

CI Plus Test Strategy

Abstract

As CI Plus gains acceptance among network operators, OEMs, and content owners, we are seeing an increasing rate of CI Plus system deployments throughout Europe. CI Plus allows premium HD content to be securely distributed, ensuring that only authorized receivers can handle the content. Because of the potential liabilities involved, it is critical that CI Plus devices adhere to all robustness and compliance rules, as mandated by the CI Plus LLP.

The same requirement of secure HD distribution was addressed in 2003 by the US OpenCable consortium, driven by CableLabs. OpenCable identified the need for extensive testing and thorough certification procedures. The CI Plus community is working toward the same goals.

This paper outlines the current test approaches, identifies areas of particular concern from both a technical and business perspective, and offers recommendations for addressing them.

Problem Summary

The DVB-CI specifications define a Common Interface between a host device (e.g. TV or STB) and a removable CAM (Conditional Access Module). The intent was to come up with a standard that allows:

- a) Pay TV access on retail devices
- b) Easy deployment of multi-vendor leased devices

With the adoption of the DVB-CI standard, manufacturers can design host devices that are compatible across heterogeneous broadcast networks, and take advantage of a well-defined CA interface for rights-based content access.

While DVB-CI accomplished many of its objectives, it needs to be enhanced to support the requirements of premium HD content.

One of the limitations of the DVB-CI specifications is that it exposes the content in the clear after it has been descrambled in the CAM on a user accessible bus (PCMCIA), thereby violating all the robustness rules associated with the licensing of HD content

The CI Plus specifications address the security limitations of DVB-CI with the addition of copy protection across the CAM-host interface. The CAM determines if a host device is entitled to the copy protected content, and if so, sends it to the host using well-established encryption technologies.

This is only a part of the security equation. CI Plus also adds the ability to control the content all the way to the host outputs, through Copy Control (usage rules) settings. If the content owner does not want to permit any copies to be made, it can be accomplished simply, through a clearly defined interface. This is especially important (and contractually mandated) for HD content.

It is clear that today, Pay TV requires modular CA, protected interfaces,

and protected outputs. It is equally clear that these demands mean an increased need for a comprehensive test strategy.

CI Plus Architecture

The CI Plus solution leverages and expands the work done by OpenCable for functional requirements and security interfaces.

Specification	Date	CA support	CP support
DVB-CI	1997-Feb	Yes	No
OpenCable	2000-April	Yes	Yes
CI Plus	2008-May	Yes	Yes

OpenCable Approach

The OpenCable specifications were released in 2000. They include a removable CAM (CableCARD), protected CAM-Host interfaces (CCIF and CCCP), and protected host outputs. The first compliant devices were deployed in 2003, after undergoing a thorough certification process. Today over 600 retail Unidirectional Cable Ready Products (UDCP) have been certified, verified, or self-verified for use with CableCARDs, and over 16 million leased set-top boxes deployed.

The CableLabs Host and CableCARD acceptance test plans (ATPs) cover core functionality, network interoperability, and security. These are published specifications, available to any manufacturer who submits a product (host or CableCARD) for certification.

The overall certification process is as follows:

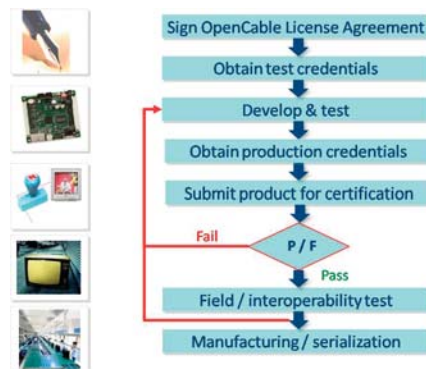


Figure 1: OpenCable Certification Process

CI Plus Solution

The CI Plus specifications were first introduced in 2008, and within a year have reached the point where network operators are deploying CI Plus-based systems. This rapid adoption shows that the specs are well-designed, but also emphasizes the need for compliance testing.

The CI Plus specifications assume a baseline DVB-CI implementation, and add:

- a) Copy Protection support, including CAM-host interface and receiver outputs.

b) Extensive interactivity support using MHEG, with support for streaming applications and CAM module-based applications.

