WHITE PAPER

TECHNOLOGY SERIES

DVB-CPCM
AN ENABLER FOR NEW CONTENT BUSINESS MODELS?

NAGRAVISION
KUDELSKI GROUP
enabling digital tv convergence

INTRODUCTION

Over the past few years the value of content being distributed over different delivery networks has greatly increased. Paradoxically, the re-distribution of content over the same networks can be accomplished with ease. This situation has led content owners to enforce security measures to protect their content – called Content Protection Technology (CPT). As a result, service providers now need to ensure that their Conditional Access Systems (CAS) interface with CPT, to reassure content owners that their content is secure.

At the same time service providers want to make their offer more attractive by making paid-for content accessible across the user domain. This means supporting convergence, or more specifically, interoperability of storage and rendering devices. Ideally CAS and CPT will be cleanly decoupled to allow service providers to choose the most suitable CPT to help them achieve their new objectives.

Enabling true convergence requires evices to be available in retail and even more importantly to remain interoperable across the entire end-user's domain. In this perspective the persistence of proprietary CPT integrated with closed ecosystems of services and devices have been a serious inhibitor for consumer acceptance and market growth.

Matching the interests of content owners, service providers, CE manufacturers and end users is not a trivial challenge and will inevitably require compromises. However success will be heavily predicated on a genuinely open approach that creates a real level playing field of media devices that provide a compelling consumer experience.

This paper mainly aims at providing selection criteria for such a CPT and eventually proposes one technology that fulfils these criteria, the DVB standard named 'Content Protection and Copy management' (CPCM).

It proceeds by examining the current situation to deduce what are the new challenges for a CAS (section 1). Then, it outlines requirements on the CPT to help the CAS take up these challenges (section 2). The main features of are then CPCM presented and assessed according to how they help meet the business objectives (section 3). A number of business models enabling new revenues from these implementations are finally proposed.

1 FROM CONDITIONAL ACCESS TO CONTENT PROTECTION

This section examines the current situation and trends in the area where service access and content protection meet. The impacts of content protection and convergence requirements on conditional access systems are deduced therefrom.

1.1 CONVENTIONAL DEFINITIONS

In the context of digital media protection, three types of technology can be distinguished: Conditional Access System, Content Protection Technology and Digital Rights Management.

A ***Conditional Access System*** (CAS) is a service protection technology, aimed at controlling access to a service on the basis of end-user entitlements. A service is a set of facilities aimed at providing content to end-user; this may include a delivery system, a content catalog, means for the end-user to subscribe, order content and control associated functionalities. When access is granted, the user is personally entitled to consume the media delivered by the service at the time of acquisition by the receiving device.

A ***Content Protection Technology*** (CPT) aims at guaranteeing that accessed content (i.e. a piece of digital media of any type, like audio, video, text, pictures, software applications and games, or any combination of such, in any format) is handled according to a given set of Usage Rules (UR). The usage rules specify permissions applying to content handling by the end-user that may consist in content consumption (viewing, playing, listening), storage, processing (edition, transcoding), moving between devices. Usage rules apply to content in the network of end-user's devices (media center, recorder, player…) or on physical content media, such as CD or DVD. Copy protection refers to a specific case under that umbrella.

A ***Digital Rights Management*** (DRM) is any technology that controls access and usage of content on an end-user basis. A DRM typically spans both content and service protection. In the case of content protection, a DRM is a CPT where UR are replaced by personalized end-user entitlements, depending on a commercial relationship between the service provider and the end-user. Usually, a DRM is a service protection technology which keeps content under its control after access.

The relationship between CPT, CAS and DRM is illustrated in *Figure 1a*. The protection technologies can be projected along two axes: the one of service versus content protection and the one of 'personalized entitlement' versus 'no-personalized-entitlement' management.

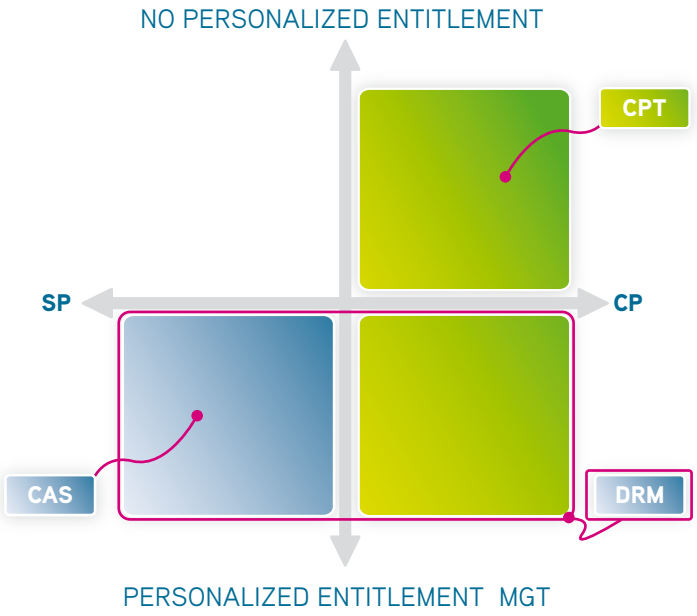

FIGURE 1a
The application fields of CAS, CPT and DRM.

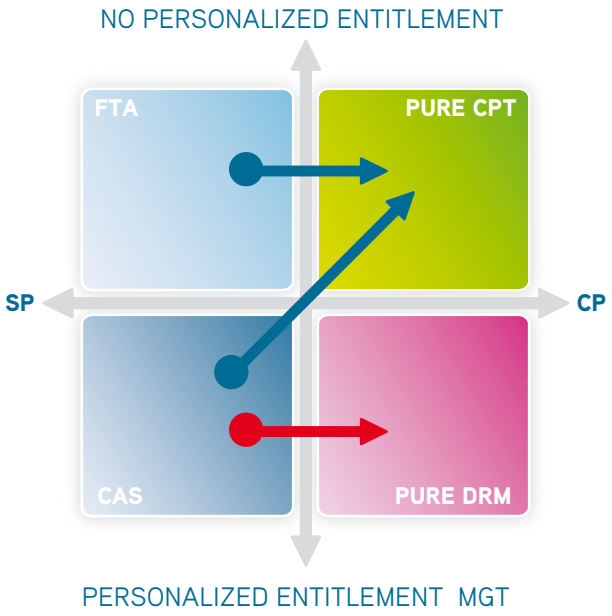

FIGURE 1b
Separate protection technologies and the acquisition of content from service (arrows).

1.2 SEPARATION OF CONCERN

The above definitions result in overlaps between CAS and DRM and between CPT and DRM. Therefore, the four areas delineated by the two axes of *Figure 1a* suggest eventually distinguishing four types of technologies. This results in a clearer separation between the various actors' perspectives and their respective requirements, as shown in this subsection.

1.2.1 Free-To-Air

The technologies protecting service access while not managing personalized user entitlements (upper-left area of *Figure 1b*) rather fit the Free-To-Air (FTA) approach of content distribution. FTA broadcasters may have to protect their service for legal reasons and law enforcement, for instance in order to respect in some way country borders. But managing personalized end-user entitlements does not fit their business model. This particular case is not covered by this paper.

1.2.2 Pure CPT

In this paper, a technology protecting content usage and not managing personalized user entitlements (upper-right area of *Figure 1b*) is designated as a 'Pure CPT'. It primarily fulfills content owners' requirements (owner of the copyright on content).

