Enova Technology Corporation

X-Wall MX+

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version 1.3

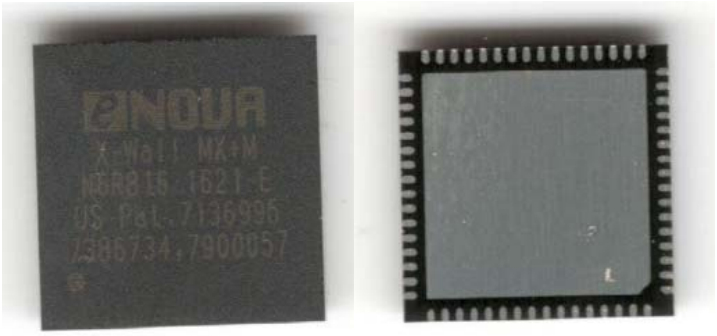

Table of Contents

List of Tables

List of Figures

Revision History

Authors	Date	Version	Comment
Chung-Yen Chiu	08/01/2016	0.1	First Draft
JC	10/03/2016	0.2	Second Draft
Chung-Yen Chiu	10/19/2016	0.3	Third Draft
JC	11/25/2016	0.4	Fourth Draft
Chung-Yen Chiu	12/02/2016	0.5	Fifth Draft
JC	12/07/2016	0.6	Sixth Draft
Chung-Yen Chiu	12/26/2016	0.7	Seventh Draft
Chung-Yen Chiu	3/15/2017	0.8	Eighth Draft
Chung-Yen Chiu	8/9/2017	0.9	Ninth Draft
Chung-Yen Chiu	8/14/2017	0.91	Tenth Draft
Chung-Yen Chiu	8/16/2017	0.92	Eleventh Draft
Chung-Yen Chiu	9/4/2017	0.93	Twelfth Draft
Robert Wann	04/07/2020	1.3	Revised firmware release; syntax correction & format

Introduction

This document defines the Security Policy for the Enova Technology Corporation X-Wall MX+. The X-Wall MX+ (hereafter referred to as the cryptographic module or the module) is a real-time Serial ATA (SATA) bridge ASIC (Application Specific Integrated Circuit). The module sits between a SATA host and a SATA device. An example of SATA host could be the main board of a personal computer (PC). An example of a SATA device could be a Solid-State Disk (SSD). The purpose of the cryptographic module is to allow authorized entities to perform cryptographic operations on messages or data sent to, received from, or kept within the module. The Module supports standard SATA interface and is compliant with the Trusted Computing Group (TCG) SSC specification Opal 2.0.

The module is intended to meet FIPS 140-2, overall level 3. Table 1 indicates the module name and version specifics. Table 2 specifies the various sections of the FIPS 140-2 standard the cryptographic module have met.

Module Name	***Hardware Version***	***Firmware Version***
X-Wall MX+	xF	mr.20.06.02.2203.CIF

Table 1 Cryptographic Module Configuration

Security Requirements	***Security Level***
1. Cryptographic Module Specification	3
2. Cryptographic Module Ports and Interfaces	3
3. Roles, Services, and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI/EMC	3
9. Self-Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
Overall Level	3

Table 2 Security level of the cryptographic module

Section 1 - Module Specification

The module is a single-chip cryptographic module which stacks up a Non-Volatile Memory (NVM) flash memory die on top of a controller die within a single ASIC package. The cryptographic boundary of the module is the outer perimeter of the chip itself. The module has an embedded micro-controller unit (MCU). Executable firmware codes are stored in the module's ROM. Additional firmware codes are stored in NVM and are dynamically copied to internal SRAM of the module. The codes stored in NVM are AES encrypted and is CMAC authenticated with a private key owned by the module. No hardware or firmware components are excluded from the requirement of FIPS140-2. The block diagram below specifies the physical boundary and logical data flow.

