpenCable website at <http://www.opencable.com/>, and information on the DOCSIS specifications can be found at the DOCSIS web site at <http://www.cablemodem.com/>.

1.3 Compliance Notation

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

“SHALL”	This word or the adjective “REQUIRED” 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 or the adjective “RECOMMENDED” 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 or the adjective “OPTIONAL” 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

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

- [A/52A] ATSC A/52A: Digital Audio Compression Standard.
- [A/53C] ATSC A/53C with Amendment 1: ATSC Digital Television Standard.
- [A/65B] ATSC A/65B: Program and System Information Protocol for Terrestrial Broadcast and Cable (Revision B).
- [CEA-542-B] EIA/CEA-542-B: Cable Television Channel Identification Plan.
- [CEA-608] CEA-608-C: Recommended Practice for Line 21 Data Service.
- [CEA-708] CEA-708-B: Digital Television (DTV) Closed Captioning.
- [47CFR15] 47CFR15: Radio Frequency Devices, Class B.
- [47CFR76] 47CFR76: Cable Television Service.
- [CCIF] OC-SP-CCIF2.0-IF-I03-051117: OpenCable™ CableCARD™ Interface 2.0 Specification, November 17, 2005, Cable Television Laboratories, Inc.
- [CCCP] OC-SP-CCCP2.0-I02-050708: OpenCable CableCARD™ Copy Protection 2.0 Specification, July 8, 2005, Cable Television Laboratories, Inc.
- [EIA-679-C] EIA-679-B C (Part B): National Renewable Security Standard, March 2000.
- [IEC 61880] IEC 61880 Video systems (525/60) – Video and accompanied data using the vertical blanking interval – Analogue interface, First Edition, 1998-01".
- [ISO 13818-1] ISO/IEC 13818-1, 2000: Information technology—Generic coding of moving pictures and associated audio (MPEG): Systems.
- [ISO 13818-2] ISO/IEC 13818-2, 2000: Information technology—Generic coding of moving pictures and associated audio (MPEG): Video.
- [ISO-13818-3] Information technology -- Generic coding of moving pictures and associated audio information -- Part 3: Audio
- [OC-SEC] OC-SP-SEC-I05-040831: OpenCable System Security Specification, August 31, 2004, Cable Television Laboratories, Inc.
- [SCTE 01] ANSI/SCTE 01, 1996: (formerly IPS-SP-400): Recommended “F” Port (Female) Specification.
- [SCTE 07] ANSI/SCTE 07, 2000: Digital Video Transmission Standard for Cable Television.
- [SCTE 20] ANSI/SCTE 20, 2004: Standard Methods for Carriage of Closed Captions and Non-Real Time Sampled Video. Note: Non-Real Time Sampled Video support is “optional” for Host Devices.
- [SCTE 55-2] ANSI/SCTE 55-2, 2002: March 10, 2002, Digital Broadband Delivery System: Out-of-Band Transport - Part 2: Mode B.
- [SCTE 55-1] ANSI/SCTE 55-1, 2002: February 25, 2002, Digital Broadband Delivery System: Out-of-Band Transport - Part 1: Mode A.
- [SCTE 18] SCTE 18, 2002 (ANSI-J-STD-042-2002): Emergency Alert Message for Cable.

- [SCTE 65] ANSI/SCTE 65, 2002: Service Information Delivered Out-of-Band for Digital Cable Television.
- [SCTE 54] ANSI/SCTE 54, 2004: Digital Video Service Multiplex and Transport System Standard for Cable Television.
- [SCTE 40] ANSI/SCTE 40, 2004: Digital Cable Network Interface Standard.
- [SCTE 43] ANSI/SCTE 43, 2003: Digital Video Systems Characteristics Standard for Cable Television.
- [SCTE 21] ANSI/SCTE 21, 2001 (formerly DVS 053): Standard for Carriage of NTSC VBI Data in Cable Digital Transport Streams.
- [CEA-23] CEA-23-A: RF Interface Specification for Television Receiving and Cable Television Systems.
- [Macrovision] Specifications of the Macrovision Copy Protection Process for STB/IRD Products Revision 7.1.S1, (October 1, 1999).
- [CEA-766-A] CEA-766-A: U.S. Regional Rating Table (RRT) and Content Advisory Descriptor for Transport of Content Advisory Information Using ATSC A/65 Program and System Information Protocol (PSIP).
- [DRI] OC-SP-DRI-I01-060109: OpenCable™ Digital Receiver Interface Protocol Specification, January 9, 2006, Cable Television Laboratories, Inc.
- [PKCS #7] Public Key Cryptographic Standard #7. The Cryptographic Message Syntax Standard from RSA Laboratories

2.2 Informative References

- [TIA-250-C] EIA/TIA-250-C: Electrical Performance Standards for Television Relay Facilities.
- [CHILA] CableLabs CableCARD-Host Interface License Agreement.
- [DTCP] [DTCP Specification] Digital Transmission Content Protection Specification: Volume 1 (Informational Version), Revision 1.4, February 2005.
- [DTCP Lic] Digital Transmission Protection License Agreement, May 2005.
- [HDCP Lic] HDCP License Agreement, August 21, 2005.
- [HDCP Spec] HDCP License Agreement, August 21, 2005."
- [MIL-C-39012] MIL-C-39012: General Specifications for Connectors, Coaxial, Radio Frequency.
- [OC-CD] OC-SP-CD-IF-I08-040831: OpenCable Common Download Specification, August 31, 2004, Cable Television Laboratories, Inc.
- [VCPS Spec] Video Content Protection System for the DVD+R/+RW Video Recording Format: System Description, Version 1.3, July 2005.
- [VCPS Lic] Video Content Protection System Agreement, Version 1.3g, 4-2005.

2.3 Reference Acquisition

CableLabs Specifications:

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone 303-661-9100; Fax 303-661-9199; Internet: <http://www.cablelabs.com/>

SCTE/DVS Standards:

- SCTE - Society of Cable Telecommunications Engineers Inc., 140 Philips Road, Exton, PA 19341: Phone: 610-363-6888 / 800-542-5040; Fax: 610-363-5898; <http://www.scte.org/>

ISO/IEC Standards:

- ISO Central Secretariat: International Organization for Standardization (ISO), 1, rue de Varembé, Case postale 56, CH-1211 Geneva 20, Switzerland; Internet: <http://www.iso.ch/>

Macrovision Copy Protection:

- Macrovision Corporation, 2830 De La Cruz Boulevard, Santa Clara, CA 95050 ;
<http://www.macrovision>.

ATSC Standards:

- Advanced Television Systems Committee (ATSC), 1750 K Street N.W., Suite 1200, Washington, DC, 20006; Phone 202 872 9160; Fax 202-828-3131; Internet <http://www.atsc.org>

3 TERMS AND DEFINITIONS

This document uses the following terms:

OpenCable Unidirectional Receiver	A cable receiver that does not include a return data channel or a user interface and is compatible with the profile defined by this specification.
Card	A PCMCIA card distributed by cable providers and inserted into a Host device to enable reception of premium services without a separate cable receiver, also called CableCARD Device and “Point of Deployment” (POD) module.
CA-Scrambling	Video that has been scrambled by the cable operator.
Digital Receiver Interface	A content transport and Command & Control protocol between the Unidirectional Cable Receiver and the Home Media Server implemented over an IP interface.
Digital Rights Management	A technology that controls access to services by preventing the unauthorized sharing or copying of digital content, and associating the use or viewing of content to specific individuals, operating systems, or hardware.
DRIT	Digital Receiver Interface Transcoder. OCURs are a version of DRITs.
Home Media Server	A Home Media Server is a system that employs one or more OCURs to securely store, distribute and/or render cable audio-visual programming services.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

ACCI	Aggregate Content Control Instructions
AES	Advanced Encryption System
APS	Analog Protection System
CA	Conditional Access
CCI	Copy Control Information
CCCP	CableCARD Copy Protection
CGMS-A	Copy Generation Management System – Analog
DES	Data Encryption Standard
DRI	Digital Receiver Interface
DRM	Digital Rights Management
DVI	Digital Video Interface
DVS	Digital Video Subcommittee
EAS	Emergency Alert System
EPG	Electronic Program Guide
EPN	Encryption Plus Non-assertion
FAT Channel	Forward Application Transport Channel
FDC	Forward Data Channel
HMS	Home Media Server
IP	Internet Protocol
MAC	Media Access Control
MMI	Man Machine Interface
MPEG	Moving Picture Experts Group
MPTS	Multiple Program Transport Stream – as defined in ISO13818-1
NTSC	National Television System Committee
OCUR	OpenCable Unidirectional Receiver
CONTROL STREAM	CA data received in a Forward Data Channel. (Sometimes referred to the OOB)

PAT	Program Association Table
PMT	Program Map Table
RF	Radio Frequency
SCTE	Society of Cable Telecommunications Engineers
SI	System Information
SRM	A System Renewability Message that is used to revoke an instance of DRM implementation. **Note this SRM should not be confused with the SRM defined in the HDCP and DTCP specification.
SPTS	Single Program Transport Stream – as defined in ISO13818-1
STT	System Time Table
VCPS	Video Content Protection System
VGA	Video Graphics Adaptor
XDS	Extended Data Service

5 OVERVIEW OF CORE SERVICES AND FUNCTIONALITIES

5.1 OCUR components

This section describes the core services that OCURs shall support as well as the core functions required to implement those services. A block diagram of the OCUR components is shown in Figure 5.1-1.