According to their business model, the content owners' goal is to ensure that content sold to service providers is used with restrictions that fit the transaction conditions. These last years, the value of distributed content has increased, in particular due to new formats, such as the case of high-definition films. In parallel, electronic devices incorporate more digital outputs, whereas the capabilities of distribution networks have also improved, due to their omnipresence and increasing bandwidth. These factors have pushed the content owners to require that digital content is put under the protection of pure CPT with high level security after its delivery.

1.2.3 CAS

The CAS is the technology protecting service access by managing personalized user entitlements (lower-left area of *Figure 1b*). It primarily fulfills service providers' requirements. According to their business model, the goal of service providers is to ensure the end-user accessing the service has paid for it, and for the specific features the end-user is willing to consume.

It is worth noting that the threats addressed by service protection are not the same as those addressed by content protection. The delivery network used by the service is considered as uncontrolled and unsecure. Generally, any person, whether authorized or not, can

physically receive the service. This is especially true in the case of broadcast content. The service provider, through an operator and a CAS, provides the expensive and complex infrastructure needed to deliver content (satellite, cable…) and related functionalities (program guide, interactive applications…). A pirate, who succeeds in finding a means to remove the service protection and distribute the method for doing so, would illegally benefit from the entire infrastructure. In the domain of content protection, once illegally accessed, the content itself must still be distributed; this potentially exposes the pirates and makes their business more difficult.

1.2.4 Pure DRM

In this paper, a technology protecting content usage by managing user entitlements (lower-right area of *Figure 1b*) is designated as 'Pure DRM'.

Indeed, there are still many on-going debates in this area. There is no clear evidence that such Pure DRM will survive. In the field of music for instance, DRM tends to disappear due to the emergence of new business models. This trend may not be relevant to the field of video content (such as movies), where the means of content production, marketing and sales cannot be compared to those of music.

However, as mentioned above, the content owners' stance is quite unambiguous nowadays. It is the association between CPT and personalized entitlement management, i.e. Pure DRM which is out of content owners' scope. By addressing separately Pure CPT and Pure DRM, solving the DRM business model issue may be postponed while Pure CPT is implemented.

1.2.5 Service protection to content protection handover

We classified the protection technologies in four categories, and this classification allows us to clearly distinguish 3 circumstances of Service Protection (SP) to Content Protection (CP) handover that make sense, as shown in *Figure 1b*. FTA broadcasters may have to interface with Pure CPT. The CAS can interface with Pure CPT or Pure DRM, depending on the business model.

1.3 CONVERGENCE AND CONTENT PROTECTION

Bringing together the need for a CAS-to-CPT interface on one hand and for convergence on the other hand is a source of new developments for the service providers and their CAS. This subsection analyzes the impacts of this mission on the CAS.

1.3.1 Meeting service providers' and content owners' requirements

Obviously, content protection is applied to content which has value for some actors in the content life-cycle: content owners and providers, or service providers. Any of these actors must ensure that its business model can survive attempts at content theft and unauthorized usage. In the end, it is their revenue that is protected. In this perspective, the interests of the various actors should converge.

For instance, in the service provider business, part of the revenue from the end-users' subscriptions is used to operate the service; another part is invested in acquiring material from content owners. In turn, this material can sometimes be obtained only if some conditions on the content usage by the end-users can be guaranteed by the service provider. Practically, this is where the service provider and content owners' interests meet and where SP and CP can be distinguished.

CHALLENGE #1: THE CAS SHOULD INTERFACE WITH A CPT IN A WAY ALLOWING REPRESENTING BOTH SERVICE PROVIDERS' AND CONTENT OWNERS' INTERESTS.

1.3.2 Trend towards convergence

A CAS could just try to respond to threats on content acquired from the service provider by forbidding in some way any usage beyond direct consumption at acquisition time. Practically, this is hard to support for two reasons:

- Such control would depend on the nature of the receiver. The service provider manages a heterogeneous set of receivers, thus the CAS cannot rely on reaching just consumption-only devices.
- The main type of receiver is a Set-Top-Box (STB) and there are STB models that integrate a Digital Video Recorder (DVR). It is a basic functionality offered to the end-user in most cases to be able to copy acquired content on this DVR.

Historically, this was not an issue for traditional service providers. Most of the time, control of the receiver outputs for recording was achieved through some standard copy protection interfaces. The CAS was in charge of signaling the parameters controlling this interface (e.g. the CCI bits in the CableCARD case). In the case of DVR, various proprietary solutions exist. They require integration between the receiver and the CAS, which is not an issue at this stage, since the CAS proprietary security just requires such integration level: the receiver cannot be agnostic to the CAS.

However, things have become significantly more complicated over the last years. As explained above, content owners strongly require that accessed content is put under the protection of a high level security CPT. But in parallel, the service providers want to make their offer more attractive by supporting convergence, or more specifically interoperability.

Convergence is defined here as the tendency to make technologies having distinct functionalities to gradually combine into one product, with the advantages of each initial component. Interoperability is defined as the ability for devices of various natures, handling content in various formats, using various technologies and various networking facilities, to exchange information and content.

Note that interoperability is significantly more than a mere nice-to-have in the case of multi-servicing. Today, many service providers operate (or plan to operate) services of different natures, for example a bouquet of broadcast pay-TV services - a satellite service, a mobile service, and an IPTV service - and a content-on-demand internet-based service. Service provides want to allow end-users who subscribed to the entire set of services to manage their accessed contents in a transparent and consistent way, regardless of the originating service. This comes back to interoperability because the different services imply different receiving devices (a mobile phone, an IDTV set and a PC in the above example).

CHALLENGE #2: THE CAS SHOULD HAND OVER CONTENT TO THE CPT IN A WAY SUPPORTING CONVERGENCE AND INTEROPERABILITY.

1.3.3 The cost issue

It must be clear that true convergence is an ambitious objective and has an inevitable price tag. Convergence entails much more than just the interoperability of CPT. It requires trans-networking (i.e. change from one network type to another) and transcoding (i.e. transformation from one content format to another). To be serviceable, it must be supported by functional features allowing the end-user to benefit from device interoperability without having to manage transcoding aspects. This requires the connected devices to be able to discover each other as well as the content items they can exchange; this may require devices to manage the network quality of service, plus a number of functionalities bound to content metadata, like subtitling or captioning. Eventually, this requires some user interface to present these operative capabilities.

Device manufacturers may bear much of the implementation costs as far as it allows them to provide user-friendly networks of interoperable devices. Alternatively, elements supporting convergence or simply interoperability, like software downloadable in a device, can be implemented by different parties, in particular by a CAS supplier like Nagravision offering end-to-end solutions (i.e. from the back-end to the entire user domain rather than just to the receiving device, as in traditional CAS).

But the costs of CPT and of CPT interoperability are to be added to the support of all the functional elements mentioned above. The incentive to bear the cost of implementation of a CPT is less obvious. Moreover, a CPT requires operational infrastructures, in particular for UR management and signaling and for security maintenance, which adds to the cost of the one-time implementation of the device features and must be supported by the service operator.

CHALLENGE #3: THE CAS SHOULD PROVIDE WAYS TO RECOVER COSTS OF CP AND CPT INTEROPERABILITY.

2 CAS REQUIREMENTS

In order to solve the cost issue, Nagravision and its customers must count on emerging synergies between the different actors as well a new business models. The proposed recipe to get momentum and cost recovery in the deployment of a CPT is to use a standard CPT and to associate security supplying to a profitable business model. This section enumerates requirements that a CPT should fulfill so to help the CAS accomplishing this mission and absorb the impacts sketched in previous section.

