Encryption & EtherHaul™ 7xx

Introduction

This document lists all functions of the EtherHaul™ 7xx series involving encryption.

Edition: B1, December 2018

SIKLU Communication Ltd.
43 Hasivim St., Petah Tikva, 49517 Israel

Encryption is applied in several functions of the EH-7xx series, as listed in the table below.

Function	Protocol	Algorithm	Notes
WebGUI Graphical user interface to manage the radio with an Internet browser, over an IP connection.	HTTPS with TLS	AES	Max key length = 256 bits
CLI Command line interface to manage the radio over an IP connection.	SSH	AES	Max key length = 256 bits
File transfer Secured file transfer protocol between radio and server, over an IP connection.	SFTP	AES	Max key length = 256 bits
SNMPv3 Secured management of radios, machine (EMS) to machine (radio), over an IP network.	SNMPv3	AES	Max key length = 128 bits
Traffic encryption between radios The traffic between the radio may be encrypted (requires SW license, and activation).	No protocol necessary between Siklu own radios.	AES	Max key length = 256 bits
SW image The SW image of the radio is signed and encrypted to prevent malicious SW updates.	No protocol necessary between Siklu radio and SW image.	AES	Max key length = 256 bits

All security functions and protocols are an integral part of Siklu EH-7xx series and their encryption capabilities cannot be changed or modified by the end-user.

Siklu EH-7xx series have no restrictions in sales; these products may be supplied by all Siklu distributors and resellers, as well as by their partners, to enterprises or private persons, by mean of cash-, mail order-, electronic transactions- or telephone sale, etc.

All Siklu products are intended for installation by trained individuals without significant support from the vendor.

- END -