

Removable Security Myths and Realities

Background

CAMS, CableCARDS and PODs are essentially different variants on the same subject of separating security from the rest of the video delivery infrastructure that a service provider uses to provide Pay-TV services to its subscribers. In Europe the DVB standardized its efforts under the term CAM (conditional access module) while in the US the same topic was addressed by the FCC in carrying out directives of a 1996 telecom law resulting in the mandatory provision by cable operators of what was originally known as POD and now is known as CableCARD and Tru2way. This standard was also widely adopted in Korea. Outside of the US and Korea CAM is more widely used and therefore in the remainder of this article the abbreviation CAM will be used to represent both CAM and CableCARD.

The physical CAM that is inserted into the host device is a PCMCIA type II card which handles decryption of video, and makes sure that only people that have paid for the channel may view it. A host device is a device capable of decoding and rendering the content after it has been descrambled and may be a set-top box (STB) or an integrated digital television (iDTV typically means that the digital tuner and demodulator are also included in the television), or even a PC.

CAMs descramble a Pay-TV signal (without respect to the actual format of the underlying signal) and so therefore, in principle, provide access to content in any format (MPEG2, MPEG4, SD, and HD signals (obviously this is implementation dependent so care must be taken to ensure that a particular CAM does implement HD or any other format). In addition, as the CAM contains the underlying security technology integrated inside (Conditional Access), it is capable of enforcing controls such as Parental control that are typically enforced by the CA system i.e. the CAM will communicate back to the host device if a pin code needs to be entered for a parentally controlled channel and will ensure that this is enforced.

Use of CAMs in PayTV

Historically service operators have been lukewarm in their support for both CAM and CableCARD. There are a number of reasons for this and often it comes down to a business decision about how to ensure that they keep as many subscribers as possible to their service. Some of the historical reasons are outlined here

1. The traditional model of pay-tv has been that an operator provides STB as part of the commercial proposal to a subscriber – this is typically “rented” to a subscriber and used to access a particular operator’s service. Historically this model has been very successful and despite the initial capital expenditure required by an operator to purchase and distribute the STBs, he quickly recovers his investment and indeed over the lifetime of the STB (7-10 years often) can produce a significant ROI by renting the boxes. In this scenario it is clear that it is not the major concern of an operator to ensure that a subscriber can use the STB to access competing services from another operator, which is one of the main virtues of a removable security approach – indeed as the boxes have been provided by him the major concern of a traditional operator is to ensure that the boxes remain secure and remain operational.
2. This brings us to the major reason for the lukewarm reception by operators of these removable security devices to date, namely the security. In many instances operators have gone to major efforts to ensure that their “embedded STBs” are secured against potential hacking attacks. For example in certain CA markets there are very strict guidelines in place concerning the STBs that operators provide in order to prevent these STBs being used to pirate the operators own service. In the case of CAM in particular this high level of security has not always been present in the provided devices and these devices are then a real security threat to an operator’s service as they can be used to gain unlawful access to the services through the use of downloaded software. In addition, the form factor of CAM devices makes them of great interest to pirates who can distribute them with relative ease when compared to the distribution of STBs.
3. The next reason is also security related but is more specifically content protection related. Unfortunately, at the time of CAM standardization there was not a major effort made to put in place a proper content protection mechanism between the CAM and host device. When using CAM the output of the device is a digital transport stream containing the video and audio services that have been descrambled by the conditional access system. This is a potential “hole” in the content protection chain although in reality it is not exploited often due to the difficulty of recording content directly from the CAM output. In reality it is easier to record content from the analog output of a STB (the infamous analog hole) and encode this to a digital format than it is to intercept the output from a CAM. However with the advent of high definition services this content protection issue is more important and will be treated in greater detail later in this article. In contrast with DVB, CableLabs (the CableCARD standardization body) did address the issue of content protection during CableCARD standardization and therefore CableCARDS do not suffer this drawback.
4. Power consumption has not been a major issue for embedded STB deployment until recently. Historically Pay-TV operators have paid little or no attention to the power consumption of their chosen set-top boxes (STBs). Recently this has changed with many governments mandating energy consumption targets on STBs and this trend is very likely to continue. Given that the average power consumption of STBs in Europe (without hard disk drives) is 7 Watts in active mode and as much as 6 Watts in standby mode it is little wonder that operators and more importantly, the general public are turning towards CAMs that have a power consumption of approximately 1 Watt in active mode and demanding that there be CAMs modules available for use in many markets.

Paradigm Shift

There is currently a paradigm shift, however, in attitudes concerning CAM and CableCARDS because the major obstacles to the successful introduction of these removable security devices are being eroded by a combination of market forces and technology improvements. Firstly, there are a number of markets where Pay-TV has flourished in which the operators do not provide a STB (markets typically called horizontal markets). In these markets the Pay-TV operators provide services to boxes that have been purchased by consumers. Typical examples of these markets are the digital terrestrial markets in Italy or in the U.K and also in Germany on both cable and satellite networks. Often in such a horizontal market the Pay-TV service operator will "certify" that host devices (both STBs and iDTVs) operate correctly according to his desired specification and will encourage STB vendors to supply and sell boxes in normal distribution outlets. The end result is that a subscriber pays himself for his STB and uses it to gain access to a particular Pay-TV service that he deems interesting. In such a market there is often pressure from the regulatory environment to ensure that a STB can be used to access services from different operators (as this deemed in the consumer interest). This is typically where a CAM or CableCARD can be used to access different services that are secured with different CA systems.

