Continental Divide Robotics

March 19, 2001

ESN Protection Description

The following measures have been taken to protect against fraud due to modification of the ESN or telephone software, in compliance with CF47, 22.919

(1) the stored ESN data in the FLASH device (which contains the information other than the ESN data) is encrypted. This ESN data is divided into four groups and interleaved with other data in the FLASH.
(2) The ESN is never transferred in a readable format across wires on the printed circuit board, nor can the ESN be read by probing the pins of any device.
(3) If the NVM (or data in FLASH) is altered, then the ESN becomes invalid and the phone will not operate.
(4) The FLASH device containing the main program software and encrypted ESN data, is permanently attached t the circuit board by soldering.
(5) The ESN write and change must be carried out at one of our manufacturing sites using a dedicated interface tool using special software, and interface box, and a PC. This interface tool will not be supplied to and vendor/distributor.
(6) To prevent fraudulent cloning and ensure that uniqueness of each ESN is protected, this product uses the Industry Standard Authentication Algorithm. This algorithm incorporates random challenges using shared secret data calculations to prevent cellular system fraud.

5255 S. Rio Grande Street Littleton, CO 80120 303-409-2990 fax: 303-707-0754