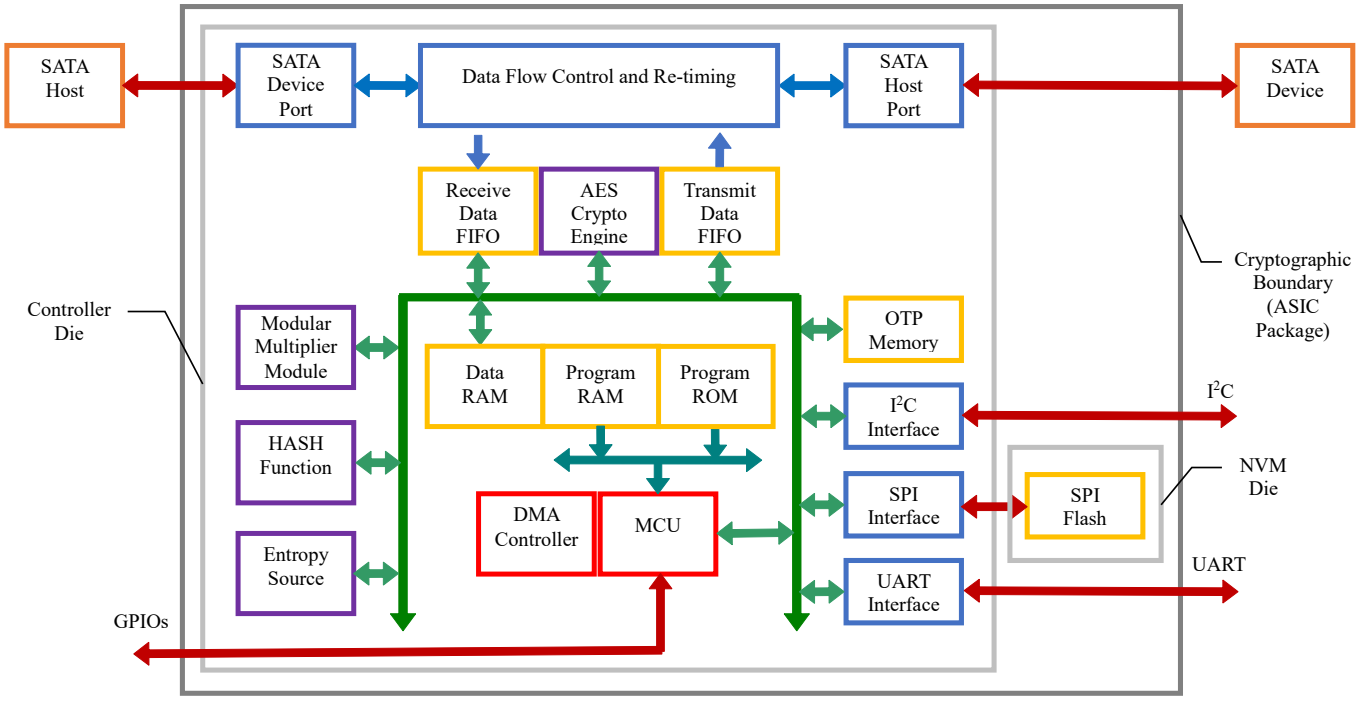

Figure 1 The X-Wall MX+ cryptographic boundary block diagram

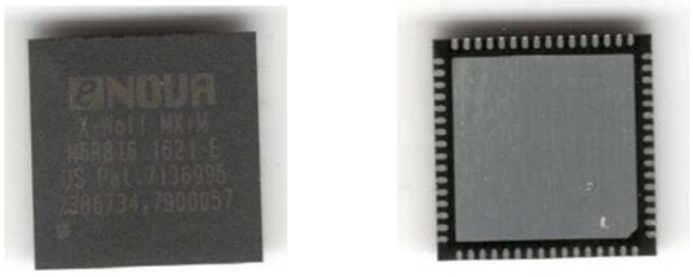

Figure 2 Top & bottom view of the X-Wall MX+ cryptographic boundary

Installation and Configuration

Guidance for the Crypto Officer

Before installation of the module, the Crypto-Officer must visually inspect the module for signs of physical damage. If any evidence of physical damage is found, the module must be replaced. The Crypto-Officer must also ensure that the module is correctly connected to the environment. The module is built with a default Manufacturer role (explained below under "Roles & Services".) The rules for installation and configuration are as follows:

