BISS

Jan 2017

BISS is supported using an optional card that sits on the encoder motherboard. If the option is fitted and correctly licensed, you will be able to encrypt your content using either BISS mode 1 or BISS E.

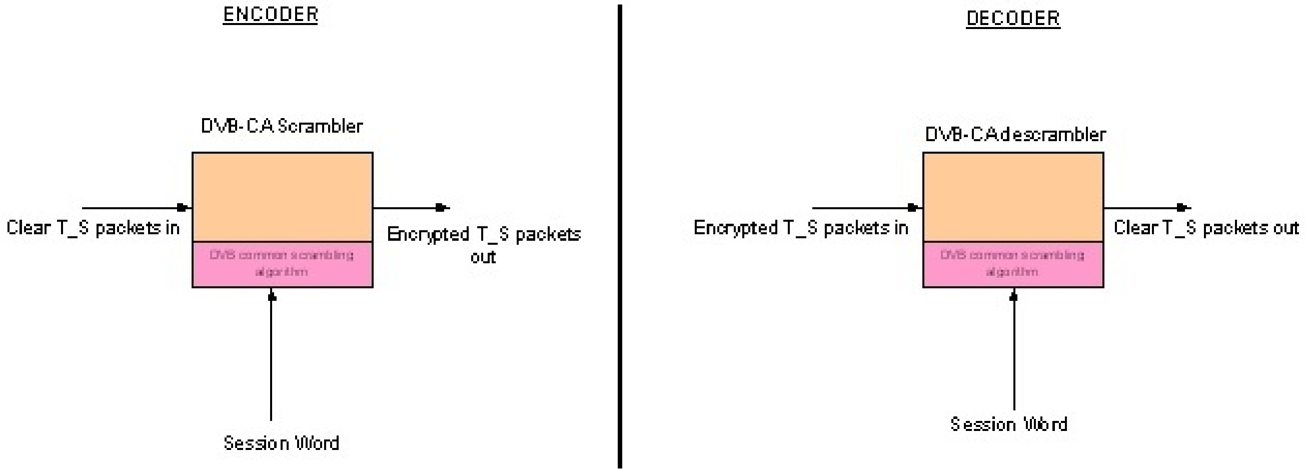
Document and Software Download

Download this document and the BISS SW

Here

BISS Mode 1

BISS mode 1 uses a DVB-CA scrambler in the encoder to encrypt services within the transport stream. To achieve this, the DVB scrambler needs to be provided with a key which determines the encryption algorithm used to perform scrambling. With BISS mode 1 this key, known as the “clear session word” or CSW, is simply entered into the encoder using the front panel. If the same key is entered into a BISS compliant receiver, then it will decrypt the encrypted service (s).



With BISS mode 1, The session word is simply entered into the decoder. As long as this matches the session word entered into the encoder, the transport stream will be decrypted.

BISS mode 1 is the simplest implementation of BISS and is useful for protecting relatively short transmissions, such as a sporting event. The CSW is normally generated at random by the user and is then communicated to the staff at the receive sites authorized to decrypt the transmission, so that they can enter the same key into their receivers.

When using BISS mode 1, you must enter the 12 digit CSW into the encoder. On most TANDBERG decoders, the CA menu is in menu 4. You will need to ensure the receiver is set to use BISS mode 1, and then enter the same CSW into the decoder that has been entered into the encoder.

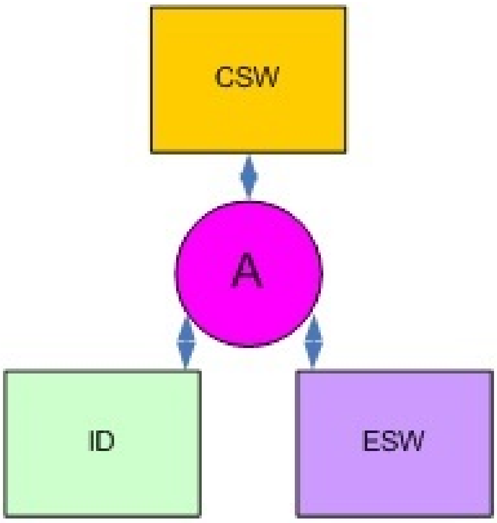
BISS E

When using BISS mode 1, anyone privy to the CSW being used can successfully decrypt the transmission. The risk is that someone who knows your CSW can illegally pass this to others, causing a security breach.

