THE UNIQUE CHALLENGES FACED BY CABLE SYSTEMS SERVING SMALLER MARKETS AS THEY EXPAND TO MEET CONDITIONAL ACCESS AND OCAP REQUIREMENTS

Gary Traver, James Capps
Comcast Media Center

Abstract

Separable security systems represent a fundamental component of a long-term migration towards an open standards / open architecture world. OCAP, the OpenCable Application Platform, which was developed for the industry by CableLabs[i], is designed to drive the future of interchangeable devices toward this vision for an open-architecture environment.

The operational rigor associated with managing devices in this interchangeable world is complex. As both separable security and OCAP evolve, the number of consumer devices able to make use of this open network will grow.

Cable systems serving smaller markets must address the expensive regulatory requirement for separable security and the migration toward OCAP at the same time that their customers have more choices for the providers of advanced video services than any other time in history[ii].

Because they lack the economies of scale afforded by cable systems serving larger markets, cable operators serving smaller communities need solutions that build upon their existing architecture. In addition, they can meet or exceed the economies of a large-market solution by pooling their resources into a centralized service bureau. However, a one-size-fits-all solution is counter-productive to a competitive marketplace. To be effective, the centralized services bureau will also need to address the unique requirements of each cable system.

INTRODUCTION

U.S. cable systems serving exurban areas of the U.S, the first markets to embrace cable television's "community antenna" technology, face the greatest challenge in creating next-generation content distribution networks. As cable nears its 60th anniversary in many of these communities, these cable system operators are tasked with meeting new conditional access requirements that potentially thwart their ability to offer advanced digital video services and threaten their survival. In addition, they must address expensive regulatory requirements at the same time that their customers have more choices for the providers of those services than any other time in history[iii].

While separable security systems represent a fundamental component of a long-term migration towards an open standards / open architecture world, the entire cable industry must respond by complying with a FCC mandate for using separable security to serve all new video customers in the short-term by July 7, 2007. For the purposes of this paper, we are assuming that separable security methodology will evolve over the next several years into a fully software-downloadable security environment.

In addition to managing the conditional access and security processes, another key element of enabling the next-generation content distribution architecture is its ability to support the open standards environment

envisioned by OCAP, the OpenCable Application Platform. OCAP, which was developed for the industry by CableLabs[iv], is designed to drive the future of interchangeable devices (i.e., STBs, PCs, TVs, etc.) that can easily connect to a cable operator's network and download that operator's user interface and the key system information that is necessary for the device to navigate within the operator's network. This future downloadable, interchangeable world creates a host of new opportunities. However, the ability to connect any device that is both security-compliant and OCAP-compliant also creates a level of complexity well beyond the scope of anything that is in place today.

Cable operators serving smaller markets must comply with security requirements without the same economies of scale as regional cable systems, which serve an urban/suburban cluster of customers from one headend. For example, the minimum cost of the headend equipment and software required to meet federal requirements for separable security are fixed. Therefore, the investment required to implement those solutions can be several magnitudes higher on a cost per subscriber basis for a small cable operator than they are for a larger cable operation. If the minimum system configuration is sized to meet a 25,000 subscriber base, operators with a 5,000 customer base must pay roughly 5 times the cost per customer, and systems in the 1,000 customer base range must pay 25 times the cost per subscriber in order to offer the same mandated solutions.

Accordingly, the same economic issue that applies to separable security also applies to the larger implementation of OCAP in these exurban markets. The systems necessary to detect, manage and deliver the other critical layers of software to enable the use of consumer-owned devices on the network have very similar requirements and thus very similar cost issues for cable operators serving smaller markets.

Finding an economically viable solution for providing these services requires some key changes to the smaller markets' systems and architecture. To provide the same scale economics as larger systems, the conditional access solutions must be able to pool subscriber bases together from many small, unaffiliated cable systems. It must do so in a manner that maintains the individual configurations and attributes of each small system and maintains the security and integrity of each system's data. The most viable approach to meet these criteria is to create a centralized service bureau type of operation.

The operational rigor associated with managing devices in this interchangeable world is complex. As both separable security and OCAP evolve, the number of consumer devices able to make use of this open network will grow. Attention to maintaining network compatibility must be focused in two directions. The focus must first be **technology forward**, to make sure that the system is capable of supporting new consumer devices as they continue to grow and evolve. It must also be **technology backward**, to ensure the legacy equipment in the cable systems continues to receive the appropriate support. Cable operators serving smaller markets must have solutions that allow them to build upon their existing architecture. The economics of their local businesses do not allow them to engage in a total overhaul of their current content distribution infrastructure.