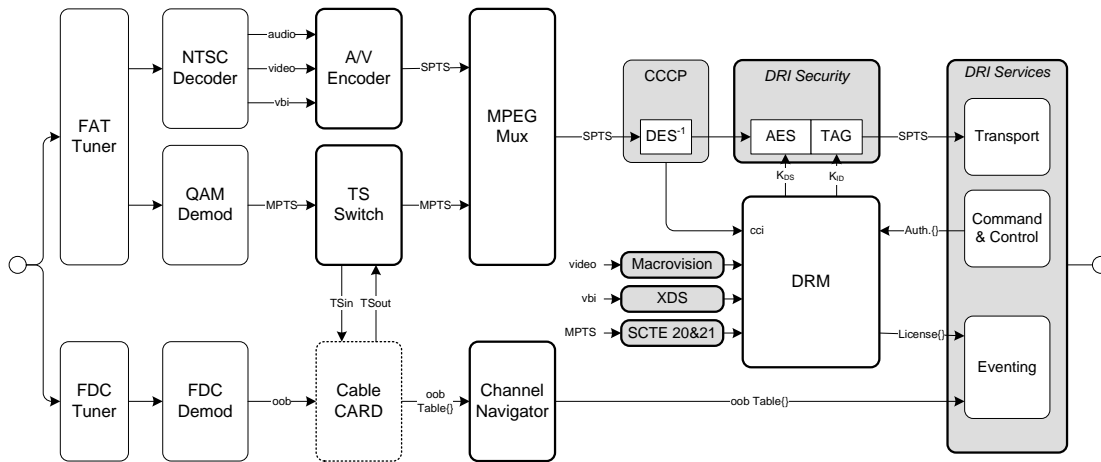


Figure 5.1-1 - Block Diagram of the OCUR (Informative)

Operational and security components are described below:

- **A/V Encoder** – This block receives an NTSC signal and performs an audio/video compression operation, as defined by this specification.
- **MPEG Mux** – This block creates an MPEG-2 Single Program Transport Stream (SPTS) with consistent PSI/SI that complies with [ISO 13818-1].
 1. If the OCUR is tuned to a digital channel; this block positively filters the selected program and its associated tuning space information.
 2. If the OCUR is tuned to an analog channel; this block combines the audio and video components and creates a PAT and a PMT tables compliant with the cable channel map.
- **Channel Navigator** – This block receives channel map and emergency alert tables from the Card to provide the following services:
 1. Defines applicable tuning parameters for a DRI tune request based on virtual channel number.
 2. Defines applicable tuning parameters for a Card firmware upgrade request.
 3. Caches all Control Stream tables and forward them through the DRI connection upon request.
- **DRI Security** – This block defines a common scrambling mechanism for the DRI connection independently of the selected DRM system. Most DRM systems are based on the AES algorithm standardized by the U.S. National Institute of Standards and Technology (FIPS PUB 197).
- **CCCP** – This block performs the task of Card authentication, CP session key generation and Copy Control Information (CCI) management as defined per [CCCP]. It provides CCI parameters to the DRM block for selection of the appropriate license.
- **Macrovision** – This block extracts the Macrovision state of the NTSC signal and transfers the equivalent APS bits to the DRM block. These values never conflict with the CCCP CCI states, which are only provided while tuned to a digital channel.

- **XDS** – This block analyses line 21 - Field 1 and 2 of the NTSC VBI interval and extracts the CGMS-A bits. The DRM system is responsible for preserving these bits in order to re-insert them on the analog outputs. These values never conflict with the CCCP CCI states, which are only provided while tuned to a digital channel.
- **DRM** – This block performs the function of a CableLabs-approved DRM transmitter.
- **DRI Command & Control Service** – This block exposes all the controls and commands to discover, reserve and use the OCUR.
- **DRI Transport Service** – This block receives a DRM-protected SPTS from the DRI Security block. Every transport interval, it creates an RTP/UDP packet and sends it to HMS. Optional modes based on native isochronous channels of the digital bus are also permitted.
- **DRI Eventing Service** – This block sends asynchronously all OCUR events, such as the DRM licenses, the FDC channel map tables and the Card changes of status.

5.1.1 Core Services (Informative)

The following services can be provided by the Core Requirements for OCURs:

- Support of NTSC audio-visual programming (unscrambled) by encoding to an SPTS as defined by this specification
- Support of digital audio-visual programming utilizing MPEG-2 main profile @ main level and main profile @ high level video and Dolby AC-3 audio including broadcast (unscrambled), subscription-based (scrambled), music channels and other services.

5.1.2 Core Functions and Features (Informative)

The features and functions of the OCUR necessary to support the core services include the following:

- Input range of 54-864 MHz or greater, analog and digital (64/256 QAM) tuning and demodulation
- Closed Caption detection for NTSC audio-visual programming according to [CEA-608] and conversion to [SCTE 21] for transmission across the DRI output
- DRM content protection on DRI output [DRI]
- Emergency Alert System detection of [SCTE 18] for transmission on DRI output
- QPSK Control Stream receiver compliant with [SCTE 55-2] and [SCTE 55-1]
- Card digital interface (see OpenCable CableCARD™ Interface 2.0 Specification [CCIF]) in one or both S-Mode or M-Mode.
- OpenCable CableCARD Copy Protection 2.0 Specification [CCCP] in one or both S-Mode or M-Mode.

5.2 General Compliance (Normative)

Any features of an OCUR mandated by law or FCC regulation (e.g., Emergency Alert System, V-Chip) SHALL be supported in the Core Requirements for all OCURs.

- | | |
|------|---|
| REQ1 | The OCUR manufacturer SHALL confirm compliance with all applicable FCC rules and regulations as found in [47CFR15] and [47CFR76]. |
| REQ2 | The OCUR manufacturer SHALL confirm compliance with all applicable UL rules and regulations as found in Table 12-1 - Environmental / Mechanical Requirements. |

- REQ3 The OCUR SHALL comply with the specifications described in
- REQ3.1 Table 7.3–1 - Analog and FAT Channel: RF Performance Parameters (0° - 40° C)
 - REQ3.2 Table 7.3–2 - FDC Channel: RF Performance Parameters (0° - 40° C)
 - REQ3.3 Table 7.3–3 - Adjacent Channel Characteristics

6 SECURITY

This section describes requirements for copy protection of video programs, security of video streams, conditional access to video streams, and security of transmitted data.

6.1 Conditional Access

- REQ4 The OCUR SHALL utilize the Card to perform the following Conditional Access (CA) functions as defined in [CCCP]: CA decryption, authorization, entitlement and Copy Protection encryption. REQ5 The CA Functions SHALL be implemented in the Card and not in the OCUR. REQ6 If CA functionality is present in the OCUR, it SHALL be disabled under all circumstances, including the absence of a Card.
- REQ7 The OCUR SHALL implement all aspects of Copy Protection binding and key generation, according to [CCCP], locally except for presentation of the MMI.

6.2 Certificate Storage and Management

- REQ8 The OCUR SHALL store the various certificates and any associated private/public keys as defined in sections 5.8 Host and CableCARD Certificate Storage and Management, 6.1.2 CableLabs Code Verification Root CA Certificate, 6.1.3 CableLabs Code Verification CA Certificate and 6.1.6 CableLabs Application Code Verification CA Certificate of the OpenCable System Security Specification [OC-SEC].
- If the OCUR implements more than one CHI, the OCUR SHALL have and employ a unique OpenCable Host Certificate for each CHI.

6.3 Analog Program Copy Protection

- REQ9 The OCUR SHALL reset all analog copy protection status after a channel change.
- REQ10 The OCUR SHALL detect the analog copy protection status of the selected NTSC channel and protect it according to Annex A.

6.4 Digital Program Copy Protection

- REQ11 The OCUR SHALL implement one or both S-Mode or M-Mode as defined by OpenCable CableCARD Copy Protection 2.0 Specification [CCCP].
- REQ12 The OCUR SHALL NOT change the CCI value used to control content output except as instructed by the Card or when reset after a channel change.
- REQ13 The OCUR SHALL detect the digital copy protection status of the selected digital program and protect in accordance with Annex A.

6.5 DRI Content Protection

- REQ14 The OCUR SHALL permit output of content only under the effective protection of a CableLabs-approved DRM system, whose DrmUUID value is not listed in the Drm_revocation_list, in accordance with Annex B.

6.6 HMS Association Recording

- REQ15 The OCUR SHALL register in non-volatile memory the HMS Association parameters listed in Table 118H6.6-1 HMS Association Record for the latest sixteen DRM-paired HMS devices.

