High Security Supplement

User Manual Supplement
for XPress™ Crypto Module
with FIPS 140-2 Security

90002005_D
June 7, 2011

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International.

Digi provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of, fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

This product could include technical inaccuracies or typographical errors. Changes are made periodically to the information herein; these changes may be incorporated in new editions of the publication.

To contact Digi International for more information about your Digi products, or for customer service and technical support, use the following contact information:

To Contact Digi International by:	**Use:**
Mail	Digi International 11001 Bren Road East Minnetonka, MN 55343 U.S.A.
World Wide Web:	http://www.digi.com/support/
email	http://www.digi.com/support/eservice
Telephone (U.S.)	(952) 912-3444 or (877) 912-3444
Telephone (other locations)	+1 (952) 912-3444 or (877) 912-3444

High Security Supplement

If you have a Digi radio with FIPS 140-2 Security, this supplement to the User Manual provides instructions for setting up the encryption. Please disregard the AES Encryption instructions in the regular manual: this supersedes them. A feature of the level of security provided is that there is no way to change the encryption method or key through the radio's interface. A separate port must be used.

The XPress™ Crypto Module is programmed and queried through a terminal interface. To use the terminal interface, you must install the following two pieces of software:

1. A driver that provides a virtual COM port through the USB connection. This driver can be downloaded from the Future Technology Devices International website, http://www.ftdichip.com. Follow their menu to the webpage for VCP drivers and choose the one that matches your operating system. Installation guides are also available in the documents section of the website.
2. A terminal emulator that will provide the user interface to the XPress™ Crypto Module. Options include Hyper-Terminal (available automatically in Windows XP and earlier operating systems) or Digi's XCTU available at www.digi.com/xctu. Customers using non-Windows OS can use tools such as minicom for Linux Ubuntu or ZTerm for Mac.

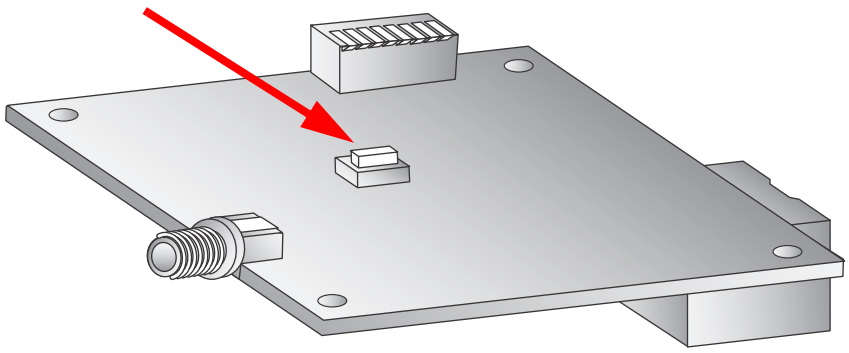
There are two roles defined for those having access to the programming interface, Crypto Officer and User. Each has a different password. Only the Crypto Officer is allowed to set the encryption method and encryption key. The user may examine self test results and firmware version only.

Step by step programming procedure:

1. Connect your hardware.

If your module is connected to a development board or is a standalone module, make sure the main power for the radio is off, and connect the XPress™ Crypto Module's USB port to your computer using a USB mini B cable.

If you have purchased an XPress™ Crypto Module as part of an XPress™ Ethernet Bridge, remove the cover of the XPress™ Ethernet Bridge using a Phillips screwdriver. The USB cable coiled inside the XPress™ Ethernet Bridge should be plugged into your PC's USB port. Power your XPress™ Ethernet Bridge using Power over Ethernet. Then press the reset button located in the middle of the XPress™ Ethernet Bridge PCB as shown in the image below.