The country's independent cable operator community must have an affordable solution that complies with

federal regulations and additional requirements regarding conditional access security systems by July of this year. While many of these systems have expanded their businesses to offer high speed data and voice services, regulatory requirements pose a real threat to their continued existence. In fact, as the American Cable Association observed: "...many of the small businesses that provide video and broadband services in rural America will cease to exist and the digital divide will actually grow[v]."

As this paper will demonstrate, a solution that is focused on the unique needs of the smaller market in the form of a centralized multi-operator services bureau can allow many cable systems to not only overcome these near-term challenges in conditional access but also provide a long-term strategy for OCAP success. This robust services platform must address many of the requirements for migrating to an all-open standards downloadable environment. By pooling these markets into a national platform, it will also allow them to offer the same access and advantages as other larger cable organizations, enabling smaller system operators to expand the lineup of advanced digital services that they can offer to their customers.

THE CHALLENGES AND OPPORTUNITIES OF NEXT-GENERATION CONDITIONAL ACCESS

While there are many challenges associated with creating secure and robust systems that meet the federal mandate for separable security, the intent of the mandate is consistent with the cable system operators' need to provide a service that responds to their customer's needs and demands. The migration towards separable security and OCAP-compliant consumer electronic devices increases the number of choices that consumers will have to experience the array of services provided by their cable operators. Further, as this environment begins to proliferate across the entire marketplace, all operators will eventually be expected by their customers to provide support for consumer-supplied devices and the type of portability that they provide. Customers who already have their own downloadable devices will exacerbate this demand even further when they move into another cable system's franchise area.

However, providing the systems and infrastructure required to provision services to a wide array of devices in this future downloadable environment is not an easy or inexpensive task. The complexity of the equipment and the systems required to support an open environment increases significantly over current operational requirements. Without economically and operationally viable alternatives, this migration could result in cable system operators struggling to provide even the most basic services under this next-generation architecture.

From the author's perspective, support for separable security and for OCAP are extensions of the same core mission. They both allow for portability and they both require the consumer device to be connected to the cable operators' network in order to get the necessary software and information required to properly receive the services provided by the operator. Most importantly, the consumer devices must depend on the equipment and systems from both of them to function properly. Therefore, from the standpoint of creating an enabling architecture to provision the devices, it makes sense to combine their functionality into a single service entity.

ADVANCING TECHNOLOGIES FOR SET-TOP OPERATIONS

A. CableCARD Implications

Section 629 of the 1996 telecom law resulted in the creation of CableCARD by pressing for separable security[vi]. Responding to this drive, the OpenCable standards were created and specified the CableCARD as a removable security device as follows:

- A Host device (set-top box or integrated television) that provides generic cable tuning and decoding capabilities that are portable across all cable networks.
- A removable CableCARD security module that separates retail delivered set-top box (Host) from proprietary conditional access systems and network messaging.
- An interface between the Host and CableCARD module, that allows for Hosts and CableCARD modules from different vendors to interoperate.

Enabling the CableCARD functionality will require interaction with various downstream systems. Beyond the additional capital outlay required for the CableCARD itself, the smaller operators will now need to ensure that their servers are capable of interacting with the set-top boxes to enable EPG and authorizations.

B. A Future Alternative to CableCARD – DCAS

A cost-effective, cable company agnostic and conditional access system agnostic alternative to the CableCARD is the Downloadable Conditional Access System (DCAS). DCAS allows the cable operator to download its conditional access system of choice to devices connected to its cable network. It is designed to operate with cable set-top boxes, integrated retail DTVs and other devices that include a secure DCAS microprocessor chip. The DCAS protocol is available to any consumer electronics manufacturer enabling a large market of devices to be available for consumers.

A relevant advantage to DCAS is responsiveness in that it is able to address security breaches more quickly and efficiently. In March of 2007, hackers cracked encryption codes used by Swiss cable operator Cable COM and digital television technology group Kudelski SA, and released them on the Internet[vii]. Web savvy pirates could transfer the published codes to a digital TV decoder called a Dreambox DN 500c, and freely access subscription video on the cable system's lineup, according to press reports. A DCAS model allows such breaches to be addressed immediately and remotely, requiring no new hardware or truck-rolls.

C. Expanding the Set-top Functions - OCAP

CableLabs originally developed the OpenCable family of standards to provide a common basis for digital cable TV systems in the U.SSupport for devices addressed via a new standard, the OpenCable Application Platform or OCAP. OCAP results in a stack of software residing between applications and the operating system within a consumer electronics device such as a set-top box or OCAP-compliant TV set. OCAP devices can have new information or applications loaded on them, often taking advantage of new two-way capabilities.