Table 6.6–1 - HMS Association Record

	Parameter	# of bits	Description
1	drm_guid	128	Global Unique Identifier for the DRM system
2	hms_association_id	160	HMS / OCUR unique association identifier provided by the DRM system
3	drm_pairing_time	64	UTC time of the latest successful DRM pairing operation based on STT received from Card.

REQ16 When the Card is present, the OCUR SHALL erase the HMS Association record that has the oldest `drm_pairing_time` if the maximum number of records have been filled and a new HMS device is successfully DRM-paired.

REQ17 When the Card is present, the OCUR SHALL update the `hms_pairing_time` parameter every time it pairs with a registered HMS.

7 UNIDIRECTIONAL PHYSICAL LAYER CHARACTERISTICS

7.1 RF Interface

REQ18 The mechanical and electrical interface between the cable plant and the OCUR SHALL be as defined in section 3 Mechanical and Electrical Interface of [CEA-23] with the additional requirements specified in the remainder of this document.

7.1.1 Maximum Individual Carrier Amplitude

REQ19 The OCUR SHALL be capable of meeting the FAT and FDC channel performance requirements in the presence of interfering signals where the maximum rms value of any individual interfering signal does not exceed the following limits (measured across 75Ω):

REQ19.1 0.5 Mhz to 42 MHz +42 dBmV

REQ19.2 42 Mhz to 52 MHz 0 dBmV

REQ19.3 52 Mhz to 54 MHz -17 dBmV

REQ19.4 The maximum rms value of any individual signal whose frequency exceeds 54 MHz is less than +20 dBmV across a 75 ohm terminating impedance measured at the input to the OCUR.

7.2 Communication Channels

REQ20 The OCUR SHALL have the following communication channels:

REQ20.1 Forward Application Transport (FAT) channels, which carry MPEG-2 Program Streams, or NTSC signals, which may contain closed caption data in the Vertical Blanking Interval

REQ20.2 Forward Data Channel (FDC)

7.2.1 Forward Application Transport (FAT) Channel

The forward application transport channel is a 64 or 256 Quadrature Amplitude Modulation (QAM) channel according to [SCTE 07] that transports approximately 27 or 39 megabits/second, respectively. The OCUR is instructed to tune to a particular FAT channel when a subscriber requests a service that requires transport on a FAT channel. FAT channels that are present on the cable plant will adhere to the STD, HRC or IRC frequency plans of [CEA-542-B] and can be located anywhere in the 54 to 864 MHz range.

REQ21 The OCUR SHALL receive signals that are compliant with [SCTE 07] for the transmission physical layer modulation, coding, synchronization, and Forward Error Correction and present the requested data stream on the DRI compliant with [DRI].

REQ22 The OCUR SHALL decode the Forward Application Transport channel over the range of input parameters as defined in Table 7.3-1 Analog and FAT Channel: RF Performance Parameters (0° - 40° C) and present the requested data stream on the DRI compliant with [DRI].

REQ23 The Forward Application Transport tuner SHALL have a frequency range of 54 to 864 MHz.

7.2.2 NTSC Channels

NTSC channels will adhere to the STD, HRC or IRC frequency plans of [CEA-542-B] and can be located anywhere in the 54 to 864 MHz range.

REQ24 The OCUR SHALL receive and present on the DRI compliant with [DRI] all existing unscrambled analog channels that meet the following conditions: NTSC RF AM-VSB modulated in accordance with FCC rules, adhering to one of the STD, HRC or IRC frequency plans of [CEA-542-B] and located in the 54 to 864 MHz range.

7.2.2.1 Vertical Blanking Interval

The Vertical Blanking Interval (VBI) contains data on line 21 of an analog television signal. During this period, the cable headend can insert VBI data signals on VBI line 21 for closed captioning. VBI data can be inserted within field 1, field 2, or both, on any analog channel operating in the 54 to 864 MHz range.

- REQ25 The OCUR SHALL detect closed captions, text mode data services, and extended data services data contained in line 21 of the VBI (field 1 and 2) of NTSC signals as defined by [CEA-608], and convert them into [SCTE 21] format and make available on the DRI connection [DRI].

7.2.3 CA Signaling on Forward Data Channel

7.2.3.1 Forward Data Channel

The FDC receiver RF front end provides the generic QPSK physical layer common to the OpenCable choices.

- REQ26 The OCUR SHALL be capable of receiving a CA Forward Data channel with parameters defined in [SCTE 55-1] and [SCTE 55-2] and passing the demodulated signal to the Card per [CCIF].
- REQ27 The OCUR SHALL receive and demodulate signals compliant with [SCTE 55-2] and [SCTE 55-1] for the FDC transmission physical layer modulation and differential coding and present the data stream on the Card interface with a bit error rate (BER) of 2.5e-06 or less.
- REQ28 The OCUR SHALL demodulate the Forward Data Channel over the range of input levels as defined in Table 7.3-2 - FDC Channel: RF Performance Parameters (0° - 40° C).
- REQ29 The Forward Data Channel tuner SHALL have a frequency range of 70 to 130 MHz and be able to tune any nominal carrier frequency defined in item 4 of Table 7.3-2 - FDC Channel: RF Performance Parameters (0° - 40° C) as directed by the Card.
- REQ30 The OCUR SHALL receive and demodulate digital QPSK FDC signals with a signal level that is ± 15 dBmV within the minimum channel spacing as specified in [SCTE 55-1] and [SCTE 55-2] and present the data stream on the Card interface with a bit error rate (BER) of 2.5e-06 or less.

7.3 Physical Layer Specifications

7.3.1 In-Band Downstream Channel, FDC Characteristics and RF Performance

- REQ31 The OCUR SHALL meet all performance requirements specified in Table 7.3-1- Analog and FAT Channel: RF Performance Parameters (0° - 40° C) and Table 7.3-2 - HMS Association Record while operating with the downstream transmission characteristics defined by [SCTE 40].
- REQ32 The OCUR SHALL use a female "F" connector meeting [SCTE 01] for the RF input.
- REQ33 The "F" connector for RF input on the OCUR SHALL have a "Cable In" label.

Table 7.3-1 - Analog and FAT Channel: RF Performance Parameters (0° - 40° C)

1.	RF Input Channel Bandwidth	6 MHz
2.	RF Input Tuning Range	54 MHz to 864 MHz IRC/HRC/Standard Channel Plans
3.	RF Input Return Loss	6 dB minimum over full tuning range
4.	RF Input Impedance	75 ohm unbalanced
5.	RF Input Level Range	Analog visual carrier(c) from 0 dBmV minimum to +15 dBmV maximum; Analog aural carrier from -10 to -17 dBc; Digital 64 QAM signal from -15 dBmV to +15 dBmV; Digital 256 QAM signal from -12 dBmV to +15 dBmV

6.	AFC Range	Better than ± 125 kHz or nominal tuning resolution of 62.5 kHz
7.	LO Leakage (Input EMC)	-37 dBmV over 54 MHz to 864 MHz
8.	Signal Leakage/RFI	Per [47CFR15]
9.	Group Delay Variation Tolerance	≤ 0.25 μ sec/MHz across the 6-MHz channel
10.	Phase Noise Tolerance	≤ -88 dB/Hz @ 10 kHz offset (relative to the center of QAM signal spectrum)
11.	Amplitude Ripple Tolerance: Digital channels Analog channels	≤ 5 dB p-p within the 6 MHz channel ≤ 4 dB p-p within the 6 MHz channel
12.	Microreflection Tolerance (assumes one dominant echo with max. specified amplitude in dB relative to the primary QAM signal)	-10 dB at < 0.5 μ sec -15 dB at < 1 μ sec -20 dB at < 1.5 μ sec -30 dB at < 4.5 μ sec Echoes > 4.5 μ sec (see Note 1)
13.	Burst Noise Tolerance	Not longer than 25 μ sec at 10 Hz repetition rate
14.	Image Rejection	Image response less than 60 dBc at final IF or baseband video output, 54 to 714 Mhz Image response less than 50 dBc at final IF or baseband video output, 714 to 860 Mhz 60dB standard to apply at 714 Mhz Two equal power CW signals, +15 dBmv $F_{\text{image}} = F_{\text{desired}} + 90$ Mhz
15.	Spurious Emissions, 5 – 864 MHz	< -37 dBmV

Table Notes:

1. *Micro-reflection longer than 4.5 microseconds rarely occur in conventional cable television systems. Moreover, very low-level micro-reflections (e.g., -40dB) longer than 4.5 microseconds cannot be measured reliably with readily available instruments. Studies on the subject of long Micro-reflections are continuing, which may result in quantifying this parameter at a future date.*

Table 7.3–2 - FDC Channel: RF Performance Parameters (0° - 40° C)

