

THE USER'S DOMAIN

CPCM: Making the Content and Device Value Chains Work for All Stakeholders

Thierry Dagaëff, PhD, Architect at Nagravision - Kudelski Group

The DVB's Content Protection and Copy Management (CPCM) open standard specifies an interoperability platform for the protection of commercial digital content. While CPCM is a Content Protection Technology (CPT) designed for consumer products, it is also the correct choice for Conditional Access System (CAS) suppliers and service providers wishing to let content flow seamlessly in the user domain to fulfil convergence needs.

A Conditional Access System is the technology used by service providers to protect access to their services. It manages personalised user entitlements and allows subscribers to access content such as movies or channel tiers if they are authorised to view them. Beyond service access, consumers would like to enjoy duly accessed content across their networked devices. Manufacturers apply themselves to support this trend toward convergence by supplying interoperable devices bridging the

the match; however, using CPCM, it can notify subscribers when this limitation will be removed and the recorded version may be played remotely. Even though subscribers may not have instant access across all their devices while the match is playing live, those same users may record it for later viewing. Secondly, consider a high value pay-per-view (PPV) event such as a high definition movie. The service provider can limit the viewing to the entitled users by restricting it to the authorised domain. The subscribers may order the PPV event when it's advertised and enjoy it when it is broadcast. In either case, subscribers can enjoy their networked CPCM devices by accessing content on those devices which, up to now, was locked to the service provider's set-top box. As viewers demand to watch programming when, where and on whatever device they select, CPCM enables extending the use of subscription events or PPV in the whole user domain.

innovate by introducing original content management exploiting mechanisms offered by CPCM. Such advanced management modes will most often benefit from the capability to bind proprietary data to CPCM content usage rules. For instance, it could be used to offer the consumer the possibility to purchase content where the viewing period has expired; in that case, the proprietary data would carry information on the repurchase mode and price.

At this stage, CPCM can be capitalised on to allow occasional links to a server. In turn, security of content protection throughout content lifecycle can partly rely on a tethered model, i.e. a model going back to vertical content management at some places and times. This is a 'weak' tethering, because it's not mandatory in the standardised CPT, and therefore there is no guarantee that every user domain will include such opportunities to connect to a server. Nonetheless, a weakly tethered system

"...advanced use cases will most often benefit from the capability to bind proprietary data to CPCM content usage rules."

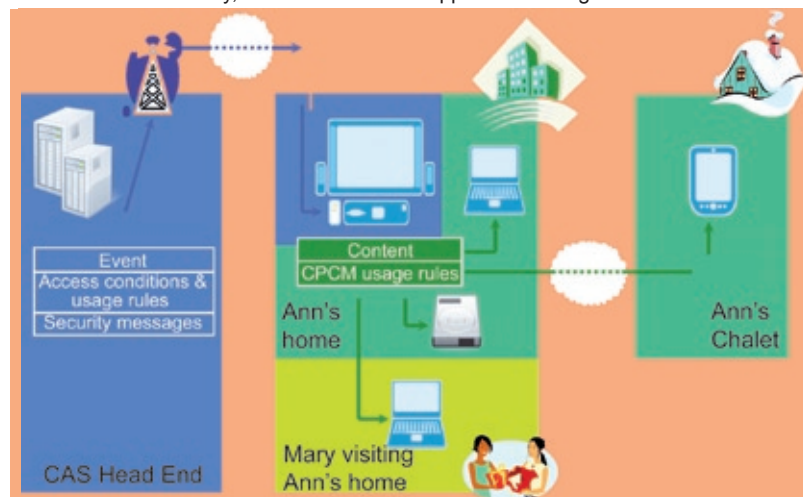
different technologies to make content exchange possible. In this context, service providers need a CPT to satisfy content owner requirements as well as to protect their revenue, by ensuring that content is used and redistributed in the user domain in a way that doesn't contradict the original access conditions applied to their services. CPCM allows these needs of consumers, manufacturers, service providers and content owners to be met by operating as a CPT, a Digital Rights Management (DRM) interoperability system and a business enabler.

CPCM is not a DRM: it cannot be used without a secure delivery system and bears no user management and no control of commercial relationships between the content provider and a subscriber. Thus CPCM relies on the participation in the content value chain of a service provider implementing a CAS or a DRM to protect delivery of content and usage rules. In addition, the CAS can contribute to the protection measures through key management, revocation signalling or vertical control of domains. This is affordable since the CAS security level is not downgraded by CPCM.

In return, CPCM can enrich business models of the service providers. Let's look at two basic examples. Firstly, the example of a sporting event that has a high value as long as it is broadcast live. Due to the legal restrictions, the service provider may forbid the redistribution over the internet during

Conditional Access Systems suppliers may phase CPCM implementation from basic to advanced levels of involvement. It can start with propagating existing business models in the home network by just re-enforcing concepts already present in CAS products, but currently limited to broadcast events; this is illustrated by the above examples. The CAS can extend existing business by using functionalities as specified by CPCM and that weren't supported by the original CAS alone; this applies, for instance, to events with Simultaneous View Count control or to rental modes. Examples have been provided by a Nagravision and Fastcom joint demo at IBC 2008. Eventually, the CAS can

provides the basis to derive innovative business models binding cost recovery to security because the extra security brought by the service provider and its CAS complements CPCM. Remember CPT is only the means while convergence is the goal. By utilising a CAS and CPCM, the service provider can let content flow in the user domain and the manufacturers implementing CPCM compliant devices get new sources of content. It's a win-win situation, where users demanding more content and accessibility from multiple devices can be satisfied, and where content owners, service providers and CE manufacturers have more opportunities to generate revenues.



The Content Value Chain From the CAS to CPCM