Protect Your Data; Safeguard Your Privacy

X-Wall MX-256C
Security Policy

Version: 1.0

Revision Date: 12/10/2010

Enova Technology Corporation

Contents

Tables

Figures

1 Module Overview

The X-Wall MX-256C is a patent protected ASIC (Application Specific Integrated Circuit) that performs hardware real-time full disk encryption on a connected SATA disk drive (SSD, Solid State Disk) through AES CBC mode of operation up to 256-bits of strength. Encryption/Decryption processes are automatic and transparent and involve absolutely no user intervention. Entire disk drives including MBR (Master Boot Record), FAT (File Allocation Table), Temporary Folders, and Operating System are real-time encrypted. There is no secret left unprotected on the entire disk drive.

The X-Wall MX-256C (hereafter referred to as the module) is a single-chip module.

The boundary of the module is the outer perimeter of the chip.

No components are excluded from the cryptographic boundary.

Figure 1 – Front of X-Wall MX-256C

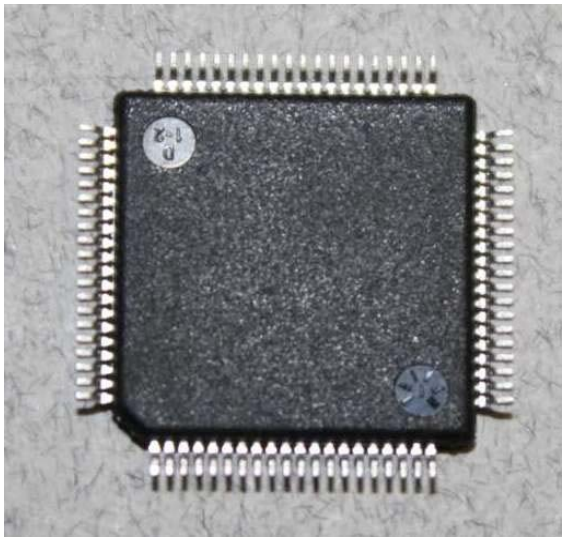

Figure 2 – Rear of X-Wall MX-256C

The configuration of hardware and firmware for this validation is:

Hardware P/N: X-Wall MX-256C; Firmware Version: 1.1.0 hard coded ROM.

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

2 Modes of Operation

2.1 FIPS Approved Mode of Operation

The module only provides a FIPS Approved mode of operation, comprising all services described in Section 5 below.

2.2 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithm.

Table 2 - FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
X-Wall MX-256C: AES - CBC mode 128, 192, and 256	250

3 Ports and Interfaces

The X-Wall MX-256C is a single-chip module with ports and interfaces as shown below.

Table 3 – X-Wall MX-256C Pins and FIPS 140-2 Physical Interface

Pin	FIPS 140-2 Designation	Name and Description
RxPA (66)	Data Input	Received differential input signals for channel A (channel #0)
RxNA (65)	Data Input	Received differential input signals for channel A (channel #0)
TxPA (62)	Data Output	Differential serial output transmitted signals for channel A (channel #0)
TxNA (61)	Data Output	Differential serial output transmitted signals for channel A (channel #0)
RxPB (68)	Data Input	Received differential input signals for channel B (channel #1)
RxNB (67)	Data Input	Received differential input signals for channel B (channel #1)
TxPB (72)	Data Output	Differential serial output transmitted signals for channel B (channel #1)
TxNB (71)	Data Output	Differential serial output transmitted signals for channel B (channel #1)
ResRef (74)	Data Input/Output	Reference register, terminated to pin VSSREFREF

Table 4 – X-Wall MX-256C Pins and FIPS 140-2 Clock and PLL Control pins

Pin	FIPS 140-2 Designation	Name and Description
XTALI (38)	Control Input	Crystal/reference clock input
XTALO (39)	Status Output	Crystal Output
RefClkSel_0 (45)	Control Input	Reference clock frequency selection
RefClkSel_1 (46)	Control Input	Reference clock frequency selection
PLLEna (42)	Control Input	PLL enabled for normal operation

Table 5 – X-Wall MX-256C Pins and FIPS 140-2 Feature Setting Pins

Pin	FIPS 140-2 Designation	Name and Description
ByPassN (9)	Control Input	Hardware traps for cryptographic engine enabling
PmMode (44)	Control Input	Built-in API command through Port Multiplier (PM) mode selection

Table 6 – X-Wall MX-256C Pins and FIPS 140-2 Control and Indicator Signals

Pin	FIPS 140-2 Designation	Name and Description
SysReset (18)	Control Input	Hardware master reset
Sync2PHY (17)	Control Input	Use PHY sync mode for data transfer
TlrDspErr (12)	Control Input	Tolerate disparity errors of ALIGH primitives during OOB
PSCROff (16)	Control Input	Turn off primitive scrambler for transmit
DSCROff (15)	Control Input	Turn off data scrambler for Tx/Rx
SSCOff (14)	Control Input	Turn off SSC mode for transmit
KeyErr (24)	Status Output	AES key indicator
BistErr (23)	Status Output	Indicates if build-in-self-test (BIST) in PHY has failed
EngErr (22)	Status Output	Indicates that the power-on-self-test for the X-Wall MX Cryptographic Engine has failed
DatXfer (43)	Status Output	Indicates that X-Wall MX has detected data transfer activities on its channels
CfgHost (21)	Control Input	Selecting host/device for channel #0 and channel #1