Secondly, with the advent of alternative delivery networks for media entertainment (traditional broadcast satellite/terrestrial/cable but also broadband IP and mobile networks), new content aggregation propositions and the different commercial bundles built around these delivery channels there is a real shift in the market towards accessing services on multiple end user devices (such as PC, mobile or different types of STB or iDTVs). Basically consumers want to be able to access their content on whatever device is their favorite one or the handiest one at viewing time. This means that each of these devices needs to be capable of providing access and from a security perspective this means that using a removable device is a way to provide a solution for this diverse spectrum of end user consumer electronic devices without needing to integrate security technology inside each one. iDTVs are a particularly good example of this trend as the newer models have integrated tuners and decoders (hence the iDTV name!) thus enabling access to services without a STB. Indeed these iDTVs include all the functionality to decode and display even high definition services except the security functionality. Of course it would be possible to include embedded security but the variety of different security systems (CA, DRM etc) make it difficult to do so – instead many iDTV vendors have chosen to include a Common Interface slot to enable removable security CAMs and would be very much in favour of service providers enabling the consumption of Pay-TV services on these iDTVs (by provision of a compatible module).

Copy Protection

So why would a Pay-TV hesitate to provide a compatible module that will enable consumption of his services on devices that he has not supplied? Well one reason that has been put forward is the subject of copy protection. As stated above the initial DVB specification of Common Interface (DVB-CI v1) omitted to treat the subject of copy protection on CAM output. In many Pay-TV systems the three major categories of content are

- Sport
- Adult
- Movies (Hollywood etc)

And there are arguments to suggest that the first two categories are less constrained by issues of copy protection. For example sport is very time constrained with live content being highly valued but recorded content being less valuable (who watches sport when the result is known?).

In reality though, content protection is absolutely an issue for all types of content and the effort required to protect the content can be seen as a direct function of the value of the content.

With Movie content clearly the situation is most critical and movie studios have rightly moved to enforce their stringent copy protection requirements through their existing distribution contracts with major Pay-TV operators. With the advent of High Definition services this is becoming even more relevant (imagine the value of the latest movies in HD format) and it is for this reason that in the digital sphere the new initiatives around HDCP are designed to ensure that there are no easily accessible digital streams available. To address these issues on CAMs, DVB has moved forward to implement a new standard known as DVB-CI v2 that should solve the copy protection issue that is present with DVB-CI v1. The work of DVB on this subject has however been slow to progress and the working group in DVB on this subject is currently stalled mainly due to different political agendas on the subject.

To solve the copy protection issue optimally requires the introduction of a DVB specification as it ensure that all compliant devices will be interoperable etc. Solving the copy protection issue in a "non-standardized" manner is relatively easy however as it simply involves the CAM module scrambling its output and the host device being capable of descrambling the signal (this obviously is a rather simplified viewpoint and ignores the actual technical complexity of copy protection solutions but the point is simply that proprietary technical solutions are easier to find than DVB standards are to put in place).

Legacy problems

As many markets are moving forward with the introduction of CAM modules based on legacy DVB CI 1.0 specifications (Italy for example) and there are millions of iDTVs being sold throughout the world, it is quite clear that there will be a problem of legacy in the sense that as the DVB CI V2.0 specification is taking a long time to complete there will be a huge number of non-compatible iDTVs in the marketplace (and therefore not capable of implementing the DVB copy protection) it is therefore of utmost importance to ensure interoperability between CAM devices and iDTVs as early as possible (to avoid disappointed consumers not being able to receive Pay-TV services on their new iDTV)..

Solutions need to be made rapidly available to the market from groups of interested parties (CAM provider and host device manufactures) that can be used in a totally secure manner to provide removable security on host devices such as iDTVs and fill the gap while DVB continues its efforts to resolve the deadlock around DVB-CI v2. Currently there is an industry consortium of CAM vendors, operators and CE vendors named Common Interface Plus (or CI+) that has published a specification for interoperability between CAM and iDTVs that solves the copy protection issues and this specification is open to manufacturers that wish to provide secure solutions for DVB CI before the introduction of the actual DVB CI V2.0 specification. This CI+ specification is now freely available for implementation by any interested party. Note however that it is a specification provided by an industry consortium is not an official DVB specification.

What does the CI+ specification address?

There are actually two main objectives of CI+ specification

- 1. Solving the copy protection issues
- 2. Improving the user experience by evolving the communication between CAM and host device to provide better graphics for example (therefore allowing an operator to customize the user interface to his own look and feel)

These two areas have been identified as barriers to the more widespread adoption of removable security and the CI+ specification is clearly attempting to remove these barriers.