1. Login with the manufacturer role on a secured channel.
2. Manufacturer should check if the module has all correct configuration items.
3. Manufacturer can (optionally) execute test services to ensure the module integrity.
4. Create a Crypto-Officer account using the provided services..
5. Logout from the module and reactivate; using the newly created Crypto-Officer account. (The module can be reverted to the uninitialized state and the process repeated if problems are encountered).
6. The Crypto-Officer cannot acquire media data read/write services. It must create a User role account to do so. This can be performed by logging into the module using an account with Crypto-Officer authority on a secured channel and creating a User account using the provided services. (A Crypto-Officer can modify or delete a User identity if necessary.)
7. Ensure that a storage media is properly connected to the module.
8. Create a media data key using the provided services.
9. Logout from the module. (The initialization process is now complete.)

A Crypto Officer can create/modify/delete a User identity and the associated CSPs; revert the cryptographic module to its uninitialized state; or scrap the cryptographic module by destroying the OTP along with all CSPs.

Guidance for the User

1. Login to the cryptographic module.
2. Check that the module has all correct configurations. (Report any abnormal conditions to the Crypto-Officer.) If login is successful, the module shall unlock the media data key and the User can now securely access the data on the media.
3. Use session key to encrypt command payloads at all times in order to reduce the chances that the security of the module could be compromised.
4. If a User believes that the module may be compromised, he or she shall cease using the module and report the issue to the Crypto-Officer.
5. Logout when finished using the module.

Modes of Operation

The cryptographic module supports the following FIPS approved and non-FIPS approved modes of operation - each of which may support all or a subset of the approved security functions and services. To confirm that the module is operating in the Approved mode of operation, the SHOW STATUS service can be invoked from the Legacy Serial ATA Security Mode. FIPS Approved mode and non-FIPS approved modes of operation are mutually exclusive. No dynamic mode switching and no CSP mixing can occur.
The FIPS approved mode of operation is described as follows:

Serial ATA Security Mode (Approved Mode)

This mode provides services through vendor specific ATA commands. In order to operate in this mode, entities with at least one User and one Crypto-Officer authority must be created. CSPs such as role authorities, HMAC/CMAC shared secret, RSA public key pairs and certificates are written into the NVM (Non-volatile random access memory). In this mode, the module allows an authenticated operator the privileges to perform security services including secure access to an attached storage media.

To invoke the FIPS approved mode, the module must be physically configured with GPIO_1 Pin #45 pulled up and running the appropriate firmware version, as per Table 1. If these conditions have been met, the module will automatically enter the approved mode, after the successful completion of the power-up self-tests.

Algorithm	Description	Certificate No.
SHS	SHA-256 hash in byte mode generates HMAC-SHA-256 message authentication codes; generates DRBG random bits; and as part of the digital signature process for RSA, and key pair generation.	SHS (Cert. #3311)
RSA	Used for key pair generation, digital signature generation & verification, and encryption/decryption (key encapsulation/de-capsulation) with key size of 2048 bits.	RSA (Cert. #2090)
RSADP	Basic RSA decryption primitive. It recovers plaintext from ciphertext using an RSA private key.	CVL (Certs. #836 and #885)
RSASP1	Basic RSA signature primitive. It produces a signature representative from a message representative under the control of a private key.	CVL (Cert. #884)
AES	AES encrypts and decrypts designated data output from, input into, or within the module. It supports ECB, CBC, and XTS modes of operation with 256-bit strength. More, it uses separated keys to encrypt/decrypt data and initial	AES (Cert. #4013)

	vectors (or data unit sequence numbers).	
HMAC	Used for generating HMAC-SHA-256 message authentication codes.	HMAC (Cert. #2627)
800-90A DRBG	A hash-based deterministic random bit generator using SHA-256.	DRBG (Cert. #1201)
800-38B CMAC	Used for generating CMAC-AES-256 message authentication code.	AES (Cert. #4025)
800-108 KDF	Key Derivation Functions using either HMAC or CMAC as pseudorandom functions.	KBKDF (Cert. #100)