2.1 CONVERGENCE AND ADVANCED CPT

As a CAS supplier, Nagravision has to satisfy two sets of requirements: the service providers' convergence objective and the content owners' need for end-to-end content protection. The first set implies that the target CPT must be advanced enough to support the reality of the user domain complexity, in contrast with a CPT limited to copy protection. The second set implies that the protection means must meet best available security level.

REQUIREMENT #1: THE CPT MUST ALLOW CONTENT TO BE EXCHANGED IN A USER DOMAIN THAT INCLUDES:

- numerous devices.
- remote devices.
- portable devices.
- devices which are not permanently connected to the others.
- devices which are not connected to an external network.
- devices that have various content usage capabilities.

REQUIREMENT #2: THE CPT MUST RELY ON STATE-OF-THE-ART SECURITY.

2.2 COMMUNICATION INTERFACES

The convergence objective requires seamless content transfer in the user domain.

Content transfer is based on the communication protocols used at the different levels of device interfaces. We will distinguish three levels: the network (concerned by connectivity, demodulation, de-multiplexing), the transport (concerned by packet definition and format of the messages carrying the content, including file format), and the encoding level (content encoding format, or codec).

Examine the situation where one device received encrypted content from a source device using given network, transport and encoding specifications and must now transfer this content item to a 'sink' device. If the communication with the sink device is based on the same specifications as the source device, the content can be transferred without additional operation. Now, suppose at the contrary that the transport type is different and requires that the intermediary device re-defines the packets; suppose in addition that the CPT specification of the encryption is based on the transport level and depends on the packet definition. Thus, the content must be transcrypted by the intermediary device, i.e. decrypted and re-encrypted according to the encryption specification for the new packet types.

In the worst case, where the content encryption specification by the CPT depends on different protocols specified for different interface levels, then a change of the specification used at any level during transfer between multiple devices necessitates a transcryption of the content.

Transcryption cannot be avoided in a network of heterogeneous devices. But the occurrence of this costly operation should be limited as much as possible. The solution is to choose a CPT that specifies encryption at one interface level only, and remains agnostic to the other levels. In this case, any transfer that does not imply a change of protocol at the level selected for encryption will not necessitate transcryption.

More precisely, encryption should occur at the level where there is the less chance for a protocol change during content exchange between heterogeneous devices. The choice of this level may depend on the context and would require further analysis.

REQUIREMENT #3: THE CPT MUST SPECIFY ENCRYPTION AT ONE OF THE NETWORK, TRANSPORT OR ENCODING LEVEL ONLY.

REQUIREMENT #4: THE CPT MUST BE ADAPTABLE TO OTHER COMMUNICATION INTERFACE LEVELS.

2.3 STANDARD VERSUS PROPRIETARY CPT

The service provider may be tempted to implement its own CPT, in particular for security reasons. This would require a significant investment whose return value is hard to estimate.

Every device of the user domain targeted by the interoperability requirements would necessitate integration with the proprietary CPT in order to handle the proprietary format of user entitlements and the proprietary content encryption algorithm (if any). We believe that integration with a significant number of device types and manufacturers is an enterprise that does not fit today's market reality and balance of powers. Moreover, each such proprietary CPT

should be approved by the content owner consortia, which would need disclosure of the specification and complex legal processes on a case-by-case basis.

Using a standard CPT trusted by content owners will solve these issues while reducing the CPT cost issue with less integration cost for greater Home Network penetration. It addresses the horizontal market. The service provider may reach devices that it has no knowledge of (i.e. which required no integration with the CAS) and that can yet be trusted. Indeed, any device on the market that complies with the selected standard CPT will be able to obtain content from the service provider. All that is needed is an Acquisition Point (AP), i.e. the component interfacing between the CAS and the CPT. This content handover will greatly help penetration of the user domain with accessed content. In turn, this penetration makes the service provider offer more attractive.

REQUIREMENT #5: THE CPT MUST BE A STANDARD.

REQUIREMENT #6: THE CPT MUST BE SUPPORTED BY MAIN CONTENT OWNERS.

2.4 INTEROPERABILITY WITH OTHER CPT

Interoperability of CPT is a requisite for convergence. If two devices are interoperable from the functional point of view of convergence, it is inacceptable that their incapacity of passing content from one protection technology to another artificially breaks this interoperability.

Implementing a widely adopted standard protection technology will diminish this risk. Nonetheless, in order to guarantee CPT interoperability in all cases, the CPT should comply with an upper layer standard, implemented as a system allowing different CP technologies to exchange content (and associated entitlements if they are DRM), i.e. a DRM Interoperability System (DIS).

REQUIREMENT #7: THE CPT MUST COMPLY TO A DIS.

2.5 STANDARD SECURITY

'CP Security' is the means ensuring that CP cannot be (easily) bypassed. A CPT relying on content encryption specifies the cryptographic algorithm used to encrypt content. But cryptography does not equal security: cryptography is the technical means to protect content, whereas security is about keeping cryptographic keys secret. It is often argued that «client side security does not work», and content protection should be ensured by implementing server side security whenever feasible. The server is the key element to provide counter-measures, renewability and resilience to the security system. The CAS supplier brings know-how and infrastructure. Thus, we need a standard CPT open to security contribution from service providers. At least, the specification of the AP must not impact the CAS by downgrading the CAS security level.

REQUIREMENT #8: THE SPECIFICATION OF THE CAS-TO-CPT INTERFACE MUST BE FLEXIBLE ENOUGH TO ALLOW PROPRIETARY SECURITY LEVELS AND ENABLE COUNTER-MEASURES.

REQUIREMENT #9: THE SPECIFICATION OF THE CAS-TO-CPT INTERFACE MUST NOT IMPACT THE CAS SECURITY.

2.6 CONTENT HANDOVER TO PURE CPT

To sum up, the following alternatives are available when content is accessed by the end-user:

- Content is kept under CAS control.
  This option can be implemented in two ways:
  - Not letting content flow beyond the point and time of acquisition: This is not compatible with the convergence objective.
  - Implementing a proprietary CPT: This may be unfeasible, would be costly, contradicts the convergence objective and would limit penetration of the user domain.

- The service provider and CAS hand over content to:
  - The end-user, who would be allowed to consume and distribute content without restrictions: This would not fit content owners' requirements.
  - Another DRM, under which the end-user may enjoy accessed content in different ways, according to the entitlements bought in some way: This would necessitate either a DIS or a proprietary implementation of an inter-DRM bridge, under contractual agreement with the other DRM, which does not fit the horizontal market.
  - A Pure CPT, under which the end-user may enjoy accessed content with permissions predetermined on a per-content basis: This fits service provider requirements and convergence objectives.

