XPress™ Crypto Module Security Policy

Level 2 Validation

90033944_B
March 14, 2011

Introduction

Purpose

This is a non-proprietary FIPS Security Policy for the Digi XPress™ Crypto Module, also known as the AW140 module. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 2 requirements. This Policy forms a part of the submission package to the testing lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard visit www.nist.gov/cmvp.

References

This Security Policy describes how this module complies with the eleven sections of the Standard:

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at www.nist.gov/cmvp.

Digi Contact Information

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

Product Description

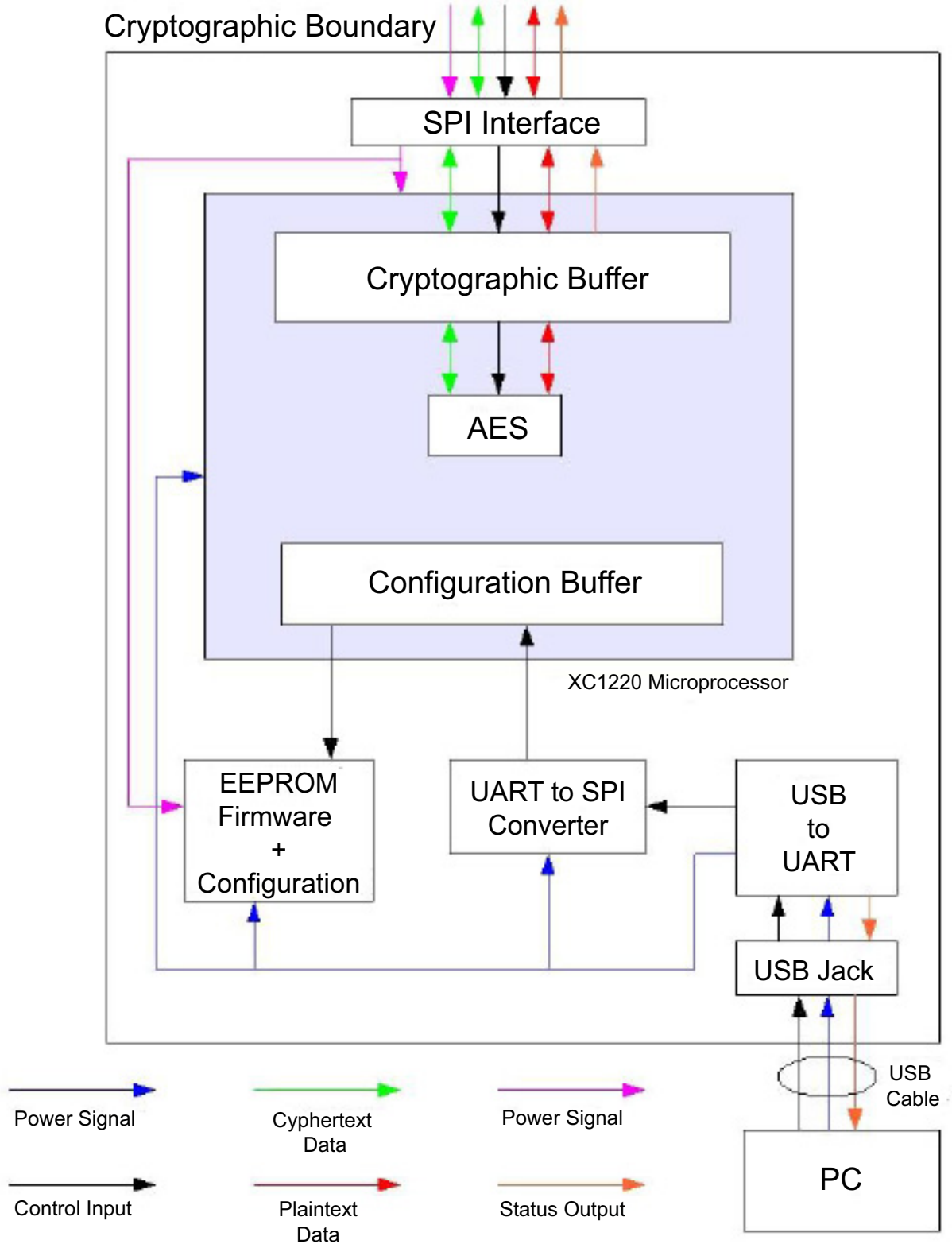
The Digi XPress™ Crypto Module is a cryptographic add-on module. The XPress™ Crypto Module is defined as a multi-chip embedded module as defined by FIPS PUB 140-2. It supports AES encryption/decryption. The cryptographic boundary is defined as the epoxy covered circuit board and all of its components. There are no exclusions from the module. The block diagram for the module is as shown below with all the inter-connections between the components of the module.