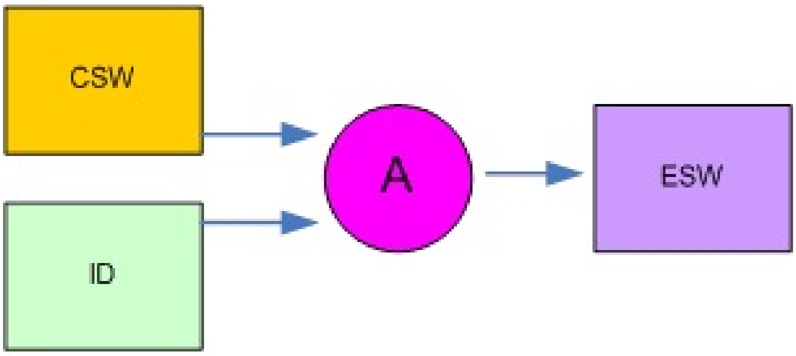
You can prevent clear keys, which is what the CSW is, from being passed on to others by using BISS E to encrypt it so that it is only decoded into its clear form by an algorithm within the receiver. The concept is simple: Rather than provide the CSW which will allow any receiver to decrypt, you provide two other numbers that if correct, will return the correct CSW within the receiver when these are passed internally through the BISS algorithm.

In BISS terminology, these two numbers which together describe the CSW are known as the “Encrypted Session Word” (ESW) and “injected user ID” (ID). A critical concept to understand with BISS-E is that the ESW and ID can be (and usually are) different for each receiver. This is because it is the combination of ESW and ID that matters. Just as 4+2 and 3+3 both equal 6, different values of ESW and ID in combination can also reflect the same CSW when passed through the BISS algorithm in a receiver.

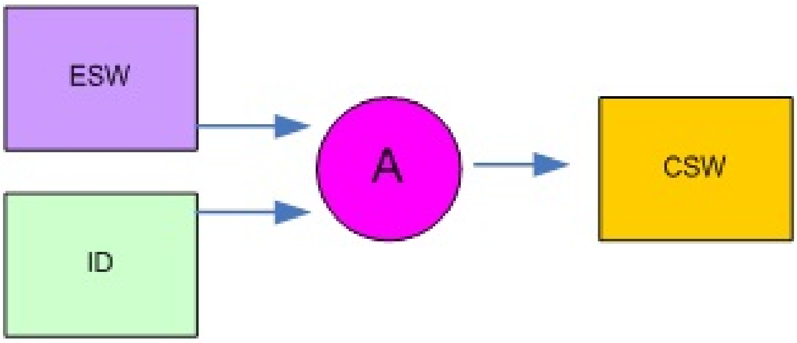
The fact that this is the case is critically important because if one of these numbers (the ID) is fixed and electrically burned into a receiver, then only the correct ESW that works as a combination with this ID to return the correct CSW can be used. In other words, if an ESW is issued for this receiver, then it will only work in that receiver if the remainder have different IDs.