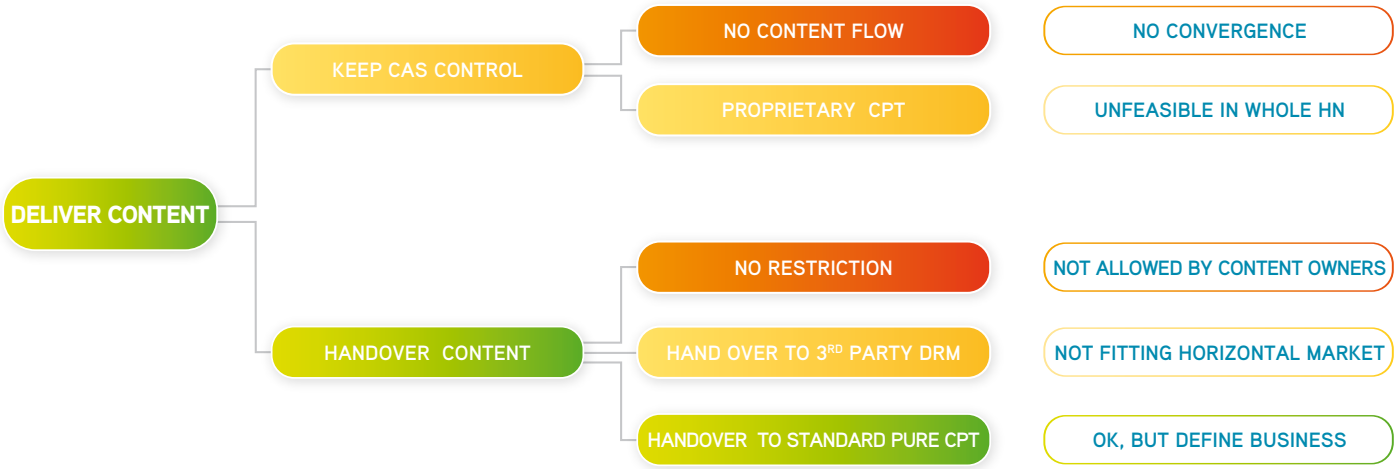

FIGURE 2
Summary of the alternatives for content handover to the user domain.
Colors: **Orange** = fails to meet requirements **Yellow** = impractical **Green** = OK.

Figure 2 illustrates this decision tree. Notice that the 'proprietary CPT ' alternative is about a CPT that would integrate the whole Home Network. Partial solutions, combining flow restriction and proprietary CPT are already implemented when it consists in just controlling the receiver and the receiver's hard disk for storage. One alternative only is left: content handover to standard Pure CPT.

Notice the two last alternatives (handing over to Pure DRM or to Pure CPT) correspond to the two CAS-to-CP handovers identified in Figure 1b and to the advocated separation of concern between Pure CPT and Pure DRM that would allow us engaging in the distinction between CAS and Pure CPT, while keeping an easy way to endorse and capitalize on Pure DRM in the future, if appropriate.

REQUIREMENT #10: THE CPT MUST BE A 'PURE CPT'.

REQUIREMENT #11: THE CPT MUST SUPPORT THE CPT/DRM SEPARATION OF CONCERN.

2.7 EFFECTIVELY ADDRESSING THE COST ISSUE

Now, the service provider selecting a CPT fulfilling the requirements enumerated above, would still need to define business models to address the cost recovery issue.

2.7.1 Default business model for content handover to Pure CPT

Firstly, by providing an interface with a standard CPT approved by content owners, valuable content will be available to service providers and their content offer will remain attractive. Secondly, an interoperable solution is a justified marketing argument to attract more subscribers.

2.7.2 CPT-based advanced business models in a weakly tethered system

Nonetheless, it is possible to capitalize on the CPT to develop new advanced business models.

We argued that the server-based security re-enforcement can be applied only through a service provider. In other words, CP in a horizontal market can be better secured if related in some way to a vertical market. An obvious intersection point between horizontal and vertical markets is the AP supplied by the CAS.

Now, security of CP must be ensured at many other places (different devices of the user domain) and times (over recorded content and its replay). From this point of view, a satisfactory CPT model should allow occasional links to a server. In turn, secure CP throughout content lifecycle should rely on a tethered model, i.e. a model going back to vertical content management at some places and times. The tethering is in this case referred to as 'weak', because it is generally not mandatory in the standardized CPT used, therefore not all devices will implement it, and hence there is no guarantee that every user domain will include such opportunities to connect to a server.

A weakly tethered system provides the basis to derive business models binding cost recovery to security. In other words, with such model, security is brought by the service provider and its CAS as a value added to the standard CPT; the CPT in turn offers means to increase profitability by conveniently exploiting the CPT functionalities, i.e. by enabling business models based on the CPT features. Some concrete examples of such models are given in the next section, dedicated to CPCM.

With such models, a service provider can expect recovering not only the cost of CPT implementation at CAS level (i.e. of AP and possibly Export Point - EP) but also part of the implementation of convergence enabling features in our end-to-end solutions. Remember CPT is only the means and convergence the goal. This can be realized by securely wrapping convergence-enabling applications with the CPT compliant elements. Figure 3 illustrates the resulting wrapping.

In this manner, the end-user benefiting from convergence has yet to accept the business model that guarantees our cost recovery. We believe this is possible because the end-user is not a priori reluctant to content protection, as far as it remains convenient and content and user entitlements can flow freely in the domain.

REQUIREMENT #12: THE CPT MUST BE OPENED TO THE WEAKLY TETHERED MODEL.

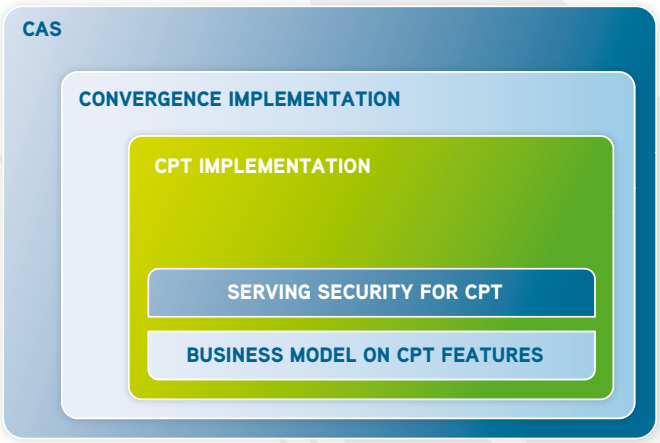

FIGURE 3
Wrapping convergence with the CPT implementation and CPT with security, so to enable implementation of business models based on the CPT features. The security is supplied by the CAS (blue) to the CPT. The business models cover the cost of convergence implementations, including CPT implementation

3 CPCM, A STANDARD ADVANCED CPT, A DIS AND A BUSINESS ENABLER

The DVB standardization body has elaborated CPCM as a Content Protection and Copy Management standard. It is defined as an open standard providing an interoperability platform for the protection and management of commercial digital content in the user domain. CPCM is being published by ETSI under code TS102 825. CPCM is a Pure CPT designed for consumer products in the user domain. This section presents CPCM by highlighting its main qualities and advantages. It then evaluates CPCM's ability to be used as a CPT that meets convergence objectives defined by the requirements listed in previous section. Finally, some business models based on CPCM are briefly discussed.

3.1 CPCM OVERVIEW

3.1.1 CPCM contributors

CPCM is an industry driven initiative in which the entire content distribution and consumption chain have been represented, namely content owners, service providers, security providers, consumer electronics manufacturers, software manufacturers and a consumer association. The primary requirement came from content owners that were seeking a trustable advanced CPT, which would address the threats against content leaking in a user domain of convergent devices as foreseen by the service providers and manufacturers. Key secondary objectives were:

- Keeping the end-users satisfied by allowing content and UR to flow seamlessly in the user domain, providing flexibility of content use despite restrictions, so to remain in line with the convergence trend. This is a condition for the CPT acceptance by users and consequently by CE manufacturers.
- Keeping the service providers satisfied by providing support for various innovative and flexible business models.

The fulfillment of these objectives was guaranteed by making different important players of the industry value chain actively collaborate with the content owners: Pay-TV operators, FTA broadcasters, CE manufacturers and CAS suppliers. They have substantially contributed to CPCM, for instance by proposing algorithms, elaborating protocols, validating security aspects, and defining the UR.

