Basics of BISS scrambling

Newtec

Innovative solutions for satellite communications

Contents

- Definition of scrambling
- BISS modes
- BISS mode 1
- BISS mode E
- Calculation of encrypted session word
- Buried ID
- Injected ID
- Connection diagram
- Rate adaptation
- Back panel description
- Operation

Scrambling

- Scrambling is a way to transform transmitted data in order to allow reception only by parties that have a valid descrambling key.
- An open standard has been defined to allow different manufactures to implement the same scrambling system.
- BISS = Basic Interoperable Scrambling System

BISS modes

- BISS mode 0 : unscrambled (clear)
- BISS mode 1 : scrambled with session word (SW)
- BISS mode E : scrambled with encrypted session word (ESW)

- The session word is the key that is used in the receiver (IRD) to descramble the transmitted data.

- Remark that BISS-E uses the same scrambling algorithm as BISS mode 1 but that there is an additional encryption on the session word.

BISS mode 1

- BISS mode 1 uses a 12 digit hexadecimal key as session word. The session word has to be announced to all parties that are allowed to descramble the received data.

- Example : 123456ABCDEF

- The session word can easily be compromised, there is no protection when communicating it to the receive site(s).

BISS mode E

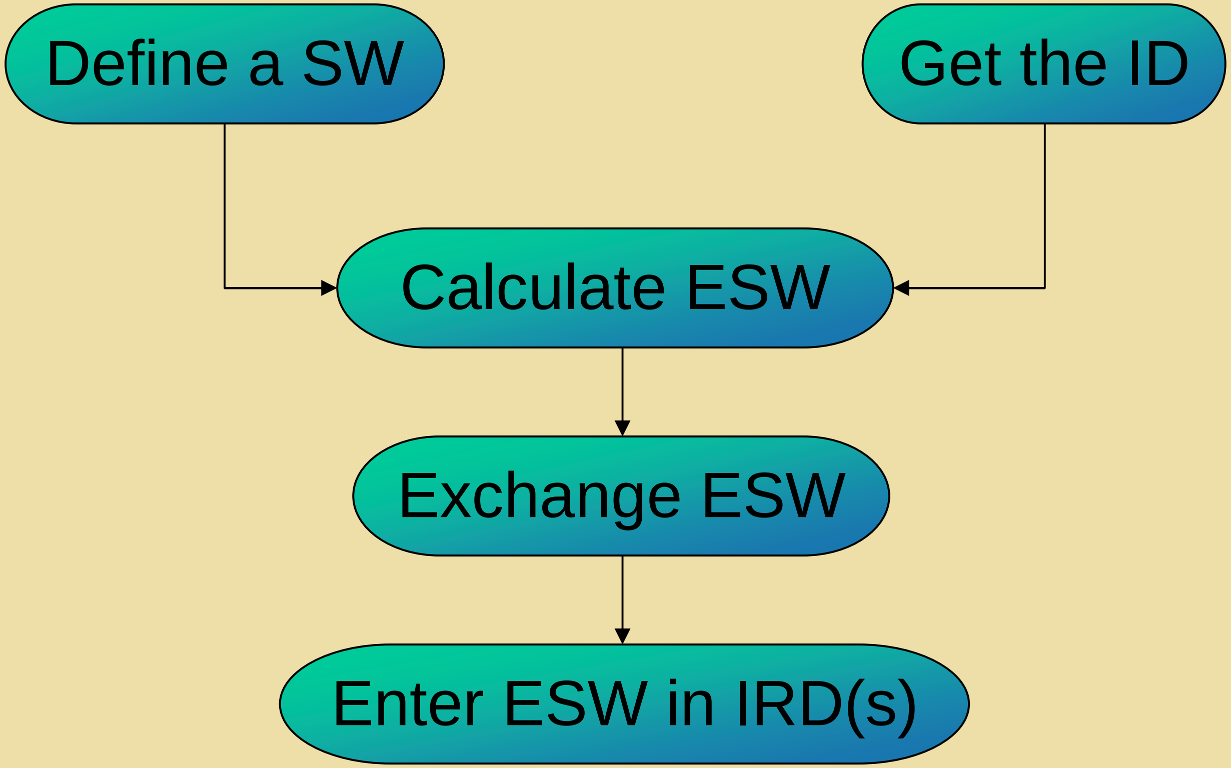
- BISS mode E : scrambled with encrypted session word (ESW)

- This mode uses the ID (identifier) of the receiver(s) and a session word to calculate an encrypted session word (16 digits hex)

- There are two possible IDs - buried ID
  - injected ID

- By encrypting the session word there is an additional protection on the session word. The ESW can be communicated using a non-secure channel since in order to descramble the received signal both the ID and the ESW need to be known.

Calculation of encrypted session word



To calculate the ESW the DES^3 algorithm is used

Buried ID

- Each receiver (IRD) holds a unique ID (cfr. serial number) that can be used to identify that specific receiver : this is called the buried ID.

- If you want to do a transmission that is to be received by only one specific receiver, use the buried ID to calculate the encrypted session word.

Injected ID

- An identifier can be entered (injected) in a receiver (IRD), this injected ID can be entered in a single or a group of IRDs.

- This allows a BISS-E protected transmission to a group of IRDs.

Rate adaptation

- MPEG null packets are stripped from the incoming transport stream. Then the scrambling algorithm is applied to the transport stream.
- After that, MPEG null packets are multiplexed with the scrambled transport stream (stuffing) to arrive at the desired output rate.

Operation BISS mode 1

- Connect the scrambler between the encoder and modulator.
- Select output interface rate (must be equal or higher than output interface rate of the encoder)
- Select BISS mode.
- In case of BISS mode 1 with clear session word, enter the 12 digit session word.
- Communicate the session word to the receive site(s).

Operation BISS mode E with buried ID

- Connect the scrambler between the encoder and modulator.
- Select output interface rate (must be equal or higher than output interface rate of the encoder)
- Select BISS mode.
- In case of BISS mode E with buried ID, get the buried ID of the IRD and use this together with a session word to calculated the encrypted session word (using the DES3 algorithm).
- Communicate the ESW to the receive site.

Operation BISS mode E with injected ID

- Connect the scrambler between the encoder and modulator.
- Select output interface rate (must be equal or higher than output interface rate of the encoder)
- Select BISS mode.
- In case of BISS mode E with injected ID, get the injected ID of the IRD(s) and use this together with a session word to calculated the encrypted session word (using the DES3 algorithm).
- Communicate the ESW to the receive site(s).

Summary

- BISS mode 1 => session word (SW)
- BISS mode E => encrypted session word (ESW)
  - SW + injected or buried ID -> ESW
- Rate adaptation

End

- Need more info?
  - contact customer support at techsupport@newtec.be
  - contact sales at sales@newtec.be
- Check our website at www.newtec.be
- Or give us a call at +32.3780.6500