# EXTENDING CONDITIONAL ACCESS SYSTEMS TO SUPPORT DRM SYSTEMS

Balu Ambady
Cable Television Laboratories, Inc.
Bill Helms
Time Warner Cable, Inc.

*Abstract*

*Conventional implementations of content security by Multiple System Operators (MSOs) rely on hardware based broadcast Conditional Access Systems (CAS). However, competitors like IPTV providers, and Internet based movie-on-demand sites have started offering high value content using content protection based on software Digital Rights Management (DRM) systems like Microsoft WMDRM, and Real Helix DRM. It appears that content providers are increasingly becoming comfortable with the reduced level of security provided by DRM systems for certain levels of content.*

*Under currently available solutions, while the content is under CAS protection, opportunities to offer innovative content packages to the customer are preserved.*

*This paper describes architectural options where CAS protected content can be transferred securely from Set Top Box (STB) devices to Portable Media (PMD) or PC devices with DRM protection. This would allow the operator to provide an enhanced home networking and content usage experience to the subscriber.*

## INTRODUCTION

### Content Protection Domains

When user subscribed content is moving from the Operator's head-end device to a STB, and then on to a Home Network device, from a content protection point of view, the content may be considered to be moving between one of the three content protection domains as shown in Figure-1:

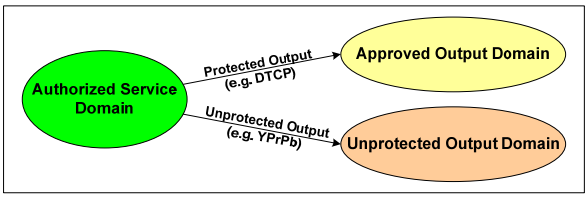


**Figure 1 – Content Protection Domains**

1) Authorized Service Domain (ASD)

Within the ASD, content is secured using the mechanisms provided by the MSO according to usage rules set by the Operator's provisioning system. Content is protected using CAS while it is transferred from the MSO head-end to the subscriber home, and by an ASD specified protection mechanism while it moves between one or more trusted devices that are part of the ASD network.

2) Approved Output Domain (AOD)

As permitted by FCC encoding rules[1], content may also be released to non-operator Content Protection (CP) or DRM systems that have been approved[2] by CableLabs®. When the content is released from the ASD to another CP system, it is considered to exit the ASD and enter the AOD. The content is still securely protected by the CP/DRM system and the encoding rules are enforced by the CP/DRM.

Several Link Protection systems like DTCP and HDCP, and DVD based recording solutions like VCPS fall under the AOD category. A PC based architecture, the OCUR (OpenCable Unidirectional Receiver) using the Microsoft WMDRM and Real Helix DRM systems for content protection also fall under this category.

3) Unprotected Output Domain (UOD)

Lower value content that require only minimal levels of protection, or no protection at all may be released to the UOD, for example to the unprotected Analog video outputs.

High Level Design Goals

While a large number of the devices that are capable of serving MSO delivered content fall under one of the three domains described earlier, many new devices like PMDs and cell phones do not readily fall under these domains. In order for the MSOs to offer the best entertainment experience for the subscriber, it is desirable to bring more of these new devices either under ASD, or AOD. In order to join the ASD or AOD, these devices must be capable of providing sufficient levels of content protection, as well as be capable of supporting the MSO defined usage rules. We offer some architectural options to achieve this goal.

The options provided in the next section provide solutions while striving to attain a balance between the needs of the main stakeholders and their needs:

1) Subscribers

- Ease of use/transparency
- Fair use
- Interoperability with other devices in the home

2) Content Provider/owner

- Sufficient protection of owner rights
- Monetization of content

3) MSO

- Ensuring a link between services provided and payment received
- Support for flexible business models, freedom to innovate
- Leverages existing infrastructure where possible
- Provide consistent MSO branded experience

4) Device manufacturer

- Easy to license technology
- High level of interoperability
- Freedom to innovate

## ACHITECTURAL OPTIONS

We offer four solutions to achieve the goals outlined above. Three of the solutions described below use Operator provided security mechanisms and thus allow the content to stay fully within the ASD, and the fourth option provides a “bridge” mechanism from ASD to a third-party DRM solution.

In the case of the three ASD solutions, encoding rules permit the operator to extend the usage rules beyond the limited usage rules expressed using the 8-bit Copy Control Information (CCI) bits[3]. This would allow for new business models for the MSOs,

and more choice for the subscriber. For example, current CCI is not sufficient to express a "rent" model where a subscriber may rent a digital content for 7 days.