Today DVB-CPCM is strongly supported by the Motion Picture Association (MPA) and content owners such as Disney or Warner Bros.

3.2 MAIN CONCEPTS AND THEIR ADVANTAGES

3.2.1 Content-centric approach

CPCM is content-centric. A Content License (CL) is bound to each content item. The CL is the CPCM data structure carrying UR and the cryptographic information needed to descramble the content to which the usage rules apply. The usage rules it embeds apply to the management of this content item only.

On top of the pre-supposed underlying HN specification, CPCM specifies a number of protocols to exchange CL, and inform on content management permissions and restrictions due to the UR settings in the CL. Through these mechanisms, devices interact with the content rather than which each other.

As a corollary, CPCM is not device-centric. CPCM does not define device types. Instead, it defines functional entities which are abstractions covering the content management types that must be distinguished from a protection point of view, i.e. for which UR associated to a content result in different responses. On top of this, CPCM defines an Instance, which is an implementation of any nature of any of this functional entity in any device. There are only five functional entities, as illustrated in Figure 4:

- The Acquisition Point (AP), receiving content from the delivering CAS or DRM. It replaces the initial protection with the CPCM one. In particular, it has the task of mapping UR or entitlements signaled by the input CAS or DRM onto a specified UR. It is the entry point of the CPCM system, i.e. the set of CPCM-compliant interconnected devices.
- The Processing Entity (PE), performing operations on content, such as format change or image handling.
- The Export Point (EP), performing the reverse function of the AP.
- The Consumption Point (CP), rendering the content to a display device.
- The Storing Entity (SE), storing content.

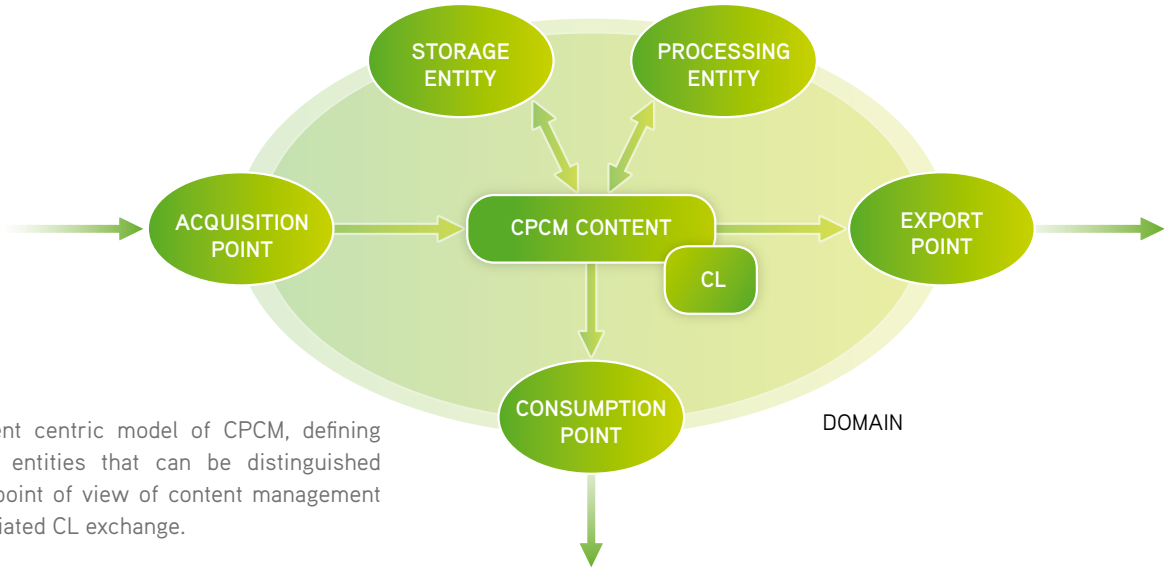

FIGURE 4
The content centric model of CPCM, defining functional entities that can be distinguished from the point of view of content management and associated CL exchange.

Highlight: The abstraction of functional entities is a key to CPCM flexibility. In particular, the specification of the AP on a per content management scenario basis makes clear how to select the scenarios we want to support and the implementation required for the envisaged case.

An example of content flow as managed by these entities is given by *Figure 5*.

Nonetheless, CPCM works on a number of assumptions regarding the underlying HN specification. In particular, it is assumed that the devices are able of two-way point-to-point communications. The implementers of CPCM must then rely on other standards to perform CPCM operations. For instance, the devices can implement DVB-HN and DLNA stacks for home networking, discovering devices and content, or controlling quality of service. These standards also specify content formats.

3.2.2 Authorized Domain Management

Another important concept in CPCM is the Authorized Domain (AD). It is a user domain which is managed from a content protection perspective. Authorized Domain Management (ADM) consists essentially in controlling AD membership, by managing CPCM instances that join or leave the user domain. The local and remote instances in the AD are counted and ceiling values are enforced. The ADM functionality is not bound to a type of device, and ADM may be managed by any type of CPCM instance. The managed AD concept makes possible to control content flow according to the domain boundaries. Basically, the ADM is performed by CPCM compliant devices in a horizontal way, i.e. without external control.

Highlight: ADM is a key to harmonization with convergence, permitting content to flow beyond the HN, into mobile and remote devices.

3.2.3 Usage rules

The CPCM usage rules (aka Usage State Information) can be used to support a number of advanced functionalities, allowing interesting scenarios.

UR FIELD	FUNCTIONALITY	EXAMPLE SCENARIO
Copy control information	The basics of all CPT, ensuring the content can be copied only if authorized.	A high value (e.g. HD) movie cannot be copied
Viewable flag	Consumption can be forbidden. This reinforces the DIS capability of CPCM.	Content for VOD consumption can be pushed. Or content can transit inside the CPCM system, before being exported to another CPT for consumption.
View window or period	This controls the time during which content can be consumed.	Content is rented. The end-user does not 'own' it but can nonetheless benefit from it beyond broadcast time.
Simultaneous View Count (SVC)	This sets the number of authorized simultaneous consumptions and exports of a given live content item inside the CPCM system. The AP managing this functionality is responsible of controlling consumption.	'Follow-me' scenario, where the end-user switches off one CP and should get the content on another CP.
Propagation information	This controls the Movement, Copying and Viewing permissions. Thanks to proximity control and ADM, the content propagation is controlled to be local, geographically limited, or authorized in the whole user domain.	Content can be acquired by a local device not belonging to the AD, e.g. by a visitor in the home of the end-user who acquired the content.
Remote access dates and flag	This controls transition of propagation restrictions. Temporary restrictions, due for instance to law enforcement may be released, and permissions extended.	Blackout can be reinforced, by not allowing content accessed at some place (e.g. the secondary home) to be viewed in a remote place (e.g. the main home where blackout could apply).
Analog export or output controls	The basic controls to address the analog leak.	High value content can be transferred to devices having digital outputs without leaking of the valuable part.
Export to other CPT	This controls the possibility to export to known CPT.	For instance, content can be exported to proprietary DRM: a key feature of DIS. Also, a key feature in non viewable content transit through the CPCM system.