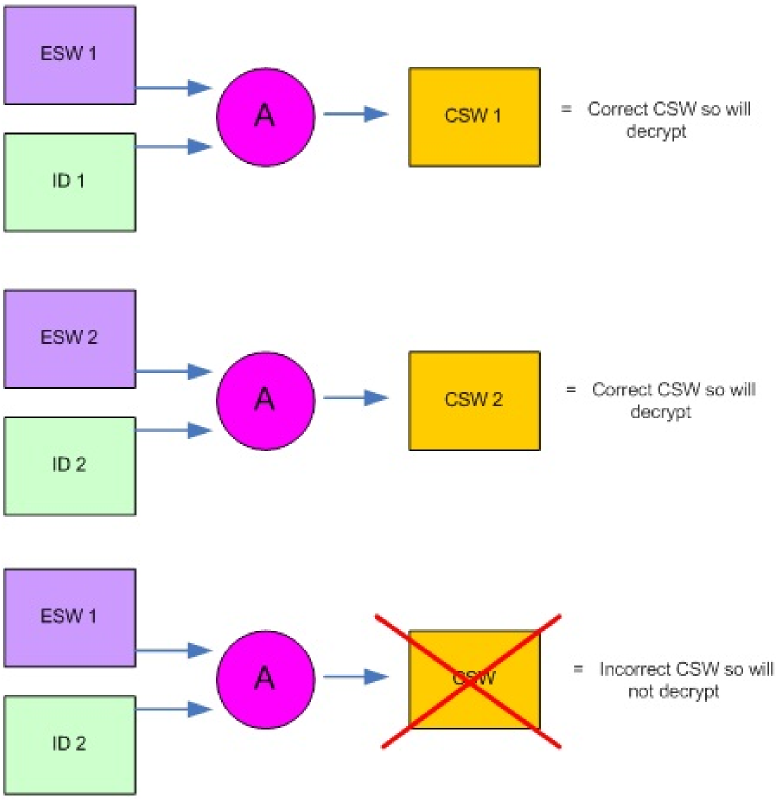
The CSW, ID and ESW are all linked by a BISS E algorithm. If you know any two, you can derive the third.



When generating BISS-E keys for distribution to clients, you will know the CSW and the ID for each receiver. A software application then generates the ESW.

