XPress™ Crypto Module Enables Fast Track FIPS 140-2 Certification

White Paper

Abstract

The purpose of this paper is to explain how the XPress Crypto Module can provide a short cut for users who require FIPS 140-2 Level 2 certification to allow their products to be used in a wide range of security sensitive applications in government, financial and other markets.

FIPS 140-2: What is it and why do you care?

The National Institute of Standards and Technology (NIST) Computer Security Division issued a series of publications to coordinate requirements and standards for cryptography modules, both hardware and software. Federal Information Processing Standard (FIPS) publication 140-2 spells out the requirements and provides for the accreditation of such modules by testing and certifying that these requirements have been met.

There are now legislative restrictions placed on federal agencies that require them to use tested and validated cryptography products. Governmental agencies as well as private industries dealing with sensitive applications such as financial and health care are relying to an increasing extent on FIPS 140-2 certified products to meet legal requirements and to ensure that sensitive data will be protected. These legislative restrictions mandate that anybody wanting to sell products incorporating data encryption into these markets will have to have official certification. Essentially, if a governmental agency needs to encrypt data, they must do it with a certified product.

The FIPS 140-2 standard can easily be obtained from the NIST website (http://csrc.nist.gov). This document indicates the requirements related to the security and design of a cryptographic module, such as specifications, ports and interfaces, roles, services and authentication, finite state model, physical security, operational environment, cryptographic key management and EMI/EMC compatibility.

The FIPS 140-2 standard defines four levels of security in order to cover a wide range of applications:

- **Security Level 1** is the lowest level and simply requires that an approved encryption algorithm or approved security function be implemented.
- **Security Level 2** adds a requirement for tamper-evidence through the use of special coatings or seals that prevent undetected access to the cryptographic keys and critical security parameters within the module. It also specifies role-based authentication, defining certain operator roles and controlling the authorization of services appropriate to each role. The XPress Crypto meets this level.
- **Security Level 3** requires tamper-resistant physical security and identity-based authentication.
- **Security Level 4** further requires a complete physical envelope of protection around the module with the intent of detecting and responding to all unauthorized attempts at physical access.

The long and difficult path to FIPS 140-2 certification

The Cryptographic Module Validation Program (CMVP) was established in 1995 and is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). Modules validated by CMVP to be in conformance with FIPS 140-2 are accepted by the federal agencies of both the USA and Canada for the protection of sensitive information.

CMVP has accredited a list of approved testing laboratories to which modules and their documentation must be submitted. At this writing there were eleven labs in the USA, two in Canada and six others around the world. The current list is available on the NIST website.

The process of obtaining a FIPS 140-2 certificate is:

- Design a module and produce initial articles for testing
- Document the module per the requirements of the standard
- Submit the module and documentation to the testing laboratory of your choice
- Wait for approval by the testing lab, making changes to the design or documentation as needed
- Submit the testing documents to NIST and CSEC for review
- Wait for review and comments, resolving any issues required by the reviewing agencies
- Wait for final approval and issuance of the certificate

If the design requires no changes, the process will typically take six months or more and cost around $100,000. If issues are discovered, the time could stretch out for years.

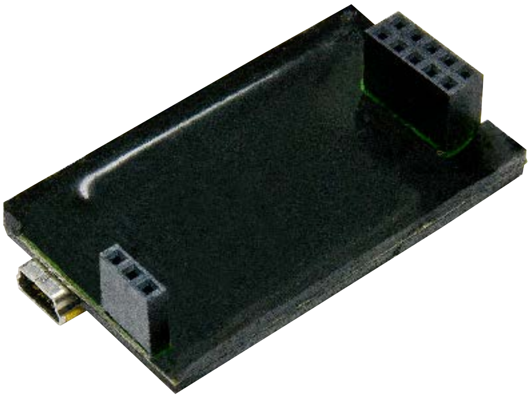
How can the XPress Crypto module shorten your time to market?

A cryptographic module that has already been issued a FIPS140-2 validation certificate may be incorporated or embedded into another product. The new product may then be marketed as FIPS sufficient, use the FIPS logo and reference the certification of that module, provided that the originally validated module has not been altered and is used to perform its cryptographic functionality. The XPress Crypto certificate number is #1452.

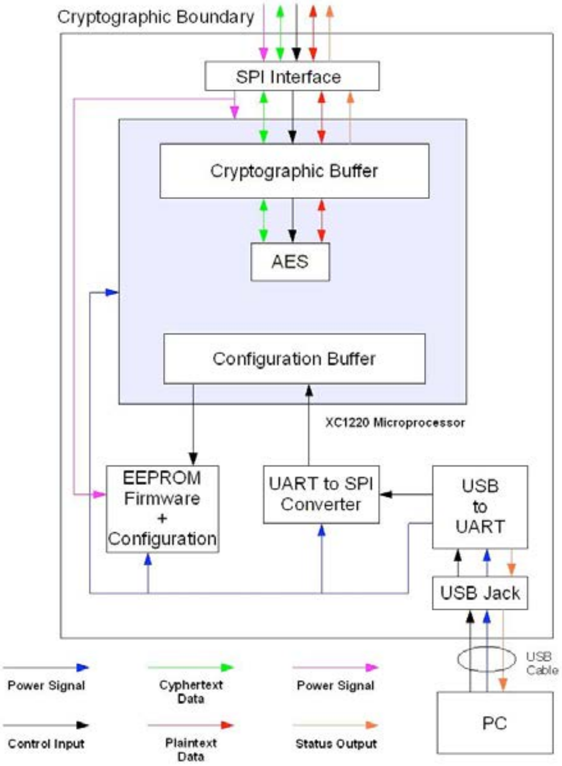
By using the XPress Crypto to implement encryption in your product, you can proceed directly from design to market and avoid the lengthy testing and certification process. In these days of rapid technological evolution, saving six months to a year in the development cycle can often mean the difference between success and failure.