Table 3 Approved cryptographic algorithms implemented in the module

Algorithm	Description
NDRNG	Hardware Entropy Source provides entropy bits to the Approved DRBG.
RSA Key Wrapping	Key establishment methodology that provides 112 bits of encryption strength.

Table 4 Allowed but non-approved cryptographic algorithms implemented

The non-FIPS approved mode of operation is described as follows:

Base-line ATA Security Mode (non-Approved Mode)

This mode provides services to securely access a storage media attached to the module. User's data written to the storage media is AES[1] encrypted by the module. User's data read from the storage media is AES decrypted by the module. The module does not store keys and CSPs inside. Data encryption/decryption keys of the storage media are electronically input through either the I^2C interface or SATA interface. In order to change to the non-Approved mode, the pin for selecting the modes of operation can be either physically connected, or directly connected through a resister or jumper to digital power or ground.

In order to switch from one mode to another, the operator shall perform the following steps:

- Power-off the module;
- Remove the resister, adjust the jumper, or do a wire jump modification (depending on how the pin is physically connected on the PCB); and
- Power-on the module and perform a hardware reset.

[1] No CAVP testing for this implementation of AES was done in the Non-Approved mode.

Section 2 - Ports and Interfaces

The cryptographic module is supplied in a 64-pin QFN package. All power inputs, data inputs, data outputs, control inputs, and status outputs are supported. *See* Table 5 Ports and associated interface types of the module.

PIN	TYPE	PIN	TYPE	PIN	TYPE	PIN	TYPE
1	C[2]	17	S	33	N	49	C/S
2	C	18	P	34	N	50	P
3	P	19	P	35	P	51	C/S
4	S	20	P	36	N	52	C/S
5	S	21	I/C	37	N	53	P
6	S	22	I/C	38	C	54	P
7	C	23	P	39	C	55	P
8	S	24	O/S	40	P	56	O/S
9	C	25	O/S	41	P	57	O/S
10	C	26	P	42	S	58	P
11	P	27	P	43	C	59	I/C
12	N	28	P	44	C/S	60	I/C
13	N	29	S	45	C/S	61	P
14	P	30	S	46	C/S	62	P
15	C	31	S	47	C/S	63	P
16	S	32	S	48	C/S	64	C
						65	P

Table 5 Ports and associated interface types of the module

[2] C: Control Interface; I: Data Input Interface; N: Not Connected; O: Data Output Interface; P: Power Port; S: Status Output Interface.

Section 3 - Roles Services and Authentication

Operators must log on to the module to acquire services. An identity is active after log-on and will remain active until logout. Some services may require the requests and responses sent, to be signed with a private key. The module authenticates the entities by verifying the MAC or Digital Signature against the associated public certificates. The cryptographic module keeps authentication results in volatile memory, whose content is zeroized if power is lost. The module uses factory-preset authentication data (SID) to authenticate the Manufacturer role. The module does not support concurrent operators.

The module supports three types of authentication methods for each role. The authentication methods are chosen once the identity's account has been created. CMAC authentication is mandate for Crypto-Officer in order to access DOWNLOAD FIRMWARE service.

Authentication protocol is challenge-response against the nonce challenge generated by the module. The operator calculates the response using the selected authentication method and credential, and sends it back to the module. Authentication fails if the response does not match to what the module calculates using the same method and credential. It passes otherwise.