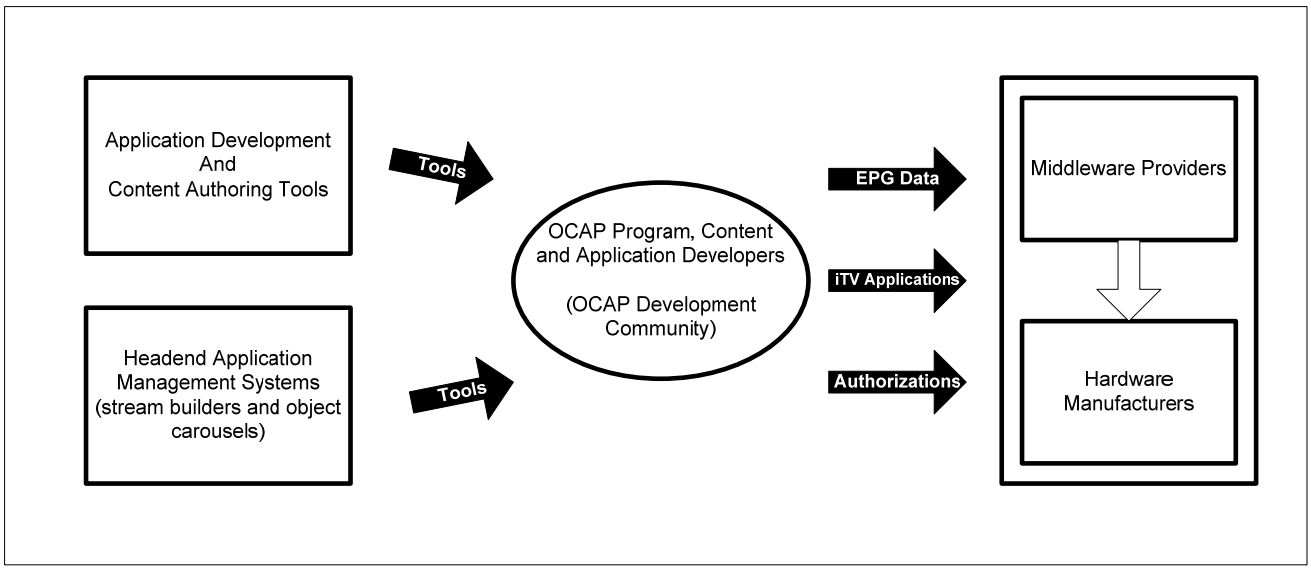

Figure 1 - High Level Diagram of OCAP Implementation

Additionally, the OpenCable environment allows multiple vendors to play in the headend space, providing functions and features previously provided by one device or vendor. As with many technological advances, increased choice bears increased complexity. Figure 1 highlights the new approach to set-top box development under an OCAP system. Various providers, vendors and systems now play under a defined specification to enable previously "built-in" functions.

UNIFYING THE SECURITY AND OCAP IMPLEMENTATION

Separable security and OCAP are currently viewed as independent issues and projects by the industry. However, when examined from the deployment and sustaining operations perspective, they can be viewed as extensions of one another. For an advanced security OCAP compliant device to connect into a cable system's network, it must first receive a series of downloads from both the systems managing the security and the systems managing OCAP functions. It must then continue to receive a series of data streams which provide necessary information and software required to sustain functionality. Therefore, from the standpoint of creating an enabling architecture to provision the devices, it makes sense to combine their functionality into a single service entity.

A. Separable Security Deployment

The first step an operator will need to undertake is the deployment of an advanced security capability. The implementation of either separable security solution, DCAS or CableCARD, is not a trivial task. Figure 2 shows the messages required to drive the CableCARD. While many of these messages and streams are already a function of existing systems, the OCAP compliant infrastructure may result in each message generator being independent.

