Decoding of Encrypted Content

Thomas Haring

Future standard: CI Plus

The currently used DVB standard provides for encrypted channels to be decoded according to the following procedure: A subscriber receives a smart card from their content provider. This smart card is equipped with a key that is required to decode encrypted channels and/or programs. The relevant key is sent to the card via satellite. As each card features a unique serial number content providers are in a position to activate or deactivate each individual smart card as necessary. In order to decode the encrypted transport stream transmitted by the satellite a code is required which is re-generated every few seconds. This code is calculated directly by the CI module or – in case a proprietary receiver with built-in card reader is used – by the internal chipset of the box, using a number of different parameters which include – among others – the key that is stored on the smart card.

Pay TV content can be decoded either by proprietary receivers – which means receivers that are specifically designed for a certain system or provider – or by using a common interface (CI). Some content providers such as Sky Digital in the United Kingdom provide proprietary receivers and consequently force their customers to only use certain approved receiver models which feature an integrated smart card reader and an internal chipset on the main board that takes care of decoding encrypted signals.

This type of encryption holds a number of benefits for providers (easy change of encryption system, full control over which features are supported by proprietary receivers, etc.). Subscribers, on the other hand, are left with no choice and have to take what their provider deems right for them. For example, content providers are able to determine that recordings that are saved on the internal hard disk cannot be transferred to external storage media such as DVDs. Or even some EPG features may be blocked, such as searching for programs on channels that are not part of the subscribed package. End users have no way of selecting alternative receivers that might offer all the features they are looking for.

Sky Digibox HD for reception of encrypted Sky Digital channels

Smart card for reception of encrypted pay TV channels

If, however, a content provider allows the use of CI (common interface) modules, subscribers are free to use the provided smart card in any receiver they like, provided it is compatible with the CI standard. This option gives full control to the user rather than the provider, as any CI compatible receiver can be used, and whenever new features become available a new receiver can be bought and used.

The so-called common interface is an interface based on PCMCIA (Personal Computer Memory Card Association). It measures 10 by 5.4 by 0.4 mm and is available for a whole range of encryption systems including Irdeto, Viaccess, Mediaguard, Nagravision and Cryptoworks. A CI module simply has to be inserted into the corresponding slot on the receiver and instantly adds the option of pay TV reception with a valid smart card. Table 1 lists the most widely used encryption systems and whether CI modules are available for them or not.

Table 1: Overview of some encryption systems

Encryption system	Developed by	CI Modul	Provider
IRDETO	Irdeto Access	YES	Multichoice Netherland
CRYPTOWORKS	Philips Electronic	YES	ORF, Digiturk, UPC
NAGRAVISION	Kudelski SA	YES	Premiere, Kabel Deutschland, Dish Canada
SECA MEDIAGUARD	Societe Europeenne de Control D`Access	YES	Canal+, TV Vlaanderen
VIACCESS	Viaccess SA	YES	TPS France, SF
CONAX	Telenor	YES	Canal Digital
VIDEOGUARD	NDS	NO	Sky
POWERVU	Scientific Atlanta	NO	Transmissions between TV stations, feeds, US Army

Everyday use

As long as a standard CI receiver is used for watching an encrypted channel everything works smoothly and no problems should arise. While a subscriber is watching pay TV the provider is constantly transmitting new keys to the smartcard so that the decoding process is not interrupted.

The advent of PVR receivers and the possibility to save the transport stream of a digital channel directly onto a hard disk has revealed some weaknesses of the decoding process. In general, a smart card can only generate the required code for channels that are transmitted on a particular transponder, which means that while it is possible to decode two channels simultaneously (one for watching live, the other for recording), these two channels need to be on the same transponder. If they are on different transponders, only one channel can be decoded while the recorded channel is saved with encryption in place, because the CI module can only deal with one transponder at a time.

If you want to solve this problem you can of course use more than one smart card and CI module, but quite honestly, who is able or willing to afford that? That's why almost all PVR receivers are designed in a way that allows storing encrypted content on their hard disk as well. This means that the (second) encrypted transport stream is saved in an unprocessed format and as soon as a user calls up the recorded program it is dealt with as if it came right from the satellite, and it is decoded on the fly by sending the data from the hard disk to the CI module first.

