

## DVB-CPCM article for September DVB Scene

Chris Hibbert, Chair DVB Copy Protection Technologies Group  
Giles Godart-Brown, Chairman DVB Copy Protection Commercial Group

This is the second article reporting on the work in DVB towards a specification for Content Protection and Copy Management. The first article was a progress report on the work in the technical sub group TM-CPT. This article addresses the issues related to compliance and interoperability currently under consideration in the commercial sub group CM-CP and the Intellectual Property Rights Module (IPRM).

The secure implementation of DVB CPCM will be dependant on the establishment of a robust compliance and interoperability regime.

Typically, implementation of its specifications is outside the scope of DVB and is left to the market, although DVB does produce implementation guidelines, and has taken practical steps to support technical compliance and interoperability testing and security of MHP applications.

Compliance and interoperability rules are needed to protect the interests of all of the different players in the value chain. This is vital to ensure not only the integrity of the specification but also a level playing field for competitive supply of horizontal market products and confidence for broadcasters and other content providers that all products will react the same way. Compliant devices should not be disadvantaged by non-compliant implementations that undermine the system.

A typical set of compliance rules for DVB CPCM would address the following:

- Definition of “defined terms”. These are terms that have a particular meaning in the document
- Usage rules compliance. This covers behaviour of devices in accordance with Usage State Instructions.
- Authorised Domain security management. Here the obligations on the handling and use of device keys, content keys and digital certificates will be laid out.
- Revocation. Ensuring the integrity of the system can be maintained by revoking access to identified content or services.
- Permitted interfaces with “other” accordant content protection systems. This is a section that will be updated as new technologies and trust authorities emerge. This is vital if interoperability is to be achieved.
- Intra and inter-Authorised Domain content flow. Products in a consumer’s home might require different rules for content flow within the local environment than for mobile or remotely located products.

Accompanying the compliance rules will be the robustness rules that address how resistant a device or system should be to circumvention. Elements of the robustness rules address construction, protecting secret and confidential

## DVB-CPCM article for September DVB Scene

information such as keys, protection of internal data paths since manufacturers cannot rely on sealed boxes, and anti-circumvention requirements that prevent features such as secret menus that disable protection.

Most of the currently available (proprietary) content protection regimes rely on the use of encryption and keys for additional security over and above the rules of compliance associated with the attendant usage signals. The encryption keys and associated technology are licensed from the technology owner to the content owner for application to the content. Also manufacturers of consumer products (whether CE or IT) that wish their products to access the encrypted content must obtain a license to the decryption keys in order to legitimately descramble the content.

These licensing regimes are voluntary. Only those manufacturers or service providers who wish to access the encrypted content need take a license to obtain the decryption keys and associated technology specifications. For those who do not wish to access the encrypted content, they need do nothing.

Enforcement against unauthorised decryption of the content by unlicensed third parties is often secured as follows:

- First, to the extent that such unauthorised access infringes upon patent rights owned by the technology owner/licensor, a patent infringement action may be brought against such unlicensed third party. Such patent rights are often referred to as “hook IP”.
- Second, in some cases, actions may be brought under the relevant anti-circumvention provisions of the Copyright Directive in the EU and the Digital Millennium Copyright Act in the US.

The central role that hook-IP plays in these content protection structures and licensing regimes is two-fold. First, it forms the basis on which to build the licensing structure. A contractual license enjoys a stronger foundation if it involves some form of proprietary intellectual property above and beyond the keys themselves. Second, the hook IP provides an important means of enforcement against unlicensed third parties that may seek to access the encrypted content without authorisation.

Traditionally the role of enforceable contractual licenses is seen as critical to content protection system. An intellectual property license that involves proprietary technology based on patent rights provides a solid and well-understood contractual basis upon which to impose the associated obligations and rules. As a result, this is one means of enforcing compliance and robustness rules which will be examined in a manner consistent with DVB practice.

## DVB-CPCM article for September DVB Scene

Hook IP is also seen as a means of enforcement against third parties that seek access to the encrypted content without authorisation (i.e., without taking a license and assuming the associated obligations). If the technology license and associated keys are bound up with proprietary patent rights, then the unauthorised use of the technology and keys will likely violate the patent rights. This then provides a legal means of pursuing such unlicensed third parties by a patent infringement lawsuit. If no hook IP exists upon which the content licensing regime is built, then enforcement against unlicensed third parties can, in certain cases, be based on anti-circumvention laws in the territory in question. However, such a course of action may not provide a sufficient means ensuring compliance with all aspects of a given specification and may not always be possible in some countries. In any event, a content protection system licensing regime that is intended to be international in scope cannot rely solely on anti-circumvention laws. Some sort of Hook IP or other means of enforcement is seen as necessary.

Public Service broadcasting in Europe is typically transmitted in the clear. As a result, no authorisation (either technical or legal, other than, in some cases, the payment of a licence fee) is required in order to receive the signal. Because the broadcast signal is received in the clear (e.g., by digital television sets), there is no authorisation “hook” for imposing conditions on such devices as to how they must handle or protect the content contained in the signal. Once we move outside of the realm of access control mechanisms the situation becomes complicated.

Free-to-air broadcasters, who have no access control, are now facing some of the same threats as operators who can rely on access control. For example, mass redistribution of content outside of the broadcast footprint.

The challenge facing DVB is to adopt a mechanism of compliance that can be applied to these cases without the keystone of the licenses associated with the access control mechanism. In completing its study of the necessary administration of DVB-CPCM, CM-CP and IPRM need to address these issues that are to a certain extent new in the DVB experience. CPCM adoption will require compliance and administration to ensure interoperability and faithful implementation of the specification, including in particular compliance to the protection requirements.