Role	Type of Authentication	Authentication Method
Crypto Officer (CO)	Identity Based	CMAC
		HMAC
		RSA Signature
User (U)	Identity Based	CMAC
		HMAC
		RSA Signature
Manufacturer (M)	Identity Based	CMAC
		HMAC
		RSA Signature

Table 6 Identification and authentication policy

CMAC - Strength of Authentication

The cipher algorithm used is AES-256 which can provide 256 bits of security. This key strength is equivalent to 2^{256} = 1.16×1077 random tries and is less than 10-6. The module runs at internal clock speed of 150 MHz (1.5×108 clock cycles per second). In the extreme case that the module executes one authentication check per clock cycle, then the probability of success within a one-minute period is 1 in 1.29 ×1067 random tries which is less than 10^{-5}.

HMAC - Strength of Authentication

The hash function used is SHA-256 which can provide up to 256 bits of security for HMAC (note SP 800-57). The shared secret it uses is also 256 bits in length. This key strength is equivalent to $2^{256} = 1.16\times10^{77}$ random tries which is less than 10^{-6}. In the extreme case that the module executes one authentication check per clock cycle, then the probability of success within a one-minute period is 1 in 1.29×10^{67} random tries which is less than 10^{-5}.

RSA Digital Signature - Strength of Authentication

External entities are authenticated using RSA-2048 digital signature schemes. The hash function used is SHA-256 which can provide up to 128 bits of security for digital signature (note SP 800-57). RSA-2048 provides 112 bits of key strength (note SP 800-57) which is equivalent to a probabilistic success rate of one in $2^{112} = 5.2\times10^{33}$ random tries which is less than 10^{-6}. In the extreme case that the module executes one authentication check per clock cycle, then the probability of success within a one-minute period is 1 in 5.78×10^{23} random tries which is less than 10^{-5}.

FIPS Approved Services - Keys, CSPs, and Types

Table 7 shows the FIPS approved cryptographic services with regard to Keys, CSPs and the corresponding Types that the module provides. Types of access are READ (R), WRITE (W), and EXECUTE (E). Access type “READ” refers to reading Keys or CSPs from their storage locations. Access type “WRITE” refers to creating, updating, or deleting Keys and/or CSPs from their storage locations. Access type “EXECUTE” refers to using Keys or CSPs to perform cryptographic functions.

Service	Role(s)	Keys & CSPs	Algorithm Cert.	RWE
KEY AGREEMENT	M, U, CO	$K_{KAS-PUB}$ $SECRETE_{KAS}$ KM_{KAS} CSP_{ID-M} CSP_{ID-CO} CSP_{ID-U} $DRBG_{SDM}$ $DRBG_{SV}$ $DRBG_{RB}$	RSA RSADP RSASP1 HMAC CMAC DRBG	R, E R, E W R, E R, E R, E W, E W, E R, E
SETUP KDF SEED KEY	M, U, CO	KM_{KAS} $K_{KDK-SESSION}$	N/A	R W
SETUP SESSION KEY	M, U, CO	$K_{KDK-SESSION}$ $K_{SESSION}$ $DRBG_{SDM}$ $DRBG_{SV}$	KDF DRBG	R, E W W, E W, E