While this is a solution that certainly has its merits, it also comes with a major drawback: Content providers change the key on their smart cards at regular intervals, and once this has happened the CI module is no longer able to generate the code required to decode data that was stored before the key change. Depending on the provider the key change intervals can range from several times a day to once every few months. The result, however, invariably stays the same and any recording not decoded by the time the smart card key is changed via satellite is lost for good.

Some smart manufacturers quickly came up with a better solution: They allow decoding and re-saving an encrypted recording so that you end up with a decoded event that is saved on the internal hard disk and yours to view without limitation. While some receivers initiate this procedure automatically, others require manual activation. What happens in each case is that the encrypted recording is sent to the CI module for decoding and then stored again on the hard disk.

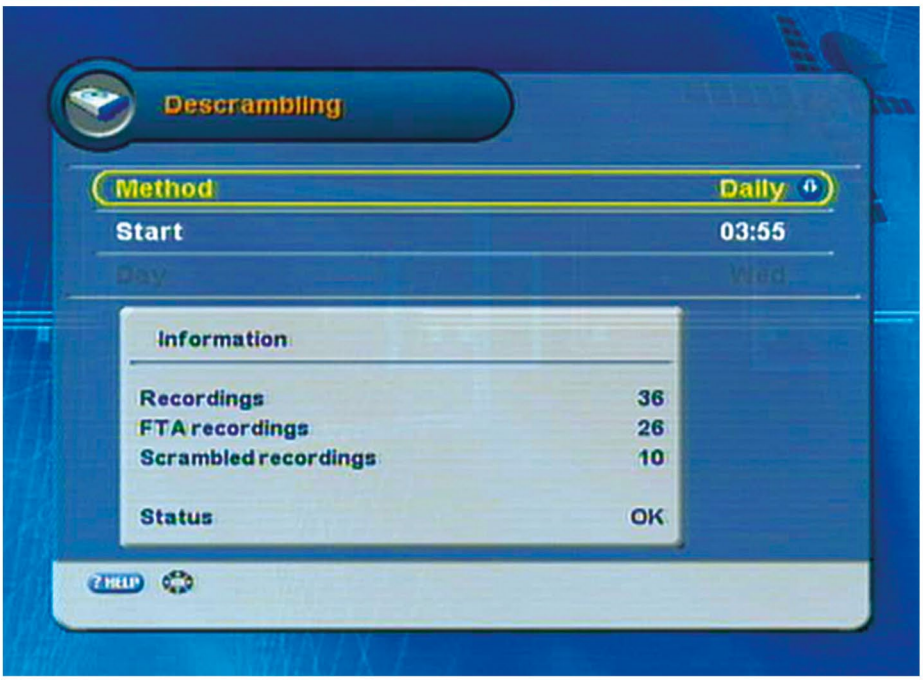
Irdeto CI module

The use of a card splitter in combination with a second CI module is another way of working yourself around inherent smart card limitations. This way the smart card is used twofold by not inserting it into the receiver but into a dedicated control box instead which in turn is connected via cable or WLAN to two cards that are slotted into the CI modules in the receivers. This way two different pay channels can be recorded simultaneously using only one smart card.