The module implements AES-128, AES-192, and AES-256 algorithms in the approved mode. The intended use of the module is an encryption/ decryption add-on module to a communicatiosn device.

The product meets the overall requirements applicable to Level 2 security for FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2
Overall Level of Certification	2

Hardware Block Diagram



Module Ports and Interfaces

The module is considered to be a multi-chip embedded module designed to meet FIPS 140-2 Level 2 requirements. The module has the following interfaces:

Data Input Interface: The SPI interface is defined as the data input interface through which data is input to the module. Each data category has its own command in order to keep data types logically separated.

Data Output Interface: As the module is being validated for Level 2 requirements, the SPI interface is defined as the data output interface.

Control Input Interface: Control input is on the USB and SPI interfaces and consists of command instructions that must be input for configuration and control of the module. See the User's Manual for Command Structure.

Status Output: Status output is on the USB and SPI interfaces. See the User's Manual for Status Output definitions.

The below table describes the relationship between the logical and physical interfaces.

FIPS 140-2 Interface	Physical Interface
Data Input Interface	10 pin 0.100 inch Header (SPI interface)
Data Output Interface	10 pin 0.100 inch Header (SPI interface)
Control Input Interface	10 pin 0.100 inch Header (SPI interface) / USB interface
Power Interface	In configuration mode powered by USB, else powered through SPI Interface
Status Output Interface	10 pin 0.100 inch Header (SPI interface) / USB interface

Roles, Services and Authentication

The XPress™ Crypto Module supports a Crypto-Officer, User role, and an Unauthenticated role. The module implements role based authentication using passwords. Authentication to the module requires a password to be set for the CO and User. The module does not support a maintenance role.

Identification and Authentication

Authentication data is protected within the EEPROM to which there is no logical access. AII ASCII characters are valid for authentication passwords.

Role	Type of Authentication	Authentication Data	Strength of Authentication
User	Role Based	8 to 32 character ASCII password	There are 94 different ASCII characters to select from for the authentication password. The minimum password size is 8 characters. Therefore, there is a minimum of 94 to the power of 8 different possible passwords. The probability that a random access attempt will succeed is p=1/94 to the 8 = 1.64 x 10 to the 16.
Crypto Officer	Role Based	8 to 32 character ASCII password	There are 94 different ASCII characters to select from for the authentication password. The minimum password size is 8 characters. Therefore, there is a minimum of 94 to the power of 8 different possible passwords. The probability that a random access attempt will succeed is p=1/94 to the 8 = 1.64 x 10 to the 16.

Roles and Services

The XPress™ Crypto Module supports the services listed in the following table. The table groups the authorized services by operator roles. The modes of access are also identified per the explanation.

R - The item is **read** or referenced by the service.

W - The item is **written** or updated by the service.

E - The item is **executed** by the service (the term is used as part of a cryptographic function).

The table below shows the services available to each role:

Cryptographic Officer - Roles and Services:

Role	Authorized Services	Keys/CSP's Associated with the Service	Access Type
CO	Import Key	Application Key	W
CO	Show Status	None	R
CO	Read Firmware Version Number	None	R
CO	Change Password	Crypto-Officer Password	W
CO	Self-Tests	None	E
CO	AES Encrypt/ Decrypt	Application Key	E

User - Roles and Services:

Role	Authorized Services	Keys/CSP's Associated with the Service	Access Type
User	Show Status	None	R
User	Read Firmware Version Number	None	R
User	Change Password	User Password	W
User	Self-Tests	None	E

Unauthenticated - Roles and Services:

Role	Authorized Services	Keys/CSP's Associated with the Service	Access Type
UA	Zeroize	Application Key and CO and User Password	W

Physical Security

The XPress™ Crypto Module is defined as a multi-chip embedded module. The XPress™ Crypto Module consists of production grade components which include standard passivation techniques. The entire module will be encapsulated in a potting material. The purpose of the potting material is to make the module opaque and provide physical evidence of tampering if an attacker attempts to remove the potting. To physically access the components of the module the potting material must be destroyed.

