

# The challenges of rights management



**David Wood**

*Head of Broadcasting Technology, EBU*

**This article gives a brief overview of some of the tools available for protecting the copyright of broadcast material; namely, conditional access, digital signatures, copy protection and watermarking.**

## Introduction

A critical question for artists or programme service providers in the media world is often the same: *How can I make sure that the programme content I created is treated in the way I want it to be, after it leaves me? How can I be sure that I still have control over what happens to it?*

Rights management is a wide subject, but comes down to a set of tools and methods for answering this question – or helping to answer it.

Individual pieces of the rights management jigsaw have been developed, and continue to be developed in separate ways. There are many ways of attacking the problem. There are many weak spots along the journey of the programme from the source to the rightful recipient. Rights management is about using different pieces of “band-aid” to cover the weak spots.

If we can consider these matters globally rather than piecemeal, the result could be more effective, more purposeful and more useful.

The story of rights management today is incomplete and continuing, in that more rational and better ways of using combinations of rights management tools will inevitably emerge, as technologies and legal specialists understand better what needs to be done, and the options for doing it. It is quite a complex – though not a really complicated –

subject. Different combinations or rights management tools will be needed for different circumstances.

## Conditional access

The first weapon in the rights management armoury is the scrambling of programme content. This is a device to control who watches the programme.

The programme content that is delivered over the transport system is arranged to be unintelligible to all, except those who have paid for the right to watch it, or those the programme provider decides should have it.

The general approach to encryption, as used in broadcasting throughout the world today, owes much to the studies in the 1980s of conditional access for the MAC system. These systems are sometimes generically called “private key” encryption systems. This is not a good term, because the key is made available to the public. A better descriptor is “single key”. The same key that “locks” away the programme at its source, is sold to the public and used to “unlock” the programme in their homes.

Predating the studies of conditional access for broadcasting, cryptologists devised more sophisticated systems which were called “public key” systems. This is also a poor term, because the key in question is not particularly more public than a private key. A better term is “two-key”. One key locks the item away at source, and a second and different key unlocks it at the destination.

You can entrust an outside agency with one of your two keys – the one that unlocks the item. He/she becomes the “trusted third party”, and people who want the key have to go to him/her to get it. The trusted third party is something like a credit rating agency, and only gives away your unlocking key to those it knows are going to pay up, etc.

By using the two keys in a particular way, a sender can target a specific individual to receive the content. Thus, a two-key system can be used to send money over a network. One important manifestation of two-key systems is their widespread use for electronic document delivery and electronic commerce over the Internet.

In some senses, if you go into the detail, you find that the one-key system is a kind of sub-set of the two-key system. Furthermore, for some services, both can be used. For example, a one-key system can be used for delivering public-offer programming to the public, and a two-key system can be used to send cash back to the programme provider, to pay for it.

## Digital signatures

A second weapon in the rights management armoury can be the digital signature. This is a device you use if you want to make sure that no-one tampers with the programme content, en route to whomever is finally supposed to have it.

The digital signature system examines the content (when it is in the form that you want it to be) then generates a number, which is like a short time-frozen snapshot of the programme. If, later on, you check this time-frozen snapshot against the programme and it doesn't match exactly, you know that someone has tampered with the programme.

The digital signature began as a tool for checking that no-one had tampered with an electronic message en route. It can also be used for programmes or segments of programmes. The digital signature is relatively short in length, and is usually sent along with the content itself. At the recipient's end, by comparing the digital signature with the programme itself, the user can tell if anything has been changed. This can be of value, and has a somewhat similar role to a signature on a letter – it is a guarantee that the content is exactly as the sender intended it to be.

## Copy protection

A third weapon in the rights management armoury is “copy protection”. This is a system designed to stop unintended recordings of programme material.

Copy protection can simply be a signal which is conveyed alongside the programme. In the CD world, there is a standardized *copy protection signalling* system, which is intended to prevent copying of the content in digital (and therefore high-quality) form. There are a series of signalling bits, which can be read and understood by a digital recorder. They can authorize:

- ⇒ no digital copies;
- ⇒ one digital copy only;
- ⇒ multiple digital copies.

The signalling flags can be set by the content provider for whichever of the above options is the right one for the service. There is also the facility for doing this with digital radio via DAB, and digital television via DVB.