In the case of the bridge from ASD to the native DRM space, certain additional encoding rule restrictions may apply.

1) Hardware ASD

This architectural approach would require all devices that are interested in joining the ASD to embed the Downloadable Conditional Access System (DCAS) Secure Micro chip and store the associated keys, secrets and Root of trust. An architectural diagram of a typical implementation of home networked ASD Host with a DVR application is shown in Figure-2.

The System on a Chip design would allow the Root, critical security parameters and keys to be securely stored on the Secure Microchip. The software modules that support ASD functionality can be securely downloaded on to the device based on this Root of trust. The ASD modules are developed by an ASD vendor, and all vendors follow a standard set of protocols, content formats and encryption schemes. In addition to allowing multiple ASD vendors to participate in this eco-system, this has the added advantage of allowing the same ASD infrastructure and standards to be utilized by both MSO leased and retail devices.

The CA protected content is converted into ASD protected content. Security Packages are created that store the usage rights to be kept with the encrypted content. The Secure Micro is responsible for key generation during encryption, and for retrieval of keys during decryption. The Host Transport processor is responsible for the actual encryption/decryption of the content.

Devices that belong to the same ASD are managed by the ASD controller by using a "Trusted List" that identifies the devices that are tied to a subscriber billing account.

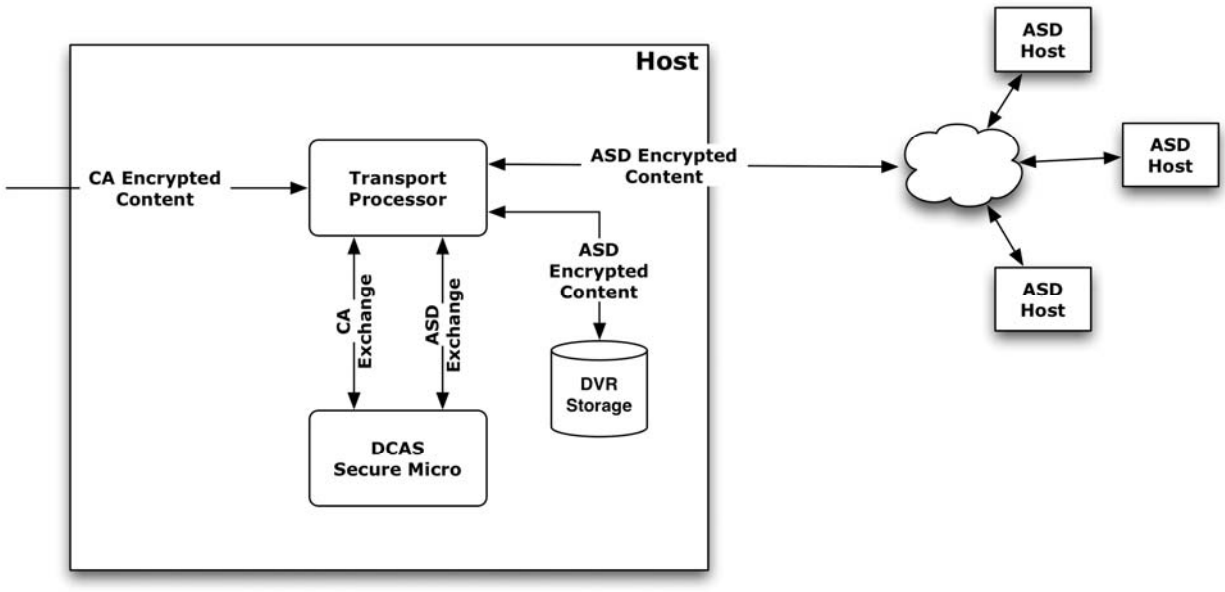


**Figure 2 – Simplified DCAS ASD Host Block Diagram**

2) Cable DRM (CDRM)

An alternate approach would be for the Cable industry to develop its own DRM solution that can run on a variety of devices that do not have the Secure Microchip or other Hardware secure storage for keys and other security parameters. Ideally, this would be a Platform/Operating System (OS) independent technology that is easy to implement on a wide variety of devices like cell phones and PMD made by different manufacturers. Content security will be based on obfuscation of keys and code, and software renewability.

The architecture for such a solution is shown in Figure-3. The components are similar to typical DRM systems, there is a DRM Client on the portable device, a Controller providing Keying, Registration and Individualization for the Client, a License Server that packages the content in DRM format and also enforces Licensing rules, and a Content Server from where the Client can access DRM protected content.

