



**Widevine<sup>®</sup> Technologies' DRM/CAS Client  
Platform Minimum Operational Environment  
*Common Reliance Proposal for Downloadable Security***

# Table of Contents

<b>1</b>	<b>Overview.....</b>	<b>3</b>
<b>2</b>	<b>Software (Network Renewable) Versus Hardware (Static) Functions of the DRM.....</b>	<b>5</b>
<b>3</b>	<b>Analog Copy Protection Requirements.....</b>	<b>6</b>
<b>4</b>	<b>Dealing with Identity.....</b>	<b>6</b>
<b>5</b>	<b>DRM Client Operational Environment.....</b>	<b>7</b>
<b>6</b>	<b>Security Robustness Guidelines for TV Receiver Devices.....</b>	<b>8</b>

# 1 Overview

Recently, the FCC issued a mandate to US video operators ascertaining if they are in compliance with the FCC's separable security initiatives. In paragraph 35 of the Commission's Second Report and Order on the implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices, the FCC stated that downloadable security technology would comply with their rule.

The Commission specifically states:

"...[T]he rule should be interpreted to require the physical separation of conditional access and other navigation functions only in the case of hardware-oriented conditional access solutions or other approaches that may preclude common reliance on the same security technology and conditional access interface. Downloadable security comports with the rule's ban on the inclusion of conditional access and other functions in a "single integrated device" because, by definition, the conditional access functionality of a device with downloadable security is not activated until it is downloaded to the box by the cable operator. To the extent a downloadable security or other similar solution provides for common reliance, as contemplated herein, we would consider the box to have a severable security component..."

However, for this mandate to be successful there must be a common reliance standard in addition to a downloadable security mandate. Downloadable security can result in significant cost reduction to the device manufacturer, video service operator, and the consumer. But to realize this cost saving the device manufactures require a definition of the minimal hardware requirements under which the conditional access system may function.

The goal of common reliance is to minimize the variation in terms of hardware and software that must be supported by the consumer electronics device. The idea is to identify a common and minimal set of operating environment requirements in which the downloadable security element functions.

In order to achieve common reliance and to innovate in the changing video consumption landscape as described below we make this proposal for a DRM Client Platform Minimum Operational Environment.

Moreover this proposal moves the development and integration burden off of the CE device manufacturer and places it where it belongs, on the DRM/CAS vendor. By providing a common and flexible environment for the downloadable security module the CE manufacturer can be assured that their device may be used on any operator's

network. In order to compete effectively the DRM/CAS supplier would need to develop solutions that work in this common environment.

The advent of Video on Demand (VOD), in-home networking, and new distribution methods are creating a move from traditional Conditional Access Systems (CAS) to use of Digital Rights Management (DRM) technologies.

Each method (CAS and DRM) has its own set of technical and business advantages and disadvantages. For the MSOs and the consumer electronics industry to fully capitalize on new business opportunities consideration of a blending or hybrid of the CAS and DRM functions is required. This will eliminate the need for the bridging of CAS to DRM. It will also allow for greater control of the MSO content even if it exits the authorized service domain.

Thought should be given to targeting content protection so it persists from the time the content enters the MSO's domain (network) until the content no longer requires protection (value has diminished to the point where content protection cost exceeds the need for protection). This can be accomplished by applying content protection (in this case content encryption) to the content itself rather than to the transport, media, or the network. Targeted encryption must be done in a manner that does not adversely affect video servers, multiplexers, network transitions and other content caches.

Due to the changing nature of the head end and network components in the next generation networks driven by concepts such as video on demand, additional flexibility in stream handling by the Consumer Premises Equipment (CPE) is required. Allowing content protection to flow through the initial home gateway to other consumer electronic devices without transform also requires separation of encryption from the transport and flexible decryption modules.

If targeted encryption is used, the content protection can even persist on removable media such as writable DVDs or Secure Digital Cards. Traditional STB chip-based solutions lack this type of flexibility.

