

AES-256 Encryption Option

for

P4dragon DR-7X00 HF Modems

19/August/2021

© 2021 **SCS** Spezielle Communications Systeme GmbH & Co. KG



1. Introduction

The Advanced Encryption Standard (AES) allows state-of-the-art data encryption, now also directly on the **SCS** HF modems - i.e. “on the fly” of an on-going PACTOR connection. The application software thus no longer has to provide encryption in the case of secure/classified data that must be passed to the other side of an HF link.

The AES-256 option can be added as extra function to the firmware for DR-7800 and DR-7400 modems, i.e. as a customized modem firmware feature. Final activation of those customized items takes place with the help of an activation code, which can be obtained from **SCS** (or authorized vendors) and must be stored in the modem.

The AES-256 option allows all information transmitted via PACTOR to be encrypted, independently of the PACTOR level (PACTOR-1/2/3/4). As soon as AES is activated, PACTOR connections can only be established with distant modems that also use AES - and same AES key.

Encrypted data is indicated in the “Dat:” field on the display of the DR-7800.



AES-256 can also be utilized for other OSI Layer 1 / 2 protocols than PACTOR, like ALE or Robust Packet Radio.

Please contact **SCS** if you need an encryption solution tailored to your needs.

2. Commands required for AES operation

cmd: AES

Value range: 0-1

Default: 0

If set to 1, AES-256 encryption is activated. AESKEY command (see below) should first be used to set the desired AES key / key phrase before activating AES, otherwise PACTOR can no longer be used.

As soon as AES is activated, valid PACTOR connections to other DR-7X00 modems can only be established if the distant modem is also working with activated AES option and using exactly the same AES key (AESKEY command). Otherwise, the establishment of a PACTOR connection is blocked immediately after first, basic synchronization, i.e. as soon as the first user data is to be exchanged.

In order to store the AES 0/1 setting in the non-volatile modem memory, please use the SAP command.

Otherwise, encryption may no longer be activated after power-cycling the modem!

cmd: AESKEY

Value range: alphanumeric key or key phrases, length 1-80 characters

Allows to set the 256 bits long AES-256 encryption key. AESKEY accepts keys or key phrases of length 1 to 80 characters. It always generates a 256 bits long hash value from the key / key phrase and only stores that hash value as actual encryption key. The original key / key phrase is not stored permanently in the modem.

You can never deduce the original key / key phrase with the help of the modem. This reduces the risk of a security breach if very similar passwords are used in a network.

Nevertheless, the key / key phrase should be changed regularly in order to make decryption attempts based on the statistical analysis of long data sets impossible.

Example:

```
cmd: AESKEY This is my new AES Key Phrase!<CR>
```

```
NEW AES256 KEY:
```

```
-----
```

```
This is my new AES Key Phrase!
```

```
[KEY LEN: 30 BYTES]
```

```
STORED
```

The new AESKEY hash value is immediately stored in the non-volatile memory. You need not to use the SAP command for that purpose.

The special keys “kill” or “KILL” cannot be defined as user keys - but lead to full erasure of the AESKEY as well its corresponding hash value.

cmd: FLICENSE

Allows to enter a license code that activates customized modem firmware features and other customized items.

Please ask **SCS** directly or your dealer when you need a license key for special (firmware) features. You always have to send us (or your vendor) the modem serial number. All licenses are tied to the modem hardware. The modem serial number can be found at the label on the modem or can be retrieved by using the “sys sern” command.

Example for retrieving the serial number:

```
cmd: sys sern
```

```
Serial number: 0100001417160605
```

Example for entering the FLICENSE command:

```
cmd: FLICENSE 0100001417160605 EABATCGUOOLHCBFACCD5
```

```
OK
```

```
THANK YOU FOR LICENSING THE P4dragon FIRMWARE!
```

```
FLICENSE: 0100001417160605 EABATCGUOOLHCBFACCD5
```

SCS

Spezielle Communications Systeme GmbH & Co. KG

Röntgenstraße 36

63454 Hanau

GERMANY

Internet: www.p4dragon.com

E-Mail: info@p4dragon.com

Tel.: +49(0)618185 00 00

Fax.: +49(0)618199 02 38