1.	Transmission Rate	1.544/3.088 Mbps [SCTE 55-2] 2.048 Mbps [SCTE 55-1]																		
2.	RF Input Channel Spacing	1.0/2.0 MHz [SCTE 55-2] 1.8 MHz [SCTE 55-1]																		
3.	RF Input Tuning Range	70 MHz to 130 MHz																		
4.	Nominal carrier frequency	Any integer multiple of 250 kHz between the minimum and maximum carrier frequencies, inclusive and the specific fixed frequency of 104.200 MHz.																		
5.	Frequency acquisition range	+/- 50 ppm																		
6.	RF Input level range	-15 to +15 dBmV rms (75 ohms) (See Note 1)																		
7.	Differential Encoding	The differential encoder SHALL accept bits (A, B) in sequence and generate phase changes as follows: <table> <tr> <th>A</th><th>B</th><th>Phase Change</th></tr> <tr> <td></td><td></td><td>default alternative</td></tr> <tr> <td>0</td><td>0</td><td>none none</td></tr> <tr> <td>0</td><td>1</td><td>+90 deg -90 deg</td></tr> <tr> <td>1</td><td>0</td><td>-90 deg +90 deg</td></tr> <tr> <td>1</td><td>1</td><td>180 deg 180 deg</td></tr> </table>	A	B	Phase Change			default alternative	0	0	none none	0	1	+90 deg -90 deg	1	0	-90 deg +90 deg	1	1	180 deg 180 deg
A	B	Phase Change																		
		default alternative																		
0	0	none none																		
0	1	+90 deg -90 deg																		
1	0	-90 deg +90 deg																		
1	1	180 deg 180 deg																		
10.	Group Delay variation tolerance	200 ns max in channel, measured over Nyquist bandwidth																		
11.	Channel Tune / Carrier acquisition time	< 500ms																		

7.3.1.1 RF Signal Levels and Adjacent Channel Characteristics**7.3.1.1.1 RF Signal Levels**

REQ34 The OCUR SHALL be capable of receiving an analog signal with a visual signal level that is within ± 3 dB of the visual signal level of any adjacent analog channel (within a 6 MHz nominal frequency separation as specified in [47CFR76].

To determine the adjacent channel characteristics between digital and analog signals, the following information is provided. The nominal relative carrier power levels for analog and digital signals are given by:

Analog channel:	0 dBc (reference level)
256 QAM FAT:	-5 \pm 2 dBc
QPSK FDC:	-8 \pm 5 dBc
64 QAM FAT:	-10 \pm 2 dBc

REQ35 The OCUR SHALL be capable of receiving a digital signal with an average RMS signal power that is within ± 6 dB of its nominal level with respect to the nominal level of the adjacent channel digital or analog signal.

It is noted that the nominal carrier power levels provided above fall within the absolute power range for digital signals, -15 dBmV to +15 dBmV. The nominal analog signal power is measured as the peak envelope power (PEP), which is the average of all the analog RMS carrier power levels measured during horizontal sync level. The nominal digital signal power is measured as the average of all the digital RMS signal power levels.

7.3.1.1.2 Adjacent Channel Characteristics

REQ36 The OCUR SHALL be capable of receiving digital and analog signals with "Worst Case" Adjacent Channel performance as characterized in Table 7.3–3 - Adjacent Channel Characteristics.

Table 7.3–3 - Adjacent Channel Characteristics

	Desired (D) Channel Modulation	Undesired (U) Adjacent Channel Modulation	Worst Case D/U Ratio*
1.	Analog NTSC	64-QAM	-1 dB
2.	Analog NTSC	256-QAM	-6 dB
3.	Analog NTSC	QPSK FDC	-6 dB
4.	64-QAM	Analog NTSC	-21 dB
5.	64-QAM	256-QAM	-21 dB
6.	64-QAM	QPSK FDC	-21 dB
7.	256-QAM	Analog NTSC	-16 dB
8.	256-QAM	64-QAM	-11 dB
9.	256-QAM	QPSK FDC	-16 dB
10.	QPSK FDC	Analog NTSC	-22 dB
11.	QPSK FDC	64-QAM	-17 dB
12.	QPSK FDC	256-QAM	-22 dB
* Independent of the D/U ratios, the C/(N+I) and the absolute signal levels range shall meet the requirements for those parameters as described elsewhere in the specification.			

7.3.1.1.3 Ranges for Digital Signals

REQ37 Independently of meeting the requirements specified in Sections 7.3.1.1.1 and 7.3.1.1.2 above, the OCUR SHALL tune and receive digital signals that fall within the ranges specified in Table 7.3–1 (QAM signals) and Table 7.3–2 - FDC Channel: RF Performance Parameters (0° - 40° C) (QPSK FDC signals).

REQ38 Independently of meeting the requirements listed in 7.3.1.1.1 RF Signal Levels and 7.3.1.1.2 Adjacent Channel Characteristics, the OCUR SHALL be capable of receiving digital 64QAM with characteristics:

REQ38.1 Level = -10 dBmV on channel 82

REQ38.2 Interleaver depth of greater than or equal to I=64 (J=2)

REQ38.3 33 dB C/N

REQ38.4 -18 dB ghost at 0.5 us

REQ38.5 25 us burst noise not greater than -15 dBmV at 10 Hz rep rate

REQ39 Independently of meeting the requirements listed in 7.3.1.1.1 RF Signal Levels and 7.3.1.1.2 Adjacent Channel Characteristics, the OCUR SHALL be capable of receiving digital 256QAM with characteristics:

REQ39.1 Level = -7 dBmV on channel 82

REQ39.2 Interleaver depth of greater than or equal to I=64 (J=2)

REQ39.3 36 dB C/N

REQ39.4 -18 dB ghost at 0.5 us

REQ39.5 16 us burst noise not greater than -12 dBmV at 10 Hz rep rate

7.3.1.1.4 *Spurious Emissions from the OCUR*

REQ40 The OCUR SHALL limit all spurious emissions according to item 15 in Table 7.3-1- Analog and FAT Channel: RF Performance Parameters (0° - 40° C).

8 CARD INTERFACE

The OCUR provides an interface to the Card to facilitate the processing of digital information, which is received over the forward application transport (FAT) channel and the forward data channel (FDC).

The interfaces between the OCUR and the Card are described in [CCIF] and referenced in Section 6.4.

- REQ41 The OCUR SHALL implement the Unidirectional Host Model in one or both S-Mode or M-Mode as specified in the following sections of [CCIF]:
- 7.0 Physical Interface_
 - 9.0 Command Channel Operation_
 - 10.6 Link Layer_
 - Annex B Error Handling_
 - Annex E DownloadIndicator Message Detail for Common Download (Normative)_
- REQ42 The OCUR SHALL support transport stream interface data rates of 26.97035 Mb/s and 38.81070 Mb/s averaged over the period between the sync bytes of successive transport packets with allowable jitter of +/- one MCLKI clock period.
- REQ101 The OCUR SHALL NOT utilize signals ITX, QTX, ETX, and CTX.
- REQ44 The OCUR SHALL NOT report a Low Speed Communication resource identifier.

8.1 OCUR Functionality with Unscrambled Content

The OCUR needs to function without a Card and process the information received via the NTSC and FAT channels directly.

The OCUR needs to have the following minimum performance characteristics without the Card:

- REQ1244 The OCUR SHALL encode and deliver to the DRI received analog television programming in one of the video formats defined in [SCTE 43] with audio encoded as either MPEG-1 Level 2 as defined by [ISO-13818-3] with support for the minimum configuration defined in [DRI], or AC-3 as defined by [A/53C], compliant with [DRI], and representative of the source content.
- REQ1245 The OCUR SHALL make available on the DRI connection [DRI] unscrambled digital standard- and high-definition audio-visual in the formats defined in [SCTE 43].

8.2 OCUR Functionality without a Card

- REQ49 When the OCUR is operating without a Card, any channel map created from Control Stream data while previously operating with a Card SHALL NOT be used.

8.3 Man Machine Interface (MMI) Support

The OCUR needs to be capable of operating in a unidirectional system and support copy protection in this operational case. As defined in [CCCP], for a unidirectional system, the copy protection system performs ID reporting utilizing the MMI resource.

- REQ50 The OCUR SHALL support the MMI resource defined in [CCIF].
- REQ51 The OCUR SHALL support the MMI protocol defined in [DRI].

8.4 Software Download

- REQ52 The OCUR SHALL download and install a single monolithic code image to replace the OCUR's entire operating code based on the One-way Broadcast protocols specified in [CCIF] and security systems specified in [OC-SEC].
- REQ53 The OCUR SHALL receive SRM defined in Annex B based on the One-way Broadcast protocols specified in [CCIF] and security systems specified in [OC-SEC].
- REQ54 The OCUR SHALL securely download and install a single monolithic code image to replace the OCUR's entire operating code delivered from the DRI.
- REQ55 The OCUR SHALL add into the `Drm_revocation_list` any `Drm_UUID(s)` with a `revocation_status = 01` when received through a SRM defined in Annex B.
- REQ56 The OCUR SHALL remove from the `Drm_revocation_list` any `Drm_UUID(s)` with a `revocation_status = 00` when received through a SRM defined in Annex B.
- REQ57 The OCUR SHALL store the `Drm_revocation_list` into non-volatile memory every time it is updated.
- REQ58 The OCUR SHALL event a URL to notify the user via the [DRI] of all DRMs it supports, whenever a DRM is added, removed, renewed or revoked as a result of software download.