In addition to providing flexible content packet handling, the use of a software based authentication module like a downloadable security system will provide the greatest flexibility and ROI on the security investment.

Content security decisions and design goals should comprehend that no security solution is "unbreakable" so instead the system must be flexible and cost effective. The real question is: "What security is good enough to allow the timely acquisition of premium content?"

## 2 Software (Network Renewable) Versus Hardware (Static) Functions of the DRM

Consumer premises electronics and system on chip implementations for content security solutions of the future shall be capable of supporting completely software implementations of the DRM client.

### Items that shall be placed under software control:

1. Key management
2. ECM and EMM extraction from Video, insertion to video, and manipulation
3. Parsing of the video transport packet prior to decode by the CODEC to determine what portions of the stream need to be passed to the hardware decryption module (if hardware decryption module is used).
4. Software decryption of the content stream allowing for change of algorithm without wholesale replacement of legacy devices and/or simulcasting content.
5. Determination of algorithm used, mode, bit lengths, initialization vector, etc.
6. Software access allowing medication of decryption packets by the DRM client

### Basic Crypto Hardware functions and interfaces if provided shall include:

1. Standard Crypto libraries/execution for both Symmetric and Asymmetric Cryptography.
2. Advanced Encryption Standard AES (see ATIS - 0800006) and RSA at a minimum should be provided.
3. Crypto Lib calls should include the ability to retrieve and return buffers of data and perform standard Crypto Library functions such as:
  - a. Encrypt
  - b. Decrypt
  - c. Key generation
  - d. Create Digital signature
  - e. Verify Signature

In summary: Avoid hardwired solutions that prohibit encrypted content from being exported to software. Provide an API where the ECM stream and all scrambled single program MPEG2 Transport packets are provided as contiguous buffers to the descrambler component for descrambling and return. If hardware decryption is used, the API should be a generic cryptographic interface where buffers of encrypted bytes, keys and algorithm configuration information are passed into the hardware. Clear text buffers must be returned to the calling application. Note this allows watermarking of the

clear compressed content before decode. The calling application would hand off the clear content to the decode module. If software decryption is used, the CPU must be sufficiently powerful to have enough free time available when playing back a 19.2Mbit/second MPEG2 stream to be able to perform AES-128 CBC (as defined in the ATIS Standard ATIS - 0800006) decryption at a rate of 19.2Mbit/second without impacting the user experience.

### 3 Analog Copy Protection Requirements

In addition to CAS/DRM and encryption, analog copy protection is required. The device should have CGMS-A capabilities and API's to trigger CGMS-A from the CAS/DRM client. The device must be able to generate at least the primary forms:

- NTSC: Line 20 (IEC 61880), Line 21 XDS (EIA/CEA 608)
- PAL: Line 23 (ETSI 300 294)
- Macrovision's ACP is often also a requirement of the studios.

### 4 Dealing with Identity

The device shall be designed in a way to allow the DRM client to ascertain a device identity. Device identity is best based upon the use of device fingerprinting. Device fingerprinting may include some of the identifiers listed below plus others. The following describes the concept of a Finger Printer, which could be found in the DRM client.

**Finger Printer:** The fingerprinting module uniquely identifies a client or server computer in the context of a system. A Fingerprint is made up of a number of elements specific to each fingerprint. These are hereafter called Ridges. Each Ridge is an element of a fingerprint that provides information to the fingerprint making it unique from all other fingerprints. Some examples of Ridges are digital certificates, hardware serial numbers, operating system version numbers, Internet protocol address and physical memory size. Each Ridge added to a Fingerprint refines the identity of the system until it can be uniquely identified within a system. The combinations of all the Fingerprints create the Handprint or System Fingerprint that uniquely identifies the personal computer, server, set top box or device within the system. The order of each of the fingerprint groups and individual Ridges affects the resulting Fingerprint and Handprint. This feature means that each user of the Fingerprint technology can generate a unique fingerprint and subsequent Handprint even though the core Ridge information being utilized is the same.