The example below shows what can potentially be improved in terms of the UI by using the CI+ browser. Normally using DVB-CI 1.0 the UI is capable of only displaying text strings sent from the CAM and uses the MMI (man machine interface of the iDTV) – in the example below the UI is done using the CI+ browser enabling graphics etc to be used and potentially enabling an operator to introduce his own branding using a CAM.

So what does this mean for the market?

Proceeding in such a manner is really the only alternative open to CAM vendors, Pay-TV operators and CE manufactures that wish to provide solutions rapidly. What happens then with these legacy modules when DVB-CI v2 becomes available?

Currently it is unclear as to the exact contents of DVB-CI v2 as it is work in progress. However it should be the case that DVB-CI v2 is backward compatible to encompass modules and iDTVs that are deployed before its completion. This means concretely that there is likelihood that a number of profiles of DVB-CI v2 co-exist (in a manner akin to the HD compatibility (HD ready, Full HD etc). This means that the so called CI+ modules should be compatible with the DVB-CI v2 specification and that they can co-exist with any improvements that may be introduced in DVB-CI v2 which would be introduced in new products produced after the publication of the DVB specifications. This can however not be guaranteed however as it is clearly depends on the final decisions taken in the standardization of DVB-CI v2

In summary on the copy protection subject there are three situations

1. DVB CI v1 which has no copy protection but is widely used in various different markets.
2. CI+ a "consortium" solution to the copy protection issue developed by industry players and plugging the hole before introduction of DVB CI v2 and in addition addressing improvement of the User Interface.
3. DVB CI v2 the official DVB specification that is currently stalled but which is designed to solve the copy protection issue for CAMs.

So what are the trends around the world?

In Europe there are a number of different efforts underway to ensure availability of CAMs and also to ensure interoperability with iDTVs. In Germany this is centered around the satellite and cable market with new operator Entavio introducing CAM modules for its innovative satellite distribution platform. These CAM modules implement all features required for the German market in terms of legislation compliance (parental control etc). Knowing that currently there are already over 500'000 deployed iDTVs in the German market and that this is increasing at a rate of approximately some 100'000 per month it can clearly be seen that the sooner other operators follow the easier it will be for consumers to benefit in full from their new iDTVs that often include an integrated QAM demodulator allowing direct access to digital cable services without the need for a STB.

In Italy the government body (DGTVI) is leading the initiative to ensure the provision of suitable CAM modules and iDTVs by introducing a specification defining interoperability (DGTVI spec). A large number of iDTV manufactures and CAM module vendors are working to ensure interoperability between products and the first certified CAMs and iDTVs were introduced in time for the Christmas 2007 market. There are large expectations for iDTV penetration in Italy (with estimates of between 1-2 Million units per year) and this offers large potential to operators who wish to provide content for consumption on these new devices. The modules certified for use in Italy by Digitvi are based on DVB CI v1.0 in order to be compatible with current generations of iDTVs and include support for 3 service providers currently (Mediaset, La 7 and Pangea).

In Sweden the innovative DTT operator Boxer has long endorsed CAMs for use with its service and now has plans to expand service to Denmark and Ireland and combining CAMs with iDTV has proven a very successful model for them.

In the U.K. where the penetration of digital television is higher than any other country in the world there are reports of 3Million iDTVs being sold per annum. Different service providers are piggybacking on this phenomenon such as TopUp TV who has introduced a CAM to provide access their services which include Setanta Sports with live English Premiership Football. Again the TopUp TV and Setanta modules are based on DVB CI v1.0

In Korea the momentum with CableCARD has been sustained over the past 24 months and there are now more than 3 Million deployed modules in Korea. The Korean government has mandated the use of CableCARDS and this is the same situation as in the U.S cable market. The level of compliance remains historically higher in Korea than in the US although over the past 9-12 months approximately 4.2 million cablecards have been deployed by the major cable operators.

>> Conclusion

The terrestrial Pay-TV operators in both the UK, Sweden and Italy are great examples of innovative service providers who realize the value of providing removable security devices in a horizontal market – content can be provided and monetized without the need for heavy capital expenditure. As usual in Pay-TV "content is king" and using CAMs is the opening new doors to exploit valuable content. Solutions are available now and can be rapidly introduced to meet existing market needs. Future standardization efforts from DVB will ensure that there is an interoperability specification that provides future proofing to operators who introduce CAMs before this standard is finalized.

As detailed early in this paper there are compelling reasons to expect the further development of markets using removable security modules – the energy awareness of the end user is one of these reasons but it should also now be clear that there are enough incentives for Pay-TV operators to embrace modules even without the drive coming from energy conscious end users and governments. The future of CAM and CableCARD seems bright and this can only be positive for both the environment and also for innovative service providers.

Headquarters

Rte de Genève 22
CH-1033 Cheseaux
Switzerland

Tel: +41 (0)21 732 04 04
Fax: +41 (0)21 732 04 15

R&D center

ZE Athélia II
531, Avenue du Serpolet
F-13704 La Ciotat Cedex
France

info@smardtv.com

www.smardtv.com