### Abbreviations

<b>BDB</b>	British Digital Broadcasting
<b>DAB</b>	Digital Audio Broad-casting
<b>DCT</b>	Discrete cosine transform
<b>DVB</b>	Digital Video Broad-casting
<b>DVD</b>	Digital versatile disc
<b>MAC</b>	Multiplexed analogue component
<b>MPEG</b>	Moving Picture Experts Group
<b>URL</b>	Uniform resource locator

If you can't trust the digital recorder to do the right thing by means of a signalling pulse, there are other options to prevent people from making unauthorized copies. These could be called "*enforced copy protection*" systems. It is also possible to add signals to the broadcast signal (or add them in the receiver), which disturb the recorders to the extent that they can't make a recording, even if they wanted to. One of the systems which do this is called "*Macrovision*". It is used in conjunction with DVDs to prevent users from making copies on their home VCRs.

These systems are not foolproof. It is quite possible to buy mechanisms to defeat copy protection signalling, as well as enforced copy protection systems.

Macrovision has reached agreements with the Hollywood film community. The system is already used by BDB in the UK. BDB digital receivers add the Macrovision signals on request from the digital broadcaster. The value of this type of system for public service broadcasting, and the way it is used, are important matters on which the EBU needs to agree.

## Watermarking

A fourth weapon in the rights management armoury is "watermarking". A watermark is an indelible hidden code word or label, which allows the origins of the material to be checked, or provides a means to transport other information. It is as if the programme is given a stamp when it is made, which describes its ownership etc. The idea is that watermarks are arranged to be invisible, not to disturb the programme in any way, and to be impossible to tamper with.

Watermarks are used in analogue television and in audio. They can consist of signalling which is hidden in a part of the picture or sound where they are not perceived – possibly tucked in beside large objects or sounds where they would not be noticed.

Watermarking is relevant and important in both *digital audio* and *digital video*. Quite different techniques may be needed in these two areas, because the nature of the content signals is different. Nevertheless, a common approach to watermark code tables for both would be beneficial, and the cross fertilization of ideas could also produce a better over-all system.

The OCTALIS project, in which the EBU participates, has developed a digital video watermarking system for MPEG-2 encoded video, which has been tested via *Eurovision* [1][2]. Essentially, the system takes a 64-bit word, which is a link (rather like a URL) to details of the ownership and origin of the programme, and then hides it in those DCT coding blocks that have high spectral occupancy, and thus where it will not be noticed. The system works well in the sense that the watermark is virtually invisible and, in any event, it simply adds noise to the visible programme content.

## Panel 1

### Requirements for the watermarking of broadcast material

A preliminary list of requirements is as follows:

- ⇒ A watermarking system should be developed as a means of delivering – via the air, a cable or a recording machine – an appropriate hidden metadata which conforms to an EBU-agreed metadata scheme for broadcasting.
- ⇒ A watermarking system is needed today for both video and audio. In future, a multimedia watermark will also be needed.
- ⇒ The watermark should be arranged to be impossible to erase or change, to be completely hidden from the viewer and listener, and not disturb the picture or picture quality, sound or sound quality, in any meaningful way.
- ⇒ The watermarking system should principally be arranged to be still present in the analogue signal, so that it is still readable on a pirated analogue tape of the programme, since this is most likely to be how the programme will be pirated.
- ⇒ The watermark should be invisible on all types of home displays, including flat-panel displays.
- ⇒ The watermark must be present on all frames of the television signal.
- ⇒ The watermark must be electronically readable.
- ⇒ The watermark must cope with zooms, etc.
- ⇒ The BER must be negligibly small.
- ⇒ Multiple watermarks must be able to co-exist.

A preliminary list of requirements for broadcast watermarking, prepared by the BMC, is shown in *Panel 1* (on the next page). This is intended to serve as an input to the EBU's new WTM project group, which will examine watermarking for the whole broadcast chain.

A new chapter in broadcasting technology is just beginning.

## Bibliography

- [1] J. Barda and L. Cheveau: **Eurovision – network security through access control and watermarking**  
EBU Technical Review, No. 281, Autumn 1999.
- [2] J. Barda and L. Cheveau: **Access control and watermarking**  
EBU Technical Review, No. 282, April 2000.