3.2.4 Security elements

CPCM provides an optimum level of security against content protection threats. The cryptographic tools and architecture are at state-of-the-art level:

- The Local Scrambling Algorithm (LSA) for content encryption is based on the AES symmetric block cipher with 128-bit key length.
- The CL is cryptographically bound to the content by carrying the encrypted content scrambling key. The CL is signed.
- Trust is established with certificate exchange and a Secure Authenticated Channel to exchange protected data is established based on Diffie-Hellman. Update of certificate fields is possible.
- Then, CL is exchanged under the Secure Authenticated Channel protection, so that only a trusted device may obtain the content scrambling key. Since the device is CPCM compliant, it can be trusted and will manage the content according to the UR in the CL.
- Proximity tools use secure round-trip time to assess locality. Locality of devices is a key parameter of content protection in CPCM, so to apply the related UR fields described above.
- Revocation lists are securely applied, allowing revocation of devices on a content basis.
- Apart from revocation, system renewability is a procedure that will be fine tuned by the specific Compliance and Robustness regime.

Highlight: This security level is a key to allow the different CAS to use CPCM without having to operate in a lower security compatible mode, and to offer their best security technology.

3.2.5 Auxiliary Data and Authorized Authenticated Agents

While the content License carries CPCM data structures essential to content protection, another CPCM container, namely the Auxiliary Data, makes it possible to securely associate various data structures of various origins with the CL and thus to bound them to the content. In particular, Auxiliary Data can be used to carry the original entitlements that were signaled by the content delivering CAS or DRM.

Proprietary entitlements in Auxiliary Data can be used after export or by any functional entity that would be able to decode them and take actions accordingly. In the case of export, the original entitlements can be restituted to the CPT to which content is exported (possibly the original DRM or a DRM that is compliant in some way with it). In the other cases, a CPCM instance may call back the AP which imported the content, and ask for permissions related to said entitlements. Typically, the AP will forward the request to an Authorized Authenticated Agent (AAA).

An AAA is a kind of proxy object, whose working is not specified by CPCM but is foreseen as an interface to proprietary systems in a number of situations. In this case, the AAA is in charge of implementing the CAS or DRM response to the request. Eventually, based on this response, the AP may send a new CL with new usage rules to the requesting instance. The process is illustrated in *Figure 5*.

Highlight: The specification of Auxiliary Data management with the enablement of 3rd party Authorized Authenticated Agent (AAA) is a key to allow extensions of CPCM use facilitating the various business models of the content delivery systems.

An Authorized Authenticated Agents can be used to:

- Renew CL, as described above.
- Assign localness between two devices: This is an alternative to CPCM specified proximity tools.
- Manage the AD: An AAA can be used to control domain joining and revise ceiling values

Highlight: By using AAA for proximity control and ADM, it is still possible to build a vertical domain on top of CPCM, if more favorable to the service provider.

3.2.6 Flexibility and modularity

CPCM provides a very flexible specification. Flexibility is ensured by many facets of the specification.

CPCM capabilities implemented in devices may vary according to several factors, for instance:

- A device may implement any of the functional entity: AP, PE, EP, CP or SE. This is specified in its certificate, in the so-called 'APECS' field.
- A device is optionally able to perform some functions, depending on its 'APECS' status: scrambling, descrambling, CL issuing…
- A device is optionally geographic aware, or ADM capable. This is specified in its certificate.
- A device may optionally support UR-related functionalities: Simultaneous view count, remote access control… It must perform the most severe content management regarding unsupported functionalities.

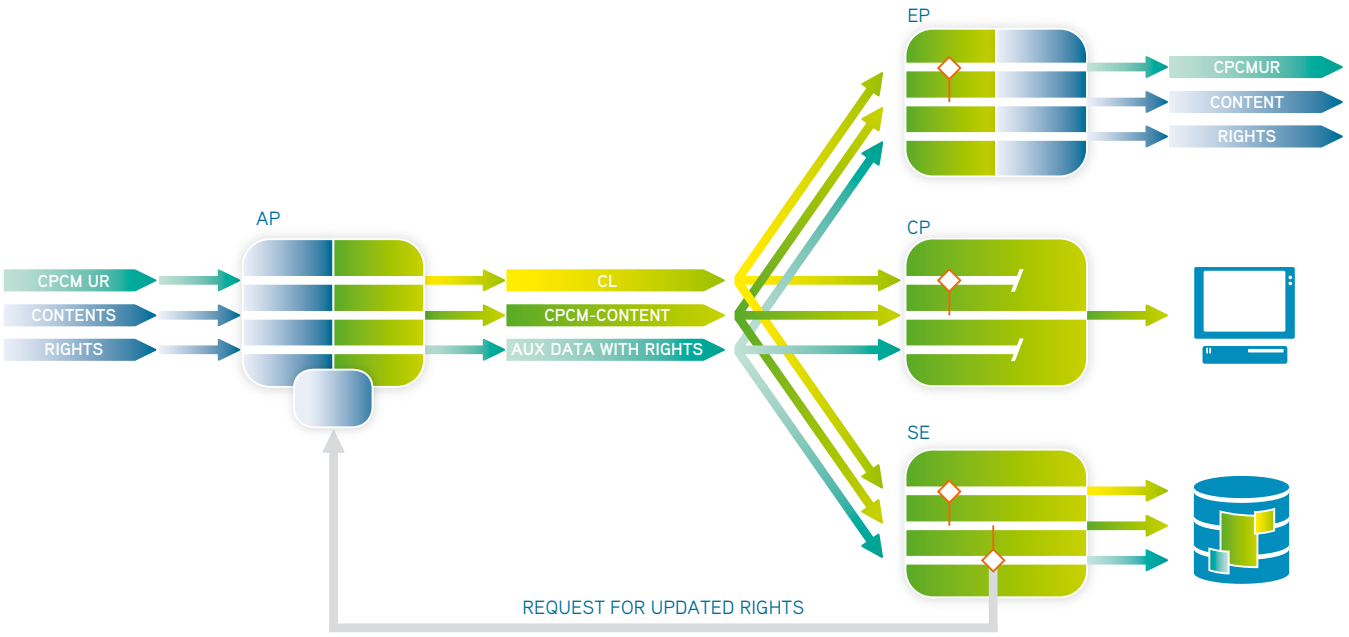

FIGURE 5

The Functional entities, CL and Auxiliary Data management: The AP encapsulates original entitlements in CPCM Auxiliary Data structure. The CP is not perturbed by these data. The EP, integrated with the CAS, may re-build the original entitlements (and the original CPCM UR format as originally signaled by the CAS). At replay request, if the CL no longer grants usage of the stored content, the SE calls back the CL creator, i.e. the AP, which interfaces with the AAA and may send a new CL depending on information from the CAS. Orange diamonds show places where permission for content handling depends on CL or Auxiliary Data

Moreover, CPCM is network and content encoding agnostic since the encryption algorithm is adapted to the MPEG2-TS format and can be adapted to other transport specifications. The choice of the communication interface level for encryption is mainly based on the DVB context. Indeed, encryption should occur at the level where there is the less chance for a protocol change during content exchange between devices. This is the case of the transport level in the DVB context, since MPEG2-TS is the DVB-preferred format. Thus, CPCM can adapt to various levels of communication interfaces with a minimum of transcryption needs.

The specification is modular. Various parts can be implemented independently (this would result in a CPCM conformant device, but not necessarily compliant to a defined Compliance and Robustness CPCM regime). For instance, the ADM or the security toolbox specifications can be implemented without conforming to content management rules, UR and the like.

Highlight: Flexibility is the key to see different ecosystems and use cases emerging, that would address different underlying technologies and situations (e.g. connected versus not-connected). We believe this should favor adoption of CPCM

Modularity of the implementation, based on the concept of CPCM instance is a key factor of interoperability.