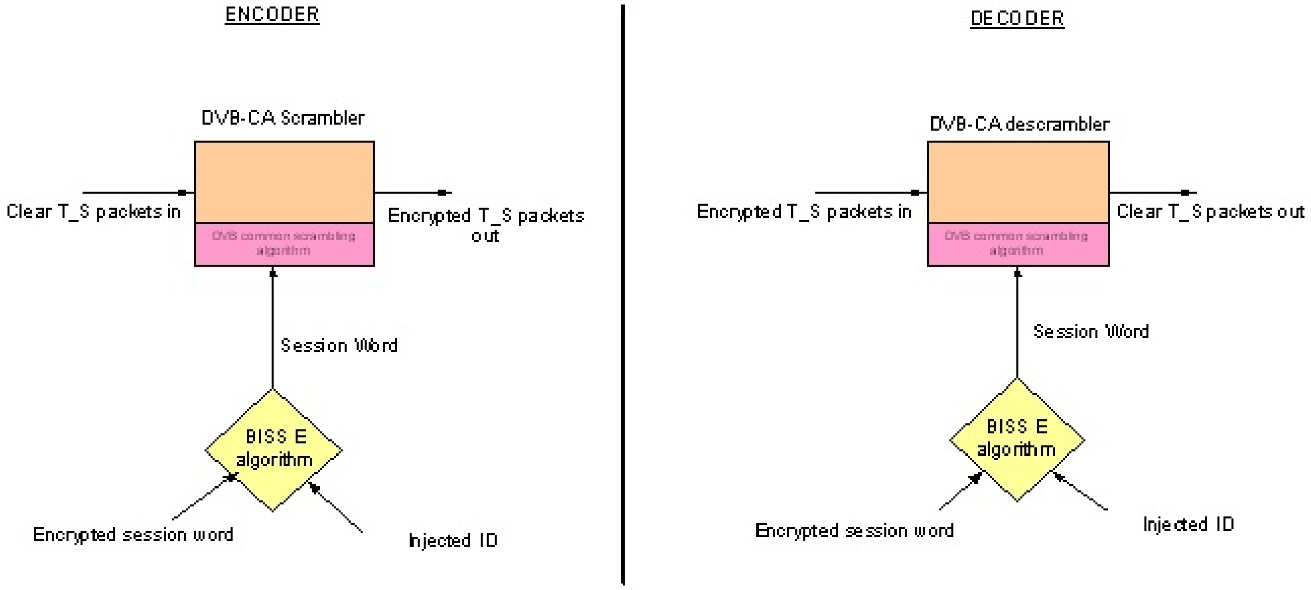


In the receiver, you must enter the ESW. The ID will already be burned into the receiver and in most cases will only be known to the system administrator generating the keys. The ESW and ID combination will be used by the receiver to internally derive the CSW. The receiver will only de-crypt correctly if the derived CSW is correct and matches the CSW used in the encoder. In most cases you cannot read the ID back from the receiver and so a receiver operator will not be aware of the value, but may be able to select from a few pre-stored ID’s.


ESW 1
ID 1
A
CSW 1
= Correct CSW so will decrypt
ESW 2
ID 2
A
CSW 2
= Correct CSW so will decrypt
ESW 1
ID 2
A
CSW
= Incorrect CSW so will not decrypt

In the above, the top key set is valid (1) and will provide the correct CSW. The same is true for keyset 2. However, in the last example, the wrong ESW has been used for ID2, and so the correct CSW will not be recovered inside the receiver. This example illustrates what would happen if there were 2 receivers with different ID's, and the recipient of ESW1 decided to pass it to another customer having a receiver with a different ID. The combination of ESW 1 and ID 2 would generate an incorrect CSW and the receiver would not be able to decrypt.

The same concept is used in both the encoder and the decoder and the algorithm used to relate the ESW, ID and the CSW is the same in every BISS-E compliant device.



The encoder and decoder both normally need an ID and ESW to be entered. The only difference is that the ID in the decoder is normally pre-set and cannot be read or changed. This stops key-sharing between customers since an ESW will only work in a receiver with a correct ID, and if all the ID's are unique, then an ESW will only work in the one, intended receiver and no other!

There are a number of ways in which this concept can be implemented and used in practice. The BISS standard lists two standardized ways known as “user mode” (which is mandatory) and “Buried_ID” (which is an option to EBU-TECH 3292 and is not implemented by TANDBERG for security reasons because it does not prevent the ID within a receiver from being read back by the user). In addition, there is a proprietary “TTV” method which is implemented on all TANDBERG receivers.

ser mode allows the ID to be entered into the receiver manually. Anyone can enter this via the web browser or front panel, but once entered the number cannot be read back again. It is expected that operators will enter the ID into the receivers before shipping them to end users, and will record the values on a database. In TANDBERG receivers, it is possible to enter up to two different IDs into the receiver, so that the end user can easily choose which is active for use with different networks for example.

TANDBERG receivers need to be put in BISS E “user mode” to allow entry of the ESW and the ID. Importantly, these numbers may either be the same for all receivers, or they could be different. This is because what is important is that the combination of ESW and ID results in the correct value for the CSW when processed by the BISS E algorithm. Creating a valid pair of CSW and ID will require knowledge of the CSW that you intend to use as well as the BISS E algorithm that relates all of these parameters. TANDBERG provides a software tool embedded within the encoder to perform this function. This is described in more detail later.

Fixed mode As an alternative to entering the ID through the front panel, which provides the risk of it being inadvertently over-written later, it is possible to electronically burn it into the receiver. This is known as “fixed ID” mode. The mode of operation is otherwise the same as with user mode (above). It is sometimes possible to store more than one burned-in number per receiver.

It is only possible for the manufacturer or specialist service departments to burn numbers into a receiver, and so this method provides an excellent way of obtaining a secure ID that is unique and that the user cannot change or read back from the device. This mode is also widely inter-operable between receivers and is used by large organizations (such as EBU).

