FIPS 140-2 Security Policy

for

Marvell Semiconductor, Inc.

Solaris 2 Cryptographic Module

Hardware Version: 88i8925, 88i8922, 88i8945, and 88i8946

Firmware Version: Solaris2-FIPS-FW-V1.0

Document Version: 1.7

1. Module Description

Solaris 2 is a single-chip hardware cryptographic module that offers a set of services that can be used to establish ownership of the hard disk drive, to perform cryptographic services to encrypt data stored on the hard disk drive, and to support authentication services for access control management of hard disk drive information and data. Solaris 2 is a highly integrated System-on-Chip (SOC) solution customized for high density hard disk drives. It employs the latest read/write channel technology with advanced error detection and correction capabilities. Solaris 2 integrates an AES hardware engine to support full drive encryption (FDE). Solaris 2 features an efficient single-chip security architecture that supports access control, authentication, and key management features. FIPS-Approved algorithms supported include the following: AES, SHA, HMAC, RSA and RNG.

The threat model Solaris 2 covers is the case of the stolen laptop that is powered down. The confidentiality of the information and data on a stolen laptop must be maintained even if the hard disk drive is removed and attempts are made to recover the data directly from the media. The module addresses this problem by encrypting all of the data on the laptop hard disk drive.

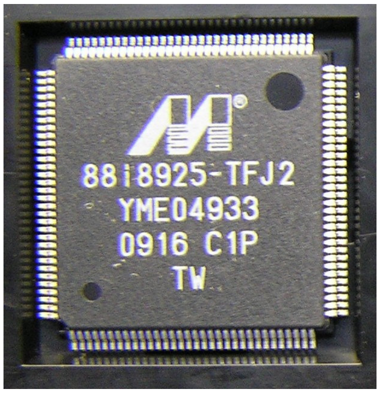
The module was designed to meet requirements of FIPS 140-2 at Security Level 2.

The cryptographic boundary of the module corresponds to the physical boundary of the chip packaging. Physical ports of the module are comprised by hardware pins.

The module always runs in the FIPS 140-2 Approved mode of operation and does not implement a Non-Approved mode of operation.

The Solaris 2 module as integrated in the reference design is not a shipping product. It will only be used for testing purposes. Solaris 2 module could potentially be integrated into a system level product by Marvell's customers targeted for production; however such configurations were not tested during the FIPS 140-2 testing process.

Figure 1. A photograph of the module.



2. Roles, Services and Authentication

The module provides the following roles: User and Crypto Officer.

The Crypto Officer configures the module and manages its cryptographic functionality.

The User utilizes the cryptographic services provided by the module.

The module supports role-based authentication. A username/password combination is utilized to authenticate the operator.

The module does not allow concurrent operators. If an authenticated session exists for a particular operator Operator 1, then another Operator 2 may only login after Operator 1 closes the session.

The password length for the operators is enforced by the module and must comprise of at least 6 alphanumeric characters.

The module provides the following services:

Service	Role	Access to Cryptographic Keys and CSPs R- read or use W – write or generate Z – zeroize
Initial Setup of the Module (will set the Crypto Officer password)	Crypto Officer	W
Log In (will access User or Crypto Officer password)	User Crypto Officer	R
Log Out	User Crypto Officer	N/A
Download RNG Seed and Seed Key (AES wrapped using Entropy Download Key)	Crypto Officer	R,W
Encrypt or Decrypt Stored Data (will use AES Media Encryption Keys)	User Crypto Officer	R
Re-Encrypt Stored Data (decrypt using an old key AES Media Encryption Key and encrypt using a new AES Media Encryption Key)	User Crypto Officer	R

Generate AES Media Encryption Keys using the ANSI X9.31 RNG)	Crypto Officer	W
Re-Purpose (will reset the module to factory defaults, zeroize passwords and re-generate Media Encryption Keys)	Crypto Officer	Z, W
Add User (will set the user password)	Crypto Officer	W
Delete User (will zeroize the password for this user)	Crypto Officer	W
Set User Password	User Crypto Officer	W
Set Crypto Officer Password	Crypto Officer	W
Upload Firmware to the Module (will verify RSA signature using RSA Firmware Upload Public Key)	Crypto Officer	R
Get Status of the Module	Crypto Officer User	N/A
Zeroize Keys and CSPs (will zeroize all unencrypted keys and CSPs)	Crypto Officer	Z
Run Self-Tests	Crypto Officer User	N/A

3. Security Functions

The table below lists Approved cryptographic algorithms employed by the module.

Algorithm	Certificate #
AES encrypt/decrypt	1153
AES encrypt/decrypt	723
RSA ANSI X9.31 signature verification	545
HMAC message authentication code	656
SHS secure hash	1067
ANSI X9.31 random number generator	638

The module does not implement non-Approved cryptographic algorithms.

4. Key Management

The following cryptographic keys are supported by the module.

Name and Type	Generation or establishment	Algorithm	Usage
AES Media Encryption Keys	Generated by the module	AES	Encryption of the storage data
AES Key Encryption Key	Pre-installed by the manufacturer	AES	Encryption of the keys and CSPs in non-volatile memory
RNG Seed Key	Input into the module encrypted using the Entropy Download Key	ANSI X9.31 RNG	Set the initial state for the RNG
RSA Firmware Upload Public Key	Pre-installed by the manufacturer	RSA	Firmware signature verification on upload
AES Entropy Download Key	Pre-installed by the manufacturer	AES	Key-encrypting-key for the RNG seed and seed key. Used to input the encrypted RNG seed and seed key

5. Self Tests.

The module runs a set of self-tests on power-up. If one of the self-tests fails, the module transitions into an error state, where all data output and cryptographic operations are disabled.

The module runs power-on self-tests for the following algorithms.

Algorithm	Test
AES implementations	Known Answer Test for each implementation
RNG	Known Answer Test
SHS	Covered by HMAC Test and RSA test
HMAC	Known Answer Test
RSA	Known Answer Test

The module implements a power on integrity-check using a 16-bit checksum.

The module implements the continuous RNG test for the ANSI X 9.31 RNG.

A firmware upload test using RSA signature is performed during the firmware upload.

6. Crypto Officer Guidance

6.1 Secure Setup Instructions.

The following steps shall be executed by the Crypto Officer to perform the initial setup of the product in the FIPS mode of operation.

1. Power the module on. This will cause the module to perform power-on self-tests.

2. Issue the TAKE_OWNERSHIP command to set the Crypto Officer username and password. To issue this command one is required to enter the default password.

   Note: it is advisable for the Crypto Officer to take ownership as soon as possible after receiving the device to prevent other parties from accessing the device.

3. Now the module is running in the FIPS mode.

6.2 Secure Operation

The following rules shall be adhered to by the Crypto Officer to achieve secure operation of the module:

1. Store the module in a physically secure location until the Secure Setup (Section 6.1) has been performed.

2. Choose a strong, non-dictionary based password composed of at least six alphanumeric characters. Do not create insecure physical records of the password.

3. Change the password on a regular basis.

4. In case the module needs to be discarded, perform key zeroization before discarding the module.

5. Close an open authenticated session as soon as all requested services have been performed by the module.

7. User Guidance

7.1 Secure Operation

The following rules shall be adhered to by the User to achieve secure operation of the module:

1. Choose a strong, non-dictionary based password that has at least 6 alphanumeric characters. Do not create insecure physical records of the password.

2. Change the password on a regular basis.

3. Close an open authenticated session as soon as the all requested services have been performed by the module.