8.5 Digital Receiver Interface (DRI) Output

The OCUR provides an interface to the Home Media Server that allows a secure control of its navigation and security services over an IP network. Other types of digital outputs are not permitted on an OCUR.

The Digital Receiver Interface protocol between the OCUR and the home media server is described in the OpenCable Digital Receiver Interface Specification [DRI].

- REQ59 The OCUR SHALL include a digital output in compliance with the Digital Receiver Interface specification [DRI].
- REQ60 The OCUR SHALL NOT include any other OpenCable defined outputs.

9 VIDEO

9.1 Analog Video

The OCUR will be introduced into an environment containing many existing analog channels. The OCUR will be able to receive analog services that are unscrambled. Analog video and audio will be NTSC-decoded in accordance with current cable-system practice and applicable FCC rules.

9.2 Digital Video

The OCUR is required to handle all digital transport streams according to the following requirements:

9.2.1 MPEG-2 Transport

- REQ61 The OCUR SHALL support System Information tables provided in [SCTE 65] for the navigation function.
- REQ62 The OCUR SHALL acquire and make available on the DRI a Digital Service contained within the same multiplex within 1.5 seconds.
- REQ63 The OCUR SHALL acquire and make available on the DRI a Digital Service contained within a different multiplex within 2.0 seconds.
- REQ64 The OCUR SHALL store the [SCTE 65] system information tables required for program navigation in non-volatile memory.

9.2.2 FAT Delivered Service/System Information

- REQ65 The OCUR SHALL make available upon request on the DRI connection [DRI] in-band System and Service Information for programs that are transported unscrambled in accordance with Section 5.5 Constraints on PSI of [SCTE 54].

9.2.3 Service/System Information provided by Card

- REQ66 The OCUR SHALL make available upon request on the DRI connection [DRI] Service/System Information provided by the Card or found In-band.

The set of MPEG-2 tables required to support the navigation function in the OCUR conforms to one or more of the profiles specified in [SCTE 65].

- REQ67 The OCUR SHALL be able to extract the channel map used for program navigation from all profiles specified in [SCTE 65].

9.2.4 Digital Television (DTV) Closed Captioning

- REQ69 The OCUR SHALL make available on the DRI connection [DRI], NTSC closed captioning information, when present in line 21 of the VBI as specified in [CEA-608], in the MPEG-2 Picture Level user_data transported according to [SCTE 21].
- REQ70 The OCUR SHALL make available on the DRI connection [DRI], Digital Television closed captioning (DTVCC) information when present in the MPEG-2 Picture Level user_data, as specified in section 9 of [CEA-708] and transported according to [A/53C] (with *cc_type* 10 or 11).
- REQ71 The OCUR SHALL make available on the DRI connection [DRI] the caption_service_descriptor, as defined in [A/65B] and carried in either the PMT of the in-band MPEG-2 transport stream or passed across the Card Extended Data Channel according to [CCIF].

9.2.5 Digital Television (DTV) Content Advisory Information

To support the interoperable availability of content advisory information for OCURs and/or Cards, OpenCable specifies the use of MPEG-2 Picture Level user_data found in [SCTE 21], the

content_advisory_descriptor passed across the Extended Data Channel, or the content_advisory_descriptor found in section 6.7.4 of [A/65B]. The syntax follows Table 6.18 in that reference. This descriptor is placed in the Program Map Table (PMT) as permitted in Table 6.16 of [A/65B] in accordance with the standard descriptor mapping for the TS_program_map_section() found in [ISO 13818-1].

The only rating region currently defined for OpenCable use is Region One (value 0x01 for the rating_region field). Semantics for the coding of the fields found in the PSIP Content Advisory Descriptor follow the rules given in section 6.74 of [A/65B].

REQ72 The OCUR SHALL make available on the DRI connection [DRI] content advisory information as specified in [CEA-608] when such information is transported according to [SCTE 21] or [SCTE 20].

REQ73 The OCUR SHALL convert and make available on the DRI any [CEA-608] NTSC content advisory information as an [A/65B] compliant content_advisory_descriptor in PMT tables as defined in Table 9.2-1.

Table 9.2-1 - Content advisory conversion table

ATSC Descriptor			608B Descriptor	
Rated_ Dimension	Rating_region	Rating_value	Rating Level	Attributes
0	US_TV	1	US_TV_None	
		2	US_TV_G	
		3	US_TV_PG	
		4	US_TV_14	
		5	US_TV_MA	
1	US_TV	1		Sexually Suggestive Dialog
2	US_TV	1		Adult Language
3	US_TV	1		Sexual Situation
4	US_TV	1		Violence
5	US_TV	1	US_TV_Y	
		2	US_TV_Y7	
6	US_TV	1		Fantasy Violence
7	MPAA	1	MPAA_NotApplicable	
		2	MPAA_G	
		3	MPAA_PG	
		4	MPAA_PG13	
		5	MPAA_R	
		6	MPAA_NC17	
		7	MPAA_X	
		8	MPAA_NotRated	

- REQ74 The OCUR SHALL make available on the DRI connection [DRI] the content advisory information as defined by [A/65B] and [CEA-766-A] when such information is transported in either the PMT of the in-band MPEG-2 transport stream or passed across the Card Extended Data Channel according to [CCIF].
- REQ103 The OCUR SHALL have the U. S. RRT (Region Rating Table for Region One) defined in [CEA-766-A] either embedded as part of the firmware or stored in non-volatile memory, such that the table is always available for use when needed.
- REQ76 The U.S. RRT SHALL be the default RRT for all OCURs. It is noted that this approach is consistent with that specified in Annex C.1 of [SCTE 65].

9.2.6 Digital Television (DTV) Emergency Alert Service (EAS)

- REQ77 The OCUR SHALL make available on the DRI connection [DRI] EAS messages as defined in [SCTE 18].
- REQ1246 When a CableCard device is not inserted the OCUR SHALL make available on the DRI connection [DRI] any EAS message found In-Band.

10 OCUR POWERING STATES

Once the OCUR has power applied and has performed Card installation and initialization, it always has access to cable network services through the Control Stream channel for receipt of messages, alarms, or notifications. Thus, when the OCUR is “On” (from the subscriber’s perspective), it is fully active and providing services to the connected HMS. When it is “Off”, it still maintains cable network connectivity and thus is still consuming power and running the processor, operating system, and navigator shell.

- REQ78 The OCUR SHALL re-acquire the FDC after being disconnected from and then reconnected to power.
- REQ79 The OCUR SHALL re-acquire the FAT and FDC after being disconnected from and then reconnected to RF cable connection.
- REQ1247 The OCUR SHALL enter background mode when the USB connection is not streaming.
- The operation of the OCUR in background mode is not defined in this document.

Card Background Mode Power Management

- REQ80 The minimum power requirements for Background mode SHALL include the following:
- REQ80.2 The OCUR FDC receiver circuitry SHALL be fully powered when a Card is inserted.
- REQ80.1 The Card SHALL be fully powered when present.

11 OCUR DIAGNOSTICS

The following requirements define the self-reporting diagnostic parameters that the OCUR use to identify its working state.

REQ84 The OCUR SHALL be capable of performing self-diagnostics and displaying a minimum set of diagnostics via LED that includes:

REQ84.1 REQ84.pending1 REQ85.1 OCUR power status

REQ84.2 REQ84.pending2 REQ85.2 OCUR boot status

REQ84.3 REQ84.pending3 REQ85.3 Indication of fatal error (e.g., Checksum error)

REQ86 The OCUR SHALL provide the following diagnostic information to the DRI connection [DRI] and to the CableCARD device interface [CCIF] if requested.

REQ86.1 OCUR power status

REQ86.2 OCUR boot status

REQ86.3 OCUR memory allocation

REQ86.4 Software version numbers of code in the OCUR

REQ86.5 Firmware version

REQ86.6 MAC addresses

REQ86.7 OCUR network addresses

REQ86.8 Status of FDC

REQ86.9 Status of FAT

REQ86.10 Current channel status

REQ100 NOTE: These diagnostics MAY also be displayed on the LED.

REQ83 The OCUR SHALL report any requested self diagnostics to the Card through the Generic Diagnostic Support resource.

The following subsections describe the self-diagnostics parameters, specified above, that are reported to the Card and made available on the DRI connection [DRI].