		$DRBG_{RB}$		R, E
SET AND GET AUTHENTICATE COUNTER VALUE	M, U, CO	$K_{SESSION}$ CV $DRBG_{SDM}$ $DRBG_{SV}$ $DRBG_{RB}$	DRBG AES	R, E W, R W, E W, E R, E
AUTHENTICATE	M, U, CO	$K_{SESSION}$ (K_{CMAC-M} /K_{HMAC-M} /K_{RSA-M}) /($K_{CMAC-USER}$ /$K_{HMAC-USER}$ /$K_{RSA-MUSER}$ /($K_{CMAC-CO}$ /$K_{HMAC-CO}$ /K_{RSA-CO}) CSP_{ID-M} /CSP_{ID-CO} /$CSP_{ID-USER}$ $DRBG_{SDM}$ $DRBG_{SV}$ $DRBG_{RB}$	AES RSA HMAC CMAC DRBG	R, E (R, E /R, E /R, E) (R, E /R, E /R, E) (R, E /R, E /R, E) R R R W, E W, E R, E
CREATE IDENTITY DELETE IDENTITY	M, CO	$K_{SESSION}$ CSP_{ID-CO} /$CSP_{ID-USER}$	AES	R, E W /W
MODIFY AUTHENTICATION CREDENTIAL	M, U, CO	$K_{SESSION}$ CSP_{ID-CO} /$CSP_{ID-USER}$	AES	R, E W /W
SETUP MEDIA DATA KEY	CO	K_{MEK} $DRBG_{SDM}$ $DRBG_{SV}$ $DRBG_{RB}$	DRBG KDF	W W, E W, E R, E
SECURE DATA WRITE SECURE DATA READ	U, CO	CSP_{ID-CO} /$CSP_{ID-USER}$ $K_{SESSION}$	AES HMAC CMAC RSA	R, E /R, E R, E
MEDIA DATA WRITE MEDIA DATA READ	U	K_{MEK}	AES	R, E
DOWNLOAD FIRMWARE	CO	$K_{SESSION}$ $K_{CMAC-CO}$ $K_{PROG-CTL}$	AES CMAC	R, E R, E R, E
SHOW STATUS	M, U, CO	N/A	N/A	N/A
ON-DEMAND SELF-TEST	M, U, CO	N/A	AES SHS HMAC CMAC	N/A

			DRBG RSA KDF	
ENCRYPT/DECRYPT ON DEMAND	U, CO	$K_{SESSION}$	AES	R, E
ZEROIZE REVERT	M, U, CO	All CSPs in NVM except CSP_{ID-M}	N/A	W
ZEROIZE ALL PANIC BUTTON	CO	KDM_{BASE} CFG_{BASE} $K_{KDK-CTL}$ $K_{CSPS-CTL}$ $K_{PROG-CTL}$ $K_{DATA-CTL}$ $K_{KDK-NVM}$	N/A	W

Table 7 FIPS approved services

Service	Role(s)	Keys & CSPs	RWE
I^2C LOAD MEDIA DATA KEY	CO, U	K_{MEK}	W
API LOAD MEDIA DATA KEY	CO, U	K_{MEK}	W
MEDIA DATA WRITE	CO, U	K_{MEK}	R, E
MEDIA DATA READ	CO, U	K_{MEK}	R, E
ON-DEMAND SELF-TEST	CO, U	N/A	N/A

Table 8 Non-FIPS Approved Services

Section 4 - Physical Security

The cryptographic module is a single-chip design that stacks an NVM (Non-Volatile Memory) die on top of a controller die in a single ASIC package. The module adopts QFN package which is a standard production-grade design without any doors or removal covers. Any Attempt to remove the hard, opaque, tamper evident coating of the packaging will show obvious signs of tamper and has a high probability of causing serious damage to the module. The module hardness testing was performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

The NVM is used for storing controller firmware and CSPs. Its wirings are concealed in the package to prevent from probing the electrical signals. The contents of the NVM are AES encrypted with a 256-bit key derived using materials stored in the One-Time Programmable (OTP) memories. This key derivation scheme is tested and follows the NIST SP 800-108 standard. The contents of the OTP are unique to each chip.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque production grade packaging	As specified per operator policy	Visually inspect the chip for signs of damage.