Highlight: By allowing partial implementations, CPCM is offering a common compatibility platform, while allowing further security enhancement in regard to CAS technologies.

3.3 CPCM APPLICATION FIELDS

By construction, CPCM has three application fields:

- CPCM is a Pure CPT. Notice CPCM is not a DRM: (1) It is not applicable to the delivery of content, and then relies on CAS or DRM for acquiring content; (2) It does not specify entitlements, i.e. a commercial relationship with the consumer.
- CPCM is a DRM interoperability System. The key aspects of interoperability are the specifications of the Acquisition and Export Points, possibly combined with carriage of 3rd party DRM entitlements into CPCM Auxiliary Data.
- CPCM is an Advanced Biz models enabler. Whereas it is not a DRM, it facilitates the implementation of advance models that would rely on the Auxiliary Data to support scenarios relying on a commercial relationship with the consumer.

As shown in *Figure 6*, this allows us to revisit at CPCM light the alternatives for content handover presented first in *Figure 2*.

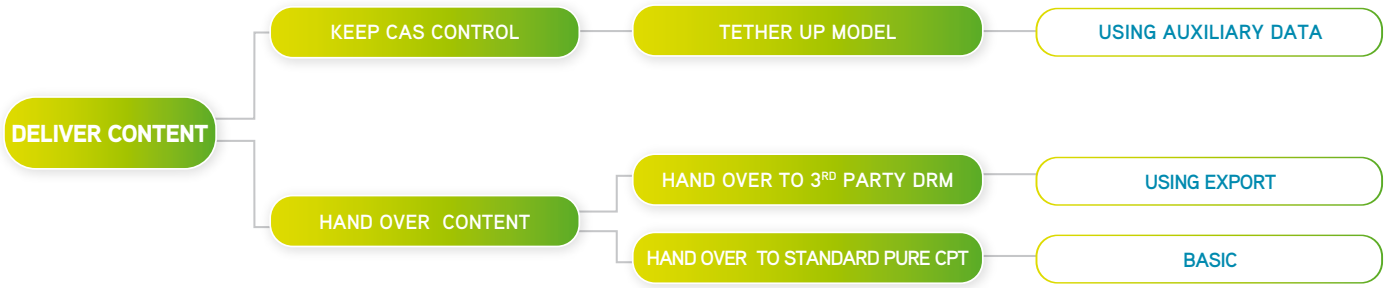

FIGURE 6
Summary of the alternatives for content handover using CPCM.

3.4 CPCM FULFILLMENT OF THE CAS REQUIREMENTS

The following table lists the requirements on the selected CPT resulting from our examination of the impacts that convergence and CPT may have on CAS and indicates how CPCM fulfills them.

	REQUIREMENT	FULFILLMENT
1	Be adapted to user domain complexity. ⁙ Support having numerous devices in domain. ⁙ Support remote devices. ⁙ Support portable devices. ⁙ Support devices not permanently connected to the others. ⁙ Support devices not connected to an external network. ⁙ Support devices that have various content usage capabilities.	This decomposes into the 6 following sub-requirements. Due to the content centric approach and ADM. Via to the ADM and proximity controls. Due to the content centric approach. Nonetheless, the adaptation to other transport specifications will be probably needed for those devices. Due to the content centric approach. Due to the content centric approach, inter-device protocols and Pure CPT' requirement fulfillment. Using the APECS.
2	Rely on state-of-the-art security.	State-of-the-art cryptography is used by CPCM specification of security tools.
3	Specify encryption at one of the network, transport or encoding level only.	CPCM specifies an encryption algorithm and its adaptation to MPEG2 TS Adaptation to other transport specifications can be added to CPCM specification in the future.
4	Be adaptable to other communication	CPCM is network and codec agnostic. interface levels.
5	Be a standard.	By definition.
6	Be supported by main content owners.	By construction.
7	Comply to a DIS.	CPCM can be used as a DIS. Thus, using CPCM makes useless to comply with an additional standard DIS layer, under the condition CPCM is selected as a DIS by other CPT.
8	Be flexible enough to allow proprietary security level and enable counter-measures.	Use CPCM revocation facility. Other updates are reported on specific Compliance and Robustness regime.
9	Do not impact the CAS security.	Due to AP specification.
10	Be a Pure CPT.	By definition.
11	Support the CPT/DRM separation.	Being a pure CPT whereas enabling embodiment of proprietary data and mechanisms that can be activated at any time during the solution deployment.
12	Be opened to the weakly tethered model.	Content handover may be based on personalized user entitlements implemented in the AP. Proprietary formats can accompany the content in the user domain for further exploitation using Auxiliary Data. Later reconnections to a server are made possible by the AAA for CL renewal or for vertical ADM.

3.5 BUSINESS ENABLER

It remains to be more explicit on the business models we can envisage with CPCM:

First, CPCM content management scenarios can be oriented toward the specific case of broadcast live events provided by Pay-TV. Here are some examples:

- ***User domain permitted PPV***. A PPV event representing a high value movie can be for instance consumed remotely but not copied.
- ***User domain controlled subscription with blackouts***. Events on a subscription sport channel have high value as long as they are live. They can be copied; they can be remotely accessed after, but not during, the broadcast.
- ***Home networked SVC***. Consumption of sport events that have a high value live should be controlled as strictly as possible, for example by limiting to a single use instance. The SVC CPCM UR can be used.
- ***Rental mode***. Valuable PPV events are permitted to be copied but can be replayed only during a limited period. The 'viewing period' CPCM UR can be used.
- ***Re-purchase offer***. Non viewable content (push VOD) or rented PPV whose viewing period is past, could be accompanied with Auxiliary Data indicating how consumption entitlements can be renewed.

These scenarios can be grouped in 3 categories:

- ***Propagation*** of existing CAS business in the HN. This scenario is just a matter of re-enforcing concepts already present in CAS products, currently limited to broadcast events. This obviously applies to the PPV and Subscription above examples. For instance, it is just a natural extension of the PPV concept applied to high value movie to not allow copy while permitting remote consumption. This also applies to the rental mode, since we have today the possibility to control entitlement expiration dates and recording in the DVR. Thus, CPCM simply allows this model to be translated in other devices of the user domain.
- ***Extension*** of existing business models. It is a matter of introducing new models, controls and permissions that can not be offered today, in a way directly based on specified CPCM functionalities. This applies to the Subscription mode with SVC control. CPCM explicitly makes this manageable.
- ***Innovation***. It consists in using CPCM to introduce original content management, not directly specified by CPCM. Such uses will most often capitalize on Auxiliary Data.

With CPCM, content handover does not imply end of income. While CAS covers the cost of content delivery, advanced business models linked to content management should cover the cost of implementation of content handover. The manner to make CPT implementation profitable is based on a commercial exploitation of above scenarios:

- ***Passive income***. This typically applies to propagation models like user domain permitted PPV and controlled Subscription. The sale price of existing products will probably not be modified, but the offer is made more attractive by permitting the content to flow in the user domain while preserving the content value.
- ***Featured income***. This can be applied to the extension models or yet to the rental mode. The CPT based feature is sold to the end-user, for instance by applying different UR in accordance with user entitlements. Models of UR profiles and user profiles can be capitalized on.
- ***Advanced income***. This applies to innovation models. The concept is to get additional revenue ensured by CAS specific controls. This combines well with feature income. For instance, re-purchase of content whose rental period has expired is performed by debiting a credit on the smart card connected to the set-to-box implementing the AP, or by calling an URL specified in the Auxiliary Data, that connects the user to a payment server.