TTV Mode The ID can be derived automatically from the electronic serial number of the receiver. Please note that the electronic serial number is different to the unit serial number printed onto the identity label. Using this electronically burned-in serial number means that each receiver will have a unique ID that the user cannot change.

This also means that a unique ESW will be required for each receiver. The ESW will only work in the receiver possessing the correct serial number (and hence ID). Only this combination will result in the correct CSW being generated when this combination is passed through the BISS E algorithm. Using this method is proprietary to TANDBERG receivers, and is selected by placing the receiver in “BISS-E TTV” mode.

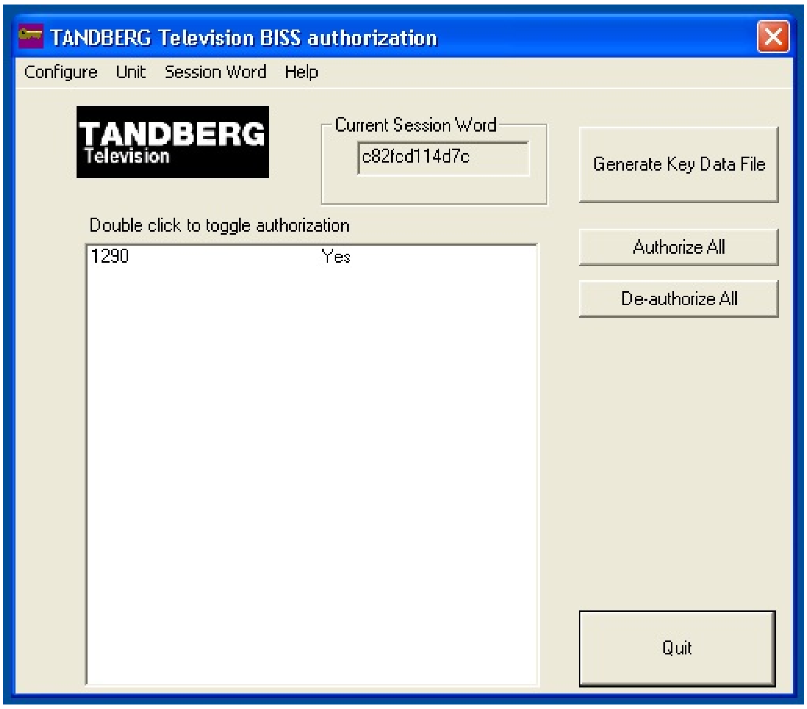
It completely prevents the possibility of valid keys being passed to others in an unauthorized way. Additionally, since a proprietary technique is used in addition to the standard BISS tools to translate the serial number into what actually becomes the ID that is used by the BISS algorithm, the fact that the electronic serial number is known and freely displayed on many devices including TT1260, TT1280 and RX1290 does not compromise security.

This is because knowledge of the BISS algorithm alone is not enough to recover the ID that our proprietary technique creates; To achieve this you must have knowledge of how the serial number is used to create the ID which is kept internal to TANDBERG Television. The TANDBERG BISS E software tool is used to create the keys in the normal way and is described in detail later in this section. The tool is able to detect automatically that a TTV serial number has been entered as the receiver ID from the number length, and will then apply the proprietary process that converts it into a standard-length ID.

Using BISS E

Once the theory is understood, using BISS E is easy. To start, it will be necessary to configure the encoder and then configure the receivers. Both steps require the use of the TANDBERG (or equivalent) BISS E key generating software. This software is embedded within the encoder, and can be down-loaded onto a PC via an Ethernet connection. To do this, proceed as follows;

1. Establish an Ethernet connection between the PC and the encoder, as though preparing to access the web-browser in the normal way.
2. When entering the IP address of the encoder into the web browser, follow with “/advanced” (for example, enter 192.168.22.50/advanced)
3. Go to “save / load” tab and “download BISS key generator”. Run the installation wizard and install the software onto your computer. You should see the following user interface when the software is run.



