Document ID: FAQ-0032
Date: 1.4.2020
V1.6

SATEL radios air interface encryption

Data security is often a concern when using radio communication. In SATEL radio products, strong AES128/256-bit encryption (CTR-mode) on the air-interface ensures privacy in the radio network. The principle of encryption in the radio path is to collect a certain amount of data to a shift register and manipulate it according to a certain rule. Every data packet is encrypted individually

The product models that support the encryption for the RF interface can be viewed in SATEL WEB sites at www.satel.com/products/. The radio models that doesn't support the encryption feature are compatible with the radio models with the encryption when the feature is disabled. The factory default value for the encryption feature is OFF state.

The setting state with the static, distributed encryption keys shall be set equally to the radios in the same radio network. The password or the keys should be kept in a safe place as the keys can't be read from the device after configuration. The equivalency of the encryption keys can be verified with key hash information from the device settings. In case the password is forgotten, a new password will need to be set for all the radios of the network.

AES is open source software from public domain. Author: Brian Gladman (U.K). The CTR-mode is SATEL's in-house implementation.

Please contact SATEL for more detailed information: Technical.Support@SATEL.com.

SATELLINE-EASy product (and variations) AES-128 encryption

The encryption key is generated from Main and Aux –keys, both with 32 marks. It is mandatory to insert both information fields with the mentioned length keys. 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 in the field. This task can be executed is SATEL factory premises and will be charged according to the service price list.

SATELLINE device models that support the encryption feature have differing FW version from the models that doesn't include encryption feature. Examples of FW variant numbering:

- ✓ 06.29.x.xx.xx for SATELLINE-EASy, EASy-Proof and SATELLINE-M3-TR1
  - 06.16.x.xx.xx without the encryption
- ✓ 06.30.x.xx.xx SURV variant for SATELLINE-EASy
  - 06.23.x.xx.xx without the encryption
- ✓ 06.31.x.xx.xx for SATELLINE-EASy Pro
  - 06.18.x.xx.xx without the encryption
- ✓ 06.32.x.xx.xx SURV variant for SATELLINE-EASy Pro
  - 06.24.x.xx.xx without the encryption

Document ID: FAQ-0032
Date: 1.4.2020
V1.6

Configuration 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 in Configuration Manager configuration SW→ SW generates the Main and Aux keys automatically

Notes:

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

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

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

- Encryption adds transmission latency in the order of 5 to10ms depending on encryption mode.

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

- Restoring factory settings does not affect to the encryption settings