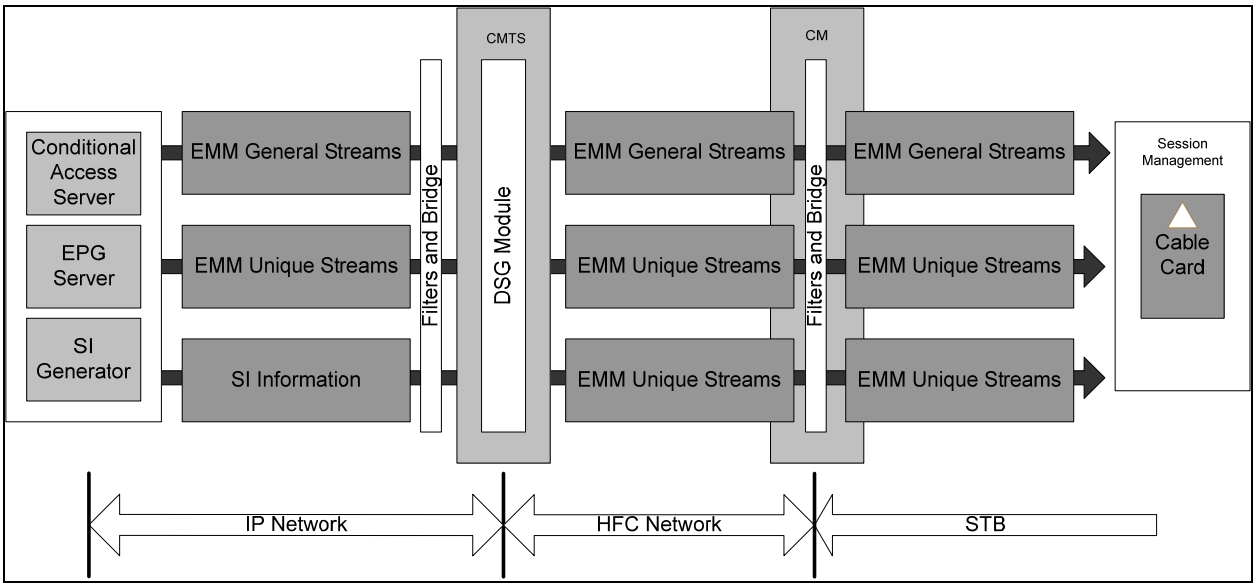

Figure 2 - Device Message Requirements

Independent servers providing EPG (Electronic Program Guide) listings data, and SI (System Information i.e., channel maps) are now necessary to ensure CableCARDs are initialized and operate in the consumer's home.

Figure 3 is the diagram provided by the FCC in its "*Report of the National Cable & Telecommunications Association on Downloadable Security*". This diagram highlights the steps required to initialize the DCAS device. As can be seen, once inserted into the consumer device and connected to the operator's network, the consumer device must communicate with an authentication proxy server located in the headend to initialize use of a system. This DCAS authentication proxy server sends the CAS download key to the set-top. Then the encrypted CAS image is sent to load the set-top box with appropriate encryption software.

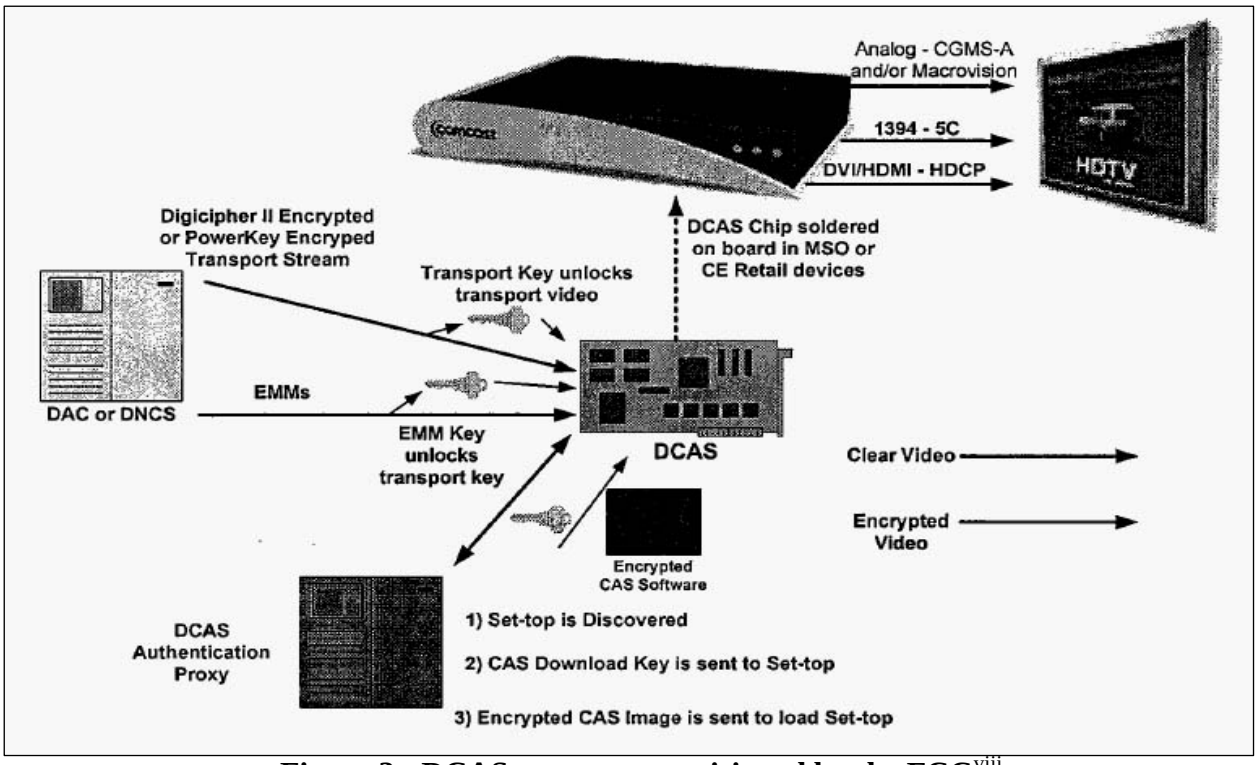

Figure 3 - DCAS process as envisioned by the FCC[viii]

Once the security system has linked with, and authenticated, the consumer device, it can then download the series of entitlements and other secure information necessary to work in conjunction with the configuration information included in the services.