Table 9 Inspection, Testing of Physical Security Mechanisms

Section 5 - Key Management

Key Storage

The module has four types of storage where Cryptographic Keys and Critical Security Parameters (CSPs) may be stored. They are:

- Registers, volatile
- OTP, non-volatile
- SRAM, volatile
- NVM, non-volatile

Key Zeroization

Key zeroization can be acquired through services. The services that zeroize or destroy cryptographic keys and CPSs include DELETE_IDENTITY, REVERT, ZEROIZE, and ZEROIZE_ALL. The ZEROIZE_ALL service destroys all storage devices including the OTP, rendering the module unusable. Ephemeral keys are destroyed automatically upon hardware reset, power removal, operator logout, end of life, or completion of authentication service.

Table 10 describes CSPs contained in the module:
.

Key/CSP	Use	Storage	Output	Gen/Establish	Destruction
KDM_{BASE}	Key Derivation Materials.	O[3]	N/A	Hardcoded	ZEROIZE ALL
CFG_{BASE}	Basic configuration settings.	O	N/A		
$K_{KDK-ROOT}$	Root Key Derivation	S,R	N/A	NIST SP 800-108 KDF	ZEROIZE, hardware reset, remove power, ZEROIZE ALL
$K_{KDK-CTL}$	Controller Key Derivation Key. Used as the derivation key to derive $K_{CSPS-CTL}$, $K_{PROG-CTL}$, and $K_{DATA-CTL}$		N/A		
$K_{CSPS-CTL}$	Controller owned 256-bit key to AES encrypt/decrypt and authenticate (using CMAC) program code (RAM code) stored in NVM.		N/A		
$K_{PROG-CTL}$	Controller owned 256-bit key to AES encrypt/decrypt and authenticate (using CMAC) program code (RAM code) stored in NVM.		N/A		
$K_{DATA-CTL}$	Controller owned 256-bit key to AES encrypt/decrypt and authenticate (using CMAC) data stored in NVM.		N/A		
$K_{KDK-NVM}$	NVM Key derivation key used as the derivation key to derive a series of keys.	S	N/A		
CSP_{ID-M}	Authentication CSP of Manufacturer identity	S,R,N	N/A	Hardcoded	ZEROIZE, hardware reset, remove power, ZEROIZE ALL
K_{HMAC-M}	256-bit key used for generating HMAC authentication code for Manufacturer identity.		N/A		
K_{CMAC-M}	256-bit key used for generating CMAC authentication code for Manufacturer identity.		N/A		
K_{RSA-M}	RSA-2048 public key with self-signed signature for Manufacturer identity.		N/A		
$K_{HMAC-CO}$	256-bit key used for generating HMAC authentication code for CO.	S,R,N	N/A	Input electronically	ZEROIZE, hardware reset, remove power, ZERIOZE ALL, REVERT
$K_{CMAC-CO}$	256-bit key used for generating CMAC authentication code for CO.		N/A		
K_{RSA-CO}	RSA-2048 public key with self-signed signature for CO.		N/A		
CSP_{ID-CO}	Authentication CSP of Crypto-Officer identity		N/A		
$K_{HMAC-USER}$	256-bit key which is used for generating HMAC		N/A		ZEROIZE, hardware reset, remove power,