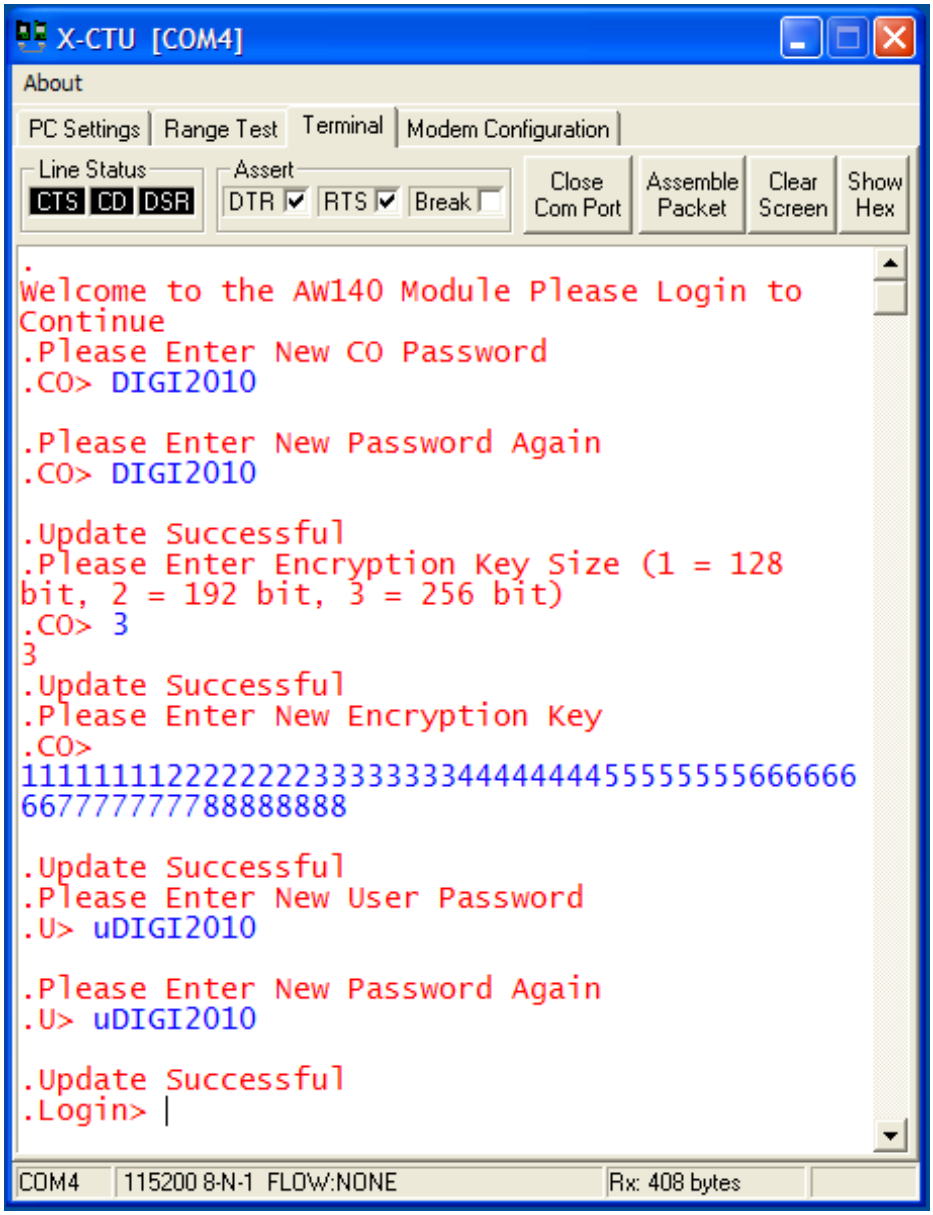
2. Open your terminal emulator program and set the COM port settings as follows:

Data bits:	8
Baud rate:	115200
Parity:	none
Stop bits:	1
Flow control:	none

3. Press any key to activate the XPress™ Crypto Module. If the module has never been programmed, setup prompts will occur as shown in the example screen shot below. If you see only a login prompt, then the module has previously been initialized. If you know the password, enter

it. If not, type “init” to erase all keys and passwords and return the module to its uninitialized state.