In a simple use case, as the 1st step a personalized copy of the Cable DRM Client that is uniquely tied to the PMD is securely downloaded. The 2nd step, high value content that the subscriber is authorized to receive is moved with Conditional Access protection to the Content Server, in this case the STB. The 3rd step, as authorized by the License server, the STB transcrypts the content in to CDRM format. The 4th step, the PMD can download this content from the STB and consume it as allowed by the CDRM usage rules.

Since the Cable DRM devices use the Operator's protection system, devices implementing this are part of the ASD. These devices support the extended usage rules using standardized protocols as in the case of Hardware ASD solution.

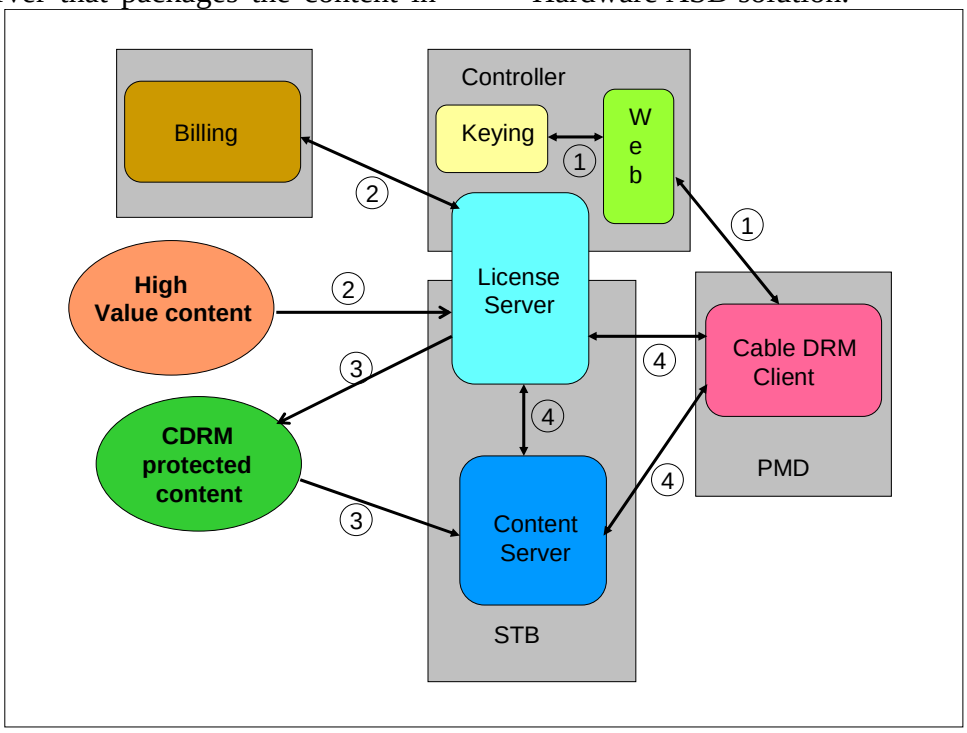


**Figure 3 – Cable DRM**

Because of the relative ease of circumventing Software DRM systems, the DRM Client should be carefully designed to preserve execution integrity and algorithm secrecy, prevent tampering, impersonation, and input spoofing.

These security goals are usually achieved in conventional software DRM systems by using the following mechanisms:

- Use of information diversity and complexity
- Use of masking techniques to mask: control flow, data/code itself, location, and usage
- Use of one-way transformations, temporal and spatial diversity
- Use of Index computations, aliasing techniques
- Use of "bad programming" practices: e.g., use of pointers, goto
    - Hard to debug (on purpose)
    - Prevent Dynamic analysis (during execution)
- Use of encrypted functions
    - Integrity Verification Kernel
- Use of "white box" techniques
- Resistance to side channel attacks ("grey-box") - however, this may be less of a concern as S/N ratios are significantly degraded in GP
- Software Key hiding
    - Many skews to prevent domino effect (of hacks)
- Use of Protected Media Paths
    - Utilize OS support (e.g., Vista PVP)
    - Disk/CD/DVD drive solutions
- Secure boot up/firmware
- Encrypted/protected memory

Other design attributes supporting security should include:

- Secure clock
    - Anti-rollback time
    - Secure (external) time source
- Secure random number generation
- Support of standard cryptographic algorithms
- Support for secure Proximity checks
- Efficient software implementation
- Robust Revocation, and Renewal mechanisms
    - Breach response readiness
    - Heart-beat checks
- Secure DRM infrastructure
    - Secure build servers
    - Secure (firewalled) download portals
- Ability to add features later
    - Watermarking, fingerprinting

- Ability to use Trusted Platform Module

Similar to the Hardware ASD, the CDRM would allow the MSOs to use a common messaging protocol, encryption scheme, data structures and extended usage rules on all of the devices on which the CDRM Client is available.