Therefore, the first step in providing advanced conditional access requires that several new applications and servers be installed and operated by the operator. To simply initialize and begin communication with the set-top box in a separable security environment, the operator must now be prepared for an increase in equipment and expertise.

B. Basic Set-top Functions under OCAP – Middleware and Application Installation

Following the initialization of the security elements, the consumer devices must be given "personality data" in the form of software. In some cases, the consumer device must acquire the OCAP software stack, a middleware software component developed to enable multiple applications to interact together. Applications, like a programming guide or an on-demand ordering system, sit on top of the middleware. Operating systems (OS) are below it. The job of the middleware is to translate what lies at the root level for what sits above it. This, for example, allows an interactive trigger from a programmer to function without needing to know what version of OS is being used in a particular model of HDTV or set-top box.

Once the stack is available on the device and fully operational, the key software applications that will remain resident in memory in the consumer device will need to be loaded. Key functions such as the main user interface, including the EPG, and other basic functions to the network, like the

applications required to receive and decipher channel maps. Figure 13 shows in additional detail the OCAP stack.

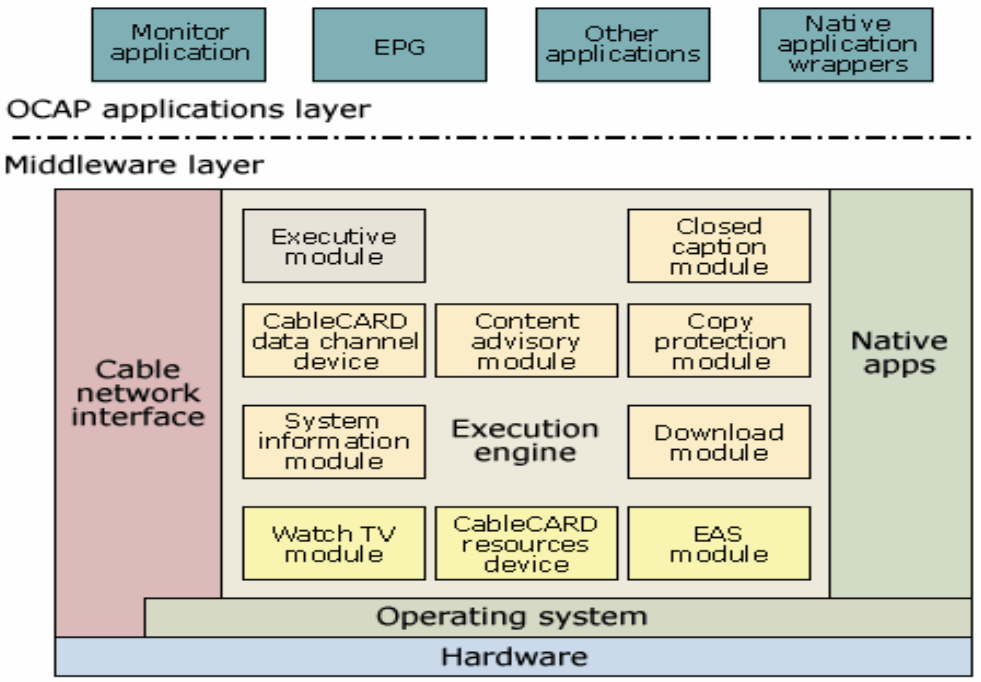

Figure 4 - OCAP Stack with Applications

Again, additional hardware will be required in the headend to load the middleware or applications. The software will be deployed using carousel file servers. Two methods are available for delivering these applications into the consumer device via the carousel file server. The first method uses the out of band data channel. The second uses the DOCSIS Set-top Gateway (DSG).

Once the middleware is installed on the set-top box, additional applications that are stored in memory in the consumer device can be installed. Examples of such applications are the main user interface or the EPG. The consumer device also has the capacity to download other applications that will reside in memory during the time that they are in use by the consumer. An example of this type of application is interactive games. The system will require one or more servers to provide these types of applications to the consumer devices.

Comparing this implementation to today's basic cable implementation shows a glimpse of the increased complications that come with the new age of cable television. The exurban operator will be challenged like never before. Even the larger system operators are concerned about the new challenges that lie ahead. In a recent article in *Communications Technology*, Chris Bowick, Cox's CTO, was quoted as saying: "… (OCAP) [is] a very complicated topic, and it's not just new set-top boxes and new software on set-top boxes …From a systems perspective, you have the addressable controller and the DSG that will be used in OCAP deployments for the two-way communications instead of the proprietary S-A and Motorola approaches we have today[ix]."