How does the XPress Crypto work?

The XPress Crypto module is a PC board with two interface ports and is potted with black, government-approved tamper-evident coating. It is quite small, measuring just 30 millimeters by 50 millimeters ($1^{3/16}$ inches by 2 inches) and consumes just 150 mW of 3.3 VDC power. The module has a Serial Peripheral Interface (SPI) port for data that is a 2x5 pin header. A second and totally separate mini USB port is used for control and critical security parameter entry.



(The 3-pin header shown in the photo to the right is just for physical support).

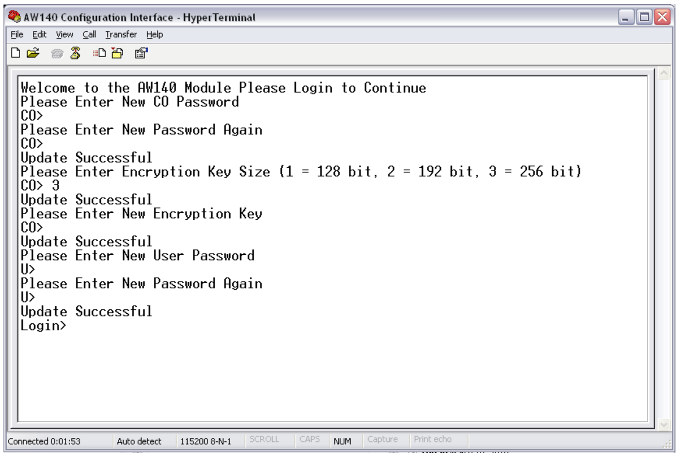


Providing two isolated ports, one for data and one for control, allows for increased security protection because the encryption method and keys cannot be seen or changed from the SPI data interface and the encrypted and plaintext data cannot be seen from the USB command interface. In fact, the two ports cannot be simultaneously powered up.

The SPI data interface easily interfaces with a SPI port on your own microcontroller circuitry, which will pass plaintext to the module and retrieve encrypted data or vice versa.

To program the encryption characteristics of the XPress Crypto module, a PC must be connected to the USB port and the SPI interface must be powered off. The module may then be programmed using a virtual COM port driver and a terminal emulator in the PC. This operation is frequently done before the module is installed and deployed in the user's system, but can also be done in the field.

The command interface for the XPress Crypto defines two user roles, the User and the Crypto Officer. Each has a different password. Only the Crypto Officer may set the encryption method and encryption key. The User role may examine self test results and see the module's firmware version.


AW140 Configuration Interface - HyperTerminal
File Edit View Call Transfer Help
Connected 0:01:53
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
Welcome to the AW140 Module Please Login to Continue
Please Enter New CO Password
CO>
Please Enter New Password Again
CO>
Update Successful
Please Enter Encryption Key Size (1 = 128 bit, 2 = 192 bit, 3 = 256 bit)
CO> 3
Update Successful
Please Enter New Encryption Key
CO>
Update Successful
Please Enter New User Password
U>
Please Enter New Password Again
U>
Update Successful
Login>
```

First steps: a possible development environment

The microcontroller that the XPress Crypto will interface with generally determines what development environment will be most useful. An alternative that we have used in our work is the Digi JumpStart Kit® for the ConnectCore™ 9P 9215 module. The ConnectCore 9P 9215 features a 32-bit processor, Ethernet networking and a range of peripheral interfaces. It supports NET+OS 7, Linux or .NET Micro Framework. We wired the SPI data interface and wrote some simple C++ subroutines to send and receive encrypted and plaintext data. If you would like to see these subroutines and a further description of this application example, please contact Digi Government Sales at govsales@digi.com or by calling 1-877-912-3444 ext.3347.

DIGI SERVICE AND SUPPORT / You can purchase with confidence knowing that Digi is always available to serve you with expert technical support and our industry leading warranty. For detailed information visit www.digi.com/support.

DIGI INTERNATIONAL WORLDWIDE HQ
877-912-3444 / 952-912-3444 / www.digi.com

DIGI INTERNATIONAL FRANCE
+33-1-55-61-98-98 / www.digi.fr

DIGI INTERNATIONAL JAPAN
+81-3-5428-0261 / www.digi-intl.co.jp

DIGI INTERNATIONAL SINGAPORE
+65-6213-5380

DIGI INTERNATIONAL CHINA
+86-21-50492199 / www.digi.com.cn