11.1 Memory Resources

REQ87 The OCUR SHALL be capable of reporting memory allocation results that SHALL include, but are not limited to:

REQ87.1 Type of memory being reported (ROM, DRAM, SRAM, Flash, and NVM)

REQ87.2 Physical size of memory type (in kilobytes, defined to 1024 bytes)

11.2 Software Versions

REQ88 The OCUR SHALL be capable of reporting software version number results, of all available applications, that SHALL include:

REQ88.1 Application's name string

REQ88.2 Application's version number

REQ88.3 Software status (active, inactive or downloading)

REQ88.4 If applicable, Application's signature

11.3 Firmware Version (OCUR)

- REQ89 The OCUR SHALL be capable of reporting firmware version results that SHALL include:
- REQ89.1 Firmware version number of entire firmware image
 - REQ89.2 Firmware's release or installation date of entire firmware image

11.4 MAC Addresses

- REQ90 The OCUR SHALL be capable of reporting media access control (MAC) address results that SHALL include:
- REQ90.1 Type of devices being reported (OCUR, Card, USB, and/or Ethernet)
 - REQ90.2 NOTE: If multiple devices of the same type exist, then the MAC address for each device type SHALL be reported.
 - REQ90.3 MAC address of each reported device

11.5 OCUR Network Addresses

- REQ92 The OCUR SHALL be capable of reporting network address results that SHALL include:
- REQ92.1 Network address of device
 - REQ92.2 NOTE: If multiple network addresses exist, then each network address SHALL be reported.

11.6 Status of FDC

- REQ94 The OCUR SHALL be capable of reporting forward data channel (FDC) status results that SHALL include:
- REQ94.1 FDC center frequency, in MHz
 - REQ94.2 Carrier lock status (e.g., LOCKED – NOT LOCKED)

11.7 Status of FAT

- REQ95 The OCUR SHALL be capable of reporting forward application transport (FAT) channel status results that SHALL include:
- REQ95.1 Modulation mode indicator; analog, 64 QAM, or 256 QAM
 - REQ95.2 Carrier lock status
 - REQ95.3 If the currently tuned channel is digital, then PCR lock status; the FAT channel tuner is locked or not locked to the currently tuned service
 - REQ95.4 Numerical estimate of the channel's signal to noise ratio in tenths of a dB
 - REQ95.5 Numerical estimate of the signal level in tenths of a dBmV
 - REQ95.6 NOTE: When operated at nominal line voltage, at normal room temperature, the reported Level and SNR SHALL be within 6 dBmV and 3 dB of the actual received channel level and SNR, respectively, for the input level range of -15 dBmV to +15 dBmV.
 - REQ95.7 NOTE: Across the input level range from -15 dBmV to +15 dBmV, for any 1 dB change in input level or SNR, the OCUR SHALL report a power change in the same direction that is not less than 0.5 dB and not more than 2.0 dB.

11.8 Current Channel Status

REQ98 The OCUR SHALL be capable of reporting current channel status results that SHALL include, but are not limited to:

REQ98.1 Channel type; analog or digital

REQ98.2 Authorization status; OCUR is authorized or not authorized for currently tuned service

REQ98.3 Purchasable status; currently tuned service may or may not be purchased

REQ98.4 Purchased status; currently tuned service is or is not purchased

REQ98.5 Preview status; currently tuned service is or is not in preview mode

11.9 DRM Pairing Message

REQ99 The OCUR SHALL be capable of reporting its current DRM Pairing Message.

12 MECHANICAL

- REQ104 The OCUR SHALL be capable of dissipating the heat from a Card drawing an average of 2.5 watts across the Card interface.
- REQ105 The OCUR SHALL have a non-removable nameplate(s) or sticker(s) that includes the following information:
- REQ105.1 Vendor ID: 24-bit vendor ID represented as 3 bytes (6 hexadecimal digits).
- REQ105.2 This number SHOULD be assigned by OpenCable to ensure uniqueness.
- REQ105.3 Vendor Name: 40 ASCII characters maximum.
- REQ105.4 Serial Number or Serial No: 40 ASCII character maximum.
- REQ106 The OCUR SHALL meet all of the requirements listed in this specification without malfunction, hardware or software failures under the conditions listed in Table 12-1.

Table 12-1 - Environmental / Mechanical Requirements

	Parameter	Value	Internal HMS Device	Standalone
1.	Input Line Voltage	95 to 125 VAC		x
2.	Input Line Frequency	57 to 63 Hz		x
3.	RF Susceptibility	RF field of 2 volts/ meter from 40 MHz to 1 GHz	x	x
4.	Lightning Surge Tolerance	UL 1409 voltage surge test 38.1, UL 1449, IEEE C62.41, IEEE 587 compliant. RF Input: 1.5 kV at 1kV/usec, 60 amp peak; AC line input: 6 kV, oscillatory 0.5 µsec rise time 100 kHz.	x	x
5.	Electrostatic Discharge	IEC 801-2, withstand 10 discharges at 15 kV to each corner of the chassis, through a 150 pf capacitor in series with 150 ohm resistor, with device chassis grounded to ESD generator		x
6.	Brown Out Effects	No corruption of non-volatile memory due to input voltage fluctuations from nominal to zero volts	x	x
7.	Operating Ambient Temperature and Humidity	0° to 40° C and 5% to 95% RH non-condensing humidity	x	x
8.	External Surface Temperature (with power applied, device on, and 25° C ambient temperature)	UL 1409 compliant. No external protruding surface point hotter than 50° C for metallic and 60° C for nonmetallic surfaces. No non-accessible surface point hotter than 65° C.	x	x
9.	Storage Temperature (non-powered, non-operating)	-20° to +60° C	x	x
10.	Storage Humidity (non-powered, non-operating)	5% to 95% RH non-condensing at 40° C	x	x

	Parameter	Value	Internal HMS Device	Standalone
11.	Altitude	Operating: -150 to 10,000 ft. AMSL Storage: -150 to 15,000 ft. AMSL _±	x	x
12.	Thermal Shock	Device meets all operational specs after subjection to: -40° C. for 30 minutes +25° C. for 10 minute +60° C. for 30 minutes _±	x	x
13.	Humidity Shock	Mil-std-810d method 507.2: Device meets all operational specs after subjection to: raise temp to +60° C and 95% RH over 26 hrs., maintain for 6 hrs., drop to 85% RH while reducing temp to +30° C over 8 hrs., maintain +30° C and 95% RH for 8 hrs. Repeat for 10 cycles.	x	x
14.	Solvent Resistance	No external surface deformation effect of common household solvents, cleaners, waxes.		x
15.	Shipping Vibration	Fully operational after subjection to swept frequency vibration test applied in each of x, y, z planes with excursion of 0.3 inches at a frequency varied from 10 to 30 Hz back to 10 Hz done six times within 30 minutes.	x	x
16.	Mounting Feet	No marks or stain to varnished wooden surface after 40° C and 95% RH exposure for 10 days under force of 1.65 lbs.		x
17.	Impact Test	Device will not develop any openings creating electrical shock risks after subjection to an impact force of 5 ft. lbs. obtained from a free fall of a 2-inch diameter solid smooth steel sphere weighing 1.18 lbs.		x
18.	Handling Drop Test	Device fully operational and not develop any openings exposing risk of electrical shock after subjection to one drop on the face of the device from a height of 20 inches onto a 2-inch thick smooth surface concrete floor.		x
19.	Strain Relief Test	For permanently attached power supply cords, device will withstand steady pull force of 35 lbs. applied to the cord.		x
20.	Non-volatile Memory Life	Non-volatile memory will have a non-powered minimum life of: 1.5 yrs storage life @ 60° C or less.	x	x
21.	Microphonic Shock	Device will remain error- or interference-free (i.e., no audio pops, clicks, no data errors, no video artifacts) when subjected to tapping with a reasonable force by placing device on a hard surface without padding or mats and inducing 20 taps from knuckles, flat hands, fists, finger nails, screwdriver handles, plastic hammers to all external surfaces of the device.	x	x

	Parameter	Value	Internal HMS Device	Standalone
22.	Physical Security/ Tamper-Resistance	Secure means of evidencing entry into the security portions of the device	x	x

Annex A OCUR-HMS CONTENT PROTECTION REQUIREMENTS (normative)

REQ113 When paired with a CableCARD, the OCUR SHALL output content received on the Cable Input ONLY on the DRI and consistent with the tables below. REQ114 The DRM SHALL specify usage rights (enforced pursuant to the applicable DRM compliance rules) to permit content output only as shown in the tables below.

Content Type designation key: A = Analog; D = Digital; numerical values 0,1,2, or 3 reflect the bit values of the successive content control value columns; X = ignore or don't care.