Implementation of either the downloadable security system or OCAP relies heavily on components not in use today by a cable operator. While every effort will no doubt be made by the numerous vendors involved in developing these systems to ensure smooth interoperability, the complexity of the initial deployment and long term operation will tax even the largest of system operators. Smaller market operators now managing their headends as "lights-out facilities", requiring little or no daily management or support, will find that the basic activities of simply adding authorizations or new set-top boxes will require complex interactive communications with local and regional security systems. This approach is beyond the technical and financial limits of many rural operators.

An OpenCable implementation, as depicted in Figure 5, is representative of what larger operators will most likely deploy. In addition to providing the fundamental services such as encryption and EPG, these cable systems will expand their competitive service mix by enabling customers with VOD, DVR and OCAP. However, Figure 5 also shows the number of headend servers and services growing substantially.

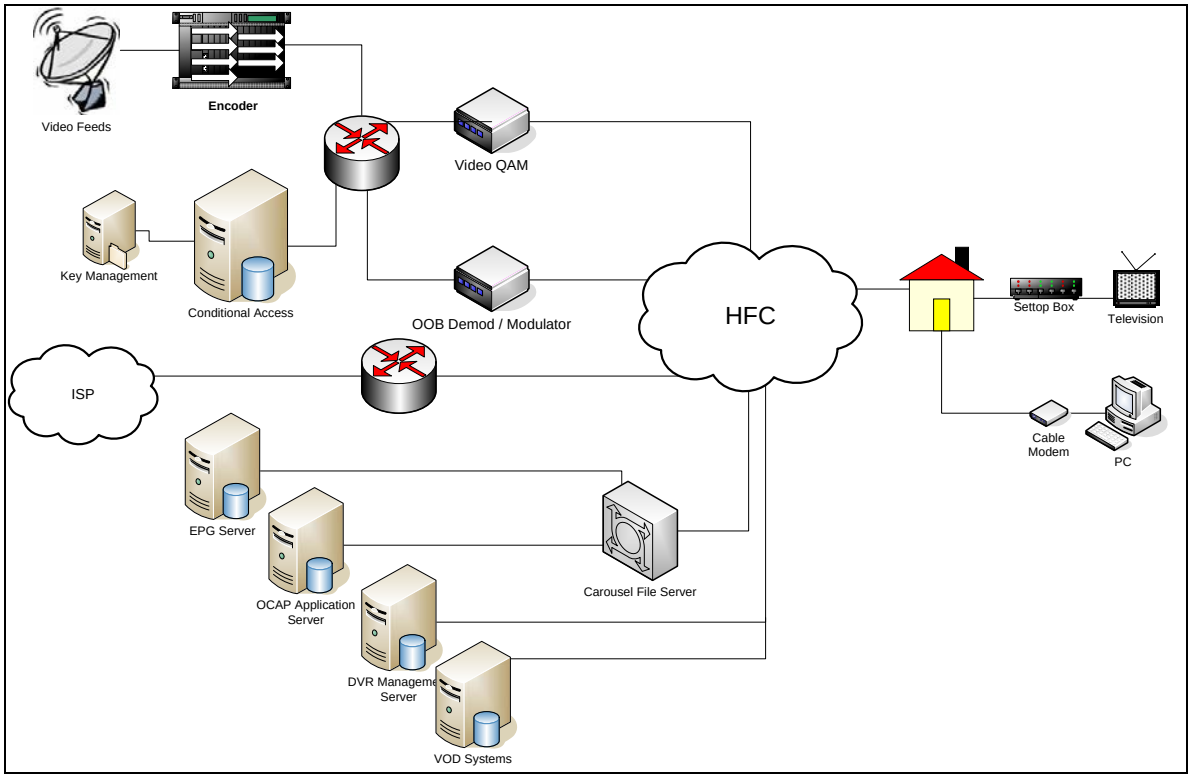

Figure 5 - Complex OCAP Implementation

DAY TO DAY OPERATIONS - ENTITLEMENT AUTHORIZATION

The small operator's task list has grown under the new FCC and OCAP guidelines.

- First and foremost, the operators must maintain control and function of the existing set-top box population. This value of this investment cannot be understated.

- Second, the operator must respond to FCC-mandated changes surrounding security. Changes in headend gear will be necessary in order to deploy the new security system(s).

- Third, the operator will need to support OCAP product offerings. Advanced services, which will drive revenue, will require the support of OCAP servers in the headend.

- Fourth, the operator must provide continuous updates to support the devices and functions that will be offered as the market continues to evolve.