Using the software is extremely easy. You will need it to configure the DSNG encoder and all of the receivers correctly.

Configuring the DSNG encoder

When in BISS E mode, the DSNG encoder will need to be configured by providing an ESW and ID which derives the CSW that you wish to use. Although the encoder has a menu option for the CSW to be entered directly, this is in fact disabled in BISS E mode, and any entries made into it will be ignored. The only active menus are the "encrypted session word" and the "injected user ID". To generate these keys, you must create a database entry for the encoder and assign it a randomly generated ID. To do this, go to

UNIT, NEW, and then under the NAME heading, enter the description "DSNG Encoder". Also enter a 14 digit number (please choose this at random) and then save the entry. You have now listed the DSNG encoder in the database and assigned it an ID. The next step is to create the CSW that will be used. The CSW is also generated at random, and the software tool has a random number generator included to perform this task for you. Simply go to SESSION WORD NEW and accept the warning. The "current session word" tab will update with a new randomly generated number. The final task is to use these two numbers (the CSW and the ID) to create an ESW. To do this, click the "authorize all" tab and then "Generate Key Data File". This will create a text file which you can now view, containing the ESW Enter the ESW and the ID into the DSNG encoder, and internally these numbers will generate the same CSW that is currently shown by the software. You should never tell anybody what the CSW is. With BISS E, there is no need to know what the clear session word is outside the task of generating the ESW and ID that will be used by customers.

Please note that this is the ONLY difference between BISS-E and BISS mode 1. Both standards are inter-operable in that the CSW is the same. With BISS mode 1, the CSW is simply known by all and entered directly, where as in BISS-E the CSW is "hidden" and only derived internally within the equipment using the combination of ID and ESW. Since this is the case, if you do know what the CSW is then please appreciate that there is no difference between using an encoder in BISS-E mode and entering a ESW and ID to generate the CSW, and putting the encoder in BISS mode 1 and entering the same CSW directly. Either will provide exactly the same outgoing transport stream. Likewise, if the ESW is not kept secret from receiver operators, they can use it to illegally decrypt your BISS E transmission by placing the receiver in BISS mode 1 and entering the CSW. The CSW can also be passed on to others who will also be able to decrypt your transmissions in the same way. It is therefore imperative that the CSW is maintained a closely guarded secret. The person issuing the keys using the software tool is the only one who needs to know the CSW since in BISS-E mode, both the encoders and decoders can be set up using the safer ESW and ID. Customers should also not know the combination of ESW and ID unless it is unavoidable since the BISS E algorithm is freely published making it possible for a technically experienced user to use the ID and ESW to work out what the CSW is.

Configuring the receivers uses a very similar process. If you are using "user mode" (as described earlier) then the process is identical. In the same way, you need to create a database entry for the receiver, randomly assign it a 14 digit "injected user ID" and then without changing the "current session word" value, press the "authorize all" and "generate key data file" tabs. You will now have the "encrypted session word" and "injected user ID" to enter into a receiver or multiple receivers. Of course, this combination will derive the same "clear session word" that the encoder is using (as long as the "current session word" value is not updated!)

If you are using the receivers in TTV mode, then when creating the database entry for the receiver, you must enter the correct serial number for the receiver. This will be the electronic DALLAS_ID for the receiver and NOT the serial number taken from the label on the side of the unit! Finding the Dallas_ID depends upon the receiver type. Some display the Dallas_ID on the web-browser; some need a software tool to read it from the receiver and some do not display it at all in which case it must be looked-up against the unit serial number on a database held within TANDBERG customer services. The number usually starts with 00080 and is a 12 digit hexadecimal number. When entering this number, the software will automatically recognize it as a 6-byte "unit serial number", which it automatically re-formats into a 7 byte BISS E compliant number. Using “fixed” key mode is identical to TTV mode in every way, except that the value of the fixed key must be known to the administrator and correctly entered into the database as a 14 digit (7 byte) number.