The fingerprint can be combined with a physical smart card or a Unit ID found in the SOC if desired in order to add the secure identity characteristics of the physical card to the device fingerprint while maintaining the flexibility and power of the downloadable security. This is sometimes done in systems where device identity is inherently weak and where the cost and inconvenience of the physical card is not a concern.

#### **4.1 Minimum Device Ridges to be available for the DRM client**

1. At least 1K bytes of non-volatile memory for each content security system's exclusive use
2. A mutually agreeable factory provisioning process to load a DRM specific or shared digital certificate into the 1K store
3. Application accessible unique Processor ID
4. Application accessible unique BIOS ID
5. Application accessible unique STB ID (Motherboard)
6. Application accessible unique hard drive ID (if hard drive is present)

### **5 DRM Client Operational Environment**

The device manufacturer shall provide robust development tools/environment. This provides a wide choice of tools and libraries, such as the following:

1. C, C++ compiler, preferably ISO C++98 ISO C90 compliant
2. ASM
3. ISO/Ansi C++ 98
4. Symbolic source level debugger

Additionally, the device manufacturer shall have operating system support for:

1. Preemptive multi-tasking or multi-threading OS with mutual exclusion synchronization objects provided
2. System health
3. Sync objects
4. Events
5. Device add/remove
6. Application startup notification

7. Directory/file access/delete add notification
8. Device driver binding
9. Must support dynamic loading of modules for update purposes.
10. Socket-like network support for UDP, TCP, and Multicast or some other out of band method for delivering EMMs and interactive TV functions.

It is recommended that a small set of operating systems be selected in order to minimize the porting effort required by the DRM/CAS vendor. This is something to be considered by the national standards bodies.

## 5.1 Tamper Resistance/Detection/Response:

Some level of tamper resistance, detection and response mechanisms should be provided by the hardware manufacturer. These hardware tamper mechanisms should allow for supplementation by software tamper protection methods.

If hardware tamper resistance is not provided then the DRM client shall be self protecting.

## 6 Security Robustness Guidelines for TV Receiver Devices

The TV receiving device should be designed and manufactured in such a way to comply with the following security robustness rules or software (network renewable mechanisms must be provided to ensure robustness):

1. The receiving device should not expose any mechanism through probing points, service menus or functions that will enable somebody to defeat or expose any of the implemented security measures.
2. The receiving device should have an externally non-readable and non-writable Boot-loader.
3. All code loaded by the Boot-loader should first be authenticated by the Boot-loader.
4. Internal keys and decrypted content should be protected from any external access. This includes physical access by monitoring data busses. This also includes access via data interfaces like Ethernet ports, serial links and USB ports.
5. The receiving device should implement tamper resistant key protection.

6. The receiving device should implement intrusion detection.
7. The receiving device should trigger an alarm and may erase keys at the detection of any security related intrusion.
8. The receiving device should be designed and manufactured with one or more unique parameters stored in read-only memory. These values should be used to uniquely identify the receiving device during the authentication process.
9. The receiving device should protect against the external revealing or discovery of any unique parameters that are used to uniquely identify the receiving device.
10. The receiving device should protect against any attempt to discover and reveal the methods and algorithms of generating keys.
11. Non-encrypted content should not be present on any user accessible busses. User accessible buses refer to buses like PCI busses and serial links. User accessible buses exclude memory buses, CPU buses and portions of the receiving device's internal architecture.
12. The flow of non-encrypted content and keys between both software and hardware distributed components in the receiving device should be protected from interception and copying.
13. Software functions should perform self checking functions to detect unauthorized modification.
14. The receiving device should protect against the disabling of the anti-taping control functionality.
15. The receiving device should disable the decryption process of content after the detection of any unauthorized modification of any of the software functions involved in the security implementation.
16. The receiving device hardware components should be designed in such a way to prevent attempts to reprogram, remove or replace any of the hardware components involved in the security solution on the receiving device.
17. The receiving device should disable the decryption process of content after the detection of the reprogramming, removal or replacement of any of the hardware components involved in the security solution of the receiving device.