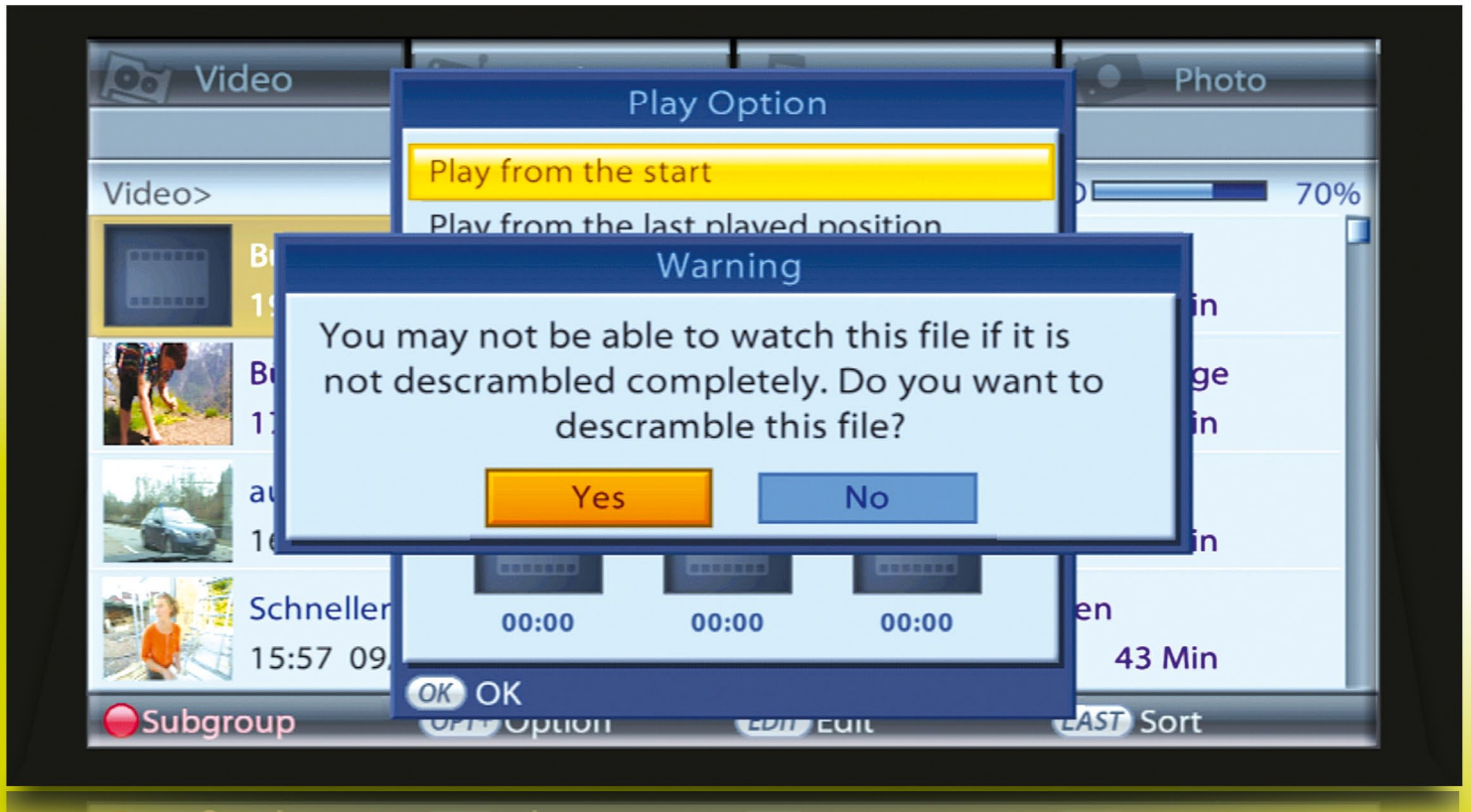
What does the future hold?

Right now a lot of effort is focused on further developing the CI specification with a project called CI Plus. This new standard will not be compatible with the current CI standard, which implies that in future subscribers of pay TV using CI Plus will have to buy new receivers. What most clearly sets apart CI Plus from the current standard is its integrated copy protection mechanism which can make it impossible to copy recorded pay TV content from a receiver's internal hard disk to any other storage medium. In addition, with CI Plus it will be possible to better protect children or minors from viewing unsuitable material. While the latter certainly is a most welcome development, imminent copy protection is a matter of heated debate. After all, even a single and perfectly legal copy of a recorded movie for private use will become a thing of the past if this feature is implemented. Users would be left with no choice but either to keep all recordings on their hard disk (which might eventually cause some storage capacity issues) or to wait until a movie they like is broadcast again.

What the new CI Plus specification suggests, however, is that content providers are free to decide themselves whether or not to activate these copy protection features. So let's hope the rules of the marketplace will finally determine that only those providers will stay in business successfully that allow their subscribers to make a DVD or Blu-Ray copy of their favourite recording.



Automatic decoding feature of a receiver



Decoding feature of a receiver