3) Software ASD

This is a modified approach that would combine the options-1 and 2 above, this option would allow existing CAS/ASD vendors to port their ASD clients into the Portable devices. The architecture and requirements for the Software Client are similar to the CDRM case, except that some of the messaging protocols may be proprietary to the CAS/ASD vendor. Another difference is that instead of a single DRM, there would be multiple CAS/ASD systems, one for each vendor.

Since the main difference between Hardware ASD and the current solution is that the security is based on obfuscated software instead of hardware stored keys, this solution maybe considered as a "Software ASD" implementation.

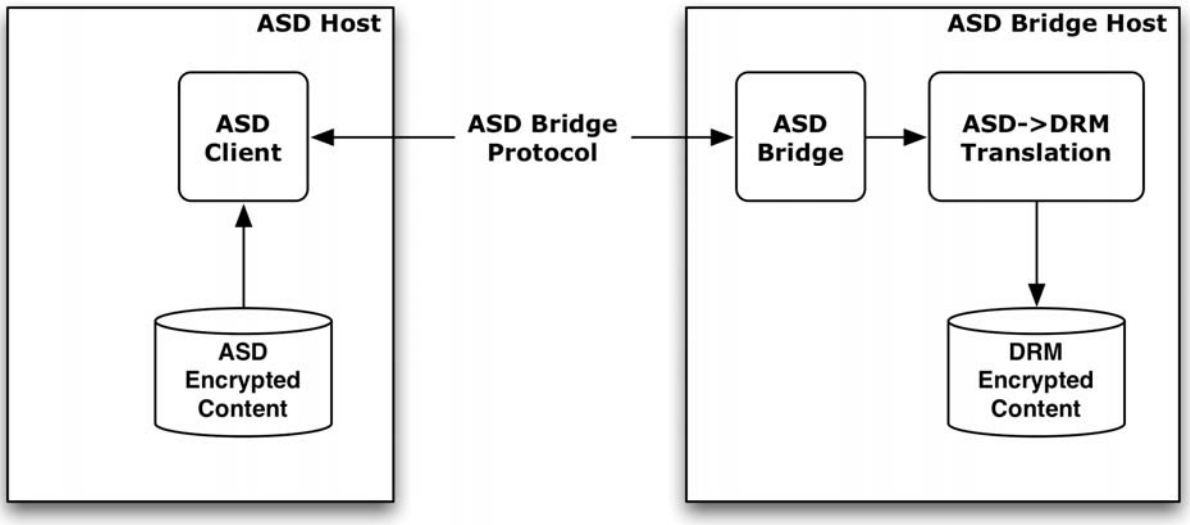


**Figure 4 – ASD/DRM Bridge**

4) ASD/DRM Bridge

The ASD/DRM Bridge model shown in Figure-4 is a compromise between the previous three models. It uses ASD protocol to exchange content with the ASD Bridge device (e.g., PMD). However, the native DRM is responsible for securing the content and obeying the MSO usage rules contained in the ASD protocol.

Of course, this requires that the bridge device translate from the ASD encryption and protocol to the native DRM encryption and protocol. Under this model, the implementation of the bridge to DRM is the responsibility of the device vendor, rather than the operator or ASD vendor.

Comparison of Options

The relative advantages and disadvantages of the four options outlined above are shown in Appendix-A.

## CONCLUSIONS

Depending on the implementation timeline, complexity of implementation, ease of licensing, cost and other factors, the Operator may select one of the four options presented above. An ASD solution that embraces the new generation of Portable devices and other Home Networked devices would help to enhance the subscriber's entertainment experience and thus would help to strengthen brand loyalty.

## References


1 The FCC Second Report and Order (FCC 03-225) Section VI-B. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-225A1.pdf

2 The FCC Second Report and Order (FCC 03-225) Section V. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-225A1.pdf

3 SCTE 41 – POD Copy Protection System http://www.scte.org/documents/pdf/ANSISCTE412004.pdf


## Appendix – Comparison of Options

| | **Hardware ASD** | **Cable DRM** | **ASD Client** | **DRM Bridge** |
|---|---|---|---|---|
| **Complexity of Licensing** | Low | Low | Low | High |
| **Cost to MSO** | High | High | Medium | Low |
| **Complexity of Development** | High | High | Medium | Medium |
| **Interoperability** | High | High | Medium | Medium |
| **Extended usage rules** | Yes | Yes | Yes | Yes with possible restrictions |