Table 7 – X-Wall MX-256C Pins and FIPS 140-2 Two-Wire Seiral Interface

Pin	FIPS 140-2 Designation	Name and Description
SDAH (48)	Data Input/Output	2-wire serial data
SCLH (47)	Data Input/Output	2-wire serial clock

Table 8 – X-Wall MX-256C Pins and FIPS 140-2 JTAG Test pins

Pin	FIPS 140-2	Name and Description

	Designation	
TCK (5)	Control Input	Test clock
TDI (3)	Data Input	Test data input
TDO (4)	Data Output	Test data output
TMS (6)	Control Input	Test mode select
TRST (7)	Control Input	Test reset

Table 9 – X-Wall MX-256C Pins and FIPS 140-2 Debug Interface

Pin	FIPS 140-2 Designation	Name and Description
IDDQEn (1)	Control Input	iDDQ test mode
Bist (2)	Control Input	Turn on build-in-self-test mode on PHY
LbEn (25)	Control Input	PHY loop back mode enabled for testing
TestIO (50)	Control Input	Select test modes for scan tests and functional tests
TestC (77)	Control Input	Select test modes for scan tests and functional tests
TestE (78)	Control Input	Select test modes for scan tests and functional tests

Table 10 – X-Wall MX-256C Pins and FIPS 140-2 Power Ground

Pin	FIPS 140-2 Designation	Name and Description
VDD18ANA (57 and 76)	Power Input	Analog 1.8V power supply
VSSANA (58 and 75)	Power Input	Analog ground of VDD18ANA
VDDSATA (60, 56 and 53)	Power Input	Digital 1.8V power supply
VSSSATA (59, 55 and 54)	Power Input	Digital ground for VDDSATA
VSSRESREF (73)	Power Input	Analog ground returned for external resistor reference
VDDP (63 and 69)	Power Input	1.8V analog power supply
VSSP (64 and 70)	Power Input	Analog ground
VDD33XW (19, 41 and 79)	Power Input	Digital 3.3V supply for chip I/O
VDD18XW (11,	Power Input	Digital 1.8V supply for chip core

28, 36 and 49)		
VSS33XW (20, 40 and 80)	Power Input	Digital ground for chip I/O
VSS18XW (8, 10, 26, 27, 33, 35 and 52)	Power Input	Digital ground for chip core
VDD18PLL (29)	Power Input	1.8V digital power supply
VSS33PLL (32)	Power Input	Analog ground
VAA33PLL (31)	Power Input	Analog 3.3V supply
VSS18PLL (30)	Power Input	Digital ground

4 Identification and Authentication Policy

4.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). Both the CO and User support the same services.

Table 11 - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to all services offered by the module.	N/A	N/A
User	This role has access to all services offered by the module.	N/A	N/A

5 Access Control Policy

5.1 Roles and Services

Table 12 –Services

Service	Description
Encrypt	Encrypts Data to be stored externally
Decrypt	Decrypts Data from external storage
Module Configuration	Non-security related configurations
Key Loading	Loads the AES key into the module
Zeroization	Zeroizes the AES key in the module
Show Status	Status is indicated by PINs being set to high or low values depending on the status of the module.
Self-Test	AES KAT run on power up of the module

Table 13 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Encrypt		X	X	
Decrypt		X	X	
Module Configuration	X			
Key Loading	X	X		
Zeroization	X			
Show Status				X
Self-Test				X

5.2 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 14 - CSPs

Key Name	Type	Description
AES Key	AES (128, 192, or 256 bit)	Used to encrypt/decrypt data

5.3 Definition of Public Keys

The module does not contain any public keys.

5.4 Definition of CSPs Modes of Access

Table 13 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **R** = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- **W** = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 15 - CSP Access Rights within Roles & Services

Role	Service	Mode	Cryptographic Key or CSP
User, CO	Key Loading	W	AES Key
User, CO	Zeroize	Z	AES Key
User, CO	Encrypt	R	AES Key
User, CO	Decrypt	R	AES Key

Other services do not have access to CSPs.

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the X-Wall MX-256C does not contain a modifiable operational environment. The firmware cannot be updated on the module.

7 Security Rules

The X-Wall MX-256C design corresponds to the following security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module provides two distinct operator roles. These are the User role and the Cryptographic Officer role.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. The cryptographic module performs the following tests:
   A. Power up Self-Test
      1. AES KAT
4. Self-test failure is indicated by high voltage on Pin EngErr (22).
5. The operator is capable of commanding the module to perform the power up self-test by cycling power or resetting the module.
6. The power up self test does not require any operator action.
7. Data output is inhibited during self-test, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any external input/output devices used for entry/output of data.
13. The module does not output plaintext CSPs.
14. The module shall not be used in bypass mode.
15. The JTAG ports are not to be accessed.

8 Physical Security Policy

8.1 Physical Security Mechanisms

The single-chip module is production quality containing standard passivation. The chip components are protected by the chip packaging. Attempts to remove the hard, opaque, tamper evident coating of the packaging have a high probability of causing serious damage to the module. Besides, the CSPs will zeroize under the following three conditions:

a. Firmware Reset;

b. Hardware Reset; and

c. Power on Reset

The module is designed and has been tested to function correctly between -45 and 90 degrees Celsius.

The module must be inspected every 90 days. The inspection must look for tamper evidence or any signs of attempts to compromise the module. These signs may include, but are not limited to, scratches on the sides or top, holes and/or missing packaging material.

9 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2 requirements.

10 References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

11 Definitions and Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standards
FSM	Finite State Model
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
ROM	Read Only Memory