Cryptographic Key Management

The following table summarizes the module's keys and CSP's:

Key / CSP's	Generation	Storage	Use	Role
Application Keys AES 128, 192, 256	Electronically entered by CO	Stored in EEPROM	AES Application Keys used for data encryption and decryption	CO
Crypto-Officer Password	Created by the Crypto-Officer	Stored in EEPROM	Used to authenticate the Crypto-Officer	CO
User Password	Created by the User	Stored in EEPROM	Used to authenticate the User	User

The keys are entered into the XPress™ Crypto Module module by the CO using the configuration interface (USB connection to a PC) and a terminal program such as HyperTerminal. The keys are stored in plaintext on the module's EEPROM to which there is no physical or logical access. The XPress™ Crypto Module module does not output or archive any keys.

The keys and passwords can be zeroized by anyone using the un-authenticated zeroize/init command, that restes teh module to a factory default state.

The module keys map to the following algorithm certificates:

Approved Security Function	Certificate
Symmetric Key Encryption/Decryption	
AES ECB (e/d; 128, 192, 256)	1291

Self-Test

The module performs the following self tests at power on, which are performed automatically and do not require operator intervention:

- AES Known Answer Tests (KATs), ECB mode for Encrypt/Decrypt
- Firmware Integrity Test. The integrity of the entire firmware image is checked using a 16 bit checksum.

The indication of whether the power-up self-tests were successful, is available using the Show Status option. The module inhibits all data output while self-tests are in process.

The XPress™ Crypto Module module does not support the following functions, and thus does not employ any conditional tests:

- Bypass Mode
- Loading of Firmware
- Random Number Generation
- Asymmetric Cryptography
- Manual Key Entry

On-Demand Self-Tests

The module must be power-cycled in order to run the on-demand self-tests, which include the AES known answer tets an the firmware integrity test.

Error State

If any power-up self-test fails, then the XPress™ Crypto Module module enters an error state in which cryptographic operations and data input/output is disabled. Errors which are considered hard errors, such as failed integrity tests or failed AES known answer tests, mean the XPress™ Crypto Module module requires service. The module will attempt to clear all other errors on its own.

Crypto-Officer and User Guidance

This section describes the configuration, maintenance, and administration of the XPress™ Crypto Module module.

Secure Setup and Initialization

Connect the XPress™ Crypto Module module to your PC using a USB A to USB mini B cable. If you have purchased a XPress™ Crypto Module as part of an XPress™ Ethernet Bridge, you will need to 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. When you are done with setup and initialization, replace the ESD cap on the USB connector to ensure the USB connector will not cause damage inside the unit, and recoil the USB cable inside the XPress™ Ethernet Bridge using the reusable cable tie.

Open a terminal program and set the COM port settings as follows:

Data Bits:	8
Baud Rate:	115200
Polarity:	None
Stop Bits:	1
Flow Control:	None

Once the terminal program is connected press any key to activate the module.

The module will prompt for a password of 8 to 32 characters. The module will determine, based on the password entered, if it is the Crypto-Officer or User that has logged in.

Once logged in a list of available commands will appear on the terminal screen.

For first time configuration, once a password has been chosen for each role, one of the following AES key sizes (AES-128, AES-192, or AES-256) must be chosen or the module will not be able to enter into a cryptographic mode of operation.

The Crypto-Officer must now import the desired key into the module.

In a non-configured state, the SPI interface is disabled and no

cryptographic operations can be processed.

Module Security Policy Rules

After the power-on self-tests are performed, the module detects if there is a USB connection present or not. If the USB connection is present then the XPress™ Crypto Module will enter configuration mode and wait for terminal activation. While the self-tests are running, data input/output is logically inhibited. Status output can be used to determine is self-tests are in process.

While in configuration mode the data interface is disabled and no cryptographic functions can be performed.

If an error occurs while the module is in configuration mode then the error will be displayed on the terminal.

If a USB connection is not detected after self-tests are completed, the module will enter normal operation. The configuration interface will be disabled and only the data interface will operate. Whatever key and algorithm choice was stored in the last configuration setup will be used to encrypt/decrypt all data on the data interface. If the module was not previously configured then it will be in a non-operational state with the error line of the SPI interface asserted.

If an error occurs while in normal operation an error line will be held high on the SPI interface and the status register can be read to determine the exact cause of the error.

Mitigation of Other Attacks

The module does not mitigate against any specific attacks.