For security reasons, it is recommended that you periodically update the “clear session word”, but only when you are prepared to re-issue new keys for both the DSNG encoder and all of the receivers.

Providing increased levels of security and functionality: TANDBERG Director

Although the security provided by the BISS open standard is sufficient to protect most contribution feeds of short duration, it is not ideal for providing longer term protection of high value content and cannot help with the management of larger contribution solutions. TANDBERG Director has been engineered as the next step up from BISS in terms of both security and functionality and expands upon the capabilities of BISS by adding several layers of additional functionality. The key differences are as follows;

Security BISS provides “fixed key” encryption with manual distribution of the keys. Essentially, this means that the algorithm used for encryption only changes when a new session word is created by the user, and when this happens the new key must be communicated to the receivers manually. Director improves upon this by ensuring that the encryption key is changed every few seconds. To achieve this, a new key is generated (typically every 20 seconds) and is automatically and securely transmitted to the receivers. Tight control over timing means that the key changes happen seamlessly, providing a dramatic improvement in system security. The automated process means that you do not have to get involved with any part of this process, saving a lot of effort. The keys are securely transmitted in encrypted form to the receives using an ECM mechanism. Furthermore, if you are transmitting more than one service then each will be encrypted differently and will always have a unique key and separate ECM.

Receiver addressability The TANDBERG Director system provides full conditional access to precisely control what a viewer can watch. With BISS, the encryption key is used to control the security of the link and determine whether the viewer can watch the content. With Director, these two functions are separated. The security of the transmission is protected by the variable key system, making it highly secure. Unless the receiver can utilize the continuous stream of ECM’s which provide the key information in encrypted form, the original key cannot be recovered and so the link remains secure. However, even if the ECM can be decrypted by a genuine Director receiver, there is a further stage of protection to go through before the content can be viewed. This mechanism involves the concept of “entitlements” and means that the receiver must be specifically authorized for each programme it can decode. This may sound complex, but the Director system makes it incredibly simple. The power this provides is equally incredible since you control what each receiver is authorized to view putting you in complete control. Central to this mechanism is a scheduler where you can list all of the programs being aired for each channel. You can then assign an entitlement to any program you wish to protect. It’s that easy! The director system will automatically monitor the schedule and will securely carry the entitlement in the ECM message to the receiver. If it is a genuine Director receiver, then it will be able to decrypt the ECM and recover the encryption key, but it will also check the entitlement being carried in the ECM against a list of pre-stored entitlements that exist in a secure area of receiver memory. If there is a match, the key will be used to decrypt. If there is no match, then decryption will not take place and the user will be informed that viewing of the content is not authorized. Since there is a separate ECM for every service, this process will occur independently on every channel, allowing the content to be protected individually in a multi-channel environment.

Entitling the receiver

Since a receiver must have the correct entitlements to access the content a user has subscribed for, it is important to have a quick and easy means of controlling the entitlement lists within a receiver. Director achieves this by creating a secure message that is transmitted over-air called an EMM. The EMM is encrypted and addressed to applicable receivers automatically; all you have to do is choose the entitlement and then choose the receivers that will receive the command from a list! Entitlements can either be added or removed from the receivers in this way. There are other ways in which entitlements can be managed, but in every case, Director will wherever possible keep an up to date record of the entitlement status of each receiver to make the management process especially simple.

Sending receiver commands

Having developed such as simple yet powerful mechanism for sending messages to receivers over-air, we have now expanded this above the ability to simply send entitlements so that you can send hardware instructions to receivers as well. Using the same secure EMM mechanism, it is possible to instruct receivers to select another service, frequency change to another satellite, display an on screen message or lock out all user controls. This is just a small selection of the commands provided by Director, which importantly also includes the ability for receivers to start upgrading their software seamlessly over air. As with other director features, you have complete control over the entire receiver network and can choose whether an individual, a group, or all receivers are affected by your commands.