[3] O = OTP, R = Registers, S = SRAM, N = NVM

	authentication code for USER.				ZEROIZE ALL, REVERT, DELETE USER service
$K_{CMAC-USER}$	256-bit key which is used for generating CMAC authentication code for USER.		N/A		
$K_{RSA-USER}$	RSA-2048 public key with self-signed signature for User.		N/A		
$CSP_{ID-USER}$	Authentication CSP of User identity.		N/A		
CV	Authentication counter values.	S,R	AES-256 encrypted with $K_{SESSION}$	Hash-DRBG	ZEROIZE, hardware reset, remove power
$K_{KAS-PUB}$	RSA-2048 public key for Key Agreement Scheme.		N/A	Input electronically.	ZEROIZE, hardware reset, remove power, completion of KAS service
SECRET E_{KAS}	Secret string for Key Agreement Scheme.		RSA-2048 encrypted with $K_{KAS-PUB}$	Hash-DRBG	
KM_{KAS}	Keying material derived from Key Agreement Scheme.		N/A	KAS Scheme	ZEROIZE, hardware reset, remove power, new KAS request
$K_{KDK-SESSION}$	Key Derivation Key for session keys.		N/A	Derived from KM_{KAS}	ZEROIZE, hardware reset, remove power, end of life-time
$K_{SESSION}$	Session Key.		N/A	NIST SP 800-108 KDF	
K_{MEK}	Media Encryption Key.		N/A	NIST SP 800-108 KDF	ZEROIZE, hardware reset, remove power, user logout
$DRBG_{SDM}$	Hash-DRBG seeding materials include random bits from an entropy source, nonce, and user strings.	S,R	N/A	NDRNG	Un-instantiation of DRBG, ZEROIZE, hardware reset, or remove power.
$DRBG_{SV}$	Hash-DRBG state vectors.		N/A		
$DRBG_{RB}$	Hash-DRBG generated random bits ready to consume.		N/A		

Table 10 Keys and CSPs

Section 6 - EMI/EMC

The X-Wall MX+ module meets Class B (Home Use) FCC requirements.

Section 7 - Self Tests

The module is designed to execute a self-test routine at power-up or after a hardware reset. If any test fails, the module will enter the error state and halt all cryptographic services; while reporting the error condition. In this instance, the module will not allow use of the corrupted CSPs. When the module encounters an error, it does not continue the execution of further tests, but rather enters the error state immediately. In the event of any self-test failure, the operator may restart the module to clear the error, however in the event of a power-up self-test failure, the module will be considered defective and no longer usable.

Power-Up/Hardware Reset Self-Test

Power-up self-tests on cryptographic algorithms are automatically executed without operator intervention. Operators can also initiate the power-up self-tests on-demand using the SELF TEST service. While the self-test routine executes, both the DATA and ERR LEDs are ON. The module turns OFF the DATA LED when it completes self-tests. The ERR LED remains ON if any error is encountered. Otherwise, it shall be turned OFF.

Firmware Integrity Tests

The module contains three integrity tests to ensure that all module components are protected against modification. At power-up, the first firmware integrity test computes an HMAC-SHA-256 value over the ROM content and checks it against the digest attached to the end of the ROM. Then, the OTP integrity test is carried out using a SHA-256 hash over all OTP content. And finally, a hierarchy of key derivation keys is generated using materials stored in the OTP. Among them a CMAC key is derived to compute the CMAC-AES-256 value over the NVM content and check it against the digest attached to the NVM.

Known Answer Tests

The module contains a known answer test (KAT) for the following cryptographic algorithms:

- AES Encrypt Known Answer Test;
- AES Decrypt Known Answer Test;

- AES-256-CMAC Known Answer Test;
- SHA-256 Known Answer Test (embedded algorithm);
- HMAC-SHA-256 Known Answer Test;
- HMAC-SHA-256 Known Answer Test (embedded algorithm);
- NIST SP 800-90A DRBG (Hash Based) Known Answer Test;
- NIST SP 800-108 KDF Known Answer Test;
- RSA 2048 Primitive Known Answer Test; and
- RSA 2048 Sign/Verify Known Answer Test.

Conditional Self-Tests

- RSA 2048 Pair-wise Consistency Test;
- Firmware Load Test (CMAC);
- Continuous DRBG Test; and
- Continuous NDRNG Test.

Other Self-Tests

- HMAC-SHA-256 Message Test (Firmware RAM Code); and
- NIST SP 800-90A, Section 11.3 (Instantiate, Generate, Reseed, Uninstantiate).

Section 8 - Design Assurance

Secure Module Distribution

The cryptographic module is shipped from the factory in its uninitialized state and is delivered to the customer by bonded courier.

Section 9 - Mitigation of Other Attacks

The cryptographic module has no design to mitigate against any specific attacks outside the scope of FIPS 140-2.

.