- Finally, the operator needs to ensure continued operation of this system to authorize and manage these services and functions.

It is this aspect of continued operation that will be most taxing to an operator. New processes and procedures required to add set-tops, replace devices and ensure appropriate billing will overwhelm the lightly staffed smaller cable systems.

A. Set-top Authorization

As with a non-CableCARD set-top box, the service provider defines the types of rights needed to access the content. Through the CA system in use (DAC, NAS, DNCS) the ECM ciphers with the broadcast key according to the profile and generates a control word (i.e., the content encryption key). The controller sends the ECM and starts streaming the content ciphered with control word.

Following that communication, the CableCard deciphers the ECM (using the broadcast key) and checks the required rights relatively to the list of rights stored in the card. If the rights are correct, the card returns the CW to the decoder that will use it to decipher the received content. When subscriber rights have to be updated, an EMM is sent to the user's CableCard. It is ciphered with the broadcast key and contains the updating information (new rights, loss of rights, increase credit limit, etc.) and the Subscriber_Id.

B. OCAP Application Authorization and Operations

The previous section addresses the steps to authorize a service. This process is largely handled by the CA system with interfaces to new external devices. The authorization of applications, and the submission of necessary data to those applications, is a much larger and more complicated endeavor. Another look at Figure 5 shows the increased number of servers providing services to the consumer devices. Previous sections discuss the fact that the applications must be loaded on top of the OCAP stack. However, the entitlement of the cable customer to receive this application and the associated data streams must also be managed. Interfaces with billing systems and entitlement servers will be required to enable customers to receive the VOD client and EPG in accordance with appropriate authorizations.

A centralized authorization management system will assist operators greatly. However, because each application is likely to be developed independently, a seamless and unified means by which each carousel file server can be managed and controlled is not likely to exist for several OCAP generations.

ECONOMIES OF SCALE FOR THE SMALLER SYSTEMS OPERATOR

A. Centralized Service Bureau

As previously mentioned, the economics for deploying next-generation content distribution systems are very different for cable system operators serving exurban markets within the U.S. In fact, the vast majority of the 7,090 cable systems in the U.S.[x] serve fewer than 25,000 customers and a significant number of them serve fewer than 5,000 customers. The American Cable Association (ACA) represents 930 independent cable systems operators that serve 8 million U.S. cable households via 5,000 systems. This translates to an average of 1,600 customers per headend and ACA indicates that more than 1,000 of these systems serve fewer than 1,000 subscribers[xi]. Many of the ACA's members also participate in the National Cable Television Co-Operative (NCTC). NCTC represents 1,100 independent cable owners of 5,500 individual systems serving more than 10 million subscribers, which also illustrates the number of cable systems serving smaller, exurban communities across the country.