For the most part, the overall certification process for CI Plus devices (host and CAM) closely resembles that of OpenCable.

One key difference between the OpenCable and CI Plus certification processes is that products are submitted with test credentials, and only given production credentials after certification.

Another differentiation is that the OpenCable ATP has an end-to-end

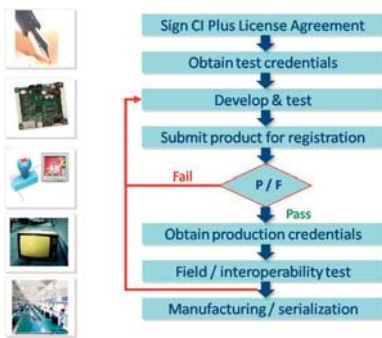


Figure 2: CI Plus Certification Process

coverage focus, while the CI Plus certification process is limited to security functionality. Core compliance and network interoperability are the responsibility of the individual operators and device OEMs.

Testing Requirements

We have seen that CI Plus testing must be performed throughout the entire development, certification, and deployment process.

The most basic strategy for interoperability testing is simply to use an actual CAM to see how the host device behaves on an operator's network. While this does give an initial indication of compatibility, it has several significant limitations:

- a) Lack of feedback. If a problem is detected, there's no reliable way to determine if the problem lies in the network, the CAM, or the host.
- b) No flexibility. There is no mechanism to intentionally alter the behavior of a CAM when testing a host. This is by design, and fully appropriate for a real module. It is not, however, well suited to a test scenario.
- c) No negative testing. Even when everything works properly under normal operating conditions, it's important to make sure everything works as expected in error conditions.
- d) Limited coverage. The DVB-CI and CI Plus specifications represent a large body of requirements. Each of these requirements should be explicitly verified. A simple CAM does not have the control and observation points that are necessary to accomplish this.

The solution to this testing problem is a comprehensive protocol analysis tool.

Test Strategy using HPNX DVB™

To make CI Plus a viable technology, device OEMs need to be confident that their products will be not only compliant with the letter of the DVB-CI and CI Plus specifications, but also ready to support the full breadth of content configurations and service applications that are allowed by the standards. This support must cover the useful life of the device, with-

out requiring expensive support calls or frequent firmware updates.

At the same time, CI Plus network operators expect to be confident that their current and planned offerings will reach their subscribers on all the generations of TV and Set-top equipment, without any distinctions in performance or functionality. The promise of any modular Pay-TV architecture is fulfilled when the devices are verified to be truly transparent to the service.

Digital Keystone is providing an advanced certification tool, HPNX DVB, to address these requirements by providing a network- and service-independent test and validation capability. HPNX DVB is an extension of the industry-standard HPNX Pro tool, and provides content security development and validation features for DVB CI Plus receivers. It consists of a specially designed hardware-based CAM emulator card and a PC appli-



Figure 3: HPNX DVB test system

cation. This combination allows the user to trigger and analyze all CAM-host communication (including critical security components), force negative test cases, and validate the behavior of the host against all DVB-CI and CI Plus requirements.

The recommended test approach uses HPNX DVB to validate:

- a) Hardware interface. Identify host type (DVB-CI or CI Plus), select desired CAM emulation mode (DVB-CI or CI Plus), discover host resource capabilities, perform physical measurements (temperature / voltage).
- b) Security implementation. Perform CAM-host pairing and authentication, configure SAC (secure authenticated channel), configure desired CCI (content control) settings, trigger real-time scrambling.
- c) System control. Generate and trigger MMI messages (DVB-CI and CI Plus), select and send MHEG-5 applications (built-in or custom).
- d) Protocol analysis. Parse, display, and filter all messages (APDU, SPDU, TPDU), capture and analyze CAM-host traces, perform SI table parsing and TEI analysis.

After going through this list of test operations, there will be a high degree of confidence that the host device is working in accordance with specifications and any network-specific conditions.

Further Resources

Further resources and product details are available at www.digitalkeystone.com



Paolo Siccardo
President, CEO
Digital Keystone