SATEL

Document ID: FAQ-0032
Date: 17.5.2018
V1.4

SATELLINE-EASy product family with AES128 encryption

SATELLINE-EASy radio modem family models currently supporting the encryption:
- SATELLINE-M3-TR1, YM6310 and YM6315
- SATELLINE-EASy (without display), YM6510 and YM6515
- SATELLINE-EASy (with display), YM6560 and YM6565
- SATEL EASy-Proof, YM6585 and YM6485
- SATELLINE-EASy Pro, YM6813

Please contact SATEL for more detailed information regarding the radio network compatibility settings in radio network between different models (channel width, radio frequency etc.).

- The encryption key is generated from Main and Aux –keys, both with 32 marks. It is <u>mandatory for the user to insert both information fields</u> with the mentioned length keys.

- The options for generating the encryption keys are:
- Manually via terminal connection:
  - Programming → 7) Additional Setup → A)Encryption:
    - 1) Encryption
    - 2) Main key
    - 3) Aux key
    - 4) Key hash
  - SL commands
    - SL%Y=**n**
      (Set Encryption mode) **n**: 0=OFF, 1=ON
    - SL%Y?
      (Get Encryption mode) respond: 0=OFF, 1=ON
    - SL%K? or SL%A)
      (Get Key hash, respond is the same)
    - SL%K=<Main key>
      (Set Main key) 32 marks [0-9, A-F, a-f]
    - SL%A=<AUX key>
    - (Set AUX key) 32 marks [0-9, A-F, a-f]

- Automatically:
  - Password key to Configuration Manager → Configuration Manager generates automatically the Main and Aux keys.

- The equivalency of the encryption keys between radio modems can be verified from the Key Hash –information field. Last 4 marks indicates the equivalency [0-9, A-F].

- LCD UI does not include any of the encryption information or settings. Encryption support can be verified from the FW version (see FW version list).

- It is NOT possible to setup a radio network with encryption enabled by using both configuration ways, manual and automatic key creation:

  o Configuration Manager does not include the Main and Aux key fields, only possible to create keys automatically with password.
  o SL command and programming menus don't include the possibility to set the password to generate the Main and Aux keys automatically.

- SATEL radio modem models FW versions supporting the encryption:

  o 06.**29**.x.xx.xx for SATELLINE-EASy, EASy-Proof and SATELLINE-M3-TR1
      (06.**16**.x.xx.xx without the encryption)
  o 06.**30**.x.xx.xx SURV variant for SATELLINE-EASy
      (06.**23**.x.xx.xx without the encryption)
  o 06.**31**.x.xx.xx for SATELLINE-EASy Pro
      (06.**18**.x.xx.xx without the encryption)
  o 06.**32**.x.xx.xx SURV variant for SATELLINE-EASy Pro
      (06.**24**.x.xx.xx without the encryption)

- The encryption works only in SATELLINE-3AS –radio compatibility mode.

- It is not possible to update the SATELLINE radio modem to AES supporting firmware from standard firmware version or vice versa in the field. This task can be executed is SATEL factory premises and will be charged according to the service price list.

- It is possible to update/downgrade the FW version variants between the CRYPT SURV and CRYPT versions.

- The key is generated by using the distributed password used key + in the beginning of the data packet transferred changing 32 byte string. Every data packet is encrypted individually.

- The encryption adds the latency time in the order of 10ms to each sent data packet (<5 characters).

- It is not recommended to use the encryption with Source Routing with <10B message sizes.

NOTE1! SATELLINE product family with air interface AES128 encryption feature is fully compatible with equivalent SATEL radio modem products when the encryption is set to OFF state. The factory default value for the encryption feature is OFF state.

NOTE2! The Full CRC16 –feature shall be disabled when radio network includes SATELLINE-M3-TR4 and SATELLINE-M3-TR3 devices in together with other radio modems with the encryption feature enabled.

NOTE3! With the current latest FW version, 06.XX.3.63.16 CRYPT, restoring factory settings doesn't effect to the encryption settings.