Analog TV Signals on OCUR's Cable Input						DRM License and Encryption on DRI	Internal HMS Retention Limit (min.)	Downstream Distribution from HMS of DRM-Protected Cable Content	Output of Content by Devices Downstream of OCUR															
									Analog Composite or Component Outputs						VGA ⁴	HDCP on DVI and HDMI	1394 / DTCP			VCPS Output Allowed				
#	Content Type	CA Scrambled	Macrovision Encoding on Video Signal	APS ¹	CGMS-A ¹	To Display Only Devices (no persistent storage)*	To External Storage Devices**	Macrovision Encoding on 480 line Video Signals	CEA-608-C and IEC 61880, or CEA-805-C encoding ⁸			Image Cons-Train ³	Max. Frame Resolution (pixels)	DTCP Encryption?	EPN ⁵		EMI							
1	A S	1	X	X	X	Not supported by the OCUR device – This requirement is enforced by the OCUR specification and not the DRM																		
2	A 300	0	AGC + 4 CS	X	X	Yes	90	Yes	No	AGC+ 4 CS	1,1	1,1	1	no	520k	Yes	Yes	1	1,1	No				
3	A 200		AGC + 2 CS							AGC+ 2 CS	1,0													
4	A 100		AGC							AGC	0,1													
5	A 33	0	none	1,1	X	Yes	90			AGC+ 4 CS	1,1	1,1	1			Yes	Yes	1	1,1	No				
6	A 31																							
7	A 32																							
8	A 30	0	none	1,0	X	Yes	90			AGC+ 2 CS	1,0	1,1	1			Yes	Yes	1	1,1	No				
9	A 23																							
10	A 21																							
11	A 22	0	none	0,1	X	Yes	90			AGC	0,1	1,1	1			Yes	Yes	1	1,1	No				
12	A 20																							
13	A 13																							
14	A 11	0	none	0,0	X	Yes	90			Yes	No	none	0,0			1,1	1	no	520k	Yes	Yes	1	1,1	No
15	A 12																							
16	A 10																							
17	A 03	0	none	0,0	X	Yes	90					none	0,0			1,1	1			Yes	Yes	1	1,1	No
18	A 01																							
19	A 02																							
20	A 00	0	none	none	none	Yes	none					Yes	0,0			0,0	0			Yes	No	1	0,0	Not Protected
21	A N											Yes	0,0			0,0	0							

Input of Digital TV on OCUR's Cable Input							DRM License and Encryption on DRI	Internal HMS Retention Limit (min.)	Downstream Distribution from HMS of DRM-Protected Cable Content	Output of Content by Devices Downstream of OCUR																	
										Analog Composite and Component Outputs					VGA ¹⁰	HDCP on DVI or HDMI	1394/DTCP			VCPS Output Allowed							
#	Content Type	CA-Scram-Bled ⁶	EPN	CIT	APS	EMI			Display Only Devices (persistent storage not allowed)*	To External Storage Devices**	Macrovision Encoding on All 480 Line Video Signals	CEA-608-B and IEC 61880, or CEA-805-C encoding ⁸			Image Cons-Train ⁹	Max. Frame Resolution (pixels)		DTCP Encryption?	EPN		EMI						
1	D1 33	1	X	0	1,1	1,1	Yes	90	Yes	No	AGC+ 4 CS	1,1	1,1	1	No	520k	Yes	Yes	1	1,1	No						
2	D1 C33			1											520k												
3	D1 23			0	1,0						AGC+ 2 CS	1,0			No												
4	D1 C23			1											520k												
5	D1 13			0	0,1						AGC	0,1			No												
6	D1 C13			1											520k												
7	D1 03			0	0,0						none	0,0			No												
8	D1 C03			1											520k												
9	D1 31	1	X	0	1,1	0,1	Yes	90			Yes	No	AGC+ 4 CS	1,1	1,1	1	No	520k	Yes	Yes	1	0,1	No				
10	D1 C31			1													520k										
11	D1 21			0	1,0								AGC+ 2 CS	1,0			No										
12	D1 C21			1													520k										
13	D1 11			0	0,1								AGC	0,1			No										
14	D1 C11			1													520k										
15	D1 01			0	0,0								none	0,0			No										
16	D1 C01			1													520k										
17	D1 32	1	X	0	1,1	1,0	Yes	None					Yes	No	AGC+ 4 CS	1,1	1,1	1	No	520k	Yes	Yes	1	1,0	Protected		
18	D1 C32			1															520k								
19	D1 22			0	1,0										AGC+ 2 CS	1,0			No								
20	D1 C22			1															520k								
21	D1 12			0	0,1										AGC	0,1			No								
22	D1 C12			1															520k								
23	D1 02			0	0,0										none	0,0			No								
24	D1 C02			1															520k								
25	D1 E30	1	0 (Signaled)	0	1,1	0,0	Yes	None		Yes					No	AGC+ 4 CS	1,1	1,1	1	No	520k	Yes	Yes	0	0,0	Protected	
26	D1 EC30			1																520k							
27	D1 E20			0	1,0											AGC+ 2 CS	1,0			No							
28	D1 EC20			1																520k							
29	D1 E10			0	0,1											AGC	0,1			No							
30	D1 EC10			1																520k							
31	D1 E00			0	0,0											none	0,0			No							
32	D1 EC00			1																520k							
33	D1 30	1	1 (Not Signaled)	0	1,1	0,0	Yes	None				Yes				No	AGC+ 4 CS	1,1	1,1	0	No	520k	Yes	No	1	0,0	Not Protected
34	D1 C30			1																	520k						
35	D1 20			0	1,0												AGC+ 2 CS	1,0			No						
36	D1 C20			1																	520k						
37	D1 10			0	0,1												AGC	0,1			no						
38	D1 C10			1																	520k						
39	D1 00			0	0,0												none	0,0			no						
40	D1 C00			1																	520k						

¹ APS and CGMS-A indicators on Analog TV input refer to Line 20 per IEC 61880 and Line 21 per [CEA-608]. REQ108 If the protection indicators conflict, the OCUR SHALL apply the more restrictive value of each APS, CGMS-A and RC.

REQ109 ² All analog composite or component outputs SHALL include the parameters shown encoded compliant with [CEA-608] and [IEC 61880] for RF, composite video, S-video and 480i component signals, and, compliant with CEA-805-C for 480p, 720p and 1080i component signals. Until 18 months after the Effective Date, this requirement is CONDITIONAL MANDATORY, applicable only when the graphics card includes support for “type B” packets as described in CEA-805-C. After 12 months, this requirement will be MANDATORY for HMSs manufactured with next generation graphics chipsets, and after 18 months will be MANDATORY for all HMSs.

³ Image Constraint is defined in [CCCP]. A Constrained Image can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

⁴ VGA outputs as defined in [CHILA]. Content output over VGA can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

⁵ The CCI and DTCP “EPN” bit value of zero signals Encryption Plus Non-assertion. The EPN value of one signals EPN mode inactive.

REQ110 ⁶ The OCUR SHALL treat all content for which it requests CA descrambling of the CableCARD as CA-Scrambled.

⁷ CCI Value per SCTE 41 2004 extended with an EPN bit defined as Encryption Plus Nonassertion. A value of 0 signals that content must remain protected.

REQ111 ⁸ All analog composite or component outputs SHALL include the parameters shown encoded compliant with [CEA-608] and IEC 61880 for RF, composite video, S-video and 480i component signals, and, compliant with CEA-805-C for 480p, 720p and 1080i component signals. Until 18 months after the Effective Date, this requirement is CONDITIONAL MANDATORY, applicable only when the graphics card includes support for “type B” packets as described in CEA-805-C. After 12 months, this requirement will be MANDATORY for HMSs manufactured with next generation graphics chipsets, and after 18 months will be MANDATORY for all HMSs.

⁹ Image Constraint is defined in [CCCP] and applies only to output at 720p or 1080i lines. A Constrained Image can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

¹⁰ VGA outputs as defined in [CHILA]. Content output over VGA can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

REQ112 ¹¹ If [SCTE 21] data is present and includes values for APS, CGMS-A, or RC, the OCUR SHALL permit the output of content only according to the values shown in the inset tables.

01/09/06

CableLabs®

35

** External Storage Devices, which are downstream devices on which Cable Content can be stored (where permitted under applicable compliance rules) and played back, shall be subject to agreed upon proximity limits (when obtaining content) and limited to Standard Definition.

Annex B Mechanism for DRM revocation

SRMs (System Renewability Messages) are used to signal revocation of a DRM installed on the OCUR. SRMs may also be used to signal removal of a previously revoked DRM from the current revocation list. REQ1540 Code Version Table (CVT) described in Table 9.19-5 of the [CCIF] specification SHALL be used to signal SRM messages as well as code image downloads. REQ1541 The code_file_name_byte field in the CVT, used to specify the Code File Name, SHALL use the following extensions to signal different types of code file download as shown in Table B–1.

Table B–1 - Code File Naming

Name	Description
<code file name>.SRM	Code file contains only the SRM (as part of the SignedContent), but not a CodeImage for download
<code file name>.IMAGE	Code file contains only the CodeImage for download, but not the SRM
<code file name>.BOTH	Code file contains both the SRM (as part of SignedContent), as well as the CodeImage for download

B.1 Image File Structure

The code download file is a file built using a PKCS #7 compliant structure that has been defined in a specific format for use with the OCUR. REQ1542 The code file SHALL comply with [OC-SEC] except as shown in this Annex, and SHALL be DER encoded. REQ1543 The code file SHALL match the structure shown in Table B–2. REQ1544 The code image SHALL include either the SRM, or the code image, or both as signaled by the Code File Name described in Table B–1.