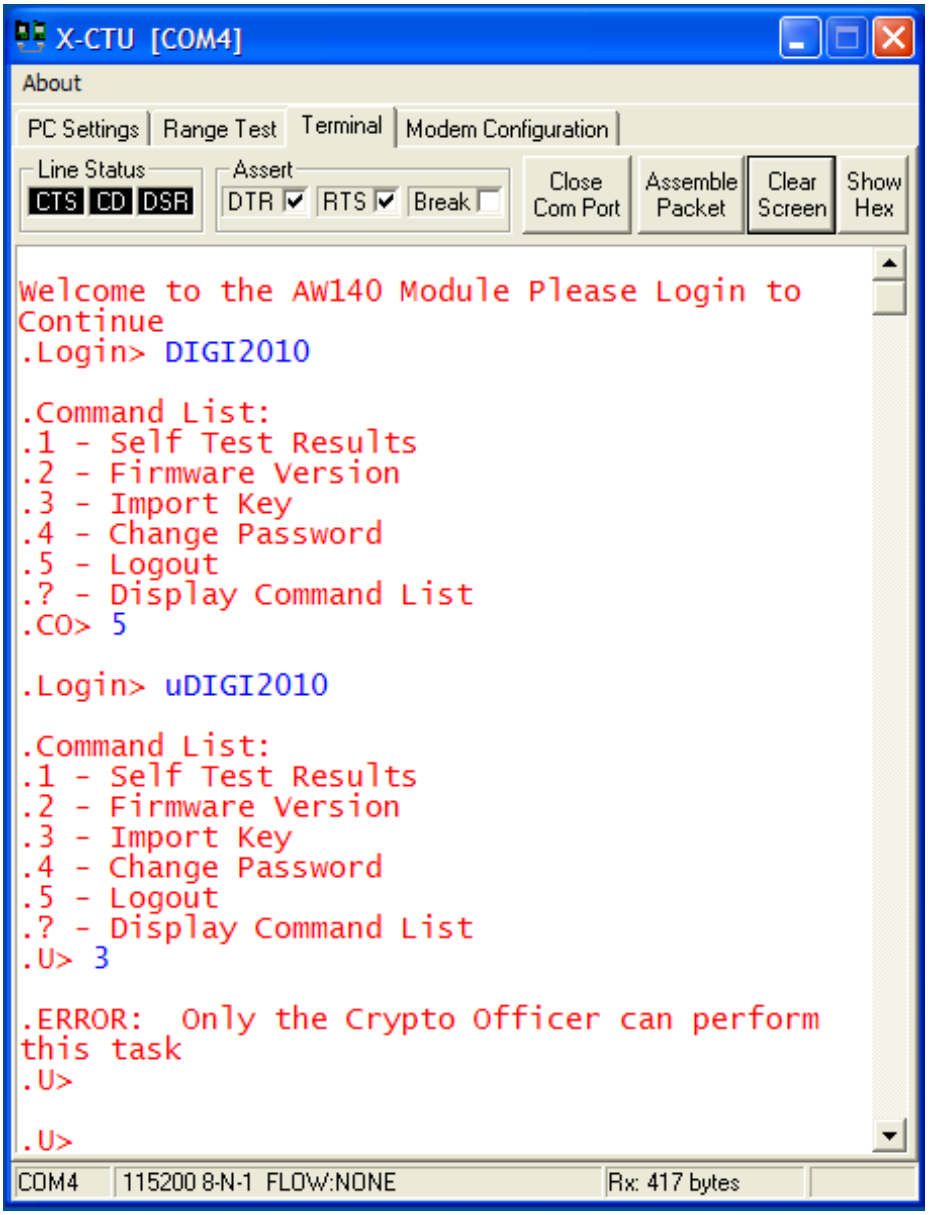
4. Initial Setup.



Passwords must be between 8 and 32 characters. Passwords are case-sensitive and any ASCII characters may be used.

You may select a 128, 192, or 256 bit encryption key. The encryption key must be entered as a 32, 48, or 64 digit hexadecimal number (0-9, a-f), corresponding to the length of the encryption key selected. If you enter less than the full number of digits, the XPress™ Crypto Module will pad your key with zeros.

5. After completing the initial setup, disconnect the USB cable. If you are using the XPress™ Crypto Module as part of an XPress™ Ethernet Bridge, replace the ESD cap on the USB connector to ensure the USB connector will not cause damage inside the unit, recoil the USB cable inside the XPress™ Ethernet Bridge using the reusable cable tie, and replace the enclosure cover. Next, power up the Digi radio to resume normal cryptographic operation.
6. It may become necessary to change the programming or test the module at some later time. Connect your hardware as shown in step 1 then set up the COM port parameters and terminal emulator program as described in step 2. A screen similar to the one below will display:



Self Test Results displays the results of the power up self test. At power up, the XPress™ Crypto Module runs a known answer test for all encryption/decryption algorithms.

Firmware Version displays the revision number of the firmware running in the XPress™ Crypto Module.

Change Algorithm and **Change Key** can only be used by the Crypto Officer Role. If the User Role attempts to run these commands, an error occurs as shown in the above screen shot.

Change Password allows a new choice for the Crypto Officer or User password, depending on which Role is logged in.

Display Command List will display the list of available commands.

Logout will log you out of the XPress™ Crypto Module.

Note: If an incorrect password is entered at the login prompt, two more tries are allowed and then the XPress™ Crypto Module enters a lockout state for 5 minutes.

7. After completing the setup or testing, log out and disconnect the USB cable. If you are using the XPress™ Crypto Module as part of an XPress™ Ethernet Bridge, replace the ESD cap on the USB connector to ensure the USB connector will not cause damage inside the unit, recoil the USB cable inside the XPress™ Ethernet Bridge using the reusable cable tie, and replace the enclosure cover. Next, power up the Digi radio to resume normal cryptographic operation.


Digi®