3.6 CONDITIONS OF SUCCESS

No matter how nicely CPCM fits the business requirements and allows for attractive new functionalities and business models, real adoption can only be measured by field deployment of CPCM. Real-world implementation will depend on many factors that are not under control of standardization bodies. This subsection examines some conditions of success for CPCM.

The first condition for CPCM to be actually implementable in our context is the creation of a Compliance and Robustness regime, applicable to pay-TV. A regime is a body that edicts rules to which implementations of the specification must comply in order to be certified. The regime mandates a certification authority to deliver certificates to compliant devices. These certificates are the seed of trust establishment between devices and content exchange. Such CPCM regimes are still to come.

Another condition of success is adoption by CE manufacturers. In this respect, we believe that momentum can be created by service providers and CAS suppliers. If a standard CPT approved by content owners is adopted by service providers and their CAS, i.e. by significant sources of content for electronic devices, manufacturers of said devices should be motivated in turn to make their products compliant to this CPT and an ecosystem should emerge.

Eventually, another success enabler would be the adoption of CPCM as a DIS. This would encourage service providers and manufacturers to capitalize on CPCM in order to offer convergent solutions. In turn, the emergence of CPCM compliant devices provides motivation to construct business models upon it.

CONCLUSION

We have analyzed the new challenges generated by the conjunction of the need of content protection beyond content access on the one hand and the convergence objectives on the other. We put forward the properties that a CAS should require from a CPT it may want to rely on in order to take up these challenges. We then applied these criteria to the DVB standard CPCM.

CPCM turns out to be very promising as a standard CPT. In particular:

- CPCM is a standard ***supported by content owners***. This should favor its adoption by main actors in the field of content protection. It allows addressing the horizontal market, achieving penetration in the user domain while reducing the implementation cost.
- CPCM will facilitate ***interoperability of devices*** in a complex user domain. Encryption occurs at the appropriate level of communication interfaces. Content may be permitted to flow between remote devices of the same domain, and it can be locally exchanged between domains. These features contribute to the improvement of the end-user's experience.
- CPCM ***does not downgrade the CAS security level***, and even allows the CAS to contribute to the content protection measures by bringing its own know-how and security mastering.
- CPCM is opened to securely carry proprietary data with the protected content and to tether content management with the delivery system. This gives the opportunity to ***bind business models to the CPT features***.
- CPCM enables ***extending the use of PPV or subscription events in the whole user domain***, defining rental modes, and setting up re-purchase mechanisms.

Like any CPT, the implementation of CPCM is a non-negligible investment for all stakeholders. Therefore its industry adoption depends on its support of all relevant business models to generate critical mass across devices and deployments, ensuring return-on-investment.

Given the richness of the supported business models and the clean decoupling from CAS we believe that this aspect presents a strong argument in favor of CPCM as a standard CPT framework.
In line with our general strategy to enable horizontal retail markets through open standards we therefore fully subscribe to this approach which is in fact a logical extension of our existing Persistent Rights Management (PRM) framework.

REFERENCES

[1] CPCM Specification parts 1 to 10 (normative parts): ETSI 102 825.

[2] M. Jeffrey, «Why CPCM?», DVB-Scene No 24, December 2007.

[3] MPAA Views on Secure Home Networking, Jim Williams, ITU-T workshop on home networking and home services, Tokyo, Japan, 17-18 June 2004, http://ftp3.itu.ch/hnhs/hnhs/Session04/S4P1_JW_SL.ppt#257,1,MPAA Views on Secure Home Networking

[4] Public Consultation on Creative Content Online in the Single Market – Submission of the "Motion Picture Association" (MPA) in response to the Questionnaire of the European Commission regarding Policy/Regulatory issues, http://ec.europa.eu/avpolicy/docs/other_actions/col_2008/comp/mpa_en.pdf

[5] Pragmatic Content Security, Nagravision series.

ACRONYMS

TERM	MEANING
AAA	Authorized Authenticated Agent: A CPCM concept designating an element which is not specified by CPCM but is nonetheless authorized in a secure manner to intervene in certain actions. It is typically a proprietary agent, implemented by 3rd party CAS or DRM.
AD	Authorized Domain: CPCM user domain which is managed from a content protection perspective.
ADM	Authorized Domain Management: The set of CPCM management tools of the AD.
AP	Acquisition Point: The component interfacing between service under CAS or DRM protection and content under a CPT protection. It is in charge of removing the protection of the DRM, replacing it by the protection of the CPT and mapping DRM entitlements to CPT usage rules. Also a CPCM entity.
CAS	Conditional Access System: A service protection technology based on managed end-user entitlements.
CL	Content License: The CPCM data structure carrying UR and the cryptographic information needed to descramble the content to which the usage rules apply.
CP	Consumption Point: A CPCM entity.
CP	Content Protection: Secure control of the usage of a content.
CPCM	Content Protection and Copy Management: Standard issued by DVB.
CPT	Content Protection Technology: A technology protecting content in the user domain, based on the specification of usage rules.
DIS	DRM Interoperability System: A technology that grounds interoperability of devices based on different CPT or DRM.
DLNA	Digital Living Network Alliance: An international cross-industry collaboration of companies focused on delivering an interoperability based on open industry standards to complete the digital convergence.
DRM	Digital Right Management: A service and content protection technology, based on managed end-user entitlements.
DVB	Digital Video Broadcasting: An international industry-led consortium committed to designing open technical standards for the global delivery of digital television and data services.
EP	Export Point: The component interfacing between two different CPT, exporting content under he protection of the first CPT to content under the protection of the second, thus transcrypting and translating UR (or entitlements). Also a CPCM entity.
HN	Home Network: A set of devices owned by a given end-user and that are interconnected in a way that allows them to exchange some content. The connection is local, i.e. the devices are in the same environment making use of a private network.
PE	Processing Entity: A CPCM entity
SE	Storing Entity: A CPCM entity
SP	Service Protection: Secure control of the access to a service.
SVC	Simultaneous View Count: A peculiar CPCM usage rules that enforces control of the number of devices entitled to consume a given content simultaneously.
UR	Usage Rules: A set of rules defined for a given CPT and which determine how the content under the protection of this CPT may be handled by the end-user.

FOR MORE INFORMATION ON THIS WHITE PAPER, PLEASE CONTACT ONE OF THE AUTHORS:

THIERRY DAGAEFF
PhD, Architect
Nagravision
thierry.dagaeff@nagra.com

CORINNE LE BUHAN
PhD, Head of publications & patents
Nagravision
corinne.lebuhan@nagra.com

LAURA FULLTON
PhD, Head of standards and emerging technologies
Nagravision
laura.fullton@nagra.com

IVAN VERBESSELT
Senior Vice President Marketing
Nagravision
ivan.verbesselt@nagra.com

MAIN OFFICE

Nagravision SA
Route de Genève 22
CH-1033 Cheseaux
Switzerland
Tel: +41 21 732 01 01
Fax: +41 21 732 01 00
nagravision@nagra.com

THE AMERICAS

Nagravision SA
Suite 300, 841 Apollo Street
El Segundo, CA 90245
USA
Tel: +1 310 335 52 25
Fax: +1 310 335 52 27
nagravision.usa@nagra.com

ASIA

Nagravision SA
8 Shenton Way
#34-02, Tamasek Tower
Singapore 068811
Tel: +65 6829 08 00
Fax: +65 6829 08 01
nagravision.asia@nagra.com

design: www.diabolo.com

www.nagravision.com