When downloading an SRM as part of the Code File, signature by CableLabs is mandatory and Co-signing by MSO is optional. When downloading a CodeImage file, signature by the manufacturer is mandatory, and co-signature by either CableLabs or MSO is optional. When downloading both SRM and CodeImage in the Code File, signature by CableLabs is mandatory for the first PKCS #7 object (Table B–5) and Co-signing by MSO is optional, and for the 2nd PKCS #7 object, signature by the manufacturer is mandatory, and Co-signing by MSO is optional.

REQ1545 When downloading the CA Certificates (e.g., a CableLabs CVC CA Certificate and/or a CableLabs Device CA Certificate) as a part of the Code File, the certificates MAY be contained in the fields specified in Table B–2, separated from the actual code image contained in the CodeImage field. Signature by CableLabs is mandatory when downloading CA certificates.

In accordance with section 9.4.2 of [OC-SEC], the final code image provided by the manufacturer is in a format compatible with the OCUR and defined by the manufacturer.

Table B–2 - Code File Structure

Code File	Description
PKCS #7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	EXPLICIT signed-data content value: includes CVS and X.509 compliant CVCs
} end PKCS #7 Digital Signature	
SignedContent {	
DownloadParameters {	Mandatory TLV format (Type 28). (Length is zero if there is no sub-TLVs.)
Srm()	Optional TLV for MSO System Renewability Message TLV format 200. Refer to section B.3.4.

Code File	Description
MfgCACerts ()	Optional TLV for one or more DER-encoded CableLabs Manufacturer CA Certificate(s) each formatted according to CableLabs Device CA-Certificate TLV format (Type 17). Refer to section B.3.1.
clabCVCRootCACert()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs CVC Root CA CA-Certificate TLV format (Type 51). Refer to section B.3.2.
clabOCURCVCCACertificate ()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs OCUR CVC CA-Certificate TLV format (Type 52). Refer to section B.3.3.
}	
CodeImage ()	Optional Upgrade code image.
<i>} end SignedContent</i>	

B.2 Signed Data

The code download file will contain the information in a PKCS #7 Signed Data content type as shown below in Table B-3. Though maintaining compliance to [OC-SEC], the structure used has been restricted in format to ease the processing performed by the OCUR to validate the signature. REQ1546 The PKCS #7 SignedData SHALL be DER encoded and exactly match the structure shown below except for any change required for DER encoding_ (e.g., the ordering of SET OF attributes). REQ1547 The OCUR SHALL reject the PKCS #7 signature if the PKCS #7 Signed Data does not match the DER encoded structure._

Table B-3 - PKCS #7 Signed Data

PKCS #7 Field	Description
SignedData {	
Version	version = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
Content Type	data (SignedContent is concatenated at the end of the PKCS #7 structure)
certificates {	CableLabs Code Verification Certificates
SignerCVC	(REQUIRED for all code files)
Co-signerCVC	(OPTIONAL; required for co-signatures)
} end certificates	
SignerInfo {	
SignerInfo {	(REQUIRED for all code images/SRMs)
Version	version = 1
IssuerAndSerialNumber	
IssuerName	
CountryName	US
OrganizationName	CableLabs
CommonName	CableLabs OCUR CVC CA
CertificateSerialNumber	<Signer CVC serial number>
DigestAlgorithm	SHA-1
AuthenticatedAttributes	
Content Type	data (contentType of signedContent)
SigningTime	UTC Time (GMT), YYMMDDHHMMSSZ
MessageDigest	Digest of the content as defined in PKCS #7
DigestEncryptionAlgorithm	RsaEncryption
EncryptedDigest	
} end mfg signer info	
CoSignerInfo {	(OPTIONAL; required for co-signatures)
Version	version = 1
IssuerAndSerialNumber	
IssuerName	
CountryName	US
OrganizationName	CableLabs
CommonName	CableLabs OCUR CVC CA
CertificateSerialNumber	<CoSigner CVC serial number>
DigestAlgorithm	SHA-1

PKCS #7 Field	Description
AuthenticatedAttributes	
Content Type	data (contentType of signedContent)
SigningTime	UTC Time (GMT), YYMMDDHHMMSSZ
MessageDigest	Digest of the content as defined in PKCS #7
DigestEncryptionAlgorithm	RsaEncryption
EncryptedDigest	
} end CoSignerInfo	
} end SignerInfo	
} end SignedData	

B.3 Signed Content

REQ1548 The SignedContent field of the Code File SHALL contain either the SRM, or the CodeImage, or both. In addition, it may contain the download parameters field, which possibly contains additional optional items - CA Certificates (e.g., a CableLabs OCUR CVC CA Certificate and/or a CableLabs Device CA Certificate).

REQ1549 If the Code file name ends with .SRM (Table B-1), then the OCUR SHALL verify that the SignedData portion of the Code File comprises of the SRM as shown in Table B-4.

REQ1550 If the Code File name ends with .IMAGE (Table B-1), then the OCUR SHALL verify that the final code image is in a format compatible with the destination OCUR. In support of the PKCS #7 signature requirements, the code content is typed as data; i.e., a simple octet string. REQ1551 In the PKCS #7 object, the SignedContent SHALL be blank, but it SHALL contain the CodeImage portion. The format of the final code image is not specified here and will be defined by each manufacturer according to their requirements.

REQ1552 If the Code File ends with .BOTH (Table B-1), then the OCUR SHALL verify that the Code File contains two PKCS #7 objects as shown in Table B-5. REQ1553 The first PKCS #7 object SHALL contain the SRM structure (shown in Table B-4) as part of the SignedContent, but the CodeImage portion SHALL be blank. REQ1554 In the second PKCS #7 object, the SignedContent SHALL be blank, but it SHALL contain the CodeImage portion with the final code image in a format compatible with the destination OCUR.

REQ1555 Each manufacturer SHOULD build their code with additional mechanisms that verify an upgrade code image is compatible with the destination OCUR.

If included in the signed content field, the certificate fields are intended to replace the CableLabs CVC Root CA or the CableLabs OCUR CVC CA Certificate(s) currently stored in the OCUR. REQ1556 If the code download and installation is successful, the OCUR SHALL update its currently stored certificates with the ones contained in the MfgCACerts, clabCVCRootCACert and clabOCURCVCCACertificate fields of the signed content field in the new Code File.

B.3.1 CableLabs Device CA-Certificate TLV Format

The attribute is a string attribute containing an X.509 CA Certificate, as defined in [OC-SEC].

Type	Length	Value
17	Variable	X.509 CableLabs Device CA Certificate (DER-encoded ASN.1)

B.3.2 CVC Root CA CA-Certificate TLV Format

The attribute is a string attribute containing an X.509 CA Certificate, as defined in [OC-SEC].

Type	Length	Value
51	Variable	X.509 CableLabs CVC Root CA Certificate (DER-encoded ASN.1)

B.3.3 CVC CA-Certificate TLV Format

The attribute is a string attribute containing an X.509 CA Certificate, as defined in [OC-SEC].

Type	Length	Value
52	Variable	X.509 CableLabs CVC CA Certificate (DER-encoded ASN.1)

B.3.4 SRM Format

REQ1557 For DRM revocation (or removal from revocation list), the SRM SHALL have the format as shown in Table B-4.

Table B-4 - SRM Structure

Syntax	# of bits	Description
Srm() { number_of_DRMs issue_date for (i=0;i<number_of_DRMs;i++) { drm_guid revocation_status } }	8 32 128 8	Number of DRMs listed in this SRM Unsigned integer quantity representing the current system time as the number of seconds since 12 AM, January 6, 1980. Global Unique Identifier for the DRM system

revocation_status: 0x00 Not revoked
 0x01 Revoked

Table B-5 - Code File Structure

Code File	Description
PKCS #7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	EXPLICIT signed-data content value: includes CVS and X.509 compliant CVCs
} end PKCS #7 Digital Signature	
SignedContent {	
DownloadParameters {	Mandatory TLV format (Type 28). (Length is non-zero)
Srm()	Mandatory TLV for MSO System Renewability Message TLV format 200. Refer to section B.3.4.
MfgCACerts ()	Optional TLV for one or more DER-encoded CableLabs Manufacturer CA Certificate(s) each formatted according to CableLabs Device CA-Certificate TLV format (Type 17) Refer to section B.3.1.
clabCVCRootCACert()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs CVC Root CA CA-Certificate TLV format (Type 51). Refer to section B.3.2.
clabOCURCVCCACertificate ()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs OCUR CVC CA-Certificate TLV format (Type 52). Refer to section B.3.3.
}	
CodeImage ()	No Upgrade code image.
} end SignedContent	
PKCS #7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	EXPLICIT signed-data content value: includes CVS and X.509 compliant CVCs
} end PKCS #7 Digital Signature	
SignedContent {	
DownloadParameters {	Mandatory TLV format (Type 28). (Length is zero)
Srm()	No SRM

Code File	Description
MfgCACerts ()	No CA Certificates
clabCVCRootCACert()	No Root CA Certificates
clabOCURCVCCACertificate ()	No CA certificates
}	
CodeImage ()	Mandatory Upgrade code image.
<i>} end SignedContent</i>	