SATEL

Document ID: FAQ-0032
Date: 29.10.2024
v.1.7

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. Depending on the encryption type, the process of encryption adds 5-10ms delay in the data flow to each sent data packet (<5 characters in AES128 and <10 in AES256).

The product models that support the encryption for the RF interface can be viewed in SATEL WEB sites at https://www.satel.com/products/radio-modems/#1-serial-radio-modem. 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.

SATEL-EASy+ product family AES-encryption

AES128-bit encryption is supported by default in the product models which support the air interface encryption feature. AES256-bit encryption is available as a DRM option (Digital Rights Management) in these product models.

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 in SATEL radio compatibility modes (SATELLINE-3AS, SATEL-8FSK-1, SATEL-8FSK-2 and SATEL-16FSK-1).

The encryption password key is generated by using Main and Aux –keys plus in the beginning of the data packet transferred changing 32-bit string. It is mandatory to insert both information keys with the mentioned length keys.

Options for generating the encryption keys are:

1. Manually via terminal connection: SL commands
2. Automatically with password via SATEL SW tools (generates automatically the Main and Aux keys). Manual modification of encryption keys is also possible via SW tools.

It is recommended to set up a radio network with encryption enabled by using only one selected configuration method. 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].

Device firmware

Radio models that support the encryption feature have differing FW versions from the models that don't support this feature. Examples of FW variant numbering:

- ✓ FW 10.x.x.x.**44** for SATEL-EASy+ and SATEL-EASy Pro+ with encryption support
  - FW 10.x.x.x.**45** without encryption support
- ✓ FW 07.**44**.x.x.x.x for SATEL Proof-TR4+ and SATEL-B2-TR4+ with encryption support
  - FW 07.**45**.x.x.x.x without encryption support
- ✓ FW 06.**29**.x.xx.xx for SATELLINE-EASy with encryption support
  - FW 06.**16**.x.xx.xx without encryption support
- ✓ FW 06.**31**.x.xx.xx for SATELLINE-EASy Pro with encryption support
  - FW 06.**18**.x.xx.xx without encryption support

It is not possible to update the radio modems without encryption support with encryption supporting firmware in the field. This task can be executed only at SATEL factory and will be charged according to the service price list.

SL commands

A terminal device can command or configure the radio modem by using Special Line (SL) commands. SL commands are applied especially in cases where radio modems are to be integrated seamlessly inside a system behind the integrator's own user interface. See device user manual for details.

Encryption feature related SL commands:

Command:	Description:	Response:
SL%Y=n	Set Encryption mode. Value of n: 0 = OFF 1= AES128 2= AES256 (DRM option)	OK or ERROR
SL%K=<Main key>	Set radio encryption MAIN key (32 characters [0...9, A...F]	OK or ERROR
SL%A=<AUX key>	Set radio encryption AUX key (32 characters [0...9, A...F]	OK or ERROR
SL%Y?	Get Encryption mode.	0 = OFF 1= AES128 2= AES256 (DRM option)
SL%K? or SL%A?	Get Key hash, respond is the same (Hex number, 4 digits [0-9, A-F])	OK or ERROR
SL**>	Save current settings as permanent settings	OK or ERROR

Notes:

- LCD UI doesn't include encryption parameters or information (encryption key hash).
- It is not recommended to use the encryption with Source Routing with <10B message sizes.

If you have any questions, please contact SATEL technical support at technical.support@satel.com.