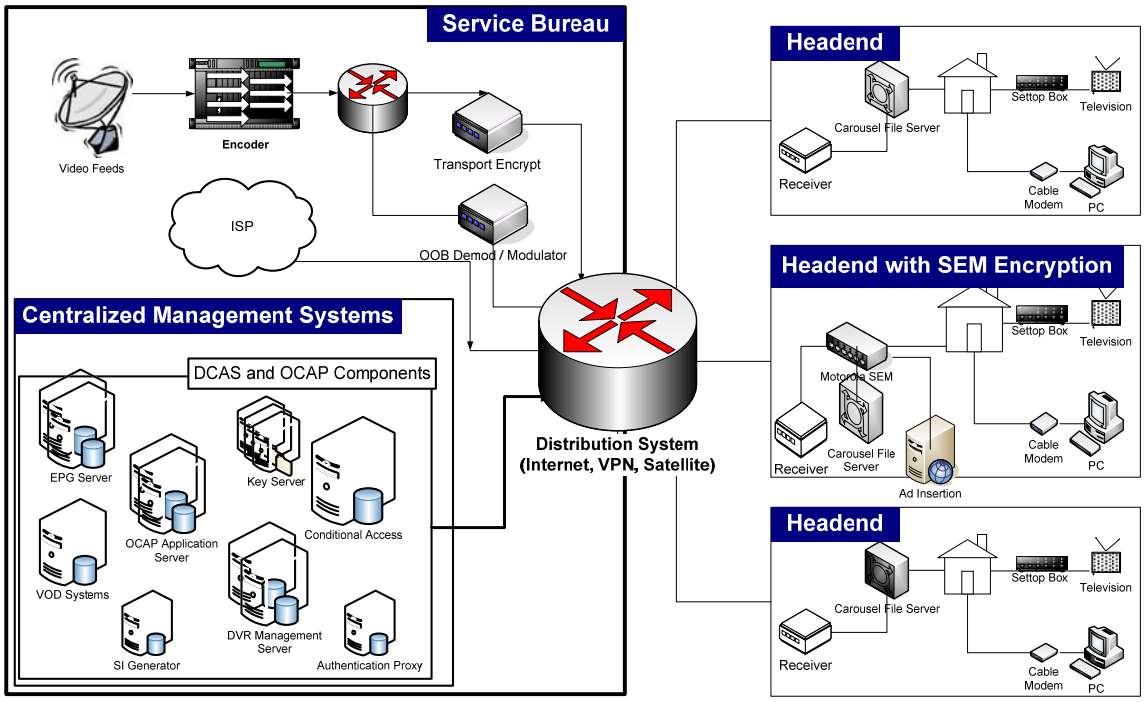

Figure 6 - Broad Deployment via Centralized Service Bureau

When we are examining how these markets will comply with the requirement for separable security and OCAP, it is important to note the additional limitations

of their current system architecture. In fact, the most recent wave of upgrades in these smaller markets was using 450 MHZ plant and equipment that came onto the market when larger systems upgraded to 750 MHz[xii]. Many of these small-market systems deployed digital video service using the first generation of digital set tops boxes.

The service bureau provides an economically viable solution to cable operators serving smaller markets by pooling many small systems to achieve economies of scale. This creates a single large installation of equipment and applications that mirrors or exceeds the economies of scale found in a large market. Staffing follows the same model. The service bureau can deploy a robust set of operations, technical engineering, and support personnel spread across the entire base of small cable systems. Because the staffing for a centralized approach equates to a small fraction of an FTE on a per system basis, a top-notch staff can be assembled to provide superior services.

In order to address the unique needs of each cable system, it will be important for the service bureau to identify and manage each configuration individually. Additional controls will need to be in place in order to ensure the security and integrity of each cable system's data.

For the service bureau approach to best serve the customer base, it needs to balance the benefits of ubiquity with individuality. The goal of both separable or downloadable security and OCAP is to offer a variety of choices into the marketplace. Offering a one-size-fits-all approach runs counter to the purpose of creating an open marketplace. Conversely, offering too many choices can increase the complexity of the operation and negatively impact the scale economics.

Regardless, each cable system needs to be treated as an individual entity. The number of and type of services deployed and the timing of each implementation will be unique for every market. The support structure of the service bureau should be supportive of each cable system's need to respond to local market demands, as operators move to offer choices that match the competitive alternatives.

Unilateral services such as unified server management, application certification and testing all ensure a quality offering to each headend. It is important that each configuration be validated and tested in a timely fashion. In addition, supplying redundant servers and high throughput systems for the entire customer base will help to ensure high availability and economies of scale.

Services from the centralized service bureau will require downstream connectivity from the service bureau via a satellite or terrestrial fiber-based data feed. The upstream requirements from the head-end to the service bureau can be managed using a secure VPN connection. Cable operators that are currently offering High Speed Internet services and/or VOIP services already have the connectivity to the Internet that is required for this upstream data channel. Now, as a result of these investments in IP-based services, cable system operators serving smaller markets possess many of the prerequisites for using centrally-supported conditional access and OCAP services for expanding their lineup of advanced digital video services.

Conclusion

Cable system operators, CE manufacturers and retailers, their customers and the regulatory community share a common vision for a fully open-cable content distribution environment that supports a wide array of devices and applications. Achieving this vision for an interchangeable world is a much steeper challenge for cable operators serving rural markets. However, their future financial viability depends upon being able to offer customers the choice, convenience, quality and ease of use that this next generation content distribution platform can provide. A centralized services bureau, which allows operators serving these smaller markets to outsource much of the capital and operating requirements of an OCAP infrastructure, represents an essential element in making the interchangeable world available to everyone.

---

[i] CableLabs' OpenCable initiative. See www.opencable.com
[ii] CED magazine, January 2007
[iii] CED magazine, January 2007
[iv] CableLabs' OpenCable initiative. See www.opencable.com
[v] "Don't Leave Rural America Behind", ACA, May 26, 2005
[vi] First FCC Report and Order: Commercial Availability of Navigation Devices (PDF). FCC (1998-06-24). Retrieved on December 26, 2006
[vii] Sonntagszeitung newspaper, March 18, 2007
[viii] U.S. Federal Communications Commission document: "CS Docket No. 97-80: Report of the National Cable & Telecommunications Association on Downloadable Security"
[ix] Interactive Momentum: Mike Robuck, Communications Technology, April 1, 2006
[x] NCTA - Key Industry Statistics 2006
[xi] ACA report to the FCC
[xii] CED magazine, January 2007

Contact Information:

Gary E. Traver
Senior Vice President and Chief Operating Officer

James A. Capps
Senior Director, Software Engineering

Comcast Media Center
4100 E. Dry Creek Road
Centennial, Colorado 80122
(303) 486-3800
www.comcastmediacenter.com